IMPLEMENTASI *HYBRID CRYPTOGRAPHY* BERBASIS *GALOIS FIELD* DALAM MENGAMANKAN PESAN

SKRIPSI

OLEH
MUHAMMAD AL HIMNI ABDIL BARR
NIM. 18610088

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

IMPLEMENTASI *HYBRID CRYPTOGRAPHY* BERBASIS *GALOIS FIELD* DALAM MENGAMANKAN PESAN

SKRIPSI

OLEH
MUHAMMAD AL HIMNI ABDIL BARR
NIM. 18610088

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

IMPLEMENTASI *HYBRID CRYPTOGRAPHY* BERBASIS *GALOIS FIELD* DALAM MENGAMANKAN PESAN

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
Muhammad Al Himni Abdil Barr
NIM. 18610088

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

IMPLEMENTASI *HYBRID CRYPTOGRAPHY* BERBASIS *GALOIS FIELD* DALAM MENGAMANKAN PESAN

SKRIPSI

Oleh
Muhammad Al Himni Abdil Barr
NIM. 18610088

Telah Disetujui Untuk Diuji

Malang, 17 Juni 2022

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah, M. Si	Ari Kusumastuti, M. Pd., M. Si
NIDT. 19900511 20160801 1 057	NIP. 19770521 200501 2 004

Mengetahui,
Ketua Program Studi Matematika

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

IMPLEMENTASI *HYBRID CRYPTOGRAPHY* BERBASIS *GALOIS FIELD* DALAM MENGAMANKAN PESAN

SKRIPSI

Oleh
Muhammad Al Himni Abdil Barr
NIM. 18610088

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 21 Juni 2022

Ketua Penguji	: Intan Nisfulaila, M. Si	.....
Anggota Penguji 1	: Hisyam Fahmi, M. Kom	.....
Anggota Penguji 2	: Muhammad Khudzaifah, M. Si	.....
Anggota Penguji 3	: Ari Kusumastuti, M. Pd., M. Si	.....

Mengetahui,
Ketua Program Studi Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertandatangan di bawah ini:

Nama	: Muhammad Al Himni Abdil Barr
NIM	: 18610088
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi
Judul Skripsi	: Implementasi *Hybrid Cryptography* Berbasis *Galois Field* Dalam Mengamankan Pesan

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 dan pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka. Apabila dikemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perilaku tersebut.

Malang, 17 Juni 2022
Yang membuat peryataan,

Muhammad Al Himni Abdil Barr
NIM. 18610088

MOTO

"Slow But Sure"

Melakukan suatu hal dengan tidak tergesa-gesa tetapi pasti

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:

Kedua orang tua tercinta yaitu Bapak Isnaini dan Ibu Ida Fitriyah, yang tidak pernah putus dalam memanjatkan do'a dan memberikan restu serta nasihat kepada penulis.

Sahabat-sahabat penulis Aisyatin Kamilah, seluruh teman-teman dari peminatan aljabar dan semua teman-teman JDFI '18, yang telah menemani dan memberi semangat kepada penulis dalam menyelesaikan skripsi ini.

Santri-santri TPQ Al-Hijrah yang telah mengajari penulis tentang sabar dan istiqomah.

KATA PENGANTAR

Segala puji syukur kehadirat Allah SWT yang telah memberikan rahmat dan hidayahnya sehingga penulis dapat menyelesaikan proposal skripsi ini sebagai syarat untuk mendapatkan gelar sarjana di bidang matematika Fakultas Sains dan Teknologi di Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Tak lupa pula ucapan terima kasih untuk pihak-pihak yang telah membantu dan memotivasi kepada penulis, yakni kepada:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, S.Pd., M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Muhammad Khudzaifah, M.Si, selaku dosen pembimbing I yang telah banyak memberi bimbingan, arahan, perbaikan, serta saran yang membangun demi kebaikan skripsi ini.
5. Ari Kusumastuti, M. Pd., M. Si., selaku dosen pembimbing II yang telah banyak memberikan bimbingan dan berbagai ilmunya kepada penulis.
6. Ibu Intan Nisfulaila, M.Si, selaku Penguji Utama dalam Ujian Skripsi yang telah memberi masukan dan saran yang membangun.
7. Dr. Heni Widayani, M.Si, selaku dosen wali yang telah memberi banyak motivasi dan semangat kepada penulis.
8. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim.
9. Kedua orang tua penulis Bapak Isnaini dan Ibu Ida Fitriyah , yang tidak pernah putus dalam memanjatkan do’a dan memberikan restu serta nasihat kepada penulis.
10. Sahabat-sahabat penulis Aisyatin Kamilah, seluruh teman-teman dari peminatan aljabar dan semua teman-teman JDFI ‘18, yang telah menemani dan memberi semangat kepada penulis dalam menyelesaikan skripsi ini.

Penulis sangat berharap dengan adanya skripsi ini dapat menambah wawasan baru bagi pembaca dan dapat membantu menyelesaikan berbagai masalah lainnya, utamanya di bidang matematika aljabar.

Malang, 17 Juni 2022

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

Abdil Barr, Muhammad Al Himni. 2022. **Implementasi *Hybrid Cryptography* Berbasis *Galois Field* Dalam Mengamankan Pesan**. Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si (II) Ari Kusumastuti, M Pd., M. Si

Kata Kunci: Pengamanan Pesan Teks, *Hybrid Cryptography*, Enkripsi, Dekripsi, *Galois Field*, *Affine Cipher*, *Diffie Hellman*

Penelitian ini difokuskan pada analisis *hybrid cryptography* berbasis *galois field* dalam mengamankan pesan. Pesan yang dimaksud dalam penelitian ini adalah pesan berupa teks. Karena saat ini sering terjadi berbagai macam masalah, utamanya dalam pengamanan pesan. Sehingga diperlukan sebuah solusi untuk menjaga pesan teks tersebut supaya dapat sampai kepada pihak yang berwenang. Metode yang digunakan pada penelitian ini adalah *hybrid cryptography*, yaitu dengan cara menggabungkan antara kriptografi kunci simetri dan kriptografi kunci asimetri. Namun, penulis menggunakan algoritma *Affine cipher* dan algoritma *Diffie Hellman*, baik pada proses enkripsi pesan maupun proses dekripsi pesan. Proses enkripsi dilakukan menggunakan algoritma *Affine cipher*, yaitu dengan menentukan kunci a, b dan melakukan perhitungan dengan rumus $C = (aP + b)\ mod\ n$. Sedangkan pada proses dekripsi dilakukan menggunakan algoritma *Diffie Hellman* kemudian dilanjut dengan menggunakan algoritma *Affine cipher*, yaitu dengan melakukan pertukaran kunci dengan rumus $X = g^x\ mod\ n$ bagi pengirim pesan dan dengan rumus $Y = g^y\ mod\ n$ bagi penerima pesan yang akan didapatkan nilai $K = K'$, selanjutnya menentukan nilai invers dari kunci a^{-1} dan pergeseran dari kunci b, selanjutnya melakukan perhitungan dengan rumus $P = (a^{-1}C - b)\ mod\ n$. Hasil dari penelitian ini menunjukkan bahwa penggabungan antara algoritma *Affine cipher* dan algoritma *Diffie Hellman* lebih aman dibandingkan dengan algoritma kriptografi selain keduanya, karena kunci yang digunakan bersifat rahasia dan hanya diketahui oleh pihak-pihak yang saling bertukar kunci. Oleh karena itu, dengan kedua algoritma kriptografi tersebut pengirim pesan maupun penerima pesan dapat merasa aman atas pesan yang ingin disampaikan kepada pihak tertentu.

ABSTRACT

Abdil Barr, Muhammad Al Himni. 2022. **On the Implementation of Galois Field-Based Hybrid Cryptography in Securing Messages**. Thesis. Mathematics Study Program, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Supervisors: (I) Muhammad Khudzaifah, M.Si (II) Ari Kusumastuti, M Pd., M. Si

Keywords: Text Message Security, Hybrid Cryptography, Encryption, Decryption, Galois Field, Affine Cipher, Diffie Hellman

This research is focused on the analysis of hybrid cryptography based on galois field in securing messages. The message referred to in this study is a message in the form of text. Because at this time there are often various kinds of problems, especially in securing messages. So we need a solution to keep these text messages from reaching the authorities. The method used in this research is hybrid cryptography, namely by combining symmetric key cryptography and asymmetric key cryptography. However, the author uses the Affine cipher algorithm and the Diffie Hellman algorithm, both in the message encryption process and the message decryption process. The encryption process is carried out using the Affine cipher algorithm, namely by determining the keys a, b and performing calculations with the formula $C = (aP + b)\ mod\ n$. While the decryption process is carried out using the Diffie Hellman algorithm and then continued by using the Affine cipher algorithm, namely by exchanging keys with the formula $X = g^x\ mod\ n$ for the sender of the message and with the formula $Y = g^y\ mod\ n$ for the recipient of the message that will be obtained value $K = K'$, then determine the inverse value of key a^{-1} and shift of key b, then perform calculations with the formula $P = (a^{-1}C - b)\ mod\ n$. The results of this study indicate that the combination of the Affine cipher algorithm and the Diffie Hellman algorithm is more secure than the cryptographic algorithms other than the two, because the key used is secret and only known by the parties who exchange keys. Therefore, with the two cryptographic algorithms, the sender of the message and the recipient of the message can feel safe for the message to be conveyed to certain parties.

مستخلص البحث

عبد البر، محمد الهمني. 2022. **تطبيق التشفير الهجين (*Hybrid Cryptography*) على أساس حقل جالوا (*Galois Field*) في تأمين الرسالة**. البحث الجامعي. قسم الرياضيات، كلية العلوم والتكنولوجيا، حامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف الأول: محمد خذيفةالماجستير، المشرف الثاني: أري كوسوماستوتي الماجستير.

الكلمات المفتاحية: أمان الرسالة النصية، التشفير الهجين (*Hybrid Cryptography*)، التشفير، فك التشفير، حقل جالوا (*Galois Field*)، التشفير الأفيني (*Affine Cipher*)، ديفي هيلمان (*Diffie Hellman*).

يكز هذا البحث على تحليل التشفير الهجين على أساس حقل جالو في تأمين الرسالة. ونوع الرسالة في هذا البحث هو رسالة نصية لأنه في هذا الوقت غالبا قد حدث عدد من مشكلات مختلفة، خاصةً في تأمين الرسالة. لذلك يحتاج إلى الحل لحفظ هذه الرسالة النصية من الوصول إلى القابل الحق. والطريقة المستخدمة في هذا البحث هي التشفير الهجين بالجمع بين تشفير المفتاح المتماثل وتشفير المفتاح غير المتماثل. ولكن استخدم الباحث خوارزمية التشفيرالأفني وخوارزمية ديفي هيلمان، سواء في كل من عملية تشفير الرسالة أو عملية فك تشفير الرسالة. وتتم عملية التشفير باستخدام خوارزمية التشفير الأفني وهي بطريقة $C = (aP + b) \ mod \ n$ تعيين المفتاح وإجراء العمليات الحسابية باستخدام الصيغة. وفي عملية فك التشفير باستخدام خوارزمية ديفي هيلمان ثم يستمر باستخدام خوارزمية التشفير الأفني، وهي بمقابلة المفتاح $X = g^x$ بصيغة مرسل الرسالة وبصيغة $Y = g^y$ قابل الرسالة للحصول على القيمة $K = K'$، ثم تعيين القيمة العكسية للمفتاح a^{-1} وتحويل المفتاح b، ثم إجراء العمليات الحسابية باستخدام الصيغة $P = (a^{-1}C - b) \ mod \ n$. وتشير نتائج هذا البحث إلى أن الجمع بين خوارزمية التشفير الأفني وخوارزمية ديفي هيلمان أكثر أمانًا من خوارزميات التشفير بسوى الخوارزميتين لأن المفتاح المستخدم سري ولا يعرفه إلا الأطراف التي تتقابل المفاتيح. فلذلك، باستخدام خوارزميتي التشفير، يستطيع أن يشعر مرسل الرسالة وقابلها بالأمان على الرسالة التي سترسلها إلى طرف معين.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pandemi covid-19 menjadi penghalang bagi masyarakat untuk beraktivitas di luar rumah. Sejak diterapkannya PPKM (Pemberlakuan Pembatasan Kegiatan Masyarakat) semua kegiatan masyarakat dilakukan secara online *(daring)*. Saat ini marak terjadi nya masalah di kalangan masyarakat yaitu dalam hal penyampaian pesan. Penyampaian pesan saat ini tidak lepas dari pemanfaatan suatu teknologi. Apalagi perkembangan teknologi di zaman sekarang berkembang sangat cepat. Padahal teknologi sendiri juga memiliki dampak negatifnya, salah satunya adalah masalah keamanannya. Tanpa menggunakan teknologi sekalipun keamanan pesan kita untuk disampaikan kepada seseorang yang hanya kita inginkan juga tidak kalah pentingnya dalam keamanannya. Perlu adanya pengetahuan tentang ilmu yang berkaitan dengan keamanan suatu pesan. Ilmu yang mempelajari tentang keamanan suatu pesan adalah kriptografi. Ilmu kriptografi sangat penting untuk dipelajari karena di zaman modern saat ini banyak sekali oknum atau pelaku yang tidak bertanggung jawab, dimana mereka memanfaatkan teknologi saat ini untuk kepentingan dirinya sendiri dan hal tersebut merugikan orang lain bahkan merugikan kita sebagai pemilik pesan.

Dalam ilmu kriptografi terdapat istilah-istilah yang menjadi dasar dalam penerapan kriptografi yaitu enkripsi dan dekripsi. Enkripsi merupakan proses merubah pesan yang terbaca menjadi pesan yang tidak terbaca dengan merubahnya ke dalam bentuk kode yang dibantu adanya kunci dan algoritma. Sedangkan dekripsi merupakan proses merubah pesan yang tidak terbaca menjadi pesan yang

terbaca dengan bantuan kunci dan algoritma juga. Oleh karena itu, dengan adanya ilmu kriptografi tersebut kita dapat memanfaatkannya dalam mengamankan pesan kita terhadap pihak-pihak yang tidak berhak atas pesan tersebut. Tidak menutup kemungkinan pula dapat meminimalisir dampak terbongkarnya suatu pesan tersebut selama pengiriman pesan berlangsung.

Algoritma pada kriptografi ada dua, yaitu algoritma kriptografi kunci simetri dan algoritma kriptografi kunci asimetri. Salah satu algoritma kriptografi kunci simetri yang terkenal adalah algoritma *Affine cipher*. *Affine cipher* adalah algoritma kriptografi yang metode penyandian pesannya menggunakan algoritma kriptogafi klasik, dimana kriptografi klasik pada dasarnya menggunakan teknik substitusi dan teknik transposisi. *Affine cipher* juga merupakan perluasan dari *Caesar cipher*, yaitu dengan cara mengalikan *plaintext P* dengan sebuah nilai m lalu menambahkan hasilnya dengan sebuah nilai b (Munir, 2019).

Begitu juga pada algoritma kriptografi kunci asimetri yang sering digunakan pada artikel, jurnal, maupun penelitian, yaitu algoritma *Diffie Hellman*. Algoritma *Diffie Hellman* atau biasa disebut pertukaran kunci digunakan untuk membangkitkan kunci yang akan digunakan oleh pengirim pesan dan penerima pesan. Algoritma *Diffie Hellman* tidak digunakan pada proses enkripsi dan dekripsi, tetapi digunakan untuk mendapatkan kunci rahasia *(secret key)* sehingga pihak lain yang tidak memiliki hak atas pesan tersebut akan kesulitan untuk meretas nya.

Suatu hal yang sangat penting bagi semua pihak untuk menjaga kerahasiaan sebuah pesan yang ingin disampaikan kepada pihak tertentu. Seperti yang telah Allah SWT firmankan di dalam Al-Qur’an, yaitu:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَخُوْنُوا اللّٰهَ وَالرَّسُوْلَ وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ

Artinya: "Wahai orang-orang beriman, janganlah kamu menghianati Allah dan Rasul dan (juga) janganlah kamu menghianati amanat yang dipercayakan kepadamu, sedang kamu mengetahui" (QS. Al-Anfal: 27).

Keunggulan dari kedua algoritma tersebut yaitu algoritma *Affine cipher* dan algoritma *Diffie Hellman* adalah memiliki proses yang sangat mudah tetapi disisi lain juga memiliki tingkat keamanan yang sangat tinggi. Karena pada algoritma kriptografi selain *Affine cipher* dan *Diffie Hellman*, baik dalam prosesnya maupun tingkat keamanannya masih sangat rumit dan tingkat keamanannya masih kurang sehingga peneliti memilih algoritma *Affine cipher* dan algoritma *Diffie Hellman* sebagai jalan keluar untuk mengatasi masalah pada keamanan pesan yang akan disampaikan kepada pihak tertentu.

Bentuk yang digunakan pada penelitian adalah menggunakan bentuk *galois field*, yaitu dengan bentuk polinomial. Karena dengan menggunakan bentuk *galois field* yang berbentuk polinomial dapat menambah tingkat keamanannya, dimana dalam proses penyandian pesan teks melalui tahap merubah setiap pesan teks menjadi bentuk biner dengan batas tertentu. Oleh karena itu, dengan menggunakan bentuk polinomial tersebut dapat menjaga keamanan pesan teks tersebut sehingga dapat sampai kepada pihak yang dituju.

Galois Field (*GF*) atau yang biasa disebut medan *Galois* merupakan jumlah himpunan yang memiliki batas tertentu. *Galois field* bisa dikatakan juga sebuah medan berhingga dengan p^n elemen, dimana p merupakan bilangan prima dan $n \geq 1$ (Irawanto, 2001). Penerapan *Galois field* biasanya dapat dinotasikan dengan $GF(p^n)$. *Galois field* yang berkaitan dengan aritmetika modular pada polinomial adalah *Galois field* yang biasanya dipakai dalam sistem kriptografi. Polinomial

Galois field merupakan kombinasi antara polinomial-polinomial dengan konstanta yang variabelnya 1 dan pangkat tertinggi dari variabelnya adalah 3.

Sebuah penelitian yang telah dilakukan sebelumnya oleh Saropah (2008), dimana dalam penelitiannya tersebut menjelaskan tentang *field* yang dikenai dengan polinomial. Adapun bentuk polinomial yang terbentuk, yaitu polinomial konstan dan polinomial tidak konstan. Bentuk polinomial konstan terdapat polinomial yang dapat difaktorkan. Sedangkan pada bentuk polinomial tidak konstan ada dua kemungkinan, yaitu terdapat polinomial yang dapat difaktorkan dan ada yang tidak dapat difaktorkan. Sebuah polinomial yang dapat difaktorkan terdapat akar penyelesaian pada lapangan tersebut, sedangkan polinomial yang tidak dapat difaktorkan disebut polinomial taktereduksi *(irreducible)* atau tidak mempunyai akar penyelesaian pada lapangan tersebut.

Berdasarkan beberapa uraian di atas, maka penulis mengangkat sebuah judul "Implementasi *Hybrid Cryptography* Berbasis *Galois Field* dalam Mengamankan Pesan".

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka rumusan masalah pada penelitian ini sebagai berikut:

1. Bagaimana proses enkripsi pesan menggunakan *Affine cipher* dan *Diffie Hellman* berbasis *Galois field* dalam mengamankan pesan?
2. Bagaimana proses dekripsi pesan menggunakan *Affine cipher* dan *Diffie Hellman* berbasis *Galois field* dalam mengamankan pesan?

1.3 Tujuan Masalah

Berdasarkan rumusan masalah di atas, maka penelitian ini memiliki tujuan sebagai berikut:

1. Untuk mengetahui proses enkripsi pesan menggunakan *Affine cipher* dan *Diffie Hellman* berbasis *Galois field* dalam mengamankan pesan.
2. Untuk mengetahui proses dekripsi pesan menggunakan *Affine cipher* dan *Diffie Hellman* berbasis *Galois field* dalam mengamankan pesan.

1.4 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Dapat menambah pengetahuan tentang proses enkripsi pesan dengan menggunakan *Affine cipher* dan *Diffie Hellman* berbasis *Galois field* dalam mengamankan pesan.
2. Dapat menambah pengetahuan tentang proses dekripsi pesan dengan menggunakan *Affine cipher* dan *Diffie Hellman* berbasis *Galois field* dalam mengamankan pesan.

1.5 Batasan Masalah

Untuk mencapai sasaran yang direncanakan, maka perlu adanya pembatasan masalah sebagai berikut:

1. Proses enkripsi dan dekripsi yang digunakan adalah polinomial $GF(2^4)$ dengan sistem bilangan biner pada batas 4 bit.
2. Proses penyandian menggunakan huruf abjad, angka $0-9$, simbol-simbol seperti [,],{,},(,),~,!,@,#,$,%,^,&,*,?,<,>,;,:,’,”, dan *space*.

BAB II
KAJIAN TEORI

2.1 Kriptografi

Secara etimologi kata kriptografi (*cryptography*) berasal dari bahasa Yunani, yaitu *kryptos* yang berarti tersembunyi dan *graphein* yang berarti menulis. Secara umum kriptografi adalah proses menulis atau menyampaikan pesan secara rahasia dan tersembunyi yang ditujukan hanya pengirim dan penerima pesan saja yang dapat melihat isinya. Kriptografi pertama kali dikenal atau dipahami sebagai ilmu tentang menyembunyikan pesan (Sadikin, 2012). Kriptografi mulai berkembang menjadi ilmu yang dimanfaatkan untuk menyelesaikan persoalan terkait keamanan pribadi dan juga verifikasinya (Diffie, 1976).

Penerapan kriptografi berkaitan dengan proses mengubah pesan asli atau pesan yang dapat dibaca menjadi pesan yang bersandi atau pesan yang tidak dapat dibaca, begitu juga sebaliknya. Proses tersebut digunakan sebagai sarana penyampaian pesan dalam berbagai bentuk tertentu yang dimana hanya pengirim dan penerima pesan saja yang dapat membacanya. Banyak aplikasi yang menggunakan atau menerapkan sistem kriptografi, seperti kartu transaksi perbankan, penyandian pada komputer, dan transaksi *e-commerce*. Metode yang paling sederhana dalam ilmu kriptografi adalah menggunakan sistem simetris atau kunci rahasia, dimana pesan tersebut disandikan dengan menggunakan kunci rahasia dan kunci rahasianya diberikan kepada penerima pesan untuk membuka pesan aslinya.

2.1.1 Komponen-Komponen Kriptografi

Adapun beberapa komponen-komponen kriptografi yang menjadi prinsip dasar dalam menerapkan pengilmuan kriptografi. Komponen-komponen tersebut diantaranya sebagai berikut:

1. Pesan*, Plaintext,* dan *Ciphertext*

Pesan merupakan terjemahan dari bahasa asing "*message*" yang artinya lambang bermakna (*meaningful symbols*), yakni lambang yang membawakan pikiran atau perasaan komunikator (Effendy, 1993). Pesan juga dimaknai oleh KBBI (Kamus Besar Bahasa Indonesia) sebagai pesan wasiat atau perkataan terahir dari seseorang sebelum wafat. Pengertian dalam studi komunikasi, pesan merupakan informasi yang disampaikan dengan kata-kata, baik ucapan maupun tulisan. Penyampaian pesan tidak hanya berisikan kata-kata atau kalimat saja, tetapi bisa juga berupa informasi, ilmu pengetahuan, nasihat, dan lainnya. Sebuah pesan dapat disampaikan dengan berbagai cara diantaranya yaitu dengan menggunakan kurir atau bisa juga menggunakan alat elektronik (seperti WhatsApp, Telegram, dan Instagram) dan pesan dapat juga disampaikan dengan secara langsung atau secara tatap muka.

Adapun hal-hal yang perlu dipertimbangkan dalam penyampaian pesan sebagai berikut:

a. *Clear*, artinya suatu pesan harus jelas. Maksudnya adalah bahasa yang digunakan dapat dibaca oleh penerima pesan tersebut.
b. *Correct*, artinya suatu pesan harus mengandung kebenaran yang sudah teruji, dimana pesan tersebut berdasarkan fakta yang ada dan tidak berdasarkan opini dari pengirim pesan.

c. *Concise*, artinya suatu pesan harus ringkas dengan tanpa mengurangi arti sesungguhnya.
d. *Comprehensive*, artinya suatu pesan harus mencakup bagian-bagian penting yang perlu disampaikan kepada penerima pesan.
e. *Concrite*, artinya suatu pesan dapat dipertanggung jawabkan oleh pengirim pesan berdasarkan fakta yang ada.
f. *Complete*, artinya suatu pesan dituliskan secara lengkap dan tersusun secara sistematis.
g. *Convising*, artinya suatu pesan harus menarik dan dapat meyakinkan bagi penerima pesan.

Begitu juga terdapat istilah-istilah yang sering dijumpai dalam penerapan ilmu kriptografi. Istilah-istilah tersebut disebut *plaintext* dan *ciphertext*. *Plaintext* adalah pesan asli atau pesan yang dapat dibaca, sedangkan *ciphertext* adalah pesan berkode atau pesan yang tidak dapat dibaca. Di samping istilah-istilah tersebut terdapat pula proses-proses yang dilalui dalam penerapan ilmu kriptografi. Proses pengubahan dari teks asli ke teks berkode disebut penyandian (*enciphering*) dan proses kebalikannya dalam pengubahan teks berkode ke teks asli disebut penguraian (*deciphering*) (Anton dan Rorres, 1998).

2. Pengirim dan Penerima

Sebuah komunikasi itu melibatkan pertukaran pesan antara 2 entitas, yaitu pengirim dan penerima. Pengirim adalah entitas yang mengirim pesan kepada entitas lain. Sedangkan penerima adalah entitas yang menerima pesan dari entitas lain. Maksud entitas disini adalah bisa berupa orang, mesin, computer, kartu kredit, dan lainnya.

3. Enkripsi dan Dekripsi

Pengilmuan kriptografi terdapat proses penyandian pesan yang harus dilakukan, baik dari pihak pengirim pesan maupun dari pihak penerima pesan. Proses tersebut disebut enkripsi dan dekripsi. Enkripsi adalah proses dimana pesan yang akan dikirimkan diubah menjadi pesan yang berkode sehingga tidak dapat dibaca oleh pihak lain (Aulia et al., 2018). Sedangkan dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali pesan berkode tersebut menjadi pesan asli sehingga dapat dibaca (Komarudin, 2013). Proses enkripsi dan dekripsi, baik bagi pengirim pesan maupun penerima pesan dapat merasa aman atas pesan yang dikirimkan maupun diterimanya sehingga dapat meminimalisir dampak dibobolnya suatu pesan oleh pihak yang tidak berhak atas pesan tersebut.

4. Sistem Kriptografi

Kriptografi membentuk sebuah sistem yang disebut sebagai sistem kriptografi. Sistem kriptografi terdiri atas algoritma kriptografi, *plaintext*, *ciphertext*, dan juga kunci.

5. Penyadap atau *Eavesdropper*

Penyadap merupakan entitas yang berusaha membobol pesan ketika pesan masih dalam proses pengiriman kepada penerima pesan. Tujuan dari penyadap tersebut adalah untuk mendapatkan informasi sebanyak-banyaknya tentang sistem kriptografi yang digunakan untuk berkomunikasi dengan maksud memecahkan *ciphertext*. Penyadapan yang dilakukan biasanya terjadi di platform internet yang sudah banyak terjadi disaat masa PPKM diterapkan.

6. Kriptanalisis

Kriptanalisis atau *cryptanalysis* adalah ilmu atau seni untuk memecahkan *ciphertext* menjadi *plaintext* tanpa harus mengetahui kunci yang digunakan. Pelaku kriptanalisis disebut sebagai kriptanalis.

2.1.2 Tujuan Kriptografi

Selain untuk meminimalisir terjadinya masalah keamanan terhadap pesan, dalam penerapan ilmu kriptografi juga memiliki tujuan sebagai berikut:

1. Kerahasiaan atau *Confidentiality*

Menjaga dan menjamin bahwa pesan tersebut tidak dapat dibaca oleh pihak-pihak yang tidak berhak dan hanya dapat diakses oleh pihak-pihak tertentu adalah suatu kewajiban bagi kita sebagai pemilik pesan tersebut. Sehingga diterapkannya ilmu kriptografi supaya tidak ada pihak yang merasa dirugikan oleh pihak lain.

2. Otentikasi atau *Authentication*

Otentikasi adalah mengidentifiasi atau pengenalan, baik secara kesatuan sistem maupun pesan itu sendiri oleh masing-masing pihak yang saling berkomunikasi untuk memastikan keaslian suatu pesan yang diterima.

3. Integritas atau *Integrity*

Integritas adalah menjamin setiap pesan yang dikirim bisa sampai kepada penerima pesan tanpa terdapat bagian pesan yang diganti, berubah runtutannya, ditambah dan dirusak. Cara kita untuk menjamin integritas pesan tetap terjaga, diperlukan kemampuan untuk mendeteksi terjadinya manipulasi pesan oleh pihak-pihak yang tidak berhak atas pesan tersebut. Maksud dari manipulasi

pesan tersebut adalah dapat berupa penggantian pesan, penyisipan pesan, maupun penghapusan pesan.

4. *Non Repudiation*

Maksud dari *non repudiation* di sini adalah mencegah pengirim maupun penerima untuk menyangkal bahwa mereka telah mengirim dan menerima pesan. Apabila terdapat sebuah pesan yang dikirim, penerima bisa membuktikan bahwa pesan tersebut terbukti dikirim oleh pengirim pesan dengan melihat bagian nama atau identitas lainnya yang tertera di dalam pesan tersebut. Begitu juga sebaliknya, apabila sebuah pesan diterima, pengirim pesan juga bisa membuktikan bahwa pesan tersebut telah diterima oleh pihak yang dituju.

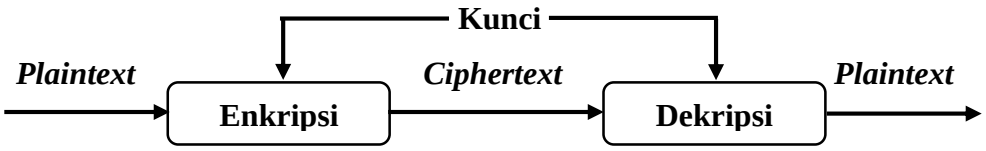
2.1.3 Algoritma Kriptografi

Algoritma kriptografi merupakan langkah-langkah yang perlu diketahui dalam menyandikan atau menyembunyikan pesan dari pihak-pihak yang tidak berhak atas suatu pesan tersebut. Algoritma kriptografi bekerja dalam kombinasi dengan menggunakan kunci publik seperti kata, nomor atau frase tertentu lainnya.

1. Kriptografi Kunci Simetri

Kriptografi kunci simetri merupakan metode enkripsi dan dekripsi yang dimana pengirim maupun penerima menggunakan kunci yang sama. Keamanan dari pesan yang menggunakan kriptografi kunci simetri ini tergantung pada kunci. Jika kunci tersebut diketahui oleh pihak lain, maka pihak lain tersebut bisa melakukan enkripsi dan dekripsi terhadap pesan tersebut. Contoh kriptografi yang memakai kunci simetri adalah *Data Ecryption Standart* (DES), *International Data Encryption Algorithm* (IDEA), *Advanced Encryption Standart* (AES), *One Time Pad* (OTP), *Blowfish,* dan lain sebagainya (Ariyus,

2006). Secara sederhana, skema pengiriman pesan dengan menggunakan kriptografi kunci simetri dapat digambarkan sebagai berikut:



Gambar 2.1 Skema Kriptografi Kunci Simetri

2. Kriptografi Kunci Asimetri

Kriptografi kunci asimetri sering juga disebut dengan kriptografi kunci publik. Artinya kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Kriptografi kunci asimetri terbagi menjadi dua bagian, yaitu kunci publik (*public key*) dan kunci pribadi (*private key*). Kunci publik adalah kunci yang semua pihak boleh mengetahui, sedangkan kunci pribadi adalah kunci yang dirahasiakan, dimana maksudnya hanya boleh diketahui oleh satu pihak saja. Contoh kriptografi yang memakai kunci asimetri adalah *Digital Signature Algorithm* (DSA), *Riverst Shamir Adleman* (RSA), *Diffie Hellman* (DH), El Gamal, *Elliptic Curve Cryptography* (ECC), dan lain sebagainya (Ariyus, 2006). Sederhananya, skema pengiriman pesan dengan mengunakan kriptografi kunci asimteri dapat digambarkan sebagai berikut:

Gambar 2.2 Skema Kriptografi Kunci Asimetri

2.1.4 *Affine Cipher*

Affine cipher merupakan perluasan dari *Caesar cipher* dengan cara mengalikan *plaintext* dengan sebuah kunci dan menambahkannya dengan sebuah kunci pergeseran. Proses enkripsi dan dekripsi pada *Affine cipher* menggunakan

dua buah kunci, yaitu kunci a dan b. Kunci a dan b merupakan kunci dari *Affine cipher* untuk setiap p huruf dalam pesan dan c merupakan huruf sandi yang dihasilkan (Sadikin, 2012).

1. Enkripsi *Affine Cipher*

Proses enkripsi pada *Affine cipher*, hal perlu diperhatikan sebelum melakukan perhitungan adalah menentukan dua buah kunci, yaitu kunci a dan kunci b. Setelah menentukan dua buah kunci tersebut, kita lakukan perhitungan dengan persamaan

$$C = (aP + b)\ mod\ n, \qquad (2.1)$$

dimana diketahui C merupakan *ciphertext* pergeseran karakter yang diketahui pada *plaintext*, a merupakan bilangan bulat yang relatif prima dengan n, b merupakan jumlah pergeseran dari nilai yang relatif prima dengan kunci a, dan n merupakan banyaknya karakter.

Contoh:

Diketahui sebuah pesan asli atau *plaintext* adalah “malang”. Setelah diketahui sebuah *plaintext* tersebut akan dilakukan proses enkripsi dengan menggunakan algoritma *Affine cipher*.

Sebelum melakukan perhitungan, hal yang perlu dilakukan terlebih dahulu adalah mengkonversikan karakter atau *plaintext* tersebut ke dalam bentuk desimal yang dapat dituliskan pada tabel berikut:

Tabel 2.1 Hasil Konversi Karakter Menjadi Angka Berdasarkan Tabel ASCII

Karakter	Angka
m	109
a	97
l	108
a	97
n	110
g	103

Setelah mendapatkan hasil dari konversi karakter menjadi angka pada tabel di atas, selanjutnya menentukan dua kunci yang digunakan dalam proses enkripsi, yaitu $n = 125$, kunci $a = 7$ (relatif prima dengan 125), kunci $b = 10$. Kemudian langkah selanjutnya melakukan perhitungan sebagai berikut:

$c_1 = (7 \cdot 109 + 10)\ mod\ 125 = 773\ mod\ 125 = 23\ mod\ 125$

(karakter ETB).

$c_2 = (7 \cdot 97 + 10)\ mod\ 125 = 689\ mod\ 125 = 64\ mod\ 125$

(karakter @).

$c_3 = (7 \cdot 108 + 10)\ mod\ 125 = 766\ mod\ 125 = 16\ mod\ 125$

(karakter DLE).

$c_4 = (7 \cdot 97 + 10)\ mod\ 125 = 689\ mod\ 125 = 64\ mod\ 125$

(karakter @).

$c_5 = (7 \cdot 110 + 10)\ mod\ 125 = 780\ mod\ 125 = 30\ mod\ 125$

(karakter RS).

$c_6 = (7 \cdot 103 + 10)\ mod\ 125 = 731\ mod\ 125 = 106\ mod\ 125$

(karakter j).

Sehingga dari proses tersebut, didapatkan sebuah pesan yang telah bersandi atau *ciphertext*, yaitu “ETB@DLE@RSj”.

2. Dekripsi *Affine Cipher*

Proses dekripsi pada *Affine cipher* ini tidak jauh beda dengan proses enkripsi *Affine cipher*. Kunci yang digunakan pada proses dekripsi sama dengan proses enkripsi *Affine cipher.* Salah satu pembeda pada proses dekripsi ini adalah persamaan yang digunakan. Persamaan yang digunakan adalah

$$P = (a^{-1}C - b)\ mod\ n, \qquad (2.2)$$

dimana kunci a^{-1} dan b disini sama dengan kunci yang digunakan pada proses enkripsi. Hanya saja nilai kunci a^{-1} merupakan invers dari kunci a dan kunci b merupakan pergeseran dari nilai kunci b.

Contoh:

Mencari kunci $a^{-1}\ mod\ 125$, yaitu

$$a^{-1} = 7x \equiv 1\ (mod\ 125),$$

adalah bilangan $x \equiv 18\ (mod\ 26)$ karena $7 \cdot 18 = 126 \equiv 1\ (mod\ 125)$.

Selanjutnya mencari pergeseran dari nilai kunci b dengan perhitungan

$$P = 18(C - b)\ mod\ 125$$

$$P = 18(C - 10)\ mod\ 125$$

$$P = 18C - 180\ mod\ 125$$

$$P = 18C - 55\ mod\ 125$$

Sehingga didapatkan nilai kunci $a^{-1} = 18$ dan $b = 55$. Setelah mendapat nilai a^{-1} dan b, kita dapat melakukan perhitungan dekripsi *Affine cipher* dari *plaintext* ETB@DLE@RSj pada Tabel 2.2 berikut:

Tabel 2.2 Hasil Konversi Karakter Menjadi Angka Berdasarkan Tabel ASCII

Karakter	Angka
ETB	23
@	64
DLE	16
@	64
RS	30
j	106

dengan perhitungan berikut:

$p_1 = (18(23) - 55)\ mod\ 125 = 359\ mod\ 125 = 109\ mod\ 125$

(karakter m).

$p_2 = (18(64) - 55)\ mod\ 125 = 1.097\ mod\ 125 = 97\ mod\ 125$

(karakter a).

$p_3 = (18(16) - 55)\ mod\ 125 = 233\ mod\ 125 = 108\ mod\ 125$

(karakter l).

$p_4 = (18(64) - 55)\ mod\ 125 = 1.097\ mod\ 125 = 97\ mod\ 125$

(karakter a).

$p_5 = (18(30) - 55)\ mod\ 125 = 485\ mod\ 125 = 110\ mod\ 125$

(karakter n).

$p_6 = (18(106) - 55)\ mod\ 125 = 1.853\ mod\ 125 = 103\ mod\ 125$

(karakter g).

Sehingga dari perhitungan di atas, didapatkan sebuah pesan asli atau *plaintext*, yaitu “malang”.

2.1.5 *Diffie Hellman*

Diffie Hellman atau biasa disebut pertukaran kunci merupakan algoritma yang dimana antara kedua belah pihak saling bertukar kunci rahasia dan hasil dari

pertukaran kunci tersebut adalah sama pada kedua pihak (Ahirwal dan Ahke, 2013). Metode tersebut diperlihatkan oleh Dr. W. Diffie dan Dr. M. E. Hellman pada tahun 1976 pada papernya yang berjudul *"New Directions in Cryptography"* yang di dalamnya memperkenalkan konsep kriptografi dengan metode baru untuk mempertukarkan kunci sesi (kunci rahasia untuk komunikasi dengan menggunakan kriptografi simetri).

Adapun algoritma *Diffie Hellman* yang perlu dilakukan sebagai berikut:

a. Menentukan bilangan prima n dan bilangan bulat tak nol yang lebih kecil dari n, yaitu g. Bilangan n dan g dapat diketahui oleh pihak lain (bersifat tidak privat atau publik).
b. Menentukan sebarang bilangan bulat positif x untuk mengirim pesan dan y untuk penerima pesan. Bilangan x dan y tidak boleh diketahui oleh pihak lain (bersifat privat).
c. Pengirim pesan menghitung $X = g^x \ mod \ n$ dan penerima pesan menghitung $Y = g^x \ mod \ n$.
d. Bilangan X dan Y merupakan *shared key* yang kemudian saling bertukar. X diberikan kepada penerima pesan dan Y diberikan kepada pengirim pesan.
e. Pengirim pesan menghitung $K = Y^x \ mod \ n$ dan penerima pesan menghitung $K = X^y \ mod \ n$.

Contoh:

Diketahui dua belah pihak yang saling bertukar kunci, yaitu Alice dan Bob. Alice dan Bob menyepakati bilangan prima $n = 83$ dan $g = 2$. Kemudian langkah selanjutnya sebagai berikut:

a. Alice memilih kunci privat $x = 40$, lalu menghitung $X = g^x \ mod \ n = 2^{40} \ mod \ 83 = 41$. Alice mengirimkan hasil X kepada Bob.
b. Bob memilih kunci privat $y = 55$, lalu menghitung $Y = g^y \ mod \ n = 2^{55} \ mod \ n = 50$. Bob mengirimkan hasil Y kepada Alice.
c. Alice menghitung $K = Y^x \ mod \ n = 50^{40} \ mod \ 83 = 78$.
d. Bob menghitung $K' = X^y \ mod \ n = 41^{55} \ mod \ 86 = 78$.
e. Sehingga Alice dan Bob mendapatkan hasil kunci yang sama, yaitu $K' = 78$.

Jadi, dari perhitungan tersebut didapatkan nilai $K = K'$ yang hasilnya sama dan kunci tersebut siap digunakan untuk melakukan komunikasi dengan kriptografi simetri.

2.2 Aritmetika Modular

Aritmetika modular (*modular arithmetic*) merupakan metode aritmetika untuk menyelesaikan permasalahan terkait bilangan bulat. Aritmetika modular juga sering digunakan dalam sistem kriptografi. Operator yang digunakan pada aritmetika modular tersebut adalah mod. Operator mod disini diartikan sebagai sisa pembagian. Misalnya 41 dibagi 7 memberikan hasil 5 dan sisa 6, dimana penulisannya yaitu $41 \ mod \ 7 = 6$ (Munir, 2008).

Definisi 2.2.1 Pembagian

Misalkan $a, b \in Z$ dengan $a \neq 0$, maka dapat dikatakan bahwa a membagi b yang dapat ditulis dengan $a|b$ yang berarti $b = ak$. Notasi pada $a|b$ dapat dibaca dengan "a membagi b", "a habis dibagi b", "a pembagi b", atau "a faktor dari b".

Jika a habis dibagi dengan b dan $0 < a < b$, maka a disebut pembagi sejati dari b. Jika a tidak habis dibagi b, maka dapat kita tulis dengan $a \nmid b$ (Irawan et al., 2014).

Contoh:

1) $2|4$, karena terdapat $2 \in Z$ sehingga $4 = 2 \cdot 2$.
2) $2 \nmid 6$, karena tidak terdapat $k \in Z$ sedemikian hingga $6 = 2k$.

Teorema 2.2.1 Algoritma Pembagian

Misalkan untuk sebarang bilangan bulat a dan b dengan $a > 0$, maka terdapat bilangan bulat q dan r yang tunggal sedemikian hingga dapat dinyatakan dengan $b = qa + r, 0 \leq r < a$ (Irawan et al., 2014).

Contoh:

Misalkan untuk sebuah bilangan bulat $a = -7$ untuk $b = 1$, maka diperoleh

$$1 = 0(-7) + 1$$

Namun, jika untuk sebuah bilangan bulat $a = -7$ untuk $b = -2$, maka diperoleh

$$-2 = 1(-7) + 5$$

Definisi 2.2.2 Kongruensi

Jika sebuah bilangan bulat M dengan $M \neq 0$ membagi selisih $a - b$, maka dapat dikatakan bahwa a kongruen dengan b modulo M. Pernyataan tersebut dapat dinotasikan dengan

$$a \equiv b(mod\ M), \qquad (2.3)$$

dimana jika $M|(a-b)$. Begitu juga sebaliknya, jika bilangan bulat M dengan $M \neq 0$ tidak membagi selisih $a-b$, maka dapat dikatakan a tidak kongruen dengan b modulo M yang dapat dinotasikan dengan

$$a \not\equiv b(mod\ M), \tag{2.4}$$

dimana jika $M \nmid (a-b)$ (Irawan et al., 2014).

Contoh:

1) $23 \equiv 3\ (mod\ 5)$, karena $(23-3)$ terbagi oleh 5.
2) $12 \not\equiv 4\ (mod\ 5)$, karena $(12-4)$ tidak terbagi oleh 5.

2.3 Sistem Bilangan Biner

Bilangan biner merupakan bilangan berbasis 2 yang hanya mempunyai 2 digit yaitu 0 dan 1 (Agus dan Taufiq, 2013). Sistem bilangan biner modern ditemukan oleh Gottfreid Wilhelm Leibniz pada abad ke-17. Sistem bilangan biner juga dapat disebut dengan istilah bit atau *binary digit*. Besaran faktor pada sistem bilangan biner adalah pangkat atau kelipatan dua. Dalam komputer, pengelompokan biner selalu berjumlah 8 dengan istilah 1 Byte atau bita, dimana 1 Byte = 8 bit. Perhitungan pada biner tidak sama dengan perhitungan basis 10 *(decimal)* (Insannudin dan Fadilah, 2005).

Berikut konversi desimal ke bentuk biner 8 bit yang dapat dituliskan pada tabel berikut:

Tabel 2.3 Konversi Desimal Ke Bentuk Biner 8 Bit

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
13	00001101
14	00001110
15	00001111
16	00010000

2.4 ASCII

ASCII (*American Standart Code for Information Interchange*) adalah kode standart yang berlaku di seluruh dunia, dimana kode tersebut berupa angka yang digunakan untuk mengkodekan karakter-karakter, baik huruf, angka maupun simbol (tanda baca). ASCII saat ini merupakan salah satu standart yang banyak digunakan pada komputer dan perangkat komunikasi (Kurnia, 2013). 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, mulai dari kode 0 hingga 255 dan juga terdiri dari alfabet $a - z$ dan $A - Z$, angka $0 - 9$, beberapa tanda baca umum dan beberapa karakter kontrol.

2.5 *Finite Field*

Finite Field atau juga dikenal dengan *Galois Field* (*GF*) adalah *field* yang jumlah himpunannya berhingga atau terbatas. *Finite field* dipakai secara luas di kriptografi, misalnya sistem sandi simetri AES (*Advanced Encryption Standart*) (Sadikin, 2012).

2.5.1 Polinomial

Polinomial atau suku banyak adalah pernyataan matematis yang berhubungan dengan jumlah perkalian pangkat dalam satu atau lebih dari satu variabel dengan koefisien. Polinomial $p(x)$ berderajat n, didefinisikan dengan suatu fungsi yang berbentuk

$$p(x) = a_0 + a_1x + a_2x + \cdots + a_nx^n, \tag{2.5}$$

Dimana n merupakan orde atau derajat persamaan (Munir, 2008). a_i adalah konstanta riil, $i = 0,1,2,3, \dots, n$ dan $a_n \neq 0$. Diketahui bahwa x merupakan peubah, sedangkan $a_0, a_1, a_2, a_3, \dots, a_n$ yang secara berurutan merupakan nilai koefisien pada persamaan $x^0, x^1, x^2, x^3, \dots, x^n$.

2.5.2 Operasi Aljabar pada Polinomial

1. Penjumlahan

Hal yang perlu diperhatikan dalam operasi polinomial penjumlahan adalah pangkat polinomialnya. Terdapat 2 macam cara menjumlahkan polinomial $f(x)$ dengan $h(x)$. Jika menjumlahkan suku yang sejenis, misalkan $3x^2$ dan $5x^2$, maka hasilnya adalah $8x^2$. Sedangkan jika menjumlahkan suku yang berbeda, misalkan $3x^2$ dan $5x^3$, maka hasilnya adalah $3x^2 + 5x^3$.

2. Pengurangan

Operasi polinomial pengurangan juga perlu diperhatikan pada pangkat polinomialnya seperti halnya penjumlahan. Jika mengurangkan suku yang sejenis, misalkan $5x^2$ dan $3x^2$, maka hasilnya adalah $2x^2$. Sedangkan jika mengurangkan suku yang berbeda, misalkan $5x^2$ dan $3x^2$, maka hasilnya adalah $5x^2 - 3x^2$.

3. Perkalian

Operasi perkalian pada polinomial memiliki sifat distributif. Bentuk dari sifat distributif dapat ditulis sebagai berikut:

$$a * (b + c) = a * b + a * c, \text{ dan}$$

$$(a + b)(c + d) = ac + ad + bc + bd, \tag{2.6}$$

dimana ambil dua polinomial sebarang dengan diketahui $a, b, c,$ dan d merupakan koefisien dari polinomial. Sifat distributif pada perkalian polinomial tersebut juga berlaku terhadap operasi penjumlahan dan operasi pengurangan. Proses perkalian pada fungsi polinomial $f(x)$ dengan fungsi polinomial $h(x)$ yaitu dengan saling mengalikan suku-suku dari kedua fungsi polinomialnya.

4. Pembagian

Operasi pembagian pada polinomial biasanya menggunakan cara bersusun dan horner. Dengan menggunakan cara bersusun dan horner kita dapat menentukan hasil bagi dan sisa pada operasi polinomial. Definisi pembagi pada polinomial dapat ditulis sebagai berikut:

$$p(x) = q(x) \cdot h(x) + s(x) \tag{2.7}$$

Keterangan:

$p(x) =$ polinomial yang akan dibagi

$q(x) =$ pembagi polinomial

$h(x) =$ hasil bagi

$s(x) =$ sisa pembagian

2.5.3 Sifat Keterbagian dan Faktorisasi Polinomial

1. Sifat Keterbagian

Jika suatu polinomial berbentuk pecahan dengan derajat pembilang yang tidak lebih kecil dari penyebutnya, maka polinomial tersebut dapat disederhanakan dengan cara keduanya dibagi dengan bilangan yang sama besar. Suatu polinomial $p(x)$ dapat dibagi dengan polinomial lainnya $q(x)$ dengan derajat yang lebih kecil dan hasilnya $h(x)$ serta sisa pembagiannya adalah $s(x)$. Pernyataan tersebut dapat ditulis sebagai berikut:

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

$$h(x) = \frac{p(x)}{q(x)}\ sisa\ s(x), \text{ atau } p(x) = q(x) \cdot h(x) + s(x) \qquad (2.8)$$

2. Faktorisasi Polinomial

Faktor dari suatu polinomial dalam matematika adalah bilangan, variabel, konstanta, suku, dan koefisien yang membagi habis polinomial dalam matematika tersebut. Perhatikan bahwa setiap polinomial dalam matematika memiliki paling sedikit dua faktor yaitu bilangan 1 dan dirinya sendiri (Anton, 1987).

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

Finite field yang memiliki struktur yang paling sederhana adalah *finite field* yang nilai order nya adalah bilangan prima, dimana biasanya dinotasikan dengan $GF(p)$. Selain $GF(p)$ berbasis bilangan prima, tipe *Galois field* yang sering dipakai pada sistem kriptografi adalah $GF(p^n)$, dimana $GF(p^n)$ berdasar pada aritmetika modular polinomial $m(x)$ yang bisa ditulis sebagai berikut:

$$m(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x^0 + x_0 \qquad (2.9)$$

Polinomial $m(x)$ adalah polinomial berderajat n yang koefisiennya adalah elemen-elemen pada $GF(p^n)$. Polinomial $m(x)$ disebut dengan *irreducible polynomial*. Karakteristik *irreducible polynomial* $m(x)$ mirip dengan bilangan prima, yaitu tidak habis dibagi kecuali oleh dirinya sendiri dan 1 (Sadikin, 2012). Elemen pada $GF(p^n)$ merupakan semua polinomial yang berderajat antara 0 sampai $n-1$ dengan koefisien yang merupakan elemen pada $GF(p)$. Misalnya elemen pada $GF(p^n)$ ditulis sebagai $f(x)$, maka

$$f(x) = a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x^0 + x_0 \qquad (2.10)$$

dengan $a_i \in GF(p^n)$ dan $a_n \neq 0$.

2.5.5 Aritmetika Modulo Polinomial

Polinomial $GF(2^n)$ terdiri dari semua himpunan polinomial yang berderajat lebih kecil dari n dan terdapat dua operator, yaitu operator penjumlahan dan perkalian.

Operator penjumlahan pada $GF(2^n)$ tersebut hampir sama dengan penjumlahan polinomial biasa. Hal yang membedakan hanya pada koefisien penjumlahannya, yaitu pada $GF(2^n)$. Penjumlahan pada $GF(2^n)$ dapat dilakukan dengan operasi *xor* seperti pada Tabel 2.4 (Sadikin, 2012):

Tabel 2.4 Operasi Penjumlahan pada $GF(2^n)$

+	0	1
0	0	1
1	1	0

Sedangkan operator perkalian pada $GF(2^n)$ juga hampir sama dengan perkalian polinomial biasa, tetapi pembedanya hanya pada koefisiennya, yaitu pada $GF(2^n)$ yang dapat dituliskan pada Tabel 2.5 berikut:

Tabel 2.5 Operasi Perkalian pada $GF(2^n)$

×	0	1
0	0	0
1	0	1

Perkalian dua polinomial $f(x)$ dan $g(x)$ dilakukan dengan menjumlahkan perkalian tiap suku polinomial pertama atau $(f(x))$ dengan polinomial kedua. Setiap perkalian x^i dengan x^j didapatkan x^{i+j}. Hasil perkalian elemen $GF(2^n)$ juga menghasilkan polinomial yang berderajat lebih dari $n-1$, maka proses reduksi dengan modular polinomial taktereduksi $m(x)$ perlu diketahui (Sadikin, 2012).

Contoh:

Jika diketahui polinomial taktereduksi adalah $m(x) = x^4 + x + 1$ pada $GF(2^4)$, maka hitunglah perkalian berikut:

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

Jawab:

1. $(x^2 + x)(x + 1) = x^2(x) + x^2(1) + x(x) + x(1)$

$= x^3 + x^2 + x^2 + x$

$= x^3 + x$

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

$= x^5 + x^4 + x^2 + x$

Perhatikan hasil perkalian di atas terdapat x^5 dan x^4 yang nilainya melebihi derajat pada $GF(2^4)$, sehingga diperlukan reduksi terhadap hasil perkalian tersebut (Sadikin, 2012). Nilai polinomial taktereduksi nya, yaitu $m(x) = x^4 + x + 1$. Karena $m(x) = 0$, maka $0 = x^4 + x + 1$, sehingga didapatkan

$$x^4 = x + 1,$$

Oleh karena itu, x^4 dapat direduksi menjadi

$x^4 = 1(x^4)$

$= 1(x + 1)$

$= x + 1$

Begitu juga x^5 yang dapat direduksi menjadi

$x^5 = x(x^4)$

$= x(x + 1)$

$= x^2 + x$

2.6 Kajian Integrasi Topik dengan Al-Qur'an/Hadist

Konsep tentang ilmu kriptografi terdapat di dalam Al-Qur'an surat An-Nisa' ayat 58 yang berbunyi:

اِنَّ اللّٰهَ يَأْمُرُكُمْ اَنْ تُؤَدُّوا الْاَمٰنٰتِ اِلٰٓى اَهْلِهَاۙ وَاِذَا حَكَمْتُمْ بَيْنَ النَّاسِ اَنْ تَحْكُمُوْا بِالْعَدْلِۗ اِنَّ اللّٰهَ نِعِمَّا يَعِظُكُمْ بِهٖۗ اِنَّ اللّٰهَ كَانَ سَمِيْعًاۢ بَصِيْرًا

Artinya: "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 Maha Mendengar lagi Maha Melihat" (QS. An-Nisa':58).

Penjelasan tafsir pada surat An-Nisa' ayat 58, yaitu Allah memerintahkan kita untuk menyampaikan amanat yang benar dan kita percayai, dimana amanat tersebut dapat disampaikan kepada yang berhak menerimanya. Berdasarkan juga pada tafsir Al-Wasith, surat An-Nisa' ayat 58 di atas memiliki makna, bahwa sesungguhnya Allah memerintahkan kita untuk menyampaikan amanat atau kewajiban-kewajiban yang dipercayakan kepada seseorang atau kepada pihak yang berhak menerimanya dan apabila kamu mengadili diantara manusia, maka Allah menetapkan hukum dengan adil (Az-Zuhaili, 2013).

Hadist al-Hasan dari Samurah, disebutkan bahwa Rasulullah Saw bersabda yang artinya:

"Sampaikanlah amanat itu kepada orang yang mempercayaimu dan janganlah kamu berkhianat terhadap orang yang berkhianat kepadamu." (Hadist riwayat Imam Ahmad).

Makna dari hadist tersebut meliputi semua jenis amanat yang harus disampaikan bagi manusia (Katsir, 2003).

2.7 Kajian Topik dengan Teori Pendukung

Sejak masa pandemi covid-19 masih gencar-gencarnya, semua aktivitas masyarakat dibatasi sehingga semua kegiatan dilakukan secara online atau melalui

internet. Saat ini sering terjadi kendala dalam masalah keamanan. Utamanya dalam masalah keamanan sebuah pesan. Masalah tersebut sering dialami oleh masyarakat karena ulah pihak-pihak yang tidak berhak dan tidak bertanggung jawab atas pesan tersebut. Contoh masalah yang sering terjadi saat ini adalah pada platform WhatsApp, Instagram, Twitter, dan media sosial lainnya. Masyarakat merasa khawatir atas pesan yang akan dikirimkan setiap ingin melakukan komunikasi dengan pihak tertentu. Karena sering terjadinya pembobolan pesan sehingga pesan tersebut dapat dibaca oleh pihak lain yang tidak berhak atas pesan tersebut.

Beberapa penjelasan di atas, dapat diketahui bahwa kita haruslah mencari solusi untuk mengatasi masalah-masalah tersebut yang saat ini sedang sering terjadi dikalangan masyarakat. Salah satu solusi yang dapat dimanfaatkan adalah ilmu kriptografi. Kriptografi merupakan ilmu yang mempelajari tentang menyandikan sebuah pesan. Oleh karena itu, dengan kita manfaatkan ilmu kriptografi tersebut dapat meminimalisir dampak terjadinya masalah keamanan pesan, baik itu pembobolan pesan, maupun lainnya.

Langkah pertama dalam penerapan ilmu kriptografi adalah menentukan sebuah pesan yang akan disandikan. Selanjutnya mengubah setiap pesan tersebut menjadi bentuk-bentuk tertentu. Bentuk-bentuk yang dapat kita gunakan dalam kriptografi ada dua bentuk, yaitu bentuk desimal dan bentuk biner. Kita dapat menggunakan salah satu dari kedua bentuk tersrbut. Kemudian menentukan kunci yang akan digunakan untuk mengamankan pesan tersebut, dimana kunci tersebut akan dikalikan dengan bentuk-bentuk pada setiap pesannya. Setelah mengalikan setiap bentuk-bentuk dari pesan tersebut dengan kuncinya, maka akan didapatkan hasilnya. Oleh karena itu, dari hasil tersebut kita dapat mengubah pesan tersebut

menjadi pesan-pesan yang tidak dapat terbaca. Begitu juga untuk membaca pesan yang tidak terbaca tersebut dapat dilakukan dengan cara yang sama, yaitu dengan cara mengalikan setiap pesan yang tidak terbaca dengan kunci yang sama pada proses penyandian pesan tersebut. Sehingga pesan tersebut akan kembali menjadi pesan yang dapat dibaca.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Pada penelitian ini, jenis penelitian yang digunakan adalah penelitian kualitatif. Tujuan pada penelitian kualitatif adalah untuk menemukan ide-ide baru, wawasan baru, bahkan bisa juga menemukan sebuah teori-teori baru. Karena sifat dari penelitian kualitatif adalah eksploratif.

3.2 Pra Penelitian

Pra penelitian yang dilakukan penulis pada penelitian ini adalah menelusuri dan juga mempelajari sebuah jurnal, artikel, referensi-referensi lainnya yang berkaitan dengan *hybrid cryptography*, baik *Affine cipher* maupun *Diffie Hellman*, dan bagaimana proses penyandian sebuah pesan teks yang akan disandikan dengan bentuk polinomial. Karena pada penelitian ini penulis menggunakan algoritma *Affine cipher* dan algoritma *Diffie Hellman* berbasis *Galois field* demi menjaga tingkat keamanan pada pesan teks.

3.3 Tahapan Penelitian

Adapun tahapan penelitian yang dilakukan pada penelitian ini dibagi menjadi dua bagian, yaitu:

1. Proses Enkripsi:
    a. Menentukan nilai dari kunci a dan nilai dari kunci b.
    b. Menentukan sebuah pesan asli *P (plaintext)* yang akan digunakan pada proses penyandian pesan.
    c. Mengubah setiap pesan tersebut ke dalam bentuk-bentuk tertentu (desimal dan biner).

d. Melakukan perhitungan dengan mengalikan setiap bentuk (desimal maupun biner) pada setiap pesan dengan kunci yang telah diketahui pada rumus $C = (aP + b)\ mod\ n$ (dimana a merupakan kunci berupa polinomial yang relatif prima dengan n, b merupakan kunci berupa pergeseran dari nilai yang relatif prima dengan kunci a, dan n merupakan banyaknya karakter pada polinomial).

e. Mengubah hasil perhitungan dari setiap pesan menjadi sebuah karakter tertentu yang sesuai pada tabel ASCII.

f. Didapatkan sebuah pesan tersandi *(ciphertext)* yang telah disandikan.

2. Proses Dekripsi:

a. Menentukan nilai n dan nilai g.

b. Menentukan nilai dari sebarang bilangan bulat, baik pengirim pesan x dan penerima pesan y yang bersifat privat (tidak diketahui publik).

c. Menentukan sebuah pesan tersandi *(ciphertext)* yang akan digunakan pada proses pengembalian pesan.

d. Mengubah setiap pesan tersebut ke dalam bentuk-bentuk tertentu (desimal dan biner).

e. Melakukan perhitungan dengan rumus $X = g^x\ mod\ n$ bagi pengirim pesan dan melakukan perhitungan dengan rumus $Y = g^y\ mod\ n$ bagi penerima pesan.

f. Melakukan pertukaran kunci dari perhitungan tersebut dan melakukan perhitungan dengan rumus $K = Y^x\ mod\ n$ bagi pengirim pesan dan melakukan perhitungan dengan rumus $K' = X^y\ mod\ n$ bagi penerima pesan sehingga didapatkan hasil nilai kunci yang sama, yaitu $K = K'$.

g. Menentukan nilai invers dari kunci a dan nilai pergeseran dari kunci b.

h. Melakukan perhitungan dengan mengalikan setiap bentuk (desimal maupun biner) pada setiap pesan dengan kunci yang telah diketahui pada rumus $P = (a^{-1}C - b)\ mod\ n$.

i. Mengubah hasil perhitungan dari setiap pesan menjadi sebuah karakter tertentu yang sesuai pada tabel ASCII.

j. Didapatkan sebuah pesan asli *(plaintext)* yang telah dikembalikan.

BAB IV
HASIL DAN PEMBAHASAN

Dalam penelitian ini, perlu diperhatikan untuk mengetahui *finite field* pada himpunan polinomial pada $GF(2^4)$. Suatu *finite field* pada himpunan polinomial $GF(2^4)$ adalah $a_0 + a_1x + a_2x^2 + a_3x^3$, dimana dapat dinyatakan ke dalam bentuk a_0, a_1, a_2, a_3 seperti yang terdapat pada tabel berikut:

Tabel 4.1 Polinomial $GF(2^4)$

No	**Polinomial $GF(2^4)$**
1	0
2	1
3	x
4	x^2
5	x^3
6	$x + 1$
7	$x^2 + 1$
8	$x^2 + x$
9	$x^3 + 1$
10	$x^3 + x$
11	$x^3 + x^2$
12	$x^2 + x + 1$
13	$x^3 + x + 1$
14	$x^3 + x^2 + 1$
15	$x^3 + x^2 + x$
16	$x^3 + x^2 + x + 1$

Definisi 4.1 *Finite field* (biasa disebut *Galois field*) pada $GF(2^n)$ memiliki elemen yang dapat dinyatakan dalam bentuk polinomial, dimana bentuk umum polinomial tersebut adalah

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n,$$

dimana dalam hal ini $a_0, \dots, a_{n-1}, a_n$ adalah koefisien-koefisien polinomial dan n adalah derajat polinomial.

Contoh:

Misalkan diketahui suatu polinomial, yaitu $f(x) = 3x^6 + x^4 - 2x + 1$. Maka, dari polinomial tersebut didapatkan sebuah polinomial yang mempunyai derajat 6. ■

Polinomial taktereduksi yang digunakan untuk mereduksi polinomial pada penelitian ini dalam proses penyandian pesan dari $GF(2^4)$ adalah $m(x) = x^4 + x + 1$. Karena derajat polinomial $m(x) = 4$, maka $x^4 + x + 1 = 0$ sehingga didapatkan $x^4 = x + 1$.

Definisi 4.2 Suatu polinomial tak konstan $f(x) \in R[x]$ dikatakan taktereduksi atas R jika $f(x)$ tidak dapat dinyatakan sebagai perkalian dua polinomial $g(x), h(x) \in R[x]$ dengan derajat $(g, h) <$ derajat (f).

Contoh:

Misalkan diketahui sebuah polinomial dengan $m(x) = x^4 + x + 1$ pada $GF(2^4)$. Hitunglah perkalian dua polinomial berikut:

1. $(x^2 + x)(x^2 + 1) = x^2(x^2) + x^2(1) + x(x^2) + x(1)$
$= x^4 + x^2 + x^3 + x$

2. $(x^3 + x)(x^3 + 1) = x^3(x^3) + x^3(1) + x(x^3) + x(1)$
$= x^6 + x^3 + x^4 + x$

Karena nilai dari hasil perhitungan tersebut melebihi derajat $GF(2^4)$, maka diperlukan reduksi pada hasil perkalian tersebut untuk proses penyandian pesan. ■

Proses enkripsi pesan yang digunakan pada penelitian ini adalah algoritma *Affine cipher* dengan rumus $C = (aP + b)\ mod\ x + 1$. Kunci yang digunakan ada dua, yaitu kunci $a = x$ dan kunci $b = x^3$. Sedangkan pada proses dekripsi pesan, algoritma yang digunakan adalah algoritma *Diffie Hellman*. Hal yang perlu diperhatikan adalah sebagai berikut:

Anggaplah Alice dan Bob adalah pihak-pihak yang saling berkomunikasi. Alice dan Bob menyepakati nilai $n = x + 1$ dan $g = x^3 + x + 1$. Nilai n dan g tidak rahasia (bersifat publik). Untuk memperoleh kunci simetri K, Alice dan Bob masing-masing melakukan perhitungan sebagai berikut:

1. Alice memilih kunci privat $x = 1$ dan melakukan perhitungan $X = g^x\ mod\ n = (x^3 + x + 1)^1 = x^3 + x + 1$. Kemudian Alice mengirimkan nilai X kepada Bob.
2. Bob memilih kunci privat $y = 2$ dan melakukan perhitungan $Y = g^y\ mod\ n = (x^3 + x + 1)^2 = x^6 + 2x^4 + 2x^3 + x^2 + 2x + 1 = x^3 + 1$. Kemudian Bob mengirimkan nilai Y kepada Alice.
3. Alice menghitung dengan rumus $K = Y^x\ mod\ n = (x^3 + 1)^1 = x^3 + 1$.
4. Bob menghitung dengan rumus $K' = X^y\ mod\ n = (x^3 + x + 1)^2 = x^3 + 1$.

Sehingga dari perhitungan tersebut didapatkan hasil nilai kunci yang sama, yaitu $K = K' = x^3 + 1$ dan kunci tersebut dapat digunakan untuk melakukan komunikasi dengan kriptografi simetri.

Kriptografi simetri yang digunakan pada penelitian ini adalah *Affine cipher* dengan rumus $P = (a^{-1}C - b)\ mod\ n$. Karena dalam proses dekripsi pada *Affine cipher* menggunakan invers dari kunci a, maka didapatkan nilai $a^{-1} = x^3 + 1$.

Selanjutnya, menentukan nilai pergeseran dari kunci b dengan menggunakan rumus $(a^{-1}C - b)\ (mod\ x + 1)$ dengan perhitungan sebagai berikut:

$$\begin{aligned}(x^3 + 1)(C - x^3) &= x^3 + 1(C) - (x^3 + 1)\, x^3\ (mod\ x + 1)\\ &= x^3 + 1(C) - x^6 - x^3\ (mod\ x + 1)\\ &= x^3 + 1(C) - x^3 - x^2 - x^3\ (mod\ x + 1)\\ &= x^3 + 1(C) - 2x^3 - x^2\ (mod\ x + 1)\\ &= x^3 + 1(C) - x^2\ (mod\ x + 1)\end{aligned}$$

Jadi, didapatkan kunci yang digunakan pada proses dekripsi pesan adalah $a^{-1} = x^3 + 1$ dan $b = x^2$.

4.1 Proses Enkripsi Pesan

1. Mengkonversi Pesan Asli Menjadi Polinomial *Galois Field*

Sebelum proses penyandian dengan menggunakan polinomial *Galois field*, langkah awal yang perlu dilakukan adalah menentukan pesan asli terlebih dahulu yang selanjutnya proses penyandian pesan.

Plaintext atau pesan asli yang digunakan dalam penelitian ini adalah "*finite field*". Selanjutnya adalah mengkonversi pesan asli ke dalam bentuk biner 8 bit dengan bantuan tabel ASCII 8 bit *(American Standart Code of Information Interchange)*. Tabel ASCII 8 bit dari pesan asli tersebut dapat dituliskan sebagai berikut:

Tabel 4.2 Hasil Konversi Karakter Asli Menjadi Biner 8 Bit

No	Karakter	Biner 8 bit
1	*f*	01100110
2	*i*	01101001
3	*n*	01101110
4	*i*	01101001
5	*t*	01110100
6	*e*	01100101
7	*space*	00100000
8	*f*	01100110
9	*i*	01101001
10	*e*	01100101
11	*l*	01101100
12	*d*	01100100

Namun, pada penelitian ini menggunakan polinomial *Galois field* 16 dengan batas biner 4 bit sehingga dari tabel 8 bit di atas dapat dipecah menjadi 4 bit yang kemudian dikonversikan ke dalam bentuk polinomial *Galois field*. Bentuk polinomial *Galois field* 16 dengan biner 4 bit dapat dituliskan dengan tabel sebagai berikut:

Tabel 4.3 Hasil Konversi Biner 4 Bit Menjadi Polinomial Galois Field 16

No	**Biner 4 bit**	**Polinomial *Galois Field* 16**
1	0000	0
2	0001	1
3	0010	x
4	0100	x^2
5	1000	x^3
6	0011	$x+1$
7	0101	x^2+1
8	0110	x^2+x
9	1001	x^3+1
10	1010	x^3+x
11	1100	x^3+x^2
12	0111	x^2+x+1
13	1011	x^3+x+1
14	1101	x^3+x^2+1
15	1110	x^3+x^2+x
16	1111	x^3+x^2+x+1

Sehingga pada tabel 4.3 dapat membantu kita dalam mengkonversikan setiap pesan ke bentuk polinomial *Galois field* 16. Langkah selanjutnya adalah mengkonversi biner 4 bit pada setiap karakter pesan ke dalam bentuk polinomial *Galois field*. Sehingga dapat dituliskan dengan tabel sebagai berikut:

Tabel 4.4 Hasil Konversi Biner 4 Bit Menjadi Polinomial Galois Field

No	Karakter	Biner 4 bit	Polinomial *Galois Field*
1	f	0110 dan 0110	$x^2 + x$ dan $x^2 + x$
2	i	0110 dan 1001	$x^2 + x$ dan $x^3 + 1$
3	n	0110 dan 1110	$x^2 + x$ dan $x^3 + x^2 + x$
4	i	0110 dan 1001	$x^2 + x$ dan $x^3 + 1$
5	t	0111 dan 0100	$x^2 + x + 1$ dan x^2
6	e	0110 dan 0101	$x^2 + x$ dan $x^2 + 1$
7	$space$	0010 dan 0000	x dan 0
8	f	0110 dan 0110	$x^2 + x$ dan $x^2 + x$
9	i	0110 dan 1001	$x^2 + x$ dan $x^3 + 1$
10	e	0110 dan 0101	$x^2 + x$ dan $x^2 + 1$
11	l	0110 dan 1100	$x^2 + x$ dan $x^3 + x^2$
12	d	0110 dan 0100	$x^2 + x$ dan x^2

2. Proses Enkripsi Pesan

Sebelum melakukan proses enkripsi pesan, sebelumnya telah diketahui sebuah kunci yang akan digunakan pada proses enkripsi pesan, yaitu $a = x$ sebagai pengali dan $b = x^3$ sebagai penggeser. Proses enkripsi pesan pada *plaintext "finite field"* dengan menggunakan rumus

$$C = (aP + b)\ mod\ x + 1,$$

dapat dilakukan dengan perhitungan sebagai berikut:

1) Menentukan hasil enkripsi pada karakter f:

   a. Diketahui *plaintext* $P_1 = (x^2 + x)$.

      Sehingga dapat ditulis dengan

$$C = (x(x^2 + x) + x^3)\ mod\ x + 1$$

$$= (x^3 + x^2 + x^3)\ mod\ x + 1$$

$$= (2x^3 + x^2)\ mod\ x + 1$$

$$= x^2$$

Jadi, hasil enkripsi dari karakter f pada P_1 adalah 0100.

b. Diketahui *plaintext* $P_2 = (x^2 + x)$.

Sehingga dapat ditulis dengan

$$C = (x(x^2 + x) + x^3)\ mod\ x + 1$$

$$= (x^3 + x^2 + x^3)\ mod\ x + 1$$

$$= (2x^3 + x^2)\ mod\ x + 1$$

$$= x^2$$

Jadi, hasil enkripsi dari karakter f pada P_2 adalah 0100.

2) Menentukan hasil enkripsi pada karakter i:

a. Diketahui *plaintext* $P_1 = (x^2 + x)$.

Sehingga dapat ditulis dengan

$$C = (x(x^2 + x) + x^3)\ mod\ x + 1$$

$$= (x^3 + x^2 + x^3)\ mod\ x + 1$$

$$= (2x^3 + x^2)\ mod\ x + 1$$

$$= x^2$$

Jadi, hasil enkripsi dari karakter i pada P_1 adalah 0100.

b. Diketahui *plaintext* $P_2 = (x^3 + 1)$.

Sehingga dapat ditulis dengan

$$C = (x(x^3 + 1) + x^3)\ mod\ x + 1$$

$$= (x^4 + x + x^3)\ mod\ x + 1$$

$$= (2x + x^3 + 1)\ mod\ x + 1$$

$$= x^3 + 1$$

Jadi, hasil enkripsi dari karakter i pada P_2 adalah 1001.

3) Menentukan hasil enkripsi pada karakter n:

a. Diketahui *plaintext* $P_1 = (x^2 + x)$.

Sehingga dapat ditulis dengan

$$\begin{aligned} C &= (x(x^2 + x) + x^3) \; mod \; x + 1 \\ &= (x^3 + x^2 + x^3) \; mod \; x + 1 \\ &= (2x^3 + x^2) \; mod \; x + 1 \\ &= x^2 \end{aligned}$$

Jadi, hasil enkripsi dari karakter n pada P_1 adalah 0100.

b. Diketahui *plaintext* $P_2 = (x^3 + x^2 + x)$.

Sehingga dapat ditulis dengan

$$\begin{aligned} C &= (x(x^3 + x^2 + x) + x^3) \; mod \; x + 1 \\ &= (x^4 + x^3 + x^2 + x^3) \; mod \; x + 1 \\ &= (2x^3 + x^2 + x + 1) \; mod \; x + 1 \\ &= x^2 + x + 1 \end{aligned}$$

Jadi, hasil enkripsi dari karakter n pada P_2 adalah 0111.

4) Menentukan hasil enkripsi pada karakter i:

a. Diketahui *plaintext* $P_1 = (x^2 + x)$.

Sehingga dapat ditulis dengan

$$\begin{aligned} C &= (x(x^2 + x) + x^3) \; mod \; x + 1 \\ &= (x^3 + x^2 + x^3) \; mod \; x + 1 \\ &= (2x^3 + x^2) \; mod \; x + 1 \end{aligned}$$

$$= x^2$$

Jadi, hasil enkripsi dari karakter i pada P_1 adalah 0100.

b. Diketahui *plaintext* $P_2 = (x^3 + 1)$

Sehingga dapat dituliskan dengan

$$C = (x(x^3 + 1) + x^3)\ mod\ x + 1$$
$$= (x^4 + x + x^3)\ mod\ x + 1$$
$$= (2x + x^3 + 1)\ mod\ x + 1$$
$$= x^3 + 1$$

Jadi, hasil enkripsi dari karakter i pada P_2 adalah 1001.

5) Menentukan hasil enkripsi pada karakter t:

a. Diketahui *plaintext* $P_1 = (x^2 + x + 1)$.

Sehingga dapat ditulis dengan

$$C = (x(x^2 + x + 1) + x^3)\ mod\ x + 1$$
$$= (x^3 + x^2 + x + x^3)\ mod\ x + 1$$
$$= (2x^3 + x^2 + x)\ mod\ x + 1$$
$$= x^2 + x$$

Jadi, hasil enkripsi dari karakter t pada P_1 adalah 0110.

b. Diketahui *plaintext* $P_2 = (x^2)$.

Sehingga dapat ditulis dengan

$$C = (x(x^2) + x^3)\ mod\ x + 1$$
$$= (x^3 + x^3)\ mod\ x + 1$$
$$= (2x^3)\ mod\ x + 1$$
$$= 0$$

Jadi, hasil enkripsi dari karakter t pada P_2 adalah 0000.

6) Menentukan hasil enkripsi pada karakter e:

a. Diketahui *plaintext* $P_1 = (x^2 + x)$.

Sehingga dapat ditulis dengan

$$C = (x(x^2 + x) + x^3) \; mod \; x + 1$$
$$= (x^3 + x^2 + x^3) \; mod \; x + 1$$
$$= (2x^3 + x^2) \; mod \; x + 1$$
$$= x^2$$

Jadi, hasil enkripsi dari karakter e pada P_1 adalah 0100.

b. Diketahui *plaintext* $P_2 = (x^2 + 1)$.

Sehingga dapat ditulis dengan

$$C = (x(x^2 + 1) + x^3) \; mod \; x + 1$$
$$= (x^3 + x + x^3) \; mod \; x + 1$$
$$= (2x^3 + x) \; mod \; x + 1$$
$$= x$$

Jadi, hasil enkripsi dari karakter e pada P_2 adalah 0010.

7) Menentukan hasil enkripsi pada karakter $space$:

a. Diketahui *plaintext* $P_1 = (x)$.

Sehingga dapat ditulis dengan

$$C = (x(x) + x^3) \; mod \; x + 1$$
$$= (x^2 + x^3) \; mod \; x + 1$$
$$= x^3 + x^2$$

Jadi, hasil enkripsi dari karakter $space$ pada P_1 adalah 1100.

b. Diketahui *plaintext* $P_2 = (0)$.

Sehingga dapat ditulis dengan

$$C = (x(0) + x^3) \; mod \; x + 1$$
$$= (0 + x^3) \; mod \; x + 1$$
$$= x^3$$

Jadi, hasil enkripsi dari karakter $space$ pada P_2 adalah 1000.

8) Menentukan hasil enkripsi pada karakter f:

a. Diketahui *plaintext* $P_1 = (x^2 + x)$.

Sehingga dapat ditulis dengan

$$C = (x(x^2 + x) + x^3) \; mod \; x + 1$$
$$= (x^3 + x^2 + x^3) \; mod \; x + 1$$
$$= (2x^3 + x^2) \; mod \; x + 1$$
$$= x^2$$

Jadi, hasil enkripsi dari karakter f pada P_1 adalah 0100.

b. Diketahui *plaintext* $P_2 = (x^2 + x)$.

Sehingga dapat ditulis dengan

$$C = (x(x^2 + x) + x^3) \; mod \; x + 1$$
$$= (x^3 + x^2 + x^3) \; mod \; x + 1$$
$$= (2x^3 + x^2) \; mod \; x + 1$$
$$= x^2$$

Jadi, hasil enkripsi dari karakter f pada P_2 adalah 0100.

9) Menentukan hasil enkripsi pada karakter i:

a. Diketahui *plaintext* $P_1 = (x^2 + x)$.

Sehingga dapat ditulis dengan

$$C = (x(x^2 + x) + x^3) \; mod \; x + 1$$
$$= (x^3 + x^2 + x^3) \; mod \; x + 1$$
$$= (2x^3 + x^2) \; mod \; x + 1$$
$$= x^2$$

Jadi, hasil enkripsi dari karakter i pada P_1 adalah 0100.

b. Diketahui *plaintext* $P_2 = (x^3 + 1)$.

Sehingga dapat ditulis dengan

$$C = (x(x^3 + 1) + x^3) \; mod \; x + 1$$
$$= (x^4 + x + x^3) \; mod \; x + 1$$
$$= (2x + x^3 + 1) \; mod \; x + 1$$
$$= x^3 + 1$$

Jadi, hasil enkripsi dari karakter i pada P_2 adalah 1001.

10) Menentukan hasil enkripsi pada karakter e:

a. Diketahui *plaintext* $P_1 = (x^2 + x)$.

Sehingga dapat ditulis dengan

$$C = (x(x^2 + x) + x^3) \; mod \; x + 1$$
$$= (x^3 + x^2 + x^3) \; mod \; x + 1$$
$$= (2x^3 + x^2) \; mod \; x + 1$$
$$= x^2$$

Jadi, hasil enkripsi dari karakter e pada P_1 adalah 0100.

b. Diketahui *plaintext* $P_2 = (x^2 + 1)$.

Sehingga dapat ditulis dengan

$$C = (x(x^2 + 1) + x^3) \; mod \; x + 1$$
$$= (x^3 + x + x^3) \; mod \; x + 1$$
$$= (2x^3 + x) \; mod \; x + 1$$
$$= x$$

Jadi, hasil enkripsi dari karakter e pada P_2 adalah 0010.

11) Menentukan hasil enkripsi pada karakter l:

a. Diketahui *plaintext* $P_1 = (x^2 + x)$.

Sehingga dapat ditulis dengan

$$C = (x(x^2 + x) + x^3) \; mod \; x + 1$$
$$= (x^3 + x^2 + x^3) \; mod \; x + 1$$
$$= (2x^3 + x^2) \; mod \; x + 1$$
$$= x^2$$

Jadi, hasil enkripsi dari karakter l pada P_1 adalah 0100.

b. Diketahui *plaintext* $P_2 = (x^3 + x^2)$.

Sehingga dapat ditulis dengan

$$C = (x(x^3 + x^2) + x^3) \; mod \; x + 1$$
$$= (x^4 + x^3 + x^3) \; mod \; x + 1$$
$$= (2x^3 + x + 1) \; mod \; x + 1$$
$$= x + 1$$

Jadi, hasil enkripsi dari karakter l pada P_2 adalah 0011.

12) Menentukan hasil enkripsi pada karakter d:

a. Diketahui *plaintext* $P_1 = (x^2 + x)$.

Sehingga dapat ditulis dengan

$$\begin{aligned} C &= (x(x^2 + x) + x^3) \; mod \; x + 1 \\ &= (x^3 + x^2 + x^3) \; mod \; x + 1 \\ &= (2x^3 + x^2) \; mod \; x + 1 \\ &= x^2 \end{aligned}$$

Jadi, hasil enkripsi dari karakter d pada P_1 adalah 0100.

b. Diketahui *plaintext* $P_2 = (x^2)$.

Sehingga dapat ditulis dengan

$$\begin{aligned} C &= (x(x^2) + x^3) \; mod \; x + 1 \\ &= (x^3 + x^3) \; mod \; x + 1 \\ &= 0 \end{aligned}$$

Jadi, hasil enkripsi dari karakter d pada P_2 adalah 0000.

c. Mengkonversikan Hasil *Ciphertext* Polinomial ke Bentuk Karakter

Setelah melakukan perhitungan pada *plaintext* di atas, langkah selanjutnya adalah menggabungkan setiap biner yang sudah dihitung menjadi biner 8 bit dan mengkonversikannya ke dalam bentuk karakter seperti pada tabel berikut:

Tabel 4.5 Hasil Konversi Hasil Enkripsi Menjadi Karakter pada Tabel ASCII

No	Polinomial	Biner 4 bit	Biner 8 Bit	Karakter
1	x^2 dan x^2	0100 dan 0100	01000100	*D*
2	x^2 dan x^3+1	0100 dan 1001	01001001	*I*
3	x^2 dan x^2+x+1	0100 dan 0111	01000111	*G*
4	x^2 dan x^3+1	0100 dan 1001	01001001	*I*
5	x^2+x dan 0	0110 dan 0000	01100000	`
6	x^2 dan x	0100 dan 0010	01000010	*B*
7	x^3+x^2 dan x^3	1100 dan 1000	11001000	≫
8	x^2 dan x^2	0100 dan 0100	01000100	*D*
9	x^2 dan x^3+1	0100 dan 1001	01001001	*I*
10	x^2 dan x	0100 dan 0010	01000010	*B*
11	x^2 dan $x+1$	0100 dan 0011	01000011	*C*
12	x^2 dan 0	0100 dan 0000	01000000	*@*

Jadi, proses di atas dapat disimpulkan bahwa hasil enkripsi dari pesan yang sudah disandikan atau *ciphertext* adalah "*DIGI`B≫DIBC@"*.

4.2 Proses Dekripsi Pesan

1. Mengkonversikan Karakter Menjadi Polinomial *Galois Field*

Langkah pertama yang perlu dilakukan dalam proses dekripsi pesan adalah mengkonversi simbol menjadi bentuk biner 8 bit sesuai dengan tabel ASCII. Berikut bentuk biner 8 bit dari tiap simbol atau *ciphertext* nya:

Tabel 4.6 Hasil Konversi Karakter Menjadi Biner 8 Bit

No	Karakter	Biner 8 bit
1	*D*	01000100
2	*I*	01001001
3	*G*	01000111
4	*I*	01001001
5	`	01100000
6	*B*	01000010
7	≫	11001000
8	*D*	01000100
9	*I*	01001001
10	*B*	01000010
11	*C*	01000011
12	@	01000000

Setelah kita dapatkan bentuk biner 8 bit dari setiap karakter tersebut, selanjutnya adalah mengkonversi bentuk biner 4 bit (pecahan dari bentuk biner 8 bit) ke dalam bentuk polinomial *Galois field* seperti pada tabel berikut:

Tabel 4.7 Hasil Konversi Biner 4 Bit Menjadi Polinomial Galois Field

No	Karakter	Biner 4 bit	Polinomial *Galois Field*
1	*D*	0100 dan 0100	x^2 dan x^2
2	*I*	0100 dan 1001	x^2 dan $x^3 + 1$
3	*G*	0100 dan 0111	x^2 dan $x^2 + x + 1$
4	*I*	0100 dan 1001	x^2 dan $x^3 + 1$
5	`	0110 dan 0000	$x^2 + x$ dan 0
6	*B*	0100 dan 0010	x^2 dan x
7	≫	1100 dan 1000	$x^3 + x^2$ dan x^3
8	*D*	0100 dan 0100	x^2 dan x^2
9	*I*	0100 dan 1001	x^2 dan $x^3 + 1$
10	*B*	0100 dan 0010	x^2 dan x
11	*C*	0100 dan 0011	x^2 dan $x + 1$
12	@	0100 dan 0000	x^2 dan 0

2. Proses Dekripsi Pesan

Dalam proses dekripsi ini, kunci yang digunakan adalah invers dari kunci a, yaitu $a^{-1} = x^3 + 1$ dan pergeseran dari kunci b, yaitu $b = x^2$. Proses dekripsi pesan pada *ciphertext "DIGI`B≫DIBC@"* dengan menggunakan rumus

$$P = (a^{-1}C - b)\ mod\ x + 1,$$

dapat dilakukan dengan perhitungan sebagai berikut:

1) Menentukan hasil dekripsi pada karakter *D*:

a. Diketahui *ciphertext* $C_1 = (x^2)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2) - x^2)\ mod\ x + 1$$
$$= (x^5 + x^2 - x^2)\ mod\ x + 1$$
$$= x^2 + x$$

Jadi, hasil dekripsi dari karakter *D* pada C_1 adalah 0110.

b. Diketahui *ciphertext* $C_2 = (x^2)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2) - x^2) \; mod \; x + 1$$
$$= (x^5 + x^2 - x^2) \; mod \; x + 1$$
$$= x^2 + x$$

Jadi, hasil dekripsi dari karakter *D* pada C_2 adalah 0110.

2) Menentukan hasil dekripsi pada karakter *I*:

a. Diketahui *ciphertext* $C_1 = (x^2)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2) - x^2) \; mod \; x + 1$$
$$= (x^5 + x^2 - x^2) \; mod \; x + 1$$
$$= x^2 + x$$

Jadi, hasil dekripsi dari karakter *I* pada C_1 adalah 0110.

b. Diketahui *ciphertext* $C_2 = (x^3 + 1)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^3 + 1) - x^2) \; mod \; x + 1$$
$$= (x^6 + x^3 + x^3 + 1 - x^2) \; mod \; x + 1$$
$$= (2x^3 + 0 + x^3 + 1) \; mod \; x + 1$$
$$= x^3 + 1$$

Jadi, hasil dekripsi dari karakter *I* pada C_2 adalah 1001.

3) Menentukan hasil dekripsi pada karakter *G*:

a. Diketahui *ciphertext* $C_1 = (x^2)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2) - x^2) \; mod \; x + 1$$
$$= (x^5 + x^2 - x^2) \; mod \; x + 1$$
$$= x^2 + x$$

Jadi, hasil dekripsi dari karakter *G* pada C_1 adalah 0110.

b. Diketahui *ciphertext* $C_2 = (x^2 + x + 1)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2 + x + 1) - x^2) \; mod \; x + 1$$
$$= (x^5 + x^4 + x^3 + x^2 + x + 1 - x^2) \; mod \; x$$
$$= (2x + 0 + x^3 + x^2 + x) \; mod \; x + 1$$
$$= x^3 + x^2 + x$$

Jadi, hasil dekripsi dari karakter *G* pada C_2 adalah 1110.

4) Menentukan hasil dekripsi pada karakter *I*:

a. Diketahui *ciphertext* $C_1 = (x^2)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2) - x^2) \; mod \; x + 1$$
$$= (x^5 + x^2 - x^2) \; mod \; x + 1$$
$$= x^2 + x$$

Jadi, hasil dekripsi dari karakter *I* pada C_1 adalah 0110.

b. Diketahui *ciphertext* $C_2 = (x^3 + 1)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^3 + 1) - x^2) \; mod \; x + 1$$
$$= (x^6 + x^3 + x^3 + 1 - x^2) \; mod \; x + 1$$
$$= (2x^3 + 0 + x^3 + 1) \; mod \; x + 1$$
$$= x^3 + 1$$

Jadi, hasil dekripsi dari karakter *I* pada C_2 adalah 1001.

5) Menentukan hasil dekripsi pada karakter `:

a. Diketahui *ciphertext* $C_1 = (x^2 + x)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2 + x) - x^2) \; mod \; x + 1$$
$$= (x^5 + x^4 + x^2 + x - x^2) \; mod \; x + 1$$
$$= (2x + 0 + x^2 + x + 1) \; mod \; x + 1$$
$$= x^2 + x + 1$$

Jadi, hasil dekripsi dari karakter ` pada C_1 adalah 0111.

b. Diketahui *ciphertext* $C_2 = (0)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(0) - x^2) \; mod \; x + 1$$
$$= (0 + 0 - x^2) \; mod \; x + 1$$
$$= -x^2$$

Jadi, hasil dekripsi dari karakter ` pada C_2 adalah 0100.

6) Menentukan hasil dekripsi pada karakter *B*:

a. Diketahui *ciphertext* $C_1 = (x^2)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2) - x^2) \; mod \; x + 1$$
$$= (x^5 + x^2 - x^2) \; mod \; x + 1$$
$$= x^2 + x$$

Jadi, hasil dekripsi dari karakter *B* pada C_1 adalah 0110.

b. Diketahui *ciphertext* $C_2 = (x)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x) - x^2) \; mod \; x + 1$$
$$= (x^4 + x - x^2) \; mod \; x + 1$$
$$= (2x + 1 - x^2) \; mod \; x + 1$$
$$= -x^2 + 1$$

Jadi, hasil dekripsi dari karakter *B* pada C_2 adalah 0101.

7) Menentukan hasil dekripsi pada karakter ≫:

a. Diketahui *ciphertext* $C_1 = (x^3 + x^2)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^3 + x^2) - x^2) \; mod \; x + 1$$
$$= (x^6 + x^5 + x^3 + x^2 - x^2) \; mod \; x + 1$$
$$= (2x^3 + 2x^2 + 0 + x) \; mod \; x + 1$$
$$= x$$

Jadi, hasil dekripsi dari karakter ≫ pada C_1 adalah 0010.

b. Diketahui *ciphertext* $C_2 = (x^3)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^3) - x^2) \; mod \; x + 1$$
$$= (x^6 + x^3 - x^2) \; mod \; x + 1$$
$$= (2x^3 + 0) \; mod \; x + 1$$
$$= 0$$

Jadi, hasil dekripsi dari karakter ≫ pada C_2 adalah 0000.

8) Menentukan hasil dekripsi pada karakter *D*:

a. Diketahui *ciphertext* $C_1 = (x^2)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2) - x^2) \; mod \; x + 1$$
$$= (x^5 + x^2 - x^2) \; mod \; x + 1$$
$$= x^2 + x$$

Jadi, hasil dekripsi dari karakter *D* pada C_1 adalah 0110.

b. Diketahui *ciphertetxt* $C_2 = (x^2)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2) - x^2) \; mod \; x + 1$$
$$= (x^5 + x^2 - x^2) \; mod \; x + 1$$
$$= x^2 + x$$

Jadi, hasil dekripsi dari karakter *D* pada C_2 adalah 0110.

9) Menentukan hasil dekripsi pada karakter *I*:

a. Diketahui *ciphertext* $C_1 = (x^2)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2) - x^2)\ mod\ x + 1$$
$$= (x^5 + x^2 - x^2)\ mod\ x + 1$$
$$= x^2 + x$$

Jadi, hasil dekripsi dari karakter *I* pada C_1 adalah 0110.

b. Diketahui *ciphertext* $C_2 = (x^3 + 1)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^3 + 1) - x^2)\ mod\ x + 1$$
$$= (x^6 + x^3 + x^3 + 1 - x^2)\ mod\ x + 1$$
$$= (2x^3 + 0 + x^3 + 1)\ mod\ x + 1$$
$$= x^3 + 1$$

Jadi, hasil dekripsi dari karakter *I* pada C_2 adalah 1001.

10) Menentukan hasil dekripsi pada karakter *B*:

a. Diketahui *ciphertetxt* $C_1 = (x^2)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2) - x^2)\ mod\ x + 1$$
$$= (x^5 + x^2 - x^2)\ mod\ x + 1$$
$$= x^2 + x$$

Jadi, hasil dekripsi dari karakter *B* pada C_1 adalah 0110.

b. Diketahui *ciphertetxt* $C_2 = (x)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x) - x^2) \; mod \; x + 1$$
$$= (x^4 + x - x^2) \; mod \; x + 1$$
$$= (2x + 1 - x^2) \; mod \; x + 1$$
$$= -x^2 + 1$$

Jadi, hasil dekripsi dari karakter *B* pada C_2 adalah 0101.

11) Menentukan hasil dekripsi pada karakter *C*:

a. Diketahui *ciphertetxt* $C_1 = (x^2)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2) - x^2) \; mod \; x + 1$$
$$= (x^5 + x^2 - x^2) \; mod \; x + 1$$
$$= x^2 + x$$

Jadi, hasil dekripsi dari karakter *C* pada C_1 adalah 0110.

b. Diketahui *ciphertext* $C_2 = (x + 1)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x + 1) - x^2) \; mod \; x + 1$$
$$= (x^4 + x^3 + x + 1 - x^2) \; mod \; x + 1$$
$$= (2x + 2 + x^3 - x^2) \; mod \; x + 1$$
$$= x^3 - x^2$$

Jadi, hasil dekripsi dari karakter *C* pada C_2 adalah 1100.

12) Menentukan hasil dekripsi pada karakter @:

a. Diketahui *ciphertext* $C_1 = (x^2)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(x^2) - x^2) \; mod \; x + 1$$
$$= (x^5 + x^2 - x^2) \; mod \; x + 1$$
$$= x^2 + x$$

Jadi, hasil dekripsi dari karakter @ pada C_1 adalah 0110.

b. Diketahui *ciphertetxt* $C_2 = (0)$.

Sehingga dapat ditulis dengan

$$P = (x^3 + 1(0) - x^2) \; mod \; x + 1$$
$$= (0 + 0 - x^2) \; mod \; x + 1$$
$$= -x^2$$

Jadi, hasil dekripsi dari karakter @ pada C_2 adalah 0100.

3. Mengkonversikan Hasil *Plaintext* Polinomial ke Dalam Karakter

Setelah perhitungan di atas diketahui, proses selanjutnya adalah menggabungkan setiap bentuk biner menjadi bentuk biner 8 bit dan mengkonversikannya ke bentuk karakter sehingga kita dapat mengetahui pesan asli yang telah disandikan tersebut. Hasil perhitungan tersebut dalam dituliskan pada tabel sebagai berikut:

Tabel 4.8 Hasil Konversi Hasil Dekripsi Menjadi Karakter pada Tabel ASCII

No	Polinomial	Biner 4 bit	Biner 8 Bit	Simbol
1	$x^2 + x$ dan $x^2 + x$	0110 dan 0110	01100110	f
2	$x^2 + x$ dan $x^3 + 1$	0110 dan 1001	01101001	i
3	$x^2 + x$ dan $x^3 + x^2 + x$	0110 dan 1110	01101110	n
4	$x^2 + x$ dan $x^3 + 1$	0110 dan 1001	01101001	i
5	$x^2 + x + 1$ dan x^2	0111 dan 0100	01110100	t
6	$x^2 + x$ dan $x^2 + 1$	0110 dan 0101	01100101	e
7	x dan 0	0010 dan 0000	00100000	$space$
8	$x^2 + x$ dan $x^2 + x$	0110 dan 0110	01100110	f
9	$x^2 + x$ dan $x^3 + 1$	0110 dan 1001	01101001	i
10	$x^2 + x$ dan $x^2 + 1$	0110 dan 0101	01100101	e
11	$x^2 + x$ dan $x^3 + x^2$	0110 dan 1100	01101100	l
12	$x^2 + x$ dan x^2	0110 dan 0100	01100100	d

Jadi, dari proses perhitungan di atas dapat disimpulkan bahwa hasil dari proses dekripsi pesan asli atau *plaintext* adalah "*finite field*".

4.3 Pembuktian Algoritma *Affine Cipher* dan *Diffie Hellman*

Adapun pembuktian algoritma yang digunakan pada penelitian ini adalah sebagai berikut:

1. *Affine Cipher*

$->\quad C \equiv (aP + b)\ mod\ n$ (enkripsi *Affine cipher*)

$->\quad aP + b \equiv C\ mod\ n$ (bersifat komutatif)

$->\quad aP + b - b \equiv C - b\ mod\ n$ (bersifat invers penjumlahan)

$->\quad aP \equiv C - b\ mod\ n$

$->\quad a^{-1}aP \equiv a^{-1}(C - b)\ mod\ n$ (bersifat identitas)

$->\quad P \equiv (a^{-1}C - b)\ mod\ n$ (dekripsi *Affine cipher*)

$->$ $P \equiv (a^{-1}C - b)\ mod\ n$ (dekripsi *Affine cipher*)

$->$ $aP \equiv a^{-1}a(C - b)\ mod\ n$ (bersifat identitas)

$->$ $aP \equiv C - b\ mod\ n$

$->$ $C - b \equiv aP\ mod\ n$ (bersifat komutatif)

$->$ $C - b + b \equiv aP + b\ mod\ n$ (bersifat invers penjumlahan)

$->$ $C \equiv (aP + b)\ mod\ n$ (enkripsi *Affine cipher*)

Jadi, terbukti bahwa dari enkripsi *Affine cipher* dan dekripsi *Affine cipher* dapat kembali ke bentuk semula. ■

2. *Diffie Hellman*

Diketahui bahwa $X = g^x\ mod\ n$ dan $Y = g^y\ mod\ n$. Sehingga didapatkan

$K = Y^x\ mod\ n$ (algoritma *Diffie Hellman*)

$K = g^{xy}\ mod\ n$

dan

$K' = X^y\ mod\ n$ (algoritma *Diffie Hellman*)

$K' = g^{xy}\ mod\ n$

Jadi, terbukti bahwa nilai $K = K' = g^{xy}\ mod\ n$. ■

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan yang telah dilakukan sebelumnya, maka didapatkan sebuah kesimpulan sebagai berikut:

1. Terdapat 3 proses inti dalam melakukan enkripsi pesan dengan polinomial *Galois field* menggunakan algoritma *Affine cipher*, yaitu langkah pertama mengkonversikan setiap karakter pesan teks menjadi bentuk polinomial dengan bantuan bilangan biner, kemudian langkah kedua adalah melakukan perhitungan dengan menggunakan rumus $C = (aP + b)\ mod\ n$ (dimana a merupakan kunci berupa polinomial yang relatif prima dengan n, b merupakan kunci berupa pergeseran dari nilai yang relatif prima dengan kunci a, dan n merupakan banyaknya karakter pada polinomial) yang dimana diketahui kunci $a = x$ dan kunci $b = x^3$. Langkah terakhir adalah mengkonversikan hasil perhitungan dari setiap karakter pesan teks menjadi karakter sehingga didapatkan sebuah karakter pesan yang tersandi.
2. Terdapat 3 proses inti dalam melakukan dekripsi pesan dengan polinomial *Galois field* menggunakan algoritma *Diffie Hellman*, yaitu langkah pertama mencari nilai dari kunci simetri K, yaitu dengan menentukan nilai n, g, kunci privat x, y, dan melakukan perhitungan dengan rumus $X = g^x\ mod\ n$ dan $Y = g^y\ mod\ n$, dimana diketahui $g = x^3 + x + 1$ sehingga didapatkan nilai kunci simetri K yang dapat digunakan untuk komunikasi dengan kriptografi kunci simetri *(Affine cipher)*. Langkah kedua adalah melakukan perhitungan dengan menggunakan rumus $P = (a^{-1}C - b)\ mod\ n$ yang dimana diketahui

kunci $a^{-1} = x^3 + 1$ dan pergeseran kunci $b = x^2$. Langkah yang terakhir adalah mengkonversikan hasil perhitungan dari setiap karakter pesan teks menjadi karakter sehingga didapatkan sebuah karakter pesan yang dapat dibaca.

5.2 Saran untuk Penelitian Lanjutan

Berdasarkan penelitian yang telah dilakukan di atas, maka saran peneliti yang dapat dilakukan selanjutnya adalah:

1. Dapat membuat penyelesaian *hybrid cryptography* dengan menggunakan sebuah pemrograman, baik dengan algoritma yang telah dibahas maupun dengan algoritma lainnya.
2. Dapat membandingkan kunci yang digunakan dengan algoritma lain yang dimana lebih efektif untuk digunakan dengan menggunakan polinomial *Galois field*.
3. Dapat menggunakan polinomial dengan variabel dan koefisien yang lebih tinggi (pada $GF(p^n)$).

DAFTAR PUSTAKA

Agus, T. H. dan Taufiq, L. A. (2013). *Sistem Komputer*. Jakarta.

Ahirwal, R. R., & Ahke, M. (2013). *Elliptic Curve Diffie-Hellman Key Exchange Algorithm for Securing Hypertext Information on Wide Area Network*. *International Journal of Computer Science and Information Technologies*, 4(2), 363-368.

Al-Qur'an dan Terjemahnya. (2019). Kementrian Agama RI.

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

Anton, H. dan Rorres, C. 1998. *Penerapan Aljabar Linear*. Jakarta: Erlangga.

Ariyus, D. 2006. *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu.

Aulia, R., Zakir, A., & Purwanto, D., A. 2018. *Penerapan Kombinasi Algoritma Base64 Dan Rot47 Untuk Enkripsi Database Pasien Rumah Sakit Jiwa Prof. Dr. Muhammad ildrem*. InfoTekJar J. Nas. Inform. dan Teknol. Jar., vol. 2, no. 2, pp. 146–151.

Az-Zuhaili, W. 2013. Tafsir Al-Wasith (Al-Qashash-An-Naas). Jakarta: Gema Insani.

Diffie, W. dan E Hellman, M. 1976. *New Directions in Cryptography*. IEEE Trans. Info. Theory IT-22.

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

Insannudin, E. dan Fadilah, N. 2005. *Modifikasi Affine Cipher dan Vigenere Cipher dengan Menggunakan N Bit.*

Irawan, W. H., Hijriyah, N., & Habibi, A. R. 2014. *Pengantar Teori Bilangan*. UIN Malang Press.

Irawanto, Bambang. 2001. *Galois Field*. Tesis Pasca Sarjana, Universitas Gajah Mada.

Juliandi, P. B. dan Kusumastuti, N. 2013. *Kriptografi Klasik dengan Metode Modifikasi Affine Cipher yang Diperkuat dengan Vigenere Cipher*. Bulletin Ilmiah Matematika Statistik, Vol. 2, Pp. 87-92.

Katsir, I. 2003. *Terjemah Tafsir Ibnu Katsir*, Jilid 2. Jakarta: Pustaka Imam Syafi'i.

Komarudin. 2013. *Sistem Keamanan Web Dengan Menggunakan Kriptografi Message Digest 5/Md5 Pada Koperasi Mitra Sejahtera Bandung*. Vol. 7, No. 1. STMIK Mardira Indonesia.

Kurnia, D. A. 2013. *Optimasi Konversi String Biner Hasil Least Significant Bit Steganography*.

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

Munir, R. 2019. *Kriptografi*. Bandung: Informatika Bandung.

Sadikin, R. 2012. *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: C.V. ANDI OFFSET.

Saropah. 2008. *Akar-Akar Polinomial Separable Sebagai Pembentuk Perluasan Normal Pada Ring Modulo*. Malang: UIN Maulana Malik Ibrahim.

LAMPIRAN

Lampiran 1 Tabel ASCII

No	Biner	Karakter
0	0000 0000	NUL
1	0000 0001	SOH
2	0000 0010	STX
3	0000 0011	ETX
4	0000 0100	EOT
5	0000 0101	ENQ
6	0000 0110	ACK
7	0000 0111	BEL
8	0000 1000	BS
9	0000 1001	HT
10	0000 1010	LF/NL
11	0000 1011	VT
12	0000 1100	FF
13	0000 1101	CR
14	0000 1110	SO
15	0000 1111	SI
16	0001 0000	DLE
17	0001 0001	DC1
18	0001 0010	DC2
19	0001 0011	DC3
20	0001 0100	DC4
21	0001 0101	NAK
22	0001 0110	SYN
23	0001 0111	ETB
24	0001 1000	CAN
25	0001 1001	EM
26	0001 1010	SUB
27	0001 1011	ESC
28	0001 1100	FS
29	0001 1101	GS
30	0001 1110	RS
31	0001 1111	US
32	0010 0000	space
33	0010 0001	!
34	0010 0010	"
35	0010 0011	#

No	Biner	Karakter
36	0010 0100	$
37	0010 0101	%
38	0010 0110	&
39	0010 0111	'
40	0010 1000	(
41	0010 1001	)
42	0010 1010	*
43	0010 1011	+
44	0010 1100	,
45	0010 1101	-
46	0010 1110	.
47	0010 1111	/
48	0011 0000	0
49	0011 0001	1
50	0011 0010	2
51	0011 0011	3
52	0011 0100	4
53	0011 0101	5
54	0011 0110	6
55	0011 0111	7
56	0011 1000	8
57	0011 1001	9
58	0011 1010	:
59	0011 1011	;
60	0011 1100	<
61	0011 1101	=
62	0011 1110	>
63	0011 1111	?
64	0100 0000	@
65	0100 0001	A
66	0100 0010	B
67	0100 0011	C
68	0100 0100	D
69	0100 0101	E
70	0100 0110	F
71	0100 0111	G

No	Biner	Karakter
72	0100 1000	H
73	0100 1001	I
74	0100 1010	J
75	0100 1011	K
76	0100 1100	L
77	0100 1101	M
78	0100 1110	N
79	0100 1111	O
80	0101 0000	P
81	0101 0001	Q
82	0101 0010	R
83	0101 0011	S
84	0101 0100	T
85	0101 0101	U
86	0101 0110	V
87	0101 0111	W
88	0101 1000	X
89	0101 1001	Y
90	0101 1010	Z
91	0101 1011	[
92	0101 1100	\
93	0101 1101	]
94	0101 1110	^
95	0101 1111	_
96	0110 0000	`
97	0110 0001	a
98	0110 0010	b
99	0110 0011	c
100	0110 0100	d
101	0110 0101	e
102	0110 0110	f
103	0110 0111	g
104	0110 1000	h
105	0110 1001	i
106	0110 1010	j
107	0110 1011	k
108	0110 1100	l
109	0110 1101	m
110	0110 1110	n
111	0110 1111	o

No	Biner	Karakter
112	0111 0000	p
113	0111 0001	q
114	0111 0010	r
115	0111 0011	s
116	0111 0100	t
117	0111 0101	u
118	0111 0110	v
119	0111 0111	w
120	0111 1000	x
121	0111 1001	y
122	0111 1010	z
123	0111 1011	{
124	0111 1100	|
125	0111 1101	}
126	0111 1110	~
127	0111 1111	DEL
128	1000 0000	Ä
129	1000 0001	Å
130	1000 0010	Ç
131	1000 0011	É
132	1000 0100	Ñ
133	1000 0101	Ö
134	1000 0110	Ü
135	1000 0111	á
136	1000 1000	à
137	1000 1001	â
138	1000 1010	ä
139	1000 1011	ã
140	1000 1100	å
141	1000 1101	ç
142	1000 1110	é
143	1000 1111	è
144	1001 0000	ê
145	1001 0001	ë
146	1001 0010	í
147	1001 0011	ì
148	1001 0100	î
149	1001 0101	ï
150	1001 0110	ñ
151	1001 0111	ó

No	Biner	Karakter
152	1001 1000	ò
153	1001 1001	Ô
154	1001 1010	ö
155	1001 1011	õ
156	1001 1100	ú
157	1001 1101	ù
158	1001 1110	û
159	1001 1111	ü
160	1010 0000	†
161	1010 0001	°
162	1010 0010	¢
163	1010 0011	£
164	1010 0100	§
165	1010 0101	•
166	1010 0110	¶
167	1010 0111	ß
168	1010 1000	®
169	1010 1001	©
170	1010 1010	™
171	1010 1011	´
172	1010 1100	¨
173	1010 1101	≠
174	1010 1110	Æ
175	1010 1111	Ø
176	1011 0000	∞
177	1011 0001	±
178	1011 0010	≤
179	1011 0011	≥
180	1011 0100	¥
181	1011 0101	µ
182	1011 0110	∂
183	1011 0111	∑
184	1011 1000	∏
185	1011 1001	π
186	1011 1010	∫
187	1011 1011	ª
188	1011 1100	º
189	1011 1101	Ω
190	1011 1110	æ

No	Biner	Karakter
191	1011 1111	ø
192	1100 0000	¿
193	1100 0001	¡
194	1100 0010	¬
195	1100 0011	√
196	1100 0100	*ƒ*
197	1100 0101	≈
198	1100 0110	Δ
199	1100 0111	«
200	1100 1000	»
201	1100 1001	…
202	1100 1010	.
203	1100 1011	À
204	1100 1100	Ã
205	1100 1101	Õ
206	1100 1110	Œ
207	1100 1111	œ
208	1101 0000	–
209	1101 0001	—
210	1101 0010	“
211	1101 0011	”
212	1101 0100	‘
213	1101 0101	’
214	1101 0110	÷
215	1101 0111	◊
216	1101 1000	ÿ
217	1101 1001	Ÿ
218	1101 1010	⁄
219	1101 1011	¤
220	1101 1100	‹
221	1101 1101	›
222	1101 1110	fi
223	1101 1111	fl
224	1110 0000	‡
225	1110 0001	·
226	1110 0010	‚
227	1110 0011	„
228	1110 0100	‰
229	1110 0101	Â

No	Biner	Karakter
230	1110 0110	Ê
231	1110 0111	Á
232	1110 1000	Ë
233	1110 1001	È
234	1110 1010	Í
235	1110 1011	Î
236	1110 1100	Ï
237	1110 1101	Ì
238	1110 1110	Ó
239	1110 1111	Ô
240	1111 0000	□
241	1111 0001	Ò
242	1111 0010	Ú
243	1111 0011	Û
244	1111 0100	Ù
245	1111 0101	ı
246	1111 0110	ˆ
247	1111 0111	˜
248	1111 1000	¯
249	1111 1001	˘
250	1111 1010	˙
251	1111 1011	˚
252	1111 1100	¸
253	1111 1101	˝
254	1111 1110	˛
255	1111 1111	

RIWAYAT HIDUP

Muhammad Al Himni Abdil Barr dilahirkan di Banyuwangi pada tanggal 1 Desember 1999. Nama panggilan Himni, tinggal di Jalan Kalilo No. 101 b RT/RW 005/002 Kelurahan Pengantigan, Kabupaten Banyuwangi, merupakan anak satu-satunya dari pasangan Bapak Isnaini dan Ibu Ida Fitriyah.

Penulis telah menempuh pendidikan formal mulai dari TK Islam Al-Khairiyah Banyuwangi dan lulus pada tahun 2006. Pada tahun yang sama penulis melanjutkan pendidikan dasar di SD Islam Al-Khairiyah Banyuwangi dan lulus pada tahun 2012. Kemudian penulis menempuh pendidikan menengah pertama di SMP Negri 3 Banyuwangi dan lulus pada tahun 2015. Selanjutnya penulis melanjutkan jenjang pendidikan menengah atas di MBI Amanatul Ummah Mojokerto dan lulus pada tahun 2018. Setelah lulus, penulis menempuh pendidikan kuliah di Universitas Islam Negeri Maulana Malik Ibrahim Malang pada tahun 2018 dengan mengambil program studi matematika.

Selama menempuh pendidikan di Universitas UIN Malang, penulis berperan aktif dalam mengembangkan kemampuan akademik. Salah satu contohnya adalah menjadi Asisten Dosen pada mata kuliah Praktikum Pemrograman Kompunter I. Selain itu, penulis juga berperan aktif dalam mengembangkan kemampuan non akademik, yaitu pada komunitas Jam'iyyah Da'wah Wa Al Fann Al Islamy (JDFI) pada bidang banjari.