ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN ALGORITMA PENGAMANAN DATA TINGKAT LANJUT UNTUK PERLINDUNGAN INFORMASI

SKRIPSI

OLEH
ISTIQOMAH
NIM. 12610037

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2018

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN ALGORITMA PENGAMANAN DATA TINGKAT LANJUT UNTUK PERLINDUNGAN INFORMASI

SKRIPSI

Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memeroleh Gelar Sarjana Matematika (S.Mat)

Oleh
Istiqomah
NIM. 12610037

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2018

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN ALGORITMA PENGAMANAN DATA TINGKAT LANJUT UNTUK PERLINDUNGAN INFORMASI

SKRIPSI

Oleh
Istiqomah
NIM. 12610037

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 04 Desember 2017

Pembimbing I	Pembimbing II
H. Wahyu H. Irawan, M.Pd	Abdul Aziz, M.Si
NIP. 19710420 200003 1 003	NIP. 19760318 200604 1 002

Mengetahui,
Ketua Jurusan Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN ALGORITMA PENGAMANAN DATA TINGKAT LANJUT UNTUK PERLINDUNGAN INFORMASI

SKRIPSI

Oleh
Istiqomah
NIM. 12610037

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 22 Desemeber 2017

Penguji Utama	: Mohammad Jamhuri, M.Si	…… …
Ketua Penguji	: Dr. Abdussakir, M.Pd	……
Sekertaris Penguji	: H. Wahyu H. Irawan, M.Pd	……
Anggota Penguji	: Abdul Aziz, M.Si	……

Mengetahui,
Ketua Jurusan Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama	:	Istiqomah
NIM	:	12610037
Jurusan	:	Matematika
Fakultas	:	Sains dan Teknologi
Judul Skripsi	:	Enkripsi dan Dekripsi Pesan Menggunakan Algoritma Pengamanan Data Tingkat Lanjut untuk Perlindungan Informasi

menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya sendiri, bukan merupakan pengambilan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar rujukan. Apabila di kemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 5 Mei 2018
Yang membuat pernyataan,

Istiqomah
NIM. 12610037

MOTO

Manusia dinilai dari perbuatan dan manfaat yang diberikan.

Menjadi mata air di manapun, kapanpun dan bagaimanapun.

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk ayahanda Ach. Muhadjir Ismail dan ibunda Salehati yang senantiasa dengan ikhlas mendoakan, memberi dukungan, motivasi, dan restunya kepada penulis dalam menuntut ilmu serta selalu memberikan teladan yang baik bagi penulis. Untuk adik tersayang Muhishah Hidayati dan keluarga besar Ismail yang selalu memberikan doa dan motivasi kepada penulis.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah Swt. atas rahmat, taufik serta hidayah-Nya sehingga penulis dapat menyelesaikan penulisan skripsi yang berjudul "Enkripsi dan Dekripsi Pesan Menggunakan Algoritma Pengamanan Data Tingkat Lanjut untuk Perlindungan Informasi" ini dengan baik. Shalawat dan salam semoga senantiasa tercurahkan kepada Muhammad Saw. yang telah menuntun umat manusia dari jaman jahil menuju jaman Islam.

Selanjutnya penulis ucapkan terima kasih kepada semua pihak yang telah mengarahkan dan membimbing sehingga skripsi ini dapat diselesaikan dengan baik. Ucapan terima kasih penulis sampaikan kepada:

1. Prof. Dr. Abdul Haris, M.Ag, selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Usman Pagalay, M.Si, selaku ketua Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. H. Wahyu H. Irawan, M.Pd, selaku dosen pembimbing I yang telah banyak memberikan arahan, nasihat, motivasi, dan berbagai pengalaman yang berharga kepada penulis.
5. Abdul Aziz, M.Si, selaku dosen pembimbing II yang telah memberikan saran dan bantuan dalam penulisan skripsi ini.

6. Segenap sivitas akademika Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang, terutama seluruh dosen atas segala ilmu dan bimbingannya.
7. Ayah dan ibu tercinta yang telah mencurahkan kasih sayang, doa, bimbingan, dan motivasi hingga selesai skripsi ini.
8. Saudara-saudara tersayang yang telah memberikan dukungan dan semangat kepada penulis.
9. Seluruh teman-teman di Jurusan Matematika angkatan 2012 yang berjuang bersama-sama untuk meraih mimpi dan terima kasih untuk kenang-kenangan indah yang dirajut bersama dalam menggapai impian.
10. Keluarga besar Himpunan Mahasiswa dan Alumni Mashduqiah Malang (HAMMASAH) yang telah memberikan dukungan, motivasi, dan kenangan yang tak terlupakan kepada penulis.
11. Semua pihak yang ikut membantu dalam menyelesaikan skripsi ini baik moril maupun materiil.

Akhirnya penulis hanya dapat berharap, dalam penulisan skripsi ini dapat ditemukan sesuatu yang dapat memberikan manfaat dan wawasan yang lebih luas atau bahkan hikmah bagi penulis, pembaca, dan bagi seluruh mahasiswa.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Malang, Mei 2018

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

Istiqomah. 2017. **Enkripsi dan Dekripsi Pesan Menggunakan Algoritma Pengamanan Data Tingkat Lanjut untuk Perlindungan Informasi**. Skripsi. Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) H. Wahyu H. Irawan, (II) Abdul Aziz, M.Si.

Kata Kunci: enkripsi, dekripsi, pesan.

Enkripsi adalah suatu proses perubahan pesan yang dapat dimengerti (plainteks) menjadi suatu pesan yang sulit dimengerti (chiperteks), sedangkan proses perubahan chiperteks menjadi plainteks disebut dekripsi. Proses enkripsi dan dekripsi pada penelitian ini membutuhkan satu kunci rahasia yang dalam perhitungannya menggunakan ekspansi kunci untuk menguatkan pesan dengan tiga kali perputaran atau tiga ronde.

Penelitian ini bertujuan untuk mengetahui proses enkripsi dan dekripsi pesan menggunakan koefisien polinomial sebagai teknik untuk mengamankan pesan. Adapun metode yang digunakan dalam penelitian ini adalah metode kepustakaan dengan langkah-langkah: 1) menentukan pesan dan panjang kunci, 2) merepresentasikan pesan dan kunci dalam bentuk heksadesimal, 3) membangkitkan atau mengekspansi kunci, dan 4) melakukan proses enkripsi pesan menggunakan kunci dengan teknik transformasi *SubBytes*, *ShiftRows*, *MixColumns*, *AddRoundKey*. Selanjutnya metode yang digunakan untuk mendekripsikan pesan dalam penelitian ini menggunakan langkah-langkah: 1) menentukan pesan tersandi (chiperteks) dan panjang kunci, 2) merepresentasikan pesan dan kunci dalam bentuk heksadesimal, dan 3) melakukan proses dekripsi pesan menggunakan kunci yang sama dengan teknik transformasi *InvSubBytes*, *InvShiftRows*, *InvMixColumns*, dan *AddRoundKey*.

Hasil penelitian menunjukkan bahwa algoritma pengamanan data tingkat lanjut dapat diterapkan untuk mengamankan pesan rahasia. Diperoleh kunci yang sama antara pengirim pesan dan penerima pesan dengan alur kunci yang berlawanan, yaitu $K = K_1K_2K_3 = K_3K_2K_1$. Proses enkripsi dilakukan dengan perhitungan menggunakan kunci yang berbeda pada setiap ronde yang merupakan hasil dari ekspansi kunci dengan urutan kunci ronde pertama, kedua dan ketiga, sedangkan proses dekripsi dilakukan dengan perhitungan menggunakan transformasi invers menggunakan kunci yang sama yang merupakan hasil dari ekspansi kunci dengan tiga kali putaran atau tiga ronde dengan urutan kunci ronde ketiga, kedua, dan pertama.

ملخص

استقامة ٢٠١٧. **تشفير اسفرة الرسالة باستخدام خوارزميات أمان البيانات المتقدمة لحماية المعلومات**. بحث الجمعي .شعبة الرياضيات .كلية العلوم والتكنولوجيا الجامعة الإسلامية الحكومية مولانا مالك إبراهيم مالانج. المشرف (١) الحاج وحي هنكي إراوان الماجيستير المشرف (٢) عبد العزيز الماجستيرز.

كلمات الرئيسية : التشفير ، فك التشفير ، رسالة.

التشفير هو عملية الترميز تحويل الرسالة المفهومة يسمى بنص المجرد إلى الرسالة مصعبة يسمى بنص مشفر، والعكس يطلق فك التشفرة. فى عملية التشفير وفك التشفير تحتاج المفتاح السري المتفقة على المرسل و المرسل. في هذا البحث الجامعي بحثت الباحثة تشفير وفك تشفير الرسالة باستخدام توسع رئيسي أو أساسي جيل إلى تعزيز الرسالة التي لم يتم سرقتها بسهولة باستخدام ثلاثة أو ثلاث جولات.

تهدف هذه الدراسة إلى تحديد رسائل التشفير وعملية فك التشفير باستخدام معاملات متعدد الحدود كطريقة لتأمين الرسائل. الطريقة المستخدمة في هذه الدراسة هي الخطوات التالية: ١) تحديد الرسالة وطول المفتاح، ٢) يمثل رسالة والمفتاح في شكل عشري، ٣) توليد أو توسيع المفتاح، ٤) يتم تشفير الرسالة باستخدام مفتاح التحول تقنيات *SubBytes*، *ShiftRows*، *MixColumn*، *AddRoundKey*. وعلاوة على ذلك، فإن الطريقة المستخدمة في فك تشفير الرسالة في هذه الدراسة هي باستخدام الخطوات التالية: ١) تحديد رسالة مشفرة *(ciphertext)* وطول المفتاح، ٢) يمثل رسالة والمفتاح في

شكل عشري، ٣) تنفيذ عملية فك الرسالة باستخدام نفس المفتاح لتقنيات التحول *AddRoundKey ،InvMixColumn ،InvshiftRows ،InvSubBytes.*

تظهر النتائج أن خوارزميات أمان البيانات المتقدمة يمكن تطبيقها لتأمين الرسائل السرية على عمليات التشفير وفك التشفير. حصلت على نفس المفاتيح بين المرسل والمرسل للرسالة، أن تتم عملية التشفير عن طريق تغيير عادي في *ciphertext* ويتم ذلك على حساب باستخدام مفاتيح مختلفة في كل جولة والتي هي نتيجة للتوسع أو إنشاء المفتاح، في حين تتم عملية فك التشفير عن طريق تغيير *ciphertext* يكون يتم تنفيذ نص عادي وحساباتها باستخدام التحويلات العكسية باستخدام نفس المفتاح الذي هو نتيجة لتوسيع المفتاح مع ثلاث جولات بترتيب المفتاح الثالث، ثم الثاني، ثم الثالث.

ABSTRACT

Istiqomah. 2017. **Encryption and Decryption of Message using Advanced Data Security Algorithms to Secure Information.** Thesis. Department of Mathematics, Faculty of Science and Technology, State Islamic University Maulana Malik Ibrahim Malang. Promotor: (I) H. Wahyu H. Irawan, M.Pd (II) Abdul Aziz, M.Si.

Keywords: Encryption, decryption, messages.

Encryption is an encoding massage from that can be understood referred to plaintext into a massage that is difficult to be understood referred ciphertext, while the opposite process is transforming chipertext into plaintext reffered to decryption. Encryption and decryption process this research need a secret key where in its calculation uses key expansion to strengthen the message by implementing three rounds process.

This aims of this study is to determine the encryption and decryption of message using polynomial coefficients as a technique to secure messages. This research used literature method by the following steps: 1) determining the message and key length, 2) representing the message and key in hexadecimal form, 3) generating or expand the key, and 4) performing the message encryption process using the key with SubBytes transformation, ShiftRows, MixColumns, AddRoundKey technique. The next method used to decrypt the message in this study uses the following steps: 1) determining the encrypted message (chiperteks) and key length, 2) representing the message and key in hexadecimal form, and 3) decrypting the message using the same key as the transformation technique InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey.

The research results show that advanced data security algorithms can be applied to determine the secret messages to process of encryption and decryption. It is obtained the same key between the sender and the receiver that is $K = K_1K_2K_3 = K_3K_2K_1$. Encryption process is done and calculating by using a different key in each round which is the result of expansion key, while the decryption process is done decoding calculations using inverse transforms and uses same key which is the result of a key expansion by three rounds or three rounds.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Sejauh abad ke dua puluh satu, teknologi penyimpan data menjadi salah satu pokok utama yang berkembang dengan pesat. Dikarenakan banyak pengguna menginginkan kerahasiaan dalam perlindungan data sehingga memerlukan suatu penyimpanan yang aman. Data-data elektrik yang bersifat program menjadi sebab perlunya data pelindung yang bersifat program. Terkait dengan perlindungan data, keamanan menjadi penting sebagai tanggung jawab setiap orang dalam memberikan perlindungan yang memadai. Di antara data-data bersifat elektrik mengandung unsur rahasia. Beberapa jenis data yang perlu diamankan yaitu, data dokumen, data usaha, data yang berupa informasi, dan lain sebagainya (Ariyus, 2006:9).

Keamanan data pada lalu lintas jaringan digunakan untuk menjaga privasi. Dalam ilmu matematika terdapat konsep aljabar yang digunakan untuk mengamankan data yang disebut kriptografi. Kriptografi berasal dari bahasa Yunani, menurut bahasa dibagi menjadi dua *kripto* dan *graphia*, *kripto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain (Ariyus, 2006:9).

Al-Quran juga menganjurkan untuk menjaga rahasia dan informasi tertentu yang dianggap penting yaitu terdapat di dalam surat an-Nisa' ayat 58 yang berbunyi:

۞ إِنَّ ٱللَّهَ يَأۡمُرُكُمۡ أَن تُؤَدُّواْ ٱلۡأَمَٰنَٰتِ إِلَىٰٓ أَهۡلِهَا وَإِذَا حَكَمۡتُم بَيۡنَ ٱلنَّاسِ أَن تَحۡكُمُواْ بِٱلۡعَدۡلِۚ إِنَّ ٱللَّهَ نِعِمَّا يَعِظُكُم بِهِۦٓۗ إِنَّ ٱللَّهَ كَانَ سَمِيعَۢا بَصِيرٗا ٥٨

"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, (dan menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha Mendengar lagi Maha Melihat".(QS an-Nisa'/4:58).

Firman Allah Swt. dalam surat an-Nisa' ayat 58 menjelaskan bahwa Allah Swt. menyuruh manusia untuk menyampaikan amanat kepada orang yang berhak menerimanya. Selain orang yang berhak menerima amanat tersebut maka orang lain tidak boleh mengetahuinya.

Dengan adanya kemungkinan penyadapan informasi, maka aspek keamanan dalam pertukaran informasi menjadi penting. Pada saat ini, pertukaran data atau informasi sering dilakukan sehingga aspek keamanan terhadap isi dokumen perlu untuk mendapat perhatian khusus agar tidak jatuh ke tangan orang-orang yang tidak bertanggung jawab dan disalahgunakan. Pengamanan dilakukan dengan mengenkrip (menyandi) informasi dengan suatu kunci khusus. Sebelum data dienkrip maka dinamakan plainteks dan setelah data dienkrip dengan suatu kunci maka dinamakan chiperteks. Selanjutnya data yang telah dienkripsi didekripsikan (diuraikan) kembali seperti bentuk semula.

Menurut Ariyus (2006) berdasarkan kunci algoritma, kriptografi dibagi menjadi menjadi algoritma simetri, algoritma asimetri, dan fungsi *Hash*. Algoritma simetri atau algoritma klasik menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, sedangkan algoritma asimetri menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi.

Enkripsi dan dekripsi dalam kriptografi modern dapat dikatakan sebagai transformasi dari suatu teks biner menjadi teks biner yang lain dengan panjang

yang terbatas. Dalam hal ini, dibutuhkan suatu sistem untuk menghimpun nilai dan operator yang mungkin bagi teks biner untuk kegiatan transformasi. Peran matematika terhadap struktur aljabar dengan kondisi operator tambahan $(+)$, perkalian $(\times)$, dan invers dari matriks.

Algoritma pengamanan data tingkat lanjut adalah algoritma kriptografi kunci simetri dengan teknik enkripsi *block cipher* dan menggunakan sistem permutasi dan substitusi (*S-Box*) secara langsung terhadap naskah, serta menggunakan operasi eksklusif OR $(\oplus)$ (Kromodimoeljo, 2010:103). Penelitian sebelumnya dilakukan oleh Dedy Alyanto (2016) mengenai penyandian data rahasia menggunakan algoritma pengamanan data tingkat lanjut menggunakan sepuluh ronde dengan panjang kunci 128 bit, 192 bit dan 256 bit. Pengamanan data tingkat lanjut merupakan algoritma yang didasarkan pada tiga kriteria utama yaitu keamanan yang cukup kuat terhadap serangan, bebas digunakan tanpa harus membayar royalti, mudah digunakan dalam *hardware* maupun *software*, serta lebih efisien dan cepat apabila dijalankan dalam berbagai *platform* 8 bit hingga 64 bit. Dalam penelitian ini dikaji proses penyandian pesan menggunakan algoritma pengamanan data tingkat lanjut yang menerapkan implemenasi dari fungsi polinomial dan Lapangan Galois yang disederhanakan menjadi tiga ronde untuk efisiensi waktu dan mempermudah dalam proses penyandian pesan dengan menggunakan panjang kunci 128 bit.

Berdasarkan uraian tersebut penelitian ini secara khusus akan mengamati dan mengkaji proses enkripsi dan dekripsi maka peneliti mengambil judul "Enkripsi dan Dekripsi Pesan Menggunakan Algoritma Pengamanan Data Tingkat Lanjut untuk Perlindungan Informasi".

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka rumusan masalah pada penelitian ini adalah:

1. Bagaimana proses enkripsi menggunakan algoritma pengamanan data tingkat lanjut untuk perlindungan informasi?
2. Bagaimana proses dekripsi menggunakan algoritma pengamanan data tingkat lanjut untuk perlindungan informasi?

1.3 Tujuan Penelitian

Sesuai dengan rumusan masalah, maka tujuan penelitian ini adalah:

1. Untuk mengetahui proses enkripsi menggunakan algoritma pengamanan data tingkat lanjut untuk perlindungan informasi.
2. Untuk mengetahui proses dekripsi menggunakan algoritma pengamanan data tingkat lanjut untuk perlindungan informasi.

1.4 Manfaat Penelitian

Sesuai dengan tujuan penelitian, maka manfaat penelitian ini sebagai berikut:

1. Bagi Penulis

   Dapat memperkaya sumber pengetahuan tentang kriptografi khususnya aljabar pada proses enkripsi dan dekripsi untuk mengamankan data dan informasi.

2. Bagi pembaca

   Dapat menambah wawasan dan pengetahuan tentang kriptografi dan solusi bagi pihak-pihak yang menggunakan sarana informasi dan komunikasi untuk dapat mengamankan data dan informasi.

3. Bagi lembaga

   Dapat menambah bahan kepustakaan dan informasi pembelajaran mata kuliah yang berhubungan dengan kriptografi.

1.5 Batasan Masalah

Agar pembahasan pada penelitian ini tidak meluas, maka penulis memberikan batasan-batasan masalah sebagai berikut:

1. Pada proses enkripsi dan dekripsi menggunakan tabel *S-Box* (*Substitution-Box*) dengan teknik matriks ordo 4×4.
2. Panjang kunci yang digunakan dalam penelitian ini adalah 128 bit.

1.6 Metode Penelitian

Dalam penelitian ini, metode yang digunakan metode kepustakaan (*library research*), yaitu menggunakan literatur yang berkaitan dengan penelitian seperti buku, jurnal penelitian, tesis, skripsi, dan laporan penelitian. Untuk mencapai tujuan yang diinginkan maka langkah-langkah yang digunakan dalam penelitian ini adalah:

1. Menentukan kunci yang akan digunakan berupa kata, angka dan karakter sepanjang 16 bit.
2. Memasukkan setiap elemen kunci ke dalam sel matriks berukuran 4×4.
3. Melakukan ekspansi kunci atau perluasan kunci.
4. Melakukan enkripsi atau penyandian pesan asli (plianteks) ke dalam bentuk pesan tersandi (chiperteks) menggunakan kunci yang telah diperoleh dari hasil ekspansi kunci (dimulai dari kunci ronde pertama, kedua dan ketiga).

5. Melakukan dekripsi atau pengubahan chiperteks (pesan tersandi) ke dalam bentuk pesan asli (plainteks) menggunakan kunci yang telah diperoleh dari hasil ekspansi kunci (dimulai pada kunci ronde ketiga, kedua dan pertama).
6. Menarik kesimpulan.

1.7 Sistematika Penulisan

Penulisan Penelitian ini dibagi menjadi empat bab dan masing-masing bab dibagi dalam subbab sebagai berikut:

Bab I Pendahuluan

Bab ini berisi tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, metode penelitian, dan sistematika penulisan.

Bab II Kajian Pustaka

Bab ini menjelaskan tentang Lapangan (*Field)*, Lapangan Galois (2^8), Pengamanan Data Tingkat Lanjut, *SubBytes*, *ShiftRows*, *MixColumns*, *AddRoundkey*, Ekspansi kunci, *InvSubBytes*, *InvShiftRows*, *InvMixColumns*, algoritma kriptografi, algoritma simetri, algoritma asimetri, serta kajian agama
mengenai ilmu kriptografi.

Bab III Pembahasan

Bab ini menguraikan secara keseluruhan langkah-langkah yang disebutkan dalam metode penelitian dan menjawab semua rumusan masalah.

Bab IV Penutup

Bab ini berisi kesimpulan penelitian dan saran untuk penelitian selanjutnya.

BAB II

KAJIAN PUSTAKA

2.1 Lapangan (*Field*)

Definisi 1 Lapangan (*Field*)

Lapangan adalah gelanggang komutatif dengan elemen satuan dan semua unsur di R mempunyai invers terhadap operasi kedua kecuali elemen nol (identitas pada operasi pertama) (Raisinghania dan Aggarwal, 1980:314). Dengan kata lain, untuk setiap elemen bukan nol $p \in R$ ada $p^{-1} \in R$ sedemikian hingga $p \cdot p^{-1} = 1$ (Wahyudin, 1989:155).

Beachy dan Blair (1990:163) mengatakan bahwa suatu lapangan F dengan operasi $(+)$ dan $(\cdot)$ harus memenuhi aksioma-aksioma berikut:

i. Tertutup.

Untuk semua $a, b \in F$ maka jumlah $a + b$ dan hasil $a \cdot b$ berada dalam F.

ii. Bersifat asosiatif.

Untuk semua $a, b, c \in F$ berlaku

$a + (b + c) = (a + b) + c$ dan $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

iii. Bersifat komutatif.

Untuk semua $a, b, c \in F$ berlaku

$a + b = b + a$ dan $a \cdot b = b \cdot a$.

iv. Bersifat distributif.

Untuk semua $a, b, c \in F$ berlaku

$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ dan $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

v. Mempunyai elemen identitas.

Pada himpunan F terdapat satu elemen identitas pada operasi penjumlahan $(+)$, dinotasikan dengan 0. Sedemikian hingga untuk semua $a \in F$, $a + 0 = a$ dan $0 + a = a$. Pada himpunan F juga terdapat satu elemen identitas pada operasi perkalian $(\cdot)$, dinotasikan dengan 1. Sedemikian hingga untuk semua $a \in F$, maka $a \cdot 1 = 1 \cdot a = a$.

vi. Mempunyai elemen invers.

Untuk setiap $a \in F$, persamaan $a + x = 0$ dan $x + a = 0$, memiliki solusi $x \in F$ disebut invers penjumlahan dari a dan dinotasikan dengan $-a$. Untuk setiap $a \in F$, persamaan $a \cdot x = 1$ dan $x \cdot a = 1$, memiliki solusi $x \in F$ disebut invers perkalian dari a dan dinotasikan dengan a^{-1}.

2.1.1 Lapangan Galois (2^8)

Definisi 2 Polinomial

Polinomial $p(x)$ berderajat n, didefinisikan sebagai suatu fungsi berbentuk:

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \qquad (2.1)$$

dengan $\boldsymbol{a_i}$ adalah konstanta riil, $\boldsymbol{i = 0, 1, 2, \ldots, n}$ dan $\boldsymbol{a_n \neq 0}$, dengan:

x : merupakan peubah.

$a_0, a_1, a_2, \ldots, a_n$: merupakan nilai koefisien peubah x.

n : merupakan orde atau derajat persamaan.

(Munir, 2008:105).

Definisi 3 Lapangan Galois

Suatu lapangan dengan p^n elemen disebut lapangan Galois berorde p^n dan dinotasikan oleh $F(p^n)$ untuk p bilangan prima dan n bilangan asli (Sadikin, 2012:79).

Ditunjukkan bahwa untuk suatu bilangan prima p dan bilangan bulat positif n, terdapat lapangan Galois ($GF(p^n)$). Untuk $n = 1$, maka bilangan bulat modulo p adalah lapangan Galois berpangkat n.

Diberikan suatu gelanggang atas polinomial $GF(2^8)$ dengan elemen p. Jika p merupakan suatu nilai dari 0 atau 1 maka terbentuk:

$$b_7 + b_6 + b_5 + b_4 + b_3 + b_2 + b_1 + b_0$$

sebagai koefisien polinomial dan dapat dituliskan pada persamaan (2.2) berikut:

$$p(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^6 + b_3x^6 + b_2x^6 + b_1x^6 + b_0 \quad (2.2)$$

Persamaan (2.2) menjelaskan bahwa pangkat tertinggi dari polinomial GF(2^8) adalah x^7 (Sadikin, 2012:78).

Tipe lapangan Galois yang sering dipakai pada sistem kriptografi adalah $p = 2$ atau $GF(2^n)$. $GF(2^n)$ berbasis aritmetika modular polinomial $p(2^n)$ dengan:

$$p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x^0 + a_0 \quad (2.3)$$

Polinomial $p(x)$ disebut dengan polinomial tak tereduksi berderajat n yang koefisiennya adalah pada $GF(p)$. Koefisien 2_n adalah elemen pada $GF(2)$ dan $2_n \neq 0$. Karakteristik polinomial tak tereduksi $p(x)$ tidak dapat dibagi habis kecuali oleh dirinya sendiri dan 1. Misal elemen pada $GF(2^n)$ ditulis sebagai $f(x)$. Maka diperoleh:

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x^0 + a_0 \quad (2.4)$$

Polinomial $q(x) = x^8 + x^4 + x^3 + x + 1$ merupakan suatu polinomial tak tereduksi atas (2^8). Ini menunjukkan bahwa $GF(2^8)$ terdiri dari semua polinomial

$$p(a) = b_7a^7 + b_6a^6 + b_5a^5 + b_4a^4 + b_3a^3 + b_2a^2 + b_1a + b_0 \quad (2.5)$$

Dengan a merupakan variabel pada koefisien $b_i \in \{0, 1\}$ dengan penjumlahan dan perkalian yang direduksi dengan modulo $q(x)$.

Contoh 1:

Diberikan suatu elemen lapangan yang dinotasikan dalam bentuk polinomial yaitu:

$$a = x^6 + x^4 + x^2 + x + 1 \quad (2.6)$$

Jika elemen a direpresentasikan dalam koefisien biner maka diperoleh nilai $a = 01010111$. Dan jika direpresentasikan dalam bentuk heksadesimal dilambangkan dengan '57' yang mengacu pada tabel ASCII. Sehingga untuk mengoperasikan dua atau lebih elemen diperoleh:

$$a_1 = a^7 + a^6 + a^4 + a^2 + a \quad (2.7)$$

dengan koefisien 11010110 dalam bentuk biner dan dilambangkan dengan $D6$ dalam notasi heksadesimal yang mengacu pada tabel ASCII. Sedangkan,

$$a_2 = a^5 + a^3 + a^2 \quad (2.8)$$

dengan koefisien 00101100 dalam bentuk biner dan dilambangkan dengan $2C$ dalam notasi heksadesimal yang mengacu pada tabel ASCII.

Penjumlahan dua elemen lapangan berhingga didefinisikan sebagai operasi XOR (penjumlahan 2 elemen dengan modulo 2) per *bit* dengan notasi biner seperti pada tabel berikut:

Tabel. 2.1 Penjumlahan pada GF (2)

+	0	1
0	0	1
1	1	0

Sebagai akibatnya, maka penyederhanaannya merupakan operasi yang identik. Ekspresi berikut ini adalah ekivalen antara satu dengan lainnya (heksadesimal, *bit*, dan notasi polinomial) (Sadikin, 2012:79).

Contoh 2:

Misalkan

$$f(x) = a_{n-1}x^{n-1} + \cdots + a_0$$

dan,

$$g(x) = b_{n-1}x^{n-1} + \cdots + b_0$$

maka aturan penjumlahan polinomialnya sebagai berikut:

$$f(x) + g(x) = (a_{n+1} + b_{n+1})x^{n-1} + \cdots + (a_0 + b_0) \quad (2.9)$$

Diberikan:

$$f(x) = x^3 + x^2 + 1$$

$$g(x) = x^2 + x$$

Maka diperoleh:

$$\begin{aligned} f(x) + g(x) &= x^3 + x^2 + 1 + x^2 + x \\ &= (1+0)x^3 + (1+1)x^2 + (0+1)x + (1+0) \\ &= (1)x^3 + (0)x^2 + (1)x + (1) \\ h(x) &= x^3 + x + 1 \end{aligned}$$

dengan menjumlahkan koefisien dari masing-masing persamaan $f(x)$ dan $g(x)$ maka diperoleh $f(x)$ yang memiliki koefisien 1101 dan $g(x)$ yang memiliki koefisien 0110 maka diperoleh suatu pesamaan baru $h(x)$ dengan koefisien 1011 dalam bentuk biner dan dilambangkan dengan $0B$ dalam notasi heksadesimal yang mengacu pada tabel ASCII.

Nilai $D6$ dalam heksadesimal dengan koefisien polinomial 11010110 memiliki bentuk polinomial $a^7 + a^6 + a^4 + a^2 + a$ dan $2C$ dalam heksadesimal dengan koefisien polinomial 00101100 memiliki bentuk polinomial $a^5 + a^3 + a^2$. Maka dapat diperoleh hasil penjumlahan dua bilangan tersebut menjadi:

$$D6 + 2C = CC$$

$$
\begin{aligned}
(a^7 + a^6 + a^4 + a^2 + a) + (a^5 + a^3 + a^2) &= (1+0)a^7 + (1+0)a^6 \\
&\quad +(0+1)a^5 + (1+0)a^4 \\
&\quad +(1+0)a^3 + (1+1)a^2 \\
&\quad +(1+0)a \\
&= (1)a^7 + (1)a^6 + (1)a^5 \\
&\quad +(1)a^4 + (1)a^3 + (0)a^2 \\
&\quad +(1)a \\
&= a^7 + a^6 + a^5 + a^4 + a^3 + a
\end{aligned}
$$

Maka diperoleh hasil untuk $(a^7 + a^6 + a^5 + a^4 + a^3 + a)$ dengan koefisien polinomial 11111010. Sehingga diperoleh nilai CC dalam notasi heksadesimal dengan merujuk pada tabel ASCII.

Kemudian pada operasi perkalian diberikan oleh suatu masukan yang dinotasikan dengan heksadesimal seperti berikut:

$$57 \cdot 83 = C1$$

$$
\begin{aligned}
(x^6 + x^4 + x^2 + x + 1) \cdot (x^7 + x + 1) &= x^{13} + x^{11} + x^9 + x^8 + x^7 + x^7 \\
&\quad +x^5 + x^3 + x^2 + x + x^6 + x^4 \\
&\quad +x^2 + x + 1 \\
&= x^{13} + x^{11} + x^9 + x^8 + x^7 + x^7 \\
&\quad +x^5 + x^3 + x^2 + x + x^6 + x^4 \\
&\quad + x^2 + x + 1 \\
&= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 \\
&\quad +x^4 + x^3 + 1
\end{aligned}
$$

Maka diperoleh hasil untuk $(x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1)$ modulo $(x^8 + x^4 + x^3 + 1)$ adalah $x^7 + x^6 + 1$.

Perhitungan $a(\alpha) \cdot b(\alpha) \, mod \, q(\alpha)$ dapat diimplementasikan dengan mengganti perkalian dengan α. Jika derajat dari $b(\alpha)$ kurang dari 7 maka perkalian dari α adalah perkalian sederhana. Sebagai contoh:

$$a(a^4 + a^3 + a^2 + 1) = a^5 + a^4 + a^3 + a$$

untuk polinomial berderajat 7, perkalian dengan α adalah berderajat lebih tinggi dengan mengikuti penjumlahan dengan polinomial tak tereduksi, khususnya:

$$\begin{aligned} a(a^7 + a^6 + a^4 + a^2 + a) &= (a^8 + a^7 + a^5 + a^3 + a^2) + (a^8 + a^4 + a^3 + a + 1) \\ &= a^7 + a^5 + a^4 + a^3 + a^2 + a + 1 \end{aligned}$$

Perkalian dengan a dapat diterjemahkan dalam kode komputer dalam 8 bit *byte*. Sehingga,

$$\begin{aligned} a &= (00000010)_2 \\ a^2 &= (00000100)_2 \\ a^3 &= (00001000)_2 \\ a^4 &= (00010000)_2 \\ a^5 &= (00100000)_2 \\ a^6 &= (01000000)_2 \\ a^7 &= (10000000)_2 \end{aligned} \tag{2.10}$$

2.2 Pengamanan Data Tingkat Lanjut

Pengamanan data tingkat lanjut merupakan algoritma pengganti dari *Data Encryption Standard* (DES). Masa berlaku DES selesai dikarenakan faktor keamanan. Pada bulan Maret 2001 ditetapkan algoritma baru yaitu pengamanan data tingkat lanjut oleh National Institute of Standards and Technology (NIST). Setelah mengalahkan lima finalis lainnya yang diseleksi oleh NIST, algoritma pengamanan data tingkat lanjut dipilih sebagai pengganti DES didasarkan pada tiga kriteria utama yaitu: keamanan, harga, dan karakteristik algoritma beserta

penggunaannya. Keamanan merupakan faktor utama sehingga tahan terhadap semua jenis serangan yang telah diketahui maupun belum diketahui. Disamping itu algoritma ini harus bebas digunakan tanpa membayar royalti. Penggunaan dalam *hardware* dan *software* juga menjadi pertimbangan karena algoritma pengamanan data tingkat lanjut efisien dan cepat jika dijalankan dalam berbagai *platform* 8 bit hingga 64 bit (Winarno, 2012:33).

Algoritma pengamanan data tingkat lanjut adalah blok chiperteks simetrik yang dapat dienkripsi dan didekripsi mengunakan kunci kriptografi sepanjang 128, 192, dan 256 bit pada blok 128 bit. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi. Perbandingan jumlah proses yang harus dilalui untuk masing-masing masukan adalah berikut:

Tabel 2.2 Tabel Jumlah Proses Berdasarkan Bit Blok dan Kunci

Panjang Kunci Dalam bit	**Panjang Kunci (Nk) Dalam *words***	**Ukuran Data (Nb) Dalam *words***	**Jumlah Proses (Nr)**
128	4	4	10
192	6	4	12
256	8	4	14

Proses kriptografi pengamanan data tingkat lanjut yang berdasarkan pada kunci sepanjang 16 bit dimana setiap ronde dengan konsisten menggunakan operasi lapangan Galois pada setiap *byte*s (*SubBytes*), operasi pada baris setiap matriks (*ShiftRows*), operasi pada setiap kolom (*MixColumns*), dan penjumlahan vektor dengan kunci yang acak (*AddRoundKey*) dijelaskan sebagai berikut:

2.2.1 *SubBytes*

Transformasi *SubBytes* dapat menggunakan tabel substitusi, yaitu dengan cara menginterpretasikan *byte* masukan $s_{i,j}$ sebagai 2 bilangan heksadesimal,

kemudian digit kiri menunjukkan indeks baris dan digit kanan menunjukkan indeks kolom pada tabel substitusi. Nilai *byte* pada tabel substitusi yang dirujuk oleh indeks baris dan kolom menjadi nilai yang mensubstitusi $s_{i,j}$ seperti yang ditunjukkan oleh tabel berikut:

Tabel 2.3 Tabel Substitusi untuk Transformasi *SubBytes*

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	FE	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	9C	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	71	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	EB	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	29	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	4A	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	50	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	10	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	64	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	DE	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	91	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	65	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	4B	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	86	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	CE	54	BB	16

Setiap elemen pada matriks 4×4 adalah suatu *byte*, yang dapat dipertimbangkan sebagai elemen dari lapangan $GF(2^8)$. Mengganti setiap elemen u tak nol dari suatu lapangan dengan $u^{-1} \in GF(2^8)$ dengan nol sebagai elemen tetap. Operasi invers ini dapat dibalik yang disebut sebagai eleman yang baru sebagai berikut:

$$b_7a^7 + b_6a^6 + b_5a^5 + b_4a^4 + b_3a^3 + b_2a^2 + b_1a + b_0 = b_7b_6b_5b_4b_3b_2b_1b_0 \quad (2.23)$$

Sehingga substitusi *byte* yaitu mengganti setiap *byte* dari matriks 4×4 dengan suatu *byte* yang ditransformasikan (Hardy dan Walker, 2003:239).

2.2.2 *ShiftRows*

Selain menggunakan substitusi untuk mengganti nilai pada elemen *state*, menggunakan permutasi pada *state*. Transformasi permutasi pada *state* disebut dengan transformasi *ShiftRows*. *ShiftRows* dilakukan dengan menjalankan operasi

circular shift left sebanyak *i* pada baris ke I pada *state*. Transformasi *ShiftRows* diberikan sebagai *ShiftRows* berikut:

$$\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} = \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{11} & s_{12} & s_{13} & s_{10} \\ s_{22} & s_{23} & s_{20} & s_{21} \\ s_{33} & s_{30} & s_{31} & s_{32} \end{bmatrix}$$

Sehingga baris pertama tetap, baris kedua diputar dan digeser satu sel ke kiri dengan satu putaran, baris ke dua diputar dengan menggeser dua sel ke kiri dalam satu putaran, dan baris ketiga diputar dengan menggeser tiga sel ke kiri dengan satu putaran. Invers dari operasi perputaran baris yang digunakan adalah pada arah yang berlawanan (Hardy dan Walker, 2003:240).

2.2.3 *MixColumns*

Tujuan transformasi *MixColumns* adalah mencampur nilai kolom-kolom pada *state* pada satu elemen *state* keluaran. Untuk melakukan pencampuran itu, transformasi *MixColumns* menggunakan operasi perkalian matrikss dengan operasi perkalian dan penjumlahan menggunakan operator pada $GF(2^8)$ dengan *irreducible polynomial* $(x^8 + x^4 + x^3 + x + 1)$. *MixColumns* merupakan transformasi linier yang diberikan sebagai berikut:

$$\begin{bmatrix} s_{11} & s_{12} & s_{13} & s_{14} \\ s_{21} & s_{22} & s_{23} & s_{24} \\ s_{31} & s_{32} & s_{33} & s_{34} \\ s_{41} & s_{42} & s_{43} & s_{44} \end{bmatrix} = \begin{bmatrix} \alpha & \alpha+1 & 1 & 1 \\ 1 & \alpha & \alpha+1 & 1 \\ 1 & 1 & \alpha & \alpha+1 \\ \alpha+1 & 1 & 1 & \alpha \end{bmatrix} \begin{bmatrix} s_{11} & s_{12} & s_{13} & s_{14} \\ s_{21} & s_{22} & s_{23} & s_{24} \\ s_{31} & s_{32} & s_{33} & s_{34} \\ s_{41} & s_{42} & s_{43} & s_{44} \end{bmatrix}$$

Ini merupakan transforasi linier yang data dibalik jika,

$$A = \begin{bmatrix} \alpha & \alpha+1 & 1 & 1 \\ 1 & \alpha & \alpha+1 & 1 \\ 1 & 1 & \alpha & \alpha+1 \\ \alpha+1 & 1 & 1 & \alpha \end{bmatrix}^{-1}$$

Maka,

$$A = \begin{bmatrix} \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha+1 & \alpha^3+\alpha^2+1 & \alpha^3+1 \\ \alpha^3+1 & \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha+1 & \alpha^3+\alpha^2+1 \\ \alpha^3+\alpha^2+1 & \alpha^3+1 & \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha+1 \\ \alpha^3+\alpha+1 & \alpha^3+\alpha^2+1 & \alpha^3+1 & \alpha^3+\alpha^2+\alpha \end{bmatrix}$$

atas $GF(2^8)$ (Hardy dan Walker, 2003:241).

2.2.4 *AddRoundKey*

Transformasi *AddRoundKey* mencampur sebuah *state* masukan dengan kunci ronde dengan operasi eksklusif OR ($\oplus$). Setiap elemen pada *state* masukan yang merupakan sebuah *byte* dikenakan operasi eksklusif OR dengan *byte* pada posisi yang sama di kunci ronde (kunci ronde direpresentasikan sebagai *state*). Transformasi *AddRoundKey* merupakan transformasi yang bersifat *self inverse*, yaitu transformasi invers sama dengan transformasi aslinya asalkan menggunakan kunci ronde yang sama. Transformasi terakhir pada setiap ronde dari tiga ronde yang merupakan penjumlahan matriks yaitu:

$$\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} = \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} + \begin{bmatrix} k_{00} & k_{01} & k_{02} & k_{03} \\ k_{10} & k_{11} & k_{12} & k_{13} \\ k_{20} & k_{21} & k_{22} & k_{23} \\ k_{30} & k_{31} & k_{32} & k_{33} \end{bmatrix}$$

Untuk α dimodifikasi dengan matriks kunci (k_{ij}) yang dihasilkan dari algoritma perluasan kunci pada setiap ronde dalam tiga ronde. Karena $u + u = 0$ pada $GF(2^8)$, ini menunjukkan bahwa transformasi invers juga merupakan penjumlahan dengan matriks yang sama (Hardy dan Walker, 2003:241).

2.2.5 Ekspansi Kunci

Matriks kunci pertama dihasilkan langsung dari kunci 128 bit.

$$(k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_A, k_B, k_C, k_D, k_E, k_F) \quad (2.24)$$

untuk setiap k_i yang melambangkan satu *byte* dengan urutan:

$$\begin{bmatrix} k_{00} & k_{01} & k_{02} & k_{03} \\ k_{10} & k_{11} & k_{12} & k_{13} \\ k_{20} & k_{21} & k_{22} & k_{23} \\ k_{30} & k_{31} & k_{32} & k_{33} \end{bmatrix} = \begin{bmatrix} k_0 & k_4 & k_8 & k_C \\ k_1 & k_5 & k_9 & k_D \\ k_2 & k_6 & k_A & k_E \\ k_3 & k_7 & k_B & k_F \end{bmatrix}$$

Tiga penjumahan kunci matriks yang dihasilkan dengan melakukan serangkaian perubahan pada kolom. Kolom paling kiri pada setiap penjumlahan matriks kunci dihasilkan setelah melakukan 4 langkah berikut:

1. Melakukan operasi rotasi dengan fungsi rotasi sebagai berikut:

$$\begin{aligned} P(a_0) &= P(a_{\pi(0)}) \\ P(a_1) &= P(a_{\pi(1)}) \\ P(a_2) &= P(a_{\pi(2)}) \\ P(a_3) &= P(a_{\pi(3)}) \end{aligned} \tag{2.25}$$

Persamaan (2.25) dirotasikan sehingga menjadi:

$$\begin{aligned} P(a_1) &= P(a_{\pi(1)}) \\ P(a_2) &= P(a_{\pi(2)}) \\ P(a_3) &= P(a_{\pi(3)}) \\ P(a_0) &= P(a_{\pi(0)}) \end{aligned} \tag{2.26}$$

Maka diperoleh untuk,

$$P\begin{bmatrix} k_{00} \\ k_{10} \\ k_{20} \\ k_{30} \end{bmatrix} = P\begin{bmatrix} k_{10} \\ k_{20} \\ k_{30} \\ k_{00} \end{bmatrix} \tag{2.27}$$

2. Melakukan transformasi *SubBytes* pada setiap *byte*. Dengan merujuk pada Tabel 2.3.
3. Menambahkan vektor berikut:

$$\begin{bmatrix} \alpha^{i-1} \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad (2.28)$$

Untuk i adalah nomor dari suatu ronde.

4. Jumlahkan kolom kiri dari kunci matriks sebelumnya.

   Sisa yang dihasilkan dari penjumlahan kolom kiri dengan tujuan ke kiri dengan kolom yang sesuai dari matriks kunci sebelumnya. Misalkan K_i^j yang merupakan kolom j dari i matriks kunci. Maka untuk $j = 2, 3, 4$ mendapatkan $K_i^j = K_i^{j-1} + K_{i-1}^j$ (Hardy dan Walker, 2003:242).

2.2.6 *InvSubBytes*

Transformasi *InvSubBytes* dapat menggunakan tabel substitusi invers yaitu dengan cara menginterpretasikan *byte* masukan $s_{i,j}$ sebagai 2 bilangan heksadesimal, kemudian digit kiri menunjukkan indeks baris dan digit kanan menunjukkan indeks kolom pada tabel substitusi. Nilai *byte* pada tabel substitusi yang dirujuk oleh indeks baris dan kolom menjadi nilai yang mensubstitusi $s_{i,j}$ seperti yang ditunjukkan oleh tabel berikut ini:

Tabel 2.4 Tabel Substitusi untuk Transformasi *InvSubBytes*

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61

2.2.7 *InvShiftRows*

Selain menggunakan substitusi untuk mengganti nilai pada elemen *state*, menggunakan permutasi pada *state*. Transformasi permutasi pada proses dekripsi disebut dengan transformasi *InvShiftRows*. *InvShiftRows* dilakukan dengan menjalankan operasi sirkular *shift right* dan kebalikan dari transformasi *ShiftRows* sebanyak *i* pada baris ke I pada *state*. Ilustrasi transformasi *InvShiftRows* dengan menggunakan fungsi permutasi sebagai berikut :

$$\begin{aligned} P(a_1a_2a_3a_4) &= (a_{\pi(1)}a_{\pi(2)}a_{\pi(3)}a_{\pi(4)}) \\ P(a_4a_1a_2a_3) &= (a_{\pi(4)}a_{\pi(1)}a_{\pi(2)}a_{\pi(3)}) \\ P(a_3a_4a_1a_2) &= (a_{\pi(3)}a_{\pi(4)}a_{\pi(1)}a_{\pi(2)}) \\ P(a_2a_3a_4a_1) &= (a_{\pi(2)}a_{\pi(3)}a_{\pi(4)}a_{\pi(1)}) \end{aligned} \tag{2.29}$$

Sehingga berdasarkan fungsi matriks :

$$\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} \tag{2.30}$$

Dan hasil yang diperoleh setelah dikenakan fungsi permutasi adalah sebagai berikut:

$$\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{13} & s_{10} & s_{11} & s_{12} \\ s_{22} & s_{23} & s_{20} & s_{21} \\ s_{31} & s_{32} & s_{33} & s_{30} \end{bmatrix} \tag{2.31}$$

2.2.8 *InvMixColumns*

Tujuan transformasi *InvMixColumns* adalah mencampur nilai kolom pada matrikss masukan pada satu elemen matriks keluaran. Seperti pada transformasi *MixColumns* untuk melakukan pencampuran, transformasi *InvMixColumns* menggunakan operasi perkalian matriks dengan operasi perkalian penjumlahan menggunakan operator pada $GF(2^8)$ dengan polinomial tak tereduksi ($x^8 + x^4 +$

$x^3 + x + 1)$. Operasi perkalian matrikss pada transformasi *MixColumns* ditunjukkan sebagai berikut:

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} . \begin{bmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \end{bmatrix} = \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix}$$

(2.32)

Matrikss *S* adalah masukan dan matriks *S'* adalah keluaran transformasi *InvMixColumns.* Merepresentasikan koefisien polinomial elemen *S* sebagai perkalian vektor antara baris ke-i pada konstanta dan kolom ke-j pada S. Perkalian dan penjumlahan menggunakan $GF(2^8)$. Untuk kolom ke $i - j = \{0,1,2,3\}$ pada keluaran transformasi *MixColumns* yaitu:

$$\begin{aligned} S'_{0,j} &= s_{0,j} \cdot (x) \oplus s_{1,j} \cdot (x+1) \oplus s_{2,j} \oplus s_{3,j} \\ S'_{0,j} &= s_{0,j} \oplus s_{1,j} \cdot (x) \oplus s_{2,j} (x+1) \oplus s_{3,j} \\ S'_{0,j} &= s_{0,j} \oplus s_{1,j} \oplus s_{2,j} \cdot (x) \oplus s_{3,j} \cdot (x+1) \\ S'_{0,j} &= s_{0,j} \cdot (x+1) \oplus s_{1,j} \oplus s_{2,j} \oplus s_{3,j} \cdot (x) \end{aligned}$$

2.3 Algoritma Kriptografi

Algoritma ditinjau berdasarkan dari kunci yang dipakai yaitu:

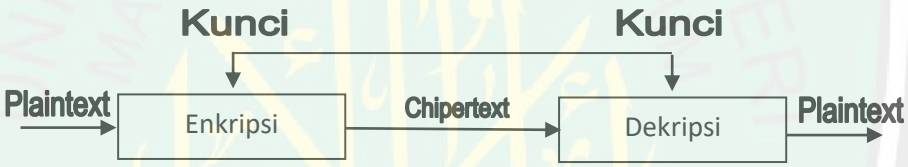
1. Algoritma simetri (menggunakan satu kunci untuk enkripsi dan dekripsi).
2. Algoritma asimetri (menggunakan kunci yang berbeda untuk enkripsi dan dekripsi).

2.3.1 Algoritma Simetri

Algoritma ini juga sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi. Bila mengirim pesan dengan menggunakan algoritma ini, si penerima pesan harus diberitahu kunci dari pesan tersebut agar dapat mendekripsikan pesan yang dikirim. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci. Jika kunci tersebut

diketahui oleh orang lain maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan tersebut (Ariyus, 2008:44). Masalah akan menjadi rumit apabila komunikasi dilakukan secara bersama-sama oleh banyak pihak dan setiap dua pihak yang melakukan pertukaran kunci, maka akan terdapat banyak kunci rahasia yang harus dipertukarkan secara aman (Riyanto, 2010:54). Algoritma yang memakai kunci simetri di antaranya adalah: (1) Substitusi, (2) Transposisi (permutasi), (3) *Data Encryption Standard* (DES), (4) *International Data Encryption Algorithm* (IDEA), (5) *Advanced Encryption Standard* (AES), dan (6) *One Time Pad* (OTP).

Secara sederhana proses pengiriman pesan dengan algoritma simetri dapat digambarkan sebagai berikut:



Gambar 2.1 Skema Algoritma Simetri

2.3.2 Algoritma Asimetri

Algoritma asimetri sering juga disebut dengan algoritma kunci publik, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu:

1. Kunci umum (*public key*) yaitu kunci yang boleh semua orang tahu (dipublikasikan).
2. Kunci rahasia (*private key*) yaitu kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang).

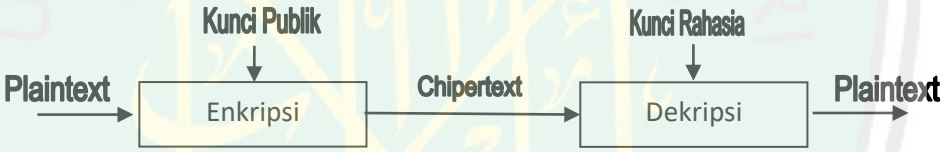
Kunci-kunci tersebut berhubungan satu sama lain. Dengan kunci publik orang dapat mengenkripsi pesan tetapi tidak dapat mengerti isi pesan. Hanya orang yang memiliki kunci rahasia yang dapat mendekripsi dan mengerti pesan tersebut. Algoritma asimetri dapat mengirimkan pesan dengan lebih aman dari

pada algoritma simetri. Contoh Bob mengirim pesan ke Alice menggunakan algoritma asimetri. Hal yang harus dilakukan adalah:

1. Bob memberitahukan kunci publiknya ke Alice.
2. Alice mengenkripsi pesan dengan menggunakan kunci publik Bob.
3. Bob mendekripsi pesan dari Alice dengan kunci rahasianya.
4. Begitu juga sebaliknya jika Bob ingin mengirim pesan ke Alice.

Algoritma yang memakai kunci publik di antaranya adalah: (1) *Digital Signature Algorithm* (DSA), (2) Rivest, Shamir, dan Adleman (RSA), (3) *Diffie-Hellman* (DH), (4) *Elliptic Curve Cryptography* (ECC), dan (5) *Kriptografi Quantum*.

Secara sederhana proses pengiriman pesan dengan algoritma asimetri dapat digambarkan sebagai berikut:



Gambar 2.2 Skema Algoritma Asimetri

2.4 Kajian Agama Mengenai Ilmu Kriptografi

Intelektual muslim dan pewaris para nabi berkewajiban untuk mempelajari ilmu pengetahuan dan ilmu al-Qur'an serta menjelaskan nilai-nilai yang sejalan dengan perkembangan masyarakat sehingga al-Qur'an dan ilmu pengetahuan dapat benar-benar berfungsi dan menjadi sumber inspirasi di masa yang akan datang. Allah Swt. berfirman dalam surah al-Kahfi/18:28, yaitu:

وَٱصۡبِرۡ نَفۡسَكَ مَعَ ٱلَّذِينَ يَدۡعُونَ رَبَّهُم بِٱلۡغَدَوٰةِ وَٱلۡعَشِيِّ يُرِيدُونَ وَجۡهَهُۥۖ وَلَا تَعۡدُ عَيۡنَاكَ عَنۡهُمۡ تُرِيدُ زِينَةَ ٱلۡحَيَوٰةِ ٱلدُّنۡيَاۖ وَلَا تُطِعۡ مَنۡ أَغۡفَلۡنَا قَلۡبَهُۥ عَن ذِكۡرِنَا وَٱتَّبَعَ هَوَىٰهُ وَكَانَ أَمۡرُهُۥ فُرُطٗا ٢٨

"Dan bersabarlah kamu bersama-sama dengan orang-orang yang menyeru Tuhannya di pagi dan senja hari dengan mengharap keridhaan-Nya; dan janganlah kedua matamu berpaling dari mereka (karena) mengharapkan perhiasan dunia ini; dan janganlah kamu mengikuti orang yang hatinya telah Kami lalaikan dari mengingati Kami, serta menuruti hawa nafsunya dan adalah keadaannya itu melewati batas."(QS Al-Kahfi/18:28)".

Diwajibkan bersikap ikhlas dan sabar dalam mempelajari dan menerapkan ilmu pengetahuan. Serta bersikap amanah dalam menyampaikan informasi atau pesan. Untuk mendapatkan pemahaman yang lebih jelas penulis memberikan sebaris kalimat atau plainteks sederhana yang akan ditransformasi dan dioperasikan dengan kunci sehingga pesan yang dikirim tidak mudah diketahui oleh dan dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Maka intelektual muslim yang merupakan harapan bangsa berkewajiban untuk membela dan memperkuat bangsa dengan ilmu pengetahuan dan al-Quran. Jiwa keikhlasan sejati senantia harus terus dipupuk agar kesabaran yang dilakukan membuahkan hasil yang baik dan bermanfaat di dunia serta akhirat. Allah Swt. berfirman dalam surah al-Baqarah/2:265, yaitu:

وَمَثَلُ ٱلَّذِينَ يُنفِقُونَ أَمۡوَٰلَهُمُ ٱبۡتِغَآءَ مَرۡضَاتِ ٱللَّهِ وَتَثۡبِيتٗا مِّنۡ أَنفُسِهِمۡ كَمَثَلِ جَنَّةِۭ بِرَبۡوَةٍ
أَصَابَهَا وَابِلٞ فَـَٔاتَتۡ أُكُلَهَا ضِعۡفَيۡنِ فَإِن لَّمۡ يُصِبۡهَا وَابِلٞ فَطَلّٞۗ وَٱللَّهُ بِمَا تَعۡمَلُونَ بَصِيرٌ

٢٦٥

"Dan perumpamaan orang-orang yang membelanjakan hartanya karena mencari keridhaan Allah dan untuk keteguhan jiwa mereka, seperti sebuah kebun yang terletak di dataran Tinggi yang disiram oleh hujan lebat, Maka kebun itu menghasilkan buahnya dua kali lipat. jika hujan lebat tidak menyiraminya, Maka hujan gerimis (pun memadai) dan Allah Maha melihat apa yang kamu perbuat "(QS Al-Baqarah/2:265).

Sehingga sepatutnya bagi muslim bersikap ikhlas dan sabar dalam mempelajari dan menerapkan ilmu pengetahuan, serta bersikap amanah dalam menyampaikan informasi atau pesan.

BAB III

PEMBAHASAN

Bab ini membahas proses enkripsi dan dekripsi pesan. Proses enkripsi dan dekripsi pesan menggunakan kunci yang sama dalam tiga ronde. Kunci yang digunakan terbagi menjadi tiga kunci yang terdiri dari satu kunci asli dan dua kunci hasil ekspansi atau pembangkitan kunci.

3.1 Proses Pembentukan dan Ekspansi Kunci

Adapun sebelum melakukan proses enkripsi dan dekripsi pesan terlebih dahulu melakukan ekspansi atau pembangkitan kunci yang dilakukan dengan langkah-langkah sebagai berikut:

1. Menentukan kunci teks/berita dalam bentuk kalimat yang berupa kata, angka dan karakter dengan panjang kunci sebanyak 16 kata/angka/karakter.
2. Mengkonversi kunci berupa kata/angka/karakter ke dalam bentuk heksadesimal.
3. Membagi kunci yang berupa kata/angka/karakter yang telah direpresentasikan dalam bentuk heksadesimal menjadi beberapa blok dan membentuk matriks. Ukuran matriks disesuaikan dengan jumlah karakter yang diambil dalam dalam setiap blok. Dalam hal ini peneliti membentuk matriks 4×4 karena mengambil 4 karakter dalam satu blok. Setiap blok menjadi baris ke i pada matriks I, dimulai pada urutan blok pertama menjadi kolom pertama pada matriks sampai kolom terakhir. Adapun susunan matriks yang penulis maksud adalah:

$$\begin{bmatrix} I_{00} & I_{04} & I_{08} & I_{12} \\ I_{01} & I_{05} & I_{09} & I_{13} \\ I_{02} & I_{06} & I_{10} & I_{14} \\ I_{03} & I_{07} & I_{11} & I_{15} \end{bmatrix} \quad (3.1)$$

Untuk memperoleh kunci baru yang merupakan hasil pembangkitan kunci dari kunci asli maka dalam hal ini matriks dibagi menjadi 4 vektor. Sehingga diperoleh vektor kolom pertama adalah:

$$\begin{bmatrix} I_{00} \\ I_{01} \\ I_{02} \\ I_{03} \end{bmatrix} \quad (3.2)$$

Dan vektor kolom kedua adalah:

$$\begin{bmatrix} I_{04} \\ I_{05} \\ I_{06} \\ I_{07} \end{bmatrix} \quad (3.3)$$

Diperoleh vektor kolom ketiga adalah:

$$\begin{bmatrix} I_{08} \\ I_{09} \\ I_{10} \\ I_{11} \end{bmatrix} \quad (3.4)$$

Kemudian vektor kolom keempat adalah:

$$\begin{bmatrix} I_{12} \\ I_{13} \\ I_{14} \\ I_{15} \end{bmatrix} \quad (3.5)$$

4. Melakukan transformasi matriks masukan $I_{i,j}$ menggunakan tabel substitusi *S-Box*, dengan cara menginterpretasikan setiap elemen pada matriks masukan $I_{i,j}$ sebagai dua bilangan heksadesimal dengan digit kiri menunjukkan indeks baris dan digit kanan menunjukkan indeks kolom pada tabel substitusi. Penulis menggunakan tabel substitusi untuk transformasi setiap elemen matriks dengan menggunakan Tabel 2.3. Untuk mendapatkan kunci baru pada ronde kedua dan

ketiga, penulis memanfaatkan kunci pertama yang diperluas atau dibangkitkan sehingga diperoleh kunci baru. Dalam hal ini penulis mengambil vektor kolom keempat pada matriks $I_{i,j}$ atau persamaan (3.5) sebagai vektor kolom yakni:

$$\begin{bmatrix} I_{12} \\ I_{13} \\ I_{14} \\ I_{15} \end{bmatrix}$$

Kolom keempat pada matriks $I_{i,j}$ kemudian ditransformasi dengan tabel substitusi sehingga matriks masukan yang diperoleh adalah:

$$\begin{bmatrix} s_{12} \\ s_{13} \\ s_{14} \\ s_{15} \end{bmatrix} \tag{3.6}$$

Selanjutnya nilai elemen yang dirujuk oleh indeks baris dan kolom tersebut menjadi nilai substitusi matriks $s_{i,j}$ yang merupakan matriks hasil transformasi substitusi setiap elemen matriks pada matriks $s_{i,j}$.

5. Melakukan proses pencampuran vektor kolom pertama matriks I_i, j pada persamaan (3.2) dengan kolom keempat matriks $s_{i,j}$ pada persamaan (3.6) untuk menghasilkan vektor kolom pertama pada matriks kunci baru. Untuk melakukan proses percampuran vektor maka dilakukan dengan operasi eksklusif XOR. Untuk melakukan penjumlahan dengan operasi XOR maka anggota dari setiap matriks dan vektor ditulis dalam bentuk polinomial sehingga dapat diperoleh koefisien polinomial dari masing-masing elemen, yang kemudian dijumlahkan berdasarkan kaidah penjumlahan pada lapangan $GF(2^8)$ menggunakan operasi XOR seperti yang dijelaskan pada persamaan (2.20). Dengan demikian maka diperoleh vektor kolom pertama matriks $t_{i,j}$ adalah:

$$\begin{bmatrix} t_{00} \\ t_{01} \\ t_{02} \\ t_{03} \end{bmatrix} \quad (3.7)$$

6. Selanjutnya dilakukan pencampuran antara vektor kolom pertama matriks $t_{i,j}$ dengan vektor koefisien maka diperoleh kunci baru dari kunci asli yang diberikan. Untuk proses pembentukan kunci ketiga dilakukan dengan langkah-langkah yang sama dengan menggunakan kunci kedua yang telah terbentuk.

1.1 3.2 Proses Enkripsi Pesan

Setelah ketiga kunci terbentuk, selanjutnya langkah-langkah untuk melakukan proses enkripsi pesan/teks berita sebagai berikut:

1. Menentukan pesan teks/berita dalam bentuk kalimat yang berupa kata, angka dan karakter dengan panjang kunci sebanyak 16 kata/angka/karakter.
2. Mengkonversi pesan teks/berita yang berupa kata/angka/karakter ke dalam bentuk heksadesimal.
3. Membagi pesan yang berupa kata/angka/karakter yang telah direpresentasikan dalam bentuk heksadesimal menjadi beberapa blok. Peneliti memilih empat karakter dalam satu blok untuk membentuk matriks. Ukuran matriks disesuaikan dengan jumlah karakter yang diambil dalam dalam setiap blok. Dalam hal ini peneliti membentuk matriks 4×4 karena mengambil 4 karakter dalam satu blok. Setiap blok menjadi baris ke i pada matriks J, dimulai dari urutan blok pertama menjadi kolom pertama pada matriks sampai kolom terakhir. Adapun susunan matriks yang penulis maksud adalah:

$$\begin{bmatrix} J_{00} & J_{04} & J_{08} & J_{12} \\ J_{01} & J_{05} & J_{09} & J_{13} \\ J_{02} & J_{06} & J_{10} & J_{14} \\ J_{03} & J_{07} & J_{11} & J_{15} \end{bmatrix} \quad (3.8)$$

4. Menentukan kunci teks/berita dalam bentuk kalimat yang berupa kata, angka dan karakter dengan panjang kunci sebanyak 16 kata/angka/karakter seperti yang sudah disusun dalam bentuk matriks $I_{i,j}$ dalam persamaan (3.1).
5. Melakukan proses pencampuran atau *AddRoundKey* antara matriks $I_{i,j}$ pada persamaan (3.1) dengan matriks $J_{i,j}$ pada persamaan (3.8) untuk menghasilkan matriks baru yang telah tersandi dengan kunci. Untuk melakukan proses percampuran dilakukan dengan operasi eksklusif XOR. Untuk melakukan penjumlahan dengan operasi XOR maka anggota dari setiap matriks ditulis dalam bentuk polinomial sehingga dapat diperoleh koefisien polinomial dari masing-masing elemen, yang kemudian dijumlahkan berdasarkan kaidah penjumlahan pada lapangan $GF(2^8)$ menggunakan operasi XOR seperti yang dijelaskan pada persamaan (2.20). Dengan demikian diperoleh matriks baru yang telah tersandi dengan kunci ronde pertama sebagai matriks $M_{i,j}$ adalah:

$$\begin{bmatrix} M_{00} & M_{04} & M_{08} & M_{12} \\ M_{01} & M_{05} & M_{09} & M_{13} \\ M_{02} & M_{06} & M_{10} & M_{14} \\ M_{03} & M_{07} & M_{11} & M_{15} \end{bmatrix} \quad (3.9)$$

6. Melakukan transformasi matriks masukan $M_{i,j}$ pada persamaan (3.9) menggunakan tabel substitusi *S-Box*, dengan cara menginterpretasikan setiap elemen pada matriks masukan $M_{i,j}$ sebagai dua bilangan heksadesimal dengan digit kiri menunjukkan indeks baris dan digit kanan menunjukkan indeks kolom pada tabel substitusi. Penulis menggunakan tabel substitusi

untuk transformasi setiap elemen matriks masukan pada Tabel 2.2. Sehingga diperoleh matriks baru $N_{i,j}$ sebagai hasil substitusi setiap elemen pada matriks masukan $M_{i,j}$ adalah:

$$\begin{bmatrix} N_{00} & N_{04} & N_{08} & N_{12} \\ N_{01} & N_{05} & N_{09} & N_{13} \\ N_{02} & N_{06} & N_{10} & N_{14} \\ N_{03} & N_{07} & N_{11} & N_{15} \end{bmatrix} \tag{3.10}$$

7. Selanjutnya matriks $N_{i,j}$ menjadi matriks masukan untuk transformasi *ShiftRows* yakni permutasi (pengubahan posisi elemen tatapi tidak merubah nilai elemen) dengan operasi *circular shift left* sebanyak *i* pada baris ke *N* pada matriks $N_{i,j}$. Memindah setiap elemen matriks berposisi ke *i* pada matriks masukan $N_{i,j}$ menjadi elemen berposisi ke *j* pada matriks keluaran $O_{i,j}$ sesuai dengan fungsi permutasi yang digunakan. Dalam hal ini peneliti menggunakan permutasi biasa dengan bentuk fungsi permutasi berikut:

$$O(N_{00}N_{01}N_{02}N_{03}) = (N_{\pi(00)}N_{\pi(01)}N_{\pi(02)}N_{\pi(03)})$$

$$O(N_{01}N_{02}N_{03}N_{00}) = (N_{\pi(01)}N_{\pi(02)}N_{\pi(03)}N_{\pi(00)})$$

$$O(N_{02}N_{03}N_{00}N_{01}) = (N_{\pi(02)}N_{\pi(03)}N_{\pi(00)}N_{\pi(01)})$$

$$O(N_{03}N_{00}N_{01}N_{02}) = (N_{\pi(03)}N_{\pi(00)}N_{\pi(01)}N_{\pi(02)})$$

8. Melakukan transformasi *MixColumns* yakni dengan mencampur vektor kolom pada matriks $O_{i,j}$ dengan suatu matriks yang memuat konstata dengan nilai koefisien terkecil dalam polinomial, yakni:

$$\begin{bmatrix} \alpha & \alpha+1 & 1 & 1 \\ 1 & \alpha & \alpha+1 & 1 \\ 1 & 1 & \alpha & \alpha+1 \\ \alpha+1 & 1 & 1 & \alpha \end{bmatrix} \tag{3.11}$$

Transformasi yang digunakan adaah transformasi linier dengan operasi ganda. Perkalian matriks menggunakan operasi perkalian dan penjumlahan matriks menggunakan operator $(\oplus)$ pada $GF(2^8)$ dengan polinomial tak tereduksi

$(x^8 + x^4 + x^3 + x + 1)$. Dalam hal ini peneliti mendefinisikan $\oplus$ sebagai penjumalahan kode menggunakan koefisien polinomial dan perkalian matriks dengan pesan yang direpresentasiakan dalam bentuk polinomial. Dalam penelitian ini setiap elemen polinomial yang berderajat ≥ 8 akan direduksi dengan $(x^8 + x^4 + x^3 + x + 1)$ karena dalam penelitian ini penulis membatasi bahwa derajat tertinggi dalam polinomial adalah 7. Semakin besar konstanta elemen yang digunakan untuk proses pencampuran kolom pada persamaan (3.11) maka nilai invers dan perhitungannya juga akan semakin besar dan panjang. Untuk mempermudah proses perhitungan pencampuran antara matriks masukan $O_{i,j}$ dan matriks yang memuat konstanta seperti pada persamaan (3.11) yang dilakukan dengan melakukan proses perkalian vektor antara baris ke i pada matriks masukan dengan kolom ke j pada matriks. Sehingga diperoleh matriks masukan baru $P_{i,j}$ adalah:

$$\begin{bmatrix} P_{00} & P_{04} & p_{08} & P_{12} \\ P_{01} & P_{05} & p_{09} & P_{13} \\ P_{02} & P_{06} & P_{10} & P_{14} \\ P_{03} & P_{07} & P_{11} & P_{15} \end{bmatrix} \quad (3.12)$$

9. Melakukan proses pencampuran atau *AddRoundKey* antara matriks $P_{I,J}$ pada persamaan (3.12) dengan kunci ronde dua untuk menghasilkan matriks baru yang telah tersandi dengan kunci baru. Untuk melakukan proses percampuran dilakukan dengan operasi eksklusif XOR. Untuk melakukan penjumlahan dengan operasi XOR maka anggota dari setiap matriks ditulis dalam bentuk polinomial sehingga dapat diperoleh koefisien polinomial dari masing-masing elemen, yang kemudian dijumlahkan berdasarkan kaidah penjumlahan pada lapangan $GF(2^8)$ menggunakan operasi XOR seperti yang dijelaskan pada

persamaan (2.20). Dengan demikian diperoleh matriks baru yang telah tersandi dengan kunci ronde pertama sebagai matriks $Q_{i,j}$ adalah:

$$\begin{bmatrix} Q_{00} & Q_{04} & Q_{08} & Q_{12} \\ Q_{01} & Q_{05} & Q_{09} & Q_{13} \\ Q_{02} & Q_{06} & Q_{10} & Q_{14} \\ Q_{03} & Q_{07} & Q_{11} & Q_{15} \end{bmatrix} \quad (3.13)$$

10. Mengulangi transformasi *SubBytes* (substitusi setiap elemen pada matriks masukan menggunakan tabel substitusi) untuk memperkuat penyandian pada pesan sehingga menghasilkan matriks masukan baru $Q_{i,j}$ sebagai berikut:

$$\begin{bmatrix} Q_{00} & Q_{04} & Q_{08} & Q_{12} \\ Q_{01} & Q_{05} & Q_{09} & Q_{13} \\ Q_{02} & Q_{06} & Q_{10} & Q_{14} \\ Q_{03} & Q_{07} & Q_{11} & Q_{15} \end{bmatrix} \quad (3.14)$$

11. Mengulangi transformasi *ShiftRows* (permutasi atau pengubahan posisi elemen tanpa mengubah nilai elemen itu sendiri) pada matriks masukan $Q_{i,j}$ utuk memperkuat peyandian dengan pengacakan atau permutasi yang teratur sehingga menghasilkan matriks masukan baru $R_{i,j}$ yaitu:

$$\begin{bmatrix} R_{00} & R_{04} & R_{08} & R_{12} \\ R_{01} & R_{05} & R_{09} & R_{13} \\ R_{02} & R_{06} & R_{10} & R_{14} \\ R_{03} & R_{07} & R_{11} & R_{15} \end{bmatrix} \quad (3.15)$$

12. Melakukan proses pencampuran atau *AddRoundKey* antara matriks $R_{I,J}$ pada persamaan (3.15) dengan kunci ronde tiga untuk menghasilkan matriks baru yang telah tersandi dengan kunci baru atau menjadi chiperteks (pesan yang tersandi). Untuk melakukan proses percampuran dilakukan dengan operasi eksklusif XOR. Dengan demikian diperoleh matriks baru yang telah tersandi dengan kunci ronde pertama sebagai matriks $U_{i,j}$ adalah:

$$\begin{bmatrix} U_{00} & U_{04} & U_{08} & U_{12} \\ U_{01} & U_{05} & U_{09} & U_{13} \\ U_{02} & U_{06} & U_{10} & U_{14} \\ U_{03} & U_{07} & U_{11} & U_{15} \end{bmatrix} \quad (3.16)$$

1.2 3.3 Proses Dekripsi Pesan

Setelah pesan tersandi atau menjadi chiperteks, selanjutnya langkah-langkah untuk melakukan proses dekripsi (perubahann pesan tersandi (chiperteks) kedalam bentuk pesan asli sehingga mudah dimengerti) pesan/teks berita sebagai berikut:

1. Menentukan pesan teks/berita dalam bentuk kalimat yang berupa kata, angka dan karakter dengan panjang kunci sebanyak 16 kata/angka/karakter. Dalam hal matriks $U_{i,j}$ menjadi matriks masukan dalam proses dekripsi.
2. Menentukan kunci teks/berita dalam bentuk kalimat yang berupa kata, angka dan karakter dengan panjang kunci sebanyak 16 kata/angka/karakter. Kunci yang digunakan pada proses dekripsi sama dengan proses enkripsi tetapi urutan kunci yang digunakan merupakan kebalikan dari proses enkripsi yakni dimulai dari kunci ronde ketiga, selanjutnya kunci ronde kedua dan kunci ronde pertama.
3. Melakukan proses pencampuran atau *AddRoundKey* antara matriks $I_{i,j}$ pada persamaan (3.1) dengan matriks kunci ronde ketiga untuk menghasilkan matriks baru yang telah tersandi dengan kunci. Untuk melakukan proses percampuran dilakukan dengan operasi eksklusif XOR. Untuk melakukan penjumlahan dengan operasi XOR maka anggota dari setiap matriks ditulis dalam bentuk polinomial sehingga dapat diperoleh koefisien polinomial dari masing-masing elemen, yang kemudian dijumlahkan berdasarkan kaidah penjumlahan pada lapangan $GF(2^8)$ menggunakan operasi XOR seperti yang

dijelaskan pada persamaan (2.20). Dengan demikian diperoleh matriks baru yang telah tersandi dengan kunci ronde pertama sebagai matriks $A_{i,j}$ adalah:

$$\begin{bmatrix} A_{00} & A_{04} & A_{08} & A_{12} \\ A_{01} & A_{05} & A_{09} & A_{13} \\ A_{02} & A_{06} & A_{10} & A_{14} \\ A_{03} & A_{07} & A_{11} & A_{15} \end{bmatrix} \quad (3.17)$$

4. Selanjutnya matriks $A_{i,j}$ menjadi matriks masukan untuk transformasi *InvShiftRows* yakni permutasi (pengubahan posisi elemen tatapi tidak merubah nilai elemen) dengan operasi *circular shift right* sebanyak *i* pada baris ke *A* pada matriks $A_{i,j}$. Memindah setiap elemen matriks berposisi ke i pada matriks masukan $A_{i,j}$ menjadi elemen berposisi ke j pada matriks keluaran $B_{i,j}$ sesuai dengan fungsi permutasi yang digunakan. Dalam hal ini peneliti menggunakan permutasi biasa dengan bentuk fungsi permutasi berikut:

$$B(A_{00}A_{01}A_{02}A_{03}) = (A_{\pi(00)}A_{\pi(01)}A_{\pi(02)}A_{\pi(03)})$$
$$B(A_{03}A_{00}A_{01}A_{02}) = (A_{\pi(03)}A_{\pi(00)}A_{\pi(01)}A_{\pi(02)})$$
$$B(A_{02}A_{03}A_{00}A_{01}) = (A_{\pi(02)}A_{\pi(03)}A_{\pi(00)}A_{\pi(01)})$$
$$B(A_{01}A_{02}A_{03}A_{00}) = (A_{\pi(01)}A_{\pi(02)}A_{\pi(03)}A_{\pi(00)})$$

5. Melakukan transformasi matriks masukan $B_{i,j}$ menggunakan tabel invers substitusi *S-Box*, dengan cara menginterpretasikan setiap elemen pada matriks masukan $B_{i,j}$ sebagai dua bilangan heksadesimal dengan digit kiri menunjukkan indeks baris dan digit kanan menunjukkan indeks kolom pada tabel substitusi. Penulis menggunakan tabel substitusi untuk transformasi setiap elemen matriks masukan yang sudah ditetapkan oleh Rinjdael seperti yang penulis jelaskan pada Tabel 2.2. Sehingga diperoleh matriks baru $C_{i,j}$ sebagai hasil substitusi setiap elemen pada matriks masukan $C_{i,j}$ adalah:

$$\begin{bmatrix} C_{00} & C_{04} & C_{08} & C_{12} \\ C_{01} & C_{05} & C_{09} & C_{13} \\ C_{02} & C_{06} & C_{10} & C_{14} \\ C_{03} & C_{07} & C_{11} & C_{15} \end{bmatrix} \quad (3.18)$$

6. Melakukan proses pencampuran atau *AddRoundKey* antara matriks $C_{I,J}$ pada persamaan (3.18) dengan kunci ronde dua untuk menghasilkan matriks baru yang telah tersandi dengan kunci baru. Untuk melakukan proses percampuran dilakukan dengan operasi eksklusif XOR. Untuk melakukan penjumlahan dengan operasi XOR maka anggota dari setiap matriks ditulis dalam bentuk polinomial sehingga dapat diperoleh koefisien polinomial dari masing-masing elemen, yang kemudian dijumlahkan berdasarkan kaidah penjumlahan pada lapangan $GF(2^8)$ menggunakan operasi XOR seperti yang dijelaskan pada persamaan (2.20). Dengan demikian diperoleh matriks baru yang telah tersandi dengan kunci ronde kedua sebagai matriks $D_{i,j}$ adalah:

$$\begin{bmatrix} D_{00} & D_{04} & D_{08} & D_{12} \\ D_{01} & D_{05} & D_{09} & D_{13} \\ D_{02} & D_{06} & D_{10} & D_{14} \\ D_{03} & D_{07} & D_{11} & D_{15} \end{bmatrix} \quad (3.19)$$

7. Melakukan transformasi *InvMixColumns* yakni dengan mencampur vektor kolom pada matriks $D_{i,j}$ dengan suatu matriks yang memuat konstata dengan nilai koefisien yang merupakan invers dari persamaan (3.11), yakni:

$$\begin{bmatrix} \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha+1 & \alpha^3+\alpha^2+1 & \alpha^3+1 \\ \alpha^3+1 & \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha+1 & \alpha^3+\alpha^2+1 \\ \alpha^3+\alpha^2+1 & \alpha^3+1 & \alpha^3+\alpha^2+\alpha & \alpha^3+\alpha+1 \\ \alpha^3+\alpha+1 & \alpha^3+\alpha^2+1 & \alpha^3+1 & \alpha^3+\alpha^2+\alpha \end{bmatrix} \quad (3.20)$$

Transformasi yang digunakan adaah transformasi linier dengan operasi ganda. Perkalian matriks menggunakan operasi perkalian dan penjumlahan matriks menggunakan operator $(\oplus)$ pada $GF(2^8)$ dengan polinomial tak tereduksi $(x^8+x^4+x^3+x+1)$. Dalam hal ini peneliti mendefinisikan $\oplus$ sebagai penjumalahan kode menggunakan koefisien polinomial dan perkalian matriks

dengan pesan yang direpresentasiakan dalam bentuk polinomial. Dalam penelitian ini setiap elemen polinomial yang berderajat ≥ 8 akan direduksi dengan $(x^8 + x^4 + x^3 + x + 1)$ karena dalam penelitian ini penulis membatasi bahwa derajat tertinggi dalam polinomial adalah 7. Semakin besar konstanta elemen yang digunakan untuk proses pencampuran kolom pada persamaan (3.11) maka nilai invers pada persamaan (3.20) dan perhitungannya juga akan semakin besar dan panjang. Untuk mempermudah proses perhitungan pencampuran antara matriks masukan $D_{i,j}$ dan matriks yang memuat nilai invers dari konstanta pada persamaan (3.20) yang dilakukan dengan melakukan proses perkalian vektor antara baris ke i pada matriks masukan dengan kolom ke j pada matriks. Sehingga diperoleh matriks masukan baru $E_{i,j}$ adalah:

$$\begin{bmatrix} E_{00} & E_{04} & E_{08} & E_{12} \\ E_{01} & E_{05} & E_{09} & E_{13} \\ E_{02} & E_{06} & E_{10} & E_{14} \\ E_{03} & E_{07} & E_{11} & E_{15} \end{bmatrix} \quad (3.21)$$

8. Mengulangi transformasi *InvShiftRows* (permutasi atau pengubahan posisi elemen tanpa mengubah nilai elemen itu sendiri) pada matriks masukan $E_{i,j}$ pada persamaan (3.21) untuk memperkuat peyandian dengan pengacakan atau permutasi yang teratur sehingga menghasilkan matriks masukan baru $F_{i,j}$ yaitu:

$$\begin{bmatrix} F_{00} & F_{04} & F_{08} & F_{12} \\ F_{01} & F_{05} & F_{09} & F_{13} \\ F_{02} & F_{06} & F_{10} & F_{14} \\ F_{03} & F_{07} & F_{11} & F_{15} \end{bmatrix} \quad (3.22)$$

9. Mengulangi transformasi *InvSubBytes* (substitusi setiap elemen pada matriks masukan menggunakan tabel substitusi) untuk memperkuat penyandian pada pesan sehingga menghasilkan matriks masukan baru $G_{i,j}$ sebagai berikut:

$$\begin{bmatrix} G_{00} & G_{04} & G_{08} & G_{12} \\ G_{01} & G_{05} & G_{09} & G_{13} \\ G_{02} & G_{06} & G_{10} & G_{14} \\ G_{03} & G_{07} & G_{11} & G_{15} \end{bmatrix} \quad (3.23)$$

10. Mengulangi proses pencampuran atau *AddRoundKey* antara matriks $G_{I,J}$ pada persamaan (3.23) dengan kunci ronde pertama untuk menghasilkan matriks baru yang telah tersandi dengan kunci baru sehingga mengembalikan pesan yang tersandi (chiperteks) ke dalam bentuk pesan asli (plainteks). Untuk melakukan proses percampuran dilakukan dengan operasi eksklusif XOR. Dengan demikian diperoleh matriks baru yang merupakan bentuk pesan asli yang tanpa sandi sebagai matriks $H_{i,j}$ adalah:

$$\begin{bmatrix} H_{00} & H_{04} & H_{08} & H_{12} \\ H_{01} & H_{05} & H_{09} & H_{13} \\ H_{02} & H_{06} & H_{10} & H_{14} \\ H_{03} & H_{07} & H_{11} & H_{15} \end{bmatrix} \quad (3.24)$$

3.4 Implementasi Proses Pembentukan dan Ekspansi Kunci

Diberikan kunci teks/berita dalam bentuk kalimat yang berupa kata, angka dan karakter dengan panjang kunci sebanyak 16 kata/angka/karakter. Dalam hal ini penulis memilih kunci dan pesan sebagai berikut:

Kunci :

UINMALIKIMALANG#

Mengkonversi kunci dan pesan yang berupa kata/angka/karakter ke dalam bentuk heksadesimal. Peneliti merujuk pada tabel sistem bilangan seperti yang penulis lampirkan pada lampiran 2. Sehingga bilangan heksadesimal yang

terbentuk berdasarkan kunci berupa kata dan karakter yang penulis berikan adalah:

U	I	N	M	A	L	I	K	I	M	A	L	A	N	G	#
55	49	4E	4D	41	4C	49	4B	49	4D	41	4C	41	4E	47	23

Kemudian membagi kunci yang berupa kata/angka/karakter yang telah direpresentasikan dalam bentuk heksadesimal menjadi beberapa blok. Peneliti memilih empat karakter dalam satu blok untuk membentuk matriks sebagai berikut:

U	I	N	M
55	49	4E	4D
I_{01}	I_{02}	I_{03}	I_{04}

A	L	I	K
41	4C	49	4B
I_{05}	I_{06}	I_{07}	I_{08}

I	M	A	L
49	4D	41	4C
I_{09}	I_{10}	I_{11}	I_{12}

A	N	G	#
41	4E	47	23
I_{13}	I_{14}	I_{15}	I_{16}

Ukuran matriks disesuaikan dengan jumlah karakter yang diambil dalam dalam setiap blok. Maka terbentuk matriks sebagai berikut:

$$\begin{bmatrix} 55 & 41 & 49 & 41 \\ 49 & 4C & 4D & 4E \\ 4E & 49 & 41 & 47 \\ 4D & 4B & 4C & 23 \end{bmatrix} \quad (3.25)$$

Matriks kunci 4×4 persamaan (3.25) menjadi kunci ronde pertama dan merupakan kunci awal untuk mendapatkan kunci pada ronde kedua dan ronde ketiga.

Untuk menghasilkan kunci ronde kedua diperlukan kunci ronde pertama sebagai pembangkit kunci ronde kedua dengan ukuran matriks yang sama yaitu 4×4 . Selanjutnya kita akan menggunakan kunci ronde pertama untuk mencari kunci ronde kedua. Kemudian kunci ronde kedua yang diperoleh digunakan sebagai pembangkit kunci ronde ketiga.

Selanjutnya persamaan (3.25) dibagi menjadi 4 vektor. Sehingga diperoleh vektor kolom pertama adalah:

$$\begin{bmatrix} 55 \\ 49 \\ 4E \\ 4D \end{bmatrix} \quad (3.26)$$

Dan vektor kolom kedua adalah:

$$\begin{bmatrix} 41 \\ 4C \\ 49 \\ 4B \end{bmatrix} \quad (3.27)$$

Diperoleh vektor kolom ketiga adalah:

$$\begin{bmatrix} 49 \\ 4D \\ 41 \\ 4C \end{bmatrix} \quad (3.28)$$

Kemudian vektor kolom keempat adalah:

$$\begin{bmatrix} 41 \\ 4E \\ 47 \\ 23 \end{bmatrix} \quad (3.29)$$

Selanjutnya melakukan rotasi pada persamaan (3.29) maka diperoleh:

$$\begin{bmatrix} 4E \\ 47 \\ 23 \\ 41 \end{bmatrix} \quad (3.30)$$

Setelah melakukan rotasi elemen pada persamaan (3.30) disubstitusi dengan tabel *S-Box*. Sehingga diperoleh hasil substitusi dengan tabel *S-Box* adalah:

$$\begin{bmatrix} 2F \\ A0 \\ 26 \\ 83 \end{bmatrix} \quad (3.31)$$

Selanjutya pencampuran persamaan (3.31) dengan vektor kolom pertama ronde pertama. Untuk melakukan proses percampuran dilakukan dengan operasi

eksklusif XOR. Untuk melakukan penjumlahan dengan operasi XOR maka anggota dari setiap matriks pada persamaan (3.31) ditulis dalam bentuk polinomial sehingga dapat diperoleh koefisien polinomial dari masing-masing elemen, yang kemudian dijumlahkan berdasarkan kaidah penjumlahan pada lapangan $GF(2^8)$ menggunakan operasi XOR sehingga diperoleh bentuk dan koefisien polinomial dari setiap elemen yang dinotasikan dalam heksadesimal pada persamaa (3.31) adalah sebagai berikut:

Vektor kolom keempat ronde pertama	Koefisien Polinomial	Bentuk Polinomial
$2F$	00101111	$= x^5 + x^3 + x^2 + x + 1$
$A0$	10100000	$= x^7 + x^5$
26	00100110	$= x^5 + x^2 + x$
83	10000011	$= x^7 + x + 1$

Vektor kolom pertama ronde pertama	Koefisien Polinomial	Bentuk Polinomial
55	01010101	$= x^6 + x^4 + x^2 + 1$
49	01001001	$= x^6 + x^3 + 1$
$4E$	01001110	$= x^6 + x^3 + x^2 + x$
$4D$	01001101	$= x^6 + x^3 + x^2 + 1$

Dengan memisalkan,

$$b_0 = 2F \oplus 55$$

$$b_1 = A0 \oplus 49$$

$$b_2 = 26 \oplus 4E$$

$$b_3 = 83 \oplus 4D$$

Maka perhitungan dari b_0 sebagai berikut:

$$b_0 = x^5 + x^3 + x^2 + x + 1 \oplus x^6 + x^4 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_0 = 00101111 \oplus 01010101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_0 = 01111010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $7A$.

Maka perhitungan dari b_1 sebagai berikut:

$$b_1 = x^7 + x^5 \oplus x^6 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_1 = 10100000 \oplus 01001001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_1 = 11101001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $E9$.

Maka perhitungan dari b_2 sebagai berikut:

$$b_2 = x^5 + x^2 + x \oplus x^6 + x^3 + x^2 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_2 = 00100110 \oplus 01001110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_2 = 01101000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 68.

Maka perhitungan dari b_3 sebagai berikut:

$$b_3 = x^7 + x + 1 \oplus x^6 + x^3 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_3 = 10000011 \oplus 01001101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_3 = 11001110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai CE.

Sehingga diperoleh hasil sebagai berikut yaitu:

$$\begin{bmatrix} 7A \\ E9 \\ 68 \\ CE \end{bmatrix} \tag{3.32}$$

Setelah melakukan pencampuran persamaan (3.31) dengan vektor kolom pertama ronde pertama sehingga menghasilkan persamaan (3.32). Langkah selanjutnya adalah pencampuran persamaan (3.32) dengan koefisien konstanta ronde dari polinomial 2^8 sebagai berikut:

Tabel. 3.1 Konstanta RCon dalam heksadesimal

	1	2	3
RC(i)	01	02	04

Sehingga perhitungan pencampuran persamaan (3.32) dengan vektor kolom pertama adalah:

Persamaan (3.32)	**Koefisien Polinomial**	**Bentuk Polinomial**
$7A$	01111010	$= x^6 + x^5 + x^4 + x^3 + x$
$E9$	11101001	$= x^7 + x^6 + x^5 + x^3 + 1$
68	01101000	$= x^6 + x^5 + x^3$
CE	11001110	$= x^7 + x^6 + x^3 + x^2 + x$

Vektor kolom pertama ronde pertama	**Koefisien Polinomial**	**Bentuk Polinomial**
01	00000001	$= 1$
00	00000000	$= 0$
00	00000000	$= 0$
00	00000000	$= 0$

Dengan memisalkan,

$$b_4 = 7A \oplus 01$$

$$b_5 = E9 \oplus 00$$

$$b_6 = 68 \oplus 00$$

$$b_7 = CE \oplus 00$$

Maka perhitungan dari b_4 sebagai berikut:

$$b_4 = x^6 + x^5 + x^4 + x^3 + x \oplus 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_4 = 01111010 \oplus 00000001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_4 = 01111011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $7B$.

Maka perhitungan dari b_5 sebagai berikut:

$$b_5 = x^7 + x^6 + x^5 + x^3 + 1 \oplus 0$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_5 = 11101001 \oplus 00000000$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_5 = 11101001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $E9$.

Maka perhitungan dari b_6 sebagai berikut:

$$b_6 = x^6 + x^5 + x^3 \oplus 0$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_6 = 01101000 \oplus 0$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_6 = 01101000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 68.

Maka perhitungan dari b_7 sebagai berikut:

$$b_7 = x^7 + x^6 + x^3 + x^2 + x \oplus 0$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_7 = 11001110 \oplus 0$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_7 = 11001110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai CE.

Sehingga hasil yang diperoleh pada vektor kolom pertama ronde kedua adalah:

$$\begin{bmatrix} 7B \\ E9 \\ 68 \\ CE \end{bmatrix} \tag{3.33}$$

Selanjutnya mencari vektor kolom kedua ronde kedua dengan melakukan XOR antara vektor kolom pertama ronde kedua dengan vektor kolom kedua ronde pertama. Sehingga perhitungan pencampuran persamaan (3.33) dengan vektor kolom pertama adalah:

Persamaan (3.33)	Koefisien Polinomial	Bentuk Polinomial
$7B$	01111011	$= x^6 + x^5 + x^4 + x^3 + x + 1$
$E9$	11101001	$= x^7 + x^6 + x^5 + x^3 + 1$
68	01101000	$= x^6 + x^5 + x^3$
CE	11001110	$= x^7 + x^6 + x^3 + x^2 + x$

Vektor kolom kedua ronde pertama	Koefisien Polinomial	Bentuk Polinomial
41	01000001	$= x^6 + 1$
$4C$	01001100	$= x^6 + x^3 + x^2$
49	01001001	$= x^6 + x^3 + 1$
$4B$	01001011	$= x^6 + x^3 + x + 1$

Dengan memisalkan,

$$b_8 = 7B \oplus 41$$

$$b_9 = E9 \oplus 4C$$

$$b_{10} = 68 \oplus 49$$

$$b_{11} = CE \oplus 4B$$

Maka perhitungan dari b_8 sebagai berikut:

$$b_8 = x^6 + x^5 + x^4 + x^3 + x + 1 \oplus x^6 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_8 = 01111010 \oplus 01000001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien dari polinomial $b_8 = 00111010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $3A$.

Maka perhitungan dari b_9 sebagai berikut:

$$b_9 = x^7 + x^6 + x^5 + x^3 + 1 \oplus x^6 + x^3 + x^2$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_9 = 11101001 \oplus 01001100$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_9 = 10100101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $A5$.

Maka perhitungan dari b_{10} sebagai berikut:

$$b_{10} = x^6 + x^5 + x^3 \oplus x^6 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{10} = 01101000 \oplus 01001001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{10} = 00101001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 29.

Maka perhitungan dari b_{11} sebagai berikut:

$$b_{11} = x^7 + x^6 + x^3 + x^2 + x \oplus x^6 + x^3 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{11} = 11001110 \oplus 01001011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{11} = 10000101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 85.

Sehingga hasil yang diperoleh pada vektor kolom kedua ronde kedua adalah:

$$\begin{bmatrix} 3A \\ A5 \\ 29 \\ 85 \end{bmatrix} \quad (3.34)$$

Selanjutnya mencari vektor kolom ketiga ronde kedua dengan melakukan XOR antara vektor kolom kedua ronde kedua dengan vektor kolom ketiga ronde pertama. Sehingga perhitungan pencampuran persamaan (3.34) dengan vektor kolom ketiga ronde pertama adalah:

Persamaan (3.34)	Koefisien Polinomial	Bentuk Polinomial
$3A$	00111010	$= x^5 + x^4 + x^3 + x$
$A5$	10100101	$= x^7 + x^5 + x^2 + 1$
29	00101001	$= x^5 + x^3 + 1$
85	10000101	$= x^7 + x^3 + 1$

Vektor kolom kedua ronde pertama	Koefisien Polinomial	Bentuk Polinomial
49	01001001	$= x^6 + x^3 + 1$
$4D$	01001101	$= x^6 + x^3 + x^2 + 1$
41	01000001	$= x^6 + 1$
$4C$	01001100	$= x^6 + x^3 + x^2$

Dengan memisalkan,

$$b_{12} = 3A \oplus 49$$

$$b_{12} = A5 \oplus 4D$$

$$b_{14} = 29 \oplus 41$$

$$b_{15} = 85 \oplus 4C$$

Maka perhitungan dari b_{12} sebagai berikut:

$$b_{12} = x^5 + x^4 + x^3 + x \oplus x^6 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{12} = 00111010 \oplus 01001001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien dari $b_{12} = 01110011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 73.

Maka perhitungan dari b_{13} sebagai berikut:

$$b_{13} = x^7 + x^5 + x^2 + 1 \oplus x^6 + x^3 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{13} = 10100101 \oplus 01001101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{13} = 11101000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $E8$.

Maka perhitungan dari b_{14} sebagai berikut:

$$b_{14} = x^5 + x^3 + 1 \oplus x^6 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{14} = 00101001 \oplus 01000001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{14} = 01101000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 68.

Maka perhitungan dari b_{15} sebagai berikut:

$$b_{15} = x^7 + x^3 + 1 \oplus x^6 + x^3 + x^2$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{15} = 10001001 \oplus 01001100$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{15} = 11001001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $C9$.

Sehingga hasil yang diperoleh pada vektor kolom kedua ronde kedua adalah:

$$\begin{bmatrix} 73 \\ E8 \\ 68 \\ C9 \end{bmatrix} \quad (3.35)$$

Sehingga kunci yang diperoleh pada ronde kedua adalah:

$$\begin{bmatrix} 7B & 3A & 73 & 32 \\ E9 & A5 & E8 & A6 \\ 68 & 29 & 68 & 2F \\ CE & 85 & C9 & EA \end{bmatrix} \quad (3.36)$$

Untuk mendapatkan kunci ronde ketiga dilakukan menggunakan cara yang sama. Sehingga diperoleh kunci ronde pertama sampai ronde ketiga seperti yang telah penulis susun dalam tabel berikut:

Tabel 3.2 Kunci Ronde Pertama, Kedua dan Ketiga

55	41	49	41	7B	3A	73	32	5D	67	14	26
49	4C	4D	4E	E9	A5	E8	A6	FC	59	B1	17
4E	49	41	47	68	29	68	2F	EF	C6	AE	81
4D	4B	4C	23	CE	85	C9	EA	ED	68	A1	4B
Ronde Pertama				Ronde Kedua				Ronde Ketiga			

3.5 Implementasi Proses Enkripsi Pesan.

Diberikan kunci dan pesan teks/berita dalam bentuk kalimat yang berupa kata, angka dan karakter dengan panjang kunci sebanyak 16 kata/angka/karakter. Dalam hal ini penulis memilih kunci dan pesan sebagai berikut:

Pesan Asli :

SABAR#DAN#IKHLAS

Selanjutnya mengkonversi pesan yang berupa kata/angka/karakter ke dalam bentuk heksadesimal. Peneliti merujuk pada tabel sistem bilangan seperti yang penulis berikan pada Lampiran 2. Sehingga bilangan heksadesimal yang terbentuk berdasarkan kunci berupa kata dan karakter yang penulis berikan adalah:

S	A	B	A	R	#	D	A	N	#	I	K	H	L	A	S
53	41	42	41	52	23	44	41	4E	23	49	4B	48	4C	41	53

Kemudian membagi pesan yang berupa kata/angka/karakter yang telah direpresentasikan dalam bentuk heksadesimal menjadi beberapa blok. Peneliti memilih empat karakter dalam satu blok untuk membentuk matriks sebagai berikut:

S	A	B	A
53	41	42	41
J_{01}	J_{02}	J_{03}	J_{04}

R	#	D	A
52	23	44	41
J_{05}	J_{06}	J_{07}	J_{08}

N	#	I	K
4E	23	49	4B
J_{09}	J_{10}	J_{11}	J_{12}

H	L	A	S
48	4C	41	53
J_{13}	J_{14}	J_{15}	J_{16}

Ukuran matriks disesuaikan dengan jumlah karakter yang diambil dalam dalam setiap blok. Adapun susunan matriks pesan pada persamaan adalah:

$$\begin{bmatrix} 53 & 52 & 4E & 48 \\ 41 & 23 & 23 & 4C \\ 42 & 44 & 49 & 41 \\ 41 & 41 & 4B & 53 \end{bmatrix} \quad (3.37)$$

dan matriks kunci pada persamaan (3.25) adalah:

$$\begin{bmatrix} 55 & 41 & 49 & 41 \\ 49 & 4C & 4D & 4E \\ 4E & 49 & 41 & 47 \\ 4D & 4B & 4C & 23 \end{bmatrix}$$

Selanjutnya melakukan proses pemcampuran atau XOR antara matriks pesan dan matriks kunci. Matriks pesan asli (plainteks) $[i, j$ di XOR dengan matriks kunci $[i, j]$ untuk $i = 1, 2, 3, 4$ dan $j = 1, 2, 3, 4$. Untuk melakukan penjumlahan dengan operasi XOR maka anggota dari setiap matriks pada persamaan (3.25) dan matriks kunci pada persamaan (3.37) ditulis dalam bentuk polinomial sehingga dapat diperoleh koefisien polinomial dari masing-masing elemen, yang kemudian dijumlahkan berdasarkan kaidah penjumlahan pada lapangan $GF(2^8)$ menggunakan operasi XOR sehingga diperoleh bentuk dan koefisien polinomial dari setiap elemen yang dinotasikan dalam heksadesimal adalah sebagai berikut:

Pesan asli (chiperteks)	Koefisien Polinomial	Bentuk Polinomial
53	00101111	$= x^5 + x^3 + x^2 + x + 1$
41	10100000	$= x^7 + x^5$
42	00100110	$= x^5 + x^2 + x$
41	10000011	$= x^7 + x + 1$
52	01010010	$= x^6 + x^4 + x$
23	00100011	$= x^5 + x + 1$
44	01000100	$= x^6 + x^2$
41	01000001	$= x^6 + 1$
$4E$	01001110	$= x^6 + x^3 + x^2 + x$
23	00100011	$= x^5 + x + 1$
49	01001001	$= x^6 + x^3 + 1$
$4B$	01001011	$= x^6 + x^3 + x + 1$
48	01001000	$= x^6 + x^3$
$4C$	01001100	$= x^6 + x^3 + x^2$
41	01000001	$= x^6 + 1$
53	01010011	$= x^6 + x^4 + x + 1$

Kunci ronde pertama	Koefisien Polinomial	Bentuk Polinomial
55	01010101	$= x^6 + x^4 + x^2 + 1$
49	01001001	$= x^6 + x^3 + 1$
$4E$	01001110	$= x^6 + x^3 + x^2 + x$
$4D$	01001101	$= x^6 + x^3 + x^2 + 1$
41	01000001	$= x^6 + 1$
$4C$	01001100	$= x^6 + x^3 + x^2$
49	01001001	$= x^6 + x^3 + 1$
$4B$	01001011	$= x^6 + x^3 + x + 1$
49	01001001	$= x^6 + x^3 + 1$
$4D$	01001101	$= x^6 + x^3 + x^2 + 1$
41	01000001	$= x^6 + 1$
$4C$	01001100	$= x^6 + x^3 + x^2$
41	01000001	$= x^6 + 1$
$4E$	01001110	$= x^6 + x^3 + x^2 + x$
47	01000111	$= x^6 + x^2 + x + 1$
23	00100011	$= x^5 + x + 1$

Dengan memisalkan,

$$b_{16} = 55 \oplus 55$$

$$b_{17} = 41 \oplus 49$$

$$b_{18} = 42 \oplus 4E$$

$$b_{19} = 41 \oplus 4D$$

$$b_{20} = 52 \oplus 41$$

$$b_{21} = 23 \oplus 4C$$

$$b_{22} = 44 \oplus 49$$

$$b_{23} = 41 \oplus 4B$$

$$b_{24} = 4E \oplus 49$$

$$b_{25} = 23 \oplus 4D$$

$$b_{26} = 49 \oplus 41$$

$$b_{27} = 4B \oplus 4C$$

$$b_{28} = 48 \oplus 41$$

$$b_{29} = 4C \oplus 4E$$

$$b_{30} = 41 \oplus 47$$

$$b_{31} = 53 \oplus 23$$

Maka perhitungan dari b_{16} sebagai berikut:

$$b_{16} = x^6 + x^4 + x^2 + 1 \oplus x^6 + x^4 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{16} = 01010101 \oplus 01010101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{16} = 00000110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 06.

Maka perhitungan dari b_{17} sebagai berikut:

$$b_{17} = x^7 + x^5 \oplus x^6 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{17} = 10100000 \oplus 01001001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{17} = 00001000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 08.

Maka perhitungan dari b_{18} sebagai berikut:

$$b_{18} = x^5 + x^2 + x \oplus x^6 + x^3 + x^2 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{18} = 00100110 \oplus 01001110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{18} = 00001100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $0C$.

Maka perhitungan dari b_{19} sebagai berikut:

$$b_{19} = x^7 + x + 1 \oplus x^6 + x^3 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{19} = 10000011 \oplus 01001101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{19} = 00001100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $0C$.

Maka perhitungan dari b_{20} sebagai berikut:

$$b_{20} = x^6 + x^4 + x \oplus x^6 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{20} = 01010010 \oplus 01000001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{20} = 00010011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 13.

Maka perhitungan dari b_{21} sebagai berikut:

$$b_{21} = x^5 + x + 1 \oplus x^6 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{21} = 00100011 \oplus 01000001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{21} = 01101111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $6F$.

Maka perhitungan dari b_{22} sebagai berikut:

$$b_{22} = x^6 + x^2 \oplus x^6 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{22} = 01000100 \oplus 01001001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{22} = 00001101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $0D$.

Maka perhitungan dari b_{23} sebagai berikut:

$$b_{23} = x^6 + 1 \oplus x^6 + x^3 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{23} = 01000001 \oplus 01001011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{23} = 00001010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $0A$.

Maka perhitungan dari b_{24} sebagai berikut:

$$b_{24} = x^6 + x^3 + x^2 + x \oplus x^6 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{24} = 01001110 \oplus 01001001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{24} = 00000111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 07.

Maka perhitungan dari b_{25} sebagai berikut:

$$b_{25} = x^5 + x + 1 \oplus x^6 + x^3 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{25} = 00100011 \oplus 01001101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{25} = 01101110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $6E$.

Maka perhitungan dari b_{26} sebagai berikut:

$$b_{26} = x^6 + x^3 + 1 \oplus x^6 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{26} = 01001001 \oplus 01000001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisienpolinomial dari $b_{26} = 00001000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 08.

Maka perhitungan dari b_{27} sebagai berikut:

$$b_{27} = x^6 + x^3 + x + 1 \oplus x^6 + x^3 + x^2$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{27} = 01001011 \oplus 01001100$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{27} = 00000111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 07.

Maka perhitungan dari b_{28} sebagai berikut:

$$b_{28} = x^6 + x^3 \oplus x^6 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{28} = 01001000 \oplus 01000001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{28} = 00001001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 09.

Maka perhitungan dari b_{29} sebagai berikut:

$$b_{29} = x^6 + x^3 + x^2 \oplus x^6 + x^3 + x^2 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{29} = 01001100 \oplus 01001110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{29} = 00000010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 02.

Maka perhitungan dari b_{30} sebagai berikut:

$$b_{30} = x^6 + 1 \oplus x^6 + x^2 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{30} = 01000001 \oplus 01000111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{30} = 00000110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 06.

Maka perhitungan dari b_{31} sebagai berikut:

$$b_{31} = x^6 + x^4 + x + 1 \oplus x^5 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{31} = 01010011 \oplus 00100011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{31} = 01110000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 70.

Sehingga hasil yang diperoleh adalah:

$$\begin{bmatrix} b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \\ b_4 & b_8 & b_{12} & b_{16} \end{bmatrix} = \begin{bmatrix} 06 & 13 & 07 & 0C \\ 08 & 6F & 6E & 02 \\ 0C & 0D & 08 & 06 \\ 0C & 0A & 07 & 70 \end{bmatrix} \quad (3.38)$$

Setelah melakukan pencampuran atau XOR antara persamaan (3.25) dengan kunci kunci pertama pada persamaan (3.37) maka matriks keluaran yakni pada persamaan (3.38).

3.2.1 Transformasi *SubBytes*

Selanjutnya melakukan transformasi setiap elemen matriks pada persamaan (3.38) menggunakan tabel substitusi *S-Box*, dengan cara menginterpretasikan setiap elemen pada matriks masukan pada persamaan (3.38)

sebagai dua bilangan heksadesimal dengan digit kiri menunjukkan indeks baris dan digit kanan menunjukkan indeks kolom pada tabel substitusi. Penulis menggunakan tabel substitusi untuk transformasi setiap elemen matriks masukan pada Tabel 2.3. Sehingga diperoleh matriks baru pada persamaan (3.39) sebagai hasil substitusi setiap elemen matriks dari persamaan (3.38) adalah:

$$\begin{bmatrix} 6F & 7D & C5 & 01 \\ 30 & A8 & 9F & 77 \\ FE & D7 & 30 & 6F \\ FE & 67 & C5 & 51 \end{bmatrix} \tag{3.39}$$

3.2.2 Transformasi *SiftRows*

Fungsi permutasi yang digunakan pada persamaan (3.40) adalah:

$$\begin{aligned} P(a_1a_2a_3a_4) &= (a_{\pi(1)}a_{\pi(2)}a_{\pi(3)}a_{\pi(4)}) \\ P(a_2a_3a_4a_1) &= (a_{\pi(2)}a_{\pi(3)}a_{\pi(4)}a_{\pi(1)}) \\ P(a_3a_4a_1a_2) &= (a_{\pi(3)}a_{\pi(4)}a_{\pi(1)}a_{\pi(2)}) \\ P(a_4a_1a_2a_3) &= (a_{\pi(4)}a_{\pi(1)}a_{\pi(2)}a_{\pi(3)}) \end{aligned} \tag{3.40}$$

Dalam hal ini penulis melakukan permutasi bertingkat dengan tujuan pengacakan dengan pola yang teratur seperti yang penulis jelaskan pada persamaan (3.40). Sehingga diperoleh hasil transformasi setiap elemen pada persamaan (3.40) dan dikenakan transformasi pergeseran elemen pada persamaan (3.41) adalah:

$$\begin{bmatrix} 67 & 7D & C5 & 01 \\ A8 & 9F & 77 & 30 \\ 30 & 6F & FE & D7 \\ 51 & FE & 67 & C5 \end{bmatrix} \tag{3.41}$$

3.2.3 Transformasi *MixColumns*

Transformasi *MixColumns* yang dilakukan dengan mencampur vektor kolom pada matriks masukan pada persamaan (3.41) dengan suatu matriks yang memuat konstata dengan nilai koefisien terkecil dalam polinomial, yakni:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \tag{3.42}$$

Elemen matriks masukan direpresentasikan ke dalam polinomial untuk mempermudah proses perhitungan dan penyandian pesan dalam transformasi pencampuran vektor kolom dengan vektor matriks konstanta maka peneliti merepresentasikan koefisien polinomial matriks masukan pada persamaan (3.41) kemudian melakukan perkalian dengan operasi $(\cdot)$ dan penjumlahan dengan operasi $(\oplus)$ seperti yang dijelaskan sebagai berikut:

Kolom 1	Koefisien Polinomial	Bentuk Polinomial
$6F$	01101111	$= x^6 + x^5 + x^3 + x^2 + x + 1$
$A8$	10101000	$= x^7 + x^5 + x^3$
30	00110000	$= x^5 + x^4$
51	01010001	$= x^6 + x^4 + 1$

Kemudian pesan dikalikan dengan matriks 4×4 berikut:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 6F \\ A8 \\ 30 \\ 51 \end{bmatrix} \tag{3.15}$$

Untuk,

$$\begin{aligned} 01 \quad & 00000001 = 1 \\ 02 \quad & 00000010 = x \\ 03 \quad & 00000011 = x + 1 \end{aligned}$$

Baris pertama pada persamaan (3.15) dikalikan dengan kolom pertama pada persamaan (3.10) dengan memisalkan.

$$X_1 = 02 \cdot 6F \oplus 03 \cdot A8 \oplus 01 \cdot 30 \oplus 01 \cdot 51$$

$$X_2 = 01 \cdot 6F \oplus 02 \cdot A8 \oplus 03 \cdot 30 \oplus 01 \cdot 51$$

$$X_3 = 01 \cdot 6F \oplus 01 \cdot A8 \oplus 02 \cdot 30 \oplus 03 \cdot 51$$

$$X_4 = 03 \cdot 6F \oplus 01 \cdot A8 \oplus 01 \cdot 30 \oplus 02 \cdot 51$$

Maka perhitungan dari X_1 sebagai berikut:

$$
\begin{aligned}
X_1 &= x(x^6+x^5+x^3+x^2+x+1) \oplus \\
&\quad (x+1)(x^7+x^5+x^3) \oplus 1(x^5+x^4) \oplus 1(x^6+x^4+1) \\
&= (x^7+x^6+x^4+x^3+x^2+x) \\
&\quad \oplus (x^8+x^6+x^4+x^7+x^5+x^3) modulo (x^4+x^3+x+1) \\
&\quad \oplus (x^5+x^4) \oplus (x^6+x^4+1) \\
&= (x^7+x^6+x^4+x^3+x^2+x) \oplus (x^6+x^7+x^5+x+1) \\
&\quad \oplus (x^5+x^4 \oplus x^6+x^4+1)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_1 = 11011110 \oplus 11100011 \oplus 00110000 \oplus 01010001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_1 = 01011110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $5C$.

Maka perhitungan dari X_2 sebagai berikut:

$$
\begin{aligned}
X_2 &= 1(x^6+x^5+x^3+x^2+x+1) \oplus \\
&\quad x(x^7+x^5+x^3) \oplus (x+1)(x^5+x^4) \oplus 1(x^6+x^4+1) \\
&= (x^6+x^5+x^3+x^2+x+1) \\
&\quad \oplus (x^8+x^6+x^4) modulo (x^4+x^3+x+1) \\
&\quad \oplus (x^6+x^5+x^5+x^4) \oplus (x^6+x^4+1) \\
&= (x^6+x^5+x^3+x^2+x+1) \oplus (x^6+x^3+x+1) \\
&\quad \oplus (x^6+x^5+x^5+x^4) \oplus (x^6+x^4+1)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_2 = 01101111 \oplus 01001011 \oplus 01010000 \oplus 010100001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_2 = 00100101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 25.

Maka perhitungan dari X_3 sebagai berikut:

$$
\begin{aligned}
X_3 &= 1(x^6+x^5+x^3+x^2+x+1) \oplus \\
&\quad 1(x^7+x^5+x^3) \oplus x(x^5+x^4) \oplus (x+1)(x^6+x^4+1) \\
&= (x^6+x^5+x^3+x^2+x+1) \oplus (x^7+x^5+x^3) \\
&\quad \oplus (x^6+x^5) \oplus (x^7+x^5+x+x^6+x^4+1)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_3 = 01101111 \oplus 10101000 \oplus 01100000 \oplus 11110011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_3 = 01010100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 54.

Maka perhitungan dari X_4 sebagai berikut:

$$\begin{aligned} X_4 &= (x+1)(x^6+x^5+x^3+x^2+x+1) \oplus \\ &\quad 1(x^7+x^5+x^3) \oplus 1(x^5+x^4) \oplus x(x^6+x^4+1) \\ &= (x^7+x^6+x^4+x^3+x^2+x+x^6+x^5+x^3+x^2+x+1) \\ &\quad \oplus (x^7+x^5+x^3) \oplus (x^5+x^4 \oplus x^7+x^5+x) \\ &= (x^7+x^5+x^4+1) \oplus (x^7+x^5+x^3) \oplus (x^5+x^4) \\ &\quad \oplus (x^7+x^5+x) \end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_4 = 10110001 \oplus 10101000 \oplus 00110000 \oplus 10100010$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_4 = 10001011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $8B$.

Selanjutnya baris kedua pada persamaan (3.15) dikalikan dengan kolom pertama pada persamaan (3.10) sebagai berikut:

Kolom 2	Koefisien Polinomial	Bentuk Polinomial
$7D$	01111101	$= x^6+x^5+x^4+x^3+x^2+1$
$9F$	10011111	$= x^7+x^4+x^3+x^2+x+1$
$6F$	01101111	$= x^6+x^5+x^3+x^2+x+1$
FE	11110111	$= x^7+x^6+x^5+x^4+x^2+x+1$

Dengan memisalkan,

$$X_5 = 02 \cdot 7D \oplus 03 \cdot 9F \oplus 01 \cdot 6F \oplus 01 \cdot FE$$

$$X_6 = 01 \cdot 7D \oplus 02 \cdot 9F \oplus 03 \cdot 67 \oplus 01 \cdot FE$$

$$X_7 = 01 \cdot 7D \oplus 01 \cdot 9F \oplus 02 \cdot 67 \oplus 03 \cdot FE$$

$$X_8 = 03 \cdot 7D \oplus 01 \cdot 9F \oplus 01 \cdot 67 \oplus 02 \cdot FE$$

Maka perhitungan dari X_5 sebagai berikut:

$$X_5 = x(x^6+x^5+x^4+x^3+x^2+1) \oplus$$

$$
\begin{aligned}
& (x+1)(x^7+x^4+x^3+x^2+x+1) \oplus \\
& 1(x^6+x^5+x^3+x^2+x+1) \oplus \\
& 1(x^7+x^6+x^5+x^4+x^3+x^2+x) \\
= \quad & (x^7+x^6+x^5+x^4+x^3+x) \\
& \oplus (x^8+x^5+x^4+x^3+x^2+x+x^7+x^4+x^3+x^2+) \\
& \oplus (x^6+x^5+x^3+x^2+x+1) \\
& \oplus (x^7+x^6+x^5+x^4+x^3+x^2+x) \\
= \quad & (x^7+x^6+x^5+x^4+x^3+x) \\
& \oplus (x^8+x^5+x^7) modulo (x^4+x^3+x+1) \\
& \oplus (x^6+x^5+x^3+x^2+x+1) \\
& \oplus (x^7+x^6+x^5+x^4+x^3+x^2+x) \\
= \quad & (x^7+x^6+x^5+x^4+x^3+x) \\
& \oplus (x^4+x^3+x+1+x^5+x^7+) \\
& \oplus (x^6+x^5+x^3+x^2+x+1) \\
& \oplus (x^7+x^6+x^5+x^4+x^3+x^2+x)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_5 = 11111010 \oplus 10111010 \oplus 01101111 \oplus 11111110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_5 = 11010001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $D1$.

Maka perhitungan dari X_6 sebagai berikut:

$$
\begin{aligned}
X_6 \quad = \quad & 1(x^6+x^5+x^4+x^3+x^2+1) \\
& \oplus x(x^7+x^4+x^3+x^2+x+1) \\
& \oplus (x+1)(x^6+x^5+x^3+x^2+x+1) \\
& \oplus 1(x^7+x^6+x^5+x^4+x^3+x^2+x) \\
= \quad & (x^6+x^5+x^4+x^3+x^2+1) \\
& \oplus (x^8+x^5+x^4+x^3+x^2+x) modulo (x^4+x^3+x+1) \\
& \oplus (x^7+x^6+x^4+x^3+x^2+x+x^6+x^5+x^3+x^2+x+1) \\
& \oplus (x^7+x^6+x^5+x^4+x^3+x^2+x) \\
= \quad & (x^6+x^5+x^4+x^3+x^2+1) \oplus (x^5+x^2+1) \\
& \oplus (x^7+x^5+x^4+1) \oplus (x^7+x^6+x^5+x^4+x^3+x^2+x)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_6 = 01111101 \oplus 00100101 \oplus 10110001 \oplus 11111110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_6 = 00010111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 17.

Maka perhitungan dari X_7 sebagai berikut:

$$
\begin{aligned}
X_7 \quad &= \quad 1(x^6+x^5+x^4+x^3+x^2+1) \oplus \\
&\quad\quad 1(x^7+x^4+x^3+x^2+x+1) \oplus \\
&\quad\quad x(x^6+x^5+x^3+x^2+x+1) \\
&\quad\quad \oplus (x+1)(x^7+x^6+x^5+x^4+x^3+x^2+x) \\
&= \quad (x^6+x^5+x^4+x^3+x^2+1) \oplus \\
&\quad\quad (x^7+x^4+x^3+x^2+x+1) \oplus (x^7+x^6+x^4+x^3+x^2+x) \\
&\quad\quad \oplus (x^8+x^7+x^6+x^5+x^4+x^3+x^2+ \\
&\quad\quad x^7+x^6+x^5+x^4+x^3+x^2+x) modulo (x^4+x^3+x+1) \\
&= \quad (x^6+x^5+x^4+x^3+x^2+1) \oplus \\
&\quad\quad (x^7+x^4+x^3+x^2+x+1) \\
&\quad\quad \oplus (x^7+x^6+x^4+x^3+x^2+x) \\
&\quad\quad \oplus (x^8+x) modulo (x^4+x^3+x+1) \\
&= \quad (x^6+x^5+x^4+x^3+x^2+1) \oplus \\
&\quad\quad (x^7+x^4+x^3+x^2+x+1) \oplus (x^7+x^6+x^4+x^3+x^2+x) \\
&\quad\quad \oplus (x^4+x^3+x+1+x) \\
&= \quad (x^6+x^5+x^4+x^3+x^2+1) \oplus \\
&\quad\quad (x^7+x^4+x^3+x^2+x+1) \oplus (x^7+x^6+x^4+x^3+x^2+x) \\
&\quad\quad \oplus (x^4+x^3++1)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_7 = 01111101 \oplus 10011111 \oplus 11011110 \oplus 00011001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_7 = 00100101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 25.

Maka perhitungan dari X_8 sebagai berikut:

$$
\begin{aligned}
X_8 \quad &= \quad (x+1)(x^6+x^5+x^4+x^3+x^2+1) \oplus \\
&\quad\quad 1(x^7+x^4+x^3+x^2+x+1) \oplus \\
&\quad\quad 1(x^6+x^5+x^3+x^2+x+1) \\
&\quad\quad \oplus x(x^7+x^6+x^5+x^4+x^3+x^2+x) \\
&= \quad (x^7+x^6+x^5+x^4+x^3+x+x^6+x^5+x^4+x^3+x^2+1) \\
&\quad\quad \oplus (x^7+x^4+x^3+x^2+x+1) \\
&\quad\quad \oplus (x^6+x^5+x^3+x^2+x+1) \\
&\quad\quad \oplus (x^8+x^7+x^6+x^5+x^4+x^3+x^2) \\
&\quad\quad modulo\ (x^4+x^3+x+1) \\
&= \quad (x^7+x^2+x+1) \oplus (x^7+x^4+x^3+x^2+x+1) \\
&\quad\quad \oplus (x^6+x^5+x^3+x^2+x+1) \\
&\quad\quad \oplus (x+1+x^7+x^6+x^5+x^2)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_8 = 10000111 + 10011111 + 01101111 + 11100111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_8 = 10010000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 90.

Selanjutnya baris ketiga pada persamaan (3.15) dikalikan dengan kolom pertama pada persamaan (3.10) sebagai berikut:

Kolom 3	Koefisien Polinomial	Bentuk Polinomial
$C5$	11000101	$= x^7 + x^6 + x^2 + 1$
77	01110111	$= x^6 + x^5 + x^4 + x^2 + x + 1$
FE	11111110	$= x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$
67	01100111	$= x^6 + x^5 + x^2 + x + 1$

Dengan memisalkan,

$$X_9 = 02 \cdot C5 \oplus 03 \cdot 77 \oplus 01 \cdot FE \oplus 01 \cdot 67$$

$$X_{10} = 01 \cdot C5 \oplus 02 \cdot 77 \oplus 03 \cdot FE \oplus 01 \cdot 67$$

$$X_{11} = 01 \cdot C5 \oplus 01 \cdot 77 \oplus 02 \cdot FE \oplus 03 \cdot 67$$

$$X_{12} = 03 \cdot C5 \oplus 01 \cdot 77 \oplus 01 \cdot FE \oplus 02 \cdot 67$$

Maka perhitungan dari X_9 sebagai berikut:

$$\begin{aligned} X_9 \quad = \quad & x(x^7 + x^6 + x^2 + 1) \oplus \\ & (x+1)(x^6 + x^5 + x^4 + x^2 + x + 1) \oplus \\ & 1(x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x) \\ & \oplus 1(x^6 + x^5 + x^2 + x + 1) \\ = \quad & (x^8 + x^7 + x^3 + x) modulo (x^4 + x^3 + x + 1) \oplus \\ & (x^7 + x^6 + x^5 + x^3 + x^2 + x + x^6 + x^5 + x^4 + x^2 + x + 1) \\ & \oplus (x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x) \\ & \oplus (x^6 + x^5 + x^2 + x + 1) \\ = \quad & (x^7 + x^4 + 1) \oplus \\ & (x^7 + x^4 + x^3 + 1) \oplus \\ & (x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x) \\ & \oplus (x^6 + x^5 + x^2 + x + 1) \end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_9 = 10010001 \oplus 10011001 \oplus 11111110 \oplus 01100111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_8 = 10010001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 91.

Maka perhitungan dari X_{10} sebagai berikut:

$$\begin{aligned}
X_{10} &= 1(x^7+x^6+x^2+1) \oplus x(x^6+x^5+x^4+x^2+x+1) \\
&\quad \oplus (x+1)(x^7+x^6+x^5+x^4+x^3+x^2+x) \\
&\quad \oplus 1(x^6+x^5+x^2+x+1) \\
&= (x^7+x^6+x^2+1) \oplus (x^7+x^6+x^5+x^3+x^2) \\
&\quad \oplus (x^8+x^7+x^6+x^5+x^4+x^3+x^2) modulo \\
&\quad (x^4+x^3+x+1+x^7+x^6+x^5+x^4+x^3+x^2+x \\
&\quad \oplus (x^6+x^5+x^2+x+1 \\
&= (x^7+x^6+x^2+1) \oplus (x^7+x^6+x^5+x^3+x^2+x) \\
&\quad \oplus (x^8+x) \\
&\quad \oplus (x^6+x^5+x^2+x+1) \\
&= (x^7+x^6+x^2+1) \oplus (x^7+x^6+x^5+x^3+x^2+x) \\
&\quad \oplus (x^4+x^3+x+1+x) \oplus x^6+x^5+x^2+x+1 \\
&= (x^7+x^6+x^2+1) \oplus (x^7+x^6+x^5+x^3+x^2+x) \\
&\quad \oplus (x^4+x^3+1) \oplus (x^6+x^5+x^2+x+1) \\
&= 11000101 \oplus 11101110 \oplus 00011001 \oplus 01100111 \\
X_{10} &= 01010101 = 55
\end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_{10} = 10010001 \oplus 10011001 \oplus 11111110 \oplus 01100111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_{10} = 01010101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 55.

Maka perhitungan dari X_{11} sebagai berikut:

$$\begin{aligned}
X_{11} &= 1(x^7+x^6+x^2+1) \oplus 1(x^6+x^5+x^4+x^2+x+1) \\
&\quad \oplus x(x^7+x^6+x^5+x^4+x^3+x^2+x) \\
&\quad \oplus (x+1)(x^6+x^5+x^2+x+1) \\
&= (x^7+x^6+x^2+1) \oplus (x^6+x^5+x^4+x^2+x+1) \\
&\quad \oplus (x^8+x^7+x^6+x^5+x^4+x^3+x^2) \\
&\quad modulo(x^4+x^3+x+1) \\
&\quad \oplus (x^7+x^6+x^3+x^2+x+x^6+x^5+x^2+x+1 \\
&= (x^7+x^6+x^2+1) \oplus (x^6+x^5+x^4+x^2+x+1) \\
&\quad \oplus (x^7+x^6+x^5+x^2+x+1) \oplus (x^7+x^5+x^3+1)
\end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_{11} = 11000101 \oplus 01110111 \oplus 11100111 \oplus 10101001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_{11} = 11111100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai FC.

Maka perhitungan dari X_{12} sebagai berikut:

$$\begin{aligned} X_{12} &= (x+1)(x^7+x^6+x^2+1) \oplus 1(x^6+x^5+x^4+x^2+x+1) \\ &\quad \oplus 1(x^7+x^6+x^5+x^4+x^3+x^2+x) \\ &\quad \oplus x(x^6+x^5+x^2+x+1) \\ &= (x^8+x^7+x^3+1+x^7+x^6+x^2+1) \\ &\quad modulo(x^4+x^3+x+1) \\ &\quad \oplus (x^6+x^5+x^4+x^2+x+1) \\ &\quad \oplus (x^7+x^6+x^5+x^4+x^3+x^2+x) \\ &\quad \oplus (x^7+x^6+x^3+x^2+x) \\ &= (x^4+x^3+x+1+x^7+x^3+1+x^7+x^6+x^2+1) \\ &\quad \oplus (x^6+x^5+x^4+x^2+x+1) \\ &\quad \oplus (x^7+x^6+x^5+x^4+x^3+x^2+x) \\ &\quad \oplus (x^7+x^6+x^3+x^2+x) \end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_{12} = 01010100 \oplus 01110111 \oplus 11111110 \oplus 11001110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_{12} = 00010011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 13.

Selanjutnya baris keempat pada persamaan (3.15) dikalikan dengan kolom pertama pada persamaan (3.10) sebagai berikut:

Kolom 4	Koefisien Polinomial	Bentuk Polinomial
01	00000001	$= 1$
30	00110000	$= x^5 + x^4$
$D7$	11010111	$= x^7 + x^6 + x^4 + x^2 + x + 1$
$C5$	11000101	$= x^7 + x^6 + x^2 + 1$

Dengan memisalkan,

$$X_{13} = 02 \cdot 01 \oplus 03 \cdot 30 \oplus 01 \cdot D7 \oplus 01 \cdot C5$$

$$X_{14} = 01 \cdot 01 \oplus 02 \cdot 30 \oplus 03 \cdot D7 \oplus 01 \cdot C5$$

$$X_{15} = 01 \cdot 01 \oplus 01 \cdot 30 \oplus 02 \cdot D7 \oplus 03 \cdot C5$$

$$X_{16} = 03 \cdot 01 \oplus 01 \cdot 30 \oplus 01 \cdot D7 \oplus 02 \cdot C5$$

Maka perhitungan dari X_{13} sebagai berikut:

$$\begin{aligned} X_{13} &= x(1) \oplus (x+1)(x^5+x^4) \oplus 1(x^7+x^6+x^4+x^2+x+1) \\ &\quad \oplus 1(x^7+x^6+x^2+1) \\ &= (x) \oplus (x^6+x^4 \oplus x^7+x^6+x^4+x^2+x+1) \\ &\quad \oplus (x^7+x^6+x^2+1) \\ &= 00000001 \oplus 01010000 \oplus 11010111 \oplus 11000101 \\ X_{13} &= 01000000 = 40 \end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_{13} = 00000001 \oplus 01010000 \oplus 11010111 \oplus 11000101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_{13} = 01000000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 40.

Maka perhitungan dari X_{14} sebagai berikut:

$$\begin{aligned} X_{14} &= 1(1) \oplus x(x^5+x^4) \oplus (x+1)(x^7+x^6+x^4+x^2+x+1) \\ &\quad \oplus 1(x^7+x^6+x^2+1) \\ &= (1) \oplus (x^6+x^5) \\ &\quad \oplus (x^8+x^7+x^5+x^3+x^2+x \ +x^7+x^6+x^4+x^2 \\ &\quad +x+1) modulo (x^4+x^3+x+1) \oplus (x^7+x^6+x^2+1) \\ &= (1) \oplus (x^6+x^5) \oplus (x^6+x^5+x) \oplus (x^7+x^6+x^2+1) \\ &= 00000001 \oplus 01100010 \oplus 01100101 \oplus 11000101 \\ X_{14} &= 01001010 = 4A \end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_{14} = 00000001 \oplus 01100010 \oplus 01100101 \oplus 11000101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_{14} = 01001010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $4A$.

Maka perhitungan dari X_{15} sebagai berikut:

$$\begin{aligned} X_{15} &= 1(1) \oplus 1(x^5 + x^4) \oplus x(x^7 + x^6 + x^4 + x^2 + x + 1) \\ &\quad \oplus (x + 1)(x^7 + x^6 + x^2 + 1) \\ &= (1) \oplus (x^5 + x^4) \oplus (x^8 + x^7 + x^5 + x^3 + x^2 + x) \\ &\quad modulo(x^4 + x^3 + x + 1) \\ &\quad \oplus (x^8 + x^7 + x + x^3 + x + x^7 + x^6 + x^2 + 1) \\ &\quad modulo(x^4 + x^3 + x + 1) \\ &= (1) \oplus (x^5 + x^4) \\ &\quad \oplus (x^4 + x^3 + x + 1 + x^7 + x^5 + x^3 + x^2 + x) \\ &\quad \oplus (x^4 + x^3 + x + 1 + x^7 + x + x^3 + x + x^7 + x^6 + x^2 + 1) \\ &= (1) \oplus (x^5 + x^4) \oplus (x^4 + 1 + x^7 + x^5 + x^2) \\ &\quad \oplus (x^6 + x^4 + x^2) \end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_{15} = 00000001 \oplus 00110000 \oplus 10110101 \oplus 01010100$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_{15} = 11010000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $D0$.

Maka perhitungan dari X_{15} sebagai berikut:

$$\begin{aligned} X_{16} &= (x + 1)(1) \oplus 1(x^5 + x^4) \oplus 1(x^7 + x^6 + x^4 + x^2 + x + 1) \\ &\quad \oplus x(x^7 + x^6 + x^2 + 1) \\ &= (x + 1) \oplus (x^5 + x^4) \oplus (x^7 + x^6 + x^4 + x^2 + x + 1) \\ &\quad \oplus (x^8 + x^7 + x^3 + x) modulo(x^4 + x^3 + x + 1) \\ &= x + 1 \oplus x^5 + x^4 \oplus x^7 + x^6 + x^4 + x^2 + x + 1 \\ &\quad \oplus x^4 + 1 + x^7 \\ &= 00000011 \oplus 00110000 \oplus 11010111 \oplus 10010001 \\ X_{16} &= 01110101 = 75 \end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$X_{16} = 00000011 \oplus 00110000 \oplus 11010111 \oplus 10010001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $X_{16} = 01110101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 75.

Sehingga hasil yang diperoleh dari proses transformasi *MixColumn* adalah sebagai berikut:

$$\begin{bmatrix} X_1 & X_5 & X_9 & X_{13} \\ X_2 & X_6 & X_{10} & X_{14} \\ X_3 & X_7 & X_{11} & X_{15} \\ X_4 & X_8 & X_{12} & X_{16} \end{bmatrix} = \begin{bmatrix} 5C & D1 & 91 & 40 \\ 25 & 17 & 55 & 4A \\ 54 & 25 & FC & D0 \\ 8B & 90 & 13 & 75 \end{bmatrix} \quad (3.42)$$

3.2.4 Transformasi *AddRoundKey* dengan kunci ronde kedua

Langkah selanjutnya adalah mencampur hasil transformasi pencampuran kolom vektor matriks masukan dan konstanta dengan kunci ronde pertama.Selanjutnya melakukan proses pemcampuran atau XOR antara matriks masukan pada persamaan (3.42) dengan matriks kunci ronde kedua. Matriks masukan pada persamaan (3.42) $[i, j]$ di XOR dengan matriks kunci ronde kedua $[i, j]$ untuk $i = 1, 2, 3, 4$ dan $j = 1, 2, 3, 4$. Untuk melakukan penjumlahan dengan operasi XOR maka anggota dari setiap matriks pada persamaan (3.42) dan matriks kunci ronde pertama penulis merepresentasikan koefisien polinomial dari setiap elemen pada matriks tersebut, kemudian dijumlahkan berdasarkan kaidah penjumlahan pada lapangan $GF(2^8)$ menggunakan operasi XOR sehingga diperoleh koefisien polinomial dari setiap elemen yang dinotasikan dalam heksadesimal adalah sebagai berikut:

Persamaan (3.42)	Koefisien Polinomial	Bentuk Polinomial
$5C$	01011100	$= x^6 + x^4 + x^3 + x^2$
25	00100101	$= x^5 + x^2 + 1$
54	01010100	$= x^6 + x^4 + x^2$
$8B$	10001011	$= x^7 + x^3 + x + 1$
$D1$	11010001	$= x^7 + x^6 + x^4 + 1$
17	00010111	$= x^4 + x^2 + x + 1$
25	00100101	$= x^5 + x^2 + 1$
90	10010000	$= x^7 + x^4$
91	10010001	$= x^7 + x^4 + 1$
55	01010101	$= x^6 + x^4 + x^2 + 1$
FC	11111100	$= x^7 + x^6 + x^5 + x^4 + x^3 + x^2$
13	00010011	$= x^4 + x + 1$
40	01000000	$= x^6$
$4A$	01001010	$= x^6 + x^3 + x$

$D0$	11010000	$= x^7 + x^6 + x^4$
75	01110101	$= x^6 + x^5 + x^4 + x^2 + 1$

Kunci ronde kedua	Koefisien Polinomial	Bentuk Polinomial
$7B$	01111011	$= x^6 + x^5 + x^4 + x^3 + x + 1$
$E9$	11101001	$= x^7 + x^6 + x^5 + x^3 + 1$
68	01101000	$= x^6 + x^5 + x^3$
CE	11001110	$= x^7 + x^6 + x^3 + x^2 + x$
$3A$	00111010	$= x^5 + x^4 + x^3 + x$
$A5$	10100101	$= x^7 + x^5 + x^2 + 1$
29	00101001	$= x^5 + x^3 + 1$
85	10000101	$= x^7 + x^2 + 1$
73	01110011	$= x^6 + x^5 + x^4 + x + 1$
$E8$	11101000	$= x^7 + x^6 + x^5 + x^3$
68	01101000	$= x^6 + x^5 + x^3$
$C9$	11001001	$= x^7 + x^6 + x^3 + 1$
32	00110010	$= x^5 + x^4 + x$
$A6$	10100110	$= x^7 + x^5 + x^2 + x$
$2F$	00101111	$= x^5 + x^3 + x^2 + x + 1$
EA	11101010	$= x^7 + x^6 + x^5 + x^3 + x$

Dengan memisalkan,

$$b_{32} = 5C \oplus 7B$$

$$b_{33} = 25 \oplus E9$$

$$b_{34} = 54 \oplus 68$$

$$b_{35} = 8B \oplus CE$$

$$b_{36} = D1 \oplus 3A$$

$$b_{37} = 17 \oplus A5$$

$$b_{38} = 25 \oplus 29$$

$$b_{39} = 90 \oplus 85$$

$$b_{40} = 91 \oplus 73$$

$$b_{41} = 55 \oplus E8$$

$$b_{42} = FC \oplus 68$$

$$b_{43} = 13 \oplus C9$$

$$b_{44} = 40 \oplus 32$$

$$b_{45} = 4A \oplus A6$$

$$b_{46} = D0 \oplus 2F$$

$$b_{47} = 75 \oplus EA$$

Maka perhitungan dari b_{32} sebagai berikut:

$$b_{32} = x^6 + x^4 + x^3 + x^2 \oplus x^6 + x^5 + x^4 + x^3 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{32} = 01011100 \oplus 01111011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{32} = 00100111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 27.

Maka perhitungan dari b_{33} sebagai berikut:

$$b_{33} = x^5 + x^2 + 1 \oplus x^7 + x^6 + x^5 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{33} = 00100101 \oplus 11101001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{33} = 11001100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai CC.

Maka perhitungan dari b_{34} sebagai berikut:

$$b_{34} = x^6 + x^4 + x^2 \oplus x^6 + x^5 + x^3$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{34} = 01010100 \oplus 01101000$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{34} = 00111100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $3C$.

Maka perhitungan dari b_{35} sebagai berikut:

$$b_{35} = x^7 + x^3 + x + 1 \oplus x^7 + x^6 + x^3 + x^2 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{35} = 10001011 \oplus 11001110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{35} = 01000101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 45.

Maka perhitungan dari b_{36} sebagai berikut:

$$b_{36} = x^7 + x^6 + x^4 + 1 \oplus x^5 + x^4 + x^3 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{36} = 11010001 \oplus 00111010$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{36} = 11101011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai EB.

Maka perhitungan dari b_{37} sebagai berikut:

$$b_{37} = x^4 + x^2 + x + 1 \oplus x^7 + x^5 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{37} = 00010111 \oplus 10100101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{37} = 10110010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $B2$.

Maka perhitungan dari b_{38} sebagai berikut:

$$b_{38} = x^5 + x^2 + 1 \oplus x^5 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{38} = 00100101 \oplus 00101001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{38} = 00001100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $0C$.

Maka perhitungan dari b_{39} sebagai berikut:

$$b_{39} = x^7 + x^4 \oplus x^7 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{39} = 10010000 \oplus 10000101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{39} = 00010101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 15.

Maka perhitungan dari b_{40} sebagai berikut:

$$b_{40} = x^7 + x^4 + 1 \oplus x^6 + x^5 + x^4 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{40} = 10010001 \oplus 01110011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{40} = 11100010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $E2$.

Maka perhitungan dari b_{41} sebagai berikut:

$$b_{41} = x^6 + x^4 + x^2 + 1 \oplus x^7 + x^6 + x^5 + x^3$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{41} = 01010101 \oplus 11101000$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{41} = 10111101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai BD.

Maka perhitungan dari b_{42} sebagai berikut:

$$b_{42} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 \oplus x^6 + x^5 + x^3$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{42} = 11111100 \oplus 01101000$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{42} = 10010100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 94.

Maka perhitungan dari b_{43} sebagai berikut:

$$b_{43} = x^4 + x + 1 \oplus x^7 + x^6 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{43} = 00010011 \oplus 11001001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{43} = 11011010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai DA.

Maka perhitungan dari b_{44} sebagai berikut:

$$b_{44} = x^6 \oplus x^5 + x^4 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{44} = 01000000 \oplus 00110010$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{44} = 01110010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 72.

Maka perhitungan dari b_{45} sebagai berikut:

$$b_{45} = x^6 + x^3 + x \oplus x^7 + x^6 + x^5 + x^3 + x^2$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{45} = 01001010 \oplus 11101100$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{45} = 11101100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai EC.

Maka perhitungan dari b_{46} sebagai berikut:

$$b_{46} = x^7 + x^6 + x^4 \oplus x^5 + x^3 + x^2 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{46} = 11010000 \oplus 00101111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{46} = 11111111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai FF.

Maka perhitungan dari b_{47} sebagai berikut:

$$b_{47} = x^6 + x^5 + x^4 + x^2 + 1 \oplus x^7 + x^6 + x^5 + x^3 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{47} = 01110101 \oplus 11101010$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{47} = 10011111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $9F$.

Hasil yang diperoleh adalah:

$$\begin{bmatrix} b_{32} & b_{36} & b_{40} & b_{44} \\ b_{33} & b_{37} & b_{41} & b_{45} \\ b_{34} & b_{38} & b_{42} & b_{46} \\ b_{35} & b_{39} & b_{43} & b_{47} \end{bmatrix} = \begin{bmatrix} 27 & EB & E2 & 72 \\ CC & B2 & BD & EC \\ 3C & 0C & 94 & FF \\ 45 & 15 & DA & 9F \end{bmatrix} \quad (3.43)$$

3.2.5 Transformasi *SubBytes*

Selanjutnya matriks masukan pada persamaan (3.43) mengalami substitusi

masing-masing elemen matriks menggunakan tabel *S-Box* agar persamaan (3.43) mengalami perubahan elemen sehingga penyandian menjadi semakin kuat. Maka hasil yang diperoleh adalah:

$$\begin{bmatrix} CC & E9 & 98 & 40 \\ 4B & 37 & 7A & CE \\ EB & FE & 22 & 16 \\ 6E & 59 & 57 & DB \end{bmatrix} \quad (3.44)$$

3.2.6 Transformasi *ShiftRows*

Matriks masukan pada persamaan (3.44) selanjutnya mengalami transformasi permutasi kembali pada setiap baris matriks dengan fungsi permutasi yang sudah penulis tentukan agar penyandian menjadi semakin kuat. Sehingga hasil yang diperoleh adalah:

$$\begin{bmatrix} CC & E9 & 98 & 40 \\ 4B & 37 & 7A & CE \\ EB & FE & 22 & 16 \\ 6E & 59 & 57 & DB \end{bmatrix} \quad (3.45)$$

3.2.7 Transformasi *AddRoundKey* dengan kunci ronde ketiga

Persamaan (3.45)	Koefisien Polinomial	Bentuk Polinomial
CC	11001100	$= x^7 + x^6 + x^3 + x^2$
$4B$	01001011	$= x^6 + x^3 + x + 1$
EB	11101011	$= x^7 + x^6 + x^5 + x^3 + x + 1$
$6E$	01101110	$= x^6 + x^5 + x^3 + x^2 + x$
$E9$	11101001	$= x^7 + x^6 + x^5 + x^3 + 1$
37	00110111	$= x^5 + x^4 + x^2 + x + 1$
FE	11111110	$= x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$
59	01011001	$= x^6 + x^4 + x^3 + 1$
98	10011000	$= x^7 + x^4 + x^3 +$
$7A$	01111010	$= x^6 + x^5 + x^4 + x^3 + x$
22	00100010	$= x^5 + x$
57	01010111	$= x^6 + x^4 + x^2 + x + 1$
40	01000000	$= x^6$
CE	11001110	$= x^7 + x^6 + x^3 + x^2 + x$
16	00010110	$= x^4 + x^2 + x$
DB	11011011	$= x^7 + x^6 + x^4 + x^3 + x^2 + x + 1$

Kunci ronde ketiga	Koefisien Polinomial	Bentuk Polinomial
$5D$	01011101	$= x^6 + x^4 + x^3 + x^2 + 1$
FC	11111100	$= x^7 + x^6 + x^5 + x^4 + x^3 + x^2$
EF	11101111	$= x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$
ED	11101101	$= x^7 + x^6 + x^5 + x^3 + x^2 + 1$
67	01100111	$= x^6 + x^5 + x^2 + x + 1$
59	01011001	$= x^6 + x^4 + x^3 + 1$
$C6$	11000110	$= x^7 + x^6 + x^2 + x$
68	01101000	$= x^6 + x^5 + x^3$
14	00010100	$= x^4 + x^2$
$B1$	10110001	$= x^7 + x^5 + x^4 + 1$
AE	10101110	$= x^7 + x^5 + x^3 + x^2 + x$
$A1$	10100001	$= x^7 + x^5 + 1$
26	00100110	$= x^5 + x^2 + x$
17	00010111	$= x^4 + x^2 + x + 1$
81	10000001	$= x^7 + 1$
$4B$	01001011	$= x^6 + x^3 + x + 1$

Dengan memisalkan,

$$b_{48} = CC \oplus 5D$$

$$b_{49} = 4B \oplus FC$$

$$b_{50} = EB \oplus EF$$

$$b_{51} = 6E \oplus ED$$

$$b_{52} = E9 \oplus 67$$

$$b_{53} = 37 \oplus 59$$

$$b_{54} = FE \oplus C6$$

$$b_{55} = 59 \oplus 68$$

$$b_{56} = 98 \oplus 14$$

$$b_{57} = 7A \oplus B1$$

$$b_{58} = 22 \oplus AE$$

$$b_{59} = 57 \oplus A1$$

$$b_{60} = 40 \oplus 26$$

$$b_{61} = CE \oplus 17$$

$$b_{62} = 16 \oplus 81$$

$$b_{63} = DB \oplus 4B$$

Maka perhitungan dari b_{48} sebagai berikut:

$$b_{48} = x^7 + x^6 + x^3 + x^2 \oplus x^6 + x^4 + x^3 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{48} = 11001100 \oplus 01011101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{48} = 10010001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 91.

Maka perhitungan dari b_{49} sebagai berikut:

$$b_{49} = x^6 + x^3 + x + 1 \oplus x^7 + x^6 + x^5 + x^4 + x^3 + x^2$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{49} = 01001011 \oplus 11111100$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{49} = 11001011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai CB.

Maka perhitungan dari b_{50} sebagai berikut:

$$b_{50} = x^7 + x^6 + x^5 + x^3 + x + 1 \oplus x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{50} = 11101011 \oplus 11101111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{50} = 11001101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai CD.

Maka perhitungan dari b_{51} sebagai berikut:

$$b_{51} = x^6 + x^5 + x^3 + x^2 + x \oplus x^7 + x^6 + x^5 + x^3 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{51} = 01101110 \oplus 11101101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{51} = 00110110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 36.

Maka perhitungan dari b_{52} sebagai berikut:

$$b_{52} = x^7 + x^6 + x^5 + x^3 + 1 \oplus x^6 + x^5 + x^2 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{52} = 11101001 \oplus 01100111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{52} = 10001110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $8E$.

Maka perhitungan dari b_{53} sebagai berikut:

$$b_{53} = x^5 + x^4 + x^2 + x + 1 \oplus x^6 + x^4 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{53} = 00110111 \oplus 01011001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{53} = 00100011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 23.

Maka perhitungan dari b_{54} sebagai berikut:

$$b_{54} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x \oplus x^7 + x^6 + x^2 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{54} = 11111110 \oplus 11000110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{54} = 11010000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $D0$.

Maka perhitungan dari b_{55} sebagai berikut:

$$b_{55} = x^6 + x^4 + x^3 + 1 \oplus x^6 + x^5 + x^3$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{55} = 01011001 \oplus 01101000$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{55} = 00000110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 06.

Maka perhitungan dari b_{56} sebagai berikut:

$$b_{56} = x^7 + x^4 + x^3 \oplus x^7 + x^3 + x^2$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{56} = 10011000 \oplus 10001100$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{56} = 10001100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $8C$.

Maka perhitungan dari b_{57} sebagai berikut:

$$b_{57} = x^6 + x^5 + x^4 + x^3 + x \oplus x^7 + x^5 + x^4 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{57} = 01111010 \oplus 10110001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{57} = 01111111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $7F$.

Maka perhitungan dari b_{58} sebagai berikut:

$$b_{58} = x^5 + x \oplus x^7 + x^5 + x^4 + x^3 + x^2$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{58} = 00100010 \oplus 10101110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{58} = 01000101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 45.

Maka perhitungan dari b_{59} sebagai berikut:

$$b_{59} = x^6 + x^4 + x^2 + x + 1 \oplus x^7 + x^5 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{59} = 01010111 \oplus 10100001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{59} = 11111000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $F8$.

Maka perhitungan dari b_{60} sebagai berikut:

$$b_{60} = x^6 \oplus x^5 + x^2 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{60} = 01000000 \oplus 00100110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{60} = 01100110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 66.

Maka perhitungan dari b_{61} sebagai berikut:

$$b_{61} = x^7 + x^6 + x^3 + x^2 + x \oplus x^4 + x^2 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{61} = 11001110 \oplus 00010111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{61} = 01011100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $5C$.

Maka perhitungan dari b_{62} sebagai berikut:

$$b_{62} = x^4 + x^2 + x \oplus x^7 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{62} = 00010110 \oplus 10000001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{62} = 01111111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $7F$.

Maka perhitungan dari b_{63} sebagai berikut:

$$b_{63} = x^7 + x^6 + x^4 + x^3 + x + 1 \oplus x^6 + x^3 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$b_{63} = 11011011 \oplus 01001011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{63} = 00011100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $1C$.

Sehingga diperoleh hasil sebagai berikut:

$$\begin{bmatrix} b_{48} & b_{52} & b_{56} & b_{60} \\ b_{49} & b_{53} & b_{57} & b_{61} \\ b_{50} & b_{54} & b_{58} & b_{62} \\ b_{51} & b_{55} & b_{59} & b_{63} \end{bmatrix} = \begin{bmatrix} 91 & 8E & 8C & 66 \\ CB & 23 & 7F & 5C \\ CD & D0 & 45 & 7F \\ 36 & 06 & F8 & 1C \end{bmatrix} \quad (3.46)$$

Persamaan (3.46) menjadi matriks keluaran dan pesan yang tersandi atau chiperteks. Sehingga elemen matriks yang termuat dalam persamaan (3.46) menjadi sebuah kalimat yang sulit dimengerti dengan merujuk pada tabel ASCII pada Lampiran 3. Sehingga teks hasil enkripsi yang diperoleh yaitu:

'ËÍ6Ž#ÐACKŒdelEøf\delFS

3.6 Implementasi Proses Dekripsi Pesan

Diberikan kunci dan pesan tersandi (chiperteks) dalam bentuk kalimat yang berupa kata, angka dan karakter dengan panjang kunci sebanyak 16 kata/angka/karakter. Dalam proses dekrisi penulis menggunakan kunci yang sama dengan proses enkripsi tetapi urutan kunci yang digunakan merupakan kebalikan dari proses enkripsi. Pada proses dekripsi dimulai dengan kunci ronde ketiga, kemudian kunci ronde kedua dan terakhir menggunakan kunci ronde pertama. Sebagaimana yang penulis jelaskan berikut:

Pesan tersandi (chiperteks) :

'ËÍ6Ž#ÐACKŒdelEøf\delFS

Selanjutnya mengkonversi kunci dan pesan yang berupa kata/angka/karakter ke dalam bentuk heksadesimal. Peneliti merujuk pada tabel sistem bilangan seperti yang penulis berikan pada Lampiran 2. Sehingga bilangan heksadesimal yang terbentuk berdasarkan kunci berupa kata dan karakter yang penulis berikan adalah:

'	Ë	Í	6	Ž	#	Ð	ACK	Œ	del	E	ø	f	\	del	FS
91	CB	CD	36	8E	23	D0	06	8C	7F	45	F8	66	5C	7F	1C

Kemudian membagi pesan tersandi yang berupa kata/angka/karakter yang telah direpresentasikan dalam bentuk heksadesimal menjadi beberapa blok. Peneliti memilih empat karakter dalam satu blok untuk membentuk matriks sebagai berikut:

'	Ë	Í	6
91	CB	CD	36
J_{01}	J_{02}	J_{03}	J_{04}

Ž	#	Ð	ACK
8E	23	D0	06
J_{05}	J_{06}	J_{07}	J_{08}

Œ	del	E	ø
8C	7F	45	F8
J_{09}	J_{10}	J_{11}	J_{12}

f	\	del	FS
66	5C	7F	1C
J_{13}	J_{14}	J_{15}	J_{16}

Ukuran matriks disesuaikan dengan jumlah karakter yang diambil dalam dalam setiap blok. Adapun susunan matriks pesan tersandi (chiperteks) pada persamaan adalah:

$$\begin{bmatrix} 91 & 8E & 8C & 66 \\ CB & 23 & 7F & 5C \\ CD & D0 & 45 & 7F \\ 36 & 06 & F8 & 1C \end{bmatrix} \quad (3.47)$$

dan matriks kunci ronde ketiga adalah:

$$\begin{bmatrix} 5D & 67 & 14 & 26 \\ FC & 59 & B1 & 17 \\ EF & C6 & AE & 81 \\ ED & 68 & A1 & 4B \end{bmatrix} \quad (3.48)$$

Selanjutnya melakukan proses pemcampuran atau XOR antara matriks pesan tersandi (chiperteks) dan matriks kunci ronde ketiga. Matriks pesan tersandi (chiperteks) $[i,j]$ di XOR dengan matriks kunci $[i,j]$ untuk $i = 1,2,3,4$ dan $j = 1,2,3,4$. Untuk melakukan penjumlahan dengan operasi XOR maka anggota dari setiap matriks pada persamaan (3.47) dan matriks kunci pada persamaan (3.48) ditulis dalam bentuk polinomial sehingga dapat diperoleh koefisien polinomial dari masing-masing elemen, yang kemudian dijumlahkan berdasarkan kaidah penjumlahan pada lapangan $GF(2^8)$ menggunakan operasi XOR sehingga diperoleh bentuk dan koefisien polinomial dari setiap elemen yang dinotasikan dalam heksadesimal adalah sebagai berikut:

Pesan tersandi (chiperteks)	**Koefisien Polinomial**	**Bentuk Polinomial**
91	10010001	$= x^7 + x^4 + 1$
CB	11001011	$= x^7 + x^6 + x^3 + x + 1$
CD	11001101	$= x^7 + x^6 + x^3 + x^2 + 1$
36	00110110	$= x^5 + x^4 + x^2 + x$
$8E$	10001110	$= x^7 + x^3 + x^2 + x$
23	00100011	$= x^5 + x + 1$
$D0$	11010000	$= x^7 + x^6 + x^4$
06	00000110	$= x^2 + x$

$8C$	10001100	$= x^7 + x^3 + x^2$
$7F$	01111111	$= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
45	01000101	$= x^6 + x^2 + 1$
$F8$	11111000	$= x^7 + x^6 + x^5 + x^4 + x^3$
66	01100110	$= x^6 + x^5 + x^2 + x$
$5C$	01011100	$= x^6 + x^4 + x^3 + x^2$
$7F$	01111111	$= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$1C$	00011100	$= x^4 + x^3 + x^2$

Kunci ronde ketiga	Koefisien Polinomial	Bentuk Polinomial
$5D$	01011101	$= x^6 + x^4 + x^3 + x^2 + 1$
FC	11111100	$= x^7 + x^6 + x^5 + x^4 + x^3 + x^2$
EF	11101111	$= x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$
ED	11101101	$= x^7 + x^6 + x^5 + x^3 + x^2 + 1$
67	01100111	$= x^6 + x^5 + x^2 + x + 1$
59	01011001	$= x^6 + x^4 + x^3 + 1$
$C6$	11000110	$= x^7 + x^6 + x^2 + x$
68	01101000	$= x^6 + x^5 + x^3$
14	00010100	$= x^4 + x^2$
$B1$	10110001	$= x^7 + x^5 + x^4 + 1$
AE	10101110	$= x^7 + x^5 + x^3 + x^2 + x$
$A1$	10100001	$= x^7 + x^5 + 1$
26	00100110	$= x^5 + x^2 + x$
17	00010111	$= x^4 + x^2 + x + 1$
81	10000001	$= x^6 + 1$
$4B$	01001011	$= x^6 + x^3 + x + 1$

Dengan memisalkan,

$$c_0 = 91 \oplus 5D$$

$$c_1 = CB \oplus FC$$

$$c_2 = CD \oplus EF$$

$$c_3 = 36 \oplus ED$$

$$c_4 = 8E \oplus 67$$

$$c_5 = 23 \oplus 59$$

$$c_6 = D0 \oplus C6$$

$$c_7 = 06 \oplus 68$$

$$c_8 = 8C \oplus 14$$

$$c_9 = 7F \oplus B1$$

$$c_{10} = 45 \oplus AE$$

$$c_{11} = F8 \oplus A1$$

$$c_{12} = 66 \oplus 26$$

$$c_{13} = 5C \oplus 17$$

$$c_{14} = 7F \oplus 81$$

$$c_{15} = 1C \oplus 4B$$

Maka perhitungan dari c_0 sebagai berikut:

$$c_0 = x^7 + x^4 + 1 \oplus x^6 + x^4 + x^3 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_0 = 10010001 \oplus 01011101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_0 = 11001100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai CC.

Maka perhitungan dari c_1 sebagai berikut:

$$c_1 = x^7 + x^6 + x^3 + x + 1 \oplus x^7 + x^6 + x^5 + x^4 + x^3 + x^2$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_1 = 11001011 \oplus 11111100$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_1 = 00110111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 37.

Maka perhitungan dari c_2 sebagai berikut:

$$c_2 = x^7 + x^6 + x^3 + x^2 + 1 \oplus x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_2 = 11001101 \oplus 11101111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_2 = 00100010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 22.

Maka perhitungan dari c_3 sebagai berikut:

$$c_3 = x^5 + x^4 + x^2 + x \oplus x^7 + x^6 + x^5 + x^3 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_3 = 00110110 \oplus 11101101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_3 = 11011011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai DB.

Maka perhitungan dari c_4 sebagai berikut:

$$c_4 = x^7 + x^3 + x \oplus x^6 + x^5 + x^2 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_4 = 10001110 \oplus 01100111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_4 = 11101001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $E9$.

Maka perhitungan dari c_5 sebagai berikut:

$$c_5 = x^5 + x + 1 \oplus x^6 + x^4 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_5 = 00100011 \oplus 01011001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_5 = 01111010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $7A$.

Maka perhitungan dari c_6 sebagai berikut:

$$c_6 = x^7 + x^6 + x^4 \oplus x^7 + x^6 + x^2 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_6 = 11010000 \oplus 11000110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_6 = 00010110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 16.

Maka perhitungan dari c_7 sebagai berikut:

$$c_7 = x^2 + x \oplus x^6 + x^5 + x^3$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_7 = 00000110 \oplus 01101000$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_7 = 01101110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $6E$.

Maka perhitungan dari c_8 sebagai berikut:

$$c_8 = x^7 + x^3 + x^2 \oplus x^4 + x^2$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_8 = 10001100 \oplus 00010100$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_8 = 10011000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 98.

Maka perhitungan dari c_9 sebagai berikut:

$$c_9 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \oplus x^7 + x^5 + x^4 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_9 = 01111111 \oplus 10110001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_9 = 11001110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai CE.

Maka perhitungan dari c_{10} sebagai berikut:

$$c_{10} = x^6 + x^2 + 1 \oplus x^7 + x^5 + x^3 + x^2 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{10} = 01000101 \oplus 10101110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{10} = 11101011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai EB.

Maka perhitungan dari c_{11} sebagai berikut:

$$c_{11} = x^7 + x^6 + x^5 + x^4 + x^3 \oplus x^7 + x^5 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{11} = 11111000 \oplus 10100001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{11} = 01011001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 59.

Maka perhitungan dari c_{12} sebagai berikut:

$$c_{12} = x^6 + x^5 + x^2 + x \oplus x^5 + x^2 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{12} = 01100110 \oplus 00100110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{12} = 01000000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 40.

Maka perhitungan dari c_{13} sebagai berikut:

$$c_{13} = x^6 + x^4 + x^3 + x^2 \oplus x^4 + x^2 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{13} = 01011100 \oplus 00010111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{13} = 01001011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $4B$.

Maka perhitungan dari c_{14} sebagai berikut:

$$c_{14} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \oplus x^7 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{14} = 01111111 \oplus 10000001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{14} = 11111110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai FE.

Maka perhitungan dari c_{15} sebagai berikut:

$$c_{15} = x^4 + x^3 + x^2 \oplus x^6 + x^3 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{15} = 00011100 \oplus 01001011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{15} = 01010111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 57.

Sehingga hasil yang diperoleh adalah:

$$\begin{bmatrix} c_0 & c_4 & c_8 & c_{12} \\ c_1 & c_5 & c_9 & c_{13} \\ c_2 & c_6 & c_{10} & c_{14} \\ c_3 & c_7 & c_{11} & c_{15} \end{bmatrix} = \begin{bmatrix} CC & E9 & 98 & 40 \\ 37 & 7A & CE & 4B \\ 22 & 16 & EB & FE \\ DB & 6E & 59 & 57 \end{bmatrix} \quad (3.49)$$

Setelah melakukan pencampuran atau XOR antara persamaan (3.47) dengan kunci kunci ronde ketiga pada persamaan (3.48) maka matriks keluaran yakni pada persamaan (3.49).

3.3.1 Transformasi *InvSiftRows*

Fungsi permutasi yang digunakan pada persamaan (3.49) adalah:

$$\begin{aligned} P(a_1a_2a_3a_4) &= (a_{\pi(1)}a_{\pi(2)}a_{\pi(3)}a_{\pi(4)}) \\ P(a_4a_1a_2a_3) &= (a_{\pi(4)}a_{\pi(1)}a_{\pi(2)}a_{\pi(3)}) \\ P(a_3a_4a_1a_2) &= (a_{\pi(3)}a_{\pi(4)}a_{\pi(1)}a_{\pi(2)}) \\ P(a_2a_3a_4a_1) &= (a_{\pi(2)}a_{\pi(3)}a_{\pi(4)}a_{\pi(1)}) \end{aligned} \tag{3.50}$$

Dalam hal ini penulis melakukan permutasi bertingkat dengan tujuan pengacakan dengan pola yang teratur seperti yang penulis jelaskan pada persamaan (3.50). Sehingga diperoleh hasil pencampuran kunci setiap elemen pada persamaan (3.49) dan dikenakan transformasi pergeseran elemen pada persamaan (3.50) adalah:

$$\begin{bmatrix} CC & E9 & 98 & 40 \\ 4B & 37 & 7A & CE \\ EB & FE & 22 & 16 \\ 6E & 59 & 57 & DB \end{bmatrix} \tag{3.51}$$

3.3.2 Transformasi *InvSubBytes*

Selanjutnya melakukan transformasi setiap elemen matriks pada persamaan (3.51) menggunakan tabel substitusi *InvS-Box*, dengan cara menginterpretasikan setiap elemen pada matriks masukan pada persamaan (3.51) sebagai dua bilangan heksadesimal dengan digit kiri menunjukkan indeks baris dan digit kanan menunjukkan indeks kolom pada tabel substitusi. Penulis menggunakan tabel substitusi invers untuk transformasi setiap elemen matriks masukan pada Tabel 2.4. Sehingga diperoleh matriks baru pada persamaan (3.52) sebagai hasil substitusi setiap elemen matriks dari persamaan (3.51) adalah:

$$\begin{bmatrix} 27 & EB & E2 & 72 \\ CC & B2 & BD & EC \\ 3C & 0C & 94 & FF \\ 45 & 15 & DA & 9F \end{bmatrix} \tag{3.52}$$

3.3.3 Transformasi *AddRoundKey* dengan kunci ronde kedua

Langkah selanjutnya adalah mencampur hasil transformasi pencampuran kolom vektor matriks masukan dan konstanta dengan kunci ronde kedua. Selanjutnya melakukan proses pemcampuran atau XOR antara matriks masukan pada persamaan (3.52) dengan matriks kunci ronde kedua. Matriks masukan pada persamaan (3.52) $[i, j]$ di XOR dengan matriks kunci ronde kedua $[i, j]$ untuk $i = 1, 2, 3, 4$ dan $j = 1, 2, 3, 4$. Untuk melakukan penjumlahan dengan operasi XOR maka anggota dari setiap matriks pada persamaan (3.52) dan matriks kunci ronde kedua, penulis merepresentasikan koefisien polinomial dari setiap elemen pada matriks tersebut, kemudian dijumlahkan berdasarkan kaidah penjumlahan pada lapangan $GF(2^8)$ menggunakan operasi XOR sehingga diperoleh koefisien polinomial dari setiap elemen yang dinotasikan dalam heksadesimal adalah sebagai berikut:

Persamaan (3.52)	Koefisien Polinomial	Bentuk Polinomial
27	00100111	$= x^5 + x^2 + x + 1$
CC	11001100	$= x^7 + x^6 + x^3 + x^2$
$3C$	00111100	$= x^5 + x^4 + x^3 + x^2$
45	01000101	$= x^6 + x^2 + 1$
EB	11101011	$= x^7 + x^6 + x^5 + x^3 + x + 1$
$B2$	10110010	$= x^7 + x^5 + x$
$0C$	00001100	$= x^3 + x^2$
15	00010101	$= x^5 + x^2 + 1$
$E2$	11100010	$= x^7 + x^6 + x^5 + x$
BD	10111101	$= x^7 + x^5 + x^4 + x^3 + x^2 + 1$
94	10010100	$= x^7 + x^4 + x^2$
DA	11011010	$= x^7 + x^6 + x^4 + x^3 + x$
72	01110010	$= x^6 + x^5 + x^4 + x$
EC	11101100	$= x^6 + x^5 + x^3 + x^2$
FF	11111111	$= x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$9F$	10011111	$= x^7 + x^4 + x^3 + x^2 + x + 1$

Kunci ronde kedua	Koefisien Polinomial	Bentuk Polinomial
$7B$	01111011	$= x^6 + x^5 + x^4 + x^3 + x + 1$
$E9$	11101001	$= x^7 + x^6 + x^5 + x^3 + 1$
68	01101000	$= x^6 + x^5 + x^3$
CE	11001110	$= x^7 + x^6 + x^3 + x^2 + x$
$3A$	00111010	$= x^5 + x^4 + x^3 + x$
$A5$	10100101	$= x^7 + x^5 + x^2 + 1$
29	00101001	$= x^5 + x^3 + 1$
85	10000101	$= x^7 + x^2 + 1$
73	01110011	$= x^6 + x^5 + x^4 + x + 1$
$E8$	11101000	$= x^7 + x^6 + x^5 + x^3$
68	01101000	$= x^6 + x^5 + x^3$
$C9$	11001001	$= x^7 + x^6 + x^3 + 1$
32	00110010	$= x^5 + x^4 + x$
$A6$	10100110	$= x^7 + x^5 + x^2 + x$
$2F$	00101111	$= x^5 + x^3 + x^2 + x + 1$
EA	11101010	$= x^7 + x^6 + x^5 + x^3 + x$

Dengan memisalkan,

$$c_{16} = 27 \oplus 7B$$

$$c_{17} = CC \oplus E9$$

$$c_{18} = 3C \oplus 68$$

$$c_{19} = 45 \oplus CE$$

$$c_{20} = EB \oplus 3A$$

$$c_{21} = B2 \oplus A5$$

$$c_{22} = 0C \oplus 29$$

$$c_{23} = 15 \oplus 85$$

$$c_{24} = E2 \oplus 73$$

$$c_{25} = BD \oplus E8$$

$$c_{26} = 94 \oplus 68$$

$$c_{27} = DA \oplus C9$$

$$c_{28} = 72 \oplus 32$$

$$c_{29} = EC \oplus A6$$

$$c_{30} = FF \oplus 2F$$

$$c_{31} = 9F \oplus EA$$

Maka perhitungan dari c_{16} sebagai berikut:

$$c_{16} = x^5 + x^2 + x + 1 \oplus x^6 + x^5 + x^4 + x^3 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{16} = 00100111 \oplus 01111011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{16} = 01011100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $5C$.

Maka perhitungan dari c_{17} sebagai berikut:

$$c_{17} = x^7 + x^6 + x^3 + x^2 \oplus x^7 + x^6 + x^5 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{17} = 11001100 \oplus 11101001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{17} = 00100101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 25.

Maka perhitungan dari c_{18} sebagai berikut:

$$c_{18} = x^5 + x^4 + x^3 + x^2 \oplus x^6 + x^5 + x^3$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{18} = 00111100 \oplus 01101000$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{18} = 01010100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 54.

Maka perhitungan dari c_{19} sebagai berikut:

$$c_{19} = x^6 + x^2 + 1 \oplus x^7 + x^6 + x^3 + x^2 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{19} = 01000101 \oplus 11001110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{19} = 10001011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $8B$.

Maka perhitungan dari c_{20} sebagai berikut:

$$c_{20} = x^7 + x^6 + x^5 + x^3 + x + 1 \oplus x^5 + x^4 + x^3 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{20} = 11101011 \oplus 00111010$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{20} = 00000001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 01.

Maka perhitungan dari c_{21}sebagai berikut:

$$c_{21} = x^7 + x^5 + x^4 + x \oplus x^7 + x^5 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{21} = 10110010 \oplus 10100101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{21} = 00010111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 17.

Maka perhitungan dari c_{22} sebagai berikut:

$$c_{22} = x^3 + x^2 \oplus x^5 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{22} = 00001100 \oplus 00101001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{22} = 00100101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 25.

Maka perhitungan dari c_{23} sebagai berikut:

$$c_{23} = x^4 + x^2 + 1 \oplus x^7 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{23} = 00010101 \oplus 10000101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{23} = 10010000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 90.

Maka perhitungan dari c_{24} sebagai berikut:

$$c_{24} = x^7 + x^6 + x^5 + x \oplus x^6 + x^5 + x^4 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{24} = 11100010 \oplus 01110011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{24} = 10010001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 91.

Maka perhitungan dari c_{25} sebagai berikut:

$$c_{25} = x^7 + x^5 + x^4 + x^3 + x^2 + 1 \oplus x^7 + x^6 + x^5 + x^3$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{25} = 10111101 \oplus 11101000$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{25} = 01010101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 55.

Maka perhitungan dari c_{26} sebagai berikut:

$$c_{26} = x^7 + x^4 + x^2 \oplus x^6 + x^5 + x^3$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{26} = 10010100 \oplus 01101000$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{26} = 11111100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai FC.

Maka perhitungan dari c_{27} sebagai berikut:

$$c_{27} = x^7 + x^6 + x^4 + x^3 + x \oplus x^7 + x^6 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{27} = 11011010 \oplus 11001001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{27} = 00010011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 13.

Maka perhitungan dari c_{28} sebagai berikut:

$$c_{28} = x^6 + x^5 + x^4 + x \oplus x^5 + x^4 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{28} = 01110010 \oplus 00110010$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{28} = 01000000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 40.

Maka perhitungan dari c_{29} sebagai berikut:

$$c_{29} = x^7 + x^6 + x^5 + x^3 + x^2 \oplus x^7 + x^6 + x^5 + x^3 + x^2$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{29} = 11101100 \oplus 11101100$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{29} = 01001010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $4A$.

Maka perhitungan daric_{30} sebagai berikut:

$$c_{30} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \oplus x^5 + x^3 + x^2 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{30} = 11111111 \oplus 00101111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $b_{30} = 11010000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $D0$.

Maka perhitungan dari c_{31} sebagai berikut:

$$c_{31} = x^7 + x^4 + x^3 + x^2 + x + 1 \oplus x^7 + x^6 + x^5 + x^3 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{31} = 10011111 \oplus 11101010$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{31} = 01110101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 75.

Sehingga hasil yang diperoleh adalah:

$$\begin{bmatrix} c_{16} & c_{20} & c_{24} & c_{28} \\ c_{17} & c_{21} & c_{25} & c_{29} \\ c_{18} & c_{22} & c_{26} & c_{30} \\ c_{19} & c_{23} & c_{27} & c_{31} \end{bmatrix} = \begin{bmatrix} 5C & 01 & 91 & 40 \\ 25 & 17 & 55 & 4A \\ 54 & 25 & FC & D0 \\ 8B & 90 & 13 & 75 \end{bmatrix} \quad (3.53)$$

3.3.4 Transformasi *InvMixColumns*

Transformasi *MixColumns* yang dilakukan dengan mencampur vektor kolom pada matriks masukan pada persamaan (3.53) dengan suatu matriks yang memuat invers dari konstata dengan nilai koefisien terkecil dalam polinomial, yakni:

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \quad (3.54)$$

Persamaan (3.53) direpresentasikan ke dalam polinomial untuk mempermudah proses perhitungan dan penyandian pesan dalam transformasi pencampuran vektor kolom dengan vektor matriks konstanta maka peneliti merepresentasikan koefisien polinomial matriks masukan pada persamaan (3.53) kemudian melakukan perkalian dengan operasi $(\cdot)$ dan penjumlahan dengan operasi $(\oplus)$ seperti yang dijelaskan sebagai berikut:

Kolom 1	Koefisien Polinomial	Bentuk Polinomial
$5C$	01011100	$= x^6 + x^4 + x^3 + x^2$
25	00100101	$= x^5 + x^2 + 1$
54	01010100	$= x^6 + x^4 + x^2$
$8B$	10001011	$= x^7 + x^3 + x + 1$

Selanjutnya pesan dikalikan dengan matriks 4×4 dibawah ini :

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} 5C \\ 25 \\ 54 \\ 8B \end{bmatrix}$$

Untuk ,

$$\begin{aligned} 09 \quad & 00001001 \quad = x^3 + 1 \\ 0B \quad & 00001011 \quad = x^3 + x + 1 \\ 0D \quad & 00001101 \quad = x^3 + x^2 + 1 \\ 0E \quad & 00001110 \quad = x^3 + x^2 + x \end{aligned}$$

Baris pertama pada persamaan (3.53) dikalikan dengan kolom pertama pada persamaan (3.54) dengan memisalkan:

$$Y_1 = 0E \cdot 5C \oplus 0B \cdot 25 \oplus 0D \cdot 54 \oplus 09 \cdot 8B$$

$$Y_2 = 09 \cdot 5C \oplus 0E \cdot 25 \oplus 0B \cdot 54 \oplus 0D \cdot 8B$$

$$Y_3 = 0D \cdot 5C \oplus 09 \cdot 25 \oplus 0E \cdot 54 \oplus 0B \cdot 8B$$

$$Y_4 = 0B \cdot 5C \oplus 0D \cdot 25 \oplus 09 \cdot 54 \oplus 0E \cdot 8B$$

Maka perhitungan dari Y_1 sebagai berikut:

$$
\begin{aligned}
Y_1 &= (x^3+x^2+x)(x^6+x^4+x^3+x^2) \\
&\quad \oplus (x^3+x+1)(x^5+x^2+1) \\
&\quad \oplus (x^3+x^2+1)(x^6+x^4+x^2) \\
&\quad \oplus (x^3+1)(x^7+x^3+x+1) \\
&= (x^9+x^7+x^6+x^5+x^8+x^6+x^5+x^4+x^7+x^5+x^4+x^3) \\
&\quad \oplus (x^8+x^5+x^3+x^6+x^3+x+x^5+x^2+1) \\
&\quad \oplus (x^9+x^7+x^5+x^8+x^6+x^4+x^6+x^4+x^2) \\
&\quad \oplus (x^{10}+x^6+x^4+x^3+x^7+x^3+x+1) \\
&= (x^9+x^8+x^5+x^3)\ modulo(\ x^5+x^4+x^2+x) \\
&\quad \oplus (x^8+x^6+x+x^2+1) modulo (x^4+x^3+x+1) \\
&\quad \oplus (x^9+x^7+x^5+x^8+x^2\ ) modulo\ (x^5+x^4+x^2+x) \\
&\quad \oplus (x^{10}+x^6+x^4+x^7+x+1)\ modulo\ (x^6+x^5+x^3+x^2) \\
&= (x^8+x^3+x^4+x^2+x)\ modulo\ (x^4+x^3+x+1) \\
&\quad \oplus x^6+x^2+\ x^4+x^3 \\
&\quad \oplus (x^7+x^8+x^4+x)\ modulo\ (x^4+x^3+x+1) \\
&\quad \oplus (x^4+x^7+x+1+x^5+x^3+x^2) \\
&= (x^2+1) \oplus (x^6+x^2+\ x^4+x^3) \oplus (x^7+\ x^3+1) \\
&\quad \oplus (x^4+x^7+x+1+x^5+x^3+x^2)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_1 = 00000101 \oplus 01011100 \oplus 10001001 \oplus 10111111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_1 = 01101111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $6F$.

Maka perhitungan dari Y_2 sebagai berikut:

$$
\begin{aligned}
Y_2 &= (x^3+1)(x^6+x^4+x^3+x^2) \oplus (x^3+x^2+x)(x^5+x^2+1) \\
&\quad \oplus (x^3+x+1)(x^6+x^4+x^2) \\
&\quad \oplus (x^3+x^2+1)(x^7+x^3+x+1) \\
&= (x^9+x^7+x^6+x^5+x^6+x^4+x^3+x^2) \\
&\quad \oplus (x^8+x^5+x^3+x^7+x^4+x^2+x^6+x^3+x) \\
&\quad \oplus (x^9+x^7+x^5+x^7+x^5+x^3+x^6+x^4+x^2) \oplus \\
&\quad (x^{10}+x^6+x^4+x^3+x^9+x^5+x^3+x^2+x^7+x^3+x+1) \\
&= (x^9+x^7+x^5+x^4+x^3+x^2) \\
&\quad \oplus (x^8+x^5+x^7+x^4+x^2+x^6+x) \\
&\quad \oplus (x^9+x^3+x^6+x^4+x^2) \\
&\quad \oplus (x^{10}+x^6+x^4+x^9+x^5+x^2+x^7+x^3+x+1) \\
&= (x^9+x^7+x^5+x^4+x^3+x^2) modulo (x^5+x^4+x^2+x) \\
&\quad \oplus (x^8+x^5+x^7+x^4+x^2+x^6+x)
\end{aligned}
$$

$$
\begin{aligned}
& modulo(x^4 + x^3 + x + 1) \\
& \oplus (x^9 + x^3 + x^6 + x^4 + x^2) modulo(x^5 + x^4 + x^2 + x) \\
& \oplus (x^{10} + x^6 + x^4 + x^9 + x^5 + x^2 + x^7 + x^3 + x + 1) \\
& modulo(x^6 + x^5 + x^3 + x^2) \\
= \; & (x^7 + x^3 + x) \oplus (x^5 + x^7 + x^2 + x^6 + x^3 + 1) \\
& \oplus (x^3 + x^6 + x^5 + x) \\
& \oplus (x^4 + x^9 + x^7 + x + 1) modulo(x^5 + x^4 + x^2 + x) \\
= \; & (x^7 + x^3 + x) \oplus (x^5 + x^7 + x^2 + x^6 + x^3 + 1) \\
& \oplus (x^3 + x^6 + x^5 + x) \oplus (x^7 + 1 + x^5 + x^2)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_2 = 10001010 \oplus 11101101 \oplus 01101010 \oplus 10100101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_2 = 10101000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $A8$.

Maka perhitungan dari Y_3 sebagai berikut:

$$
\begin{aligned}
Y_3 = \; & (x^3 + x^2 + 1)(x^6 + x^4 + x^3 + x^2) \oplus (x^3 + 1)(x^5 + x^2 + 1) \\
& \oplus (x^3 + x^2 + x)(x^6 + x^4 + x^2) \\
& \oplus (x^3 + x + 1)(x^7 + x^3 + x + 1) \\
= \; & (x^9 + x^7 + x^6 + x^5 + x^8 + x^6 + x^5 + x^4 + x^6 + x^4 + x^3 + x^2) \\
& \oplus (x^8 + x^5 + x^3 + x^5 + x^2 + 1) \\
& \oplus (x^9 + x^7 + x^5 + x^8 + x^6 + x^4 + x^6 + x^4 + x^2) \\
& \oplus (x^{10} + x^6 + x^4 + x^3 + x^8 + x^4 + x^2 + x + x^7 + x^3 + x + 1) \\
= \; & (x^9 + x^7 + x^8 + x^6 + x^3 + x^2) \oplus (x^8 + x^3 + x^2 + 1) \\
& \oplus (x^9 + x^7 + x^5 + x^8 + x^2) \oplus (x^{10} + x^6 + x^8 + x^2 + x^7 + 1) \\
= \; & (x^9 + x^7 + x^8 + x^6 + x^3 + x^2) \; modulo \; (x^5 + x^4 + x^2 + x) \\
& \oplus (x^8 + x^3 + x^2 + 1) \; modulo \; (x^4 + x^3 + x + 1) \\
& \oplus (x^9 + x^7 + x^5 + x^8 + x^2) \; modulo \; (x^5 + x^4 + x^2 + x) \oplus \\
& (x^{10} + x^6 + x^8 + x^2 + x^7 + 1) \; modulo \; (x^6 + x^5 + x^3 + x^2) \\
= \; & (x^7 + x^8 + x^6 + x^3 + x^2 + x^5 + x^4 + x^2 + x) \\
& \oplus (x^3 + x^2 + 1 + x^4 + x^3 + x + 1) \\
& \oplus (x^7 + x^5 + x^8 + x^2 + x^5 + x^4 + x^2 + x) \\
& \oplus (x^6 + x^8 + x^2 + x^7 + 1 + x^6 + x^5 + x^3 + x^2) \\
= \; & (x^7 + x^8 + x^6 + x^3 + x^5 + x^4 + x) \oplus (x^2 + x^4 + x) \\
& \oplus (x^7 + x^8 + x^4 + x) \oplus (x^8 + x^7 + 1 + x^5 + x^3) \\
= \; & (x^7 + x^8 + x^6 + x^3 + x^5 + x^4 + x) \; modulo \; (x^4 + x^3 + x + 1) \\
& \oplus (x^2 + x^4 + x) \\
& \oplus (x^7 + x^8 + x^4 + x) \; modulo \; (x^4 + x^3 + x + 1) \\
& \oplus (x^8 + x^7 + 1 + x^5 + x^3) \; modulo \; (x^4 + x^3 + x + 1) \\
= \; & (x^7 + x^6 + x^5 + 1) \oplus (x^2 + x^4 + x) \\
& \oplus (x^7 + x^3 + 1) \oplus (x^7 + x^5 + x^4 + x)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_3 = 11100010 \oplus 00010110 \oplus 10001010 \oplus 10110010$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_3 = 00110000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 30.

Maka perhitungan dari Y_4 sebagai berikut:

$$\begin{aligned}
Y_4 &= (x^3 + x + 1)(x^6 + x^4 + x^3 + x^2) \\
&\quad \oplus (x^3 + x^2 + 1)(x^5 + x^2 + 1) \\
&\quad \oplus (x^3 + 1)(x^6 + x^4 + x^2) \\
&\quad \oplus (x^3 + x^2 + x)(x^7 + x^3 + x + 1) \\
&= (x^9 + x^7 + x^6 + x^5 + x^7 + x^5 + x^4 + x^3 + x^6 + x^4 + x^3 + x^2) \\
&\quad \oplus (x^8 + x^5 + x^3 + x^7 + x^4 + x^2 + x^5 + x^2 + 1) \\
&\quad \oplus (x^9 + x^7 + x^5 + x^6 + x^4 + x^2) \\
&\quad \oplus (x^{10} + x^6 + x^4 + x^3 + x^9 + x^5 + x^3 + x^2 \\
&\quad + x^8 + x^4 + x^2 + x) \\
&= (x^9 + x^2)\ modulo\ (x^5 + x^4 + x^2 + x) \\
&\quad \oplus (x^8 + x^3 + x^7 + x^4 + 1)\ modulo\ (x^4 + x^3 + x + 1) \\
&\quad \oplus (x^9 + x^7 + x^5 + x^6 + x^4 + x^2)\ modulo\ (x^5 + x^4 + x^2 + x) \\
&\quad \oplus (x^{10} + x^6 + x^9 + x^5 + x^8 + x)\ modulo\ (x^6 + x^5 + x^3 + x^2) \\
&= (x^9 + x^2)\ modulo\ (x^5 + x^4 + x^2 + x) \\
&\quad \oplus (x^8 + x^3 + x^7 + x^4 + 1)\ modulo\ (x^4 + x^3 + x + 1) \\
&\quad \oplus (x^9 + x^7 + x^5 + x^6 + x^4 + x^2)\ modulo\ (x^5 + x^4 + x^2 + x) \\
&\quad \oplus ((x^{10} + x^6 + x^9 + x^5 + x^8 + x) \\
&\quad modulo\ (x^6 + x^5 + x^3 + x^2) \\
&= (x^5 + x^4 + x) \oplus (x^7 + x) \oplus (x^7 + x^6 + x) \\
&\quad \oplus (x^8 + x^3 + x^5 + x^4)\ modulo\ (x^4 + x^3 + x + 1) \\
&= (x^5 + x^4 + x) \oplus (x^7 + x) \oplus (x^7 + x^6 + x) \oplus (x^5 + x + 1)
\end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_4 = 00110010 \oplus 10000010 \oplus 11000010 \oplus 00100011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_4 = 01010001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 51.

Kolom 2	Koefisien Polinomial	Bentuk Polinomial
01	00000001	$= 1$
17	00010111	$= x^4 + x^2 + x + 1$
25	00100101	$= x^5 + x^2 + 1$
90	10010000	$= x^7 + x^4$

Baris pertama pada persamaan (3.53) dikalikan dengan kolom kedua pada persamaan (3.54) dengan memisalkan:

$$Y_5 = 0E \cdot 01 \oplus 0B \cdot 17 \oplus 0D \cdot 25 \oplus 09 \cdot 90$$

$$Y_6 = 09 \cdot 01 \oplus 0E \cdot 17 \oplus 0B \cdot 25 \oplus 0D \cdot 90$$

$$Y_7 = 0D \cdot 01 \oplus 09 \cdot 17 \oplus 0E \cdot 25 \oplus 0B \cdot 90$$

$$Y_8 = 0B \cdot 01 \oplus 0D \cdot 17 \oplus 09 \cdot 25 \oplus 0E \cdot 90$$

Maka perhitungan dari Y_5 sebagai berikut:

$$\begin{aligned} Y_5 &= (x^3+x^2+x)(1) \oplus (x^3+x+1)(x^4+x^2+x+1) \\ &\quad \oplus (x^3+x^2+1)(x^5+x^2+1) \oplus (x^3+1)(x^7+x^4) \\ &= (x^3+x^2+x) \oplus (x^7+x^5+x^4+x^3+x^5+x^3+x^2+x \\ &\quad +x^4+x^2+x+1) \\ &\quad \oplus (x^8+x^5+x^3+x^7+x^4+x^2+x^5+x^2+1) \\ &\quad \oplus (x^{10}+x^7+x^7+x^4) \\ &= (x^3+x^2+x) \oplus (x^7+1) \oplus (x^8+x^3+x^7+x^4+1) \oplus \\ &\quad (x^{10}+x^4) \\ &= (x^3+x^2+x) \oplus (x^7+1) \\ &\quad \oplus (x^8+x^3+x^7+x^4+1)\ modulo\ (x^4+x^3+x+1) \\ &\quad \oplus (x^{10}+x^4)\ modulo\ (x^6+x^5+x^3+x^2) \\ &= (x^3+x^2+x) \oplus (x^7+1) \oplus (x^7+x) \\ &\quad \oplus (x^4+x^6+x^5+x^3+x^2) \end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_5 = 00001110 \oplus 10000001 \oplus 10000010 \oplus 01111100$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_5 = 01111101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $7D$.

Maka perhitungan dari Y_6 sebagai berikut:

$$\begin{aligned} Y_6 &= (x^3+1)(1) \oplus (x^3+x^2+x)(x^4+x^2+x+1) \\ &\quad \oplus (x^3+x+1)(x^5+x^2+1) \oplus (x^3+x^2+1)(x^7+x^4) \\ &= (x^3+1) \oplus (x^7+x^5+x^4+x^3 \\ &\quad +x^6+x^4+x^3+x^2+x^4+x^2+x+1) \\ &\quad \oplus (x^8+x^5+x^3+x^6+x^3+x+x^5+x^2+1) \\ &\quad \oplus (x^{10}+x^7+x^9+x^6+x^7+x^4) \end{aligned}$$

$$
\begin{aligned}
&= (x^3+1) \oplus (x^7+x^5+x^4+x^6+x+1) \\
&\quad \oplus (x^8+x^6+x+x^2+1) \oplus (x^{10}+x^7+x^9+x^6+x^7+x^4) \\
&= (x^3+1) \oplus (x^7+x^5+x^4+x^6+x+1) \\
&\quad \oplus (x^8+x^6+x+x^2+1)\ modulo\ (x^4+x^3+x+1) \\
&\quad \oplus (x^{10}+x^7+x^9+x^6+x^7+x^4) \\
&\quad modulo\ (x^6+x^5+x^3+x^2) \\
&= (x^3+1) \oplus (x^7+x^5+x^4+x^6+x+1) \\
&\quad \oplus (x^6+x^2+x^4+x^3) \oplus (x^9+x^4+x^5+x^3+x^2) \\
&\quad modulo (x^5+x^4+x^2+x) \\
&= (x^3+1) \oplus (x^7+x^5+x^4+x^6+x+1) \\
&\quad \oplus (x^6+x^2+x^4+x^3) \oplus (x^3+x)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_6 = 00001001 \oplus 11110011 \oplus 01011100 \oplus 00001010$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_6 = 10011111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $9F$.

Maka perhitungan dari Y_7 sebagai berikut:

$$
\begin{aligned}
Y_7 &= (x^3+x^2+1)(1) \oplus (x^3+1)(x^4+x^2+x+1) \\
&\quad \oplus (x^3+x^2+x)(x^5+x^2+1) \\
&\quad \oplus (x^3+x+1)(x^7+x^4) \\
&= (x^3+x^2+1) \oplus (x^7+x^5+x^4+x^3+x^4+x^2+x+1) \\
&\quad \oplus (x^8+x^5+x^3+x^7+x^4+x^2+x^6+x^3+x) \\
&\quad \oplus (x^{10}+x^7+x^8+x^5+x^7+x^4) \\
&= (x^3+x^2+1) \oplus (x^7+x^5+x^3+x^2+x+1) \\
&\quad \oplus (x^5+x^7+x^2+x^6+x^3+1) \oplus (x^6+x^2+x+1)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_7 = 00001101 \oplus 10101111 \oplus 11101101 \oplus 01000111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_7 = 01101111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $6F$.

Maka perhitungan dari Y_8 sebagai berikut:

$$
\begin{aligned}
Y_8 &= (x^3+x+1)(1) \oplus (x^3+x^2+1)(x^4+x^2+x+1) \\
&\quad \oplus (x^3+1)(x^5+x^2+1) \oplus (x^3+x^2+x)(x^7+x^4) \\
&= (x^3+x+1) \oplus
\end{aligned}
$$

$$
\begin{aligned}
& (x^7 + x^5 + x^4 + x^3 + x^6 + x^4 + x^3 + x^2 + x^4 + x^2 + x + 1) \\
& \oplus (x^8 + x^5 + x^3 + x^5 + x^2 + 1) \\
& \oplus (x^{10} + x^7 + x^9 + x^6 + x^8 + x^5) \\
= \; & (x^3 + x + 1) \oplus (x^7 + x^5 + x^6 + x^4 + x + 1) \\
& \oplus (x^8 + x^3 + x^2 + 1) \; modulo \; (x^4 + x^3 + x + 1) \\
& \oplus (x^{10} + x^7 + x^9 + x^6 + x^8 + x^5) modulo (x^6 + x^5 + x^3 + x^2) \\
= \; & (x^3 + x + 1) \oplus (x^7 + x^5 + x^6 + x^4 + x + 1) \\
& \oplus (x^2 + \; x^4 + x) \\
& \oplus (x^7 + x^9 + x^8 + x^3 + x^2) modulo (x^5 + x^4 + x^2 + x) \\
= \; & (x^3 + x + 1) \oplus (x^7 + x^5 + x^6 + x^4 + x + 1) \\
& \oplus (x^2 + \; x^4 + x) \oplus (x^7 + x^5 + \; 1)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_8 = 00001011 \oplus 11110011 \oplus 00010110 \oplus 10100001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_8 = 11111110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai FE.

Kolom 3	Koefisien Polinomial	Bentuk Polinomial
91	10010001	$= x^7 + x^4 + 1$
55	01010101	$= x^6 + x^4 + x^2 + 1$
FC	11111100	$= x^7 + x^6 + x^5 + x^4 + x^3 + x^2$
13	00010011	$= x^4 + x + 1$

Baris pertama pada persamaan (3.60) dikalikan dengan kolom ketiga pada persamaan (3.59) dengan memisalkan:

$$Y_9 = 0E \cdot 91 \oplus 0B \cdot 55 \oplus 0D \cdot FC \oplus 09 \cdot 13$$

$$Y_{10} = 09 \cdot 91 \oplus 0E \cdot 55 \oplus 0B \cdot FC \oplus 0D \cdot 13$$

$$Y_{11} = 0D \cdot 91 \oplus 09 \cdot 55 \oplus 0E \cdot FC \oplus 0B \cdot 13$$

$$Y_{12} = 0B \cdot 91 \oplus 0D \cdot 55 \oplus 09 \cdot \; FC \oplus 0E \cdot 13$$

Maka perhitungan dari Y_9 sebagai berikut:

$$
\begin{aligned}
Y_9 \quad = \quad & (x^3 + x^2 + x)(x^7 + x^4 + 1) \oplus (x^3 + x + 1)(x^6 + x^4 + x^2 + 1) \\
& \oplus (x^3 + x^2 + 1)(x^7 + x^6 + x^5 + x^4 + x^3 + x^2) \\
& \oplus (x^3 + 1)(x^4 + x + 1)
\end{aligned}
$$

$$
\begin{aligned}
= \; & (x^{10}+x^7+x^3+x^9+x^6+x^2+x^8+x^5+x) \\
& \oplus (x^9+x^7+x^5+x^3+x^7+x^5+x^3+x+x^6+x^4+x^2+1) \\
& \oplus (x^{10}+x^9+x^8+x^7+x^6+x^5+x^9+x^8+x^7+x^6+x^5 \\
& +x^4+x^7+x^6+x^5+x^4+x^3+x^2) \\
& \oplus (x^7+x^4+x^3+x^4+x+1) \\
= \; & (x^{10}+x^7+x^3+x^9+x^6+x^2+x^8+x^5+x) \\
& \oplus (x^9+x+x^6+x^4+x^2+1) \\
& \oplus (x^{10}++x^7+x^6+x^5+x^3+x^2) \\
& \oplus (x^7+x^3+x+1) \\
= \; & (x^{10}+x^7+x^3+x^9+x^6+x^2+x^8+x^5+x) \\
& modulo(x^6+x^5+x^3+x^2) \\
& \oplus (x^9+x+x^6+x^4+x^2+1) modulo(x^5+x^4+x^2+x) \\
& \oplus (x^{10}++x^7+x^6+x^5+x^3+x^2) \\
& modulo(x^6+x^5+x^3+x^2) \oplus (x^7+x^3+x+1) \\
= \; & (x^7+x^9+x^8+x) modulo(x^5+x^4+x^2+x) \\
& \oplus (x^6+1+x^5) \oplus (x^7) \oplus (x^7+x^3+x+1 \\
& x^7+x^8+x^5+x^4+x^2) \\
& \oplus (x^6+1+x^5) \oplus (x^7) \oplus (x^7+x^3+x+1 \\
& x^7+x^5+x^2+x^3+x+1) \\
& \oplus (x^6+1+x^5) \oplus (x^7) \oplus (x^7+x^3+x+1)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_9 = 10101111 \oplus 01100001 \oplus 10000000 \oplus 10001011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_9 = 11000101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $C5$.

Maka perhitungan dari Y_{10} sebagai berikut:

$$
\begin{aligned}
Y_{10} = \; & (x^3+1)(x^7+x^4+1) \oplus (x^3+x^2+x)(x^6+x^4+x^2+1) \\
& \oplus (x^3+x+1)(x^7+x^6+x^5+x^4+x^3+x^2) \\
& \oplus (x^3+x^2+1)(x^4+x+1) \\
= \; & (x^{10}+x^7+x^3+x^7+x^4+1) \oplus \\
& (x^9+x^7+x^5+x^3+x^8+x^6+x^4+x^2+x^7+x^5+x^3+x) \\
& \oplus (x^{10}+x^9+x^8+x^7+x^6+x^5+x^8 \\
& +x^7+x^6+x^5+x^4+x^3+x^7+x^6+x^5+x^4+x^3+x^2) \\
& \oplus (x^7+x^4+x^3+x^6+x^3+x^2+x^4+x+1) \\
= \; & (x^{10}+x^3+x^4+1) modulo(x^6+x^5+x^3+x^2) \\
& \oplus (x^9+x^8+x^6+x^4+x^2+x) modulo(x^5+x^4+x^2+x) \\
& \oplus (x^{10}+x^9+x^7+x^6+x^5+x^2) \\
& modulo(x^6+x^5+x^3+x^2) \oplus (x^7+x^6+x^2+x+1) \\
= \; & (x^4+1+x^6+x^5+x^2) \\
& \oplus (x^8+x^6+x^5) modulo(x^4+x^3+x+1) \\
& \oplus (x^9+x^7+x^3) modulo(x^5+x^4+x^2+x)
\end{aligned}
$$

$$\begin{aligned} & \oplus (x^7 + x^6 + x^2 + x + 1) \\ = \; & (x^4 + 1 + x^6 + x^5 + x^2) \oplus (x^6 + x^5 + x^4 + x^3 + x + 1) \\ & \oplus (x^7 + x^3 + x^5 + x^4 + x^2 + x) \oplus (x^7 + x^6 + x^2 + x + 1) \end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_{10} = 01110101 \oplus 01111011 \oplus 10111110 \oplus 11000111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_{10} = 01110111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 77.

Maka perhitungan dari Y_{11} sebagai berikut:

$$\begin{aligned} Y_{11} = \; & (x^3 + x^2 + 1)(x^7 + x^4 + 1) \oplus (x^3 + 1)(x^6 + x^4 + x^2 + 1) \\ & \oplus (x^3 + x^2 + x)(x^7 + x^6 + x^5 + x^4 + x^3 + x^2) \\ & \oplus (x^3 + x + 1)(x^4 + x + 1) \\ = \; & (x^{10} + x^7 + x^3 + x^9 + x^6 + x^2 + x^7 + x^4 + 1) \\ & \oplus (x^9 + x^7 + x^5 + x^3 + x^6 + x^4 + x^2 + 1) \\ & \oplus (x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^9 + x^8 \\ & + x^7 + x^6 + x^5 + x^4 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3) \\ & \oplus (x^7 + x^4 + x^3 + x^5 + x^2 + x + x^4 + x + 1) \\ = \; & (x^{10} + x^3 + x^9 + x^6 + x^2 + x^4 + 1) \\ & modulo(x^6 + x^5 + x^3 + x^2) \\ & \oplus (x^9 + x^7 + x^5 + x^3 + x^6 + x^4 + x^2 + 1) \\ & modulo(x^5 + x^4 + x^2 + x) \\ & \oplus (x^{10} + x^8 + x^7 + x^6 + x^5 + x^3) \\ & modulo(x^6 + x^5 + x^3 + x^2) \\ & \oplus (x^7 + x^3 + x^5 + x^2 + 1) \\ = \; & (x^9 + x^4 + 1 + x^5) modulo(x^5 + x^4 + x^2 + x) \\ & \oplus (x^7 + x^3 + x^6 + 1 + x) \\ & \oplus (x^8 + x^7 + x^2) modulo(x^4 + x^3 + x + 1) \\ & \oplus (x^7 + x^3 + x^5 + x^2 + 1) \\ = \; & (1 + x^2 + x) \oplus (x^7 + x^3 + x^6 + 1 + x) \\ & \oplus (x^7 + x^2 + x^4 + x^3 + x + 1) \oplus (x^7 + x^3 + x^5 + x^2 + 1) \end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_{11} = 00000111 \oplus 11001011 \oplus 10011111 \oplus 10101101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_{11} = 11111110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai FE.

Maka perhitungan dari Y_{12} sebagai berikut:

$$
\begin{aligned}
Y_{12} &= (x^3+x+1)(x^7+x^4+1) \\
&\quad \oplus (x^3+x^2+1)(x^6+x^4+x^2+1) \\
&\quad \oplus (x^3+1)(x^7+x^6+x^5+x^4+x^3+x^2) \\
&\quad \oplus (x^3+x^2+x)(x^4+x+1) \\
&= (x^{10}+x^7+x^3+x^8+x^5+x+x^7+x^4+1) \\
&\quad \oplus (x^9+x^7+x^5+x^3+x^8+x^6+x^4+x^2 \\
&\quad +x^6+x^4+x^2+1) \\
&\quad \oplus (x^{10}+x^9+x^8+x^7+x^6+x^5+x^7 \\
&\quad +x^6+x^5+x^4+x^3+x^2) \\
&\quad \oplus (x^7+x^4+x^3+x^6+x^3+x^2+x^5+x^2+x) \\
&= (x^{10}+x^3+x^8+x^5+x+x^4+1) \\
&\quad modulo(x^6+x^5+x^3+x^2) \\
&\quad \oplus (x^9+x^7+x^5+x^3+x^8+1) modulo(x^5+x^4+x^2+x) \\
&\quad \oplus (x^{10}+x^9+x^8+x^4+x^3+x^2) \\
&\quad modulo(x^6+x^5+x^3+x^2) \oplus x^7+x^4+x^6+x^5+x \\
&= (x^8+x+x^4+1+x^6+x^2) modulo(x^4+x^3+x+1) \\
&\quad \oplus (x^9+x^7+x^3+x^8+1+x^4+x^2+x) \\
&\quad modulo(x^5+x^4+x^2+x) \\
&\quad \oplus (x^9+x^8+x^4+x^6+x^5) modulo(x^5+x^4+x^2+x) \\
&\quad \oplus (x^7+x^4+x^6+x^5+x) \\
&= (x^6+x^2+x^3) \oplus (x^7+x^3+x^8+1+x^5) \\
&\quad \oplus (x^6+x^2+x^4+x^3+1) \oplus (x^7+x^4+x^6+x^5+x) \\
&= (x^6+x^2+x^3) \oplus (x^7+x^5+x^4+x) \\
&\quad \oplus (x^6+x^2+x^4+x^3+1) \oplus (x^7+x^4+x^6+x^5+x)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_{12} = 01001100 \oplus 10110010 \oplus 01011101 \oplus 11110010$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_{12} = 01100111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 67.

Kolom 4	Bentuk Biner	Bentuk Polinomial
40	01000000	$= x^6$
$4A$	01001010	$= x^6+x^3+x$
$D0$	11010000	$= x^7+x^6+x^4$
75	01110101	$= x^6+x^5+x^4+x^2+1$

Baris pertama pada persamaan (3.60) dikalikan dengan kolom keempat pada persamaan (3.59) dengan memisalkan:

$$Y_{13} = 0E \cdot 40 \oplus 0B \cdot 4A \oplus 0D \cdot D0 \oplus 09 \cdot 75$$

$$Y_{14} = 09 \cdot 40 \oplus 0E \cdot 4A \oplus 0B \cdot D0 \oplus 0D \cdot 75$$

$$Y_{15} = 0D \cdot 40 \oplus 09 \cdot 4A \oplus 0E \cdot D0 \oplus 0B \cdot 75$$

$$Y_{16} = 0B \cdot 40 \oplus 0D \cdot 4A \oplus 09 \cdot\ D0 \oplus 0E \cdot 75$$

Maka perhitungan dari Y_{13} sebagai berikut:

$$\begin{aligned}
Y_{13} &= (x^3 + x^2 + x)(x^6) \oplus (x^3 + x + 1)(x^6 + x^3 + x) \\
&\quad \oplus (x^3 + x^2 + 1)(x^7 + x^6 + x^4) \\
&\quad \oplus (x^3 + 1)(x^6 + x^5 + x^4 + x^2 + 1) \\
&= (x^9 + x^8 + x^7) \\
&\quad \oplus (x^9 + x^6 + x^4 + x^7 + x^4 + x^2 + x^6 + x^3 + x) \\
&\quad \oplus (x^{10} + x^9 + x^7 + x^9 + x^8 + x^6 + x^7 + x^6 + x^4) \\
&\quad \oplus (x^9 + x^8 + x^7 + x^5 + x^3 + x^6 + x^5 + x^4 + x^2 + 1) \\
&= (x^9 + x^8 + x^7) \oplus (x^9 + x^7 + x^2 + x^3 + x) \\
&\quad \oplus (x^{10} + x^8 + x^4) \\
&\quad \oplus x^9 + x^8 + x^7 + x^3 + x^6 + x^4 + x^2 + 1 \\
&= (x^9 + x^8 + x^7) modulo (x^5 + x^4 + x^2 + x) \\
&\quad \oplus (x^9 + x^7 + x^2 + x^3 + x) modulo (x^5 + x^4 + x^2 + x) \\
&\quad \oplus (x^{10} + x^8 + x^4) modulo (x^6 + x^5 + x^3 + x^2) \\
&\quad \oplus (x^9 + x^8 + x^7 + x^3 + x^6 + x^4 + x^2 + 1 \\
&\quad modulo\ x^5 + x^4 + x^2 + x) \\
&= (x^8 + x^7 + x^5 + x^4 + x^2 + x) modulo (x^4 + x^3 + x + 1) \\
&\quad \oplus (x^7 + x^3 + \ x^5 + x^4) \\
&\quad \oplus (x^8 + x^4 + \ x^6 + x^5 + x^3 + x^2) modulo (x^4 + x^3 + x + 1) \\
&\quad \oplus (x^9 + x^8 + x^7 + x^3 + x^6 + 1 \ + \ x^5 + x) \\
&\quad modulo (x^5 + x^4 + x^2 + x) \\
&= (x^7 + x^5 + x^2 + \ x^3 + 1) \oplus \\
&\quad (x^7 + x^3 + \ x^5 + x^4) \oplus (x^6 + x^5 + x^2 + x + 1) \\
&\quad \oplus (x^8 + x^7 + x^3 + x^6 + 1 \ + \ x^4 + x^2) \\
&\quad modulo (x^4 + x^3 + x + 1) \\
&\quad x^7 + x^5 + x^2 + \ x^3 + 1 \oplus x^7 + x^3 + \ x^5 + x^4 \\
&\quad \oplus \ x^6 + x^5 + x^2 + x + 1 \oplus x^7 + x^6 + x^2 + x
\end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_{13} = 10101101 \oplus 10111000 \oplus 01100111 \oplus 11000110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_{13} = 00000001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 01.

Maka perhitungan dari Y_{14} sebagai berikut:

$$\begin{aligned}
Y_{14} &= (x^3 + 1)(x^6) \oplus (x^3 + x^2 + x)(x^6 + x^3 + x) \\
&\quad \oplus (x^3 + x + 1)(x^7 + x^6 + x^4)
\end{aligned}$$

$$
\begin{aligned}
& \oplus (x^3+x^2+1)(x^6+x^5+x^4+x^2+1) \\
= \; & (x^9+x^6) \oplus (x^9+x^6+x^4+x^8+x^5+x^3+x^7+x^4+x^2) \\
& \oplus (x^{10}+x^9+x^7+x^8+x^7+x^5+x^7+x^6+x^4) \\
& \oplus (x^9+x^8+x^7+x^5+x^3+x^8+x^7+x^6+x^4+x^2 \\
& +x^6+x^5+x^4+x^2+1) \\
= \; & (x^9+x^6) \oplus (x^9+x^6+x^8+x^5+x^3+x^7+x^2) \\
& \oplus (x^{10}+x^9+x^7+x^8+x^5+x^6+x^4) \oplus (x^9+x^3+1) \\
= \; & (x^9+x^6) modulo (x^5+x^4+x^2+x) \\
& \oplus (x^9+x^6+x^8+x^5+x^3+x^7+x^2) \\
& modulo (x^5+x^4+x^2+x) \\
& \oplus (x^{10}+x^9+x^7+x^8+x^5+x^6+x^4) \\
& modulo (x^6+x^5+x^3+x^2) \\
& \oplus (x^9+x^3+1) modulo (x^5+x^4+x^2+x) \\
= \; & (x^6+x^5+x^4+x^2+x) \\
& \oplus (x^6+x^8+x^3+x^7+x^4+x) \\
& \oplus (x^9+x^7+x^8+x^4+x^3+x^2) modulo (x^5+x^4+x^2+x) \\
& \oplus (x^3+1+x^5+x^4+x^2+x) \\
= \; & (x^6+x^5+x^4+x^2+x) \\
& \oplus (x^6+x^8+x^3+x^7+x^4+x) modulo (x^4+x^3+x+1) \\
& \oplus (x^7+x^8+x^3+x^5+x) modulo (x^4+x^3+x+1) \\
& \oplus (x^3+1+x^5+x^4+x^2+x) \\
= \; & (x^6+x^5+x^4+x^2+x) \oplus (x^6+x^7+1) \\
& \oplus (x^7+x^5+x^4+1) \oplus (x^3+1+x^5+x^4+x^2+x)
\end{aligned}
$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_{14} = 01110110 \oplus 11000001 \oplus 10110001 \oplus 00111111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_{14} = 00110000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 30.

Maka perhitungan dari Y_{15} sebagai berikut:

$$
\begin{aligned}
Y_{15} = \; & (x^3+x^2+1)(x^6) \oplus (x^3+1)(x^6+x^3+x) \\
& \oplus (x^3+x^2+x)(x^7+x^6+x^4) \\
& \oplus (x^3+x+1)(x^6+x^5+x^4+x^2+1) \\
= \; & (x^9+x^8+x^6) \oplus (x^9+x^6+x^4+x^6+x^3+x) \\
& \oplus (x^{10}+x^9+x^7+x^9+x^8+x^6+x^8+x^7+x^5) \\
& \oplus (x^9+x^8+x^7+x^5+x^3+x^7+x^6+x^5+x^3+x \\
& +x^6+x^5+x^4+x^2+1) \\
= \; & (x^9+x^8+x^6) \oplus (x^9+x^4+x^3+x) \\
& \oplus (x^{10}+x^6+x^5) \\
& \oplus (x^9+x^8+x+x^5+x^4+x^2+1) \\
= \; & (x^9+x^8+x^6) modulo (x^5+x^4+x^2+x) \\
& \oplus (x^9+x^4+x^3+x) modulo (x^5+x^4+x^2+x)
\end{aligned}
$$

$$\begin{aligned} & \oplus (x^{10}+x^6+x^5) modulo (x^6+x^5+x^3+x^2) \\ & \oplus (x^9+x^8+x+x^5+x^4+x^2+1) \\ & modulo (x^5+x^4+x^2+x) \\ = \; & (x^8+x^6+x^5+x^4+x^2+x) modulo (x^4+x^3+x+1) \\ & \oplus (x^3+x^5+x^2) \oplus (x^3+x^2) \\ & \oplus (x^8+1) modulo (x^4+x^3+x+1) \\ = \; & (x^6+x^5+x^2+x^3+1) \oplus (x^3+x^5+x^2) \\ & \oplus (x^3+x^2) \oplus (x^4+x^3+x) \end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_{15} = 01101101 \oplus 00101100 \oplus 00001100 \oplus 00011010$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_{15} = 11010111$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $D7$.

Maka perhitungan dari Y_{16} sebagai berikut:

$$\begin{aligned} Y_{16} = \; & (x^3+x+1)(x^6) \oplus (x^3+x^2+1)(x^6+x^3+x) \\ & \oplus (x^3+1)(x^7+x^6+x^4) \\ & \oplus (x^3+x^2+x)(x^6+x^5+x^4+x^2+1) \\ = \; & (x^9+x^7+x^6) \\ & \oplus (x^9+x^6+x^4+x^8+x^5+x^3+x^6+x^3+x) \\ & \oplus (x^{10}+x^9+x^7+x^7+x^6+x^4) \\ & \oplus (x^9+x^8+x^7+x^5+x^3+x^8+x^7+x^6+x^4+x^2 \\ & +x^7+x^6+x^5+x^3+x) \\ = \; & (x^9+x^7+x^6) modulo (x^5+x^4+x^2+x) \\ & \oplus (x^9+x^4+x^8+x^5+x) modulo (x^5+x^4+x^2+x) \\ & \oplus (x^{10}+x^9+x^6+x^4) modulo (x^6+x^5+x^3+x^2) \\ & \oplus (x^9+x^4+x^2+x^7+x) modulo (x^5+x^4+x^2+x) \\ = \; & (x^7+x^6+x^5+x^4+x^2+x) \\ & \oplus (x^8+x^2) modulo (x^4+x^3+x+1) \\ & \oplus (x^9+x^4+x^5+x^3+x^2) modulo (x^5+x^4+x^2+x) \\ & \oplus (x^7+x^5) \\ = \; & (x^7+x^6+x^5+x^4+x^2+x) \\ & \oplus (x^2+x^4+x^3+x+1) \oplus (x^3+x) \oplus (x^7+x^5) \end{aligned}$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$Y_{16} = 11110110 \oplus 00011111 \oplus 00001010 \oplus 10100000$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $Y_{16} = 11000101$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $C5$.

Sehingga hasil yang diperoleh dari proses transformasi *InvMixColumn* adalah sebagai berikut:

$$\begin{bmatrix} Y_1 & Y_5 & Y_9 & Y_{13} \\ Y_2 & Y_6 & Y_{10} & Y_{14} \\ Y_3 & Y_7 & Y_{11} & Y_{15} \\ Y_4 & Y_8 & Y_{12} & Y_{16} \end{bmatrix} = \begin{bmatrix} 6F & 7D & C5 & 01 \\ A8 & 9F & 77 & 30 \\ 30 & 6F & FE & D7 \\ 51 & FE & 67 & C5 \end{bmatrix} \quad (3.55)$$

3.3.5 Transformasi *InvSiftRows*

Mengulangi transformasi *InvSiftRows* pada matriks masukan persamaan (3.55) menggunakan fungsi permutasi yang digunakan pada persamaan (3.55). Sehingga diperoleh hasil permutasi bertingkat yang dikenakan transformasi pergeseran elemen pada persamaan (3.56) adalah:

$$\begin{bmatrix} 6F & 7D & C5 & 01 \\ 30 & A8 & 9F & 77 \\ FE & D7 & 30 & 6F \\ FE & 67 & C5 & 51 \end{bmatrix} \quad (3.56)$$

3.3.6 Transformasi *InvSubBytes*

Selanjutnya melakukan pengulangan transformasi setiap elemen matrikspada persamaan (3.56) menggunakan tabel substitusi *InvS-Box* pada Tabel 2.4. Diperoleh matriks baru pada persamaan (3.57) sebagai hasil substitusi setiap elemen matriks dari persamaan (3.56) adalah:

$$\begin{bmatrix} 06 & 13 & 07 & 09 \\ 08 & 6F & 6E & 02 \\ 0C & 0D & 08 & 06 \\ 0C & 0A & 07 & 70 \end{bmatrix} \quad (3.57)$$

3.3.7 Transformasi *AddRounKey*

Selanjutnya melakukan pengulangan pencampuran kunci pertama dengan persamaan (3.57). Sehingga diperoleh matriks baru pada persamaan (3.58) sebagai pencampuran setiap elemen matriks kunci ronde pertama dengan persamaan (3.57) adalah:

Persamaan (3.57)	Koefisien Polinomial	Bentuk Polinomial
06	00000110	$= x^2 + x$
08	00001000	$= x^3$
0C	00001100	$= x^3 + x^2$
0C	00001100	$= x^3 + x^2$
13	00010011	$= x^4 + x + 1$
6F	01101111	$= x^6 + x^5 + x^3 + x^2 + x + 1$
0D	00001101	$= x^3 + x^2 + 1$
0A	00001010	$= x^3 + x$
07	00000111	$= x^2 + x + 1$
6E	01101110	$= x^6 + x^5 + x^3 + x^2 + x$
08	00001000	$= x^3$
07	00000111	$= x^2 + x + 1$
09	00001001	$= x^3 + 1$
02	00000010	$= x$
06	00000110	$= x^2 + x$
70	01110000	$= x^6 + x^5 + x^4$

Kunci ronde pertama	Koefisien Polinomial	Bentuk Polinomial
55	01010101	$= x^6 + x^4 + x^2 + 1$
49	01001001	$= x^6 + x^3 + 1$
4E	01001110	$= x^6 + x^3 + x^2 + x$
4D	01001101	$= x^6 + x^3 + x^2 + 1$
41	01000001	$= x^6 + 1$
4C	01001100	$= x^6 + x^3 + x^2$
49	01001001	$= x^6 + x^3 + 1$
4B	01001011	$= x^6 + x^3 + x + 1$
49	01001001	$= x^6 + x^3 + 1$
4D	01001101	$= x^6 + x^3 + x^2 + 1$
41	01000001	$= x^6 + 1$
4C	01001100	$= x^6 + x^3 + x^2$
41	01000001	$= x^6 + 1$
4E	01001110	$= x^6 + x^3 + x^2 + x$
47	01000111	$= x^6 + x^2 + x + 1$
23	00100011	$= x^5 + x + 1$

Dengan memisalkan,

$$c_{32} = 06 \oplus 55$$

$$c_{33} = 08 \oplus 49$$

$$c_{34} = 0C \oplus 4E$$

$$c_{35} = 0C \oplus 4D$$

$$c_{36} = 13 \oplus 41$$

$$c_{37} = 6F \oplus 4C$$

$$c_{38} = 0D \oplus 49$$

$$c_{39} = 0A \oplus 4B$$

$$c_{40} = 07 \oplus 49$$

$$c_{41} = 6E \oplus 4D$$

$$c_{42} = 08 \oplus 41$$

$$c_{43} = 07 \oplus 4C$$

$$c_{44} = 09 \oplus 41$$

$$c_{45} = 02 \oplus 4E$$

$$c_{46} = 06 \oplus 47$$

$$c_{47} = 70 \oplus 23$$

Maka perhitungan dari c_{32} sebagai berikut:

$$c_{32} = x^2 + x \oplus x^6 + x^4 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{32} = 00000110 \oplus 01010101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{32} = 01010011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 53.

Maka perhitungan dari c_{33} sebagai berikut:

$$c_{33} = x^3 \oplus x^6 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{33} = 00001000 \oplus 01001001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{33} = 01000001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 41.

Maka perhitungan dari c_{34} sebagai berikut:

$$c_{34} = x^3 + x^2 \oplus x^6 + x^3 + x^2 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{34} = 00001100 \oplus 01001110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{34} = 01000010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 42.

Maka perhitungan dari c_{35} sebagai berikut:

$$c_{35} = x^3 + x^2 \oplus x^6 + x^3 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{35} = 00001100 \oplus 01001101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{35} = 01000001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 41.

Maka perhitungan dari c_{36} sebagai berikut:

$$c_{36} = x^4 + x + 1 \oplus x^6 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{36} = 00010011 \oplus 01000001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{36} = 01010010$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 52.

Maka perhitungan dari c_{37} sebagai berikut:

$$c_{37} = x^6 + x^5 + x^3 + x^2 + x + 1 \oplus x^6 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{37} = 01101111 \oplus 01000001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{37} = 00100011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 23.

Maka perhitungan dari c_{38} sebagai berikut:

$$c_{38} = x^6 + x^2 \oplus x^6 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{38} = 00001101 \oplus 01001001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{38} = 01000100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 44.

Maka perhitungan dari c_{39} sebagai berikut:

$$c_{39} = x^3 + x \oplus x^6 + x^3 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{39} = 00001010 \oplus 01001011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{39} = 01000001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 41.

Maka perhitungan dari c_{40} sebagai berikut:

$$c_{40} = x^2 + x + 1 \oplus x^6 + x^3 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{40} = 00000111 \oplus 01001001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{40} = 01001110$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $4E$.

Maka perhitungan dari c_{41} sebagai berikut:

$$c_{41} = x^6 + x^5 + x^3 + x^2 + x \oplus x^6 + x^3 + x^2 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{41} = 01101110 \oplus 01001101$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{41} = 00100011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 23.

Maka perhitungan dari c_{42} sebagai berikut:

$$c_{42} = x^3 \oplus x^6 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{42} = 00001000 \oplus 01000001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{42} = 01001001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 49.

Maka perhitungan dari c_{43} sebagai berikut:

$$c_{43} = x^2 + x + 1 \oplus x^6 + x^3 + x^2$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{43} = 00000111 \oplus 01001100$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{43} = 01001011$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $4B$.

Maka perhitungan dari c_{44} sebagai berikut:

$$c_{44} = x^3 + 1 \oplus x^6 + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{44} = 00001001 \oplus 01000001$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{44} = 01001000$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 48.

Maka perhitungan dari c_{45} sebagai berikut:

$$c_{45} = x \oplus x^6 + x^3 + x^2 + x$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{45} = 00000010 \oplus 01001110$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{45} = 01001100$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai $4C$.

Maka perhitungan dari c_{46} sebagai berikut:

$$c_{46} = x^2 + x \oplus x^6 + x^2 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{46} = 00000110 \oplus 01000111$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{46} = 01000001$. Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh nilai 41.

Maka perhitungan dari c_{47} sebagai berikut:

$$c_{47} = x^6 + x^5 + x^4 \oplus x^5 + x + 1$$

Dengan koefisien dari polinomial maka dapat ditulis sebagai:

$$c_{47} = 01110000 \oplus 00100011$$

Berdasarkan kaidah penjumlahan ekslusif OR maka diperoleh koefisien polinomial dari $c_{47} = 01010011$. Sehingga dalam notasi heksadesimal denga merujuk pada tabel ASCII diperoleh nilai 53.

Sehingga hasil yang diperoleh adalah:

$$\begin{bmatrix} c_{32} & c_{36} & c_{40} & c_{44} \\ c_{33} & c_{37} & c_{41} & c_{45} \\ c_{34} & c_{38} & c_{42} & c_{46} \\ c_{35} & c_{39} & c_{43} & c_{47} \end{bmatrix} = \begin{bmatrix} 53 & 52 & 4E & 48 \\ 41 & 23 & 23 & 4C \\ 42 & 44 & 49 & 41 \\ 41 & 41 & 4B & 53 \end{bmatrix} \quad (3.58)$$

Sehingga dalam notasi heksadesimal dengan merujuk pada tabel ASCII diperoleh pesan asli (plainteks) yang dapat dibaca dan dimengerti sebagai berikut:

SABAR#DAN#IKHLAS

3.7 Ilmu Kriptografi dalam Konteks Keagamaan

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Pengamanan dilakukan dengan mengenkrip (menyandi) informasi dengan suatu kunci khusus. Data asli atau data yang belum dienkrip dinamakan plainteks sedangkan data yang tersandi dengan suatu kunci maka dinamakan chiperteks. Selanjutnya data yang telah dienkripsi dideskripsikan (diuraikan) kembali seperti bentuk semula.

Kegiatan enkripsi atau penyandian pesan dengan suatu kunci khusus harus memiliki keamanan yang kuat dan tidak mudah disadap menggunakan beberapa transformasi agar pesan yang dienkripsi tidak mudah dipahami orang lain. Namun pesan yang diterima juga harus sesuai dengan pesan yang disampaikan. Dalam konteks ini, Allah Swt. juga menghendaki setiap umat-Nya untuk bersikap amanah dalam menyampaikan informasi atau pesan sebagaimana yang dinyatakan dalam al-Quran surah al-Kahfi/18:28, yaitu:

وَٱصۡبِرۡ نَفۡسَكَ مَعَ ٱلَّذِينَ يَدۡعُونَ رَبَّهُم بِٱلۡغَدَوٰةِ وَٱلۡعَشِيِّ يُرِيدُونَ وَجۡهَهُۥۖ وَلَا تَعۡدُ عَيۡنَاكَ عَنۡهُمۡ تُرِيدُ زِينَةَ ٱلۡحَيَوٰةِ ٱلدُّنۡيَاۖ وَلَا تُطِعۡ مَنۡ أَغۡفَلۡنَا قَلۡبَهُۥ عَن ذِكۡرِنَا وَٱتَّبَعَ هَوَىٰهُ وَكَانَ أَمۡرُهُۥ فُرُطٗا ٢٨

"Dan bersabarlah kamu bersama-sama dengan orang-orang yang menyeru Tuhannya di pagi dan senja hari dengan mengharap keridhaan-Nya; dan janganlah kedua matamu berpaling dari mereka (karena) mengharapkan perhiasan dunia ini; dan janganlah kamu mengikuti orang yang hatinya telah Kami lalaikan dari mengingati Kami, serta menuruti hawa nafsunya dan adalah keadaannya itu melewati batas"(QS al-Kahfi/18:28).

Selanjutnya untuk menyampaikan informasi maka chiperteks harus dikembalikan kepada bentuk semula agar mudah dimengerti dan dipahami oleh penerima pesan. Proses pengembalian pesan dari chiperteks menjadi teks asli (plainteks) membutuhkan beberapa transformasi yang merupakan balikan atau invers dari transformasi yang dipakai pada proses enkripsi atau penyandian. Oleh karena itu pengembalian pesan kepada bentuk teks asli harus sesuai dan tidak mengalami tambahan atau pengurangan karakter sehingga dapat dimengerti dan dipahami oleh penerima pesan sebagaimana firman Allah Swt. dalam surah al-Anfal/8:27 yang berbunyi:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَخُونُواْ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓاْ أَمَٰنَٰتِكُمۡ وَأَنتُمۡ تَعۡلَمُونَ ٢٧

"Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui"(QS al-Anfal/8:27).

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan pembahasan yang telah dilakukan sebelumnya dapat diperoleh kesimpulan sebagai berikut:

1. Untuk mengawali penyandian pesan dengan menggunakan algoritma pengamanan data tingkat lanjut untuk mengamankan informasi yang penulis berikan berupa teks asli "SABAR#DAN#IKHLAS" dan kunci "UINMALIKIMALANG#". Kemudian mengkonversi pesan dan kunci dalam heksadesimal. Setelah mendapatkan pesan dan kunci dalam heksadesimal maka dibagi menjadi beberapa blok. Dalam setiap blok berisi empat karakter. Selanjutnya bentuk blok-blok pesan dan kunci yang terkonversi dalam heksadesimal menjadi penyusun matrik 4×4. Penulis menggunakan tiga kali perputaran atau ronde untuk melakukan penyandian atau enkripsi pesan sehingga memakai tiga kunci yang berbeda dalam setiap ronde. Sehingga dilakukan ekspansi atau perluasan kunci untuk memperoleh kunci kedua dan ketiga seperti yang penulis jelaskan pada bab pemhasan. Dengan langkah-langkah 1) Melakukan operasi rotasi dengan suatu fungsi rotasi, 2) Melakukan substitusi pada setiap elemen matriks kunci, 3) Melakukan penjumlahan dengan konstanta ronde. Diperoleh hasil ekspansi atau perluasan kunci menjadi tiga kunci ronde sebagai berikut:

55	41	49	41	7B	3A	73	32	5D	67	14	26
49	4C	4D	4E	E9	A5	E8	A6	FC	59	B1	17
4E	49	41	47	68	29	68	2F	EF	C6	AE	81
4D	4B	4C	23	CE	85	C9	EA	ED	68	A1	4B
Ronde Pertama				Ronde Kedua				Ronde Ketiga			

Pesan/berita dan kunci berupa huruf/angka/karakter dikonversi ke dalam bentuk heksadesimal dan dibagi menjadi beberapa blok sehingga membentuk matriks 4 × 4 dan melakukan transformasi *AddRoundKey* atau pencampuran kunci yakni XOR antara plainteks dengan kunci ronde pertama, kemudian melakukan transformasi *SubBytes* (substitusi setiap elemen matriks masukan) dengan merujuk pada tabel *S-Box*. Dilanjutkan dengan melakukan transformasi *ShiftRows*, *MixColumn*, *AddRoundKey* dengan kunci ronde kedua, transformasi *SubBytes* kedua, transformasi *ShiftRows* kedua, dan *AddRoundKey* dengan kunci ronde ketiga. Diperoleh matriks barikut:

$$\begin{bmatrix} 91 & 8E & 8C & 66 \\ CB & 23 & 7F & 5C \\ CD & D0 & 45 & 7F \\ 36 & 06 & F8 & 1C \end{bmatrix}$$

yang merupakan pesan tersandi (chiperteks) dan merupakan hasil enkripsi. Dengan mengubah hasil enkripsi ke dalam bentuk heksadesimal diperoleh pesan yang rumit dan tidak dapat dimengerti berupa karakter/angka/huruf yaitu "'ËÍ6Ž#ÐACKŒdelEøf\delFS".

2. Proses deskripsi merupakan proses untuk menentukan teks asli pada chiperteks dan kunci yang diberikan. Hasil chiperteks yang penulis berikan adalah "'ËÍ6Ž#ÐACKŒdelEøf\delFS". Untuk mengembalikan chiperteks pada bentuk semula maka dilakukan langkah-langkah 1) Data masukan berupa pesan/berita tersandi (chiperteks) berupa huruf/angka/karakter adalah "'ËÍ6Ž#ÐACKŒdelEøf\delFS". Menggunakan kunci yang diperoleh dari hasil ekspansi kunci dengan urutan kunci yang merupakan kebalikan dari proses enkripsi (dimulai pada kunci ronde ketiga, kedua dan pertama).

Selanjutnya chiperteks dan kunci berupa huruf/angka/karakter dikonversi ke dalam bentuk heksadesimal dan dibagi menjadi beberapa blok sehingga membentuk matriks seperti yang penulis jelaskan pada proses ekspansi kunci dan melakukan proses transformasi *AddRoundKey* atau *Initial Round* yakni XOR antara chiperteks dengan kunci ronde ketiga. Dilanjutkan dengan melakukan trasformasi *InvShiftRows*, *InvSubBytes* (substitusi setiap elemen matriks masukan dengan merujuk pada tabel invers *S-Box*), *AddRoundKey* dengan kunci ronde kedua, transformasi *InvMixColumns*, transformasi *InvShiftRows* kedua, transformasi *InvSubBytes* kedua, dan *AddRoundKe* dengan kunci ronde pertama. Diperoleh hasil sebagai berikut:

$$\begin{bmatrix} 53 & 52 & 4E & 48 \\ 41 & 23 & 23 & 4C \\ 42 & 44 & 49 & 41 \\ 41 & 41 & 4B & 53 \end{bmatrix}$$

yang merupakan pesan asli (plainteks) dan merupakan hasil dekripsi. Dengan mengubah hasil dekripsi ke dalam bentuk karakter diperoleh pesan asli yang dapat dimengerti dan dipahami berupa sebuah pesan/berita taks yaitu "SABAR#DAN#IKHLAS".

4.2 Saran

Pada penelitian ini membahas tentang proses enkripsi dan dekripsi pesan menggunakan panjang kunci 128 *bit* dan transformasi sebanyak tiga ronde menggunakan tiga kunci berbeda untuk perlindungan pesan. Untuk penelitian selanjutnya, disarankan untuk menggunakan panjang kunci yang berbeda dengan tingkat keamanan yang lebih tinggi menggunakan metode kriptografi yang lebih kompleks.

DAFTAR RUJUKAN

Ad-Dimasyqi. 2001. *Tafsir Ibnu Katsir*. Bandung: Sinar Baru Algensindo.

Ariyus, D. 2006. *Kriptografi Keamanan Data dan Komunikasi.* Yogyakarta: Graha Ilmu.

Ariyus, D. 2008. *Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi.* Yogyakarta: C.V ANDI OFFSET.

Beachy, J.A. dan Blair, W.D.1990. *Abstract Algebra with A Concrete Introduction.* New Jesey: Prentice Hall.

Hardy, D.W. dan Walker, C.L.. 2003. *Applied Algebra Codes, Chipers, and Discrete Algorithms,* New Jesey: Prentice Hall.

Kromodimoeljo, S. 2010. *Teori dan Aplikasi Kriptografi*. Jakarta: SPK IT Consulting.

Munir, R. 2008. *Metode Numerik*. Bandung: INFORMATIKA.

Raisinghania, M.D. dan Aggarwal, R.S. 1980. *Modern Algebra*. New Delhi: S. Chand & Company LTD.

Sadikin, R. 2012. *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: CV ANDI OFFSET.

Wahyudin. 1989. *Aljabar Modern*. Bandung: TARSITO.

Winarno, A. 2012. *Polynomial Function dan Implementasinya dalam Algoritma Advanced Encryption Standard pada Database Accounting*. Makalah Seminar Nasional Matematika dan Pendidikan Matematika dengan tema "Kontribusi Pendidikan Matematika dalam Membangun Karakter Guru dan Siswa". Yogyakarta: Jurusan Pendidikan Matematika UNY tanggal 10 November 2012.

Lampiran 1

Representasi Biner untuk Polynomial Pada $GF(2^8)$

	Bentuk Polinomial		Koefisien Polinomial
a^0	0	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 0\cdot x^3 + 0\cdot x^2 + 0\cdot x + 0$	00000000
a^1	1	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 0\cdot x^3 + 0\cdot x^2 + 0\cdot x + 1$	00000001
a^2	x	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 0\cdot x^3 + 0\cdot x^2 + 1\cdot x + 0$	00000010
a^3	$x+1$	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 0\cdot x^3 + 0\cdot x^2 + 1\cdot x + 1$	00000011
a^4	x^2	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 0\cdot x^3 + 1\cdot x^2 + 0\cdot x + 0$	00000100
a^5	x^2+1	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 0\cdot x^3 + 1\cdot x^2 + 0\cdot x + 1$	00000101
a^6	x^2+x	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 0\cdot x^3 + 1\cdot x^2 + 1\cdot x + 0$	00000110
a^7	x^2+x+1	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 0\cdot x^3 + 1\cdot x^2 + 1\cdot x + 1$	00000111
a^8	x^3	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 1\cdot x^3 + 0\cdot x^2 + 0\cdot x + 0$	00001000
a^9	x^3+1	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 1\cdot x^3 + 0\cdot x^2 + 0\cdot x + 1$	00001001
a^{10}	x^3+x	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 1\cdot x^3 + 0\cdot x^2 + 1\cdot x + 0$	00001010
a^{11}	x^3+x+1	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 1\cdot x^3 + 0\cdot x^2 + 1\cdot x + 1$	00001011
a^{12}	x^3+x^2	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 1\cdot x^3 + 1\cdot x^2 + 0\cdot x + 0$	00001100
a^{13}	x^3+x^2+1	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 1\cdot x^3 + 1\cdot x^2 + 0\cdot x + 1$	00001101
a^{14}	x^3+x^2+x	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 1\cdot x^3 + 1\cdot x^2 + 1\cdot x + 0$	00001110
a^{15}	x^3+x^2+x+1	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 1\cdot x^3 + 1\cdot x^2 + 1\cdot x + 1$	00001111
a^{16}	x^4	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 1\cdot x^4 + 0\cdot x^3 + 0\cdot x^2 + 0\cdot x + 0$	00010000
a^{17}	x^4+1	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 1\cdot x^4 + 0\cdot x^3 + 0\cdot x^2 + 0\cdot x + 1$	00010001
a^{18}	x^4+x	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 1\cdot x^4 + 0\cdot x^3 + 0\cdot x^2 + 1\cdot x + 0$	00010010
a^{19}	x^4+x+1	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 1\cdot x^4 + 0\cdot x^3 + 0\cdot x^2 + 1\cdot x + 1$	00010011
a^{20}	x^4+x^2	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 1\cdot x^4 + 0\cdot x^3 + 1\cdot x^2 + 0\cdot x + 0$	00010100
a^{21}	x^4+x^2+1	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 1\cdot x^4 + 0\cdot x^3 + 1\cdot x^2 + 0\cdot x + 1$	00010101
a^{22}	x^4+x^2+1	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 1\cdot x^4 + 0\cdot x^3 + 1\cdot x^2 + 1\cdot x + 0$	00010110
a^{23}	x^4+x^2+x+1	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 1\cdot x^4 + 0\cdot x^3 + 1\cdot x^2 + 1\cdot x + 1$	00010111
a^{24}	x^4+x^3	$= 0\cdot x^7 + 0\cdot x^6 + 0\cdot x^5 + 1\cdot x^4 + 1\cdot x^3 + 0\cdot x^2 + 0\cdot x + 0$	00011000

a^{25}	$x^4 + x^3 + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 1$	00011001
a^{26}	$x^4 + x^3 + x$	$= 0 \cdot x^7 + 0 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 0$	00011010
a^{27}	$x^4 + x^3 + x + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 1$	00011011
a^{28}	$x^4 + x^3 + x^2$	$= 0 \cdot x^7 + 0 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 0$	00011100
a^{29}	$x^4 + x^3 + x^2 + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1$	00011101
a^{30}	$x^4 + x^3 + x^2 + x$	$= 0 \cdot x^7 + 0 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 0$	00011110
a^{31}	$x^4 + x^3 + x^2 + x + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 1$	00011111
a^{32}	x^5	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 0$	00100000
a^{33}	$x^5 + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 1$	00100001
a^{34}	$x^5 + x$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 0$	00100010
a^{35}	$x^5 + x + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 1$	00100011
a^{36}	$x^5 + x^2$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 0$	00100100
a^{37}	$x^5 + x^2 + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1$	00100101
a^{38}	$x^5 + x^2 + x$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 0$	00100110
a^{39}	$x^5 + x^2 + x + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 1$	00100111
a^{40}	$x^5 + x^3$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 0$	00101000
a^{41}	$x^5 + x^3 + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 1$	00101001
a^{42}	$x^5 + x^3 + x$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 0$	00101010
a^{43}	$x^5 + x^3 + x + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 1$	00101011
a^{44}	$x^5 + x^3 + x^2$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 0$	00101100
a^{45}	$x^5 + x^3 + x^2 + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1$	00101101
a^{46}	$x^5 + x^3 + x^2 + x$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 0$	00101110
a^{47}	$x^5 + x^3 + x^2 + x + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 1$	00101111
a^{48}	$x^5 + x^4$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 0$	00110000
a^{49}	$x^5 + x^4 + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 1$	00110001
a^{50}	$x^5 + x^4 + x$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 0$	00110010
a^{51}	$x^5 + x^4 + x + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 1$	00110011
a^{52}	$x^5 + x^4 + x^2$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 0$	00110100
a^{53}	$x^5 + x^4 + x^2 + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1$	00110101
a^{54}	$x^5 + x^4 + x^2 + x$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 0$	00110110
a^{55}	$x^5 + x^4 + x^2 + x + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 1$	00110111

a^{56}	$x^5 + x^4 + x^3$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 0$	00111000
a^{57}	$x^5 + x^4 + x^3 + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 1$	00111001
a^{58}	$x^5 + x^4 + x^3 + x$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 0$	00111010
a^{59}	$x^5 + x^4 + x^3 + x + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 1$	00111011
a^{60}	$x^5 + x^4 + x^3 + x^2$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 0$	00111100
a^{61}	$x^5 + x^4 + x^3 + x^2 + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1$	00111101
a^{62}	$x^5 + x^4 + x^3 + x^2 + x$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 0$	00111110
a^{63}	$x^5 + x^4 + x^3 + x^2 + x + 1$	$= 0 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 1$	00111111
a^{64}	x^6	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 0$	01000000
a^{65}	$x^6 + 1$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 1$	01000001
a^{66}	$x^6 + x$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 0$	01000010
a^{67}	$x^6 + x + 1$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 1$	01000011
a^{68}	$x^6 + x^2$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 0$	01000100
a^{69}	$x^6 + x^2 + 1$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1$	01000101
a^{70}	$x^6 + x^2 + x$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 0$	01000110
a^{71}	$x^6 + x^2 + x + 1$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 1$	01000111
a^{72}	$x^6 + x^3$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 0$	01001000
a^{73}	$x^6 + x^3 + 1$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 1$	01001001
a^{74}	$x^6 + x^3 + x$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 0$	01001010
a^{75}	$x^6 + x^3 + x + 1$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 1$	01001011
a^{76}	$x^6 + x^3 + x^2$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 0$	01001100
a^{77}	$x^6 + x^3 + x^2 + 1$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1$	01001101
a^{78}	$x^6 + x^3 + x^2 + x$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 0$	01001110
a^{79}	$x^6 + x^3 + x^2 + x + 1$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 1$	01001111
a^{80}	$x^6 + x^4 +$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 0$	01010000
a^{81}	$x^6 + x^4 + +1$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 1$	01010001
a^{82}	$x^6 + x^4 + x$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 0$	01010010
a^{83}	$x^6 + x^4 + x + 1$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 1$	01010011
a^{84}	$x^6 + x^4 + x^2$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 0$	01010100
a^{85}	$x^6 + x^4 + x^2 + 1$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1$	01010101
a^{86}	$x^6 + x^4 + x^2 + x$	$= 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 0$	01010110

a^{87}	$x^6+x^4+x^2+x+1$	$=0\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+1$	01010111
a^{88}	$x^6+x^4+x^3$	$=0\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+0$	01011000
a^{89}	$x^6+x^4+x^3+1$	$=0\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+1$	01011001
a^{90}	$x^6+x^4+x^3+x$	$=0\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+0$	01011010
a^{91}	$x^6+x^4+x^3+x+1$	$=0\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+1$	01011011
a^{92}	$x^6+x^4+x^3+x^2$	$=0\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+0$	01011100
a^{93}	$x^6+x^4+x^3+x^2+1$	$=0\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+1$	01011101
a^{94}	$x^6+x^4+x^3+x^2+x$	$=0\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+0$	01011110
a^{95}	$x^6+x^4+x^3+x^2+x+1$	$=0\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+1$	01011111
a^{96}	x^6+x^5	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+0$	01100000
a^{97}	x^6+x^5++1	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+1$	01100001
a^{98}	x^6+x^5+x	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+0$	01100010
a^{99}	x^6+x^5+x+1	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+1$	01100011
a^{100}	$x^6+x^5+x^2$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+0$	01100100
a^{101}	$x^6+x^5+x^2+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+1$	01100101
a^{102}	$x^6+x^5+x^2+x$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+0$	01100110
a^{103}	$x^6+x^5+x^2+x+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+1$	01100111
a^{104}	$x^6+x^5+x^3$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+0$	01101000
a^{105}	$x^6+x^5+x^3+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+1$	01101001
a^{106}	$x^6+x^5+x^3+x$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+0$	01101010
a^{107}	$x^6+x^5+x^3+x+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+1$	01101011
a^{108}	$x^6+x^5+x^3+x^2$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+0$	01101100
a^{109}	$x^6+x^5+x^3+x^2+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+1$	01101101
a^{110}	$x^6+x^5+x^3+x^2+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+0$	01101110
a^{111}	$x^6+x^5+x^3+x^2+x+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+1$	01101111
a^{112}	$x^6+x^5+x^4$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+0$	01110000
a^{113}	$x^6+x^5+x^4+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+1$	01110001
a^{114}	$x^6+x^5+x^4+x$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+0$	01110010
a^{115}	$x^6+x^5+x^4+x+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+1$	01110011
a^{116}	$x^6+x^5+x^4+x^2$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+0$	01110100
a^{117}	$x^6+x^5+x^4+x^2+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+1$	01110101

a^{118}	$x^6+x^5+x^4+x^2+x$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+0$	01110110
a^{119}	$x^6+x^5+x^4+x^2+x+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+1$	01110111
a^{120}	$x^6+x^5+x^4+x^3$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+0$	01111000
a^{121}	$x^6+x^5+x^4+x^3+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+1$	01111001
a^{122}	$x^6+x^5+x^4+x^3+x$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+0$	01111010
a^{123}	$x^6+x^5+x^4+x^3+x+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+1$	01111011
a^{124}	$x^6+x^5+x^4+x^3+x^2$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+0$	01111100
a^{125}	$x^6+x^5+x^4+x^3+x^2+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+1$	01111101
a^{126}	$x^6+x^5+x^4+x^3+x^2+x$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+0$	01111110
a^{127}	$x^6+x^5+x^4+x^3+x^2+x+1$	$=0\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+1$	01111111
a^{128}	x^7	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+0$	10000000
a^{129}	x^7+1	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+1$	10000001
a^{130}	x^7+x	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+0$	10000010
a^{131}	x^7+x+1	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+1$	10000011
a^{132}	x^7+x^2	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+0$	10000100
a^{133}	x^7+x^2+1	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+1$	10000101
a^{134}	x^7+x^2+x	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+0$	10000110
a^{135}	x^7+x^2+x+1	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+1$	10000111
a^{136}	x^7+x^3	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+0$	10001000
a^{137}	x^7+x^3+1	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+1$	10001001
a^{138}	x^7+x^3+x	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+0$	10001010
a^{139}	x^7+x^3+x+1	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+1$	10001011
a^{140}	$x^7+x^3+x^2$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+0$	10001100
a^{141}	$x^7+x^3+x^2+1$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+1$	10001101
a^{142}	$x^7+x^3+x^2+x$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+0$	10001110
a^{143}	$x^7+x^3+x^2+x+1$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+1$	10001111
a^{144}	x^7+x^4	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+0$	10010000
a^{145}	x^7+x^4+1	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+1$	10010001
a^{146}	x^7+x^4+x	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+0$	10010010
a^{147}	x^7+x^4+x+1	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+1$	10010011
a^{148}	$x^7+x^4+x^2$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+0$	10010100

a^{149}	$x^7+x^4+x^2+1$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+1$	10010101
a^{150}	$x^7+x^4+x^2+x$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+0$	10010110
a^{151}	$x^7+x^4+x^2+x+1$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+1$	10010111
a^{152}	$x^7+x^4+x^3$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+0$	10011000
a^{153}	$x^7+x^4+x^3+1$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+1$	10011001
a^{154}	$x^7+x^4+x^3+x$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+0$	10011010
a^{155}	$x^7+x^4+x^3+x+1$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+1$	10011011
a^{156}	$x^7+x^4+x^3+x^2$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+0$	10011100
a^{157}	$x^7+x^4+x^3+x^2+1$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+1$	10011101
a^{158}	$x^7+x^4+x^3+x^2+x$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+0$	10011110
a^{159}	$x^7+x^4+x^3+x^2+x+1$	$=1\cdot x^7+0\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+1$	10011111
a^{160}	x^7+x^5	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+0$	10100000
a^{161}	x^7+x^5+1	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+1$	10100001
a^{162}	x^7+x^5+x	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+0$	10100010
a^{163}	x^7+x^5+x	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+1$	10100011
a^{164}	$x^7+x^5+x^2$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+0$	10100100
a^{165}	$x^7+x^5+x^2+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+1$	10100101
a^{166}	$x^7+x^5+x^2+x$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+0$	10100110
a^{167}	$x^7+x^5+x^2+x+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+1$	10100111
a^{168}	$x^7+x^5+x^3$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+0$	10101000
a^{169}	$x^7+x^5+x^3+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+1$	10101001
a^{170}	$x^7+x^5+x^3+x$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+0$	10101010
a^{171}	$x^7+x^5+x^3+x+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+1$	10101011
a^{172}	$x^7+x^5+x^3+x^2$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+0$	10101100
a^{173}	$x^7+x^5+x^3+x^2+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+1$	10101101
a^{174}	$x^7+x^5+x^3+x^2+x$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+0$	10101110
a^{175}	$x^7+x^5+x^3+x^2+x+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+1$	10101111
a^{176}	$x^7+x^5+x^4$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+0$	10110000
a^{177}	$x^7+x^5+x^4+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+1$	10110001
a^{178}	$x^7+x^5+x^4+x$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+0$	10110010
a^{179}	$x^7+x^5+x^4+x+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+1$	10110011

a^{180}	$x^7+x^5+x^4+x^2$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+0$	10110100
a^{181}	$x^7+x^5+x^4+x^2+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+1$	10110101
a^{182}	$x^7+x^5+x^4+x^2+x$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+0$	10110110
a^{183}	$x^7+x^5+x^4+x^2+x+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+1$	10110111
a^{184}	$x^7+x^5+x^4+x^3$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+0$	10111000
a^{185}	$x^7+x^5+x^4+x^3+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+1$	10111001
a^{186}	$x^7+x^5+x^4+x^3+x$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+0$	10111010
a^{187}	$x^7+x^5+x^4+x^3+x+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+1$	10111011
a^{188}	$x^7+x^5+x^4+x^3+x^2$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+0$	10111100
a^{189}	$x^7+x^5+x^4+x^3+x^2+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+1$	10111101
a^{190}	$x^7+x^5+x^4+x^3+x^2+x$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+0$	10111110
a^{191}	$x^7+x^5+x^4+x^3+x^2+x+1$	$=1\cdot x^7+0\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+1$	10111111
a^{192}	x^7+x^6	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+0$	11000000
a^{193}	x^7+x^6+1	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+1$	11000001
a^{194}	x^7+x^6+x	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+0$	11000010
a^{195}	x^7+x^6+x+1	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+1$	11000011
a^{196}	$x^7+x^6+x^2$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+0$	11000100
a^{197}	$x^7+x^6+x^2+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+1$	11000101
a^{198}	$x^7+x^6+x^2+x$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+0$	11000110
a^{199}	$x^7+x^6+x^2+x+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+1$	11000111
a^{200}	$x^7+x^6+x^3$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+0$	11001000
a^{201}	$x^7+x^6+x^3+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+1$	11001001
a^{202}	$x^7+x^6+x^3+x$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+0$	11001010
a^{203}	$x^7+x^6+x^3+x+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+1$	11001011
a^{204}	$x^7+x^6+x^3+x^2$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+0$	11001100
a^{205}	$x^7+x^6+x^3+x^2+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+1$	11001101
a^{206}	$x^7+x^6+x^3+x^2+x$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+0$	11001110
a^{207}	$x^7+x^6+x^3+x^2+x+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+1$	11001111
a^{208}	$x^7+x^6+x^4$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+0$	11010000
a^{209}	$x^7+x^6+x^4+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+1$	11010001
a^{210}	$x^7+x^6+x^4+x$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+0$	11010010

a^{211}	$x^7+x^6+x^4+x+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+1$	11010011
a^{212}	$x^7+x^6+x^4+x^2$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+0$	11010100
a^{213}	$x^7+x^6+x^4+x^2+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+1$	11010101
a^{214}	$x^7+x^6+x^4+x^2+x$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+0$	11010110
a^{215}	$x^7+x^6+x^4+x^2+x+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+1$	11010111
a^{216}	$x^7+x^6+x^4+x^3$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+0$	11011000
a^{217}	$x^7+x^6+x^4+x^3+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+1$	11011001
a^{218}	$x^7+x^6+x^4+x^3+x$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+0$	11011010
a^{219}	$x^7+x^6+x^4+x^3+x+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+1$	11011011
a^{220}	$x^7+x^6+x^4+x^3+x^2$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+0$	11011100
a^{221}	$x^7+x^6+x^4+x^3+x^2+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+1$	11011101
a^{222}	$x^7+x^6+x^4+x^3+x^2+x$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+0$	11011110
a^{223}	$x^7+x^6+x^4+x^3+x^2+x+1$	$=1\cdot x^7+1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+1$	11011111
a^{224}	$x^7+x^6+x^5$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+0$	11100000
a^{225}	$x^7+x^6+x^5+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+1$	11100001
a^{226}	$x^7+x^6+x^5+x$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+0$	11100010
a^{227}	x^7+x^6+x+1	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+1$	11100011
a^{228}	$x^7+x^6+x^5+x^2$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+0$	11100100
a^{229}	$x^7+x^6+x^5+x^2+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+1$	11100101
a^{230}	$x^7+x^6+x^5+x^2+x$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+0$	11100110
a^{231}	$x^7+x^6+x^5+x^2+x+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+1$	11100111
a^{232}	$x^7+x^6+x^5+x^3$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+0$	11101000
a^{233}	$x^7+x^6+x^5+x^3+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+1$	11101001
a^{234}	$x^7+x^6+x^5+x^3+x$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+0$	11101010
a^{235}	$x^7+x^6+x^5+x^3+x+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+1$	11101011
a^{236}	$x^7+x^6+x^5+x^3+x^2$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+0$	11101100
a^{237}	$x^7+x^6+x^5+x^3+x^2+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+1$	11101101
a^{238}	$x^7+x^6+x^5+x^3+x^2+x$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+0$	11101110
a^{239}	$x^7+x^6+x^5+x^3+x^2+x+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+1$	11101111
a^{240}	$x^7+x^6+x^5+x^4$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+0$	11110000
a^{241}	$x^7+x^6+x^5+x^4+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x+1$	11110001

a^{242}	$x^7+x^6+x^5+x^4+x$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+0$	11110010
a^{243}	$x^7+x^6+x^5+x^4+x+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+1$	11110011
a^{244}	$x^7+x^6+x^5+x^4+x^2$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+0$	11110100
a^{245}	$x^7+x^6+x^5+x^4+x^2+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+1$	11110101
a^{246}	$x^7+x^6+x^5+x^4+x^2+x$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+0$	11110110
a^{247}	$x^7+x^6+x^5+x^4+x^2+x+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+1$	11110111
a^{248}	$x^7+x^6+x^5+x^4+x^3$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+0$	11111000
a^{249}	$x^7+x^6+x^5+x^4+x^3+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+1$	11111001
a^{250}	$x^7+x^6+x^5+x^4+x^3+x$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+0$	11111010
a^{251}	$x^7+x^6+x^5+x^4+x^3+x+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+1$	11111011
a^{252}	$x^7+x^6+x^5+x^4+x^3+x^2$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+0$	11111100
a^{253}	$x^7+x^6+x^5+x^4+x^3+x^2+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+0\cdot x+1$	11111101
a^{254}	$x^7+x^6+x^5+x^4+x^3+x^2+x$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+0$	11111110
a^{255}	$x^7+x^6+x^5+x^4+x^3+x^2+x+1$	$=1\cdot x^7+1\cdot x^6+1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+1$	11111111

Lampiran 2

Tabel Sistem Bilangan 4 *bit*

Digit Heksadesimal	4 bit
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110

Lampiran 3

Tabel ASCII

Decimal	Octal	Hexadecimal	Code	Description
000	000	00	NUL	Null
001	001	01	SOH	Start Of Heading
002	002	02	STX	Start of TeXt
003	003	03	ETX	End of TeXt
004	004	04	EOT	End Of Transmission
005	005	05	ENQ	ENQuiry
006	006	06	ACK	ACKnowledge
007	007	07	BEL	BELl. Caused teletype machines to ring a bell. Causes a beep in many common terminals and terminal emulation programs.
008	010	08	BS	BackSpace. Moves the cursor move backwards (left) one space.
009	011	09	HT	Horizontal Tab. Moves the cursor right to the next tab stop. The spacing of tab stops is dependent on the output device, but is often either 8 or 10 characters wide.
010	012	0A	LF	Line Feed. Moves the cursor to a new line. On Unix systems, moves to a new line AND all the way to the left.
011	013	0B	VT	Vertical Tab
012	014	0C	FF	Form Feed. Advances paper to the top of the next page (if the output device is a printer).
013	015	0D	CR	Carriage Return. Moves the cursor all the way to the left, but does not advance to the next line.
014	016	0E	SO	Shift Out
015	017	0F	SI	Shift In
016	020	10	DLE	Data Link Escape
017	021	11	DC1	Device Control 1
018	022	12	DC2	Device Control 2
019	023	13	DC3	Device Control 3
020	024	14	DC4	Device Control 4
021	025	15	NAK	Negative AcKnowledge
022	026	16	SYN	SYNchronous idle

023	027	17	ETB	End of Transmission Block
024	030	18	CAN	CANcel
025	031	19	EM	End of Medium
026	032	1A	SUB	SUBstitute
027	033	1B	ESC	ESCape
028	034	1C	FS	File Separator

Decimal	Octal	Hexadecimal	Code	Description
029	035	1D	GS	Group Separator
030	036	1E	RS	Record Separator
031	037	1F	US	Unit Separator

Decimal	Octal	Hexadecimal	Character	Decimal	Octal	Hexadecimal	Character
032	040	20	Space	049	061	31	1
033	041	21	!	050	062	32	2
034	042	22	"	051	063	33	3
035	043	23	#	052	064	34	4
036	044	24	$	053	065	35	5
037	045	25		054	066	36	6
038	046	26	&	055	067	37	7
039	047	27	'	056	070	38	8
040	050	28	(	057	071	39	9
041	051	29	)	058	072	3A	:
042	052	2A	*	059	073	3B	;
043	053	2B	+	060	074	3C	<
044	054	2C	,	061	075	3D	=
045	055	2D	-	062	076	3E	>
046	056	2E	.	063	077	3F	?
047	057	2F	/	064	100	40	@
048	060	30	0				

Decimal	Octal	Hexadecimal	Character	Decimal	Octal	Hexadecimal	Character
032	040	20	Space	049	061	31	1
033	041	21	!	050	062	32	2
034	042	22	"	051	063	33	3
035	043	23	#	052	064	34	4

036	044	24	$	053	065	35	5
037	045	25		054	066	36	6
038	046	26	&	055	067	37	7
039	047	27	'	056	070	38	8
040	050	28	(	057	071	39	9
041	051	29	)	058	072	3A	:
042	052	2A	*	059	073	3B	;
043	053	2B	+	060	074	3C	<
044	054	2C	,	061	075	3D	=
045	055	2D	-	062	076	3E	>
046	056	2E	.	063	077	3F	?
047	057	2F	/	064	100	40	@
048	060	30	0				

Decimal	Octal	Hexadecimal	Character	Decimal	Octal	Hexadecimal	Character
091	133	5B	[	123	173	7B	{
092	134	5C	\	124	174	7C	|
093	135	5D	]	125	175	7D	}
094	136	5E	^	126	176	7E	~
095	137	5F	_	127	177	7F	delete
096	140	60	'				

Decimal	Octal	Hexadecimal	Character	Decimal	Octal	Hexadecimal	Character
128	200	80	•	160	240	A0	non-breaking space
129	201	81	•	161	241	A1	¡
130	202	82	,	162	242	A2	¢
131	203	83	*ƒ*	163	243	A3	£
132	204	84	„	164	244	A4	¤
133	205	85	…	165	245	A5	¥
134	206	86	†	166	246	A6	¦
135	207	87	‡	167	247	A7	§
136	210	88	ˆ	168	250	A8	¨
137	211	89	‰	169	251	A9	©
138	212	8A	Š	170	252	AA	ª
139	213	8B	‹	171	253	AB	«

Decimal	Octal	Hexadecimal	Character	Decimal	Octal	Hexadecimal	Character
140	214	8C	Œ	172	254	AC	¬
141	215	8D	•	173	255	AD	-
142	216	8E	Ž	174	256	AE	®
143	217	8F	•	175	257	AF	¯
144	220	90	•	176	260	B0	°
145	221	91	'	177	261	B1	±
146	222	92	'	178	262	B2	²
147	223	93	"	179	263	B3	³
148	224	94	•	180	264	B4	´
149	225	95	•	181	265	B5	µ
150	226	96	–	182	266	B6	¶
151	227	97	—	183	267	B27	·
152	230	98	˜	184	270	B8	¸
153	231	99	™	185	271	B9	¹
154	232	9A	š	186	272	BA	º
155	233	9B	›	187	273	BB	»
156	234	9C	œ	188	274	BC	¼
157	235	9D	•	189	275	BD	½
158	236	9E	Ÿ	190	276	BE	¾
159	237	9F	Ÿ	191	277	BF	¿

Decimal	Octal	Hexadecimal	Character	Decimal	Octal	Hexadecimal	Character
192	300	C0	À	224	340	E0	à
193	301	C1	Á	225	341	E1	á
194	302	C2	Â	226	342	E2	â
195	303	C3	Ã	227	343	E3	ã
196	304	C4	Ä	228	344	E4	ä

Decimal	Octal	Hexadecimal	Character	Decimal	Octal	Hexadecimal	Character
197	305	C5	Å	229	345	E5	å
198	306	C6	Æ	230	346	E6	æ
199	307	C7	Ç	231	347	E7	ç
200	310	C8	È	232	350	E8	è
201	311	C9	É	233	351	E9	é
202	312	CA	Ê	234	352	EA	ê

203	313	CB	Ë	235	353	EB	ë
204	314	CC	Ì	236	354	EC	ì
205	315	CD	Í	237	355	ED	í
206	316	CE	Î	238	356	EE	î
207	317	CF	Ï	239	357	EF	ï
208	320	D0	Đ	240	360	F0	ð
209	321	D1	Ñ	241	361	F1	ñ
210	322	D2	Ò	242	362	F2	ò
211	323	D3	Ó	243	363	F3	ó
212	324	D4	Ô	244	364	F4	ô
213	325	D5	Ö	245	365	F5	õ
214	326	D6	Ö	246	366	F6	ö
215	327	D7	×	247	367	F7	÷
216	330	D8	Ø	248	370	F8	ø
217	331	D9	Ù	249	371	F9	ù
218	332	DA	Ú	250	372	FA	ú
219	333	DB	Û	251	373	FB	û
220	334	DC	Ü	252	374	FC	ü
221	335	DD	Ý	253	375	FD	ý
222	336	DE	Þ	254	376	FE	þ
223	337	DF	ß	255	377	FF	