ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN POLINOMIAL *GALOIS FIELD* DENGAN ALGORITMA *HILL CIPHER*

SKRIPSI

OLEH
AMELIA VEGA
NIM. 17610056

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2022

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN POLINOMIAL *GALOIS FIELD* DENGAN ALGORITMA *HILL CIPHER*

SKRIPSI

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

Oleh
Amelia Vega
NIM. 17610056

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2022

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN POLINOMIAL *GALOIS FIELD* DENGAN ALGORITMA *HILL CIPHER*

SKRIPSI

Oleh
Amelia Vega
NIM. 17610056

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 29 November 2021

Pembimbing I,	Pembimbing II,
Dr. H. Imam Sujarwo, M.Pd	Muhammad Khudzaifah, M.Si
NIP. 19630502 198703 1 005	NIDT. 19900511 20160801 1 057

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129 200012 2 005

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN POLINOMIAL *GALOIS FIELD* DENGAN ALGORITMA *HILL CIPHER*

SKRIPSI

Oleh
Amelia Vega
NIM. 17610056

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
Untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 07 Januari 2022

Penguji Utama : Mohammad Nafie Jauhari, M.Si .....

Ketua Penguji : Angga Dwi Mulyanto, M.Si .....

Sekertaris Penguji: Dr. H. Imam Sujarwo, M.Pd .....

Anggota Penguji : Muhammad Khudzaifah, M.Si .....

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129 200012 2 005

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Amelia Vega

NIM : 17610056

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Enkripsi dan Dekripsi Pesan Menggunakan Polinomial *Galois Field* dengan Algoritma *Hill Cipher*

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, 16 Januari 2022

Yang membuat pernyataan,

Amelia Vega

NIM. 17610056

MOTO

“berilah tanpa mengharapkan imbalan, dahulukan orang tua diatas segalanya dan jangan berharap lebih terhadap manusia”

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:

Ibu Supiyati dan Bapak Sumaryono yang telah memberikan dukungan secara material dan spiritual yang menjadikan penulis bisa mencapai keberhasilan dan dapat menyelesaikan tugas dengan sebaik mungkin. Kesusahpayahan mereka dalam membimbing dan memberikan kelayakan hidup kepada penulis merupakan motivasi dalam hidup penulis untuk meraih mimpi dan kesuksesan dimana untuk membahagiakan mereka. Tidak lupa kepada adik tercinta, Rofid Zainnazar yang senantiasa memberikan kasih sayang, dukungan, motivasi dan do'anya kepada penulis.

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarokatuh.

Puji syukur kehadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul "Enkripsi dan Dekripsi Pesan Menggunakan Polinomial *Galois Field* dengan Algoritma *Hill Cipher*" sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang Matematika di Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Sholawat dan salam semoga tetap tercurahkan kepada baginda Nabi Muhammad SAW yang telah membimbing manusia dari zaman jahiliyah menuju zaman islamiah.

Dalam proses penyusunan skripsi ini, penulis banyak menerima bimbingan, masukan, dan arahan dari berbagai pihak. Oleh karena itu melalui halaman ini penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Prof. Dr. M. Zainuddin, MA 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. Elly Susanti, M.Sc. selaku Ketua Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang
4. Dr. H. Imam Sujarwo, M.Pd selaku Dosen Pembimbing I yang telah memberikan banyak ilmu, arahan, nasihat dan motivasi kepada penulis.
5. Muhammad Khudzaifah, M.Si selaku Dosen Pembimbing II yang banyak memberikan ilmu, arahan dan masukan kepada penulis.

6. Muhammad Nafie Jauhari, M.Si dan Angga Dwi Mulyanto, M.Si selaku Dosen Penguji yang banyak memberikan saran dan masukan kepada penulis.
7. Segenap sivitas akademika Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang, terutama jajaran dosen yang telah memberikan pengalaman perkuliahan yang sangat luar biasa.
8. Ayah dan ibu yang selalu mengirimkan dukungan dan doa terbaik kepada penulis.
9. Seluruh teman-teman di Program Studi Matematika Angkatan 2017.
10. Semua pihak yang tidak dapat disebutkan satu-persatu yang telah ikut serta membantu menyelesaikan penyusunan skripsi ini, baik dukungan moril maupun material.

Penulis sadar tidak bisa memberikan apapun selain ucapan terima kasih dan doa semoga Allah membalas kebaikan jasa dengan balasan yang sebaik-baiknya. Penulis berharap semoga skripsi ini dapat bermanfaat, baik bagi penulis maupun pembaca.

Wassalamualaikum Warahmatullahi Wabarakatuh.

Malang, 16 Januari 2022

Penulis

DAFTAR ISI

HALAMAN JUDUL

HALAMAN PENGAJUAN

HALAMAN PERSETUJUAN

HALAMAN PERNYATAAN KEASLIAN TULISAN

HALAMAN MOTO

HALAMAN PERSEMBAHAN

KATA PENGANTAR viii

DAFTAR ISI x

DAFTAR TABEL xii

ABSTRAK xiii

ABSTRACT xiv

ملخص xv

BAB I PENDAHULUAN

1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Tujuan Penelitian 5
1.4 Manfaat Penelitian 5
1.5 Batasan Masalah 6
1.6 Metode Penelitian 6
1.7 Sistematika Penulisan 7

BAB II KAJIAN PUSTAKA

2.1 Kriptografi 9
2.1.1 Pengertian Kriptografi 9
2.1.2 Elemen-Elemen Kriptografi 10
2.1.3 Tujuan Kriptografi 16
2.1.4 Aritmatika Modular 17
2.1.5 Sistem Bilangan Biner 20
2.1.6 *ASCII* 21
2.1.7 Kriptografi Simetris 21
2.1.8 Kriptografi Kunci Asimetris 22
2.2 *Finite Field* 22
2.2.1 Polinomial 22
2.2.2 Operasi Aljabar pada Polinomial 23
2.2.3 Sifat Keterbagian dan Faktorisasi 24

2.2.4 *Finite Field* dengan Elemen Polinomial *GF* (2^n).....25
2.3 *Hill Cipher*.....26
2.3.1 Matriks.....29
2.4 Kajian Keislaman.....35

BAB III PEMBAHASAN

3.1 Proses Enkripsi Pesan Menggunakan Polinomial *Galois Field* dengan Algoritma *Hill Cipher*.....38
3.1.1 Mengonversi Karakter Pesan Teks ke dalam Bentuk Polinomial *Galois Field*.....38
3.1.2 Melakukan Proses Perhitungan pada Polinomial dengan Meggunakan *Hill Cipher*.....42
3.1.3 Mengonversi Hasil Perhitungan pada Polinomial *Galois Field* ke dalam Bentuk Karakter.....47
3.2 Proses Dekripsi Pesan Menggunakan Polinomial *Galois Field* dengan Algoritma *Hill Cipher*.....48
3.2.1 Mengonversi Karakter Pesan Tersandi ke dalam Bentuk Polinomial *Galois Field*.....48
3.2.2 Melakukan Proses Perhitungan pada Polinomial dengan Menggunakan Algoritma *Hill Cipher*.....50
3.2.3 Mengonversi Hasil Perhitungan pada Polinomial *Galois Field* ke dalam Bentuk Karakter.....55
3.3 Kajian Agama.....56

BAB IV PENUTUP

4.1 Kesimpulan.....59
4.2 Saran.....60

DAFTAR PUSTAKA

LAMPIRAN

RIWAYAT HIDUP

DAFTAR TABEL

Tabel 2.1 Skema Bilangan Biner 20
Tabel 2.2 Konversi Karakter ke dalam Desimal 27
Tabel 2.3 Konversi Karakter ke dalam Desimal 28
Tabel 3.1 Kode dan Simbol Biner Tabel *ASCII* 38
Tabel 3.2 Polinomial $GF\ 2^8$ 39
Tabel 3.3 Konversi Biner 8-bit ke dalam Polinomial *Galois Field* 2^8 40
Tabel 3.4 Konversi Pesan ke dalam Biner 8-bit 41
Tabel 3.5 Konversi Karakter Pesan ke dalam Polinomial $GF\ 2^8$ 42
Tabel 3.6 Konversi Hasil Enkripsi $GF\ 2^8$ Menjadi Karakter 47
Tabel 3.7 Konversi Karakter Ciphertext *GF* 2^8 Menjadi Biner 8-bit 49
Tabel 3.8 Konversi Biner 8-bit Sesuai Polinomial *GF* 49
Tabel 3.9 Konversi Hasil Dekripsi Polinomial *GF* 2^8 Menjadi Karakter 55

ABSTRAK

Vega, Amelia. 2022. **Enkripsi dan Dekripsi Pesan Menggunakan Polinomial Galois Field dengan Algoritma Hill Cipher**. Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Dr. H. Imam Sujarwo, M.Pd (II) Muhammad Khudzaifah, M.Si.

Kata kunci: *Galois Field*, *Hill Cipher*, penyandian

Suatu informasi sangatlah mudah untuk didapatkan ketika teknologi sudah berkembang begitu cepat dan penting untuk mengamankan informasi agar terhindar dari pihak yang tidak bertanggung jawab yang ingin menyalahgunakan. Pesan yang tidak aman akan merugikan pemilik pesan, oleh karena itu banyak penelitian yang berhubungan dengan keamanan pesan. Penelitian ini bertujuan untuk memperdalam tentang pengamanan pesan berupa penyandian menggunakan polinomial *Galois Field* dengan salah satu algoritma simetris penyandian yaitu algoritma *Hill Cipher*. Enkripsi merupakan proses mengonversi pesan menjadi kode rahasia sedangkan dekripsi merupakan proses kebalikannya. Proses enkripsi dan dekripsi dalam pembahasan ini dilakukan dengan merubah karakter pesan ke dalam bentuk polinomial *Galois Field*, kemudian mengoperasikan perhitungan berdasarkan algoritma *Hill Cipher*, dan selanjutnya merubah hasil operasi perhitungan menjadi bentuk karakter kembali. Berdasarkan modifikasi yang dilakukan, rumus enkripsi dan dekripsinya akan menjadi perkalian dengan modulo berupa polinomial. Pada penelitian ini kunci enkripsi dan dekripsinya berupa matriks dengan elemen didalamnya adalah anggota polinomial *Galois Field* dan hasilnya berupa pesan teracak dari 256 karakter pada biner bit-8. Dari penelitian ini kita memperoleh wawasan penyandian yang dapat dilakukan dengan menggunakan polinomial dimana nantinya akan dapat dimanfaatkan pada penyandian bentuk lainnya.

ABSTRACT

Vega, Amelia. 2022. **Message Encryption and Decryption Using Polynomial Galois Field with Hill Cipher Algorithm**. Essay. Mathematics Study Program, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University Malang. Supervisor: (I) Dr. H. Imam Sujarwo, M.Pd (II) Muhammad Khudzaifah, M.Sc.

Keywords: Galois Field, Hill Cipher, encoding

An information is extremely easy to obtain when technology is evolving so fast and it is important to secure the information to avoid irresponsible parties who want to abuse it. Messages that are not safe will harm the owner of the message, therefore a lot of research is related to message security. This study aims to deepen the message security in encoded form using Galois Field polynomials with one of the symmetric encryption algorithms, namely the Hill Cipher algorithm. Encryption is the process of converting a message into a secret code while decryption is the reverse process. The encryption and decryption process in this discussion is carried out by changing the message character into Galois Field polynomial form, then operating calculations based on the Hill Cipher algorithm, and then changing the results of the calculation operations into character form again. Based on the modifications have been made, the encryption and decryption formulas will be multiplied by modulo in polynomials form. In this study, the encryption and decryption keys are in matrix form with elements in it are members of the Galois Field polynomial and the result is a random message of 256 characters in binary bit-8. From this research, we gain insight into the encoding that can be done using polynomials which can be used later in other forms of encoding.

ملخص

فيجا، أميليا. 2022 .**شفرة الرسالة ووصفها باستخدام متعدد حدود *Galois Field* بخوارزمية *Hill Cipher***. البحث الجامعي. قسم الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف الأول: الدكتور إمام سجاروو، الماجستير الحاج، والمشرف الثاني، محمد خذيفة، الماجستير.

الكلمات المفتاحية: *Galois Field*، *Hill Cipher*، الشفرة

المعلومات المحصولة بسهلة عندما تتطور التكنولوجيا سريعا واطمئنها مهمة لتجنب الأطراف غير المسؤولة التي تريد أن تفرطها. والرسالة غير الآمنة ستضر بمالك الرسالة، لذلك يوجد كثير من البحث الذي يتعلق بأمان الرسالة. تهدف هذه البحث لتعميق أمان الرسالة يعني شفرة باستخدام متعدد حدود *Galois Field* بإحدى خوارزميات الشفرة المتماثل وهي خوارزمية *Hill Cipher*. الشفرة هي عملية تحويل رسالة إلى شفرة سرية وأما الوصف هو عملية عكسية. تتم عملية الشفرة والوصف لهذا البحث بطريق تغيير حرف الرسالة إلى شكل متعدد حدود *Galois Field* ، ثم تشغيل العمليات الحسابية على أساس خوارزمية *Hill Cipher*، ثم تغيير نتائج العمليات الحسابية إلى شكل حرف مرة أخرى. وبناءً على التعديل الذي تم إجراؤه ستصير صيغة الشفرة ووصفها ضربا ب*modulo* بوجود متعدد الحدود. وفي هذا البحث مفتاح الشفرة ووصفها بشكل القالب بعناصر فيها أعضاء متعدد حدود *Galois Field* ونتيجته هي رسالة عشوائية مكونة من 256 حرفًا على 8-bit الثنائي. ومن هذا البحث، يمكننا أن ننال المعرفة عن الشفرة التي تستطيع إجراءها بمتعدد الحدود حيث تستطيع استفادتها على الشفرة بشكل آخر.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Informasi saat ini tidak lepas dari memanfaatkan suatu teknologi. Sedangkan teknologi sendiri memiliki dampak negarif didalamnya, salah satunya yaitu terkait keamanan. Keamanan informasi pribadi kita ataupun informasi yang ingin kita sampaikan kepada seorang tertentu juga tidak kalah pentingnya untuk diamankan meskipun tanpa menggunakan teknologi. Sehingga pengetahuan tentang ilmu terkait keamanan informasi penting untuk ada. Ilmu yang mempelajari tentang keamanan informasi dinamakan kriptografi. Ilmu kriptografi sangatlah penting untuk diteliti karena pada zaman modern seperti sekarang banyak sekali oknum yang sangat tidak bertanggung jawab dimana mereka memanfaatkan teknologi untuk kepentingan dirinya sendiri dan itu akan merugikan kita sebagai pemilik informasi. Informasi itu sendiri merupakan pesan yang terdiri dari deretan pernyataan-pernyataan yang runtut dari suatu simbol.

Enkripsi dan dekripsi adalah istilah-istilah yang ada di dalam kriptografi. Enkripsi merupakan proses mengubah teks-biasa ke dalam teks-sandi. Proses dilakukan dengan bantuan kunci dan juga algoritma sedangkan dekripsi adalah proses merubah teks-sandi menjadi teks-biasa seperti semula. Teks-sandi merupakan hasil pesan yang telah tersandi sehingga pesan akan sulit terdeteksi maksud didalamnya selama kunci untuk membukanya tidak diketahui. Pesan yang telah tersandi tidak hanya diharapkan untuk menyembunyikan pesan tetapi juga keefisienannya dalam membuka pesan tersebut.

Pesan yang tersandi dengan baik adalah yang susah diretas oleh pihak ketiga tetapi mudah untuk dibuka oleh pihak yang memiliki kunci.

Galois Field (*GF*) adalah *field* atau bisa juga disebut lapangan dimana jumlah himpunan yang dimiliki terbatas. *Galois Field* dipakai secara meluas di dalam kriptografi salah satunya yaitu dalam sistem sandi simetri *AES (Adveced Encryption Standard)* (Sadikin, 2012). *AES* diadopsi oleh pemerintah Amerika Serikat dan menjadi standar enkripsi pada kunci simetris. Sistem dalam sandi simetris menggunakan algoritma sandi dimana metode penyandian dan pembuka sandi menggunakan kunci yang sama. *Galois Field* yang berbasis pada aritmatika modular pada polinomial merupakan tipe *galois field* yang biasa dipakai dalam sistem kriptografi.

Polinomial atau biasa disebut dengan suku banyak merupakan suatu pernyataan matematika yang didalamnya melibatkan penjumlahan pada perkalian dalam pangkat di dalam satu atau lebih variabel dengan suatu koefisien. Operasi dasar di dalam persamaan polinomial itu sama dengan sistem persamaan kuadrat, diantaranya yaitu operasi perkalian dan penjumlahan suku banyak. Operasi pembagian dalam suku banyak juga bisa dilakukan terhadap fungsi lainnya dan terdapat juga sisa pembagian ketika fungsi yang dibagi tidak menghasilkan 0. Polinomial *Galois field* sendiri adalah kombinasi polinomial-polinomial dengan konstanta dari variabelnya adalah kurang dari dua dan dimana pangkat tertinggi dari variabelnya adalah $n - 1$.

Algoritma di dalam kriptografi kunci simetris salah satunya yang terkenal adalah algoritma *Hill Cipher*, dimana algoritma ini menerapkan aritmatika modular yang kuncinya menggunakan sebuah matriks. *Hill Cipher* merupakan salah satu

algoritma kriptografi klasik yang sangat sulit untuk dipecahkan oleh kriptanalis apabila yang diketahui hanyalah berkas ciphertextnya saja (Munir, 2006). Teknik enkripsi *Hill Cipher* yaitu dengan membagi setiap karakter yang akan dienkripsi sesuai dengan jumlah matriks kunci yang digunakan. Apabila terjadi adanya pengurangan karakter ataupun bit, maka akan dilakukan penambahan karakter sembarang sampai sesuai dengan jumlah matriks kunci tersebut (Sihombing, 2014).

Konsep tentang ilmu kriptografi juga terdapat dalam Al-Qur'an yaitu yang berupa amanat, hal tersebut terdapat di dalam surat An-Nisa' ayat 58 yang berbunyi:

إِنَّ اللَّهَ يَأْمُرُكُمْ أَنْ تُؤَدُّوا الْأَمَانَاتِ إِلَىٰ أَهْلِهَا وَإِذَا حَكَمْتُمْ بَيْنَ النَّاسِ أَنْ

تَحْكُمُوا بِالْعَدْلِ ۚ إِنَّ اللَّهَ نِعِمَّا يَعِظُكُمْ بِهِ ۗ إِنَّ اللَّهَ كَانَ سَمِيعًا بَصِيرًا

"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': 58).

Berdasarkan tafsir Al-Wasith (2012), Amanat dan menjaga amanat diharuskan dalam segala hal, baik dalam diri, harta milik orang lain, barang titipan, tidak menipu dalam bermuamalat, jihad, dan memberi nasihat, tidak menyebarkan rahasia dan aib orang lain, amanat dalam agama dengan mengerjakan yang diperintahkan Allah SWT dan menjauhi larangannya, amanat dalam diri dengan hanya melakukan perbuatan yang berguna bagi pribadi, baik dalam agama, dunia maupun akhirat, tidak melakukan amalan apapun yang membahayakan di akhirat dan dunia, menjauhi faktor-faktor yang menyebabkan penyakit, menerapkan aturan-aturan kesehatan, dan tidak menyebabkan diri celaka. Penjelasan tafsir surat An-Nisa' ayat 58 ini kita diperintahkan untuk menyampaikan amanat yang benar yang sudah kita selidiki asal muasalnya dan kita percayai untuk akhirnya akan disampaikan kepada yang berhak menerimanya dan

tidak lalai akan amanat tersebut, berdasarkan penjelasan tersebut maka hal ini termasuk dalam ilmu kriptografi dimana suatu pesan harus diamankan supaya terjaga kerahasiaannya dari yang tidak berhak menerimanya hingga akhirnya sampai kepada penerimanya.

Pada penelitian Viswanath dkk (2015) dengan judul "*A Public Key Cryptosystem Using Hill's Cipher*" didalamnya memaparkan tentang penggunaan algoritma *Hill Cipher* yang diarahkan ke dalam algoritma asimetris dengan menggunakan dua kunci, sedangkan algoritma *Hill Cipher* sendiri hakikatnya merupakan algoritma simetris yang hanya menggunakan satu kunci dalam melakukan penyandian. Pada penelitian Irawan dkk (2020) dengan judul "*Combination of Hill Cipher Algorithm and Caesar Cipher Algorithm for Exam Data Security*" didalamnya memaparkan penggunaan algoritma *Hill Cipher* yang dimodifikasi dengan algoritma *Caesar Cipher* dalam penyandian untuk mengamankan data dan didalamnya juga memaparkan keterlibatan bilangan biner dalam operasi kombinasi yang dilakukan. Berdasarkan semua pemaparan sebelumnya, maka penulis mengangkat judul "Enkripsi dan Dekripsi Pesan Menggunakan Polinomial *Galois Field* dengan algoritma *Hill Cipher*" dimana penulis ingin memanfaatkan algoritma *Hill Cipher* dengan memodifikasinya menggunakan polinomial *Galois Field* untuk penyandian pesan.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka penelitian ini mempunyai rumusan masalah sebagai berikut:

1. Bagaimana proses enkripsi pesan menggunakan polinomial *Galois Field* dengan algoritma *Hill Cipher*?

2. Bagaimana proses dekripsi pesan menggunakan polinomial *Galois Field* dengan algoritma *Hill Cipher*?

1.3 Tujuan Penelitian

Berdasarkan latar belakang di atas maka penelitian ini mempunyai tujuan sebagai berikut:

1. Untuk mengetahui proses enkripsi pesan menggunakan polinomial *Galois Field* dengan algoritma *Hill Cipher*.
2. Untuk mengetahui proses dekripsi pesan menggunakan polinomial *Galois Field* dengan algoritma *Hill Cipher*.

1.4 Manfaat Penelitian

Penulis berharap bahwa di dalam penulisan penelitian ini dapat memberikan manfaat diantaranya:

1. Dapat menambahkan pengetahuan keilmuan tentang Algoritma *Hill Cipher* dan pengetahuan lainnya yang terkait yaitu tentang polinomial dan sistem bilangan biner yang bisa digunakan di dalam ilmu kriptografi.
2. Dapat digunakan sebagai tambahan dalam bahan kepustakaan dan memberikan informasi dalam pembelajaran mata kuliah yang terkait kriptografi.
3. Dapat memperkaya sumber pengetahuan terkait kriptografi dan menjadi sebuah penyelesaian masalah bagi pengguna teknologi dalam menggunakan informasi dan komunikasi dimana supaya dapat dilakukan pengiriman pesan dengan aman.

1.5 Batasan Masalah

Supaya pembahasan di dalam penelitian ini tidak meluas maka peneliti memberikan batasan-batasan masalah sebagai berikut:

Konversi biner yang digunakan hanya pada biner pada bit-8 dengan *Galois Field* yang digunakan yaitu pada $GF\ 2^8$.

1.6 Metode Penelitian

Metode yang dipergunakan di dalam penelitian ini merupakan metode kepustakaan (*library research*) yaitu dimana suatu penelitian menggunakan literatur yang berkaitan terhadap yang diteliti seperti jurnal penelitian, buku, skripsi dan laporan penelitian. Supaya mencapai tujuan yang dikehendaki maka berikut merupakan langka-langkah yang digunakan:

1. Proses enkripsi pesan menggunakan polinomial *Galois Field* dengan algoritma *Hill Cipher*.
    a. Mengonversi karakter pesan yang ingin disandikan ke dalam bentuk polinomial *Galois Field* dengan bantuan bilangan biner.
    b. Melakukan proses perhitungan pada polinomial *Galois Field* dengan menggunakan algoritma *Hill Cipher*.
    c. Mengonversi hasil perhitungan pada polinomial *Galois Field* ke dalam bentuk karakter dengan bantuan bilangan biner.
2. Proses dekripsi pesan menggunakan polinomial *Galois Field* dengan algoritma *Hill Cipher*.
    a. Mengonversi karakter pesan tersandi ke dalam bentuk polinomial *Galois Field* dengan bantuan bilangan biner.

b. Melakukan proses perhitungan pada polinomial *Galois Field* dengan menggunakan algoritma *Hill Cipher*.

c. Mengonversi hasil perhitungan pada polinomial *Galois Field* ke dalam bentuk karakter dengan bantuan bilangan biner.

1.7 Sistematika Penulisan

Sistematika penulisan di dalam penelitian ini terdiri dari empat bab dan pada masing-masing bab tersebut dibagi ke dalam subbab dengan rumusan sebagai berikut:

BAB I Pendahuluan

Pendahuluan di dalamnya memuat latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, metode penelitian, dan sistematika penulisan.

BAB II Kajian Pustaka

Kajian pustaka di dalamnya berisikan teori-teori dan konsep-konsep yang dapat mendukung dalam penelitian. Teori atau konsep tersebut meliputi pengertian kriptografi, elemen-elemen kriptografi, tujuan kriptografi, aritmatika modulo, sistem bilangan biner, *ASCII*, kriptografi kunci simetris dan asimetris, *finite field*, polinomial, operasi aljabar pada polinomial, sifat keterbagian dan faktorisasi polinomial, *hill cipher*, matriks dan kajian keagamaan.

BAB III Pembahasan

Pembahasan di dalamnya berisikan tentang penjelasan dan penguraian secara keseluruhan langkah-langkah yang telah disebutkan dalam metode penelitian dan menjawab rumusan masalah.

BAB IV Penutup

Penutup di dalamnya berisikan kesimpulan dari hasil pembahasan dan saran yang ingin disampaikan penulis kepada pembaca.

BAB II

KAJIAN PUSTAKA

2.1 Kriptografi

2.1.1 Pengertian Kriptografi

Secara estimologi kata kriptografi (*Cryptography*) berasal dari bahasa Yunani, yaitu *kryptos* yang berarti tersembunyi dan *graphein* yang berarti tulisan. Kriptografi pertama kali dikenal atau dipahami sebagai ilmu tentang menyembunyikan pesan (Sadikin, 2012). Kriptografi adalah studi tentang teknik komunikasi aman yang memungkinkan hanya pengirim dan penerima pesan yang dituju untuk melihat isinya. Kriptografi mulai berkembang menjadi ilmu yang dimanfaatkan untuk menyelesaikan persoalan terkait keamanan pribadi dan juga verifikasinya (Whirfield, 1976).

Kriptografi berkaitan terhadap proses mengubah pesan biasa menjadi pesan yang tidak dapat dipahami begitupun sebaliknya. Metode ini digunakan sebagai sarana penyimpanan dan pengiriman data dalam berbagai bentuk tertentu dimana hanya mereka yang ditujukan yang dapat memproses dan membacanya. Kriptografi tidak hanya melindungi data dari peretas, tetapi juga bisa digunakan sebagai otentikasi pengguna (Ariyus, 2012). Banyak aplikasi yang menggunakan ilmu kriptografi diantaranya seperti kartu transaksi perbankan, sandi komputer, dan transaksi *e-commerce*. Metode paling sederhana dalam kriptografi adalah menggunakan sistem kunci simetris dimana pesan akan di enkripsi dengan menggunakan kunci simetris dan kemudian pesan yang disandikan berikut kuncinya dikirim kepada penerima untuk didekripsi (Mukhtar, 2018).

2.1.2 Elemen-Elemen Kriptografi

1. Pesan, *Plaintext,* dan *Chipertext*

Pesan merupakan terjemahan dari bahasa asing "*message*" yang artinya adalah lambang bermakna (*meaningful symbols*), yakni lambang yang membawakan pikiran atau perasaan komunikator (Rakhmat, 1985). Pesan merupakan komunikasi yang disampaikan pengirim kepada sekelompok penerima atau beberapa penerima. Pesan merupakan bagian dari unsur di dalam proses komunikasi. Sebuah pesan dapat dikirimkan dengan berbagai cara diantaranya yaitu dengan menggunakan kurir ataupun secara elektronik dan pesan dapat disampaikan dengan menggunakan media komunikasi maupun bertatap muka secara langsung. Dalam studi komunikasi, pesan merupakan informasi yang disampaikan dengan kata-kata, baik ucapan maupun tulisan. Pesan dapat berisi informasi, hiburan, ilmu pengetahuan, nasihat atau propaganda (Siahaan, 1991).

Pesan merupakan suatu ide atau gagasan yang dituangkan ke dalam lambang-lambang dimana untuk disebarkan lalu kemudian diteruskan oleh komunikator yang difungsikan untuk menciptakan komunikasi yang baik dan akurat antara komunikator dan komunikan (Rakhmat, 1993). Suatu pesan harus disampaikan sebaik mungkin, hal yang perlu dipertimbangkan dalam menyampaikan pesan diantaranya:

1) *Clear*, artinya suatu pesan haruslah jelas dimana bahasa yang digunakan mudah untuk dipahami.
2) *Correct*, artinya suatu pesan haruslah mengandung kebenaran yang sudah teruji dimana pesan itu berdasarkan fakta dan tidak meragukan.

3) *Concise*, artinya suatu pesan haruslah ringkas dan tanpa mengurangi arti sesungguhnya.
4) *Comprehensive*, artinya suatu pesan itu mencakup bagian-bagian yang penting yang harus diketahui komunikan.
5) *Concrite*, artinya pesan itu nyata yaitu dapat dipertanggung jawabkan berdasarkan data dan fakta yang ada.
6) *Complete*, artinya pesan itu lengkap dan penulisannya disusun secara sistematis.
7) *Convinsing*, artinya pesan itu haruslah menarik dan meyakinkan karena logis.
8) Pesan itu disampaikan dengan baru.
9) Nilai di dalam suatu pesan mengandung pertentangan antara bagian yang satu dengan yang lainnya (Siahaan, 1991).

Dalam bahasa kriptografi, kode-kode disebut sandi (*cipher*), pesan yang tidak dikode disebut teks-biasa (*plaintext*) dan pesan-pesan yang dikode disebut teks-sandi (*ciphertext*). Proses pengubahan dari teks-biasa ke teks-sandi disebut penyandian (*enciphering*) dan proses kebalikannya yaitu pengubahan dari teks-sandi ke teks-biasa disebut penguraian (*deciphering*) (Mukhtar, 2018).

2. Enkripsi dan Dekripsi

Tugas mendasar dan klasik dari kriptografi adalah memberikan *confidentintiality* dengan metode enkripsi (Hoffstein dkk, 2012). Pesan yang akan dikirim bisa menjadi beberapa teks, data numerik, program yang dapat dijalankan atau jenis informasi lainnya atau yang bisa disebut sebagai *plaintext*. Pengirim mengenkripsi *plaintext* dan mendapatkan *ciphertext*. *Ciphertext*

ditransmisikan ke penerima kemudian penerima mengubah *ciphertext* kembali ke teks biasa dengan dekripsi. Untuk mendekripsi, penerima membutuhkan beberapa informasi rahasia, yaitu kunci dekripsi. Kunci memiliki kemungkinan untuk menghadang *ciphertext*, namun enkripsi harus menjamin kerahasiaan dan pencegahan kepada penerima, supaya penerima mendapatkan segala informasi tentang pesan berkode dari *ciphertext*. Setiap metode enkripsi menyediakan algoritma enkripsi (E) dan algoritma dekripsi (D). Dalam skema enkripsi klasik, kedua algoritma bergantung pada kunci rahasia yang sama yaitu misalkan k, kunci k ini digunakan untuk keduanya, yaitu enkripsi dan dekripsi (Whirfield dan Martin, 1976).

Metode enkripsi kunci publik atau metode asimetris adalah dimana setiap penerima pesan memiliki kunci pribadinya yaitu $k = (pk\ sk)$, terdiri dari dua bagian: pk adalah kunci enkripsi untuk dibuat publik, sk adalah kunci dekripsi dan dirahasiakan (Kromodimoeljo, 2009). Jika pengirim ingin mengirim file pesan m kepada penerima, pengirim mengenkripsi m dengan menggunakan enkripsi penerima yang diketahui publik dengan kunci pk. Penerima mendekripsikan *ciphertext* dengan menggunakan kunci dekripsi sk, yaitu hanya diketahui olehnya. Maka kita punya

$$D(sk, E(pk, m)) = m \tag{2.1}$$

Secara matematis, enkripsi kunci publik disebut sebagai *one-way function*. Setiap orang dapat dengan mudah mengenkripsi teks biasa dengan menggunakan kunci publik pk, tetapi arah lainnya-lah yang sulit. Secara praktis tidak mungkin untuk menyimpulkan *plaintext* dari *ciphertext*, tanpa mengetahui kunci rahasia sk. Metode enkripsi kunci publik memerlukan

komputasi yang lebih kompleks dan kurangnya keefisienan dibandingkan dengan metode simetris klasik. Metode simetris digunakan untuk enkripsi data dalam jumlah besar (Kromodimoeljo, 2009). Sebelum menerapkan enkripsi simetris, pengirim dan penerima harus menyetujui sebuah kunci untuk menyimpan kunci ini supaya rahasia dan mereka membutuhkan saluran komunikasi yang aman.

3. Pengirim dan Penerima

Pengirim merupakan tindakan pengiriman oleh suatu entitas dalam kepentingan berkomunikasi berupa pesan ataupun dokumen kepada entitas yang lain, sedangkan entitas yang menerima pesan ataupun dokumen dalam proses komunikasi dinamakan penerima (Kurniawan, 2004). Entitas disini yang dimaksud adalah orang, komputer, kartu kredit dan lainnya.

4. Algoritma Kriptografi

Algoritma kriptografi merupakan fungsi matematika atau aturan yang dipakai untuk enkripsi dan dekripsi. Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yaitu berupa himpunan yang berisi elemen-elemen *plaintext* dan himpunan yang berisi elemen-elemen *ciphertext*, dimana enkripsi dan dekripsinya merupakan fungsi yang memetakkan elemen-elemen antara dua himpunan tersebut (Kurniawan, 2004).

5. Sistem Kriptografi

Sistem kriptografi merupakan kumpulan dari algoritma kriptografi, termasuk *plaintext* dan *ciphertext* berikut kuncinya (Ariyus, 2012).

6. Penyadap Serangan

Penyadap merupakan seorang entitas yang berusaha mengambil pesan ketika pesan sedang ditransmisikan yang bertujuan untuk mendapatkan informasi sebanyak mungkin mengenai sistem kriptografi yang dipakai untuk berkomunikasi dengan maksud untuk memecahkan *ciphertext*. Kriptanalisis adalah ilmu yang mempelajari serangan terhadap skema kriptografi (Ariyus, 2012). Serangan yang berhasil dilakukan, misalnya, memulihkan teks biasa (atau bagian dari *plaintext*) dari *ciphertext*, mensubstitusi bagian dari pesan asli. Keamanan sistem kriptografi harus sepenuhnya didasarkan pada kunci rahasia.

Serangan terhadap kerahasiaan skema enkripsi mencoba memulihkan teks biasa dari *ciphertext*, atau bahkan lebih drastis, untuk memulihkan kunci rahasia. Musuh tidak mencoba mengubah pesan tetapi dia memantau saluran komunikasi dan titik akhir saluran. Jadi dia mungkin tidak hanya menghadang *ciphertext*, tetapi (setidaknya dari waktu ke waktu) dia mungkin bisa mengamati enkripsi dan dekripsi pesannya tanpa memiliki informasi tentang kunci. Misalnya, musuh adalah operator komputer bank. Dia melihat *ciphertext* yang masuk dan terkadang juga *plaintext* yang sesuai, atau dia mengamati teks biasa yang keluar dan teks sandi yang dihasilkan, mungkin dia akan berhasil mengenkripsi teks biasa atau mendekripsi teks sandi pilihan miliknya sendiri.

Serangan yang mungkin terjadi bergantung pada sumber daya sebenarnya dari musuh. Mereka biasanya diklasifikasikan sebagai berikut (Hoffstein dkk, 2012):

1) Serangan hanya teks sandi.

   Penyadap memiliki kemampuan untuk mendapatkan *ciphertext*. Ini kemungkinan besar akan menjadi kasus dalam berbagai situasi enkripsi. Bahkan jika peretas tidak bisa melakukan serangan yang lebih canggih, orang harus berasumsi bahwa dia bisa mendapatkan akses ke dalam pesan terenkripsi. Metode enkripsi yang tidak bisa menahan serangan *ciphertext-only* sama sekali tidak aman.

2) Serangan teks biasa.

   Penyadap memiliki kemampuan untuk mendapatkan pasangan *plaintext-ciphertext*. Menggunakan informasi dari pasangan ini, dia mencoba mendekripsikan *ciphertext* dimana dia tidak memiliki *plaintext*-nya. Sekilas mungkin tampak bahwa informasi seperti itu biasanya tidak tersedia untuk seorang penyerang tetapi itu sangat sering tersedia. Pesan mungkin dikirim dan masuk ke dalam format standar yang diketahui penyadap.

3) Serangan teks-teks yang dipilih.

   Penyadap memiliki kemampuan untuk mendapatkan *ciphertext* untuk *plaintext* yang dia pilih. Kemudian dia mencoba untuk mendekripsi sebuah *ciphertext* yang tidak memiliki *plaintext*. Mungkin ini tampak kecil kemungkinannya dimana terdapat banyak kasus dimana peretas dapat melakukan hal ini, contohnya:

   Misalkan andi merupakan peretas, mengirimkan beberapa informasi menarik kepada korban yang dituju dan yang diyakini akan mengenkripsi dan mengirimkannya. Jenis serangan ini mengasumsikan

bahwa penyadap pertama-tama harus mendapatkan pasangan *plaintext* yang diinginkannya dan kemudian melakukan analisisnya, tanpa interaksi lebih lanjut. Ini berarti bahwa dia hanya memerlukan akses ke perangkat enkripsi satu kali.

4) Serangan teks-teks yang dipilih secara adaptif.

   Ini sama dengan sebelumnya, sekarang penyadap dapat melakukan beberapa analisis pada pasangan *plaintext-ciphertext*, dan kemudian mendapatkan lebih banyak pasangan. Penyadap mungkin beralih di antara kumpulan memasang pasangan dan melakukan analisis sesering yang dia suka. Ini berarti bahwa dia memiliki akses panjang ke perangkat enkripsi atau dapat memanfaatkannya berulang kali.

5) Serangan *ciphertext* yang dipilih dan dipilih secara adaptif.

   Kedua serangan ini mirip dengan serangan teks biasa di atas. Penyadap dapat memilih *ciphertext* dan mendapatkan teks biasa yang sesuai. Dia memiliki akses ke perangkat dekripsi.

7. Kriptanalisis dan Kriptologi

Kriptologi (*cryptanalysis*) adalah ilmu yang mempelajari serangan terhadap skema kriptografi. Pelaku terhadap serangan dalam skema kriptografi dinamakan kriptanalisis (Ariyus, 2012). Kriptologi adalah studi mengenai kriptografi dan kriptanalisis.

2.1.3 Tujuan Kriptografi

Memberikan kerahasiaan bukan satu-satunya tujuan kriptografi. Kriptografi juga digunakan untuk memberikan solusi terhadap masalah lain diantaranya (Whirfield dan Martin, 1976):

1. **Integritas Data**

Penerima pesan harus dapat memeriksa apakah pesan itu diubah selama transmisi, baik secara tidak sengaja atau dengan sengaja. Tidak ada yang bisa menggantikan pesan palsu untuk pesan asli, atau untuk sebagian dari itu.

2. **Otentikasi**

Penerima pesan harus dapat memverifikasi asalnya. Seharusnya tidak ada yang bisa mengirim pesan ke penerima dan berpura-pura menjadi pengirim (otentikasi asal data). Saat memulai komunikasi, pengirim dan penerima harus dapat mengidentifikasi satu sama lain (otentikasi asal data).

3. ***Non-repudiation***

Pengirim seharusnya tidak dapat menyangkal bahwa dia sebelumnya telah mengirimkan pesan. Jika pesan ditulis di atas kertas, media kertas sendiri menyediakan keamanan terhadap manipulasi. Tetapi jika media elektronik digunakan, media itu sendiri tidak memberikan keamanan sama sekali, karena mudah untuk diganti *byte* dalam pesan selama transmisi melalui jaringan komputer, dan itu sangat mudah didapatkan jika jaringan dapat diakses oleh publik, seperti internet. Jadi meskipun enkripsi memiliki sejarah yang panjang, 3 kebutuhan akan teknik integritas dan otentikasi data dihasilkan dari peningkatan yang pesat dimana pentingnya komunikasi elektronik. Terdapat metode simetris serta kunci publik untuk dapat memastikan integritas suatu pesan.

2.1.4 Aritmatika Modular

Aritmatika modular merupakan aritmatika yang banyak digunakan dalam kriptografi. Aritmatika modular (*modular arithmetic*) merupakan metode

aritmatika untuk menyelesaikan permasalahan terkait bilangan bulat. Mod merupakan operator yang digunakan pada aritmatika modulo. Operator mod memberikan sisa pembagian (Munir, 2008). Misalnya 41 dibagi 7 memberikan hasil 5 dan sisa 6, dimana penulisannya yaitu $41\ mod\ 7 = 6$.

Definisi 2.1 Pembagian

Jika $a, b \in \mathbb{Z}, b \neq 0$ maka dapat dikatakan bahwa b membagi a, dilambangkan dengan $b|a$, yang berarti bahwa $a = bx$ untuk a tunggal $x \in \mathbb{Z}$, dilambangkan dengan $x = a/b$ (Hadley, 1992). Perhatikan bahwa ada dan tunggalnya x menunjukkan bahwa b tidak boleh 0. Kita juga dapat mengatakan bahwa a habis dibagi dengan b. Jika b tidak membagi a, maka kita tulis $b \nmid a$ dan mengatakan bahwa a tidak habis dibagi b. Kita katakan bahwa pembagian dengan nol tidak terdefinisi.

Contoh:

- $5|10$, karena terdapat $k = 2$ sehingga $5k = 10$
- $3 \nmid 7$, karena tidak ada nilai k yang memenuhi $3k = 7$

Teorema 2.1 Algoritma Pembagian

Jika $a \in \mathbb{N}$ dan $b \in \mathbb{Z}$, maka terdapat bilangan bulat tunggal $q, r \in \mathbb{Z}$ dengan $0 \leq r < a$ dan $b = aq + r$ (Hadley, 1992).

Untuk mengatakan bahwa b membagi a adalah dimana a adalah kelipatan dari b dan b adalah pembagi dari a. Perhatikan juga bahwa b membagi a sama dengan sisa atas pembagian a dengan b adalah nol. Ketika setiap pembagi $b \neq a$ dari a dikatakan *proper divisor* dari a. jika kita memiliki dua bilangan bulat a dan b, maka *common divisor* dari a dan b adalah bilangan asli n yang merupakan pembagi dari keduanya yaitu a dan b.

Contoh:

Misalkan $a = -7$, Untuk $a = 1, -2{,}61$ dan 59 maka dapat dituliskan sebagai

$1 = 0(-7) + 1$

$2 = 1(-7) + 5$

$61 = (-8)(-7) + 5$

$-59 = 9(-7) + 4$

Definisi 2.2 Kongruensi

Jika $n \in \mathbb{N}$ maka dapat kita katakan bahwa a kongruen dengan b modulo n jika $n|(a - b)$, dinotasikan dengan

$$a \equiv b(mod\ n)$$

Sebaliknya, jika $n \nmid (a - b)$ maka dapat ditulis

$$a \not\equiv b(mod\ n)$$

dan dapat dikatakan bahwa a dan b adalah tidak kongruen modulo n, atau bahwa a tidak kogruen dengan b modulo n (Hadley, 1992).

Contoh:

- $27 \equiv 5\ (mod\ 2\ )$

  27 kongruen dengan 5 modulo 2, yang artinya 27 dan 5 dibagi 2 bersisa 1 atau $2|(27 - 5)$

- $13 \equiv -2\ (mod\ 5\ )$

13 kongruen dengan -2 modulo 5, lebih mudah difahami ketika berbentuk $5|(13 + 2)$ atau artinya sama dengan 13 dan -2 dibagi 5 bersisa 0 atau tidak memiliki sisa.

2.1.5 Sistem Bilangan Biner

Bilangan biner merupakan bilangan berbasis dua yang hanya mempunyai dua digit yaitu 0 dan 1 (Haryanto dan Sucipto, 2013). 0 dan 1 disebut sebagai bilangan *bynari digit* atau bit. Gottfried Wilhelm Leibniz merupakan penemu dari sistem bilangan biner modern pada abad ke-17. Dasar dari semua sistem bilangan berbasis digital merupakan sistem bilangan biner. Bobot faktor untuk bilangan biner adalah pangkat atau kelipatan dua. Sistem biner dapat dikonversikan ke dalam sistem bilangan Oktal atau Hexadesimal. Sistem bilangan biner digunakan oleh perangkat digital seperti komputer dimana pengelompokan binernya selalu berjumlah 8 yang memiliki istilah yaitu 1-byte atau bita. Dalam perangkat digital, *low* atau tidak berhasil ditandai dengan 0 sedangkan 1 jika *high* atau berhasil. Perhitungan pada biner berbeda dengan perhitungan basis 10 (desimal). Berikut merupakan skema bilangan biner:

Tabel 2.1 Skema Bilangan Biner

Desimal	**Biner (8-bit)**
0	00000000
1	00000001
2	00000010
3	00000011
4	00000100
5	00000101
6	00000110
7	00000111
8	00001000
9	00001001
10	00001010
11	00001011
12	00001100

Desimal	Biner (8-bit)
13	00001101
14	00001110
15	00001111
16	00010000

2.1.6 *ASCII*

ASCII (*American Standard Code for Information Interchange*) merupakan pengkodean karakter, dimana karakter yang dikodekan yaitu huruf, angka, dan tanda baca. *ASCII* merupakan standar yang dipakai untuk merepresentasikan karakter-karakter tersebut. Kode *ASCII* memiliki komposisi bilangan biner sebanyak 8-bit yang dimulai dari 0000 0000 hingga 1111 1111. Jumlah kombinasi karakter yang dihasilkan adalah sebanyak 256, dimulai dari kode 0 hingga 255, diantaranya mencakup alfabet a−z, A−Z, 0−9, beberapa tanda baca yang umum digunakan dan beberapa karakter control. *ASCII* saat ini merupakan salah satu standar yang banyak dipergunakan pada komputer dan perangkat komunikasi.

2.1.7 Kriptografi Simetris

Algoritma enkripsi seringkali dibagi menjadi dua kategori, yang dikenal sebagai enkripsi simetris dan asimetris. Perbedaan mendasar antara kedua metode enkripsi ini bergantung pada sebuah fakta dimana algoritma enkripsi simetris menggunakan sebuah kunci, sedangkan enkripsi asimetris menggunakan dua kunci yang saling berhubungan (Kurniawan, 2004). Dengan perbedaan seperti itu, walaupun terlihat sangat sederhana, hal ini memiliki perbedaan fungsional antara kedua jenis teknik enkripsi dan bagaimana mereka dipergunakan. Kriptografi kunci simetris merupakan metode enkripsi dimana pengirim maupun penerima memiliki kunci yang sama.

Dikarenakan kecepatannya, algoritma enkripsi simetris lebih luas digunakan untuk melindungi informasi dalam banyak sekali sistem komputer modern. Contohnya, *Advanced Encryption Standard* (*AES*) digunakan oleh pemerintah Amerika Serikat untuk mengenkripsi informasi sensitif dan rahasia. *AES* menggantikan *Data Encryption Standard* (*DES*) yang sebelumnya digunakan, yang dikembangkan pada tahun 1970-an sebagai standar untuk enkripsi simetris (Kurniawan, 2004).

2.1.8 Kriptografi Kunci Asimetris

Enkripsi asimetris dapat diaplikasikan ke sistem yang dimana banyak pengguna dapat mengenkripsi dan mendekripsi pesan atau rangkaian data, terutama pada saat kecepatan dan daya komputasi bukan merupakan masalah utama (Kromodimoeljo, 2009). Satu contoh dari sistem tersebut adalah enkripsi email, dimana kunci publik dapat digunakan untuk mengenkripsi pesan, dan kunci pribadi dapat digunakan untuk mendekripsi pesan tersebut.

2.2 *Finite Field*

Finite Field atau dikenal juga dengan *Galois Field* (GF) adalah *field* yang jumlah himpunannya terbatas. *Galois Field* dipakai secara luas dalam kriptografi contohnya yaitu dalam sistem sandi simetri *AES (Adveced Encryption Standard)* (Sadikin, 2012).

2.2.1 Polinomial

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

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \qquad (2.2)$$

a_i adalah konstanta riil, $i = 0,1,2,3, \dots, n$ dan $a_n \neq 0$. Dengan x merupakan peubah, sedangkan $a_0, a_1, a_2, \dots, a_n$ secara berurutan merupakan nilai koefisian persamaan $x^0, x^1, x^2, \dots, x^n \cdot n$ merupakan orde atau derajat persamaan (Munir, 2008).

2.2.2 Operasi Aljabar pada Polinomial

1. **Penjumlahan**

   Cara untuk menjumlahkan polinomial $f(x)$ dengan $g(x)$ adalah dengan menjumlahkan suku yang sejenis contohnya yaitu $4x^3$ dan $9x^3$, ketika ditambahkan maka akan menjadi $13x^3$, akan tetapi suku yang jenisnya lain misalkan $4x^4$ dan $9x^3$ jika ditambahkan akan menjadi $4x^4 + 9x^3$. Pada penjumlahan polinomial yang perlu diperhatikan dalam melakukan operasinya adalah pada pangkat polinomial yang dimilikinya.

2. **Pengurangan**

   Cara untuk mengurangkan polinomial $f(x)$ dengan $h(x)$ adalah dengan mengurangi suku yang sejenis contohnya yaitu $7x^2$ dan $3x^2$ dapat dikurangkan menjadi $4x^2$, akan tetapi suku yang jenisnya lain misalkan $7x^3$ dan $3x^2$ bila dikurangkan akan menjadi $7x^3 - 3x^2$. Dalam pengurangan pada polinomial yang perlu diperhatikan dalam melakukan operasinya adalah pada pangkat polinomial yang dimilikinya.

3. **Perkalian**

   Perkalian pada polinomial memiliki sifat distributif. Cara untuk mengalikan polinomial *f*(*x*) dengan *g*(*x*) yaitu dengan saling mengalikan suku-suku dari kedua polinomialnya. Sifat perkalian ini berlaku juga pada distributif

perkalian terhadap operasi penjumlahan ataupun distributif perkalian terhadap operasi pengurangan (Anton dan Rorres, 1998).

$$f(x) \cdot g(x) = (ax3 + bx2 + cx + d)(ex3 + fx2 + gx + h)$$

$$= aex6 + (af + be)\,x5 + (ag + bf + ce)\,x4 + (ah + bg + cf + de)\,x3 + (bh + cg + df)\,x2 + (ch + dg)\,x + dh$$

4. Pembagian

Salah satu metode yang dapat dipakai untuk melakukan operasi pembagian pada polinomial adalah dengan horner (Anton dan Rorres, 1998). Dengan cara horner dan bersusun kita dapat menentukan hasil bagi dan sisa pada operasi polinomial. Pembagian dengan koefisien yang tak tentu mengikuti definisi pembagian polinomial berikut:

$$p(x) = q(x) \cdot h(x) + s(x) \qquad (2.3)$$

Keterangan:

$p(x) =$ yang dibagi

$q(x) =$ pembagi

$h(x) =$ hasil bagi

$s(x) =$ sisa pembagian

2.2.3 Sifat Keterbagian dan Faktorisasi

1. Sifat Keterbagian Polinomial

Suatu polinomial yang berbentuk pecahan dengan derajat pembilangnya lebih besar dari penyebut, maka penyederhanaan polinomialnya dapat dilakukan dengan keduanya dibagi dengan bilangan yang sama besar. Suatu polinom $p(x)$ dapat dibagi dengan polinom lainnya $q(x)$ dengan derajat lebih kecil dan hasilnya $h(x)$ serta sisa pembagian adalah $s(x)$, yaitu (Anton, 1987):

$$Pembagi\ polinomial = \frac{sisa\ pembagian}{pembagi} + hasil\ bagi$$

$$h(x) = \frac{p(x)}{q(x)} sisa\ s(x) \tag{2.4}$$

2. Faktorisasi Polinomial

Faktor dari suatu ungkapan matematika adalah bilangan, variabel, konstata, suku dan koefisien yang membagi habis ungkapan matematika tersebut. Setiap bentuk atau ekspresi matematika memiliki paling sedikit dua faktor yaitu bilangan 1 dan dirinya sendiri (Anton, 1987).

2.2.4 *Finite Field* dengan Elemen Polinomial *GF* (2^n)

Selain (p) yang berbasis bilangan prima p, jenis *Galois Field* yang sering digunakan dalam sistem kriptografi adalah $GF(p^n) \cdot GF(p^n)$ berbasis pada aritmatika modular polinomial $m(x)$:

$$m(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^0 + x_0 \tag{2.5}$$

Polinomial $m(x)$ disebut dengan *irreducible polynomial* $m(x)$ adalah polinomial berderajat n yang koefisiennya adalah pada $GF(p^n)$. Elemen a_i adalah elemen pada $GF(p^n)$ dan $a_n \neq 0$. Karakteristik *irreducible polynomial* $m(x)$ menyerupai bilangan prima, yaitu tidak dapat habis dibagi kecuali oleh dirinya sendiri dan 1 (Sadikin, 2012).

Elemen pada $GF(p^n)$ merupakan semua polinomial yang berderajat antara 0 sehingga $n-1$ dengan koefisiennya merupakan elemen pada $GF(p)$. Misalkan elemen pada $GF(p^n)$ ditulis sebagai (x) maka $f(x)$ adalah:

$$f(x) = a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x^0 + x_0 \tag{2.6}$$

Ketika koefisien a_i berada pada $GF(p)$, variabel x pada $f(x)$ bersifat tidak ditentukan tapi nilai pangkat i pada x^i menyatakan posisi koefisien a_i.

Jika $p = 2$ maka terbentuk $GF(2^n)$ yang merupakan struktur aljabar yang sering digunakan dalam kriptografi karena elemen $GF(2^n)$ dapat dipresentasikan secara langsung sebagai nilai biner (Sadikin, 2012). Elemen pada $GF(2^n)$ adalah polinomial dengan derajat kurang dari n yaitu:

$$f(x) = a_{n-1}x^{n-1} + \cdots + a_1x^0 + x_0 \quad (2.7)$$

dengan koefisien a_i bernilai 0 atau 1 (Sadikin, 2012).

2.3 *Hill Cipher*

Hill Cipher merupakan salah satu kunci algoritma simetris dalam kriptografi (ilmu tentang membuat dan memecahkan kode dan sandi) yang menggunakan matriks $m \times m$ sebagai kunci dalam proses enkripsi dan dekripsinya dimana m merupakan bilangan bulat tak negatif antara $0,1,\ldots,m-1$ dengan m merupakan panjang alfabet. Dasar teori dalam algoritma *Hill Cipher* merupakan perkalian matriks dengan invers matriks (Supranto, 2003). *Hill Cipher* adalah *Block Cipher*. Enkripsi menggunakan *Hill Cipher* yang pertama adalah menentukan matriks $n \times n$ sebagai kunci enkripsi. Matriks K yang menjadi kunci haruslah matriks yang *invertible* dimana mempunyai *multiplicative inverse* K^{-1} sehingga $K \cdot K^{-1} = K^{-1} \cdot K = I$ (Gazali, 2005). Kemudian menentukan pesan yang ingin disandikan dengan menghapus semua spasi dan simbol tanda baca, setelah itu merubah karakter menjadi angka antara $0-25$. Langkah selanjutnya adalah membagi rangkaian angka menjadi blok-blok berukuran n, jika E adalah matriks $n \times n$ maka ukuran blok adalah n. Kemudian tulis setiap blok sebagai vektor kolom berukuran n dan ambil masing-masing vektor kemudian kalikan dengan matriks E. Langkah terakhir

adalah ambil vektor hasil perkalian dan tulis entri vektor secara berurutan dan ubah nomor ke dalam karakter kembali. Sedangkan untuk melakukan dekripsinya adalah yang pertama yaitu menentukan $D = E\ (mod\ 26)$ yang menjadi kunci dekripsinya. Langkah selanjutnya adalah mengambil ciphertextnya dan mengubah menjadi matriks C, setelah itu menghitung $DC = M$. Kemudian mengubah matriks M menjadi pesan teks biasa.

Contoh:

Proses Enkripsi

Text asli: MATEMATIKA

Kunci: $K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$

$K^{-1} = \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix}$

mengorespondenkan abjad dengan numerik

Tabel 2.2 Konversi Karakter ke dalam Desimal

M	A	T	E	M	A	T	I	K	A
12	0	19	4	12	0	19	8	10	0

Melakukan perhitungan dengan 2 balok antara kunci dengan pesan:

$$\begin{bmatrix} 12 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} = \begin{bmatrix} (12 \cdot 11) + (0 \cdot 8) \\ (12 \cdot 3) + (0 \cdot 7) \end{bmatrix} = \begin{bmatrix} 132 \\ 36 \end{bmatrix} mod\ 26 = \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}$$

$$\begin{bmatrix} 19 \\ 4 \end{bmatrix} \cdot \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} = \begin{bmatrix} (19 \cdot 11) + (4 \cdot 8) \\ (19 \cdot 3) + (4 \cdot 7) \end{bmatrix} = \begin{bmatrix} 209 + 32 \\ 57 + 28 \end{bmatrix} mod\ 26 = \begin{bmatrix} 7 \\ 1 \end{bmatrix} = \begin{bmatrix} H \\ B \end{bmatrix}$$

$$\begin{bmatrix} 12 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} = \begin{bmatrix} (12 \cdot 11) + (0 \cdot 8) \\ (12 \cdot 3) + (0 \cdot 7) \end{bmatrix} = \begin{bmatrix} 132 \\ 36 \end{bmatrix} mod\ 26 = \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}$$

$$\begin{bmatrix} 19 \\ 8 \end{bmatrix} \cdot \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} = \begin{bmatrix} (19 \cdot 11) + (8 \cdot 8) \\ (19 \cdot 3) + (8 \cdot 7) \end{bmatrix}$$

$$= \begin{bmatrix} 209 + 64 \\ 57 + 56 \end{bmatrix} mod\ 26 = \begin{bmatrix} 13 \\ 10 \end{bmatrix} = \begin{bmatrix} N \\ K \end{bmatrix}$$

$$\begin{bmatrix}10\\0\end{bmatrix}\cdot\begin{bmatrix}11 & 8\\3 & 7\end{bmatrix}=\begin{bmatrix}(10\cdot 11)+(0\cdot 8)\\(10\cdot 3)+(0\cdot 7)\end{bmatrix}=\begin{bmatrix}110\\30\end{bmatrix} mod\ 26=\begin{bmatrix}6\\4\end{bmatrix}=\begin{bmatrix}G\\E\end{bmatrix}$$

Sehingga diperoleh *Ciphertext*: CKHBCKNKGE

Proses Dekripsi

Ciphertext: CKHBCKNKGE

Kunci: $K^{-1}=\begin{bmatrix}7 & 18\\23 & 11\end{bmatrix}$

mengorespondenkan abjad dengan numerik

Tabel 2.3 Konversi Karakter ke dalam Desimal

C	K	H	B	C	K	N	K	G	E
2	10	7	1	2	10	13	10	6	4

Melakukan perhitungan sebagai berikut:

$$\begin{bmatrix}2\\10\end{bmatrix}\cdot\begin{bmatrix}7 & 18\\23 & 11\end{bmatrix}=\begin{bmatrix}(2\cdot 7)+(10\cdot 18)\\(2\cdot 23)+(10\cdot 11)\end{bmatrix}=\begin{bmatrix}14+180\\46+110\end{bmatrix} mod\ 26=\begin{bmatrix}12\\0\end{bmatrix}$$

$$=\begin{bmatrix}M\\A\end{bmatrix}$$

$$\begin{bmatrix}7\\1\end{bmatrix}\cdot\begin{bmatrix}7 & 18\\23 & 11\end{bmatrix}=\begin{bmatrix}(7\cdot 7)+(1\cdot 18)\\(7\cdot 23)+(1\cdot 11)\end{bmatrix}=\begin{bmatrix}49+18\\161+11\end{bmatrix} mod\ 26=\begin{bmatrix}19\\4\end{bmatrix}=\begin{bmatrix}T\\E\end{bmatrix}$$

$$\begin{bmatrix}2\\10\end{bmatrix}\cdot\begin{bmatrix}7 & 18\\23 & 11\end{bmatrix}=\begin{bmatrix}(2\cdot 7)+(10\cdot 18)\\(2\cdot 23)+(10\cdot 11)\end{bmatrix}$$

$$=\begin{bmatrix}14+180\\46+110\end{bmatrix} mod\ 26=\begin{bmatrix}12\\0\end{bmatrix}=\begin{bmatrix}M\\A\end{bmatrix}$$

$$\begin{bmatrix}13\\10\end{bmatrix}\cdot\begin{bmatrix}7 & 18\\23 & 11\end{bmatrix}=\begin{bmatrix}(13\cdot 7)+(10\cdot 18)\\(13\cdot 23)+(10\cdot 11)\end{bmatrix}$$

$$=\begin{bmatrix}91+180\\299+110\end{bmatrix} mod\ 26=\begin{bmatrix}19\\8\end{bmatrix}=\begin{bmatrix}T\\I\end{bmatrix}$$

$$\begin{bmatrix}6\\4\end{bmatrix}\cdot\begin{bmatrix}7 & 18\\23 & 11\end{bmatrix}=\begin{bmatrix}(6\cdot 7)+(4\cdot 18)\\(6\cdot 23)+(4\cdot 11)\end{bmatrix}$$

$$=\begin{bmatrix}42+72\\138+44\end{bmatrix} mod\ 26=\begin{bmatrix}10\\0\end{bmatrix}=\begin{bmatrix}K\\A\end{bmatrix}$$

Maka diperoleh pesan asli: MATEMATIKA

2.3.1 Matriks

1. Pengertian Matriks

Di dalam aljabar linier, matriks adalah kumpulan elemen berbentuk persegi panjang yang disusun menjadi baris dan kolom. Matriks $r \times c$ memiliki r baris dan c kolom (Hadley, 1992).

Bentuk umum dari matriks $A_{r\times c}$ adalah:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1c} \\ a_{21} & a_{22} & \cdots & a_{2c} \\ \vdots & \vdots & \vdots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rc} \end{bmatrix}$$

a_{rc} menunjukkan elemen dalam A pada baris r dan kolom c (Anton, 1987). Matriks menggunakan indeks berbasis 1, jadi baris dan kolom pertama diberi nomor satu. Misalkan a_{11}, dibaca "a satu dua" bukan "a dua belas" dimana ini adalah elemen pada baris pertama dan kolom kedua. Matriks dengan jumlah baris yang sama dengan kolom disebut matriks persegi. Elemen diagonal matriks persegi adalah elemen yang indeks baris dan kolomnya sama.

$$B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix}$$

Misalnya elemen diagonal dari matriks 3×3 adalah m_{11}, m_{22}, m_{33}. Elemen lainnya adalah elemen non-diagonal. Elemen-elemen diagonal membentuk diagonal matriks. Jika semua elemen non-diagonal dalam suatu matriks adalah nol, maka matriks tersebut adalah matriks diagonal, contohnya:

$$M = \begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

Contoh matriks:

Matriks $A_{2\times2} = \begin{bmatrix} 1 & 4 \\ 4 & 6 \end{bmatrix}$

Matriks $A_{2\times3} = \begin{bmatrix} 4 & 3 & 9 \\ 8 & 7 & 7 \end{bmatrix}$

Matriks $A_{3\times2} = \begin{bmatrix} 3 & 4 \\ 7 & 9 \\ 5 & 0 \end{bmatrix}$

2. Operator Matriks

Matriks dapat memiliki jumlah baris dan kolom yang positif, termasuk satu. Apabila matriks $A = (a_{ij})$ dan $B = (b_{ij})$ dengan m baris dan n kolom, dijumlahkan atau dikurangkan maka akan didapatkan matriks ketiga yaitu matriks $C = (c_{ij})$ dengan m baris dan n kolom dimana elemen-elemennya didapatkan dengan menjumlahkan atau mengurangkan elemen-elemen matriks A dengan elemen-elemen matriks B yaitu bahwa $c_{ij} = a_{ij} \pm b_{ij}$, untuk semua i dan j, dimana c_{ij} yaitu elemen dari baris ke-i dan kolom ke-j. Jika A adalah suatu matriks dan c adalah suatu skalar, maka hasil kali *(product)* cA adalah matriks yang diperoleh dengan mengalikan masing-masing entri dari A oleh c (Anton, 1987).

Apabila $A_{m\times n} = (a_{ij})$ adalah matriks dengan m baris dan n kolom, $B_{n\times p} = (b_{ij})$ matriks dengan n baris dan p kolom, kemudian dengan perkalian matriks $A \times B = A \cdot B = AB$, maksudnya adalah suatu matriks $C_{m\times p}; (AB = C)$, yang merupakan matriks dengan m baris dan p kolom, dimana elemen C dari baris ke-i kolom ke-j diperoleh dengan formula:

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}$$

$$c_{ij} = \sum_{t=1}^{n} a_{it} b_{tj} \tag{2.8}$$

dimana $i = 1,2,\ldots$,m dan $j = 1,2,\ldots,p$

Jika diperhatikan dengan seksama, agar hasil kali AB dapat dicari, syarat utama yang perlu dipenuhi ialah bahwa jumlah kolom dari matriks A, atau matriks yang pertama harus sama dengan jumlah baris dari matriks B, dalam ilustrasi sebelumnya, masing-masing sebesar n. Selain dari pada itu baris dari matriks $C = AB$ ternyata merupakan baris dari matriks A (sebesar m). Sedangkan kolomnya merupakan kolom matriks B (sebesar p). Jadi di dalam menentukan apakah dua buah matriks bisa dikalikan atau tidak dan sekaligus untuk menentukan jumlah baris dan kolom dari hasil kalinya, kita harus yakin benar bahwa jumlah kolom dari matriks sebelah kiri (matriks A) harus sama dengan jumlah baris dari matriks sebelah kanan (matriks B)

$$A_{m\times n}\, B_{n\times p} = C_{m\times p} \tag{2.9}$$

Di dalam hal ini yaitu apabila jumlah kolom A sama dengan jumlah baris B, maka A dan B dikatakan *conformable* untuk perkalian, ini berarti bahwa bisa dicari hasil kali AB (Gazali, 2005).

Contoh matriks penjumlahan:

Misalkan: $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$

Misalkan: $B = \begin{bmatrix} 1 & 3 & 7 \\ 11 & 13 & 17 \\ 21 & 23 & 29 \end{bmatrix}$

Maka $A + B = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} + \begin{bmatrix} 1 & 3 & 7 \\ 11 & 13 & 17 \\ 21 & 23 & 29 \end{bmatrix}$

Maka $A + B = \begin{bmatrix} 1+1 & 2+3 & 3+7 \\ 4+11 & 5+13 & 6+17 \\ 7+21 & 8+23 & 9+29 \end{bmatrix}$

Maka $A + B = \begin{bmatrix} 2 & 5 & 10 \\ 15 & 18 & 23 \\ 28 & 31 & 38 \end{bmatrix}$

Contoh matriks perkalian:

Misalkan: $A = \begin{bmatrix} 1 & 2 & 3 \\ 8 & 7 & 1 \\ 7 & 3 & 0 \end{bmatrix}$

Maka $3A = 3 \times \begin{bmatrix} 1 & 2 & 3 \\ 8 & 7 & 1 \\ 7 & 3 & 0 \end{bmatrix}$

Maka $3A = \begin{bmatrix} 3 \cdot 1 & 3 \cdot 2 & 3 \cdot 3 \\ 3 \cdot 8 & 3 \cdot 7 & 3 \cdot 1 \\ 3 \cdot 7 & 3 \cdot 3 & 3 \cdot 0 \end{bmatrix}$

Maka $3A = \begin{bmatrix} 3 & 6 & 9 \\ 24 & 21 & 3 \\ 21 & 9 & 0 \end{bmatrix}$

Contoh lainnya:

Misalkan: $A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 0 & 1 \\ 2 & 3 & 1 \end{bmatrix}$

Misalkan: $B = \begin{bmatrix} 1 & 3 & 0 \\ 2 & 3 & 1 \\ 0 & 1 & 2 \end{bmatrix}$

Maka $A \times B = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 0 & 1 \\ 2 & 3 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 3 & 0 \\ 2 & 3 & 1 \\ 0 & 1 & 2 \end{bmatrix}$

$$A \times B = \begin{bmatrix} (1 \cdot 1) + (2 \cdot 2) + (3 \cdot 0) & (1 \cdot 3) + (2 \cdot 3) + (3 \cdot 1) \\ (2 \cdot 1) + (0 \cdot 2) + (1 \cdot 0) & (2 \cdot 3) + (0 \cdot 3) + (1 \cdot 1) \\ (2 \cdot 1) + (3 \cdot 2) + (1 \cdot 0) & (2 \cdot 3) + (3 \cdot 3) + (1 \cdot 1) \end{bmatrix}$$

$$\begin{matrix} (1 \cdot 0) + (2 \cdot 1) + (3 \cdot 2) \\ (2 \cdot 0) + (0 \cdot 1) + (1 \cdot 2) \\ (2 \cdot 0) + (3 \cdot 1) + (1 \cdot 2) \end{matrix} \Bigg]$$

Maka $A + B = \begin{bmatrix} 1+4+0 & 3+6+3 & 0+2+6 \\ 2+0+0 & 6+0+1 & 0+0+2 \\ 2+6+0 & 6+9+1 & 0+3+2 \end{bmatrix}$

$A + B = \begin{bmatrix} 5 & 12 & 8 \\ 2 & 7 & 2 \\ 8 & 15 & 5 \end{bmatrix}$

3. Transpos Matriks

Misalkan matriks M dengan dimensi $r \times c$. Transpos M (dilambangkan M^T) adalah matriks $c \times r$ dimana kolom-kolom dibentuk dari baris-baris M. Dengan kata lain, $M_{ij}^T = M_{ji}$. Ini (membalik) matriks secara diagonal. Biasanya transpos dari matriks A diberi simbol A' (baca A aksen) dan ditulis: $A' = (a'_{ij} = a_{ji})$ (Gazali, 2005).

Berikut contoh transpos matriks:

Misalkan $X = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 6 & 5 & 4 \end{bmatrix}$

Maka $X^T = \begin{bmatrix} 1 & 4 & 7 & 10 \\ 2 & 5 & 8 & 11 \\ 3 & 6 & 9 & 12 \end{bmatrix}$

Atau bisa juga:

$Y = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$

$Y^T = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix}$

Terdapat dua pengamatan yang cukup jelas, tetapi signifikan, mengenai transpos matriks:

1) $(M^T)^T = M$ untuk matriks M dari setiap dimensi. Dengan kata lain, jika kita mentranspos sebuah matriks kemudian mentransposnya lagi, kita mendapatkan matriks aslinya.
2) $D^T = D$ untuk sembarang matriks diagonal D, termasuk matriks identitas I.

4. Matriks Invers

Misalkan A merupakan matriks kuadrat, dan apabila dapat dicari matriks B sehingga $AB = BA = I$, maka matriks A dikatakan *invertible* atau dapat dibalik dan B dinamakan invers (*inverse*) dari matriks A. Jika A dapat dibalik, maka inversnya biasa dinyatakan dalam bentuk A^{-1} (Kusumawati, 2009). Sehingga $AA^{-1} = I$ dan $A^{-1}A = I$

Contoh invers matriks:

Misalkan $X = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$ dan Y adalah invers dari X

$Y\ atau\ X^{-1} = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix}$

Karena $XY = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

dan $YX = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix}\begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

5. Matriks Identitas

Matriks diagonal istimewa adalah matriks identitas (*Identity Matrix*). Matriks identitas itu istimewa karena merupakan elemen identitas perkalian untuk matriks. Matriks identitas berdimensi n, dilambangkan I_n adalah matriks $n \times n$ dengan 1 pada diagonal utamanya dan 0 pada entri diluar

diagonal utamanya. Sehinga jika matriks $A = (a_{ij})$, $i = j = 1,2,\ldots,n$, dan apabila

$$a_{ij} = 1 \text{ untuk } i = j$$

$$a_{ij} = 0 \text{ untuk } i \neq j$$

maka matriks A dikatakan matriks identitas (Supranto, 1984).

Contoh matriks identitas:

$n = 2$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$n = 3$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$n = 4$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

2.4 Kajian Keislaman

Di dalam Al-Qu'ran, terdapat beberapa ayat terkait dalam menyampaikan amanat, diantaranya yaitu:

1. Surat Al Mu'minun ayat 8

وَالَّذِيْنَ هُمْ لِاَمٰنٰتِهِمْ وَعَهْدِهِمْ رَاعُوْنَ

"*Dan orang-orang yang memelihara amanat-amanat (yang dipikulnya) dan janjinya*" (Al Mu'minun: 8)

Menurut tafsir Al-Wasith (2012), ayat ini menggambarkan salah satu sifat orang mukmin, yaitu orang-orang mukmin baik laki-laki maupun perempuan memelihara janji dan amanat. Mereka menunaikan amanat kepada yang berhak dan tidak berkhianat. Bila berjanji dengan orang lain, mereka menempati syarat-syarat perjanjian. Menunaikan amanat dan memenuhi janji adalah sifat orang beriman. Sementara berkhianat dan ingkar adalah sifat orang munafik (Az-zuhaili, 2012).

2. Surat Al Ma'arij ayat 32

وَالَّذِيْنَ هُمْ لِاَمٰنٰتِهِمْ وَعَهْدِهِمْ رَاعُوْنَۚ

"*Dan orang-orang yang memelihara amanat-amanat (yang dipikulnya) dan janjinya*" (Al Ma'arij: 32)

Menurut tafsir Al-Wasith (2012), ayat ini menjelaskan salah satu golongan orang yang dikecualikan dari kekacauan dan goncangan yang menimpa seseorang ketika dalam ketamakan, yaitu orang-orang yang menunaikan amanat yang dipercayakan kepada mereka, menunaikannya kepada pemiliknya, mereka juga memenuhi perjanjian, kesepakatan, akad-akad yang telah disetujui. Mereka tidak melanggar akad jual beli dan apapun syarat yang telah disepakati. Apabila dipercaya mereka tidak berkhianat, apabila mengadakan perjanjian mereka tidak melanggar, apabila berbicara mereka tidak dusta. Ketiganya adalah sifat kaum mukminin, sedangkan kebalikannya adalah sifat kaum munafik.

3. Surat Al Ahzab ayat 72

اِنَّا عَرَضْنَا الْاَمَانَةَ عَلَى السَّمٰوٰتِ وَالْاَرْضِ وَالْجِبَالِ فَاَبَيْنَ اَنْ يَّحْمِلْنَهَا وَاَشْفَقْنَ مِنْهَا وَحَمَلَهَا الْاِنْسَانُۗ اِنَّه كَانَ ظَلُوْمًا جَهُوْلً

"*Sesungguhnya Kami telah mengemukakan amanat kepada langit, bumi dan gunung-gunung, maka semuanya enggan untuk memikul amanat itu dan mereka khawatir akan mengkhianatinya, dan dipikullah amanat itu oleh manusia. Sesungguhnya, manusia itu amat zalim dan amat bodoh"*

Tanggung jawab atas beban-beban taklif jelas sensitif, bahaya, dan berat. Allah SWT menawarkan amanat, maksudnya beban-beban taklif Ilahi secara keseluruhan berupa kewajiban, ketaatan dan larangan ke seluruh penjuru langit dan bumi, semuanya tidak mau memikul tanggung jawab semua itu karena takut, lalu manusia menanggungnya padahal manusia lemah, hanya saja manusia tidak memperkirakan beban itu. Manusia sangat menganiaya diri sendiri, sangat tidak tahu ukuran tanggung jawab yang ia pikul. Manusia yang dimaksud adalah anak cucu Adam seperti yang dikemukakan oleh sekelompok ulama seperti Ibnu Abbas, Dhahhak, dan lainnya. (Az-zuhaili, 2013).

BAB III

PEMBAHASAN

3.1 Proses Enkripsi Pesan Menggunakan Polinomial *Galois Field* dengan Algoritma *Hill Cipher*

Penulis menggunakan pesan “matematika tidak mudah” dalam proses enkripsi menggunakan plinomial *Galois Field* dengan menggunakan Algoritma *Hill Cipher* dimana polinomial yang digunakan yaitu pada *Galois Field* 2^8. Berikut merupakan langkah-langkah yang perlu dilakukan:

3.1.1 Mengonversi Karakter Pesan Teks ke dalam Bentuk Polinomial *Galois Field*

Karakter pada pesan teks dapat diubah ke dalam bentuk polinomial *Galois Field* yaitu dengan cara mengubah karakter pada pesan teks ke dalam bentuk biner. Biner yang dapat digunakan dimana sangat meluas dan sering dijumpai pada kriptografi adalah bilangan biner pada jumlah 8-bit. Biner dengan jumlah 8-bit merupakan biner yang umum digunakan dimana biner ini memiliki sebanyak 256 karakter yang ada. Karaker dan juga biner 8-bit yang ada tertuang pada tabel *ASCII*. Tabel ini memuat daftar semua huruf dalam alfabet romawi dengan tambahan beberapa karakter dan di dalam tabel ini setiap karakter diwakilkan dengan kode dan salah satunya adalah kode biner pada bit 8. Berikut merupakan contoh beberapa karakter dan kode binernya pada tabel *ASCII*:

Tabel 3.1 Kode dan Simbol Biner Tabel *ASCII*

Desimal	Biner	Karakter
⋮	⋮	⋮
97	01100001	a
98	01100010	b
99	01100011	c

Desimal	Biner	Karakter
100	01100100	d
101	01100101	e
102	01100110	f
103	01100111	g
104	01101000	h
⋮	⋮	⋮

Suatu himpunan polinomial *Galois Field* merupakan kombinasi dari polinomial- polinomial dengan koefisiennya adalah tidak lebih dari dua. Polinomial *Galois Field* pada kombinasi yang terkait dengan biner, yaitu menggunakan 2^n dimana pangkat tertingginya adalah $n-1$. Bentuk polinomialnya yaitu $a_0 + a_1x + a_2x^2 + a_3x^3$, Polinomial *Galois Field* dapat dinyatakan dalam bentuk b_0, b_1, b_2, b_3, ... Berikut merupakan anggota polinomial *Galois Field* 2^8:

Tabel 3.2 Polinomial $GF\ 2^8$

No.	**Himpunan Polinomial *Galois Field* 2^8**
1	0
2	1
3	x
4	x^2
5	x^3
6	x^4
7	x^5
8	x^6
9	x^7
10	$x+1$
11	x^2+1
12	x^3+1
13	x^4+1
14	x^5+1
15	x^6+1
16	x^7+1
17	x^2+x
18	x^3+x
19	x^4+x
20	x^5+x

No.	Himpunan Polinomial *Galois Field* 2^8
21	$x^6 + x$
22	$x^7 + x$
⋮	⋮
256	$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

Pada polinomial *Galois Field* sendiri juga dapat diubah ke dalam bentuk biner dimana bentuk pada polinomial menentukan bentuk biner pada polinomial tersebut. Karena biner sendiri sistem penulisannya hanya pada dua angka yaitu 0 dan 1 dimana memiliki dua karakter. Pembahasan polinomial *Galois Field* disini yang digunakan adalah polinomial *Galois Field* yang tertutup pada 2^n. Pangkat tertinggi pada kombinasi polinomial *Galois Field* pada 2^n adalah $n-1$. Contohnya yaitu pada polinomial *Galois Field* 2^2, maka kombinasi yang dimiliki adalah $0,1,x$ dan $x+1$, atau membentuk sebanyak 4 karakter. Karakter pada polinomial *Galois Field* juga memiliki bentuk biner. Berikut merupakan bentuk biner pada polinomial *Galois Field* 2^8:

Tabel 3.3 Konversi Biner 8-bit ke dalam Polinomial *Galois Field* 2^8

No.	Biner 8-bit	Polinomial *Galois Field* 2^8
1	00000000	0
2	00000001	1
3	00000010	x
4	00000100	x^2
5	00001000	x^3
6	00010000	x^4
7	00100000	x^5
8	01000000	x^6
9	10000000	x^7
10	00000011	$x + 1$
11	00000101	$x^2 + 1$
12	00001001	$x^3 + 1$
13	00010001	$x^4 + 1$
14	00100001	$x^5 + 1$
15	01000001	$x^6 + 1$
16	10000001	$x^7 + 1$
17	00000110	$x^2 + x$

No.	Biner 8-bit	Polinomial *Galois Field* 2^8
18	00001010	$x^3 + x$
19	00010010	$x^4 + x$
20	00100010	$x^5 + x$
21	01000010	$x^6 + x$
22	10000010	$x^7 + x$
⋮	⋮	⋮
256	11111111	$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

Berikut merupakan proses enkripsi dengan pesannya yaitu "matematika tidak mudah" pada polinomial 2^8. Langkah pertama yang perlu dilakukan adalah mengkonversi pesan teks menjadi bentuk biner dengan melihat kode pada tabel *ASCII*. Berikut merupakan bentuk biner dari pesan teks yang digunakan:

Tabel 3.4 Konversi Pesan ke dalam Biner 8-bit

No.	Karakter	Biner 8-bit
1	m	01101101
2	a	01100001
3	t	01110100
4	e	01100101
5	m	01101101
6	a	01100001
7	t	01110100
8	i	01101001
9	k	01101011
10	a	01100001
11	*space*	00100000
12	t	01110100
13	i	01101001
14	d	01100100
15	a	01100001
16	k	01101011
17	*space*	00100000
18	m	01101101
19	u	01110101
20	d	01100100
21	a	01100001
22	h	01101000

Selanjutnya adalah mengonversikan karakter pesan dari biner 8-bit pada karakter pesan ke dalam polinomial *Galois Field*

Tabel 3.5 Konversi Karakter Pesan ke dalam Polinomial $GF\ 2^8$

No.	Karakter	Biner 8-bit	Polinomial
1	m	01101101	$x^6 + x^5 + x^3 + x^2 + 1$
2	a	01100001	$x^6 + x^5 + 1$
3	t	01110100	$x^6 + x^5 + x^4 + x^2 + 1$
4	e	01100101	$x^6 + x^5 + x^2 + 1$
5	m	01101101	$x^6 + x^5 + x^3 + x^2 + 1$
6	a	01100001	$x^6 + x^5 + 1$
7	t	01110100	$x^6 + x^5 + x^4 + x^2 + 1$
8	i	01101001	$x^6 + x^5 + x^3 + 1$
9	k	01101011	$x^6 + x^5 + x^3 + x + 1$
10	a	01100001	$x^6 + x^5 + 1$
11	*space*	00100000	x^5
12	t	01110100	$x^6 + x^5 + x^4 + x^2 + 1$
13	i	01101001	$x^6 + x^5 + x^3 + 1$
14	d	01100100	$x^6 + x^5 + x^2 + 1$
15	a	01100001	$x^6 + x^5 + 1$
16	k	01101011	$x^6 + x^5 + x^3 + x + 1$
17	*space*	00100000	x^5
18	m	01101101	$x^6 + x^5 + x^3 + x^2 + 1$
19	u	01110101	$x^6 + x^5 + x^4 + x^2 + 1$
20	d	01100100	$x^6 + x^5 + x^2 + 1$
21	a	01100001	$x^6 + x^5 + 1$
22	h	01101000	$x^6 + x^5 + x^3$

3.1.2 Melakukan Proses Perhitungan pada Polinomial dengan Menggunakan *Hill Cipher*

Dalam melakukan perhitungan diperlukan adanya kunci. Kunci yang dapat digunakan dalam melakukan enkripsi pada pesan adalah berupa polinomial di dalam matriks, karena menggunakan algoritma *Hill Cipher*. Kunci matriks yang dapat digunakan disini adalah matriks persegi dengan ordo genap pada ruang lingkup *GF* 2^8. Ordo matriks genap minimal pada *GF* 2^8 disini adalah 2×2 dan jika diatas itu maka berkelipatan dua. Pada pembahasan ini kunci matriks persegi yang berelemenkan polinomial *GF* 2^8 dengan ordo yang dipakai ordo minimal 2×2 yaitu $\begin{bmatrix} x^3 + 1 & x \\ x^5 & x^3 + 1 \end{bmatrix}$.

Proses penyandian dalam penelian ini menggunakan polinomial *Galois Field* dengan karakter pesan terhubung dengan tabel karakter pada biner 8-bit dalam tabel *ASCII*. Proses selanjutnya adalah melakukan perkalian pada polinomial hasil konversi pesan teks dengan kunci. Algoritma kombinasi yang digunakan dalam penelitian ini adalah menggunakan *Hill Cipher*. *Hill Cipher* sendiri merupakan algoritma dengan operasinya menggunakan matriks. Sehingga dalam penelitian ini operasi yang digunakan adalah matriks dengan elemen di dalamnya berupa polinomial *Galois Field* 2^8. Rumus dari *Hill Cipher* sendiri adalah $K \cdot P \; mod \; 26$, sehingga rumus ini dikombinasikan berdasarkan polinomial yang digunakan maka menjadi $K \cdot P \; mod \; x^8 + x^4 + x^3 + x + 1$. Penggunaan modulo disini bertujuan supaya operasi yang dilakukan tidak lebih kecil atau lebih meluas dari $GF \; 2^8$. Dengan K merupakan kunci dengan bentuk matriks dimana di dalamnya berelemenkan polinomial $GF \; 2^8$.

Kunci yang digunakan dalam melakukan proses enkripsi pada pesan ini adalah berupa matriks dengan elemen didalamnya berupa polinomial $GF \; 2^8$. Kunci yang digunakan dalam pembahasan pada polinomial $GF \; 2^8$ disini adalah $K = \begin{bmatrix} x^3 + 1 & x \\ x^5 & x^3 + 1 \end{bmatrix}$. Rumus algoritma *Hill Cipher* yang telah dikombinasikan dengan menggunakan polinomial GF sehingga menjadi $K \cdot P \; mod \; x^8 + x^4 + x^3 + x + 1$. Maka proses enkripsinya adalah sebagai berikut:

Proses perhitungan enkripsi pesan pada polinomial *GF* 2^8 dengan kunci $K = \begin{bmatrix} x^3 + 1 & x \\ x^5 & x^3 + 1 \end{bmatrix}$:

Karakter "$matematika$"

$$P = \begin{bmatrix} x^6+x^5+x^3+x^2+1 & x^6+x^5+x^4+x^2+1 \\ x^6+x^5+1 & x^6+x^5+x^2+1 \end{bmatrix}$$

$$\begin{matrix} x^6+x^5+x^3+x^2+1 & x^6+x^5+x^4+x^2+1 & x^6+x^5+x^3+x+1 \\ x^6+x^5+1 & x^6+x^5+x^3+1 & x^6+x^5+1 \end{matrix}\Bigg]$$

$$C = K \cdot P \; mod \; x^8+x^4+x^3+x+1$$

$$K \cdot P = \begin{bmatrix} x^3+1 & x \\ x^5 & x^3+1 \end{bmatrix} \times \begin{bmatrix} x^6+x^5+x^3+x^2+1 \\ x^6+x^5+1 \end{bmatrix}$$

$$\begin{matrix} x^6+x^5+x^4+x^2+1 & x^6+x^5+x^3+x^2+1 \\ x^6+x^5+x^2+1 & x^6+x^5+1 \end{matrix}$$

$$\begin{matrix} x^6+x^5+x^4+x^2+1 & x^6+x^5+x^3+x+1 \\ x^6+x^5+x^3+1 & x^6+x^5+1 \end{matrix}\Bigg]$$

$$C = \begin{bmatrix} (x^3+1)(x^6+x^5+x^3+x^2+1)+(x)(x^6+x^5+1) \\ (x^5)(x^6+x^5+x^3+x^2+1)+(x^3+1)(x^6+x^5+1) \end{bmatrix}$$

$$\begin{matrix} (x^3+1)(x^6+x^5+x^4+x^2+1)+(x)(x^6+x^5+x^2+1) \\ (x^5)(x^6+x^5+x^4+x^2+1)+(x^3+1)(x^6+x^5+x^2+1) \end{matrix}$$

$$\begin{matrix} (x^3+1)(x^6+x^5+x^3+x^2+1)+(x)(x^6+x^5+1) \\ (x^5)(x^6+x^5+x^3+x^2+1)+(x^3+1)(x^6+x^5+1) \end{matrix}$$

$$\begin{matrix} (x^3+1)(x^6+x^5+x^4+x^2+1)+(x)(x^6+x^5+x^3+1) \\ (x^5)(x^6+x^5+x^4+x^2+1)+(x^3+1)(x^6+x^5+x^3+1) \end{matrix}$$

$$\begin{matrix} (x^3+1)(x^6+x^5+x^3+x+1)+(x)(x^6+x^5+1) \\ (x^5)(x^6+x^5+x^3+x+1)+(x^3+1)(x^6+x^5+1) \end{matrix}\Bigg] mod \; x^8+x^4+x^3$$

$$+x+1$$

$$C = \begin{bmatrix} (x^9+x^8+2x^6+2x^5+2x^3+x^2+1)+(x^7+x^6+x) \\ (x^{11}+x^{10}+x^8+x^7+x^5)+(x^9+x^8+x^6+x^5+x^3+1) \end{bmatrix}$$

$$\begin{matrix} (x^9+x^8+x^7+x^6+2x^5+x^4+x^3+x^2+1)+(x^7+x^6+x^3+x) \\ (x^{11}+x^{10}+x^9+x^7+x^5)+(x^9+x^8+x^6+2x^5+x^3+x^2+1) \end{matrix}$$

$$\begin{matrix} (x^9+x^8+2x^6+2x^5+2x^3+x^2+1)+(x^7+x^6+x) \\ (x^{11}+x^{10}+x^8+x^7+x^5)+(x^9+x^8+x^6+x^5+x^3+1) \end{matrix}$$

$$\begin{matrix} (x^9+x^8+x^7+x^6+2x^5+x^4+x^3+x^2+1)+(x^7+x^6+x^4+x) \\ (x^{11}+x^{10}+x^9+x^7+x^5)+(x^9+x^8+2x^6+x^5+2x^3+1) \end{matrix}$$

$$\begin{matrix}(x^9+x^8+2x^6+x^5+x^4+2x^3+x+1)+(x^7+x^6+x)\\(x^{11}+x^{10}+x^8+x^6+x^5)+(x^9+x^8+x^6+x^5+x^3+1)\end{matrix}\Big] mod\ x^8+x^4$$

$$+x^3+x+1$$

$$C=\begin{bmatrix}x^9+x^8+x^7+x^6+x^2+x+1\\x^{11}+x^{10}+x^9+x^7+x^6+x^3+1\end{bmatrix}$$

$$\begin{matrix}x^9+x^8+x^4+x^2+x+1\\x^{11}+x^{10}+x^8+x^7+x^6+x^5+x^3+x^2+1\end{matrix}$$

$$\begin{matrix}x^9+x^8+x^7+x^6+x^2+x+1 & x^9+x^8+x^3+x^2+x+1\\x^{11}+x^{10}+x^9+x^7+x^6+x^3+1 & x^{11}+x^{10}+x^8+x^7+1\end{matrix}$$

$$\begin{matrix}x^9+x^8+x^7+x^6+x^5+x^4+1\\x^{11}+x^{10}+x^9+x^3+1\end{matrix}\Big] mod\ x^8+x^4+x^3+x+1$$

$$C=\begin{bmatrix}x^7+x^6+x^5+x^3+x & x^5+x^4+x^3+x & x^7+x^6+x^5+x^3+x\\x^6+x^3+x+1 & x^6+x & x^6+x^3+x+1\end{bmatrix}$$

$$\begin{matrix}x^5+x & x^7+x^6+x^4+x^3+x^2\\x^5+x^3+x^2+x & x^7+x^3+x+1\end{matrix}\Big]$$

Karakter " $tidak$"

$$P=\begin{bmatrix}x^5 & x^6+x^5+x^3+1 & x^6+x^5+1\\x^6+x^5+x^4+x^2+1 & x^6+x^5+x^2+1 & x^6+x^5+x^3+x+1\end{bmatrix}$$

$$C=K\cdot P\ mod\ x^8+x^4+x^3+x+1$$

$$K\cdot P=\begin{bmatrix}x^3+1 & x\\x^5 & x^3+1\end{bmatrix}\times$$

$$\begin{bmatrix}x^5 & x^6+x^5+x^3+1 & x^6+x^5+1\\x^6+x^5+x^4+x^2+1 & x^6+x^5+x^2+1 & x^6+x^5+x^3+x+1\end{bmatrix}$$

$$C=\begin{bmatrix}(x^3+1)(x^5)+(x)(x^6+x^5+x^4+x^2+1)\\(x^5)(x^5)+(x^3+1)(x^6+x^5+x^4+x^2+1)\end{bmatrix}$$

$$\begin{matrix}(x^3+1)(x^6+x^5+x^3+1)+(x)(x^6+x^5+x^2+1)\\(x^5)(x^6+x^5+x^3+1)+(x^3+1)(x^6+x^5+x^2+1)\end{matrix}$$

$$\begin{matrix}(x^3+1)(x^6+x^5+1)+(x)(x^6+x^5+x^3+x+1)\\(x^5)(x^6+x^5+1)+(x^3+1)(x^6+x^5+x^3+x+1)\end{matrix}\Big] mod\ x^8+x^4+x^3$$

$$+x+1$$

$$C = \begin{bmatrix} (x^8 + x^5) + (x^7 + x^6 + x^5 + x^3 + x) \\ (x^{10}) + (x^9 + x^8 + x^7 + x^6 + 2x^5 + x^4 + x^3 + x^2 + 1) \end{bmatrix}$$

$$(x^9 + x^8 + 2x^6 + x^5 + 2x^3 + 1) + (x^7 + x^6 + x^3 + x)$$
$$(x^{11} + x^{10} + x^8 + x^5) + (x^9 + x^8 + x^6 + 2x^5 + x^3 + x^2 + 1)$$

$$(x^9 + x^8 + x^6 + x^5 + x^3 + 1) + (x^7 + x^6 + x^4 + x^2 + x)$$
$$(x^{11} + x^{10} + x^5) + (x^9 + x^8 + 2x^6 + x^5 + x^4 + 2x^3 + x + 1)\Big] mod\ x^8 + x^4$$

$$+ x^3 + x + 1$$

$$C = \begin{bmatrix} x^8 + x^7 + x^6 + x^3 + x \\ x^{10} + x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1 \end{bmatrix}$$

$$x^9 + x^8 + x^7 + x^6 + x^5 + x^3 + x + 1$$
$$x^{11} + x^{10} + x^9 + x^6 + x^5 + x^3 + x^2 + 1$$

$$x^9 + x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$x^7 + 2x^6 + 2x^5 + 2x^4 + 3x^3 + 2x^2 + x\Big] mod\ x^8 + x^4 + x^3 + x + 1$$

$$C = \begin{bmatrix} x^7 + x^6 + x^4 + 1 & x^7 + x^6 + x^2 + x & x^7 + x^4 + x \\ x^7 + x^4 + x^3 + x^2 & x^7 + x^6 + x^5 + x^3 + x^2 + x + 1 & x^7 + x^3 + x \end{bmatrix}$$

Karakter " $mudah$"

$$P = \begin{bmatrix} x^5 & x^6 + x^5 + x^4 + x^2 + 1 & x^6 + x^5 + 1 \\ x^6 + x^5 + x^3 + x^2 + 1 & x^6 + x^5 + x^2 + 1 & x^6 + x^5 + x^3 \end{bmatrix}$$

$$C = K \cdot P\ mod\ x^8 + x^4 + x^3 + x + 1$$

$$K \cdot P = \begin{bmatrix} x & x^9 \\ x^8 & x \end{bmatrix} \times$$

$$\begin{bmatrix} x^5 & x^6 + x^5 + x^4 + x^2 + 1 & x^6 + x^5 + 1 \\ x^6 + x^5 + x^3 + x^2 + 1 & x^6 + x^5 + x^2 + 1 & x^6 + x^5 + x^3 \end{bmatrix}$$

$$C = \begin{bmatrix} (x^3 + 1)(x^5) + (x)(x^6 + x^5 + x^3 + x^2 + 1) \\ (x^5)(x^5) + (x^3 + 1)(x^6 + x^5 + x^3 + x^2 + 1) \end{bmatrix}$$

$$(x^3 + 1)(x^6 + x^5 + x^4 + x^2 + 1) + (x)(x^6 + x^5 + x^2 + 1)$$
$$(x^5)(x^6 + x^5 + x^4 + x^2 + 1) + (x^3 + 1)(x^6 + x^5 + x^2 + 1)$$

$$(x^3 + 1)(x^6 + x^5 + 1) + (x)(x^6 + x^5 + x^3)$$
$$(x^5)(x^6 + x^5 + 1) + (x^3 + 1)(x^6 + x^5 + x^3)\Big] mod\ x^8 + x^4 + x^3 + x + 1$$

$$C = \begin{bmatrix} (x^8 + x^5) + (x^7 + x^6 + x^4 + x^3 + x) \\ (x^{10}) + (x^9 + x^8 + 2x^6 + 2x^5 + 2x^3 + x^2 + 1) \end{bmatrix}$$

$$(x^9 + x^8 + x^7 + x^6 + 2x^5 + x^4 + x^3 + x^2 + 1) + (x^7 + x^6 + x^3 + x)$$
$$(x^{11} + x^{10} + x^9 + x^7 + x^5) + (x^9 + x^8 + x^6 + 2x^5 + x^3 + x^2 + 1)$$

$$\begin{matrix}(x^9 + x^8 + x^6 + x^5 + x^3 + 1) + (x^7 + x^6 + x^4) \\ (x^{11} + x^{10} + x^5) + (x^9 + x^8 + 2x^6 + x^5 + x^3)\end{matrix}\Big] mod\ x^8 + x^4 + x^3 + x + 1$$

$$C = \begin{bmatrix} x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x \\ x^{10} + x^9 + x^8 + x^2 + 1 \end{bmatrix}$$

$$x^9 + x^8 + x^4 + x^2 + x + 1$$
$$x^{11} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^3 + x^2 + 1$$

$$\begin{matrix} x^9 + x^8 + x^7 + x^5 + x^4 + x^3 + 1 \\ x^{11} + x^{10} + x^9 + x^8 + x^3 \end{matrix}\Big] mod\ x^8 + x^4 + x^3 + x + 1$$

$$C = \begin{bmatrix} x^7 + x^6 + x^5 + 1 & x^5 + x^4 + x^3 + x & x^7 + x^4 + x^2 \\ x^6 + x^2 & x^6 + x & x^7 + x^4 + 1 \end{bmatrix}$$

3.1.3 Mengonversi Hasil Perhitungan pada Polinomial *Galois Field* ke dalam Bentuk Karakter

Langkah terakhir yang perlu dilakukan adalah mengonversi hasil perkalian polinomial ke dalam bentuk biner dan menggabungkannya kembali menjadi biner bit-8 dan mengubahnya menjadi karakter berdasarkan kode pada tabel *ASCII*. Berikut merupakan prosesnya:

Tabel 3.6 Konversi Hasil Enkripsi $GF\ 2^8$ Menjadi Karakter

No.	Polinomial	Biner	Karakter
1	$x^7 + x^6 + x^5 + x^3 + x$	11101010	ê
2	$x^6 + x^3 + x + 1$	01001011	K
3	$x^5 + x^4 + x^3 + x$	00111010	:
4	$x^6 + x$	01000010	B
5	$x^7 + x^6 + x^5 + x^3 + x$	11101010	ê
6	$x^6 + x^3 + x + 1$	01001011	K
7	$x^5 + x$	00100010	“
8	$x^5 + x^3 + x^2 + x$	00101110	.
9	$x^7 + x^6 + x^4 + x^3 + x^2$	11011100	Ü
10	$x^7 + x^3 + x + 1$	10001011	<
11	$x^7 + x^6 + x^4 + 1$	11010001	Ñ
12	$x^7 + x^4 + x^3 + x^2$	10011100	œ
13	$x^7 + x^6 + x^2 + x$	11000110	Æ
14	$x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$	11101111	ï

No.	Polinomial	Biner	Karakter
15	$x^7 + x^4 + x$	10010010	
16	$x^7 + x^3 + x$	10001010	Š
17	$x^7 + x^6 + x^5 + 1$	11100001	á
18	$x^6 + x^2$	01000100	D
19	$x^5 + x^4 + x^3 + x$	00111010	:
20	$x^6 + x$	01000010	B
21	$x^7 + x^4 + x^2$	10010100	”
22	$x^7 + x^4 + 1$	10010001	‘

Pesan tersandi yang didapatkan dari proses algoritma *Hill Cipher* pada polinomial *GF* 2^8 dengan kunci $K = \begin{bmatrix} x^3+1 & x \\ x^5 & x^3+1 \end{bmatrix}$, pesan tersandi yang didapatkan adalah “êK:BêK“.Ü<ÑœÆï’ŠáD:B”‘”.

3.2 Proses Dekripsi Pesan Menggunakan Polinomial *Galois Field* dengan Algoritma *Hill Cipher*

Terdapat tiga proses yang sama dalam pembalikan pesan terkunci dengan pesan terkuncinya yaitu “êK:BêK“.Ü<ÑœÆï’ŠáD:B”‘” pada $GF\ 2^8$. Berikut merupakan langkah dan prosesnya di dalamnya:

3.2.1 Mengonversi Karakter Pesan Tersandi ke dalam Bentuk Polinomial *Galois Field*

Sama halnya dengan proses pertama yang perlu dilakukan saat melakukan enkripsi, proses dalam melakukan pembalikan pesan juga sama yaitu yang pertama adalah melakukan konversi pesan tersandi menjadi bentuk polinomial *Galois Field*. Dalam pengkonversi pesan tersandi ini menjadi bentuk biner adalah dengan melihat kode pada tabel *ASCII*. Berikut merupakan bentuk biner dari pesan tersandi atau ciphertext sebelumnya:

Tabel 3.7 Konversi Karakter Ciphertext *GF* 2^8 Menjadi Biner 8-bit

No.	Karakter	Biner 8-bit
1	ê	11101010
2	K	01001011
3	:	00111010
4	B	01000010
5	ê	11101010
6	K	01001011
7	“	00100010
8	.	00101110
9	Ü	11011100
10	<	10001011
11	Ñ	11010001
12	œ	10011100
13	Æ	11000110
14	ï	11101111
15	¸	10010010
16	Š	10001010
17	á	11100001
18	D	01000100
19	:	00111010
20	B	01000010
21	”	10010100
22	‘	10010001

Selanjutnya adalah membagi biner sejumlah bit dari pangkat polinomial kemudian mengkonversi menjadi karakter polinomial *Galois Field* sebagai berikut:

Tabel 3.8 Konversi Biner 8-bit Sesuai Polinomial *GF*

No.	Biner 8-bit	Polinomial
1	11101010	$x^7 + x^6 + x^5 + x^3 + x$
2	01001011	$x^6 + x^3 + x + 1$
3	00111010	$x^5 + x^4 + x^3 + x$
4	01000010	$x^6 + x$
5	11101010	$x^7 + x^6 + x^5 + x^3 + x$
6	01001011	$x^6 + x^3 + x + 1$
7	00100010	$x^5 + x$
8	00101110	$x^5 + x^3 + x^2 + x$
9	11011100	$x^7 + x^6 + x^4 + x^3 + x^2$

No.	Biner 8-bit	Polinomial
10	10001011	$x^7 + x^3 + x + 1$
11	11010001	$x^7 + x^6 + x^4 + 1$
12	10011100	$x^7 + x^4 + x^3 + x^2$
13	11000110	$x^7 + x^6 + x^2 + x$
14	11101111	$x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$
15	10010010	$x^7 + x^4 + x$
16	10001010	$x^7 + x^3 + x$
17	11100001	$x^7 + x^6 + x^5 + 1$
18	01000100	$x^6 + x^2$
19	00111010	$x^5 + x^4 + x^3 + x$
20	01000010	$x^6 + x$
21	10010100	$x^7 + x^4 + x^2$
22	10010001	$x^7 + x^4 + 1$

3.3.2 Melakukan Proses Perhitungan pada Polinomial dengan Menggunakan Algoritma *Hill Cipher*

Proses dalam pembalikan pesan juga membutuhkan adanya kunci pembalik. Kunci pembalik merupakan kunci dekripsi yang merupakan kunci untuk membalikkan pesan yang tersandi menjadi pesan-teks dengan cara menginverskan kuncinya. Karena kunci yang dipakai adalah matriks dengan komponen didalamnya adalah polinomial $GF\ 2^8$ maka kunci pembalik juga merupakan matriks dengan elemennya yaitu $GF\ 2^8$ dimana kunci awal dan kunci pembalik jika dioperasikan maka menghasilkan matriks identitas.

Selanjutnya adalah melakukan operasi perhitungan pada polinomialnya dengan menggunakan algoritma *Hill Cipher*, dari rumus awal *Hill Cipher* adalah $P = K^{-1} \cdot C\ mod\ 26$, setelah dimodifikasi dengan polinomial $GF\ 2^8$ maka menjadi $P = K^{-1} \cdot C\ mod\ x^8 + x^4 + x^3 + x + 1$.

Sebelum melangkah pada proses perhitungan yang perlu dilakukan adalah menentukan invers kuncinya untuk proses pembalikan. Kunci yang digunakan di dalam pembahasan ini adalah berupa matriks dengan ordo 2×2 dan matriks identitas pada matriks ordo 2×2 adalah $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Didalam proses dekripsi, invers dari kunci digunakan untuk mengubah pesan bersandi menjadi pesan asli atau teks-biasa dimana invers dari kunci akan dioperasikan dengan karakter seperti sebelumnya. Pencarian invers dari kunci adalah sebagai berikut:

Kunci pada polinomial *GF* 2^2dengan kunci $K = \begin{bmatrix} x^3+1 & x \\ x^5 & x^3+1 \end{bmatrix}$

$I = K \cdot K^{-1}$

$K^{-1} = \begin{bmatrix} x^3+1 & x \\ x^5 & x^3+1 \end{bmatrix}$

$K \cdot K^{-1} = \begin{bmatrix} x^3+1 & x \\ x^5 & x^3+1 \end{bmatrix} \times \begin{bmatrix} x^3+1 & x \\ x^5 & x^3+1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

Rumus yang akan digunakan untuk mendekripsikan pesan berkode yang telah diperoleh dari pembahasan diatas, menjadi pesan asli adalah $(K)^{-1} \cdot C \ mod \ x^8 + x^4 + x^3 + x + 1$. Sehingga proses dekripsinya adalah sebagai berikut:

Berikut proses perhitungan dekripsi pesan pada polinomial *GF* 2^8 dengan kunci invers $K^{-1} = \begin{bmatrix} x^3+1 & x \\ x^5 & x^3+1 \end{bmatrix}$:

Karakter “êK:BêK“.Ü<”

$$C = \begin{bmatrix} x^7+x^6+x^5+x^3+x & x^5+x^4+x^3+x & x^7+x^6+x^5+x^3+x \\ x^6+x^3+x+1 & x^6+x & x^6+x^3+x+1 \\ x^5+x & x^7+x^6+x^4+x^3+x^2 \\ x^5+x^3+x^2+x & x^7+x^3+x+1 \end{bmatrix}$$

$P = K^{-1} \cdot C \ mod \ x^8 + x^4 + x^3 + x + 1$

$$K^{-1} \cdot C = \begin{bmatrix} x^3+1 & x \\ x^5 & x^3+1 \end{bmatrix} \times$$

$$\begin{bmatrix} x^7+x^6+x^5+x^3+x & x^5+x^4+x^3+x & x^7+x^6+x^5+x^3+x \\ x^6+x^3+x+1 & x^6+x & x^6+x^3+x+1 \end{bmatrix}$$

$$\begin{matrix} x^5+x & x^7+x^6+x^4+x^3+x^2 \\ x^5+x^3+x^2+x & x^7+x^3+x+1 \end{matrix}\Bigg]$$

$$P = \begin{bmatrix} (x^3+1)(x^7+x^6+x^5+x^3+x)+(x)(x^6+x^3+x+1) \\ (x^5)(x^7+x^6+x^5+x^3+x)+(x^3+1)(x^6+x^3+x+1) \end{bmatrix}$$

$$(x^3+1)(x^5+x^4+x^3+x)+(x)(x^6+x)$$
$$(x^5)(x^5+x^4+x^3+x)+(x^3+1)(x^6+x)$$

$$(x^3+1)(x^7+x^6+x^5+x^3+x)+(x)(x^6+x^3+x+1)$$
$$(x^5)(x^7+x^6+x^5+x^3+x)+(x^3+1)(x^6+x^3+x+1)$$

$$(x^3+1)(x^5+x)+(x)(x^5+x^3+x^2+x)$$
$$(x^5)(x^5+x)+(x^3+1)(x^5+x^3+x^2+x)$$

$$\begin{matrix} (x^3+1)(x^7+x^6+x^4+x^3+x^2)+(x)(x^7+x^3+x+1) \\ (x^5)(x^7+x^6+x^4+x^3+x^2)+(x^3+1)(x^7+x^3+x+1) \end{matrix}\Bigg] mod\ x^8+x^4$$

$$+x^3+x+1$$

$$P = \begin{bmatrix} (x^{10}+x^9+x^8+x^7+2x^6+x^5+x^4+x^3+x)+(x^7+x^4+x^2+x) \\ (x^{12}+x^{11}+x^{10}+x^8+x^6)+(x^9+2x^6+x^4+2x^3+x+1) \end{bmatrix}$$

$$(x^8+x^7+x^6+x^5+2x^4+x^3+x)+(x^7+x^2)$$
$$(x^{10}+x^9+x^8+x^6)+(x^9+x^6+x^4+x)$$

$$(x^{10}+x^9+x^8+x^7+2x^6+x^5+x^4+x^3+x)+(x^7+x^4+x^2+x)$$
$$(x^{12}+x^{11}+x^{10}+x^8+x^6)+(x^9+2x^6+x^4+2x^3+x+1)$$

$$(x^8+x^5+x^4+x)+(x^6+x^4+x^3+x^2)$$
$$(x^{10}+x^6)+(x^8+x^6+2x^5+x^4+x^3+x^2+x)$$

$$\begin{matrix} (x^{10}+x^9+2x^7+2x^6+x^5+x^4+x^3+x^2)+(x^8+x^4+x^2+x) \\ (x^{12}+x^{11}+x^9+x^8+x^7)+(x^{10}+x^7+x^6+x^4+2x^3+x+1) \end{matrix}\Bigg] mod\ x^8$$

$$+x^4+x^3+x+1$$

$$P = \begin{bmatrix} x^{10}+x^9+x^8+x^5+x^3+x^2 \\ x^{12}+x^{11}+x^{10}+x^9+x^8+x^6+x^4+x+1 \end{bmatrix}$$

$$x^8 + x^6 + x^5 + x^3 + x^2 + x$$
$$x^{10} + x^8 + x^4 + x$$

$$x^{10} + x^9 + x^8 + x^5 + x^3 + x^2$$
$$x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x + 1$$

$$x^8 + x^6 + x^5 + x^3 + x^2 + x$$
$$x^{10} + x^8 + x^4 + x^3 + x^2 + x$$

$$\begin{matrix} x^{10} + x^9 + x^8 + x^5 + x^3 + x \\ x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x + 1 \end{matrix} \Big] mod\ x^8 + x^4 + x^3 + x + 1$$

$$P = \begin{bmatrix} x^6 + x^5 + x^3 + x^2 + 1 & x^6 + x^5 + x^4 + x^2 + 1 \\ x^6 + x^5 + 1 & x^6 + x^5 + x^2 + 1 \end{bmatrix}$$

$$\begin{matrix} x^6 + x^5 + x^3 + x^2 + 1 & x^6 + x^5 + x^4 + x^2 + 1 \\ x^6 + x^5 + 1 & x^6 + x^5 + x^3 + 1 \end{matrix}$$

$$\begin{matrix} x^6 + x^5 + x^3 + x + 1 \Big] \\ x^6 + x^5 + 1 \end{matrix}$$

Karakter “ÑœÆï’Š”

$$C = \begin{bmatrix} x^7 + x^6 + x^4 + 1 & x^7 + x^6 + x^2 + x & x^7 + x^4 + x \\ x^7 + x^4 + x^3 + x^2 & x^7 + x^6 + x^5 + x^3 + x^2 + x + 1 & x^7 + x^3 + x \end{bmatrix}$$

$$P = K^{-1} \cdot C\ mod\ x^8 + x^4 + x^3 + x + 1$$

$$K^{-1} \cdot C$$

$$= \begin{bmatrix} x^3 + 1 & x \\ x^5 & x^3 + 1 \end{bmatrix}$$

$$\times \begin{bmatrix} x^7 + x^6 + x^4 + 1 & x^7 + x^6 + x^2 + x & x^7 + x^4 + x \\ x^7 + x^4 + x^3 + x^2 & x^7 + x^6 + x^5 + x^3 + x^2 + x + 1 & x^7 + x^3 + x \end{bmatrix}$$

$$P = \begin{bmatrix} (x^3 + 1)(x^7 + x^6 + x^4 + 1) + (x)(x^7 + x^4 + x^3 + x^2) \\ (x^5)(x^7 + x^6 + x^4 + 1) + (x^3 + 1)(x^7 + x^4 + x^3 + x^2) \end{bmatrix}$$

$$\begin{matrix} (x^3 + 1)(x^7 + x^6 + x^2 + x) + (x)(x^7 + x^6 + x^5 + x^3 + x^2 + x + 1) \\ (x^5)(x^7 + x^6 + x^2 + x) + (x^3 + 1)(x^7 + x^6 + x^5 + x^3 + x^2 + x + 1) \end{matrix}$$

$$\begin{matrix} (x^3 + 1)(x^7 + x^4 + x) + (x)(x^7 + x^3 + x) \\ (x^5)(x^7 + x^4 + x) + (x^3 + 1)(x^7 + x^3 + x) \end{matrix} \Big] mod\ x^8 + x^4 + x^3 + x + 1$$

$$P = \begin{bmatrix} (x^{10} + x^9 + 2x^7 + x^6 + x^4 + x^3 + 1) + (x^8 + x^5 + x^4 + x^3) \\ (x^{12} + x^{11} + x^9 + x^5) + (x^{10} + 2x^7 + x^6 + x^5 + x^4 + x^3 + x^2) \end{bmatrix}$$

$$(x^{10}+x^9+x^7+x^6+x^5+x^4+x^2+x)$$
$$(x^{12}+x^{11}+x^7+x^6)$$

$$+(x^8+x^7+x^6+x^4+x^3+x^2+x)$$
$$+(x^{10}+x^9+x^8+x^7+2x^6+2x^5+x^4+2x^3+x^2+x+1)$$

$$\begin{matrix}(x^{10}+2x^7+2x^4+x)+(x^8+x^4+x^2)\\(x^{12}+x^9+x^6)+(x^{10}+x^7+x^6+x^4+x^3+x)\end{matrix}\Big] mod\ x^8+x^4+x^3+x$$

$$+1$$

$$P=\begin{bmatrix}x^{10}+x^9+x^8+x^6+x^5+1\\x^{12}+x^{11}+x^{10}+x^9+x^6+x^4+x^3+x^2\end{bmatrix}$$

$$x^{10}+x^9+x^8+x^5+x^3$$
$$x^{12}+x^{11}+x^{10}+x^9+x^8+x^6+x^4+x^2+x+1$$

$$\begin{matrix}x^{10}+x^8+x^4+x^2+x\\x^{12}+x^{10}+x^9+x^7+x^4+x^3+x\end{matrix}\Big] mod\ x^8+x^4+x^3+x+1$$

$$P=\begin{bmatrix}x^5 & x^6+x^5+x^3+1 & x^6+x^5+1\\x^6+x^5+x^4+x^2+1 & x^6+x^5+x^2+1 & x^6+x^5+x^3+x+1\end{bmatrix}$$

Karakter “áD:B”“”

$$C=\begin{bmatrix}x^7+x^6+x^5+1 & x^5+x^4+x^3+x & x^7+x^4+x^2\\x^6+x^2 & x^6+x & x^7+x^4+1\end{bmatrix}$$

$$P=K^{-1}\cdot C\ mod\ x^8+x^4+x^3+x+1$$

$$K^{-1}\cdot C=\begin{bmatrix}x^3+1 & x\\x^5 & x^3+1\end{bmatrix}\times$$

$$\begin{bmatrix}x^7+x^6+x^5+1 & x^5+x^4+x^3+x & x^7+x^4+x^2\\x^6+x^2 & x^6+x & x^7+x^4+1\end{bmatrix}$$

$$P=\begin{bmatrix}(x^3+1)(x^7+x^6+x^5+1)+(x)(x^6+x^2)\\(x^5)(x^7+x^6+x^5+1)+(x^3+1)(x^6+x^2)\end{bmatrix}$$

$$(x^3+1)(x^5+x^4+x^3)+(x)(x^6+x)$$
$$(x^5)(x^5+x^4+x^3)+(x^3+1)(x^6+x)$$

$$\begin{matrix}(x^3+1)(x^7+x^4+x^2)+(x)(x^7+x^4+1)\\(x^5)(x^7+x^4+x^2)+(x^3+1)(x^7+x^4+1)\end{matrix}\Big] mod\ x^8+x^4+x^3+x+1$$

$$P=\begin{bmatrix}(x^{10}+x^9+x^8+x^7+x^6+x^5+x^3+1)+(x^7+x^3)\\(x^{12}+x^{11}+x^{10}+x^5)+(x^9+x^6+x^5+x^2)\end{bmatrix}$$

$$(x^8 + x^7 + x^6 + x^5 + 2x^4 + x^3 + x) + (x^7 + x^2)$$
$$(x^{10} + x^9 + x^8 + x^6) + (x^9 + x^6 + x^4 + x)$$

$$\begin{matrix}(x^{10} + 2x^7 + x^5 + x^4 + x^2) + (x^8 + x^5 + x) \\ (x^{12} + x^9 + x^7) + (x^{10} + 2x^7 + x^4 + x^3 + 1)\end{matrix}\Big] mod\ x^8 + x^4 + x^3 + x + 1$$

$$P = \begin{bmatrix} x^{10} + x^9 + x^8 + x^6 + x^5 + 1 & x^8 + x^6 + x^5 + x^3 + x^2 + x \\ x^{12} + x^{11} + x^{10} + x^9 + x^6 + x^2 & x^{10} + x^8 + x^4 + x \end{bmatrix}$$

$$\begin{matrix} x^{10} + x^8 + x^4 + x^2 + x \\ x^{12} + x^{10} + x^9 + x^7 + x^4 + x^3 + 1 \end{matrix}\Big] mod\ x^8 + x^4 + x^3 + x + 1$$

$$P = \begin{bmatrix} x^5 & x^6 + x^5 + x^4 + x^2 + 1 & x^6 + x^5 + 1 \\ x^6 + x^5 + x^3 + x^2 + 1 & x^6 + x^5 + x^2 + 1 & x^6 + x^5 + x^3 \end{bmatrix}$$

3.2.3 Mengonversi Hasil Perhitungan pada Polinomial *Galois Field* ke dalam Bentuk Karakter

Langkah yang dilakukan untuk membalikkan pesan tersandi adalah mengonversi hasil perkalian polinomial ke dalam bentuk biner 8-bit menjadi bentuk simbol seperti tabel berikut:

Tabel 3.9 Konversi Hasil Dekripsi Polinomial *GF* 2^8 Menjadi Karakter

No.	Polinomial	Biner	Karakter
1	$x^6 + x^5 + x^3 + x^2 + 1$	01101101	m
2	$x^6 + x^5 + 1$	01100001	a
3	$x^6 + x^5 + x^4 + x^2 + 1$	01110100	t
4	$x^6 + x^5 + x^2 + 1$	01100101	e
5	$x^6 + x^5 + x^3 + x^2 + 1$	01101101	m
6	$x^6 + x^5 + 1$	01100001	a
7	$x^6 + x^5 + x^4 + x^2 + 1$	01110100	t
8	$x^6 + x^5 + x^3 + 1$	01101001	i
9	$x^6 + x^5 + x^3 + x + 1$	00110001	k
10	$x^6 + x^5 + 1$	01100001	a
11	x^5	00100000	*space*
12	$x^6 + x^5 + x^4 + x^2 + 1$	01110100	t
13	$x^6 + x^5 + x^3 + 1$	01101001	i
14	$x^6 + x^5 + x^2 + 1$	01100100	d
15	$x^6 + x^5 + 1$	01100001	a
16	$x^6 + x^5 + x^3 + x + 1$	01101011	k
17	x^5	00100000	*space*
18	$x^6 + x^5 + x^3 + x^2 + 1$	01101101	m
19	$x^6 + x^5 + x^4 + x^2 + 1$	01110101	u

No.	Polinomial	Biner	Karakter
20	$x^6 + x^5 + x^2 + 1$	01100100	d
21	$x^6 + x^5 + 1$	01100001	a
22	$x^6 + x^5 + x^3$	01101000	h

Sehingga semua perhitungan menunjukkan pembalikan pesan dari tersandi menjadi pesan aslinya yaitu “matematika tidak mudah”.

3.3 Kajian Agama

Konsep keamanan pesan sama halnya dengan menjaga amanat dan tertuang pada beberapa surat yaitu pada surat Al Mu’minun ayat 8, Al Ma’arij ayat 32 dan Al Ahzab ayat 72. Pesan haruslah terjaga keamanannya dari pihak yang tidak berhak untuk mendapatkannya. Pesan yang terjaga keamannnya merupakan salah satu amanat yang juga harus dijaga oleh yang memegang amanat maupun orang yang menerimanya supaya tidak disalah gunakan oleh yang bersangkutan.

Hudzaifah Radhiyallahu’anhu berkata: “Rasulullah SAW telah menceritakan kepada kami dua hadits, aku telah melihat yang satu dan sedang menanti yang kedua. Rasulullah SAW menceritakan bahwa amanat (iman) pada mulanya turun dalam lubuk hati manusia, lalu mereka mengerti dari Al-Qur'an dan mengetahui dari Sunnatur Rasul. Kemudian menceritakan tercabutnya amanat (iman), ketika orang sedang tidur, tercabutlah amanat dari hatinya, sehingga tinggal bekasnya seperti bintik yang hampir hilang, kemudian tidur lagi, maka tercabut sehingga tinggal bekasnya seperti kapal (kulit yang mengeras karena sering bergesekan dengan benda), bagaikan bara api yang engkau injak di bawah telapak kaki, sehingga mengembang (membengkak) maka tampaknya membesar tetapi tidak ada apa-apanya, maka pada esok harinya orang-orang berjual beli, dan sudah tidak terdapat orang yang amanat, dapat dipercaya, sehingga mungkin disebut-sebut ada

dari suku Bani Fulan seorang yang amanat (dapat dipercaya), sehingga dipuji-puji: Alangkah pandainya, alangkah ramahnya, alangkah baiknya, padahal di dalam hatinya tidak ada iman seberat zarrah sekali pun. (Dikeluarkan oleh Bukhari pada Kitab ke-81, Kitab Kelembutan bab ke-35, bab terangkatnya amanat) Hudzaifah berkata: “Dan aku pernah berada dalam suatu masa, tidak usah memilih orang dalam jual beli, jika bertepatan seorang muslim, maka ia baik karena takut hukum agamanya, dan jika seorang Kristen (atau kafir) maka ia takut dari hukuman pemerintahnya, adapun sekarang ini, maka aku tidak bisa mempercayai kecuali satu dua orang saja, yaitu fulan dan fulan” (Baqi, 2017).

Amanat bukan hal mudah yang bisa kita lakukan tetapi merupakan perkara yang sulit terhadap orang-orang yang tersadar bahwa dirinya hanyalah makhluk yang harus taat terhadap kholiknya. Ketika Ma'qil bin Yasar Radhiyallahu’anhu sakit, dia dijenguk oleh gubernur Ubaidillah bin Ziyad, maka Ma’qil berkata: “Aku akan menyampaikan kepadamu suatu hadits yang telah aku dengar dari Rasulullah SAW yang bersabda: ‘Siapa yang diamanati oleh Allah untuk memimpin rakyat, lalu ia tidak memimpinnya dengan tuntunan yang baik, maka ia tidak akan dapat merasakan bau surga’” (Baqi, 2017). Dari hadis ini terlihat bahwa menjalankan amanat tidaklah mudah sehingga Allah memberikan jaminan negara kepada siapa yang tidak menjalankan amanat dengan baik, oleh karena itu pentingnya untuk menjaga ucapan dan perbuatan yang sudah diamanatkan untuk kita jaga karena konsekuensinya sangat besar.

Penyandian pesan juga tidak lepas dari yang namanya amanat. Ketika pesan yang sangat penting tidak tersandi dengan baik dan dapat diretas oleh pihak ketiga maka akan membahayakan pemilik informasi begitupun dengan amanat jika tidak

dijaga dan dijalankan dengan baik maka akan berakibat buruk terhadap orang yang bertanggung jawab terhadap amanat tersebut dan akan mendapatkan balasan dan akibat yang buruk terhadap manusia sendiri maupun terhadap sang kholik.

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan pembahasan yang telah dilakukan maka didapatkan kesimpulan sebagai berikut:

1. Pada pesan "matematika tidak mudah" dalam pembahasan ini yaitu pada $GF\ 2^8$ dengan kunci matriks yang digunakan adalah matriks ordo 2×2. Berdasarkan modifikasi algoritma *Hill Cipher* maka rumus pada operasi perhitungannya menjadi $K \cdot P\ mod\ x^8 + x^4 + x^3 + x + 1$. Hasil pesan terkunci dari proses perhitungan pada $GF\ 2^8$ dengan kunci yang digunakan yaitu $K = \begin{bmatrix} x^3 + 1 & x \\ x^5 & x^3 + 1 \end{bmatrix}$ adalah "êK:BêK".Ü<ÑœÆï'ŠáD:B"'".
2. Pesan tersandi "êK:BêK".Ü<ÑœÆï'ŠáD:B"'" pada $GF\ 2^8$ didapatkan kunci pembaliknya adalah $K^{-1} = \begin{bmatrix} x^3 + 1 & x \\ x^5 & x^3 + 1 \end{bmatrix}$ dimana secara tidak sengaja ternyata sama dengan kunci enkripsinya. Pesan tersandi ini dilakukan proses pembalikan dengan dikonversi ke dalam bentuk biner kemudian dioperasikan hasil dari polinomial $GF\ 2^8$ yang didapatkan. Berdasarkan modifikasi algoritma *Hill Cipher* maka rumus perhitungannya menjadi $K^{-1} \cdot C\ mod\ x^8 + x^4 + x^3 + x + 1$. Pesan aslinya yaitu "matematika tidak mudah" akan didapatkan ketika perhitungan selesai dilakukan dan telah dikonversikan kembali ke dalam bentuk karakter.

4.2 Saran

Berdasarkan penelitian yang telah dilakukan, maka berikut merupakan saran peneliti untuk dapat dilakukan penelitian lainnya:

1. Membuat dalam bentuk pemrogaraman berdasarkan yang telah dibahas maupun dengan menggunakan algoritma lainnya.
2. Membandingkan kunci yang digunakan dengan algoritma lain yang mana lebih efektif untuk digunakan dengan menggunakan polinomial *Galois Field*.
3. Menggunakan polinomial dengan variabel dan koefisien yang lebih tinggi.

DAFTAR PUSTAKA

Al-Qur'an. 2007. *Al-Qur'an dan Terjemahnya*. Bogor: Yayasan Penyelenggara Penerjemah/Penafsir Terjemah oleh Lajnah Penafsir Mushaf Al-Qur'an Departemen Agama Republik Indonesia.

Anton, Howard. 1987. *Aljabar Linier Elementer (Edisi Kelima)*. Jakarta: Erlangga.

Anton, Howard dan Rorres Chris. 1998. *Penerapan Aljabar Linear*. Jakarta: Erlangga.

Ariyus, Dony. 2012. *Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi. Yogyakarta*: Penerbit Andi.

Az-zuhaili, Wahbah. 2012. *Tafsir Al-Wasith (Al-Faatihah-At-Taubah)*. Jakarta: Gema Insani.

Az-zuhaili, Wahbah. 2012. *Tafsir Al-Wasith (Yunus-An-Naml)*. Jakarta: Gema Insani.

Az-zuhaili, Wahbah. 2013. *Tafsir Al-Wasith (Al-Qashash-An-Naas)*. Jakarta: Gema Insani.

Baqi, Muhammad Fu'ad Abdul. 2017. *Shahih Bukhari Muslim (Al-Lu'lu' Wal Marjan)*. Jakarta: Kompas Gramedia.

Effendy, Onong Uchjana. 1993. *Ilmu, Teori dan Filsafat Komunikasi*. Bandung: PT Citra Aditya Bakti.

Gazali, Wikaria. 2005. *Matriks & Transformasi Linear*. Yogyakarta: Graha Ilmu.

Hadley, William George. 1992. *Aljabar Linear*. Jakarta: Erlangga.

Haryanto, T. A. dan Sucipto A. T. L. 2013. *Sistem Komputer*. Jakarta: Politeknik Negeri Media Kreatif.

Hoffstein, J., Pipher, J., & Silverman, J.H. 2012. *An Introduction to Mathematical Cryptography (Second Edition)*. London: Sage Publications

Irawan, A. S. Y., Heryana, N., & Solehudin, A. 2020. Combination of Hill Cipher Algorithm and Caesar Cipher Algorithm for Exam Data Security. *Buana Information Technology and Computer Sciences (BIT and CS),* 1(2): 42-45.

Kurniawan, Yusuf. 2004. *Kriptografi Keamanan Internet & Jaringan Komunikasi*. Yogyakarta: Graha Ilmu.

Kromodimoeljo, Sentot. 2009. *Teori dan Aplikasi Kriptografi*. 2009. Jakarta: Andi Publisher

Kusumawati, Ririen. 2009. *Aljabar Linear & Matriks*. Malang: UIN-Malang Press.

Mukhtar, Harun. 2018. *Kriptografi untuk Keamanan Data*. Yogyakarta: Deepublish

Munir, Rinaldi. 2008. *Matematika Diskrit*. Bandung: Informatika.

Rakhmat, Effendi. 1993. *Public Relations Dalam Teori dan Prakter*. Jakarta: Gramedia Pustaka Umum.

Sadikin, Rifki. 2012. *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: CV Andi Offset.

Siahaan, S. M. 1991. *Komunikasi Pemahaman dan Penerapan*. Jakarta: BPK Gunung Mulia.

Sihombing, Kennedy Samuel. 2014. *Analisis Fraud Diamond Dalam Mendeteksi Financial Statement Fraud: Study Empiris Pada Peusahaan Manufaktur yang Terdaftar di BEI*. Diponegoro: Fakultas Ekonomi dan Bisnis, Universitas Diponegoro.

Supranto, J. 2003. *Pengantar Matrix (Edisi Revisi)*. Jakarta: Rineka Cipta.

Viswanath, M. K., & Kumar, M. R. 2015. A Public Key Cryptosystem Using Hill's Cipher. *Journal of Discrete Mathematical Science and Cryptography*, 18(1): 129-138.

Whirfield, Diffie., & Martin, E. Hellman. (1976). *New Direction in Cryptography. California*: Stanford EE.

LAMPIRAN

Tabel ASCII

Desimal	Biner	Karakter
0	00000000	NUL
1	00000001	SOH
2	00000010	STX
3	00000011	ETX
4	00000100	EOT
5	00000101	ENQ
6	00000110	ACK
7	00000111	BEL
8	00001000	BS
9	00001001	HT
10	00001010	LF
11	00001011	VT
12	00001100	FF
13	00001101	CR
14	00001110	SO
15	00001111	SI
16	00010000	DLE
17	00010001	DC1
18	00010010	DC2
19	00010011	DC3
20	00010100	DC4
21	00010101	NAK
22	00010110	SYN
23	00010111	ETB
24	00011000	CAN
25	00011001	EM
26	00011010	SUB
27	00011011	ESC
28	00011100	FS
29	00011101	GS
30	00011110	RS
31	00011111	US
32	00100000	Space
33	00100001	!
34	00100010	“
35	00100011	#
36	00100100	$
37	00100101	%
38	00100110	&

Desimal	Biner	Karakter
39	00100111	‘
40	00101000	(
41	00101001	)
42	00101010	*
43	00101011	+
44	00101100	,
45	00101101	-
46	00101110	.
47	00101111	/
48	00110000	0
49	00110001	1
50	00110010	2
51	00110011	3
52	00110100	4
53	00110101	5
54	00110110	6
55	00110111	7
56	00111000	8
57	00111001	9
58	00111010	:
59	00111011	;
60	00111100	<
61	00111101	=
62	00111110	>
63	00111111	?
64	01000000	@
65	01000001	A
66	01000010	B
67	01000011	C
68	01000100	D
69	01000101	E
70	01000110	F
71	01000111	G
72	01001000	H
73	01001001	I
74	01001010	J
75	01001011	K
76	01001100	L
77	01001101	M

Desimal	Biner	Karakter
78	01001110	N
79	01001111	O
80	01010000	P
81	01010001	Q
82	01010010	R
83	01010011	S
84	01010100	T
85	01010101	U
86	01010110	V
87	01010111	W
88	01011000	X
89	01011001	Y
90	01011010	Z
91	01011011	[
92	01011100	\
93	01011101	]
94	01011110	^
95	01011111	_
96	01100000	`
97	01100001	a
98	01100010	b
99	01100011	c
100	01100100	d
101	01100101	e
102	01100110	f
103	01100111	g
104	01101000	h
105	01101001	i
106	01101010	j
107	01101011	k
108	01101100	l
109	01101101	m
110	01101110	n
111	01101111	o
112	01110000	p
113	01110001	q
114	01110010	r
115	01110011	s
116	01110100	t
117	01110101	u
118	01110110	v
119	01110111	w
120	01111000	x
121	01111001	y
122	01111010	z

Desimal	Biner	Karakter
123	01111011	{
124	01111100	|
125	01111101	}
126	01111110	~
127	01111111	DEL
128	10000000	€
129	10000001	ʊ
130	10000010	‚
131	10000011	*ƒ*
132	10000100	„
133	10000101	…
134	10000110	ł
135	10000111	ǂ
136	10001000	ˆ
137	10001001	‰
138	10001010	Š
139	10001011	<
140	10001100	Œ
141	10001101	□
142	10001110	Ž
143	10001111	m̶
144	10010000	n̶
145	10010001	‘
146	10010010	’
147	10010011	‟
148	10010100	”
149	10010101	•
150	10010110	-
151	10010111	_
152	10011000	˜
153	10011001	™
154	10011010	š
155	10011011	>
156	10011100	œ
157	10011101	Ꝑ
158	10011110	ž
159	10011111	Ÿ
160	10100000	Ꝼ
161	10100001	¡
162	10100010	¢
163	10100011	£
164	10100100	¤
165	10100101	¥
166	10100110	¦
167	10100111	§

Desimal	Biner	Karakter
168	10101000	¨
169	10101001	©
170	10101010	ª
171	10101011	«
172	10101100	¬
173	10101101	ƍ
174	10101110	®
175	10101111	¯
176	10110000	°
177	10110001	±
178	10110010	²
179	10110011	³
180	10110100	´
181	10110101	µ
182	10110110	¶
183	10110111	·
184	10111000	¸
185	10111001	¹
186	10111010	º
187	10111011	»
188	10111100	¼
189	10111101	½
190	10111110	¾
191	10111111	¿
192	11000000	À
193	11000001	Á
194	11000010	Â
195	11000011	Ã
196	11000100	Ä
197	11000101	Å
198	11000110	Æ
199	11000111	Ç
200	11001000	È
201	11001001	É
202	11001010	Ê
203	11001011	Ë
204	11001100	Ì
205	11001101	Í
206	11001110	Î
207	11001111	Ï
208	11010000	Đ
209	11010001	Ñ
210	11010010	Ò
211	11010011	Ó
212	11010100	Ô

Desimal	Biner	Karakter
213	11010101	Õ
214	11010110	Ö
215	11010111	×
216	11011000	Ø
217	11011001	Ù
218	11011010	Ú
219	11011011	Û
220	11011100	Ü
221	11011101	Ý
222	11011110	Þ
223	11011111	ß
224	11100000	à
225	11100001	á
226	11100010	â
227	11100011	ã
228	11100100	ä
229	11100101	å
230	11100110	æ
231	11100111	ç
232	11101000	è
233	11101001	é
234	11101010	ê
235	11101011	ë
236	11101100	ì
237	11101101	í
238	11101110	î
239	11101111	ï
240	11110000	ð
241	11110001	ñ
242	11110010	ò
243	11110011	ó
244	11110100	ô
245	11110101	õ
246	11110110	ö
247	11110111	÷
248	11111000	ø
249	11111001	ù
250	11111010	ú
251	11111011	û
252	11111100	ü
253	11111101	ý
254	11111110	þ
255	11111111	ÿ

RIWAYAT HIDUP

Amelia Vega, lahir di Banyuwangi pada tanggal 30 Oktober 1998. Anak pertama dari Bapak Sumaryono dan Ibu Supiyati dan memiliki adik laki-laki bernama Rofid Zainnazar. Penulis dibesarkan dilingkungan yang sehat dan baik di daerah Desa Setail Kecamatan Genteng Kabupaten Banyuwangi. Pernah mengenyam Pendidikan formal dimulai dari TK Dahlia, melanjutkan Pendidikan dasar di SD Muhammadiyah 6 Genteng, melanjutkan ke SMP Negeri 1 Genteng, dilanjutkan dengan Pendidikan di SMA Negeri 2 Genteng pada jurusan Matematika dan Ilmu Pengetahuan Alam dan terakhir menempuh Pendidikan Strata 1 di Universitas Islam Negeri Maulana Malik Ibrahim Malang pada Program Studi Matematika Fakultas Sains dan Teknologi. Disamping itu, penulis juga mengenyam Pendidikan non-formal dimulai pada semester 3 masa perkuliahan di Pondok Pesantren Mahasiswi Al-azkiya' Malang.

KEMENTRIAN RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No. 50 Dinoyo Malang Telp/Fax.(0341)558933

BUKTI KONSULTASI SKRIPSI

Nama : **Amelia Vega**
NIM : 17610056
Fakultas/ Program Studi : Sains dan Teknologi/ Matematika
Judul Skripsi : **Enkripsi dan Dekripsi Pesan Menggunakan Polinomial *Galois Field* dengan Algoritma *Hill Cipher***
Pembimbing I : Dr. H. Imam Sujarwo, M.Pd
Pembimbing II : **Muhammad Khudzaifah, M.Si**

No.	Tanggal	Hal	Tanda Tangan
1.	**19 Maret 2021**	**Konsultasi Bab I dan Bab II**	1.
2.	25 Maret 2021	Revisi Bab I dan Bab II	2.
3.	**16 April 2021**	**ACC Bab I dan Bab II**	3.
4.	23 April 2021	Konsultasi Bab III dan **Penulisan**	4.
5.	27 April 2021	Konsultasi Keagamaan Bab I **dan Bab II**	5.
6.	05 Mei 2021	Konsultasi Bab III dan Bab IV	6.
7.	07 Mei 2021	**ACC Keagamaan Bab I dan** Bab II	7.
8.	**06 Sepember 2021**	**Revisi Bab III dan Bab IV**	**8.**
9.	04 Oktober 2021	ACC Bab III dan Bab IV	9.
10.	06 Oktober 2021	**Konsultasi Bab I, Bab III dan** Keagamaan Bab III	10.
11.	01 November 2021	**ACC Bab I, Bab III dan** Keagamaan Bab III	11.
12.	09 Januari 2022	**Konsultasi dan ACC** Keseluruhan	12.

No.	Tanggal	Hal	Tanda Tangan
13.	09 Januari 2022	Konsultasi dan ACC Keseluruhan	13.

Malang, 09 Januari 2022
Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129 200012 2 005