ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN *VIGENERE-MULTIPLICATIVE CIPHER* DAN *LINEAR BLOCK CIPHER* (LBC)

SKRIPSI

OLEH
AULIA NANDA HERAWATI
NIM. 18610056

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

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN *VIGENERE-MULTIPLICATIVE CIPHER* DAN *LINEAR BLOCK CIPHER* (LBC)

SKRIPSI

OLEH
AULIA NANDA HERAWATI
NIM. 18610056

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

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN *VIGENERE-MULTIPLICATIVE CIPHER* DAN *LINEAR BLOCK CIPHER* (LBC)

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
Aulia Nanda Herawati
NIM. 18610056

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

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN *VIGENERE-MULTIPLICATIVE CIPHER* DAN *LINEAR BLOCK CIPHER* (LBC)

SKRIPSI

Oleh
Aulia Nanda Herawati
NIM. 18610056

Telah Diperiksa dan Disetujui Untuk Diuji
Tanggal 16 Juni 2022

Dosen Pembimbing I	Dosen Pembimbing II
Evawati Alisah, M.Pd	Erna Herawati, M.Pd
NIP. 19720604 199903 2 001	NIDT. 19760723 20180201 2 222

Mengetahui,
Ketua Program Studi Matematika

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

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN *VIGENERE-MULTIPLICATIVE CIPHER* DAN *LINEAR BLOCK CIPHER* (LBC)

SKRIPSI

Oleh
Aulia Nanda Herawati
NIM. 18610056

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

Tanggal 21 Juni 2022

Ketua Penguji	: Muhammad Khudzaifah, M.Si	.....
Anggota Penguji I	: Mohammad Nafie Jauhari, M.Si	.....
Anggota Penguji II	: Evawati Alisah, M.Pd	.....
Anggota Penguji III	: Erna Herawati, M.Pd	.....

Mengetahui,
Ketua Program Studi Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertandatangan dibawah ini:

Nama : Aulia Nanda Herawati

NIM : 18610056

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Enkripsi dan Dekripsi Pesan Menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC)

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 pustaka. Apabila di kemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 13 Juni 2022

Yang membuat pernyataan,

Aulia Nanda Herawati

NIM. 18610056

MOTO

Allah tidak membebani seseorang melainkan sesuai dengan kesanggupannya

(*Q.S Al-Baqarah*:286)

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:

Kedua orang tua tercinta, beserta seluruh keluarga yang senantiasa memanjatkan do'a terbaik, memberi nasihat, motivasi, dukungan spiritual dan finansial serta kasih sayang yang tak terhingga kepada penulis.

Seluruh sahabat dan teman-teman penulis, yang telah memberi semangat dan motivasi kepada penulis dalam menyelesaikan skripsi ini.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji syukur kepada Allah SWT yang telah melimpahkan seluruh rahmat, taufik, dan hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Enkripsi dan Dekripsi Pesan Menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC)" sebagai salah satu syarat untuk mendapatkan gelar sarjana dalam bidang Matematika di Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Shalawat serta salam tetap tercurahkan kepada junjungan Nabi Muhammad SAW yang telah membimbing dari zaman kegelapan menuju zaman yang terang yakni agama Islam.

Dalam proses penyusunan skripsi ini, penulis banyak mendapatkan bimbingan dan arahan dari berbagai pihak. Untuk itu, penulis menyampaikan banyak terima kasih dan penghargaan terutama 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. Evawati Alisah, M.Pd, selaku dosen pembimbing I yang telah banyak memberikan bimbingan, arahan, motivasi, serta saran yang membangun dalam penulisan skripsi ini.
5. Erna Herawati, M.Pd, selaku dosen pembimbing II yang telah memberikan bimbingan, arahan, dan motivasi kepada penulis.
6. Muhammad Khudzaifah, M.Si, selaku Ketua Penguji dalam Seminar Proposal, Seminar Hasil dan Sidang Skripsi yang telah memberikan kritik dan saran yang membangun kepada penulis.
7. Mohammad Nafie Jauhari, M.Si, selaku Anggota Penguji I yang telah memberikan kritik dan saran yang membangun serta berbagai ilmunya kepada penulis.

8. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim beserta seluruh staff dan karyawan.
9. Ibunda tercinta Sulistiyowati dan seluruh keluarga, yang senantiasa selalu memberikan semangat, dukungan, serta memanjatkan do'a terbaik untuk kelancaran penulis.
10. Seluruh teman-teman di Program Studi Matematika angkatan 2018, yang telah memberikan do'a, bantuan, semangat serta dukungan kepada penulis dalam menyelesaikan skripsi ini.
11. Indri Fatikhu Aflikh yang telah membantu penulis dalam belajar bahasa pemrograman.
12. Angger Ferdi Bimantoro yang selalu memberikan motivasi kepada penulis.

Semoga penulisan skripsi ini dapat menambah wawasan keilmuan dan memberikan manfaat baik untuk penulis maupun pembaca.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, 13 Juni 2022

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR SIMBOL

C_i : Nilai karakter cipherteks ke-i
CT_t : Nilai karakter cipherteks ke-t
P_i : Nilai karakter plainteks ke-i
PT_t : Nilai karakter plainteks ke-t
k_i : Nilai karakter kunci ke-i
k_m : Kunci enkripsi pertama pada *Multiplicative Cipher*
k_n : Kunci enkripsi kedua pada *Multiplicative Cipher*
${k_m}^{-1}$: Kunci dekripsi pertama pada *Multiplicative Cipher*
${k_m}^{-1}$: Kunci dekripsi kedua pada *Multiplicative Cipher*

DAFTAR LAMPIRAN

ABSTRAK

Herawati, Aulia Nanda, 2022. **Enkripsi dan Dekripsi Pesan Menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC).** Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Maulana Malik Ibrahim Malang. Pembimbing: (I) Evawati Alisah M.Pd., (II) Erna Herawati, M.Pd.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi, *Vigenere-Multiplicative Cipher*, *Linear Block Cipher* (LBC).

Kriptografi merupakan ilmu dan seni yang bertujuan untuk menjaga kerahasiaan pesan. Dalam kriptografi terdapat dua proses yakni enkripsi dan dekripsi. Enkripsi merupakan proses mengubah pesan asli (plainteks) menjadi pesan yang tersandikan (cipherteks). Dekripsi adalah proses mengembalikan pesan yang tersandikan menjadi pesan asli. Penelitian ini menggunakan dua metode dalam kriptografi klasik yang mana teknik penyandiannya menggunakan kunci simetri diantaranya *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC). Adapun tujuan dari penelitian ini adalah untuk mengetahui proses enkripsi dan dekripsi menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC). Dalam proses enkripsi dan dekripsi, peneliti menggunakan bantuan pemrograman Python. Pada proses enkripsi yaitu dengan melakukan enkripsi menggunakan *Vigenere-Multiplicative Cipher* dan selanjutnya dienkripsi kembali menggunakan *Linear Block Cipher* (LBC). Adapun proses dekripsi adalah dengan melakukan dekripsi menggunakan *Linear Block Cipher* (LBC) dan dilanjutkan dengan dekripsi menggunakan *Vigenere-Multiplicative Cipher*. Pembentukan kunci pada *Linear Block Cipher* (LBC) menggunakan aturan *general linear group* dengan menunjukkan bahwa $\mathbb{Z}_{59}$ adalah lapangan berhingga dan membangun suatu *general linear group* yaitu $GL_4(\mathbb{Z}_{59})$.

ABSTRACT

Herawati, Aulia Nanda, 2022. **The Encryption and Decryption Message Using Vigenere-Multiplicative Cipher and Linear Block Cipher (LBC)**. Thesis. Mathematics Study Program. Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Supervisor: (I) Evawati Alisah, M.Pd., (II) Erna Herawati, M.Pd.

Keywords: Cryptography, Encryption, Decryption, Vigenere-Multiplicative Cipher, Linear Block Cipher.

Cryptography is a science and art that aims to maintain the confidentiality of messages. In cryptography there are two processes namely encryption and decryption. Encryption is the process of converting the original message (plaintext) into an encrypted message (ciphertext). Decryption is the process of turning an encrypted message back into the original message. This study uses two methods in classical cryptography where the encryption technique uses a symmetric key including the Vigenere-Multiplicative Cipher and LBC. The purpose of this study was to determine the process of encryption and decryption using Vigenere-Multiplicative Cipher and LBC. In the process of encryption and decryption, the researcher uses the help of Python programming. The encryption process was done by encrypting it using Vigenere-Multiplicative Cipher and then re-encrypting it by using LBC. As for the decryption process, decryption is done using LBC and followed by decryption using Vigenere-Multiplicative Cipher. The key formation in LBC. uses general linear group rules by showing that $\mathbb{Z}_{59}$ is a finite field and constructs a general linear group that is $GL_4(\mathbb{Z}_{59})$.

مستخلص البحث

هيراواتي، أولية نندا. ٢٠٢٢. التشفير و وصف الرسالة باستخدام *Vigenere-Multiplicative Cipher & Linear Block Cipher (LBC)*. البحث العلمي. قسم الرياضيات، كلية العلوم و التكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية بمالانج. المشرفة : ١). إيفاواتي أليسة ، الماجستير، ٢). إرناهيراواتي ، الماجستير

الكلمات المفتاحية: كيرفتوكيرفي، التشفير، الوصف، *Vigenere-Multiplicative Cipher*، *Linear Block Cipher* (*LBC*)

كيرفتوكيرفي (*kriptografi*) هو علم وفن يهدف إلى الحفاظ على سرية الرسالة. في التشفير، كان عمليتان هما التشفير و الوصف. التشفير هو عملية تحويل الرسالة الأصلية (*plainteks*) إلى رسالة مشفرة (*cipherteks*). فك التشفير هو عملية تحويل رسالة مشفرة إلى الرسالة الأصلية. تستخدم هذه الدراسة طريقتين في التشفير الكلاسيكي حيث تستخدم تقنية التشفير مفتاحًا متماثلًا *Vigenere-Multiplicative Cipher* و *Linear Block Cipher* (*LBC*). و أما الأهداف من هذا البحث هو معرفة عملية التشفير و الوصف باستخدام-*Vigenere Multiplicative Cipher*و *Linear Block Cipher* (*LBC*) . و أما عملية الوصف هو بإجراء الوصف باستخدام *Linear Block Cipher* (*LBC*) و يتبعها بإجراء الوصف باستخدام -*Vigenere Multiplicative Cipher*. تشكيل المفتاح على الخطي (LBC) *Linear Block Cipher* مجموعة خطية عامة من خلال الإظها يدل على أن $\mathbb{Z}_{59}$ هو مجال محدود وإنشاء مجموعة خطية عام، $(GL_4(\mathbb{Z}_{59})$.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Kriptografi merupakan teknik untuk menjaga kerahasiaan pesan agar tidak mudah dipecahkan oleh pihak yang tidak berhak atas pesan tersebut. Dalam kriptografi, terdapat dua proses utama yakni enkripsi dan dekripsi. Teknik melindungi informasi dengan mengubahnya menjadi pesan yang acak (cipherteks) dan tidak dapat dibaca disebut enkripsi. Sedangkan teknik mengubah pesan menjadi teks biasa (plainteks) disebut dekripsi. Proses enkripsi dan dekripsi ini membutuhkan kunci sebagai parameter. Sebuah fungsi matematika yang diperlukan untuk proses enkripsi dan dekripsi adalah algoritma kriptografi. Perkembangan algoritma kriptografi mulai dari algoritma yang sederhana sampai yang kompleks bertujuan agar pesan yang dienkripsi aman dari serangan kriptaanalisis (Munir, 2019).

Salah satu penerapan kriptografi adalah digunakan untuk melindungi pesan teks. Di era digital sekarang perkembangan teknologi yang sangat pesat diiringi dengan perubahan cara berkomunikasi dalam masyarakat. Banyaknya komunikasi yang dapat dilakukan melalui internet salah satu contohnya mengirim pesan teks melalui email. Hal ini menjadikan kehidupan manusia lebih mudah. Akan tetapi internet bukanlah media komunikasi yang cukup aman karena banyak cara yang dapat digunakan oleh pengguna yang tidak sah untuk mengakses informasi. Sehingga keamanan data atau informasi menjadi hal utama dari pengguna internet untuk menjaga privasi mereka. Dalam upaya melindungi data supaya tidak mudah dikenal oleh pihak yang tidak berkepentingan perlu adanya suatu mekanisme yang

baik dalam mengamankan pesan. Hal ini sepadan dengan konsep amanah yang terdapat dalam Al-Qur'an.

Amanah dapat diartikan sebagai bentuk kewajiban untuk bersikap profesional terhadap sesuatu yang telah diberikan Allah mencakup segala macam profesi yang melekat pada diri manusia (Hermawan dkk, 2020). Amanah berarti menunaikan segala sesuatu yang telah menjadi kewajiban yang diberikan kepada seseorang untuk dijaga dan dijalankan sebaik mungkin. Dengan kata lain menjaga amanah berarti menjaga kepercayaan. Salah satu perintah Allah SWT dalam menjaga amanah yang terdapat dalam Al-Qur'an Surah Al-Anfal ayat 27 yang artinya:

"*Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul dan janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepada kamu, sedang kamu mengetahui."(Q.S Al-Anfal:27).*

Amanah yang diberikan Allah SWT kepada kita tidak hanya berupa agama, keluarga, harta dan kekayaan, jiwa dan raga namun juga dapat berupa sebuah dokumen rahasia milik negara, data pribadi, bahkan informasi yang telah diamanahkan kepada kita. Sebagai orang yang telah diberi amanah, kita harus bisa menjaga amanah tersebut agar tidak disalahgunakan oleh pihak yang tidak bertanggungjawab. Kriptografi adalah salah satu cara untuk mengamankan data atau informasi tersebut.

Penerapan dalam proses enkripsi dan dekripsi dapat dilakukan dengan bantuan pemrograman Python. Python dikenal sebagai bahasa pemrograman yang mudah dimengerti karena memiliki kode-kode pemrograman yang sangat lengkap dan jelas. Secara istilah, Python adalah bahasa pemrograman multi-paradigma yang dapat mengasah kemampuan seorang *programmer* dalam menggunakan berbagai fitur dan kelebihan yang terdapat pada Python untuk membuat sebuah program

sederhana hingga yang kompleks. Bahasa pemrograman ini dapat digunakan di berbagai bidang, salah satunya dalam pengembangan perangkat lunak yang berjalan di berbagai platform sistem operasi. Hal ini membuat distribusi aplikasi yang dilakukan menggunakan Python memiliki sifat *multi-platform* dan sangat luas. Beberapa platform yang mendukung Python antara lain: Linux/Unix, Windows, Mac OS X, Java Virtual Machine, OS/2, Amiga, Palm, dan Symbian (untuk produk-produk nokia) (Enterprise, 2019).

Pada penelitian sebelumnya yang telah dilakukan oleh Hamza Touil, Nabil El Akkad dan Khalid Satori (2020) berjudul "*Hybrid Cryptographic Method Using Vigenere and Hill Cipher*" membahas proses enkripsi dan dekripsi menggunakan dua metode yaitu *Vigenere Cipher* dan *Hill Cipher*. Penggabungan kedua metode ini untuk mengatasi kelemahan dari metode *Vigenere Cipher* yang dapat dengan mudah diketahui panjang kuncinya dengan metode kasiski. Sehingga diperlukan kombinasi dengan metode klasik lainnya yaitu *Hill Cipher*. Pada metode *Hill Cipher* beberapa karakter yang sama pada plainteks tidak selalu diubah menjadi karakter baru yang sama pada cipherteks. Hal ini membuat metode *Hill Cipher* sulit dipecahkan oleh kriptanalis. Penelitian yang telah dilakukan oleh Nisrina Yulia Setyawati, Adi Nur Khofid, Alessandro U.B Rundi dan Vera Wati (2021) berjudul "Modifikasi Kriptografi Klasik Kombinasi *Vigenere Cipher* dan *Caesar Cipher*" membahas proses enkripsi dan dekripsi menggunakan metode *Vigenere Cipher* dan *Caesar Cipher* dengan melakukan perhitungan secara manual dan program. Dalam memperoleh cipherteksnya yaitu dengan melakukan proses enkripsi menggunakan metode *Vigenere Cipher* dan setelah didapatkan hasil cipherteks sementara dilanjut dengan proses enkripsi menggunakan metode *Caesar Cipher*. Sedangkan untuk

proses dekripsinya yaitu dengan melakukan dekripsi menggunakan metode *Caesar Cipher* dan setelah didapatkan hasil plainteks sementara dilanjut dengan dekripsi menggunakan metode *Vigenere Cipher*. Penggabungan metode *Vigenere Cipher* dan *Caesar Cipher* ini menggunakan kata kunci yang berbeda. *Vigenere Cipher* menggunakan kunci berupa teks sedangkan *Caesar Cipher* menggunakan pergeseran angka sebagai kuncinya. Penerapan kedua metode tersebut dilakukan untuk meningkatkan keamanan pesan teks dan diterapkan secara terpisah agar dapat dibandingkan keefektifannya dalam menyandikan sebuah pesan. Namun, karakter yang digunakan hanya berupa huruf kapital saja sehingga memiliki keterbatasan jikalau mengenkripsi kalimat yang terdapat angka dan simbol. Penelitian yang telah dilakukan oleh Prakash Kuppuswamy, Saeed Q Al-Khalidi Al-Maliki (2021) berjudul *"A Novel Symmetric Hybrid Cryptography Technique Using Linear Block Cipher (LBC) and Simple Symmetric Key*" membahas proses enkripsi dan dekripsi menggunakan metode *Linear Block Cipher* (LBC) dan kunci simetri sederhana atau yang dapat dikenal dengan metode *Multiplicative Cipher*.

Berdasarkan penelitian yang telah dilakukan oleh beberapa peneliti tersebut, peneliti berharap dapat melakukan suatu penelitian baru dengan menggabungkan dua metode yaitu *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC). Untuk metode *Vigenere Cipher*, peneliti mengkombinasikan dengan *Multiplicative Cipher* di mana melibatkan dua fungsi matematika yaitu penjumlahan dan perkalian. Untuk *Linear Block Cipher* (LBC), peneliti memperjelas pembentukan kunci enkripsi dan dekripsi menggunakan aturan *general linear group*. *General linear group* merupakan himpunan semua matriks yang berukuran $n \times n$ atas lapangan berhingga dengan syarat determinan matriks tidak nol. Aturan ini

memiliki keunggulan yang terletak pada ruang plainteks yang lebih besar sehingga cipherteks menjadi lebih acak dan keamanan pengiriman data menjadi lebih aman. Salah satu kriptografi klasik yang dapat dimodifikasi dengan aturan *general linear group* ialah *block cipher* di mana rangkaian bit-bit plainteks dibagi menjadi blok-blok bit dengan panjang yang sama. Blok cipherteks yang dihasilkan berukuran sama dengan blok plainteks (Munir, 2019).

1.2 Rumusan Masalah

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

1. Bagaimana proses enkripsi pesan menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC)?
2. Bagaimana proses dekripsi pesan menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC)?

1.3 Tujuan Penelitian

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

1. Mengetahui proses enkripsi pesan menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC).
2. Mengetahui proses dekripsi pesan menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC).

1.4 Manfaat Penelitian

Penelitian ini dibuat dengan harapan untuk memberikan manfaat yaitu sebagai berikut:

1. Bagi Penulis

   Dapat menambah wawasan keilmuan dengan memperbanyak literatur terkait kriptografi khususnya pada metode *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC) serta mendapatkan cara untuk mengamankan pesan teks, sehingga dapat mengimplementasikannya dan bermanfaat untuk menjaga keamanan data.

2. Bagi Lembaga

   Penelitian ini dapat digunakan sebagai tambahan bahan kepustakaan di program studi Matematika khususnya untuk mata kuliah yang berkaitan dengan kriptografi di bidang aljabar.

3. Bagi Pembaca

   Dapat menambah wawasan yang dapat digunakan sebagai bahan referensi dalam pengembangan penelitian selanjutnya.

1.5 Batasan Masalah

Adapun batasan masalah pada penelitian ini adalah sebagai berikut :

1. Menggunakan karakter huruf A-Z, angka 0-9, spasi, dan beberapa simbol yaitu ! “ # $ % & ‘ ( ) * + , - . / : ; < = > ? @
2. Kunci enkripsi dan dekripsi pada metode *Vigenere-Multiplicative Cipher* adalah kata kunci *Vigenere Cipher* yaitu “M4LAN6” dan sebarang bilangan bulat positif (k_m) yaitu 25 dan bilangan bulat negatif (k_n) yaitu -7. Adapun

kunci dekripsinya adalah invers perkalian modulo dari masing-masing k_m dan k_n yaitu 26 dan 42.

3. Kunci enkripsi pada metode *Linear Block Cipher* (LBC) menggunakan aturan *general linear group*.
4. Kunci dekripsi pada metode *Linear Block Cipher* (LBC) menggunakan aturan *general linear group* berdasarkan kunci enkripsi.

1.6 Definisi Istilah

Beberapa definisi istilah yang digunakan dalam penelitian adalah sebagai berikut:

1. Enkripsi

   Enkripsi adalah proses menyandikan pesan asli (plainteks) ke dalam bentuk pesan yang tidak dapat dipahami maknanya (cipherteks).

2. Dekripsi

   Dekripsi adalah proses mengembalikan pesan yang tersandikan (cipherteks) ke dalam bentuk pesan aslinya (plainteks).

3. Pesan

   Pesan adalah data atau informasi yang dapat dibaca, dipersepsi dan dimengerti maknanya.

4. Plainteks

   Plainteks adalah pesan asli berupa teks yang dapat dipahami maknanya.

5. Cipherteks

   Cipherteks adalah pesan teks yang tersandi.

6. Cipher

   Cipher adalah fungsi matematika yang digunakan untuk enkripsi dan dekripsi.

7. Kunci

   Kunci adalah parameter yang digunakan dalam enkripsi dan dekripsi.

8. Kriptanalisis

   Kriptanalisis adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan dalam enkripsi dan dekripsi.

9. Kriptanalis

   Kriptanalis adalah orang yang melakukan kriptanalisis.

BAB II
KAJIAN TEORI

2.1 Teori Pendukung

2.1.1 Teori Bilangan

Aritmatika lanjut yang merupakan salah satu cabang matematika karena saling berkaitan dengan sifat-sifat dan hubungan antara jenis bilangan tertentu disebut dengan teori bilangan. Dalam bidang kriptografi, teori bilangan (*number theory*) berperan penting karena menjadi dasar untuk memahami khususnya pada algoritma kriptografi kunci publik. Bilangan yang dimaksudkan dalam teori bilangan hanyalah bilangan bulat (Munir, 2019). Bilangan bulat merupakan bilangan yang tidak memiliki bagian desimal maupun pecahan. Notasi himpunan semua bilangan bulat menggunakan huruf $\mathbb{Z}$ yang mana diambil dari kata *Zahlen* dalam bahasa Jerman yang artinya bilangan. Himpunan semua bilangan bulat terdiri dari tiga bagian antara lain yaitu nol $\{0\}$, bilangan bulat positif di mana bilangan bulat yang lebih besar dari nol atau dikenal dengan bilangan asli misalnya $\{1,2,3,4,5, \dots\}$ yang dapat dituliskan sebagai $\mathbb{Z}^+$ dan bilangan bulat negatif di mana bilangan bulat yang lebih kecil dari nol misalnya $\{\dots, -5, -4, -3, -2, -1\}$ yang dapat dituliskan sebagai $\mathbb{Z}^-$ (Irawan dkk, 2014).

2.1.1.1 Aritmatika Modulo

Aritmatika modulo merupakan salah satu fundamental matematika yang banyak digunakan dalam kriptografi. Dengan kata lain, aritmatika modulo memiliki berbagai aplikasi dalam kriptografi (Kraft & Washington, 2018). Aritmatika modulo digunakan agar operasi aritmatika selalu menghasilkan bilangan bulat pada lingkup yang sama. Misalnya, pada algoritma kriptografi

klasik digunakan alfabet “A” sampai dengan “Z”, dipetakan dahulu menjadi $\{A, \cdots, Z\}$ menjadi $\{0, \cdots, 25\}$. Aritmatika modulo ini bertujuan supaya transformasi penyandian selalu bernilai $\{0, \cdots, 25\}$ sehingga memiliki pasangan simbol yang digunakan (Sadikin, 2012).

Operasi aritmatika membutuhkan dua masukan yakni sebuah bilangan bulat a dan sebuah bilangan bulat positif yang disebut modulo m. Asumsikan bahwa a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi modulo mengembalikan r di mana merupakan sisa bagi atas operasi a dibagi dengan m. Operasi modulo dapat dinotasikan sebagai $a\ mod\ m$ (dibaca “$a\ modulo\ m$”). Hasil operasi modulo m terletak di dalam himpunan $\{0.1.2. \ldots . m - 1\}$ (Sadikin, 2012).

Contoh :

a. Tentukan hasil operasi artimatika modulo dari $32\ (mod\ 7)$

   32 dibagi dengan 7 adalah 4 dengan sisa 4, maka dapat dituliskan sebagai $32 = (7 \times 4) + 4$. Jadi, $32\ (mod\ 7) = 4$.

b. Tentukan hasil operasi aritmatika modulo dari $-16\ (mod\ 5)$

   -16 dibagi dengan 5 adalah -3 dengan sisa -1, maka dapat dituliskan sebagai $-16 = \big(5 \times (-3)\big) - 1$. Sehingga, $-16\ (mod\ 5) = -1$, agar bernilai positif -1 ditambah dengan nilai modulo 5 menghasilkan 4. Jadi $-16\ (mod\ 5) = 4$.

2.1.1.2 Kongruensi Modulo

Kongruensi modulo adalah sebuah pengkajian lebih lanjut mengenai keterbagian dalam himpunan bilangan bulat. Dua buah bilangan bulat a dan b dikatakan kongruen pada modulo m jika memiliki sisa bagi yang sama. Untuk

merepresentasikan sebuah kongruensi dapat dinotasikan dengan ≡. Asumsikan bahwa a dan b adalah dua buah bilangan bulat dan m adalah bilangan bulat positif atau dapat dituliskan sebagai $a.b.m \in \mathbb{Z}$ dan $m \neq 0$ maka a dikatakan kongruen dengan b modulo m apabila m membagi habis $a - b$. Pernyataan ini dinotasikan $a \equiv b \ (mod\ m)$ yang dapat dibaca "a kongruen dengan b modulo m" (Irawan dkk, 2014).

Contoh :

Tentukan kongruensi modulo dari:

a. $8 \equiv 3 \ (mod\ 5)$, karena $5|(8-3)$
b. $15 \equiv 6 \ (mod\ 9)$, karena $9|(15-6)$
c. $27 \equiv 5 \ (mod\ 11)$, karena $11|(27-5)$

2.1.1.3 Pembagi Bersama Terbesar (PBB)

Asumsikan bahwa a dan b adalah bilangan bulat dan keduanya tidak nol, maka himpunan pembagi persekutuannya memiliki elemen terbesar d yang disebut dengan Pembagi Bagian Terbesar (PBB) atau *greatest common divisor* (gcd) dari a dan b yang dapat dituliskan sebagai (Kraft & Washington, 2018):

$$d = \gcd(a, b).$$

Contoh:

Tentukan gcd dari kedua bilangan berikut:

a. $\gcd(24{,}52) = 4$,
b. $\gcd(9{,}27) = 9$
c. $\gcd(15{,}28) = 1$

2.1.1.4 Relatif Prima

Dua buah bilangan bulat a dan b dapat dikatakan relatif prima apabila $gcd(a.b) = 1$. Jika a dan b relatif prima, maka terdapat bilangan bulat m dan n, sedemikian sehingga (Munir, 2019):

$$ma + nb = 1$$

Contoh :

Himpunan semua pembagi dari 14 adalah:

$$A = \{-14, -7, -2, -1,1,2,7,14\},$$

dan himpunan semua pembagi dari 15 adalah:

$$B = \{-15, -5, -3, -1,1,3,5,15\}.$$

Himpunan semua pembagi persekutuan dari 14 dan 15 ialah: $S = \{-1,1\}$.

Karena dalam himpunan S terdapat elemen terbesar yaitu 1, maka $gcd(14,15) = 1$.

Jadi, bilangan 14 dan 15 dapat dikatakan relatif prima karena $gcd(14,15) = 1$, atau dapat ditulis sebagai:

$$(-1).14 + 1.15 = 1$$

dengan $m = -1$ dan $n = 1$.

2.1.1.5 Balikan Modulo

Dalam aritmatika modulo, kita mengenal balikan (invers) perkalian. Dapat dikatakan bahwa dua buah bilangan bulat dari a dan b memiliki invers perkalian modulo m jika $ab \equiv 1\ (mod\ m)$. Balikan (invers) modulo dapat dinotasikan $\frac{1}{a}$ atau sering dituliskan sebagai a^{-1} (Munir, 2019). Tidak semua elemen pada $\mathbb{Z}_m$ memiliki balikan (invers) perkalian. Secara matematika dapat dibuktikan bahwa elemen yang memiliki invers perkalian hanya elemen yang

merupakan bilangan relatif prima terhadap m, yaitu untuk $a \in \mathbb{Z}_m$ berlaku $\gcd(a.m) = 1$ (Sadikin, 2012).

Menurut definisi relatif prima yaitu dua buah bilangan bulat a dan m relatif prima jika $\gcd(a.m) = 1$ maka terdapat bilangan bulat p dan q sedemikian sehingga:

$$pa + qm = 1$$

yang menunjukkan bahwa

$$pa + qm = 1 \ (mod\ m).$$

Dikarenakan $qm \equiv 0 \ (mod\ m)$, maka

$$pa \equiv 1 \ (mod\ m).$$

Dapat dilihat dari bentuk kekongruenan yang terakhir menyatakan bahwa p merupakan balikan dari a modulo m (Munir, 2019).

Berdasarkan pemaparan di atas menjelaskan bahwa untuk menemukan balikan dari a modulo m, harus membuat kombinasi lanjar dari a dan m sama dengan 1. Koefisien a dari kombinasi lanjar tersebut yaitu p yang merupakan balikan dari a modulo m (Munir, 2019).

Contoh :

Tentukan balikan modulo dari

a. $25 \ (mod\ 7\ )$

   Karena $\gcd(25,7) = 1$, maka $25^{-1} \ (mod\ 7)$ ada.

   Misalkan

   $$25^{-1}(mod\ 7) = x,$$

   berdasarkan definisi kekongruenan dapat dituliskan dalam hubungan kesamaan yaitu

$$25x \equiv 1\ (mod\ 7) \text{ atau } 25x = 1 + 7k,$$

di mana dapat disusun menjadi bentuk

$$x = \frac{(1 + 7k)}{25}$$

dengan k adalah sebarang bilangan bulat yaitu $k = 0, \pm 1, \pm 2, \pm 3, \cdots$

sedemikian sehingga

jika $k = 0$ maka $x = \frac{(1+7.0)}{25} = \frac{1}{25}$

jika $k = 1$ maka $x = \frac{(1+7.1)}{25} = \frac{8}{25}$

jika $k = 2$ maka $x = \frac{(1+7.2)}{25} = \frac{15}{25}$

jika $k = 3$ maka $x = \frac{(1+7.3)}{25} = \frac{22}{25}$

⋮

jika $k = 7$ maka $x = \frac{(1+7.7)}{25} = \frac{50}{25} = 2$

dengan mencoba beberapa macam nilai k, maka untuk $k = 7$ diperoleh solusi x bilangan bulat. Jadi, $25^{-1}(mod\ 7) = 2$ karena $25 \cdot 2 \equiv 1(mod\ 7)$.

b. $20\ (mod\ 5)$

Karena $\gcd(20,5) = 5 \neq 1$, maka balikan dari $20\ (mod\ 5)$ tidak ada.

2.1.1.6 Kekongruenan Lanjar

Kekongruenan lanjar merupakan kekongruenan yang berbentuk $ax \equiv b\ (mod\ m)$. dengan m adalah bilangan bulat positif, a dan b sebarang bilangan bulat dan x ialah peubah bilangan bulat. Berdasarkan definisi kekongruenan, $ax \equiv b\ (mod\ m)$. dapat dituliskan dalam hubungan kesamaan $ax = b + km$ di mana dapat disusun menjadi bentuk sebagai berikut:

$$x = \frac{b + km}{a}$$

dengan k yaitu sebarang bilangan bulat. Untuk menemukan solusi kekongruenan lanjar dapat dilakukan dengan mencoba beberapa nilai $k = 0,1,2,$ ... dan $k = -1, -2,$ ... maka akan diperoleh semua nilai x bilangan bulat (Munir, 2019).

Contoh:

Tentukan nilai x dari $3x \equiv 8(mod\ 10)$.

Kekongruenan $3x \equiv 8(mod\ 10)$ dapat dituliskan sebagai

$$3x = 8 + 10k$$

atau

$$x = \frac{8 + 10k}{3}.$$

Untuk,

$k = 0 \rightarrow x = \frac{8+10\cdot 0}{3} = \frac{8}{3}$ (bukan solusi, karena bukan bilangan bulat)

$k = 1 \rightarrow x = \frac{8+10\cdot 1}{3} = \frac{18}{3} = 6$ (solusi)

2.1.2 Matriks

Matriks merupakan susunan bilangan berbentuk segiempat yang disusun dalam baris dan kolom. Bilangan yang disusun pada matriks disebut entri atau elemen pada matriks. Elemen suatu matriks terdiri dari baris ke-i dan kolom ke-j yang dinotasikan dengan a_{ij} . Penamaan suatu matriks menggunakan huruf kapital, sedangkan elemennya menggunakan huruf non kapital. Ukuran atau ordo suatu matriks digambarkan dalam bentuk jumlah baris dan kolom. Baris pada suatu matriks disusun secara horizontal, sedangkan kolom disusun secara vertikal. Matriks A yang berordo $m \times n$ dapat ditulis dengan $A_{m\times n}$. Secara umum matriks A dengan ordo $m \times n$ dapat ditulis sebagai (Anton & Rorres, 2010):

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Matriks yang hanya memiliki satu baris disebut matriks baris, sedangkan matriks yang hanya memiliki satu kolom disebut matriks kolom. Matriks dengan banyaknya baris dan kolomnya sama dapat dikatakan sebagai matriks persegi. Dengan kata lain, apabila A memiliki ordo $n \times m$ maka A dikatakan matriks persegi jika $n = m$. Bentuk penulisan matriks persegi $n \times n$ selanjutnya cukup dituliskan matriks n. Suatu matriks dapat dioperasikan sama halnya dengan operasi aljabar biasa diantaranya yaitu penjumlahan, pengurangan, perkalian matriks dengan skalar, dan perkalian matriks dengan matriks.

2.1.2.1 Operasi Matriks

Perkalian matriks dapat didefinisikan apabila suatu matriks A dengan ordo $m \times k$ dan B adalah suatu matriks dengan ordo $k \times n$, maka hasil perkalian dari matriks AB adalah matriks $m \times n$ di mana untuk menentukan elemen pada baris i dan kolom j dari matriks AB, pisahkan baris i dari matriks A dan kolom j dari matriks B. Kemudian, kalikan elemen-elemen yang bersesuaian dengan baris dan kolom tersebut dan lakukan penjumlahan dari hasil kali yang telah diperoleh (Anton & Rorres, 2010).

Contoh:

Misalkan suatu matriks A dan B adalah

$$A = \begin{bmatrix} 1 & 2 & 4 \\ 2 & 6 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 4 & 1 & 4 & 3 \\ 0 & -1 & 3 & 1 \\ 2 & 7 & 5 & 2 \end{bmatrix}$$

Karena matriks A berordo 2×3 dan matriks B berordo 3×4, maka hasil kali matriks AB berordo 2×4. Untuk menentukannya, kalikan elemen-elemen yang bersesuaian dan lakukan operasi penjumlahan dari hasil kali yang diperoleh. Berikut adalah hasil kali dari matriks AB:

$$\begin{bmatrix} 1 & 2 & 4 \\ 2 & 6 & 0 \end{bmatrix} \begin{bmatrix} 4 & 1 & 4 & 3 \\ 0 & -1 & 3 & 1 \\ 2 & 7 & 5 & 2 \end{bmatrix} = \begin{bmatrix} 12 & 27 & 30 & 13 \\ 8 & -4 & 26 & 12 \end{bmatrix}.$$

dengan perhitungan elemennya ialah misalkan kita pilih elemen dalam baris ke-1 dan kolom ke-1, kemudian kalikan masing-masing elemen yang bersesuaian dan jumlahkan dengan hasil kali yang diperoleh sebagai berikut:

$$(1 \cdot 4) + (2 \cdot 0) + (4 \cdot 2) = 12.$$

Hal tersebut berlaku juga untuk menentukan elemen-elemen berikutnya.

Perkalian matriks dengan skalar dapat didefinisikan apabila suatu matriks A dikalikan dengan k adalah sebarang skalar, maka hasil kali dari kA diperoleh dari perkalian setiap elemen pada matriks A dengan bilangan k. Matriks tersebut dapat dikatakan sebagai kelipatan skalar. Dalam notasi matriks secara umum apabila suatu matriks A dituliskan sebagai berikut :

$$A = [a_{ij}]$$

maka

$$(kA)_{ij} = k(A)_{ij} = ka_{ij},$$

Contoh :

a. Misalkan matriks dengan ordo 2×3 adalah

$$A = \begin{bmatrix} 2 & 3 & 4 \\ 1 & 3 & 1 \end{bmatrix}$$

dengan sebarang skalar $k = 2$

maka

$$2A = \begin{bmatrix} 4 & 6 & 8 \\ 2 & 6 & 2 \end{bmatrix}.$$

b. Misalkan matriks dengan ordo 3×2 adalah

$$B = \begin{bmatrix} 0 & 2 \\ 7 & -1 \\ 3 & -5 \end{bmatrix}$$

dengan sebarang skalar $k = -1$

maka

$$(-1)B = \begin{bmatrix} 0 & -2 \\ -7 & 1 \\ -3 & 5 \end{bmatrix}.$$

2.1.2.2 Transpos Matriks

Transpos matriks A merupakan suatu matriks yang diperoleh dari pengubahan setiap baris menjadi kolom dari matriks A atau pengubahan setiap kolom menjadi baris dari matriks A. Dalam transpos matriks ini, kolom pertamanya menjadi baris pertama dari matriks A, kolom kedua menjadi baris kedua dari matriks A, dan seterusnya. Transpos matriks A dapat dinotasikan sebagai A^T atau A'. Apabila matriks A berordo $n \times m$ maka transpos matriks A berordo $m \times n$ (Anton & Rorres, 2010).

Contoh :

Diberikan suatu matriks A dengan ordo 2×3 yaitu:

$$A = \begin{bmatrix} 5 & -2 & 1 \\ 3 & 6 & 4 \end{bmatrix}$$

maka matriks transpos A adalah matriks dengan ordo 3×2 yaitu:

$$A^T = \begin{bmatrix} 5 & 3 \\ -2 & 6 \\ 1 & 4 \end{bmatrix}.$$

2.1.2.3 Determinan Matriks

Salah satu konsep dasar dalam matriks adalah determinan. Determinan matriks didefinisikan sebagai nilai skalar yang merupakan fungsi dari elemen suatu matriks persegi. Determinan matriks dapat dinotasikan sebagai $\det(A)$ atau $|A|$. Determinan dapat diartikan pula sebagai selisih dari hasil perkalian elemen-elemen pada kedua diagonal suatu matriks yaitu diagonal utama dan diagonal sekunder. Oleh karena itu, determinan selalu dikaitkan dengan matriks persegi karena kedua diagonal tersebut hanya dimiliki oleh matriks persegi (Anton & Rorres, 2010). Determinan dari matriks dengan ordo 2×2 yang dituliskan sebagai $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dapat ditentukan dengan cara sebagai berikut:

$$|A| = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

Contoh:

Misalkan suatu matriks A dengan ordo 2×2 adalah

$$A = \begin{bmatrix} 2 & 5 \\ 1 & 7 \end{bmatrix}$$

maka determinan dari matriks A adalah

$$|A| = \begin{vmatrix} 2 & 5 \\ 1 & 7 \end{vmatrix} = (2 \cdot 7) - (5 \cdot 1) = 14 - 5 = 9.$$

2.1.2.4 Adjoin Matriks

Apabila suatu matriks A adalah matriks dengan ordo $n \times n$ dan C_{ij} didefinisikan sebagai matriks kofaktor dari A. Transpos dari matriks kofaktor A dapat didefinisikan sebagai adjoin dari A dan dapat dinotasikan sebagai $adj(A)$ (Anton & Rorres, 2010).

Contoh:

Misalkan suatu matriks A dengan ordo 3×3

$$A = \begin{bmatrix} 3 & 2 & -1 \\ 1 & 6 & 3 \\ 2 & -4 & 0 \end{bmatrix}$$

Kofaktor dari matriks A adalah $c_{11} = 12$, $c_{12} = 6$, $c_{13} = -16$, $c_{21} = 4$, $c_{22} = 2$, $c_{23} = 16$, $c_{31} = 12$, $c_{32} = -10$, $c_{33} = 16$

maka matriks kofaktor A adalah

$$C_A = \begin{bmatrix} 12 & 6 & -16 \\ 4 & 2 & 16 \\ 12 & -10 & 16 \end{bmatrix}$$

Sehingga adjoin dari A adalah

$$adj(A) = \begin{bmatrix} 12 & 4 & 12 \\ 6 & 2 & -10 \\ -16 & 16 & 16 \end{bmatrix}.$$

2.1.2.5 Invers Matriks

Apabila suatu matriks A adalah matriks persegi dan apabila suatu matriks B dengan ukuran yang sama sedemikian sehingga $AB = BA = I$, maka matriks A dapat dibalik (*invertible*) dan matriks B dikatakan sebagai invers dari matriks A. Apabila matriks A dapat dibalik, maka invers matriks tersebut dapat dinotasikan sebagai A^{-1} (Anton & Rorres, 2010). Misalkan suatu matriks berordo 2×2 yang dapat dituliskan sebagai matriks A yaitu:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

memiliki invers jika dan hanya jika $ad - bc \neq 0$ dan invers dari matriks A dituliskan dengan rumus (Ririen Kusumawati, 2009):

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} \frac{d}{ad - bc} & -\frac{b}{ad - bc} \\ -\frac{c}{ad - bc} & \frac{a}{ad - bc} \end{bmatrix}.$$

Contoh:

Misalkan suatu matriks A dengan ordo 2×2 adalah

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

determinan dari matriks A adalah

$$|A| = -1$$

karena $-1 \neq 0$ maka matriks A memiliki invers yaitu

$$A^{-1} = \frac{1}{-1}\begin{bmatrix} 5 & -2 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} -5 & 2 \\ 3 & -1 \end{bmatrix}.$$

2.1.3 Bilangan Prima dan Bilangan Komposit

Bilangan prima adalah bilangan asli yang tepat mempunyai dua pembagi. Sedangkan bilangan yang mempunyai lebih dari dua pembagi disebut bilangan komposit. Dengan kata lain, jika sebuah bilangan bulat $p > 1$ bukan bilangan prima, maka p dinamakan bilangan komposit (Irawan dkk, 2014).

Contoh:

a. 2, 3, 4 dan 7 adalah bilangan-bilangan prima, karena pembaginya adalah 1 dan bilangan itu sendiri. Sedangkan 4, 6, 8 dan 9 adalah bilangan komposit, seperti 4 memiliki pembagi 1, 2 dan 4.
b. -3, -5 bukan bilangan prima, demikian pula -6, -8 bukan bilangan komposit, karena bilangan prima dan bilangan komposit itu lebih besar dari 1 atau bilangan bulat positif lebih dari 1.

2.1.4 Lapangan

Definisi 2.1

Suatu lapangan F adalah himpunan elemen-elemen yang tertutup terhadap dua operasi biner, yaitu penjumlahan dan perkalian yang dinotasikan dengan $(+)$ dan $(\cdot)$ yang memenuhi beberapa aksioma berikut untuk semua $a, b, c \in F$.

i. $a + (b + c) = (a + b) + c$

ii. $a + b = b + a$

iii. Terdapat elemen $0 \in F$ sedemikian sehingga $a + 0 = a$

iv. Terdapat elemen $-a \in F$ sedemikian sehingga $a + (-a) = 0$

v. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

vi. $a \cdot b = b \cdot a$

vii. Terdapat elemen $1 \in F$ sedemikian sehingga $a \cdot 1 = a$

viii. Untuk setiap $a \neq 0$, maka terdapat elemen $a^{-1} \in F$ sedemikian sehingga $a \cdot a^{-1} = 1$

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

(Gilbert & Gilbert, 2009)

Contoh:

Diberikan himpunan $\mathbb{Z}_7 = \{\bar{0}.\bar{1}.\bar{2}.\bar{3}.\bar{4}.\bar{5}.\bar{6}\}$ yang merupakan himpunan semua bilangan bulat modulo 7 dengan operasi penjumlahan modulo 7 dan operasi perkalian modulo 7 yaitu $(\mathbb{Z}_7.+.\cdot)$, maka $(\mathbb{Z}_7.+.\cdot)$ merupakan suatu lapangan. Berikut adalah bukti yang ditunjukkan dengan Tabel Cayley $\mathbb{Z}_7$:

Tabel 2.1 Tabel Cayley $\mathbb{Z}_7$ Hasil Penjumlahan Modulo 7

$+_7$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

Berdasarkan Tabel 2.1 di atas, himpunan $\mathbb{Z}_7$ terhadap operasi penjumlahan modulo 7 memenuhi sifat tertutup, elemen identitasnya adalah 0, setiap elemennya memiliki invers terhadap penjumlahan modulo 7, yaitu $-0 = 0$, $-1 = 6$, $-2 = 5$,$-3 = 4$, $-4 = 3$. $-5 = 2$, $-6 = 1$. Tabel simetris terhadap diagonal utama, sehingga penjumlahan modulo 7 bersifat komutatif.

Tabel 2.2 Tabel Cayley $\mathbb{Z}_7$ Hasil Perkalian Modulo 7

$*_7$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	5	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Berdasarkan Tabel 2.2 di atas, himpunan $\mathbb{Z}_7$ terhadap operasi perkalian modulo 7 untuk perkalian modulo 7 memenuhi sifat tertutup, elemen identitasnya adalah 1, setiap elemennya memiliki invers terhadap perkalian modulo 7, yaitu $1^{-1} = 1$, $2^{-1} = 4$,$3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$, $6^{-1} = 6$. Tabel simetris terhadap diagonal utama, sehingga perkalian modulo 7 bersifat komutatif.

Definisi 2.2

Suatu lapangan F dengan unsur berhingga adalah lapangan berhingga (A.Vanstone & Oorschot, 1989).

Teorema 2.1

$\mathbb{Z}_n$ merupakan lapangan berhingga jika dan hanya jika n bilangan prima (A.Vanstone & Oorschot, 1989).

Bukti:

($\Rightarrow$) Akan ditunjukkan $\mathbb{Z}_n$ merupakan lapangan berhingga jika n bilangan prima.

Andaikan jika n bukan bilangan prima, maka n adalah bilangan bulat komposit yang berarti bahwa $n = ab$, di mana a dan b bilangan prima, $a > 1, b < n - 1$. Karena $\mathbb{Z}_n$ merupakan lapangan, maka setiap elemen yang tak nol pasti memiliki invers. Misalkan c adalah invers dari b, yang berarti bahwa $bc \equiv 1(mod\ n)$ dan $abc \equiv a(mod\ n)$. Karena $n = ab$, maka $ab \equiv 0(mod\ n)$. Hal ini kontradiksi dengan pengandaian bahwa n bukan bilangan prima. Jadi, haruslah n bilangan prima.

($\Leftarrow$) Akan ditunjukkan n bilangan prima jika $\mathbb{Z}_n$ merupakan lapangan berhingga.

Diketahui n bilangan prima. Untuk dapat membuktikan bahwa $\mathbb{Z}_n$ merupakan lapangan, maka akan dibuktikan bahwa setiap elemen tak nolnya memiliki invers. Karena n adalah bilangan prima, maka $\text{PBB}(n, a) = 1$, untuk $0 < a < n$. Dengan kata lain, n dan a adalah dua buah bilangan bulat yang relatif prima. Akibatnya terdapat bilangan bulat x dan y sedemikian sehingga $x \cdot n + y \cdot a = 1$ yang berarti bahwa $y \cdot a \equiv 1(mod\ n)$, diperoleh $y \equiv a^{-1}(mod\ n)$. Terbukti bahwa setiap elemen tak nolnya memiliki invers. Jadi $\mathbb{Z}_n$ merupakan lapangan jika n bilangan

prima. Karena $\mathbb{Z}_n$ memiliki unsur berhingga maka $\mathbb{Z}_n$ merupakan lapangan berhingga (A.Vanstone & Oorschot, 1989). ■

2.1.5 *General Linear Group*

General linear group atau $GL_n(F)$ didefinisikan sebagai himpunan semua matriks yang berukuran $n \times n$ dengan entri-entri dari F atas lapangan berhingga (*finite field*) dengan ketentuan determinan matriks tersebut tidak nol. Sebagai contoh lapangan F adalah $\mathbb{Q}$ (*rationals*), $\mathbb{R}$ (*reals*), $\mathbb{Z}_n$ (*integer numbers*) dengan n bilangan prima dan sebagainya (S.Dummit & M.Foote, 2004).

Misalkan A dan B adalah himpunan $n \times n$ matriks di mana determinan dari kedua matriks tersebut tidak nol dengan entri-entri dari F. Untuk perkalian matriks AB dapat dihitung dengan rumus yang sama seperti halnya yang digunakan ketika $F = \mathbb{R}$ yang mana hasil perkalian dari matriks AB adalah bersifat asosiatif. Juga, karena $\det(AB) = \det(A) \cdot \det(B)$, hal ini menunjukkan bahwa jika $\det(A) \neq 0$ dan $\det(B) \neq 0$, maka $\det(AB) \neq 0$. Sehingga, $GL_n(F)$ tertutup terhadap perkalian matriks. Selain itu, $\det(A) \neq 0$ jika dan hanya jika A memiliki invers matriks. Jadi, untuk setiap $A \in GL_n(F)$ memiliki invers, dengan kata lain $A^{-1} \in GL_n(F)$. Hal ini menunjukkan bahwa $AA^{-1} = A^{-1}A = I$, di mana I adalah matriks identitas yang berukuran $n \times n$. Dengan demikian, $GL_n(F)$ adalah grup terhadap perkalian matriks, yang dapat disebut dengan *general linear group* dari derajat n (S.Dummit & M.Foote, 2004).

Contoh:

Misalkan $A = \begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix} \in GL_2(\mathbb{Z}_7)$.

Diketahui bahwa $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.

Kemudian, menentukan determinan matriks A yaitu:

$\det(A) = \begin{vmatrix} 4 & 5 \\ 6 & 3 \end{vmatrix} = 5 - 2 = 3\ (mod\ 7)$.

Invers matriks A dapat dihitung sebagai berikut:

$$A^{-1} = \frac{1}{3}\begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}.$$

Bentuk $\frac{1}{3}$ atau dapat dituliskan sebagai 3^{-1} diubah menjadi bentuk bilangan bulat dengan melakukan operasi balikan modulo 7 yang dapat dihitung menggunakan kekongruenan lanjar:

Misalkan

$$3^{-1}(mod\ 7) = x,$$

berdasarkan definisi kekongruenan dapat dituliskan dalam hubungan kesamaan yaitu

$$3x \equiv 1\ (mod\ 7) \text{ atau } 3x = 1 + 7k,$$

di mana dapat disusun menjadi bentuk

$$x = \frac{(1 + 7k)}{3}$$

dengan k adalah sebarang bilangan bulat yaitu $k = 0. \pm 1. \pm 2. \pm 3. \ldots$

sedemikian sehingga

jika $k = 0$ maka $x = \frac{(1+7,0)}{3} = \frac{1}{3}$

jika $k = 1$ maka $x = \frac{(1+7,1)}{3} = \frac{8}{3}$

jika $k = 2$ maka $x = \frac{(1+7,2)}{3} = \frac{15}{3} = 5$

dengan mencoba beberapa macam nilai k, maka untuk $k = 2$ diperoleh solusi x bilangan bulat. Jadi, $3^{-1}(mod\ 7) = 5$ karena $3 \cdot 5 \equiv 1\ (mod\ 7)$.

Sehingga,

$$A^{-1} = 5\begin{bmatrix}3 & 2\\ 1 & 4\end{bmatrix} = \begin{bmatrix}1 & 3\\ 5 & 6\end{bmatrix} \in GL_2(\mathbb{Z}_7)$$

Kemudian, periksa bahwa perkalian antara dua matriks tersebut adalah matriks identitas yaitu sebagai berikut:

$$\begin{bmatrix}4 & 5\\ 6 & 3\end{bmatrix}\begin{bmatrix}1 & 3\\ 5 & 6\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \in GL_2(\mathbb{Z}_7),$$

2.1.6 Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani yang terdiri dari dua kata yakni *cryptos* dan *graphein. Cryptos* yang memiliki arti rahasia, sedangkan *graphein* yang memiliki arti tulisan. Kriptografi secara bahasa berarti tulisan rahasia. Secara terminologinya, kriptografi adalah ilmu dan seni yang bertujuan memelihara keamanan pesan yang akan dikirimkan dengan cara mengubahnya menjadi bentuk yang tidak dapat dipahami lagi maknanya. Pada dasarnya, dalam pertukaran pesan melibatkan dua objek yaitu pengirim dan penerima. Objek yang mengirim pesan kepada objek lainnya disebut pengirim (*sender*). Sedangkan objek yang menerima pesan disebut penerima (*receiver*). Kedua objek tersebut dapat berupa orang, mesin, robot, maupun komputer (Munir, 2019).

Kriptografi dapat dikatakan sebagai studi matematis untuk memecahkan dua jenis persoalan terkait privasi dan autentikasi. Sistem privasi bertujuan agar data atau informasi tidak diretas oleh pihak yang tidak berwenang. Sistem autentikasi bertujuan untuk memastikan pesan yang dikirim sampai pada penerima yang dituju (Diffie & Hellman, 1976). Dalam kriptografi terdapat dua proses utama yaitu enkripsi dan dekripsi. Proses menyandikan pesan asli (plainteks) menjadi pesan yang tidak dimengerti maknanya dikenal dengan enkripsi, sedangkan proses mengembalikan pesan yang tersandikan (cipherteks) ke bentuk pesan aslinya dikenal dengan dekripsi. Dalam proses enkripsi menerima masukan berupa

plainteks dan kunci sebagai parameternya, keluarannya berupa cipherteks atau pesan tersandikan. Sedangkan dalam proses dekripsi menerima masukan berupa cipherteks dan kunci sebagai parameternya, keluarannya berupa plainteks atau pesan aslinya (Munir, 2019).

Kriptografi ini memberikan beberapa layanan keamanan yaitu sebagai berikut:

1. Kerahasiaan (*confidentiality*) adalah layanan yang menjaga keamanan dari isi pesan yang telah disandikan agar pihak yang tidak memiliki hak tidak dapat membaca isi pesan tersebut.
2. Integritas data (*data integrity*) adalah layanan yang menjamin bahwa penerima mendapatkan informasi pesan yang masih asli yang mana isi dari pesan tersebut belum pernah diubah maupun dimanipulasi selama proses pengiriman pesan.
3. Autentikasi (*authentication*) adalah layanan yang berhubungan dengan mengidentifikasi kebenaran pihak-pihak yang melakukan komunikasi. Kedua pihak tersebut harus memastikan bahwa pesan yang mereka terima adalah benar dari pengirim dan penerima.

(Munir, 2019).

2.1.7 Kriptografi Klasik dan Modern

Berdasarkan perkembangannya, kriptografi terbagi menjadi dua jenis diantaranya yaitu kriptografi klasik dan kriptografi modern. Teknik penyandian pada kriptografi klasik menggunakan satu kunci yang dimiliki oleh pengirim dan penerima. Kriptografi klasik ini dapat disebut dengan algoritma simetri. Dalam pengiriman pesan, penerima harus diberitahu kunci dari pesan tersebut agar dapat

mendekripsi pesan yang dikirim. Sehingga, tingkat keamanan pesan yang menggunakan algoritma ini tergantung pada kunci. Contoh dari algoritma simetri adalah *Caesar Cipher*, *Affine Cipher*, *Vigenere Cipher*, *Playfair Cipher*, *Vernam Cipher* dan sebagainya. Sedangkan teknik penyandian pada kriptografi modern menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya, sehingga dapat disebut dengan algoritma asimetri. Kunci pada algoritma asimetri ini terbagi menjadi dua yaitu kunci umum (*public key*) di mana semua orang boleh tahu dan kunci privat (*private key*) di mana hanya boleh diketahui oleh satu orang. Seseorang dapat mengenkripsi pesan dengan kunci umum (*public key*) namun tidak dapat mendekripsinya karena hanya orang yang memiliki kunci pribadi (*private key*) yang dapat mendekripsi pesan tersebut. Contoh dari algoritma asimetri adalah *Riverst Shamir Adleman* (RSA), *Elliptic Curve Cryptography* (ECC), dan sebagainya (Munir, 2019).

Menurut definisi istilah, algoritma merupakan rangkaian langkah-langkah logis dalam pemecahan masalah yang disusun secara sistematis. Algoritma kriptografi adalah langkah-langkah logis mengenai cara menyandikan pesan dari oknum-oknum yang tidak memiliki hak atas pesan tersebut. Algoritma kriptografi ini bekerja dalam kombinasi dengan menggunakan kunci seperti kata, nomor atau frase tertentu. Algoritma kriptografi memiliki tiga fungsi dasar yaitu enkripsi, dekripsi dan kunci. Enkripsi adalah hal yang berperan penting dalam kriptografi di mana berupa pengamanan data yang akan dikirimkan dengan tujuan agar terjaga kerahasiaannya. Dalam proses enkripsi ini merubah plainteks menggunakan algoritma yang telah ditentukan menjadi cipherteks. Sedangkan dekripsi merupakan proses kebalikan dari enkripsi sehingga pesan dapat tersampaikan dan

dipahami oleh penerima. Dalam proses enkripsi dan dekripsi memerlukan sebuah parameter yang disebut dengan kunci (Ariyus, 2006).

2.1.8 *Vigenere-Multiplicative Cipher*

Vigenere Cipher ini dipublikasikan oleh Blaise de Vigenere pada tahun 1586, tetapi algoritma tersebut baru dikenal luas 200 tahun kemudian, yang diberi nama *Vigenere Cipher*. *Vigenere Cipher* adalah salah satu kriptografi klasik yang menggunakan satu kunci yang sama dalam proses enkripsi dan dekripsi. Setiap huruf plainteks yang sama dapat memiliki huruf cipherteks yang berbeda-beda bergantung pada huruf kunci yang dikenakan. Jadi, dengan menggunakan *Vigenere Cipher* kita dapat mencegah frekuensi huruf-huruf di dalam cipherteks mempunyai pola yang sama dengan frekuensi huruf-huruf di dalam plainteks (Munir, 2019).

Kelemahan dari *Vigenere Cipher* yaitu adanya pengulangan kunci yang berupa susunan huruf yang diulang secara periodik sesuai dengan panjang plainteks (Munir, 2019). Untuk mengurangi kelemahan *Vigenere Cipher*, maka *Vigenere Cipher* dikombinasikan dengan sebuah kriptografi klasik yaitu *Multiplicative Cipher*. *Multiplicative Cipher* adalah salah satu kriptografi klasik yang melibatkan operasi perkalian dari kunci rahasia dengan plainteks. Proses enkripsi dalam metode ini menggunakan sebarang bilangan bulat positif dan negatif sebagai kuncinya. Sebaliknya, dalam proses dekripsi menggunakan invers perkalian modulo dari kedua bilangan yang telah ditetapkan sebagai kunci enkripsi sebelumnya (Som & Ghosh, 2011).

Enkripsi dan dekripsi dengan *Vigenere Cipher* dapat dituliskan secara matematis. Misalkan kunci dengan panjang i adalah rangkaian $k_1 k_2 \dots k_i$, plainteks

adalah rangkaian $P_1P_2 \dots P_i$ dan cipherteks adalah rangkaian $C_1C_2 \dots C_i$, maka enkripsi pada *Vigenere Cipher* dapat dinyatakan sebagai berikut:

$$C_i = (P_i + k_i)\ (mod\ 26)$$

(Munir, 2019).

Dekripsi pada *Vigenere Cipher* dilakukan dengan cara yang berkebalikan di mana secara matematis dapat dinyatakan sebagai berikut:

$$P_i = (C_i - k_i)\ (mod\ 26)$$

di mana,

P_i : Nilai karakter plainteks ke-i

C_i : Nilai karakter cipherteks ke-i

k_i : Nilai karakter kunci ke-i

(Munir, 2019).

Enkripsi dan dekripsi pada *Multiplicative Cipher* dapat dituliskan secara matematis. Misalkan k_m adalah kunci enkripsi *Multiplicative Cipher* pertama, di mana berupa sebarang bilangan bulat positif, k_n adalah kunci enkripsi *Multiplicative Cipher* kedua, di mana berupa sebarang bilangan bulat negatif dan cipherteks adalah rangkaian $CT_1CT_2 \dots CT_t$ maka enkripsi pada *Multiplicative Cipher* dapat dinyatakan sebagai berikut:

$$CT_t = (C_i \times k_m \times k_n)\ (mod\ 26)$$

di mana,

CT_t : Nilai karakter cipherteks ke-t

C_i : Nilai karakter cipherteks ke-i

k_m : kunci enkripsi *Multiplicative Cipher* pertama

k_n : kunci enkripsi *Multiplicative Cipher* kedua

(Aung dkk, 2019).

Dekripsi pada *Multiplicative Cipher* dilakukan dengan cara yang berkebalikan. Kunci dekripsi diperoleh berdasarkan kunci enkripsi sebelumnya dengan melakukan operasi invers perkalian modulo di mana dapat dihitung menggunakan kekongruenan lanjar. Secara matematis dapat dinyatakan sebagai berikut:

$$PT_t = \left(CT_t \times {k_m}^{-1} \times {k_n}^{-1}\right)(mod\ 26)$$

di mana,

PT_t : Nilai karakter plainteks ke-t

CT_t : Nilai karakter cipherteks ke-t

${k_m}^{-1}$: kunci dekripsi *Multiplicative Cipher* pertama

${k_n}^{-1}$: kunci dekripsi *Multiplicative Cipher* kedua

(Aung dkk, 2019).

Contoh:

Tabel 2. 3 Indeks Karakter Plainteks pada *Vigenere-Multiplicative Cipher*

Karakter	A	B	C	D	E	F	G	H	I	J	K	L	M
Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12
Karakter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Indeks	13	14	15	16	17	18	19	20	21	22	23	24	25

Berdasarkan Tabel 2.3 diberikan sebuah plainteks yang digunakan adalah "**THIS IS A SECRET**" dengan kunci "**MOBILE**". Berikut ini adalah enkripsi menggunakan *Vigenere Cipher*:

Tabel 2. 4 Plainteks pada *Vigenere-Multiplicative Cipher*

Plainteks	T	H	I	S	I	S	A	S	E	C	R	E	T
Indeks	19	7	8	18	8	18	0	18	4	2	17	4	19
Kunci	M	O	B	I	L	E	M	O	B	I	L	E	M
Indeks	12	14	1	8	11	4	12	14	1	8	11	4	12

Berdasarkan Tabel 2.4 di atas, maka dapat dilakukan perhitungan enkripsi menggunakan *Vigenere Cipher* sebagai berikut:

$C_1 = (19 + 12)\ (mod\ 26) = 5$

$C_2 = (7 + 14)\ (mod\ 26) = 21$

$C_3 = (8 + 1)\ (mod\ 26) = 9$

$C_4 = (18 + 8)\ (mod\ 26) = 0$

$C_5 = (8 + 11)\ (mod\ 26) = 19$

$C_6 = (18 + 4)\ (mod\ 26) = 22$

$C_7 = (0 + 12)\ (mod\ 26) = 12$

$C_8 = (18 + 14)\ (mod\ 26) = 6$

$C_9 = (4 + 1)\ (mod\ 26) = 5$

$C_{10} = (2 + 8)\ (mod\ 26) = 10$

$C_{11} = (17 + 11)\ (mod\ 26) = 2$

$C_{12} = (4 + 4)\ (mod\ 26) = 8$

$C_{13} = (19 + 12)\ (mod\ 26) = 5$

Cipherteks sementara yang dihasilkan dari perhitungan enkripsi menggunakan *Vigenere Cipher* adalah FVJATWMGFKCIF.

Langkah selanjutnya yaitu melakukan proses enkripsi menggunakan *Multiplicative Cipher*. Plainteks pada *Multiplicative Cipher* didasarkan pada

cipherteks sementara yang telah diperoleh dari proses enkripsi menggunakan *Vigenere Cipher*, di mana $k_m = 3$ dan $k_n = -5$. Adapun perhitungan enkripsinya yaitu sebagai berikut:

$CT_1 = \big(5 \times 3 \times (-5)\big)(mod\ 26) = 3$

$CT_2 = \big(21 \times 3 \times (-5)\big)(mod\ 26) = 23$

$CT_3 = \big(9 \times 3 \times (-5)\big)(mod\ 26) = 21$

$CT_4 = \big(0 \times 3 \times (-5)\big)(mod\ 26) = 0$

$CT_5 = \big(19 \times 3 \times (-5)\big)(mod\ 26) = 1$

$CT_6 = \big(22 \times 3 \times (-5)\big)(mod\ 26) = 8$

$CT_7 = \big(12 \times 3 \times (-5)\big)(mod\ 26) = 2$

$CT_8 = \big(6 \times 3 \times (-5)\big)(mod\ 26) = 14$

$CT_9 = \big(5 \times 3 \times (-5)\big)(mod\ 26) = 3$

$CT_{10} = \big(10 \times 3 \times (-5)\big)(mod\ 26) = 6$

$CT_{11} = \big(2 \times 3 \times (-5)\big)(mod\ 26) = 22$

$CT_{12} = \big(8 \times 3 \times (-5)\big)(mod\ 26) = 10$

$CT_{13} = \big(5 \times 3 \times (-5)\big)(mod\ 26) = 3$

Cipherteks yang dihasilkan dari kedua metode adalah DXLDBICODGWKD.

Selanjutnya, melakukan proses dekripsi untuk mengembalikan cipherteks menjadi plainteks. Secara berurutan dengan mendahulukan proses dekripsi menggunakan *Multiplicative Cipher* kemudian dilanjutkan dengan proses dekripsi menggunakan *Vigenere Cipher* adalah sebagai berikut:

Pertama menentukan nilai ${k_m}^{-1}(mod\ n)$ yang dapat dihitung menggunakan kekongruenan lanjar.

Misalkan k_m adalah 3, maka dapat dituliskan sebagai

$$3^{-1}(mod\ 26) = x\ ,$$

berdasarkan definisi kekongruenan dapat dituliskan dalam hubungan kesamaan yaitu

$$3x \equiv 1(mod\ 26) \text{ atau } 3x = 1 + 26k\ ,$$

di mana dapat disusun menjadi bentuk

$$x = \frac{(1 + 26k)}{3}\ ,$$

dengan k adalah sebarang bilangan bulat yaitu $k = 0, \pm1, \pm2, \pm3, \cdots$

sedemikian sehingga

jika $k = 0$ maka $x = \frac{(1+26.0)}{3} = \frac{1}{3}$

jika $k = 1$ maka $x = \frac{(1+26.1)}{3} = \frac{27}{3} = 9$

dengan mencoba beberapa macam nilai k, maka untuk $k = 1$ diperoleh solusi x bilangan bulat. Jadi, $3^{-1}(mod\ 26) = 9$ karena $9 \cdot 3 \equiv 1\ (mod\ 26)$

Kemudian menentukan nilai ${k_n}^{-1}(mod\ n)$ yang dapat pula dihitung menggunakan kekongruenan lanjar.

Misalkan k_n adalah -5, maka dapat dituliskan sebagai

$$(-5)^{-1}(mod\ 26) = x\ ,$$

berdasarkan definisi kekongruenan dapat dituliskan dalam hubungan kesamaan yaitu

$$(-5)x \equiv 1(mod\ 26) \text{ atau } (-5)x = 1 + 26k\ ,$$

di mana dapat disusun menjadi bentuk

$$x = \frac{(1 + 26k)}{-5}\ ,$$

dengan k adalah sebarang bilangan bulat yaitu $k = 0, \pm1, \pm2, \pm3, \cdots$

sedemikian sehingga

jika $k = 0$ maka $x = \frac{(1+26.0)}{-5} = \frac{1}{-5}$

jika $k = -1$ maka $x = \frac{(1+26.(-1))}{-5} = \frac{-25}{-5} = 5$

dengan mencoba beberapa macam nilai k, maka untuk $k = -1$ diperoleh solusi x bilangan bulat. Jadi, $(-5)^{-1}(mod\ 26) = 5$ karena $(-5) \cdot 5 \equiv 1\ (mod\ 26)$

Langkah selanjutnya adalah melakukan perhitungan dekripsi menggunakan *Multiplicative Cipher* adalah sebagai berikut:

$PT_1 = (3 \times 9 \times 5)\ (mod\ 26) = 5$

$PT_2 = (23 \times 9 \times 5)\ (mod\ 26) = 21$

$PT_3 = (21 \times 9 \times 5)\ (mod\ 26) = 9$

$PT_4 = (0 \times 9 \times 5)\ (mod\ 26) = 0$

$PT_5 = (1 \times 9 \times 5)\ (mod\ 26) = 19$

$PT_6 = (8 \times 9 \times 5)\ (mod\ 26) = 22$

$PT_7 = (2 \times 9 \times 5)(mod\ 26) = 12$

$PT_8 = (14 \times 9 \times 5)(mod\ 26) = 6$

$PT_9 = (3 \times 9 \times 5)(mod\ 26) = 5$

$PT_{10} = (6 \times 9 \times 5)(mod\ 26) = 10$

$PT_{11} = (22 \times 9 \times 5)(mod\ 26) = 2$

$PT_{12} = (10 \times 9 \times 5)(mod\ 26) = 8$

$PT_{13} = (3 \times 9 \times 5)(mod\ 26) = 5$

Plainteks sementara yang dihasilkan dari perhitungan dekripsi menggunakan *Multiplicative Cipher* adalah FVJATWMGFKCIF.

Langkah selanjutnya yaitu melakukan proses dekripsi menggunakan *Vigenere Cipher*. Plainteks pada *Vigenere Cipher* didasarkan pada plainteks sementara yang telah diperoleh dari proses dekripsi menggunakan *Multiplicative Cipher*. Adapun perhitungan dekripsinya yaitu sebagai berikut:

$P_1 = (5 - 12)(mod\ 26) = 19$

$P_2 = (21 - 14)(mod\ 26) = 7$

$P_3 = (9 - 1)(mod\ 26) = 8$

$P_4 = (0 - 8)(mod\ 26) = 18$

$P_5 = (19 - 11)(mod\ 26) = 8$

$P_6 = (22 - 4)(mod\ 26) = 18$

$P_7 = (12 - 12)(mod\ 26) = 0$

$P_8 = (6 - 14)(mod\ 26) = 18$

$P_9 = (5 - 1)(mod\ 26) = 4$

$P_{10} = (10 - 8)(mod\ 26) = 2$

$P_{11} = (2 - 11)(mod\ 26) = 17$

$P_{12} = (8 - 4)(mod\ 26) = 4$

$P_{13} = (5 - 12)(mod\ 26) = 19$

Dengan demikian diperoleh kembali plainteks adalah THISISASECRET.

2.1.9 *Linear Block Cipher* (LBC)

Pada *block cipher*, rangkaian bit-bit plainteks dibagi menjadi blok-blok bit dengan panjang sama. Setiap blok bit plainteks dienkripsi dengan bit-bit kunci yang panjangnya sama dengan blok plainteks. Pada proses menghasilkan blok cipherteks yang berukuran sama dengan blok plainteks. Hal yang serupa juga berlaku pada

proses dekripsi dilakukan dengan cara yang sama seperti enkripsi, blok cipherteks dienkripsi dengan kunci yang sama (Munir, 2019).

Block cipher dimodifikasi dengan memanfaatkan aturan pembentukan kunci salah satunya yaitu menggunakan aturan *general linear group*. Perpaduan keduanya dapat dinamakan sebagai *Linear Block Cipher* (LBC). Metode *Linear Block Cipher* (LBC) adalah salah satu kriptografi klasik yang mana teknik penyandiannya menggunakan kunci simetri. (Kuppuswamy & Al-Maliki, 2021).

Contoh :

Tabel 2.5 Indeks Karakter Plainteks pada *Linear Block Cipher* (LBC)

Karakter	A	B	C	D	E	F	G	H	I	J	K	L	M
Indeks	1	2	3	4	5	6	7	8	9	10	11	12	13
Karakter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Indeks	14	15	16	17	18	19	20	21	22	23	24	25	26
Karakter	0	1	2	3	4	5	6	7	8	9	spasi		
Indeks	27	28	29	30	31	32	33	34	35	36	37		

Berdasarkan Tabel 2.5 di atas, dengan sebuah plainteks yang akan digunakan adalah EXTENDEDHILLCIPHER dengan kunci enkripsi yaitu:

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

dengan determinan matriks A adalah

$$\det(A) = \begin{vmatrix} 3 & 2 & 1 \\ 5 & 4 & 6 \\ 9 & 7 & 8 \end{vmatrix} = 34 \ (mod\ 37).$$

Kemudian, membagi plainteks menjadi blok-blok sesuai dengan kunci matriks yaitu 3×3 sebagai berikut:

Tabel 2.6 Blok-Blok Plainteks

E	E	E	I	C	H
X	N	D	L	I	E
T	D	H	L	P	R

Berdasarkan Tabel 2.6 maka langkah selanjutnya adalah mengkonversi plainteks ke $\mathbb{Z}_{37}$ dan membaginya ke dalam blok sebagai berikut:

Tabel 2.7 Blok Indeks Karakter Plainteks

5	5	5	9	3	8
24	14	4	12	9	5
20	4	8	12	16	18

Berdasarkan Tabel 2.7 di atas, maka dapat dilakukan perhitungan enkripsi menggunakan *Linear Block Cipher* (LBC) dengan melakukan operasi perkalian matriks antara kunci enkripsi dengan masing-masing blok yaitu sebagai berikut:

$$\begin{bmatrix}3 & 2 & 1\\5 & 4 & 6\\9 & 7 & 8\end{bmatrix}\begin{bmatrix}5\\24\\20\end{bmatrix}(mod\ 37)=\begin{bmatrix}83\\241\\373\end{bmatrix}(mod\ 37)=\begin{bmatrix}9\\19\\3\end{bmatrix}$$

$$\begin{bmatrix}3 & 2 & 1\\5 & 4 & 6\\9 & 7 & 8\end{bmatrix}\begin{bmatrix}5\\14\\4\end{bmatrix}(mod\ 37)=\begin{bmatrix}47\\105\\175\end{bmatrix}(mod\ 37)=\begin{bmatrix}10\\31\\27\end{bmatrix}$$

$$\begin{bmatrix}3 & 2 & 1\\5 & 4 & 6\\9 & 7 & 8\end{bmatrix}\begin{bmatrix}5\\4\\8\end{bmatrix}(mod\ 37)=\begin{bmatrix}31\\89\\137\end{bmatrix}(mod\ 37)=\begin{bmatrix}31\\15\\26\end{bmatrix}$$

$$\begin{bmatrix}3 & 2 & 1\\5 & 4 & 6\\9 & 7 & 8\end{bmatrix}\begin{bmatrix}9\\12\\12\end{bmatrix}(mod\ 37)=\begin{bmatrix}63\\165\\261\end{bmatrix}(mod\ 37)=\begin{bmatrix}26\\17\\2\end{bmatrix}$$

$$\begin{bmatrix}3 & 2 & 1\\5 & 4 & 6\\9 & 7 & 8\end{bmatrix}\begin{bmatrix}3\\9\\16\end{bmatrix}(mod\ 37)=\begin{bmatrix}43\\147\\218\end{bmatrix}(mod\ 37)=\begin{bmatrix}6\\36\\33\end{bmatrix}$$

$$\begin{bmatrix}3 & 2 & 1\\5 & 4 & 6\\9 & 7 & 8\end{bmatrix}\begin{bmatrix}8\\5\\18\end{bmatrix}(mod\ 37)=\begin{bmatrix}52\\168\\251\end{bmatrix}(mod\ 37)=\begin{bmatrix}15\\20\\29\end{bmatrix}$$

Cipherteks yang dihasilkan adalah ISCJ404OZZQBF96OT2.

Selanjutnya, proses dekripsi digunakan untuk mengembalikan cipherteks menjadi plainteks diawali dengan pembentukan kunci dekripsi pada *Linear Block Cipher* (LBC) menggunakan aturan *general linear group* adalah sebagai berikut:

1. Menunjukkan bahwa $\mathbb{Z}_{37}$ adalah lapangan berhingga.

   Berdasarkan Teorema 2.1 menyatakan bahwa $\mathbb{Z}_n$ adalah lapangan berhingga jika dan hanya jika n bilangan prima, maka terbukti bahwa $\mathbb{Z}_{37}$ adalah lapangan berhingga.

2. Membangun suatu *general linear group* yaitu $GL_3(\mathbb{Z}_{37})$ sebagai berikut:

   a. Menentukan determinan dari matriks A.

   $$det(A) = \begin{vmatrix} 3 & 2 & 1 \\ 5 & 4 & 6 \\ 9 & 7 & 8 \end{vmatrix} = 34 \ (mod\ 37)$$

   b. Lakukan operasi invers pada matriks A sebagai berikut:

   $$A^{-1} = \frac{1}{34}\begin{bmatrix} 27 & 28 & 8 \\ 14 & 15 & 24 \\ 36 & 34 & 2 \end{bmatrix} \in GL_3(\mathbb{Z}_{37})$$

   Bentuk $\frac{1}{34}$ atau bisa dituliskan sebagai 34^{-1} diubah menjadi bentuk bilangan bulat dengan melakukan operasi balikan modulo 37 yang dapat dihitung menggunakan kekongruenan lanjar:

   Misalkan

   $$34(mod\ 37) = x,$$

   berdasarkan definisi kekongruenan dapat dituliskan dalam hubungan kesamaan yaitu

   $$34x \equiv 1 \ (mod\ 37) \text{ atau } 34x = 1 + 37k.$$

   di mana dapat disusun menjadi bentuk

$$x = \frac{(1 + 37k)}{34}$$

dengan k adalah sebarang bilangan bulat yaitu $k = 0, \pm 1, \pm 2, \pm 3, \cdots$

sedemikian sehingga

jika $k = 0$ maka $x = \frac{(1+37.0)}{34} = \frac{1}{34}$

jika $k = 1$ maka $x = \frac{(1+37.1)}{34} = \frac{38}{34}$

jika $k = 2$ maka $x = \frac{(1+37.2)}{34} = \frac{75}{34}$

jika $k = 3$ maka $x = \frac{(1+37.3)}{34} = \frac{112}{34}$

$\vdots$

jika $k = 11$ maka $x = \frac{(1+37.11)}{34} = \frac{408}{34} = 12$

dengan mencoba beberapa macam nilai k, maka untuk $k = 11$ diperoleh solusi x bilangan bulat. Jadi, $34^{-1}(mod\ 37) = 12$ karena $34 \cdot 12 \equiv 1\ (mod\ 37)$ sehingga,

$$A^{-1} = 12\begin{bmatrix} 27 & 28 & 8 \\ 14 & 15 & 24 \\ 36 & 34 & 2 \end{bmatrix} = \begin{bmatrix} 28 & 3 & 22 \\ 20 & 32 & 29 \\ 25 & 1 & 24 \end{bmatrix} \in GL_3(\mathbb{Z}_{37})$$

Matriks A^{-1} ini akan ditetapkan sebagai kunci dekripsi *Linear Block Cipher* (LBC).

Selanjutnya, dapat dilakukan perhitungan dekripsi menggunakan *Linear Block Cipher* (LBC) dengan cara melakukan operasi perkalian matriks antara kunci dekripsi dengan masing-masing blok yaitu sebagai berikut:

$$\begin{bmatrix} 28 & 3 & 22 \\ 20 & 32 & 29 \\ 25 & 1 & 24 \end{bmatrix}\begin{bmatrix} 9 \\ 19 \\ 3 \end{bmatrix}(mod\ 37) = \begin{bmatrix} 375 \\ 875 \\ 316 \end{bmatrix}(mod\ 37) = \begin{bmatrix} 5 \\ 24 \\ 20 \end{bmatrix}$$

$$\begin{bmatrix} 28 & 3 & 22 \\ 20 & 32 & 29 \\ 25 & 1 & 24 \end{bmatrix}\begin{bmatrix} 10 \\ 31 \\ 27 \end{bmatrix}(mod\ 37) = \begin{bmatrix} 967 \\ 1975 \\ 929 \end{bmatrix}(mod\ 37) = \begin{bmatrix} 5 \\ 14 \\ 4 \end{bmatrix}$$

$$\begin{bmatrix}28 & 3 & 22\\ 20 & 32 & 29\\ 25 & 1 & 24\end{bmatrix}\begin{bmatrix}31\\ 15\\ 26\end{bmatrix}(mod\ 37)=\begin{bmatrix}1485\\ 1854\\ 1414\end{bmatrix}(mod\ 37)=\begin{bmatrix}5\\ 4\\ 8\end{bmatrix}$$

$$\begin{bmatrix}28 & 3 & 22\\ 20 & 32 & 29\\ 25 & 1 & 24\end{bmatrix}\begin{bmatrix}26\\ 17\\ 2\end{bmatrix}(mod\ 37)=\begin{bmatrix}823\\ 1122\\ 715\end{bmatrix}(mod\ 37)=\begin{bmatrix}9\\ 12\\ 12\end{bmatrix}$$

$$\begin{bmatrix}28 & 3 & 22\\ 20 & 32 & 29\\ 25 & 1 & 24\end{bmatrix}\begin{bmatrix}6\\ 36\\ 33\end{bmatrix}(mod\ 37)=\begin{bmatrix}1002\\ 2229\\ 978\end{bmatrix}(mod\ 37)=\begin{bmatrix}3\\ 9\\ 16\end{bmatrix}$$

$$\begin{bmatrix}28 & 3 & 22\\ 20 & 32 & 29\\ 25 & 1 & 24\end{bmatrix}\begin{bmatrix}15\\ 20\\ 29\end{bmatrix}(mod\ 37)=\begin{bmatrix}1118\\ 1781\\ 1091\end{bmatrix}(mod\ 37)=\begin{bmatrix}8\\ 5\\ 18\end{bmatrix}$$

Dengan demikian diperoleh kembali plainteks dari *Linear Block Cipher* (LBC) adalah EXTENDEDHILLCIPHER.

2.1.10 Python

Tahun 1991 pertama kali Python dikembangkan oleh programmer kelahiran Belanda bernama Guido van Rossum di CWI, Amsterdam sebagai kelanjutan dari bahasa pemrograman ABC. Guido memiliki ketertarikan pada acara televisi Monty Python's Flying Circus, sehingga ia memilih nama Python sebagai bahasa pemrograman ciptaannya. Sekelompok programmer yang dikoordinir oleh Guido dan *Python Software Foundation* terus melakukan pengembangan pada Python hingga saat ini. Kini, distribusi Python telah mencapai versi 3.7 (Enterprise, 2019).

Python merupakan bahasa pemrograman interpretatif yang dianggap mudah untuk dipelajari dan menekankan pada keterbacaan kode. Python memiliki keunggulan untuk menuntaskan pembuatan beberapa aplikasi berbasis kecerdasan buatan (*artificial intelligence*) yang memuat kata kunci big data, deep learning, data science, machine learning, serta data mining. Secara umum, Python berbentuk pemrograman fungsional, pemrograman imperatif, dan pemrograman berorientasi

objek. Berbagai keperluan pengembangan perangkat lunak yang dapat berjalan dengan platform sistem operasi juga bisa dilakukan oleh Python (Enterprise, 2019).

Dalam bahasa pemrograman Python terdapat beberapa fitur dan kelebihan diantaranya:

1. Telah tersedia koleksi kepustakaan yang banyak, beberapa modul pemrograman yang siap pakai untuk berbagai keperluan dalam pembuatan perangkat lunak.
2. Mempunyai struktur bahasa yang sederhana, mudah dipahami, dan jelas.
3. Mendukung multi-paradigma pemrograman yang berorientasi objek sekaligus prosedural.
4. Seperti dengan Java, Python mempunyai sistem pengelolaan memori otomatis atau yang disebut dengan *garbage collection*.
5. Pengembangan mudah dilakukan dengan menciptakan modul-modul baru yang dapat dibangun dengan bahasa Python.

(Enterprise, 2019).

2.2 Kajian Integrasi Topik dengan Al-Qur'an

Al-Qur'an merupakan wahyu dari Allah kepada Nabi Muhammad dengan perantara Malaikat Jibril sebagai tuntunan dan pedoman bagi umat Islam dalam menjalani kehidupan di dunia. Salah satu konsep yang paling mendasari dalam Al-Qur'an ialah amanah, karena pada hakikatnya dalam Al-Qur'an terdapat perintah dan larangan Allah di mana hal itu dapat dikatakan sebagai amanah bagi manusia dan semua makhluk ciptaan-Nya. Amanah merupakan wujud ketaatan manusia terhadap seluruh pokok ajaran Islam. Sebagai umat manusia yang telah diberi

amanah oleh orang lain, kita wajib menjaga kepercayaan tersebut karena dalam menjaga amanah berkaitan dengan menjaga hubungan dengan Allah serta menjaga hubungan sesama manusia (Hermawan dkk, 2020). Sebagaimana konsep amanah yang telah dijelaskan dalam Al-Qur'an surah Al-Anfal ayat 27 yang artinya:

"*Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul dan janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepada kamu, sedang kamu mengetahui*".

Menurut tafsir Al-Misbah yang dimaksud amanah Allah adalah segala sesuatu yang ada dalam genggaman manusia. Tidak hanya agama yang merupakan amanah Allah, akan tetapi bumi dan segala isinya, keluarga dan anak-anaknya serta jiwa dan raga tiap-tiap manusia dengan segala kemampuan yang melekat pada dirinya adalah amanah Allah. Sebagai umat Islam senantiasa wajib memelihara serta mengembangkan amanah dari Allah yang telah diberikan kepada diri kita masing-masing. Selain amanah Allah, ada beberapa hal yang berkaitan dengan amanah manusia terhadap manusia diantaranya penitipan harta benda, ikatan perjanjian yang telah disepakati sebelumnya bahkan sebuah rahasia yang dibisikkan. Seluruh amanah baik amanah Allah maupun amanah sesama manusia haram hukumnya jikalau mengkhianatinya. Khianat kepada Allah bersifat hakiki karena segala hal yang termasuk dalam apa yang diamanahkan oleh manusia terhadap manusia lain bersumber dari-Nya, berbeda dengan khianat kepada selain Allah bersifat majasi yang mengisyaratkan bahwa pengkhianatan amanah manusia tidak lebih kecil dosanya dan tidak lebih kurang dampak buruknya daripada mengkhianati Allah dan Rasul-Nya (Shihab, 2002).

Dalam perspektif Islam, makna kata amanah sangatlah luas yang mana mencakup perasaan manusia untuk melakukan sesuatu yang telah dipercayakan kepada dirinya berdasarkan kesadaran dan tanggung jawab masing-masing diri

kepada Allah. Amanah tidak lepas dari dua hal yakni lisan dan perbuatan, karena hal utama dalam amanah adalah memelihara dan menunaikan segala sesuatu yang telah dibebankan kepadanya terkait urusan agama maupun umum serta urusan dunia maupun akhirat (Hermawan dkk, 2020). Sebagaimana firman Allah yang ada dalam Al-Qur'an Surah Al-Ma'arij ayat 32 yang artinya:

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

Menurut Muhammad Naasib Ar-Rifa'i dalam buku ringkasan tafsir Ibnu Katsir yakni sebagai orang amanah apabila mereka diberi kepercayaan maka mereka tidak mengkhianatinya, akan tetapi mereka menunaikan amanah itu kepada yang berhak, apabila mereka dititipkan sesuatu tidak berkhianat, melainkan mereka akan menjaga amanah yang mereka emban, dan apabila berjanji tidak pernah melanggar janji-janji yang telah mereka buat. Lawan dari sifat amanah adalah sifat khianat. Selain dalam Al-Qur'an terdapat dalih hadis yang melarang seseorang untuk berkhianat karena sifat khianat adalah salah satu perbuatan orang-orang yang munafik sebagaimana sabda Rasulullah SAW yang artinya:

"*Tanda-tanda orang munafik ada tiga; jika berbicara berdusta, jika berjanji mengingkari, dan jika dipercaya berkhianat."(H.R. Bukhari, Muslim, Tirmidzi dan Nasa'i).*

(Ar-Rifa'i, 2000)

2.3 Kajian Topik dengan Teori Pendukung

Dalam penelitian ini disusun berdasarkan berbagai macam teori pendukung diantaranya yaitu kriptografi yang memiliki dua proses utama yakni enkripsi dan dekripsi. Enkripsi adalah proses mengubah plainteks menjadi cipherteks, sedangkan dekripsi adalah proses mengembalikan cipherteks menjadi plainteks.

Metode yang digunakan dalam proses enkripsi dan dekripsi adalah *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC). *Vigenere-Multiplicative Cipher* merupakan kriptografi klasik di mana menggunakan kunci simetri berupa kata kunci *Vigenere Cipher* dan bilangan bulat positif serta bilangan bulat negatif untuk proses enkripsinya. Sedangkan dalam proses dekripsinya tetap menggunakan kata kunci *Vigenere Cipher,* namun untuk kunci dekripsi pada *Multiplicative Cipher* menggunakan invers perkalian modulo dari kunci enkripsi sebelumnya. Adapun cara untuk menghitung invers perkalian modulo tersebut dapat menggunakan kekongruenan lanjar. Selanjutnya, *Linear Block Cipher* (LBC) adalah kriptografi klasik yang menggunakan kunci simetri berupa matriks persegi. Pembentukan kunci enkripsi dan dekripsi pada metode ini menggunakan aturan *general linear group*. Adapun proses enkripsi dan dekripsinya melibatkan perkalian matriks antara kunci dengan masing-masing blok. Dalam proses enkripsi dan dekripsi dari kedua algoritma peneliti menggunakan bantuan pemrograman Python yang dikenal sebagai bahasa pemrograman interpretatif yang dianggap mudah untuk dipahami serta memiliki kode-kode pemrograman yang lengkap dan jelas.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Metode yang digunakan dalam penelitian enkripsi dan dekripsi pada pesan teks menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC) adalah metode studi pustaka atau studi literatur yaitu penelitian yang dilakukan dengan cara mengumpulkan data dan informasi dengan mengkaji berbagai macam sumber literatur meliputi buku, jurnal, artikel, dan sebagainya yang berkaitan dengan topik penelitian.

3.2 Pra Penelitian

Dalam proses penelitian ini diawali dengan mengumpulkan serta memahami konsep-konsep yang mendasari topik penelitian dari berbagai sumber literatur. Langkah yang harus dilakukan adalah memahami landasan teori yang berkaitan dengan teori bilangan, matriks, *general linear group*, kriptografi dan klasifikasinya serta mengkaji beberapa ayat dalam Al-Qur'an yang dapat diintegrasikan dengan topik penelitian ini.

3.3 Tahapan Penelitian

3.3.1 Proses Enkripsi Menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC)

Adapun langkah-langkah pada proses enkripsi menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC) adalah sebagai berikut:

1. Menetapkan indeks karakter dari plainteks.
2. Mengkonversi plainteks menurut indeks karakter yang telah ditetapkan.
3. Menunjukkan bahwa $\mathbb{Z}_{59}$ adalah lapangan berhingga.
4. Membangun suatu *general linear group* yaitu $GL_4(\mathbb{Z}_{59})$.
5. Melakukan simulasi untuk proses enkripsi pesan menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC).

3.3.2 Proses Dekripsi Menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC)

Adapun langkah-langkah pada proses dekripsi menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC) adalah sebagai berikut:

1. Menunjukkan bahwa $\mathbb{Z}_{59}$ adalah lapangan berhingga.
2. Membangun suatu *general linear group* yaitu $GL_4(\mathbb{Z}_{59})$.
3. Melakukan simulasi untuk proses dekripsi pesan menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC).

BAB IV
HASIL DAN PEMBAHASAN

4.1 Proses Enkripsi Menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC)

Proses enkripsi akan dilakukan menggunakan dua metode, yaitu *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC) secara berurutan. Adapun proses enkripsi menggunakan *Vigenere-Multiplicative Cipher* adalah sebagai berikut:

1. Menetapkan indeks karakter dari plainteks.

Tabel 4.1 Indeks Karakter dari Plainteks

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
0	1	2	3	4	5	6	7	8	9
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
10	11	12	13	14	15	16	17	18	19
U	**V**	**W**	**X**	**Y**	**Z**	**0**	**1**	**2**	**3**
20	21	22	23	24	25	26	27	28	29
4	**5**	**6**	**7**	**8**	**9**	**spasi**	**!**	**“**	**#**
30	31	32	33	34	35	36	37	38	39
$	**%**	**&**	**‘**	**(**	**)**	*****	**+**	**,**	**-**
40	41	42	43	44	45	46	47	48	49
.	**/**	**:**	**;**	<	=	>	**?**	**@**	
50	51	52	53	54	55	56	57	58	

2. Mengkonversi plainteks (P_i) yang akan dienkripsi menurut indeks karakter yang telah ditetapkan.

   Plainteks : PROGRAM STUDI MATEMATIKA 2018###

Tabel 4.2 Konversi Plainteks

P	**R**	**O**	**G**	**R**	**A**	**M**	**spasi**	**S**	**T**	**U**
15	17	14	6	17	0	12	36	18	19	20
D	**I**	**spasi**	**M**	**A**	**T**	**E**	**M**	**A**	**T**	**I**
3	8	36	12	0	19	4	12	0	19	8
K	**A**	**spasi**	**2**	**0**	**1**	**8**	**#**	**#**	**#**	
10	**0**	36	28	26	27	34	39	39	39	

3. Menunjukkan bahwa $\mathbb{Z}_{59}$ adalah lapangan berhingga.

   Berdasarkan Teorema 2.1 menyatakan bahwa $\mathbb{Z}_n$ adalah lapangan berhingga jika dan hanya jika n bilangan prima.

   Bukti:

   ($\Rightarrow$) Akan ditunjukkan $\mathbb{Z}_{59}$ merupakan lapangan berhingga jika 59 bilangan prima.

   Andaikan jika n bukan bilangan prima, maka n adalah bilangan bulat komposit yang berarti bahwa $n = ab$, di mana a dan b adalah bilangan prima, $a > 1, b < n - 1$. Pilih $n = 58$, maka $n = 2 \cdot 29$ di mana 2 dan 29 adalah bilangan prima. Karena $\mathbb{Z}_n$ merupakan lapangan, maka setiap elemen yang tak nolnya pasti memiliki invers. Misalkan c adalah invers dari b, yang berarti bahwa $bc \equiv 1(mod\ n)$ atau $29 \cdot 29^{-1} \equiv 1(mod\ 58)$ dan $abc \equiv a(mod\ n)$ atau $2 \cdot 29 \cdot 29^{-1} \equiv 2(mod\ 58)$. Karena $58 = 2 \cdot 29$ maka $2 \cdot 29 \equiv 0(mod\ 58)$. Hal ini kontradiksi dengan pengandaian bahwa n bukan bilangan prima. Jadi, haruslah n bilangan prima.

($\Leftarrow$) Akan ditunjukkan 59 bilangan prima jika $\mathbb{Z}_{59}$ merupakan lapangan berhingga.

Diketahui 59 bilangan prima. Untuk dapat membuktikan bahwa $\mathbb{Z}_{59}$ merupakan lapangan, maka akan dibuktikan bahwa setiap elemen tak nolnya memiliki invers. Pilih $a = 2$, maka PBB$(59,2) = 1$, untuk $0 < 2 < 59$. Dengan kata lain, 59 dan 2 adalah dua buah bilangan bulat yang relatif prima. Akibatnya terdapat bilangan bulat x dan y sedemikian sehingga $-1 \cdot 59 + 30 \cdot 2 = 1$ yang berarti bahwa $30 \cdot 2 \equiv 1(mod\ 59)$, diperoleh $30 \equiv 2^{-1}(mod\ 59)$. Terbukti bahwa setiap elemen tak nolnya memiliki invers. Jadi $\mathbb{Z}_{59}$ merupakan lapangan karena 59 bilangan prima. Karena $\mathbb{Z}_{59}$ memiliki unsur berhingga maka $\mathbb{Z}_{59}$ merupakan lapangan berhingga (A.Vanstone & Oorschot, 1989). ■

4. Membangun suatu *general linear group* yaitu $GL_4(\mathbb{Z}_{59})$ untuk pembentukan kunci enkripsi pada *Linear Block Cipher* (LBC)

$$A = \begin{bmatrix} 4 & 2 & 2 & 3 \\ 2 & 5 & 1 & 2 \\ 3 & 2 & 4 & 3 \\ 7 & 4 & 3 & 2 \end{bmatrix} \in GL_4(\mathbb{Z}_{59})$$

$$|A| = \begin{vmatrix} 4 & 2 & 2 & 3 \\ 2 & 5 & 1 & 2 \\ 3 & 2 & 4 & 3 \\ 7 & 4 & 3 & 2 \end{vmatrix} = 50\ (mod\ 59)$$

Determinan dari matriks A adalah $50\ (mod\ 59)$, di mana tidak sama dengan nol, yang berarti bahwa matriks A dapat digunakan sebagai kunci enkripsi.

5. Melakukan simulasi untuk proses enkripsi menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC) adalah sebagai berikut:

a. Menentukan kunci enkripsi pada *Vigenere-Multiplicative Cipher* dengan kata kunci *Vigenere Cipher* yaitu M4LAN6.

b. Mengkonversi kata kunci *Vigenere Cipher* (k_i) menurut indeks karakter yang telah ditetapkan.

Tabel 4.3 Kata Kunci Enkripsi *Vigenere Cipher*

k_1	k_2	k_3	k_4	k_5	k_6
M	**4**	**L**	**A**	**N**	**6**
12	30	11	0	13	32

c. Menentukan kunci *Multiplicative Cipher* pertama dengan memilih sebarang bilangan bulat positif, sebut sebagai "k_m". Bilangan bulat positif yaitu:

$$k_m = 25$$

Kunci *Multiplicative Cipher* pertama atau k_m ini akan ditetapkan sebagai kunci enkripsi.

d. Menentukan kunci *Multiplicative Cipher* kedua dengan memilih sebarang bilangan bulat negatif, sebut sebagai "k_n". Bilangan bulat negatif yaitu:

$$k_n = -7$$

Kunci *Multiplicative Cipher* kedua atau k_n ini akan ditetapkan sebagai kunci enkripsi.

e. Lakukan perhitungan enkripsi menggunakan *Vigenere-Multiplicative Cipher* dengan rumus yaitu:

$$C_i = (P_i + k_i) \times k_m \times k_n \ (mod\ 59)$$

Adapun perhitungan enkripsinya adalah sebagai berikut:

$C_1 = (15 + 12) \times 25 \times (-7)(mod\ 59) = 54$

$C_2 = (17 + 30) \times 25 \times (-7)(mod\ 59) = 35$

$C_3 = (14 + 11) \times 25 \times (-7)(mod\ 59) = 50$

$C_4 = (6 + 0) \times 25 \times (-7)(mod\ 59) = 12$

$C_5 = (17 + 13) \times 25 \times (-7)(mod\ 59) = 1$

$C_6 = (0 + 32) \times 25 \times (-7)(mod\ 59) = 5$

$C_7 = (12 + 12) \times 25 \times (-7)(mod\ 59) = 48$

$C_8 = (36 + 30) \times 25 \times (-7)(mod\ 59) = 14$

$C_9 = (18 + 11) \times 25 \times (-7)(mod\ 59) = 58$

$C_{10} = (19 + 0) \times 25 \times (-7)(mod\ 59) = 38$

$C_{11} = (20 + 13) \times 25 \times (-7)(mod\ 59) = 7$

$C_{12} = (3 + 32) \times 25 \times (-7)(mod\ 59) = 11$

$C_{13} = (8 + 12) \times 25 \times (-7)(modM\ 59) = 40$

$C_{14} = (36 + 30) \times 25 \times (-7)(mod\ 59) = 14$

$C_{15} = (12 + 11) \times 25 \times (-7)(mod\ 59) = 46$

$C_{16} = (0 + 0) \times 25 \times (-7)(mod\ 59) = 0$

$C_{17} = (19 + 13) \times 25 \times (-7)(mod\ 59) = 5$

$C_{18} = (4 + 32) \times 25 \times (-7)(mod\ 59) = 13$

$C_{19} = (12 + 12) \times 25 \times (-7)(mod\ 59) = 48$

$C_{20} = (0 + 30) \times 25 \times (-7)(mod\ 59) = 1$

$C_{21} = (19 + 11) \times 25 \times (-7)(mod\ 59) = 1$

$C_{22} = (8 + 0) \times 25 \times (-7)(mod\ 59) = 16$

$C_{23} = (10 + 13) \times 25 \times (-7)(mod\ 59) = 46$

$C_{24} = (0 + 32) \times 25 \times (-7)\ (mod\ 59) = 5$

$C_{25} = (36 + 12) \times 25 \times (-7)\ (mod\ 59) = 37$

$C_{26} = (28 + 30) \times 25 \times (-7)\ (mod\ 59) = 57$

$C_{27} = (26 + 11) \times 25 \times (-7)(mod\ 59) = 15$

$C_{28} = (27 + 0) \times 25 \times (-7)\ (mod\ 59) = 54$

$C_{29} = (34 + 13) \times 25 \times (-7)\ (mod\ 59) = 35$

$C_{30} = (39 + 32) \times 25 \times (-7)(mod\ 59) = 24$

$C_{31} = (39 + 12) \times 25 \times (-7)(mod\ 59) = 43$

$C_{32} = (39 + 30) \times 25 \times (-7)(mod\ 59) = 20$

Cipherteks sementara yang dihasilkan dari *Vigenere-Multiplicative Cipher* adalah <9.MBF,O@“HL$O*AFN,BBQ*F!?P<9Y‘U

f. Menentukan plainteks pada pada *Linear Block Cipher* (LBC) yang didasarkan pada cipherteks sementara dari *Vigenere-Multiplicative Cipher*.

g. Membagi indeks karakter dari plainteks menjadi 4 blok yaitu sebagai berikut:

Tabel 4.4 Blok Indeks Karakter Cipherteks Sementara

54	1	58	40	5	1	37	35
35	5	38	14	13	6	57	24
50	48	7	46	48	46	15	43
12	14	11	0	1	5	54	20

h. Lakukan perhitungan enkripsi menggunakan *Linear Block Cipher* (LBC) dengan cara melakukan operasi perkalian matriks kunci enkripsi dengan masing-masing blok yaitu sebagai berikut:

$$\begin{bmatrix} 4 & 2 & 2 & 3 \\ 2 & 5 & 1 & 2 \\ 3 & 2 & 4 & 3 \\ 7 & 4 & 3 & 2 \end{bmatrix} \begin{bmatrix} 54 \\ 35 \\ 50 \\ 12 \end{bmatrix} (mod\ 59) = \begin{bmatrix} 422 \\ 357 \\ 468 \\ 692 \end{bmatrix} (mod\ 59) = \begin{bmatrix} 9 \\ 3 \\ 55 \\ 43 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 2 & 2 & 3 \\ 2 & 5 & 1 & 2 \\ 3 & 2 & 4 & 3 \\ 7 & 4 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 5 \\ 48 \\ 14 \end{bmatrix} (mod\ 59) = \begin{bmatrix} 152 \\ 103 \\ 247 \\ 199 \end{bmatrix} (mod\ 59) = \begin{bmatrix} 34 \\ 44 \\ 11 \\ 22 \end{bmatrix}$$

$$\begin{bmatrix}4&2&2&3\\2&5&1&2\\3&2&4&3\\7&4&3&2\end{bmatrix}\begin{bmatrix}58\\38\\7\\11\end{bmatrix}(mod\ 59)=\begin{bmatrix}355\\335\\311\\601\end{bmatrix}(mod\ 59)=\begin{bmatrix}1\\40\\16\\11\end{bmatrix}$$

$$\begin{bmatrix}4&2&2&3\\2&5&1&2\\3&2&4&3\\7&4&3&2\end{bmatrix}\begin{bmatrix}40\\14\\46\\0\end{bmatrix}(mod\ 59)=\begin{bmatrix}280\\196\\332\\474\end{bmatrix}(mod\ 59)=\begin{bmatrix}44\\19\\37\\2\end{bmatrix}$$

$$\begin{bmatrix}4&2&2&3\\2&5&1&2\\3&2&4&3\\7&4&3&2\end{bmatrix}\begin{bmatrix}5\\13\\48\\1\end{bmatrix}(mod\ 59)=\begin{bmatrix}145\\125\\236\\233\end{bmatrix}(mod\ 59)=\begin{bmatrix}27\\7\\0\\56\end{bmatrix}$$

$$\begin{bmatrix}4&2&2&3\\2&5&1&2\\3&2&4&3\\7&4&3&2\end{bmatrix}\begin{bmatrix}1\\16\\46\\5\end{bmatrix}(mod\ 59)=\begin{bmatrix}143\\138\\234\\219\end{bmatrix}(mod\ 59)=\begin{bmatrix}25\\20\\57\\42\end{bmatrix}$$

$$\begin{bmatrix}4&2&2&3\\2&5&1&2\\3&2&4&3\\7&4&3&2\end{bmatrix}\begin{bmatrix}37\\57\\15\\54\end{bmatrix}(mod\ 59)=\begin{bmatrix}454\\482\\447\\640\end{bmatrix}(mod\ 59)=\begin{bmatrix}41\\10\\34\\50\end{bmatrix}$$

$$\begin{bmatrix}4&2&2&3\\2&5&1&2\\3&2&4&3\\7&4&3&2\end{bmatrix}\begin{bmatrix}35\\24\\43\\20\end{bmatrix}(mod\ 59)=\begin{bmatrix}334\\273\\385\\510\end{bmatrix}(mod\ 59)=\begin{bmatrix}39\\37\\31\\38\end{bmatrix}$$

Dari hasil perhitungan enkripsi di atas dapat dituliskan dalam tabel berikut:

Tabel 4.5 Hasil Enkripsi

Indeks Karakter Cipherteks	Cipherteks
9, 3, 55, 43	JD=‘
34, 44, 11, 22	8(LW
1, 40, 16, 11	B$QL
44, 19, 37, 2	(T!C
27, 7, 0, 56	1HA>
25, 20, 57, 42	ZU?&
41, 10, 34, 50	%K8.
39, 37, 31, 38	#!5“

Dengan demikian, cipherteks yang dihasilkan dari kedua metode yaitu *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC) adalah JD=‘8(LWB$QL(T!C1HA> ZU?& %K8. #!5“

4.2 Proses Dekripsi Menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC)

Proses dekripsi digunakan untuk mengembalikan cipherteks menjadi plainteks yang berisi makna pesan aslinya. Secara berurutan proses dekripsi yang mana mendahulukan proses dekripsi *Linear Block Cipher* (LBC) kemudian dilanjutkan dengan dekripsi *Vigenere-Multiplicative Cipher*. Dalam proses dekripsi ini menggunakan cipherteks yang diperoleh dari proses enkripsi dari kedua metode yaitu *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC) pada pembahasan sebelumnya.

Adapun proses dekripsi menggunakan *Linear Block Cipher* (LBC) adalah sebagai berikut:

1. Menunjukkan bahwa $\mathbb{Z}_{59}$ adalah lapangan berhingga.

   Berdasarkan Teorema 2.1 menyatakan bahwa $\mathbb{Z}_n$ adalah lapangan berhingga jika dan hanya jika n bilangan prima.

   Bukti:

   ($\Rightarrow$) Akan ditunjukkan $\mathbb{Z}_{59}$ merupakan lapangan berhingga jika 59 bilangan prima.

   Andaikan jika n bukan bilangan prima, maka n adalah bilangan bulat komposit yang berarti bahwa $n = ab$, di mana a dan b adalah bilangan prima, $a > 1, b < n - 1$. Pilih $n = 58$, maka $n = 2 \cdot 29$ di mana 2 dan 29 adalah bilangan prima. Karena $\mathbb{Z}_n$ merupakan lapangan, maka setiap elemen

yang tak nolnya pasti memiliki invers. Misalkan c adalah invers dari b, yang berarti bahwa $bc \equiv 1(mod\ n)$ atau $29 \cdot 29^{-1} \equiv 1(mod\ 58)$ dan $abc \equiv a(mod\ n)$ atau $2 \cdot 29 \cdot 29^{-1} \equiv 2(mod\ 58)$. Karena $58 = 2 \cdot 29$ maka $2 \cdot 29 \equiv 0(mod\ 58)$. Hal ini kontradiksi dengan pengandaian bahwa n bukan bilangan prima. Jadi, haruslah n bilangan prima.

($\Leftarrow$) Akan ditunjukkan 59 bilangan prima jika $\mathbb{Z}_{59}$ merupakan lapangan berhingga.

Diketahui 59 bilangan prima. Untuk dapat membuktikan bahwa $\mathbb{Z}_{59}$ merupakan lapangan, maka akan dibuktikan bahwa setiap elemen tak nolnya memiliki invers. Pilih $a = 2$, maka $\text{PBB}(59,2) = 1$, untuk $0 < 2 < 59$. Dengan kata lain, 59 dan 2 adalah dua buah bilangan bulat yang relatif prima. Akibatnya terdapat bilangan bulat x dan y sedemikian sehingga $-1 \cdot 59 + 30 \cdot 2 = 1$ yang berarti bahwa $30 \cdot 2 \equiv 1(mod\ 59)$, diperoleh $30 \equiv 2^{-1}(mod\ 59)$. Terbukti bahwa setiap elemen tak nolnya memiliki invers. Jadi $\mathbb{Z}_{59}$ merupakan lapangan karena 59 bilangan prima. Karena $\mathbb{Z}_{59}$ memiliki unsur berhingga maka $\mathbb{Z}_{59}$ merupakan lapangan berhingga (A.Vanstone & Oorschot, 1989). ■

2. Membangun suatu *general linear group* yaitu $GL(4, \mathbb{Z}_{59})$ untuk pembentukan kunci dekripsi pada *Linear Block Cipher* (LBC)

$$A = \begin{bmatrix} 4 & 2 & 2 & 3 \\ 2 & 5 & 1 & 2 \\ 3 & 2 & 4 & 3 \\ 7 & 4 & 3 & 2 \end{bmatrix} \in GL_4(\mathbb{Z}_{59})$$

$$|A| = \begin{vmatrix} 4 & 2 & 2 & 3 \\ 2 & 5 & 1 & 2 \\ 3 & 2 & 4 & 3 \\ 7 & 4 & 3 & 2 \end{vmatrix} = 50\ (mod\ 59)$$

Kemudian, lakukan operasi invers pada matriks A sebagai berikut:

$$A^{-1} = \frac{1}{50}\begin{bmatrix} 42 & 16 & 21 & 37 \\ 25 & 28 & 58 & 54 \\ 55 & 8 & 6 & 48 \\ 45 & 53 & 8 & 40 \end{bmatrix} \in GL_4(\mathbb{Z}_{59})$$

Bentuk $\frac{1}{50}$ atau bisa dituliskan sebagai 50^{-1} diubah menjadi bentuk bilangan bulat dengan melakukan operasi balikan modulo 59 yang dapat dihitung menggunakan kekongruenan lanjar:

Misalkan

$$50^{-1}(mod\ 59) = x,$$

berdasarkan definisi kekongruenan dapat ditulis dalam hubungan kesamaan yaitu

$$50x \equiv 1\ (mod\ 59) \text{ atau } 50x = 1 + 59k,$$

di mana dapat disusun menjadi bentuk

$$x = \frac{(1 + 59k)}{50}$$

dengan k adalah sebarang bilangan bulat yaitu $k = 0, \pm1, \pm2, \pm3, \cdots$

sedemikian sehingga

jika $k = 0$ maka $x = \frac{(1+59\cdot0)}{50} = \frac{1}{50}$

jika $k = 1$ maka $x = \frac{(1+59\cdot1)}{50} = \frac{60}{50}$

jika $k = 2$ maka $x = \frac{(1+59\cdot2)}{50} = \frac{119}{50}$

jika $k = 3$ maka $x = \frac{(1+59\cdot3)}{50} = \frac{178}{50}$

$\vdots$

jika $k = 11$ maka $x = \frac{(1+59\cdot11)}{50} = \frac{650}{50} = 13$

dengan mencoba beberapa macam nilai k, maka untuk $k = 11$ diperoleh solusi x bilangan bulat. Jadi, $50^{-1}(mod\ 59) = 13$ karena $50 \cdot 13 \equiv 1\ (mod\ 59)$ sehingga,

$$A^{-1} = 13 \begin{bmatrix} 42 & 16 & 21 & 37 \\ 25 & 28 & 58 & 54 \\ 55 & 8 & 6 & 48 \\ 45 & 53 & 8 & 40 \end{bmatrix} = \begin{bmatrix} 15 & 31 & 37 & 9 \\ 30 & 10 & 46 & 53 \\ 7 & 45 & 19 & 34 \\ 54 & 40 & 45 & 48 \end{bmatrix} \in GL_4(\mathbb{Z}_{59})$$

Periksa bahwa perkalian matriks A dengan matriks A^{-1} adalah matriks identitas.

$$\begin{bmatrix} 4 & 2 & 2 & 3 \\ 2 & 5 & 1 & 2 \\ 3 & 2 & 4 & 3 \\ 7 & 4 & 3 & 2 \end{bmatrix} \begin{bmatrix} 15 & 31 & 37 & 9 \\ 30 & 10 & 46 & 53 \\ 7 & 45 & 19 & 34 \\ 54 & 40 & 45 & 48 \end{bmatrix} (mod\ 59) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Dengan demikian, A^{-1} ditetapkan sebagai kunci dekripsi *Linear Block Cipher* (LBC).

3. Melakukan simulasi untuk proses dekripsi menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC) yaitu sebagai berikut:

a. Atur indeks karakter pada pesan teks yang telah terenkripsi menjadi 4 blok sesuai dengan k matriks.

Tabel 4. 6 Blok Indeks Karakter Plainteks Sementara

9	34	1	44	27	25	41	39
3	44	40	19	7	20	10	37
55	11	16	37	0	57	34	31
43	22	11	2	56	42	50	38

b. Lakukan perhitungan dekripsi menggunakan operasi perkalian matriks dari kunci dekripsi dengan masing-masing blok.

$$\begin{bmatrix}15 & 31 & 37 & 9\\ 30 & 10 & 46 & 53\\ 7 & 45 & 19 & 34\\ 54 & 40 & 45 & 48\end{bmatrix}\begin{bmatrix}9\\3\\55\\43\end{bmatrix}(mod\ 59)=\begin{bmatrix}2650\\5109\\2705\\5145\end{bmatrix}(mod\ 59)=\begin{bmatrix}54\\35\\50\\12\end{bmatrix}$$

$$\begin{bmatrix}15 & 31 & 37 & 9\\ 30 & 10 & 46 & 53\\ 7 & 45 & 19 & 34\\ 54 & 40 & 45 & 48\end{bmatrix}\begin{bmatrix}34\\44\\11\\22\end{bmatrix}(mod\ 59)=\begin{bmatrix}2479\\3132\\3175\\5147\end{bmatrix}(mod\ 59)=\begin{bmatrix}1\\5\\48\\14\end{bmatrix}$$

$$\begin{bmatrix}15 & 31 & 37 & 9\\ 30 & 10 & 46 & 53\\ 7 & 45 & 19 & 34\\ 54 & 40 & 45 & 48\end{bmatrix}\begin{bmatrix}1\\40\\16\\11\end{bmatrix}(mod\ 59)=\begin{bmatrix}1946\\1749\\2485\\2902\end{bmatrix}(mod\ 59)=\begin{bmatrix}58\\38\\7\\11\end{bmatrix}$$

$$\begin{bmatrix}15 & 31 & 37 & 9\\ 30 & 10 & 46 & 53\\ 7 & 45 & 19 & 34\\ 54 & 40 & 45 & 48\end{bmatrix}\begin{bmatrix}44\\19\\37\\2\end{bmatrix}(mod\ 59)=\begin{bmatrix}2636\\3318\\1934\\4897\end{bmatrix}(mod\ 59)=\begin{bmatrix}40\\14\\46\\0\end{bmatrix}$$

$$\begin{bmatrix}15 & 31 & 37 & 9\\ 30 & 10 & 46 & 53\\ 7 & 45 & 19 & 34\\ 54 & 40 & 45 & 48\end{bmatrix}\begin{bmatrix}27\\7\\0\\56\end{bmatrix}(mod\ 59)=\begin{bmatrix}1126\\3848\\2408\\4426\end{bmatrix}(mod\ 59)=\begin{bmatrix}5\\13\\48\\1\end{bmatrix}$$

$$\begin{bmatrix}15 & 31 & 37 & 9\\ 30 & 10 & 46 & 53\\ 7 & 45 & 19 & 34\\ 54 & 40 & 45 & 48\end{bmatrix}\begin{bmatrix}25\\20\\57\\42\end{bmatrix}(mod\ 59)=\begin{bmatrix}3482\\5798\\3586\\6731\end{bmatrix}(mod\ 59)=\begin{bmatrix}1\\16\\46\\5\end{bmatrix}$$

$$\begin{bmatrix}15 & 31 & 37 & 9\\ 30 & 10 & 46 & 53\\ 7 & 45 & 19 & 34\\ 54 & 40 & 45 & 48\end{bmatrix}\begin{bmatrix}41\\10\\34\\50\end{bmatrix}(mod\ 59)=\begin{bmatrix}2633\\5544\\3083\\6544\end{bmatrix}(mod\ 59)=\begin{bmatrix}37\\57\\15\\54\end{bmatrix}$$

$$\begin{bmatrix}15 & 31 & 37 & 9\\ 30 & 10 & 46 & 53\\ 7 & 45 & 19 & 34\\ 54 & 40 & 45 & 48\end{bmatrix}\begin{bmatrix}39\\37\\31\\38\end{bmatrix}(mod\ 59)=\begin{bmatrix}3221\\4980\\3819\\6805\end{bmatrix}(mod\ 59)=\begin{bmatrix}35\\24\\43\\20\end{bmatrix}$$

Berdasarkan hasil perhitungan yang diperoleh dari proses dekripsi pada *Linear Block Cipher* (LBC), maka indeks karakter plainteks tersebut akan digunakan sebagai indeks karakter cipherteks pada proses dekripsi menggunakan *Vigenere-Multiplicative Cipher*. Adapun proses dekripsi menggunakan *Vigenere-Multiplicative Cipher* adalah sebagai berikut:

c. Kata kunci dekripsi pada *Vigenere Cipher* sama dengan kata kunci enkripsinya yaitu sebagai berikut:

Tabel 4.7 Kata Kunci Dekripsi *Vigenere Cipher*

k_1	k_2	k_3	k_4	k_5	k_6
M	**4**	**L**	**A**	**N**	**6**
12	30	11	0	13	32

Kata kunci ini akan diulang sesuai dengan banyaknya jumlah cipherteks.

d. Menentukan kunci dekripsi pertama pada *Multiplicative Cipher* yang mana berdasarkan kunci enkripsi yang telah ditetapkan sebelumnya dengan melakukan operasi balikan modulo 59, sebut sebagai "$k_m{}^{-1}$".

Diketahui:

$$k_m = 25$$

maka $k_m{}^{-1}$ dapat dihitung menggunakan kekongruenan lanjar

$$25^{-1}(mod\ 59) = x,$$

berdasarkan definisi kekongruenan dapat dituliskan dalam hubungan kesamaan yaitu

$$25x \equiv 1\ (mod\ 59) \text{ atau } 25x = 1 + 59k,$$

di mana dapat disusun menjadi bentuk

$$x = \frac{(1 + 59k)}{25}$$

dengan k adalah sebarang bilangan bulat yaitu $k = 0, \pm1, \pm2, \pm3, \cdots$

sedemikian sehingga

jika $k = 0$ maka $x = \frac{(1+59\cdot0)}{25} = \frac{1}{25}$

jika $k = 1$ maka $x = \frac{(1+59\cdot1)}{25} = \frac{60}{25}$

jika $k = 2$ maka $x = \frac{(1+59\cdot 2)}{25} = \frac{119}{25}$

⋮

jika $k = 11$ maka $x = \frac{(1+59\cdot 11)}{25} = \frac{650}{25} = 26$

dengan mencoba beberapa macam nilai k, maka untuk $k = 11$ diperoleh solusi x bilangan bulat. Jadi, $25^{-1}\ (mod\ 59) = 26$ karena $25 \cdot 26 \equiv 1(mod\ 59)$. Invers dari kunci enkripsi atau ${k_m}^{-1}$ ini akan ditetapkan sebagai kunci dekripsi pertama pada *Multiplicative Cipher*.

e. Menentukan kunci dekripsi kedua pada *Multiplicative Cipher* yang mana berdasarkan kunci enkripsi yang telah ditetapkan sebelumnya dengan melakukan operasi balikan modulo 59, sebut sebagai "${k_n}^{-1}$".

Diketahui:

$$k_n = -7$$

maka ${k_n}^{-1}$ dapat dihitung menggunakan kekongruenan lanjar

$$(-7)^{-1}(mod\ 59) = x,$$

berdasarkan definisi kekongruenan dapat dituliskan dalam hubungan kesamaaan yaitu

$$(-7)x \equiv 1\ (mod\ 59) \text{ atau } (-7)x = 1 + 59k,$$

di mana dapat disusun menjadi bentuk

$$x = \frac{(1 + 59k)}{-7}$$

dengan k adalah sebarang bilangan bulat yaitu $k = 0, \pm 1, \pm 2, \pm 3, \cdots$

sedemikian sehingga

jika $k = 0$ maka $x = \frac{(1+59\cdot 0)}{-7} = \frac{1}{-7}$

jika $k = -1$ maka $x = \frac{(1+59\cdot(-1)}{-7} = \frac{-58}{-7}$

jika $k = -2$ maka $x = \frac{(1+59\cdot(-2)}{-7} = \frac{-117}{-7}$

⋮

jika $k = -5$ maka $x = \frac{(1+59\cdot(-5)}{-7} = \frac{-294}{-7} = 42$

dengan mencoba beberapa macam nilai k, maka untuk $k = -5$ diperoleh solusi x bilangan bulat. Jadi, $(-7)^{-1}\ (mod\ 59) = 42$ karena $(-7) \cdot 42 \equiv 1(mod\ 59)$. Invers dari kunci enkripsi atau ${k_n}^{-1}$ ini akan ditetapkan sebagai kunci dekripsi kedua pada *Multiplicative Cipher*.

f. Lakukan operasi perkalian dari hasil dekripsi menggunakan *Linear Block Cipher* (LBC) dengan nilai ${k_m}^{-1}$ dan ${k_n}^{-1}$ kemudian kurangi dengan indeks karakter pada kata kunci *Vigenere Cipher* (k_i) yang dapat dituliskan dengan rumus berikut:

$$P_i = \left(C_i \times {k_m}^{-1} \times {k_n}^{-1}\right) - k_i\ (mod\ 59)$$

Adapun perhitungan dekripsinya yaitu sebagai berikut:

$P_1 = (54 \times 26 \times 42) - 12\ (\ mod\ 59) = 15$

$P_2 = (35 \times 26 \times 42) - 30\ (\ mod\ 59) = 17$

$P_3 = (50 \times 26 \times 42) - 11\ (\ mod\ 59) = 14$

$P_4 = (12 \times 26 \times 42) - 0\ (\ mod\ 59) = 6$

$P_5 = (1 \times 26 \times 42) - 13\ (\ mod\ 59) = 17$

$P_6 = (5 \times 26 \times 42) - 32\ (\ mod\ 59) = 0$

$P_7 = (48 \times 26 \times 42) - 12\ (mod\ 59) = 12$

$P_8 = (14 \times 26 \times 42) - 30\ (mod\ 59) = 36$

$P_9 = (58 \times 26 \times 42) - 11\ (mod\ 59) = 18$

$P_{10} = (38 \times 26 \times 42) - 0(mod\ 59) = 19$

$P_{11} = (7 \times 26 \times 42) - 13\ (mod\ 59) = 20$

$P_{12} = (11 \times 26 \times 42) - 32\ (mod\ 59) = 3$

$P_{13} = (40 \times 26 \times 42) - 12\ (mod\ 59) = 8$

$P_{14} = (14 \times 26 \times 42) - 30\ (mod\ 59) = 36$

$P_{15} = (46 \times 26 \times 42) - 11\ (mod\ 59) = 12$

$P_{16} = (0 \times 26 \times 42) - 0\ (mod\ 59) = 0$

$P_{17} = (5 \times 26 \times 42) - 13\ (mod\ 59) = 19$

$P_{18} = (13 \times 26 \times 42) - 32\ (mod\ 59) = 4$

$P_{19} = (48 \times 26 \times 42) - 12\ (mod\ 59) = 12$

$P_{20} = (1 \times 26 \times 42) - 30\ (mod\ 59) = 0$

$P_{21} = (1 \times 26 \times 42) - 11\ (mod\ 59) = 19$

$P_{22} = (16 \times 26 \times 42) - 0\ (mod\ 59) = 8$

$P_{23} = (46 \times 26 \times 42) - 13\ (mod\ 59) = 10$

$P_{24} = (5 \times 26 \times 42) - 32\ (mod\ 59) = 0$

$P_{25} = (37 \times 26 \times 42) - 12\ (mod\ 59) = 36$

$P_{26} = (57 \times 26 \times 42) - 30\ (mod\ 59) = 28$

$P_{27} = (15 \times 26 \times 42) - 11\ (mod\ 59) = 26$

$P_{28} = (54 \times 26 \times 42) - 0\ (mod\ 59) = 27$

$P_{29} = (35 \times 26 \times 42) - 13\ (mod\ 59) = 34$

$P_{30} = (24 \times 26 \times 42) - 32\ (mod\ 59) = 39$

$P_{31} = (43 \times 26 \times 42) - 12\ (mod\ 59) = 39$

$P_{32} = (20 \times 26 \times 42) - 30\ (mod\ 59) = 39$

Dengan demikian, diperoleh kembali plainteks dari kedua metode yaitu *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC) adalah PROGRAM STUDI MATEMATIKA 2018###.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pembahasan, dapat ditarik kesimpulan sebagai berikut:

1. Pada proses enkripsi pesan yang dilakukan menggunakan metode *Vigenere-Multiplicative Cipher* yang kemudian dienkripsi kembali menggunakan metode *Linear Block Cipher* (LBC). Menetapkan indeks karakter dari plainteks, mengkonversi plainteks, dan melakukan simulasi untuk proses enkripsi. Rumus perhitungan enkripsi pada *Vigenere-Multiplicative Cipher* adalah $C_i = (P_i + k_i) \times k_m \times k_n \ (mod\ 59)$, setelah itu dilanjutkan dengan melakukan proses enkripsi menggunakan *Linear Block Cipher* (LBC). Menunjukkan bahwa $\mathbb{Z}_{59}$ adalah lapangan berhingga, membangun suatu $GL_4(\mathbb{Z}_{59})$, dan melakukan simulasi untuk proses enkripsi dengan cara melakukan operasi perkalian matriks antara kunci dengan masing-masing blok.
2. Pada proses dekripsi untuk mengembalikan cipherteks ke bentuk pesan aslinya (plainteks) dengan melakukan proses dekripsi menggunakan metode *Linear Block Cipher* (LBC) yang kemudian dilanjutkan dengan metode *Vigenere-Multiplicative Cipher*. Menunjukkan bahwa $\mathbb{Z}_{59}$ adalah lapangan berhingga, membangun suatu $GL_4(\mathbb{Z}_{59})$, dan melakukan simulasi untuk proses dekripsi dengan cara melakukan operasi perkalian matriks antara kunci dengan masing-masing blok. Rumus perhitungan dekripsi pada *Vigenere-Multiplicative Cipher* $P_i = \left(C_i \times {k_m}^{-1} \times {k_n}^{-1}\right) - k_i \ (mod\ 59)$.

5.2 Saran

Dalam penelitian selanjutnya untuk metode *Vigenere-Multiplicative Cipher* disarankan untuk menggunakan kunci dan karakter yang lebih bervariasi atau dapat dikombinasikan dengan kriptografi klasik lainnya. Sedangkan untuk metode *Linear Block Cipher* (LBC) disarankan untuk membangun suatu *general linear group* dengan derajat (n) dan himpunan bilangan bulat (Z_n) yang lebih banyak agar lebih aman dan sulit dipecahkan.

DAFTAR PUSTAKA

A.Vanstone, S., & Oorschot, P. C. (1989). *An Introduction to Error Correcting Codes With Applications.* Norwell: Kluwer Academic Publishers.

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

Anton, H., & Rorres, C. (2010). *Elementary Linear Algebra Application Version.* New Jersey: John Willey & Sons, Inc.

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

Ar-Rifa'i, M. N. (2000). *Ringkasan Tafsir Ibnu Katsir, Jilid 4.* Jakarta: Gema Insani Press.

Aung, T. M., Naing, H. H., & Hla, N. N. (2019). A Complex Transformation of Monoalphabetic Cipher to Polyalphabetic Cipher. *International Journal of Machine Learning and Computing*, 296-303.

Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography. *IEEE Transactions on Inforation Theory*, 644-654.

Enterprise, J. (2019). *Python untuk Programmer Pemula.* Jakarta: PT Elex Media Komputindo.

Gilbert, L., & Gilbert, J. (2009). *Elements of Modern Algebra.* Canada: Nelson Education.

Hermawan, I., Ahmad, N., & Suhartini, A. (2020). Konsep Amanah dalam Perspektif Pendidikan Islam. *Jurnal Pendidikan, Sosial, dan Agama*, 141-152.

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

Kraft, J. S., & Washington, L. C. (2018). *An Introduction to Number Theory with Cryptography.* Washington: CRC Press.

Kuppuswamy, P., & Al-Maliki, S. Q.-K. (2021). A Novel Symmetric Hybrid Cryptography Technique Using Linear Block Cipher (LBC) and Simple Symmetric Key. *Journal of Theoretical and Applied Information Technology* , 2216-2226.

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

Ririen Kusumawati, M. (2009). *Aljabar Linear dan Matriks.* Malang: UIN Malang Press.

S.Dummit, D., & M.Foote, R. (2004). *Abstract Algebra.* New Jersey: John Wiley and Sons, Inc.

Sadikin, R. (2012). *Kriptografi Untuk Keamanan Jaringan.* Yogyakarta: CV Andi Offset.

Setyawati, N. Y., Khofid, A. N., Rundi, A. U., & Wati, V. (2021). Modifikasi Kriptografi Klasik Kombinasi Metode Vigenere Cipher dan Caesar Cipher. *Journal of Smart System*, 1-8.

Shihab, M. Q. (2002). *Tafsir Al-Misbah: Pesan, Kesan dan Keserasian Al-Qur'an.* Jakarta: Lentera Hati.

Som, S., & Ghosh, S. (2011). A Survey of Traditional or Character Oriented Symmetric Key Cryptography. *International Journal of Advanced Research in Computer Science*, 147-151.

Touil, H., Akkad, N. E., & Satori, K. (2020). Text Encryption:Hybrid Cryptographic Method Using Vigenere and Hill Ciphers. *International Conference on Intelligent Systems and Computer Vision*, 1-6.

LAMPIRAN

Lampiran 1 Enkripsi Menggunakan *Vigenere-Multiplicative Cipher*

```
#Menentukan kunci enkripsi pertama Multiplicative Cipher (km)
def modInverse(km, m):
    for x in range(1, m):
        if (((km%m) * (x%m)) % m == 1):
            return x
km = int(input("Masukkan bilangan bulat: "))
m = int(input("Modulo: "))
if(modInverse(km,m)):
    print('Invers perkalian dari', km, 'modulo', m, 'ada.', 'Anda boleh lanjut untuk
    menentukan kn.')
else:
    print('tidak ditemukan, pilih bilangan bulat lainnya')
#Menentukan kunci enkripsi kedua Multiplicative Cipher (kn)
def modInverse(kn, m):
    for x in range(1, m):
        if (((kn%m) * (x%m)) % m == 1):
            return x
kn = int(input("Masukkan bilangan bulat: "))
m = int(input("Modulo: "))
if(modInverse(kn,m)):
    print('Invers perkalian dari', kn, 'modulo', m, 'ada.', 'Anda boleh lanjut untuk
    proses enkripsi')
else:
    print('tidak ditemukan, pilih bilangan bulat lainnya')
#Enkripsi Menggunakan Vigenere-Multiplicative Cipher
import numpy as np
def K2T(n):
    A=[chr(i) for i in
list(range(65,91))+list(range(48,58))+list(range(32,48))+list(range(58,65))]
```

```
    B=list(range(59))
    return dict(zip(B,A))[n]
def T2K(t):
    t=t.upper()
    A=[chr(i) for i in
list(range(65,91))+list(range(48,58))+list(range(32,48))+list(range(58,65))]
    B=list(range(59))
    return dict(zip(A,B))[t]
plainteks = input("Masukkan Plainteks: ")
P = [T2K(i) for i in plainteks]
print("P =",P)
print("")
keyword = input("Masukkan Keyword: ")
keyword = (keyword*(len(plainteks)//len(keyword)+1))[0:len(plainteks)]
k = [T2K(i) for i in keyword]
print("k =",k)
print("")
km=int(input("km :"))
print("")
kn=int(input("kn :"))
print("")
CT = [np.mod((P[i]+K[i])*km*kn,59) for i in range(len(plainteks))]
print("CT =",CT)
CTTeks = "".join([K2T(i) for i in CT])
print("Cipherteks: ",CTTeks)
```

Lampiran 2. Dekripsi Menggunakan *Vigenere-Multiplicative Cipher*

```
# Menentukan kunci dekripsi pertama Multiplicative Cipher (km^-1)
def mod Inverse(km, m):
    for x in range(1, m):
        if (((km%m) * (x%m)) % m == 1):
            return x
km = int(input("Masukkan km: "))
m = int(input("Modulo: "))
if(modInverse(km,m)):
    print('Invers perkalian dari', km, 'modulo', m, 'adalah', modInverse(km,m), '.
    Anda boleh lanjut untuk menentukan kn.')
else:
    print('tidak ditemukan')
# Menentukan kunci dekripsi kedua Multiplicative Cipher (kn^-1)
def modInverse(kn, m):
    for x in range(1, m):
        if (((kn%m) * (x%m)) % m == 1):
            return x
kn = int(input("Masukkan kn: "))
m = int(input("Modulo: "))
if(modInverse(kn,m)):
    print('Invers perkalian dari', kn, 'modulo', m, 'adalah', modInverse(kn,m), 'Anda
    boleh lanjut untuk proses dekripsi.')
else:
    print('tidak ditemukan')
#Dekripsi Menggunakan Vigenere-Multiplicative Cipher
import numpy as np
def K2T(n):
    A=[chr(i) for i in
list(range(65,91))+list(range(48,58))+list(range(32,48))+list(range(58,65))]
```

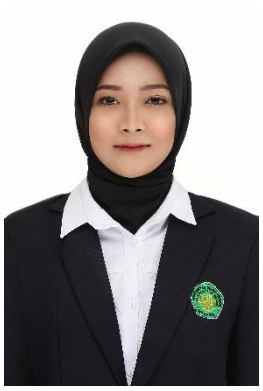
```
    B=list(range(59))
    return dict(zip(B,A))[n]
def T2K(t):
    t=t.upper()
    A=[chr(i) for i in
list(range(65,91))+list(range(48,58))+list(range(32,48))+list(range(58,65))]
    B=list(range(59))
    return dict(zip(A,B))[t]
cipherteks = input("Masukkan Ciphertеks: ")
C = [T2K(i) for i in cipherteks]
print("P =",P)
print("")
keyword = input("Masukkan Keyword: ")
keyword = (keyword*(len(cipherteks)//len(keyword)+1))[0:len(cipherteks)]
k = [T2K(i) for i in keyword]
print("k =",k)
print("")
km=int(input("km :"))
print("")
kn=int(input("kn :"))
print("")
PT = [np.mod((C[i]*km*kn)-k[i],59) for i in range(len(cipherteks))]
print("PT =",PT)
PTTeks = "".join([K2T(i) for i in PT])
print("Plainteks: ",PTTeks)
```

Lampiran 3. Enkripsi dan Dekripsi Menggunakan *Linear Block Cipher*

```
import numpy as np
def K2T(n):
    A=[chr(i) for i in
list(range(65,91))+list(range(48,58))+list(range(32,48))+list(range(58,65))]
    B=list(range(59))
    return dict(zip(B,A))[n]
def T2K(t):
   t=t.upper()
   A=[chr(i) for i in
list(range(65,91))+list(range(48,58))+list(range(32,48))+list(range(58,65))]
   B=list(range(59))
   return dict(zip(A,B))[t]
plainteks = input("Masukkan Plainteks: ")
P = [T2K(i) for i in plainteks]
print("P =",P)
print("")
n = 4
x = [P[i:i+n] for i in range(0, len(P), n)]
my_matrix = np.array(x).reshape(8, 4).T
print(my_matrix)
my_matrix[0:4,0:1]
K = np.array([[4,2,2,3],[2,5,1,2],[3,2,4,3],[7,4,3,2]], dtype=int)
print(K)
e=np.matmul(K,my_matrix)
e
h=np.matmul(K,my_matrix) % 59
h
m=59
def Adjoint_Mat(K,K_det,m):
      K1 = np.linalg.inv(K)
```

```
    K2 = K1 * K_det % m
    K2 = np.around(K2)
    K2 = K2.astype(np.int)
    return K2
def Multi_Inverse(x,m):
    y = 0
    while(y < m):
        res = (x * y) % m
        if res == 1:
        print("Di mod%d,Nilai determinan dari kunci enkripsi adalah%d, Invers perkaliannya adalah%d" % (m,x,y))
        break
        else:
            y = y + 1
            if y == m:
                print(x,"Di mod",m,"Tidak memiliki invers perkalian modulo")
                return 0
    return y
def Decrypt_Key(K,m):
    K_det = np.linalg.det(K).round()
    K2 = Adjoint_Mat(K, K_det, m)
    y = Multi_Inverse(K_det, m)
    K3 = y * K2 % m
    return K3
k = Decrypt_Key(K,m)
print("Kunci dekripsinya adalah\n",k)
d = np.matmul(k,h)
d
d1 = np.matmul(k,h) % 59
d1
```

RIWAYAT HIDUP



Aulia Nanda Herawati, biasa disapa Aulia, merupakan putri semata wayang dari Bapak Bugy Hernoko Wisnu Husodo dan Ibu Sulistiyowati. Ia dilahirkan di Kota Sidoarjo pada tanggal 25 Juli 2000. Ia tinggal di Dusun Pager RT 03 RW 12, Desa Sawotratap, Kecamatan Gedangan, Kabupaten Sidoarjo.

Penulis menempuh pendidikan mulai dari RA Al-Hidayah dan lulus tahun 2006, setelah itu menempuh pendidikan dasar di SD Negeri Sawotratap IV dan lulus pada tahun 2012, selanjutnya menempuh pendidikan menengah pertama di SMP Negeri 4 Waru dan lulus pada tahun 2015, kemudian menempuh pendidikan menegah atas di SMK Sepuluh Nopember Sidoarjo dan lulus pada tahun 2018. Pada tahun yang sama, ia menempuh pendidikan perguruan tinggi di Universitas Islam Negeri Maulana Malik Ibrahim Malang pada Program Studi Matematika, Fakultas Sains dan Teknologi.

KEMENTERIAN AGAMA 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 : Aulia Nanda Herawati
NIM : 18610056
Fakultas / Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Enkripsi dan Dekripsi Pesan Menggunakan *Vigenere-Multiplicative Cipher* dan *Linear Block Cipher* (LBC)
Pembimbing I : Evawati Alisah, M.Pd
Pembimbing II : Erna Herawati, M.Pd

No	Tanggal	Hal	Tanda Tangan
1.	2 Februari 2022	Konsultasi Bab 1	1.
2.	14 Februari 2022	Revisi Bab 1	2.
3.	18 Februari 2022	Konsultasi Bab 2	3.
4.	21 Februari 2022	Konsultasi kajian agama	4.
5.	4 Maret 2022	Revisi Bab 2	5.
6.	11 Maret 2022	Konsultasi Bab 3	6.
7.	18 Maret 2022	Revisi Bab 3	7.
8.	21 Maret 2022	ACC Bab 1-3 oleh Dosen Pembimbing I	8.
9.	22 Maret 2022	ACC Bab 1-3 oleh Dosen Pembimbing II	9.
10.	15 April 2022	Konsultasi Revisi Seminar Proposal dengan Dosen Pembimbing I	10.
11.	28 April 2022	Konsultasi Bab 4	11.
12.	17 Mei 2022	Konsultasi Bab 5	12.
13.	24 Mei 2022	ACC Bab 4 dan Bab 5 oleh Dosen Pembimbing I	13.
14.	27 Mei 2022	ACC Bab 4 dan Bab 5 oleh Dosen Pembimbing II	14.
15.	10 Juni 2022	Konsultasi Revisi Seminar Hasil	15.
16.	15 Juni 2022	Konsultasi kajian agama Bab 2	16.
17.	22 Juni 2022	ACC Keseluruhan	17.

Malang, 22 Juni 2022
Mengetahui,
Ketua Program Studi Matematika

Dr.Elly Susanti, M.Sc
NIP.197411292000122005