PROSES PERTUKARAN KUNCI KRIPTOGRAFI *DIFFIE-HELLMAN* DENGAN MENGGUNAKAN ALGORITMA *HILL CIPHER*

SKRIPSI

OLEH
SRI WIDATI EKA KAPTI
NIM. 18610010

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

PROSES PERTUKARAN KUNCI KRIPTOGRAFI *DIFFIE-HELLMAN* DENGAN MENGGUNAKAN ALGORITMA *HILL CIPHER*

SKRIPSI

OLEH
SRI WIDATI EKA KAPTI
NIM. 18610010

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

PROSES PERTUKARAN KUNCI KRIPTOGRAFI *DIFFIE-HELLMAN* DENGAN MENGGUNAKAN ALGORITMA *HILL CIPHER*

SKRIPSI

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

Oleh
SRI WIDATI EKA KAPTI
NIM. 18610010

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

PROSES PERTUKARAN KUNCI KRIPTOGRAFI *DIFFIE-HELLMAN* DENGAN MENGGUNAKAN ALGORITMA *HILL CIPHER*

SKRIPSI

Oleh
Sri Widati Eka Kapti
NIM. 18610010

Telah Diperiksa dan Disetujui Untuk Diuji
Malang, 05 Desember 2022

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah, M.Si	Erna Herawati, M.Pd
NIDT. 19900511201608011 057	NIDT. 19760723 20180201 2 222

Mengetahui,
Ketua Program Studi Matematika

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

PROSES PERTUKARAN KUNCI KRIPTOGRAFI *DIFFIE-HELLMAN* DENGAN MENGGUNAKAN ALGORITMA *HILL CIPHER*

SKRIPSI

Oleh
Sri Widati Eka Kapti
NIM. 18610010

Telah Dipertahankan di Depan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk *Memperoleh Gelar Sarjana Matematika (S.Mat)*
Tanggal 14 Desember 2022

Ketua Penguji	: Juhari, M.Si	.....
Anggota Penguji *I*	: *Dr. H. Imam Sujarwo, M.Pd*	.....
Anggota Penguji II	: Muhammad Khudzaifah, M.Si	.....
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 bertanda tangan di bawah ini :

Nama : Sri Widati Eka Kapti

NIM : 18610010

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Proses Pertukaran Kunci Kriptografi *Diffie-Hellman* dengan Menggunakan Algoritma *Hill Cipher*

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

Malang, 14 Desember 2022

Yang membuat pernyataan

Sri Widati Eka Kapti

NIM. 18610010

MOTO

“Tidak ada masalah yang tidak terselesaikan ketika kita bersabar, berusaha, dan yakin akan pertolongan Allah”

حَسْبُنَا اللهُ وَنِعْمَ الْوَكِيْلُ نِعْمَ الْمَوْلَى وَنِعْمَ النَّصِيْرُ

"Cukuplah bagi kami Allah, sebaik-baiknya pelindung dan sebaik-baiknya penolong kami.”

PERSEMBAHAN

Skripsi ini penulis bersembahkan untuk :

Kedua orang tua penulis ayah Santoso dan ibu Jumaroh, serta keluarga yang selalu memberikan dukungan secara materil maupun non materil, semangat, dan do’a disetiap proses yang dilalui penulis.

Teman-teman yang juga memberikan motivasi dan semangat kepada penulis.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur dipanjatkan kepada Allah SWT atas rahmat, taufik, serta hidayah-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul "Proses Pertukaran Kunci Kriptografi *Diffie-Hellman* dengan Menggunakan Algoritma *Hill Cipher*" sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang matematika di Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Shalawat serta salam senantiasa tercurahkan kepada Rasulullah SAW yang telah membimbing dan menjadi suri tauladan terbaik bagi umat Islam.

Dalam proses penyusunan skripsi ini, penulis mendapatkan banyak bimbingan juga saran dari berbagai pihak. Oleh karena itulah ucapan terima kasih sebesar-besarnya penulis tujukan kepada :

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, S.Pd., M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Muhammad Khudzaifah, M.Si, selaku dosen pembimbing I yang telah memberikan banyak memberikan bimbingan, arahan, serta saran dan berbagai pengalaman yang berharga kepada penulis.
5. Erna Herawati, M.Pd selaku dosen pembimbing II yang telah banyak memberikan arahan dan nasihat kepada penulis.

6. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim
7. Orang tua dan seluruh keluarga yang telah memberikan do'a, semangat, dan nasihat kepada penulis.
8. Seluruh mahasiswa angkatan 2018.

Penulis menyadari penyusunan skripsi ini masih banyak kekurangan dan jauh dari kata sempurna, oleh karena itulah kritik dan saran yang membangun dari segenap pembaca sangat diharapkan. Besar harapan bagi penulis agar skripsi ini dapat bermanfaat bagi yang membutuhkannya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, 14 Desember 2022

Penulis

DAFTAR ISI

DAFTAR TABEL

ABSTRAK

Kapti, Sri Widati Eka. 2022. **Proses Pertukaran Kunci Kriptografi *Diffie-Hellman* Dengan Menggunakan Algoritma *Hill Cipher*.** Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing (I): M. Khudzaifah, M. Si, Pembimbing (II): Erna Herawati, M. Pd.

Kata Kunci : Proses Pertukaran Kunci, *Diffie-Hellman, Hill Cipher*.

Kriptografi dilakukan untuk mengamankan pesan dari orang-orang yang tidak berhak mengetahuinya. *Hill Cipher* menggunakan matriks sebagai kunci dalam proses melakukan enkripsi dan dekripsi. Sedangkan *Diffie-Hellman* lebih berfokus pada proses pertukaran kunci antara pengirim dengan penerima. Penggunaan algoritma *Hill Cipher* akan membuat keamanan kriptografi *Diffie-Hellman* semakin kuat. Dikarenakan nilai bilangan prima g pada *Diffie-Hellman* diganti dengan matriks yang berperan sebagai kunci pada proses enkripsi dan dekripsi. Tujuan dari penelitian ini adalah untuk mengetahui karakteristik dari matriks yang bisa digunakan sebagai kunci algoritma *Hill Cipher* dan untuk mengetahui bagaimana proses pertukaran kunci kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher*. Langkah-langkah yang dilakukan yaitu, pertama menentukan karakteristik matriks yang lebih efektif digunakan dalam kriptografi *Diffie-Hellman*. Langkah kedua yaitu melakukan proses enkripsi kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher*. Langkah terakhir yaitu melakukan proses dekripsi kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher*. Hasil dari penelitian ini didapatkan bahwa Karakteristik matriks K yang digunakan adalah matriks non singular yang relatif prima dengan modulo 53. Proses pertukaran kunci kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher* dilakukan dengan membangkitkan bilangan prima n dan matriks g yang entri-entrinya berupa bilangan prima. Matriks tersebut kemudian akan ditukarkan sesuai dengan algoritma *Diffie-Hellman* dan didapatkan matriks kunci K. Matriks K inilah yang selanjutnya akan digunakan dalam proses enkripsi dan dekripsi dengan menggunakan algoritma *Hill Cipher*. Adapun untuk kedepannya, penelitian ini bisa digunakan untuk memperkuat algoritma *Hill Cipher* agar bisa lebih mengamankan pesan yang dikirimkan karena menggunakan pertukaran kunci kriptografi *Diffie-Hellman* yang memiliki kunci publik dan kunci privat dalam proses enkripsi dan dekripsinya.

ABSTRACT

Kapti, Sri Widati Eka. 2022. **Diffie-Hellman Cryptographic Key Exchange Process Using The Hill Cipher Algorithm.** Thesis. Mathematics Study Program, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Supervisor (I): M. Khudzaifah, M. Si, Supervisor (II): Erna Herawati, M. Pd.

Keywords : Key Exchange Process, Diffie-Hellman, Hill Cipher.

Cryptography is used to secure messages from people who do not have the right to know about them. Hill Cipher uses the matrix as a key in the process of performing encryption and decryption. Whereas the Diffie-Hellman algorithm focuses more on the process of exchanging keys between the sender and the receiver. The use of the Hill Cipher algorithm will make Diffie-Hellman's cryptographic security even stronger. Because the prime number value g in Diffie-Hellman is replaced with a matrix that acts as a key in the encryption and decryption process. This research was conducted using a qualitative method where the purpose of this study was to find out the characteristics of the matrix that can be used as a Hill Cipher algorithm key key and to find out how the Diffie-Hellman cryptography key exchange process using the Hill Cipher algorithm. The results of this study found that the characteristics of the K matrix used are relatively prime non-singular matrices with modulo 53. The process of exchanging Diffie-Hellman cryptographic keys using the Hill Cipher algorithm is carried out by generating prime numbers n and matrices g whose entries are primes. The matrix will then be exchanged according to the Diffie-Hellman algorithm and obtained the key matrix K. Matrix K will then be used in the encryption and decryption process using the Hill Cipher algorithm. As for the future, this research can be used to strengthen the Hill Cipher algorithm so that it can better secure the messages sent because it uses the Diffie-Hellman cryptographic key exchange which has a public key and a private key in the encryption and decryption process.

مستخلص البحث

كبتي، سري ويداتي إيكا. ٢٠٢٢. **عملية تبادل مفاتيح تشفير *Hill Cipher* باستخدام خوارزم *Diffie-Hellman***. البحث العلمي. قسم الرياضيات، كلية العلوم والتكنولوجيا ،جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج .المشرف الأول: محمد خديفة، الماجستير، المشرفة الثانية: إيرنا هراواتي، الماجستير.

الكلمات الرئيسية: عملية التبادل الرئيسية ، *Hill Cipher*، *Diffie-Hellman*

يتم التشفير لتأمين الرسائل من الأشخاص الذين ليس لديهم الحق في معرفتها. يستخدم *Hill Cipher* المصفوفة كمفتاح في عملية إجراء التشفير وفك التشفير. بينما يركز *Diffie-Hellman* أكثر على عملية تبادل المفاتيح بين المرسل والمتلقي. سيؤدي استخدام خوارزمية *Hill Cipher* إلى جعل أمان تشفير *Diffie-Hellman* أقوى. لأنه يتم استبدال قيمة العدد الأولي في *Diffie-Hellman* g بمصفوفة تعمل كمفتاح في عملية التشفير وفك التشفير. الغرض من هذه الدراسة هو معرفة خصائص المصفوفة التي يمكن استخدامها كمفتاح لخوارزمية Hill Cipher ومعرفة كيفية عملية تبادل مفتاح تشفير *Diffie-Hellman* باستخدام خوارزمية *Hill Cipher*. الخطوات المتخذة هي ، أولا ، تحديد خصائص المصفوفة التي يتم استخدامها بشكل أكثر فعالية في تشفير *Diffie-Hellman*. الخطوة الثانية هي إجراء عملية تشفير *Diffie-Hellman* باستخدام خوارزمية *Hill Cipher*. الخطوة الأخيرة هي تنفيذ عملية فك تشفير *تشفير Diffie-Hellman* باستخدام خوارزمية *Hill Cipher*. وجدت نتائج هذه الدراسة أن خصائص مصفوفة K المستخدمة هي مصفوفات أولية غير مفردة نسبيا مع 53 modulo. يتم تنفيذ عملية تبادل مفاتيح تشفير *Diffie-Hellman* باستخدام خوارزمية *Hill Cipher* عن طريق إنشاء أعداد أولية ومصفوفات تكون إدخالاتها أعدادا أولية. سيتم بعد ذلك تبادل المصفوفة وفقا لخوارزمية *Diffie-Hellman*mg والحصول على المصفوفة الرئيسية K. سيتم بعد ذلك استخدام Matrix K في عملية التشفير وفك التشفير باستخدام *خوارزمية Hill Cipher*. بالنسبة للمستقبل ، يمكن استخدام هذا البحث لتقوية خوارزمية *Hill Cipher* بحيث يمكنها تأمين الرسائل المرسلة بشكل أفضل لأنها تستخدم تبادل مفاتيح التشفير *Diffie-Hellman* الذي يحتوي على مفتاح عام ومفتاح خاص في عملية التشفير وفك التشفير.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Berkomunikasi antara satu manusia dengan manusia yang lain adalah hal yang wajar, bahkan merupakan hal penting sebagai sarana untuk saling memahami. Ada banyak cara untuk berkomunikasi, salah satunya adalah melalui tulisan. Sebelum adanya perkembangan media untuk mendokumentasikan dan menyimpan tulisan, pengiriman informasi dari satu tempat ke tempat lainnya sudah terjadi. Dengan berkembangnya cara pengiriman pesan, berkembang pula cara menyembunyikan pesan dari orang-orang yang tidak berhak mengetahuinya walaupun mereka berhasil menemukan pesan tersebut. Dari sinilah, lahir suatu ilmu baru yang disebut dengan kriptografi. (Ariyus, 2008).

Kriptografi adalah salah satu cara untuk mengamankan pesan agar dapat diterima oleh orang yang dituju tanpa adanya kebocoran data. Oleh karena itu, terus dilakukan pengembangan untuk menghalangi dan menyulitkan pihak ketiga untuk menemukan makna sebenarnya dalam pesan yang dikirimkan. Adanya pihak yang tidak bertanggung jawab inilah yang membuat pengirim pesan harus memastikan keamanan dari pesan yang dikirim agar sampai dengan aman kepada penerima. Dengan kata lain, terdapat amanah yang harus dijaga supaya tidak jatuh ke tangan orang yang salah. Karena menyampaikan amanah kepada yang berhak menerimanya adalah perintah Allah SWT sebagaimana disebutkan dalam ayat berikut :

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

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

Dalam QS. An-Nisa':58, perintah Allah untuk menyampaikan amanah kepada yang berhak menerimanya adalah sejalan dengan konsep digunakannya kriptografi untuk mengamankan pesan. Selain itu, pesan juga merupakan amanah yang harus dijaga kerahasiaannya dan disampaikan kepada orang yang berhak.

Seiring dengan berkembangnya jaman, kriptografi banyak mengalami perkembangan baik dalam proses enkripsi maupun dekripsi yang melibatkan lebih dari satu algoritma maupun modifikasi dari salah satu algoritma kriptografi itu sendiri. Dalam penelitian yang dilakukan oleh Fatimatuzzahro' (2021) yang berjudul "Penerapan Kriptografi Hibrida Menggunakan Algoritma *Hill Cipher* dan Rivest Shamir Adleman (RSA) pada Pengamanan Pesan Teks" didapatkan bahwa pada proses enkripsi keamanan pesan terletak pada kerahasiaan kunci pesan. Karena kunci dari algoritma *Hill Cipher* menggunakan matriks, maka semakin besar ukuran matriks kunci yang digunakan maka waktu yang diperlukan untuk proses enkripsi akan semakin banyak. Berdasarkan hasil dari proses dekripsi untuk mengubah cipherteks menjadi plainteks, keamanan enkripsi kunci pesan terletak pada pengambilan sebarang nilai p dan q yang diperlukan pada proses pembuatan kunci publik dan kunci privat. Semakin besar nilai p dan q, maka waktu yang diperlukan untuk melakukan proses enkripsi akan semakin lama.

Selanjutnya, pada penelitian yang dilakukan oleh Tika Khairani, Kiswara Agung Santoso, dan Ahmad Kamsyakawuni (2021) dengan judul "Pengkodean Monoalphabetic Menggunakan *Affine Cipher* dengan Kunci *Diffie-Hellman*"

disimpulkan bahwa pengkodean dengan menggunakan *Affine Cipher* dengan kunci *Diffie-Hellman* lebih aman daripada dengan kunci biasa. Kekuatan dari dua kriptografi tersebut terletak pada kunci privat. Selama kerahasiaan dari kunci privat dapat terjaga, maka pesan tidak dapat dipecahkan. Berdasarkan pada penelitian-penelitian yang telah dilakukan sebelumnya terutama pada *Hill Cipher* dan *Diffie-Hellman,* peneliti tertarik untuk mengetahui karakteristik matriks yang lebih efektif digunakan dalam kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher* serta proses enkripsi dan dekripsi pada protocol pertukaran kunci kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher*. Sebab tidak sebarang matriks bisa digunakan sebagai matriks kunci pada algoritma *Hill Cipher*. Terdapat ciri tertentu dari suatu matriks kunci agar bisa digunakan dalam proses enkripsi dan dekripsi. Selain itu, proses enkripsi dan dekripsi yang dilakukan dengan melibatkan dua algoritma dapat meningkatkan keamanan pada pesan yang dikirimkan.

1.2 Rumusan Masalah

Berdasarkan latar belakang diperoleh rumusan masalah sebagai berikut :

1. Bagaimana karakteristik matriks yang lebih efektif digunakan dalam pertukaran kunci kriptografi *Diffie-Hellman*?
2. Bagaimana proses enkripsi pada protokol pertukaran kunci kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher*?
3. Bagaimana proses dekripsi pada protokol pertukaran kunci kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher?*

1.3 Tujuan Penelitian

Tujuan dilakukannya penelitian ini adalah sebagai berikut :

1. Untuk mengetahui karakteristik matriks yang lebih efektif digunakan dalam pertukaran kunci kriptografi *Diffie-Hellman*.
2. Untuk mengetahui proses enkripsi pada protokol pertukaran kunci kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher*.
3. Untuk mengetahui proses dekripsi pada protokol pertukaran kunci kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher*.

1.4 Manfaat Penelitian

Adapun manfaat dari penelitian ini secara ilmiah adalah untuk memperkuat keamanan pesan yang dikirim. Pada Badan Siber dan Sandi Negara penelitian ini bermanfaat untuk menjaga informasi negara agar tidak digunakan oleh pihak yang tidak bertanggung jawab.

1.5 Batasan Masalah

Supaya peneliti bisa fokus terhadap masalah yang dirumuskan dan bisa mencapai tujuan yang telah ditentukan, maka diberikan beberapa batasan masalah sebagai berikut :

1. Matriks kunci yang digunakan adalah matriks persegi 3×3 yang memiliki invers.
2. Jika banyak kolom plainteks yang digunakan tidak sesuai dengan ukuran kunci matriks, kekurangan karakter akan diisi dengan spasi.
3. Pada kriptografi *Diffie-Hellman* ditentukan nilai $x = 1$ atau $y = 1$.

4. Entri-entri dari matriks yang digunakan harus bilangan prima.

1.6 Definisi Istilah

Definisi atau arti dari istilah-istilah yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Kriptografi : ilmu dan seni untuk menjaga keamanan pesan ketika dikirim dari suatu tempat ke tempat lain.
2. Algoritma : urutan langkah-langkah logis untuk menyelesaikan masalah yang disusun secara sistematis.
3. *Diffie-Hellman:* sebuah algoritma yang memungkinkan kedua pihak saling bertukar kunci melalui jaringan publik.
4. *Hill Cipher* : salah satu algoritma kriptografi simetri yang kuncinya berupa matriks untuk melakukan proses enkripsi dan dekripsi dengan aritmatika modulo.
5. Enkripsi : proses mengubah plainteks (teks asli) menjadi cipherteks.
6. Dekripsi : proses mengubah cipherteks menjadi plainteks (teks asli).
7. Kunci privat : kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang).
8. Kunci publik : kunci yang boleh diketahui oleh semua orang.

BAB II
KAJIAN TEORI

2.1 Teori Pendukung

2.1.1 Matriks

Definisi 2.1 :

Matriks adalah sekumpulan bilangan yang disusun secara baris dan kolom dan ditempatkan pada kurung biasa atau kurung siku. (Pratama, dkk, 2021)

Bilangan atau fungsi yang dimaksud disebut *entri* atau elemen matriks. Matriks mempunyai baris dan kolom. Banyaknya baris dan banyaknya kolom pada matriks disebut dengan ordo. Secara umum sebuah matriks ditulis seperti :

$$\begin{bmatrix} a_{11} & a_{21} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

Dua matriks disebut sama jika ordonya sama dan entri yang seletak bernilai sama. Dilihat dari ordonya, matriks mempunyai banyak jenis. Berikut adalah beberapa jenis matriks :

1. Matriks bujur sangkar yaitu matriks yang banyak barisnya sama dengan banyak kolom.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{23} & a_{33} \end{bmatrix}$$

2. Matriks satuan

   Matriks satuan disebut juga matriks identitas. Yaitu matriks yang entri-entri pada diagonal utamanya adalah 1 dan entri-entri lainnya adalah 0. Matriks identitas dilambangkan dengan I_n, dengan n adalah ordo dari matriks tersebut.

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

3. Matriks invers

   Suatu matriks B dikatakan sebagai matriks *invers* dari A jika memenuhi $BA = AB = I$. Secara umum invers matriks B dinyatakan dengan A^{-1}.

   Untuk matriks dengan ordo 2×2, rumus inversnya adalah sebagai berikut:

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

   Untuk matriks dengan ordo 3×3, rumus inversnya adalah :

   Misalkan $A = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix}$, maka $A^{-1} = \frac{1}{\det(A)}\, adj\,(A)$,

   dengan $\det(A) \neq 0$

Pada matriks berlaku lima operasi matriks, yaitu:

1. Penjumlahan matriks
2. Perkalian matriks dengan skalar
3. Perkalian dua matriks
4. *Transpose* matriks
5. *Trace* matriks

Adapun sifat-sifat operasi aritmetika pada matriks adalah :

1. Misalkan $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dan $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, maka penjumlahan matriks A dan B serta perkalian matriks A dan B dengan skalar memenuhi sifat-sifat berikut :

   a. $A + B = B + A$ (sifat komutatif)

   b. $(A + B) + C = A + (B + C)$ (sifat asosiatif)

c. $A + O = O + A$ (sifat matriks nol, identitas penjumlahan)

d. $A + (-A) = -A + A = O$ (sifat negatif matriks)

e. $k(A + B) = kA + kB$ (sifat distributif terhadap skalar k)

f. $(k + I)A = kA + IA$ (sifat distributif terhadap skalar k dan l)

g. $(kl)A = k(lA)$ (sifat asosiatif terhadap perkalian skalar)

h. $1A = A$ (sifat perkalian dengan skalar 1)

('Imrona, 2009)

2. Perkalian matriks

Jika $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dan $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, pada perkalian matriks berlaku 11 sifat sebagai berikut :

a. Pada umumnya berlaku sifat $AB \neq BA$

b. $(AB)C = A(BC)$ (sifat asosiatif)

c. $AI = IA = A$ (sifat matriks satuan, identitas perkalian)

d. $AO = OA = O$ (sifat matriks nol)

e. $A^n = \begin{cases} \underbrace{AAA \dots A}_{n\ kali} & , \text{jika } n = 1,2, \dots \\ I & , \text{jika } n = 0 \end{cases}$

f. $A^r A^s = A^{r+s}$, jika r dan s bilangan asli.

g. Matriks diagonal $D = \begin{bmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & d_n \end{bmatrix}$,

berlaku $D^k = \begin{bmatrix} {d_1}^k & 0 & \dots & 0 \\ 0 & {d_2}^k & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & {d_n}^k \end{bmatrix}$

h. Jika $AB = 0$, tidak dijamin berlaku $A = 0$ atau $B = 0$ atau $BA = 0$.

i. $(kA)B = k(AB) = A(kB)$

j. $(A + B)C = AC + BC$

k. $C(A + B) = CA + CB$

('Imrona, 2009)

3. *Transpose* dan *trace* matriks

Misalkan $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dan $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, maka berlaku sifat :

a. $(AB)^T = B^T A^T$ (urutan operasi dibalik)

b. $(kA)^T = kA^T$

c. $(A + B)^T = A^T + B^T$ (sifat *transpose* matriks terhadap penjumlahan)

d. $Trace\ (A + B) = trace\ (A) + trace\ (B)$

e. $Trace\ (A^T) = trace\ (A)$ (tidak ada perubahan *trace* pada operasi *transpose*)

f. $Trase\ (kA) = k\ trace\ (A)$

g. $Trace\ (I_{n \times n}) = n$

('Imrona, 2009)

2.1.2 Keterbagian

Definisi 2.2 :

Misalkan $a, b \in Z$, dengan $a \neq 0$, maka a disebut membagi b ditulis sebagai $a|b$ apabila $b = ak$, untuk suatu $k \in Z$. (Irawan, dkk, 2014)

Dari definisi 2.2, notasi $a|b$ dibaca dengan :

1. "a membagi b" atau
2. "b habis dibagi a" atau
3. "a pembagi b" atau
4. "a faktor dari b" atau
5. "b kelipatan dari a"

Jika a tidak membagi b, maka ditulis sebagai $a \nmid b$. (Irawan, dkk, 2014)

Contoh :

$4|20$, karena terdapat $5 \in Z$ sehingga $20 = 4.5$

$3 \nmid 53$, karena tidak terdapat $k \in Z$ sedemikian hingga $53 = 3k$

Definisi 2.3 :

Bilangan bulat positif a adalah pembagi persekutuan dari b dan c yang tidak nol jika $a|b$ dan $a|c$. Selanjutnya bilangan bulat a adalah pembagi persekutuan terbesar atau $Greatest\ Common\ Divisor$ atau GCD dari bilangan bulat tidak nol b dan c jika a adalah bilangan bulat positif terbesar sehingga jika $a|b$ dan $a|c$. (Irawan, dkk, 2014)

Atau ditentukan bilangan bulat b dan c (keduanya tidak nol) maka bilangan bulat a disebut pembagi persekutuan terbesar dari b dan c, jika dipenuhi :

a. $a > 0$
b. $a|b$ dan $a|c$

c. Jika $d|b$ dan $d|c$, maka $d|a$

Notasi : Pembagi persekutuan terbesar dari b dan c dituliskan $a = (b, c)$ dan karena $a > 0$ maka $a = (b, c) \geq 1$. Sehingga $(b, c) = (b, -c) = (-b, -c)$.

(Irawan, dkk, 2014)

Contoh :

Pembagi persekutuan terbesar dari 18 dan 24 adalah 6 ditulis $(18,24) = 6$

Begitu pula= $(18, -24) = (-18, 24) = (-18, -24) = 6$

2.1.3 Aritmatika Modular

Aritmatika modular termasuk salah satu konsep matematika yang digunakan untuk membuat sistem kriptografi dan analisis sistem kriptografi, terutama sistem kriptografi klasik. (Sadikin, 2012). Kriptografi klasik adalah kriptografi yang algoritmanya menggunakan satu kunci untuk mengamankan data. Algoritma klasik biasanya menggunakan dua teknik dasar yaitu :

1. Teknik substitusi, yaitu teknik yang dilakukan dengan mengganti setiap karakter teks asli dengan karakter lain.
2. Teknik transposisi (permutasi), yaitu teknik yang dilakukan dengan menggunakan permutasi karakter (Ariyus, 2008).

Pada kriptografi klasik yang menggunakan alfabet latin “A” sampai “Z”, alfabet yang digunakan $\{A, \dots, Z\}$ akan dipetakan menjadi $\{0, \dots, 25\}$. Aritmatika modular digunakan agar transformasi penyandian selalu bernilai $\{0, \dots, 25\}$ sehingga memiliki pasangan simbol yang digunakan.

Aritmatika modular menggunakan operator modular, yaitu sebuah bilangan bulat a dan sebuah bilangan bulat n yang disebut modulus. Operasi modular disimbolkan dengan :

$$a \, mod \, n = r$$

Contoh : Hasil dari $58 \, mod \, 7$ adalah 2. Karena $58 = (7 \times 8) + 2$

Karena tujuan dari operasi modular adalah mengembalikan nilai r yang merupakan sisa bagi atas operasi a dibagi n, maka hasil dari $58 \, mod \, 7 = 2$

Definisi 2.4 :

Jika sebuah bilangan bulat M yang tidak nol, membagi selisih $a - b$, maka kita katakan a kongruen dengan b modulo M, dan ditulis :

$$a \equiv b \text{ (mod } M)$$

Jika $a - b$ tidak habis dibagi M, maka dikatakan a tidak kongruen dengan b mod M, dan ditulis :

$$a \not\equiv \text{b (mod } M)$$

Jika $M > 0$ dan $M|(a - b)$ maka ada suatu bilangan bulat t sehingga $a - b = Mt$. Sehingga $a \equiv b \ (mod \, M)$ dapat juga dinyatakan sebagai $a - b = Mt$. Ini sama artinya dengan $a \equiv b \ (mod \, M)$ atau beda antara a dan b merupakan kelipatan M. Jadi, $a \equiv b \ (mod \, M)$ dapat juga dinyatakan $a = Mt + b$, yaitu $a = b$ ditambah kelipatan M. (Irawan, dkk, 2014)

Contoh :

$8 \equiv 2$ (mod 3) karena $8 - 2 = 2.3$

Teorema 2.1 :

Misalkan a, b dan c adalah bilangan bulat dan m adalah bilangan asli, maka berlaku:

1. Sifat refleksi, yaitu $a \equiv a \pmod{m}$
2. Sifat simetris, jika $a \equiv b \pmod{m}$, maka :

   $b \equiv a \pmod{m}$ dan $a - b = 0 \pmod{m}$ adalah pernyataan yang ekuivalen.
3. Transitif, jika $a \equiv b \pmod{m}$ dan $b \equiv c \pmod{m}$, maka $a \equiv c \pmod{m}$

Bukti :

1. Jika $m \neq 0$ maka $m|0$ yang dapat dituliskan sebagai $m|a - a$. Menurut definisi berlaku $a \equiv a \pmod{m}$ untuk semua bilangan bulat a dan $m \neq 0$.
2. Karena $a \equiv b \pmod{m}$ berarti $m|a - b$. Menurut definisi ada keterbagian bilangan bulat t sehingga :

   $m|a - b$ dapat dinyatakan $a - b = tm$

   $\Leftrightarrow -(a - b) = -tm$

   $\Leftrightarrow b - a = (-t)m$

   Menurut definisi, ini berarti $b \equiv a \pmod{m}$

   $a \equiv b \pmod{m}$ berarti $m|a - b$. Menurut definisi 2.4 ada bilangan bulat t sehingga $m|a - b$ dapat dinyatakan $a - b = tm$.

   Untuk setiap $(a - b) - 0 = tm$ maka $(a - b) \equiv 0 \pmod{m}$
3. Karena $a \equiv b \pmod{m}$ berarti $m|a - b$ (menurut Definisi 2.4)

   Karena $b \equiv c \pmod{m}$ berarti $m|b - c$ (menurut Definisi 2.4)

   Menurut definisi kongruensi modulo pada keterbagian terdapat bilangan bulat t_1 dan t_2 sehingga :

   $m|a - b$ dapat dinyatakan sebagai $a - b = t_1 m$,

   $m|b - c$ dapat dinyatakan sebagai $b - c = t_2 m$,

   kedua persamaan tersebut dijumlahkan sehingga diperoleh :

$$a - c = (t_1 + t_2)m$$

Menurut definisi kongruensi modulo dapat disimpulkan $a - c \equiv (\text{mod } m)$.

(Irawan, dkk, 2014)

Definisi 2.5 :

Misalkan A dan B adalah matriks $n \times k$ dengan entri-entrinya bilangan bulat, dengan unsur ke (i, j) berturut-turut adalah a_{ij} dan b_{ij}. Matriks A dikatakan kongruen dengan B modulo m jika $a_{ij} \equiv b_{ij}$ (mod m) untuk setiap pasang (i, j) dengan $1 \leq i \leq n$ dan $i \leq j \leq k$ dan dinotasikan dengan

$$A \equiv B \text{ (mod } m)$$

(Irawan, dkk, 2014)

Contoh :

$\begin{bmatrix} 529 & 460 \\ 483 & 437 \end{bmatrix} \equiv \begin{bmatrix} 9 & 18 \\ 15 & 21 \end{bmatrix}$ mod 26

karena 26 habis membagi $\begin{bmatrix} 529 & 460 \\ 483 & 437 \end{bmatrix} - \begin{bmatrix} 9 & 18 \\ 15 & 21 \end{bmatrix}$

Definisi 2.6 :

Jika A' dan A adalah matriks $n \times n$ dari bilangan-bilangan bulat, dan $A'A \equiv AA \equiv I$ (mod m) dimana :

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

adalah matriks identitas berorder n, maka A' dikatakan invers dari A modulo m. Jika A' invers dari A dan $B \equiv A'$ (mod m), maka B juga invers dari dari A karena $BA \equiv A'A \equiv I$ (mod m). Sebaliknya jika B_1 dan B_2 keduanya invers dari A maka $B_1 \equiv B_2$ (mod m). Dengan demikian $B_1A \equiv B_2A \equiv I$ (mod m), dan diperoleh

$B_1AB_1 \equiv B_2AB_2 \equiv I \pmod{m}$. Sehingga dapat disimpulkan bahwa $B_1 \equiv B_2 \pmod{m}$. (Irawan, dkk, 2014)

Contoh :

Misalkan $A = \begin{bmatrix} 19 & 6 \\ 5 & 23 \end{bmatrix}$ terdapat matriks $A' = \begin{bmatrix} 9 & 18 \\ 15 & 21 \end{bmatrix}$

Sehingga $AA' = \begin{bmatrix} 19 & 6 \\ 5 & 23 \end{bmatrix}\begin{bmatrix} 9 & 18 \\ 15 & 21 \end{bmatrix} = \begin{bmatrix} 261 & 468 \\ 390 & 573 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 26$

dan $\begin{bmatrix} 9 & 18 \\ 15 & 21 \end{bmatrix}\begin{bmatrix} 19 & 6 \\ 5 & 23 \end{bmatrix} = \begin{bmatrix} 261 & 468 \\ 390 & 573 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 26$

Dari contoh tersebut dapat diketahui bahwa $\begin{bmatrix} 9 & 18 \\ 15 & 21 \end{bmatrix}$ adalah invers dari $\begin{bmatrix} 19 & 6 \\ 5 & 23 \end{bmatrix}$ mod 26

Teorema 2.2 :

Misalkan $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ adalah matriks bilangan bulat sedemikian sehingga $\Delta = \det A = ad - bc$ adalah relatif prima terhadap bilangan bulat positif m, maka $A = \bar{\Delta}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ dimana Δ adalah invers dari Δ mod m, dan A adalah invers dari A mod m. (Irawan, dkk, 2014)

Bukti :

Akan ditunjukkan bahwa matriks $\bar{A}$ adalah invers dari A modulo m, dengan menunjukkan bahwa $A\bar{A} \equiv \bar{A}A \equiv I \pmod{m}$

$$A\bar{A} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix}\bar{\Delta}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$\equiv \bar{\Delta}\begin{bmatrix} ad - bc & -ab + ba \\ cd - dc & -cb + da \end{bmatrix} = \bar{\Delta}\begin{bmatrix} ad - bc & 0 \\ 0 & -cb + da \end{bmatrix}$$

$$\equiv \bar{\Delta}\begin{bmatrix} \Delta & 0 \\ 0 & \Delta \end{bmatrix} \equiv \begin{bmatrix} \bar{\Delta}\Delta & 0 \\ 0 & \bar{\Delta}\Delta \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv I \pmod{m}$$

$$\bar{A}A \equiv \bar{\Delta}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\equiv \bar{\Delta}\begin{bmatrix} ad-bc & 0 \\ 0 & -cb+da \end{bmatrix}$$

$$\equiv \bar{\Delta}\begin{bmatrix} \Delta & 0 \\ 0 & \Delta \end{bmatrix}\begin{bmatrix} \bar{\Delta}\Delta & 0 \\ 0 & \bar{\Delta}\Delta \end{bmatrix}$$

$$\equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv I \pmod{m}$$

dimana $\bar{\Delta}$ adalah invers dari $\Delta \pmod{m}$, karena $(\Delta, m) = 1$ (Irawan, dkk, 2014)

Contoh :

Misalkan $A = \begin{bmatrix} 19 & 6 \\ 5 & 23 \end{bmatrix}$ maka det $A = 407$

Invers dari $407 \pmod{26}$ adalah $(\bar{A}) = 23$, karena $\bar{A}A = 407.23 = 9361 \equiv 1 \pmod{26}$ maka diperoleh :

$$A = 23\begin{bmatrix} 23 & -6 \\ -5 & 19 \end{bmatrix} = \begin{bmatrix} 529 & 460 \\ 483 & 437 \end{bmatrix} \bmod 26 \equiv \begin{bmatrix} 9 & 18 \\ 15 & 21 \end{bmatrix}$$

Definisi 2.7 :

Adjoin matriks $A_{n\times n}$ adalah suatu matriks $n \times n$ dimana unsur (i, j) adalah C_{ji}, dengan C_{ji} adalah -1^{i+j} kali determinan dari matriks yang diperoleh dengan menghapus baris ke-i dan kolom ke-j dari A. Adjoin A dinotasikan dengan adj(A).

Misalkan matriks $A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$ dengan unsur-unsurnya a_{ij} dan

(adj A)$= \begin{bmatrix} C_{11} & C_{21} & \dots & C_{n1} \\ C_{12} & a_{22} & \dots & C_{n2} \\ \dots & \dots & \dots & \dots \\ C_{1n} & C_{2n} & \dots & C_{nn} \end{bmatrix}$ dengan unsur-unsurnya C_{ji} dimana

$C_{ij} = (-1)^{i+j}\left|M_{ij}\right|$ yang diperoleh dengan menghapus baris ke-i dan kolom ke-j dari matriks A. (Irawan, dkk, 2014)

Contoh :

Misalkan, $A = \begin{bmatrix} 2 & 1 & 4 \\ 3 & 2 & 1 \\ 5 & 1 & 1 \end{bmatrix}$ dimana entri-entri dari matriks $A \in Z$

$M_{11} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = (2.1 - 1.1) = (2 - 1) = 1$

$C_{11} = 1$

$M_{12} = \begin{bmatrix} 3 & 1 \\ 5 & 1 \end{bmatrix} = (3.1 - 5.1) = (3 - 5) = -2$

$C_{12} = 2$

$M_{13} = \begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix} = (3.1 - 5.2) = (3 - 10) = -7$

$C_{13} = -7$

$M_{21} = \begin{bmatrix} 1 & 4 \\ 1 & 1 \end{bmatrix} = (1.1 - 1.4) = (1 - 4) = -3$

$C_{21} = 3$

$M_{22} = \begin{bmatrix} 2 & 4 \\ 5 & 1 \end{bmatrix} = (2.1 - 5.4) = (2 - 20) = -18$

$C_{22} = -18$

$M_{23} = \begin{bmatrix} 2 & 1 \\ 5 & 1 \end{bmatrix} = (2.1 - 5.1) = (2 - 5) = -3$

$C_{23} = 3$

$M_{31} = \begin{bmatrix} 1 & 4 \\ 2 & 1 \end{bmatrix} = (1.1 - 4.2) = (1 - 8) = -7$

$C_{31} = -7$

$M_{32} = \begin{bmatrix} 2 & 4 \\ 3 & 1 \end{bmatrix} = (2.1 - 4.3) = (2 - 12) = -10$

$C_{32} = 10$

$M_{33} = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} = (2.2 - 3.1) = (4 - 3) = 1$

$C_{33} = 1$

$$(\text{adj } A)=\begin{bmatrix} C_{11} & C_{21} & C_{31} \\ C_{12} & C_{22} & C_{32} \\ C_{13} & C_{23} & C_{33} \end{bmatrix}=\begin{bmatrix} 1 & 3 & -7 \\ 2 & -18 & 10 \\ -7 & 3 & 1 \end{bmatrix}$$

Teorema 2.3 :

Jika A adalah matriks $n \times n$ dengan unsur-unsurnya bilangan bulat dan m adalah bilangan bulat positif, sedemikian sehingga $(\det A, m) = 1$, maka matriks $A = \Delta(adj\ A)$ adalah invers dari A modulo m, dimana Δ adalah invers dari $\Delta = \det A$ modulo m.

Bukti :

Jika $(\det A, m) = 1$, maka $\det(A) \neq 0$

Dengan menggunakan teorema sebelumnya diperoleh $A(\text{adj } A) = (\det A)I = \Delta I$. Karena $(\det A, m) = 1$, maka terdapat $\bar{\Delta}$ invers dari $\Delta = \det A$ modulo m. Sehingga $A(\Delta \text{ adj } A) \equiv A(\text{adj } A)\ \bar{\Delta} \equiv \Delta\bar{\Delta}\ I \equiv I \pmod{m}$. Ini menunjukkan bahwa $A = \Delta$ (adj A) adalah invers dari A modulo m. (Irawan, dkk, 2014)

Definisi 2.8

Sistem residu reduksi modulo m adalah suatu himpunan bilangan bulat r_i sedemikian sehingga $(r_i, m) = 1$, jika $i \neq j$ maka $r_i \neq r_j \pmod{m}$, dan setiap bilangan yang relatif prima terhadap m pasti kongruen modulo m dengan satu anggota r_i dari himpunan tersebut. (Irawan, dkk, 2014)

2.1.4 Keprimaan

Definisi 2.9

Bilangan prima adalah bilangan asli yang tepat mempunyai dua pembagi. Sedangkan bilangan yang mempunyai lebih dari dua pembagi disebut bilangan komposit. (Irawan, dkk, 2014)

Contoh :

$2,3,11,53$ adalah bilangan-bilangan prima, karena pembaginya adalah 1 dan bilangan itu sendiri. Sedangkan $12, 18$ adalah bilangan komposit karena 12 memiliki pembagi $1, 2, 3, 4, 6, 12$ dan 18 memiliki pembagi $1, 2, 3, 6, 9, 18$.

Definisi 2.10 :

Bilangan a dan b dikatakan prima relatif jika $(a, b) = 1$. Begitu pula bilangan bulat $a_1, a_2, \ldots, a_n$ adalah prima relatif jika $(a_1, a_2, \ldots, a_n) = 1$. Dapat dikatakan bahwa $a_1, a_2, \ldots, a_n$ adalah prima relatif bila pasangan $(a_i, a_j) = 1$ untuk semua $i = 1, 2, 3, \ldots, n$ dan $j = 1, 2, 3, \ldots, n$. Ada pula yang menganggap $(a, b) = 1$ dikatakan bahwa a dan b adalah koprima atau a adalah prima pada b. (Irawan, dkk, 2014)

Contoh :

Misalkan terdapat $a = 3$ dan $b = 53$. Bilangan a dan b adalah prima relatif karena $(3, 53) = 1$.

2.1.5 Determinan

Definisi 2.11

Determinan adalah susunan elemen a_{ij} yang disusun atas baris-baris dan kolom-kolom dengan syarat banyaknya baris = banyaknya kolom. (Andari, 2017) Determinan dinotasikan dengan $|\ \ |$. Determinan derajad n, artinya determinan terdiri dari n baris dan n kolom. a_{ij} artinya elemen tersebut terletak pada baris ke-i dan kolom ke-j.

Sifat – sifat determinan :

1. Nilai/ harga suatu determinan tidak berubah jika baris dijadikan kolom atau kolom dijadikan baris.

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{vmatrix}$$

atau $|A| = |A^T|$

2. Jika dalam suatu determinan terdapat suatu baris/ kolom yang semua elemennya nol, maka nilai/ harga determinan $= 0$.

$$\begin{vmatrix} a_{11} & 0 & a_{13} \\ a_{21} & 0 & a_{23} \\ a_{31} & 0 & a_{33} \end{vmatrix} = 0$$

3. Jika dalam suatu determinan 2 baris/ 2 kolom yang berurutan ditukar tempatnya, maka nilai/ harga determinan hanya berubah tanda.

Jika $\begin{vmatrix} a_{11} & x & a_{13} \\ a_{21} & y & a_{23} \\ a_{31} & z & a_{33} \end{vmatrix} = k$, maka $\begin{vmatrix} a_{11} & a_{12} & x \\ a_{21} & a_{22} & y \\ a_{31} & a_{32} & z \end{vmatrix} = -k$

4. Jika dalam suatu determinan terdapat 2 baris/ 2 kolom yang entrinya identik/ sama, maka nilai/ harga determinan sama dengan 0.

$$\begin{vmatrix} a_{11} & x & x \\ a_{21} & y & y \\ a_{31} & z & z \end{vmatrix} = 0$$

5. Jika setiap elemen suatu baris atau kolom dalam suatu determinan digandakan dengan k, maka nilai/ harga determinan baru $= k$ kali determinan semula.

$$\begin{vmatrix} a_{11} & ka_{12} & a_{13} \\ a_{21} & ka_{22} & a_{23} \\ a_{31} & ka_{32} & a_{33} \end{vmatrix} = k \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

6. Jika suatu baris atau suatu kolom dalam determinan ditambah suatu nilai tertentu, maka nilai/ harga determinan yang baru sama dengan determinan

semula ditambah dengan determinan dimana baris atau kolomnya diganti dengan nilai penambahnya.

$$\begin{vmatrix} a_{11} & a_{12} & a_{13}+x \\ a_{21} & a_{22} & a_{23}+y \\ a_{31} & a_{32} & a_{33}+z \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & x \\ a_{21} & a_{22} & y \\ a_{31} & a_{32} & z \end{vmatrix}$$

7. Jika suatu baris/ kolom dalam suatu determinan merupakan kelipatan baris/ kolom yang lain, maka harga determinan sama dengan nol.
8. Jika setiap elemen suatu baris atau kolom ditambah atau dikurangi k kali baris atau kolom yang lain, maka nilai/ harga determinan tidak berubah.

(Andari, 2017)

2.1.6 Kriptografi

Kriptografi dapat diartikan sebagai seni maupun ilmu yang menghasilkan pesan rahasia. Kriptografi memiliki dua konsep utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses penyandian plainteks menjadi cipherteks. Dekripsi adalah proses mengembalikan cipherteks menjadi plainteks semula. Dalam enkripsi maupun dekripsi dibutuhkan kunci yang menjadi parameter dalam melakukan prosesnya (Yusfrizal, 2019).

Kriptografi memiliki beberapa komponen, yaitu :

1. Enkripsi dan dekripsi yang juga merupakan konsep utama dalam kriptografi.
2. Kunci.

   Kunci digunakan untuk melakukan proses enkripsi dan dekripsi. Kunci terbagi menjadi dua yaitu kunci rahasia *(private key)* dan kunci umum *(public key)*.

3. *Plaintext*.

   Plaintext disebut juga dengan *cleartext* yaitu pesan yang ditulis atau diketik yang memiliki makna. Teks asli inilah yang nantinya akan diproses menggunakan algoritma kriptografi untuk menjadi cipherteks.

4. *Ciphertext*.

   Ciphertext merupakan suatu pesan yang telah melalui proses enkripsi. Pesan yang ada tidak bisa dibaca karena berupa karakter-karakter yang tidak mempunyai makna (arti).

5. Pesan.

   Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran komunikasi data, dsb) atau yang disimpan dalam media perekaman (kertas, storage, dsb).

6. *Cryptanalysis*.

   Cryptanalysis bisa diartikan sebagai analisis kode atau suatu ilmu untuk mendapatkan teks-asli tanpa harus mengetahui kunci yang sah secara wajar. Jika berhasil, maka proses tersebut dinamakan *breaking code*. Analisis kode juga dapat menemukan kelemahan dari suatu algoritma kriptografi dan akhirnya dapat menemukan kunci atau *plainteks* dari *cipherteks* yang dienkripsi dengan algoritma tertentu (Ariyus, 2008).

Algoritma kriptografi adalah fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Aman atau tidaknya algoritma kriptografi ditentukan oleh lama waktu yang digunakan untuk memecahkan sandi. Semakin lama waktu yang dibutuhkan untuk memecahkan sandi, maka algoritma itu semakin kuat dan aman

untuk digunakan. Algoritma kriptografi dapat dikelompokkan menjadi algoritma simetri dan asimetri.

Algoritma simetri dapat dianalogikan dengan menggunakan sebuah kotak, gembok, dan kunci gembok. Misalkan A ingin mengirim sebuah surat kepada B dengan menggunakan sebuah kotak sebagai media untuk menyimpan surat tersebut dengan kondisi dimana A dan B sama-sama memiliki kunci gembok yang sama. A memasukkan surat ke dalam kotak, dan menggembok kotak tersebut sehingga orang lain tidak bisa membacanya. Proses yang dilakukan oleh A disebut dengan enkripsi. Kemudian kotak yang berisi surat dikirimkan kepada B. Ketika kotak sampai di tangan B, si B membuka kotak dengan menggunakan kunci gembok lalu membaca suratnya. Proses yang dilakukan oleh B disebut dekripsi. Kelemahan algoritma ini adalah menggunakan kunci enkripsi dan dekripsi yang sama sehingga pengirim dan penerima harus bekerja sama untuk merahasiakan kunci tersebut (Munir dalam Yonathan, dkk,2021). Contoh dari algoritma simetri adalah *DES, T-DES, E-DES, AES, Blowfish, RC6, RC4, RC2, Twofish, Serpent, IDEA, CAST*.

Algoritma Asimetri membutuhkan kunci publik dan kunci privat untuk digunakan oleh pihak yang berkomunikasi. Pengirim mengenkripsi pesan dengan menggunakan kunci publik, sedangkan penerima akan mendekripsikan *ciphertext* yang dikirim dengan menggunakan kunci privat. Algoritma asimetri dianalogikan dengan kotak surat, alamat dari kotak surat, dan kunci kotak surat. Kotak surat secara umum dapat digunakan oleh siapa saja, namun hanya dapat dibuka oleh pemiliknya. Alamat kotak surat adalah kunci publik yang siapa saja dapat mengetahuinya. Kunci kotak surat adalah kunci privat yang bersifat sangat rahasia

dan hanya dimiliki oleh si pemilik kotak surat. Kelemahan dari algoritma asimetri adalah waktu pemrosesan yang lebih lama dibandingkan dengan algoritma simetri karena pembangkitan kunci menggunakan bilangan yang kompleks. Contoh dari algoritma asimetri adalah *RSA, Diffie-Hellman, Digital Secure, XTR, ECC, EES*. (Munir dalam Yonathan, dkk, 2021).

2.1.7 Proses Pertukaran Kunci

Kriptografi asimetri memiliki dua buah kunci yaitu kunci publik dan kunci privat. Kunci publik dapat diketahui oleh semua orang. Sedangkan kunci privat hanya diketahui oleh pihak tertentu dan kerahasiaannya sangat terjaga. Walaupun kriptografi asimetri lebih kuat dari segi keamanan, namun kriptografi simetri masih banyak digunakan karena lebih mudah dalam pengaplikasiannya. Proses pertukaran kunci dilakukan dengan menukarkan kunci publik. Adapun kriptografi yang menggunakan pertukaran kunci pada prosesnya adalah kriptografi *Diffie-Hellman.* Dimana selanjutnya kriptografi *Diffie-Hellman* akan dikombinasikan dengan kriptografi simetri lainnya agar tingkat keamanan pesan lebih terjamin.

Berikut adalah parameter umum yang digunakan pada proses pertukaran kunci :

1. Misalkan terdapat dua orang user yang berkomunikasi, yaitu user 1 dan user 2.
2. Mula-mula user 1 dan user 2 menyepakati bilangan prima yang besar, yaitu n dan g sedemikian hingga $g < n$.

3. Bilangan n dan g tidak perlu rahasia. Bahkan, user 1 dan user 2 dapat membicarakannya melalui saluran yang tidak aman sekalipun.

   (Sembiring, 2015)

2.1.8 Diffie-Hellman

Kriptografi ini diperkenalkan oleh Whitfield Diffie dan Martin Hellman tahun 1975. Dasar dari algoritma *Diffie-Hellman* adalah matematika dasar dari aljabar eksponen dan aritmatika modulus. Algoritma ini menjadi solusi dari pertukaran kunci melewati saluran yang tidak aman. *Diffie-Hellman* tidak berfokus pada enkripsi dan dekripsi, tetapi lebih kepada proses matematika yang dilakukan untuk menghasilkan kunci rahasia yang dapat di sebarluaskan antara pengirim dan penerima secara bebas tanpa harus khawatir dapat dibaca oleh pihak yang tidak bertanggung jawab (Mulyadi, 2019). Parameter umum yang digunakan pada kriptografi *Diffie-Hellman* sama dengan yang telah disebutkan pada 2.1.4.

Algoritma kriptografi *Diffie-Hellman* :

Sean dan Sion menyepakati bilangan prima yang besar yaitu n dan g sedemikian hingga $g < n$.

1. Sean membangkitkan bilangan prima yang besar, yaitu x dan mengirim hasil perhitungan berikut kepada Sion :

   $$X = g^x \ mod \ n$$

2. Sion membangkitkan bilangan prima yang besar, yaitu y dan mengirim hasil perhitungan berikut kepada Sean :

   $$Y = g^y \ mod \ n$$

3. Sion menghitung $K = Y^x \ mod \ n$

4. Sean menghitung

$$K' = X^y \ mod \ n$$

Jika $K = K'$ maka perhitungan yang dilakukan Sean dan Sion adalah benar.

Contoh : Sean dan Sion menyepakati $n = 89$ dan $g = 5 \ \ (g < n)$

1. Sean memilih $x = 36$ dan menghitung :

$$X = g^x \ mod \ n = 5^{36} \ mod \ 89 = 67$$

2. Sion memilih $y = 58$ dan menghitung :

$$Y = g^y \ mod \ n = 5^{58} \ mod \ 89 = 22$$

3. Sean menghitung kunci simetri K,

$$K = Y^x \ mod \ n = 22^{36} \ mod \ 89 = 32$$

4. Sion menghitung kunci simetri K',

$$K' = X^y \ mod \ n = 67^{58} \ mod \ 89 = 32$$

Jadi, Sean dan Sion sekarang sudah mempunyai kunci enkripsi yang sama, yaitu $K = 32$.

2.1.9 Algoritma *Hill Cipher*

Ditemukan oleh Lester S. Hill pada tahun 1929. *Hill Cipher* termasuk dalam algoritma klasik yang menggunakan teknik substitusi *polyalphabet,* yaitu setiap karakter teks-kode dapat menggantikan lebih dari satu macam karakter teks asli (Ariyus, 2008). Prinsip *Hill Cipher* adalah sebuah matriks dapat digunakan untuk mentransformasikan *plaintext* menjadi *ciphertext*.

1. Proses Enkripsi

   Proses enkripsi dilakukan dengan memasukkan plainteks atau pesan yang asli yang akan dikirimkan. Secara matematik, enkripsi *plaintext* P =

$(p_1, p_2, \dots, p_n)$ dengan matriks kunci $\mathrm{K} = [k_{ij}]$ menghasilkan *ciphertext* $\mathbf{C} = (\boldsymbol{c_1}, \boldsymbol{c_2}, \dots, \boldsymbol{c_n})$ dinyatakan sebagai :

$$\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ k_{n1} & k_{n2} & \dots & k_{nn} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix} \bmod n$$

atau dalam notasi $\mathrm{C} = \mathrm{KP} \bmod n$

2. Proses Dekripsi

Proses dekripsi merupakan kebalikan *(reserve)* dari proses enkripsi. Untuk melakukan dekripsi, penerima pesan perlu menghitung *invers* dari matriks kunci. (Ginting, 2020)

Sedangkan dekripsi *ciphertext* $\mathrm{C} = (c_1, c_2, \dots, c_n)$ dengan matriks kunci $\mathrm{K}^{-1} = [k_{ij}]^{-1}$ menghasilkan plaintext $\mathrm{P} = (p_1, p_2, \dots, p_n)$ dinyatakan sebagai :

$$\begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ k_{n1} & k_{n2} & \dots & k_{nn} \end{bmatrix}^{-1} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} \bmod n$$

atau dalam notasi $\mathrm{P} = \mathrm{K}^{-1}\mathrm{C} \bmod n$.

Sebagai contoh, untuk $n = 3$, maka persamaan enkripsi dan dekripsi dinyatakan sebagai berikut :

Ekripsi : $\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \bmod n$

Dekripsi : $\begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix}^{-1} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} \bmod n$

Yang terpenting adalah bagaimana menghitung matriks *invers* (K^{-1}) sedemikian sehingga $KK^{-1} = I$, yang dalam hal ini I adalah matriks identitas

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

Menghitung matriks invers dalam aritmatika modulo tidak boleh menghasilkan negatif dan pecahan, karena operasi kriptografi hanya dalam bilangan bulat tak negatif. Jika ada perhitungan menghasilkan bilangan negatif, maka harus diganti dengan bilangan positif yang kongruen dalam modulo n. (Munir, 2019)

Contoh enkripsi dan dekripsi dengan algoritma *Hill Cipher :*

Enkripsi

Plainteks : LOVEYOURSELF

$C = KP \bmod 26$

Enkripsi tiga huruf pertama : LOV = (11, 14, 21)

Cipherteks : C = $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 11 \\ 14 \\ 21 \end{bmatrix} = \begin{bmatrix} 530 \\ 924 \\ 449 \end{bmatrix} mod\ 26 = \begin{bmatrix} 10 \\ 14 \\ 7 \end{bmatrix}$ = KOH

Enkripsi tiga huruf kedua : EYO = (4, 24, 14)

Cipherteks : C=$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 4 \\ 24 \\ 14 \end{bmatrix} = \begin{bmatrix} 546 \\ 810 \\ 322 \end{bmatrix} mod\ 26 = \begin{bmatrix} 0 \\ 4 \\ 10 \end{bmatrix}$=AEK

Enkripsi tiga huruf ketiga : URS = (20, 17, 18)

Cipherteks : C = $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 20 \\ 17 \\ 18 \end{bmatrix} = \begin{bmatrix} 719 \\ 1104 \\ 416 \end{bmatrix} mod\ 26 = \begin{bmatrix} 17 \\ 12 \\ 0 \end{bmatrix}$= RMA

Enkripsi tiga huruf keempat : ELF = (4, 11, 5)

Cipherteks : C = $\begin{bmatrix}17 & 17 & 5\\21 & 18 & 21\\2 & 2 & 19\end{bmatrix}\begin{bmatrix}4\\11\\5\end{bmatrix} = \begin{bmatrix}280\\387\\125\end{bmatrix} mod\ 26 = \begin{bmatrix}20\\23\\21\end{bmatrix}$= UXV

Cipherteks dari LOVEYOURSELF adalah KOHAEKRMAUXV

Dekripsi

$P = K^{-1}C$

K = $\begin{bmatrix}17 & 17 & 5\\21 & 18 & 21\\2 & 2 & 19\end{bmatrix}$ $K^{-1} = \begin{bmatrix}4 & 9 & 15\\15 & 17 & 6\\24 & 0 & 17\end{bmatrix}$

Chiperteks : KOH atau $C = (10, 14, 7)$

Plainteks: $\begin{bmatrix}4 & 9 & 15\\15 & 17 & 6\\24 & 0 & 17\end{bmatrix}\begin{bmatrix}10\\14\\7\end{bmatrix} = \begin{bmatrix}271\\430\\359\end{bmatrix} mod\ 26 = \begin{bmatrix}11\\14\\21\end{bmatrix}$ = LOV

Chiperteks : AEK atau $C = (0, 4, 10)$

Plainteks: $\begin{bmatrix}4 & 9 & 15\\15 & 17 & 6\\24 & 0 & 17\end{bmatrix}\begin{bmatrix}0\\4\\10\end{bmatrix} = \begin{bmatrix}186\\128\\170\end{bmatrix} mod\ 26 = \begin{bmatrix}4\\24\\14\end{bmatrix}$ = EYO

Chiperteks : RMA atau $C = (17, 12, 0)$

Plainteks: $\begin{bmatrix}4 & 9 & 15\\15 & 17 & 6\\24 & 0 & 17\end{bmatrix}\begin{bmatrix}17\\12\\0\end{bmatrix} = \begin{bmatrix}176\\459\\408\end{bmatrix} mod\ 26 = \begin{bmatrix}20\\17\\18\end{bmatrix}$ = URS

Chiperteks : UXV atau $C = (20, 23, 21)$

Plainteks: $\begin{bmatrix}4 & 9 & 15\\15 & 17 & 6\\24 & 0 & 17\end{bmatrix}\begin{bmatrix}20\\23\\21\end{bmatrix} = \begin{bmatrix}602\\817\\837\end{bmatrix} mod\ 26 = \begin{bmatrix}4\\11\\5\end{bmatrix}$ = ELF

Plainteks dari KOHAEKRMAUXV adalah LOVEYOURSELF

2.2 Kajian Integrasi Topik dengan Al-Quran dan Hadits

Dalam hal ini yaitu kajian integrasi topik dengan amanah. Menurut Ahmad Musthafa Al-Maraghi, amanah adalah segala sesuatu yang harus dijaga dipelihara supaya dapat tersampaikan kepada yang berhak atasnya. Amanah terbagi menjadi tiga, yaitu :

1. Amanah manusia kepada Allah

   Amanah manusia kepada Allah adalah takwa kepada Allah dengan melaksanakan perintah Allah dan menjauhi larangan Allah SWT. Selain itu juga menggunakan karunia yang diberikan oleh Allah SWT dengan sebaik-baiknya untuk hal-hal yang bermanfaat.

2. Amanah kepada sesama manusia

   Menjalankan amanah kepada sesama manusia bukanlah suatu hal yang mudah, terutama dalam bentuk uang atau harta. Karena orang akan mudah tergoda terhadap hal-hal yang berbau duniawi. Contoh amanah kepada sesama manusia adalah menjaga barang titipan tanpa menguranginya, dan mengembalikannya kepada pemilik yang sah.

3. Amanah manusia kepada dirinya sendiri

   Menyangkut kebaikan terhadap dirinya sendiri dalam urusan agama dan dunia, dengan cara tidak melakukan hal-hal yang merugikan baik di dunia maupun di akhirat. (Andika, dkk, 2020).

Adapun ayat yang menjelaskan tentang amanah dalam Al-Qur’an terdapat dalam :

1. QS. Al-Anfal ayat 27 :

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَخُوْنُوا اللّٰهَ وَالرَّسُوْلَ وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ

”Wahai orang-orang yang beriman! Janganlah kamu mengkhianati Allah dan Rasul dan (juga) janganlah kamu mengkhianati amanat yang dipercayakan kepadamu, sedang kamu mengetahui.”(QS. Al-Anfal:27)

Dalam tafsir Al-Qur'an Kementrian Agama RI, tafsir mufradat digunakan untuk mempermudah dalam memahami teks perkara yang terdapat dalam Al-Qur'an. Surat ini dinamakan Al-Anfal yang memiliki arti harta rampasan perang. Hal itu dikarenakan kata Al-Anfal yang terdapat pada permulaan surat ini berasal dari bahasa arab yang berarti "Jarahan", juga persoalan yang menonjol yang dibahas dalam surat ini adalah tentang harta rampasan perang, hukum perang, dan hal-hal yang berhubungan dengan perang pada umumnya. Surat al –Anfal adalah surat ke-8 dalam Al-Qur'an yang terdiri atas 75 ayat dan merupakan surat Madaniyah. Menurut riwayat Ibnu Abbas, surat ini diturunkan berkenaan dengan perang Badar yang terjadi pada tahun 2H, dimana perang ini memiliki arti yang sangat penting karena merupakan peristiwa yang menentukan jalan sejarah perkembangan Islam. Perang yang dimenangkan oleh umat Islam yang berkekuatan kecil melawan kaum musyrik yang berjumlah besar dan memiliki perlengkapan yang cukup ini memperoleh harta rampasan yang tidak sedikit sehingga timbul masalah bagaimana membagi-bagikan harta rampasan perang itu. Oleh sebab itulah, Allah menurunkan ayat pertama surat ini.

Tafsir Al-Muyassar untuk surat Al-Anfal ayat 27 yaitu : "Wahai orang-orang yang beriman kepada Allah dan Rasul-Nya, dan mengikuti syariat-Nya, janganlah kalian mengkhianati Allah dan Rasul-Nya dengan meninggalkan perintah-perintah-Nya dan mengerjakan apa yang Dia larang. Janganlah kalian menyia-nyiakan apa yang Allah percayakan kepada kalian, sedangkan kalian mengetahui bahwa amanah (kepercayaan) itu wajib ditunaikan. (Basyir, dkk, 2011). Selain amanah kepada Allah, amanah kepada sesama manusia, dan amanah kepada diri sendiri, manusia juga memiliki amanah dalam menjaga rahasia. Yaitu

apabila seseorang menyampaikan sesuatu yang penting dan rahasia kepada orang lain, maka sesuatu yang akan disampaikan tersebut merupakan bentuk amanah yang harus dijaga, tanpa boleh diketahui oleh orang yang tidak berhak agar dapat hidup dengan tenang, damai, dan jauh dari dendam. Karenanya setiap muslim dituntut untuk mampu membedakan mana perkataan atau urusan yang termasuk dalam rahasia dan mana yang bukan. Sebagaimana Rasulullah SAW bersabda :

إِذَا حَدَّثَ رَجُلٌ رَجُلاً بِحَدِيْثٍ ثُمَّ الْتَفَتَ فَهُوَ أَمَانَةٌ

"Apabila seseorang membicarakan sesuatu kepada orang lain (sambil) menoleh ke kiri dan ke kanan (karena yang dibicarakan itu rahasia) maka itulah amanah (yang harus dijaga)." (HR. Abu Dawud)

2. Q.S Al-Mu'minun : 8

وَالَّذِينَ هُم لِاَمٰنٰتِهِم وَعَهدِهِم رَاعُونَ

"Perkawinan adalah amanat, maka setiap orang harus memeliharanya dengan baik. Meski begitu, tidak hanya amanat perkawinan yang harus dipelihara, melainkan semua amanat. Dan beruntunglah orang yang memelihara amanat-amanat yang dipikulkan atas mereka dan memelihara janjinya yang dijalin dengan pihak lain."(QS. Al-Mu'minun:8)

Menurut Kemenag, dalam ayat ini Allah menerangkan tentang sifat keenam dari orang-orang mukmin yag beruntung yaitu suka memelihara amanat-amanat yang dipikulnya. Yaitu bilamana kepada mereka dititipkan barang atau uang sebagai amanat yang harus disampaikan kepada orang lain, maka mereka benar-benar menyampaikan amanat itu sebagaimana mestinya dan tidak berbuat khianat. Demikian pula bila mereka mengadakan perjanjian, mereka memenuhinya dengan sempurna.

3. Q.S Al Ahzab : 72

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

"Sesungguhnya Kami telah menawarkan amanat kepada langit, bumi dan gunung-gunung; tetapi semuanya enggan untuk memikul amanat itu dan mereka khawatir tidak akan melaksanakannya (berat), lalu dipikullah amanat itu oleh manusia. Sungguh, manusia itu sangat zalim dan sangat bodoh."
(QS. Al-Ahzab:27)

Tafsir dari ayat tersebut menurut Kemenag adalah sebagai berikut :

Sesungguhnya Allah telah menawarkan tugas-tugas keagamaan kepada langit, bumi, dan gunung-gunung. Karena ketiganya tidak mempunyai persiapan untuk menerima amanat yang berat itu, maka semuanya enggan untuk memikul amanat yang ditawarkan Allah itu. Kemudian amanat untuk melaksanakan tugas-tugas keagamaan itu ditawarkan kepada manusia. Mereka menerimanya dengan konsekuensi barang siapa yang melaksanakan itu akan diberi pahala dan dimasukkan ke dalam surga. Sedangkan barang siapa yang mengkhianatinya akan disiksa dan dimasukkan ke dalam api neraka. Walaupun secara fisik manusia lebih kecil daripada langit, bumi, maupun gunung, manusia mampu mengemban tugas-tugas yang diberikan oleh Allah karena manusia memiliki potensi. Tetapi pada diri manusia terdapat sifat ambisi dan syahwat yang sering mengelabuhi mata dan menutup pandangan hatinya, sehingga Allah menyifatinya dengan amat zalim dan bodoh karena kurang memikirkan akibat-akibat dari penerimaan amanat itu.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian yang dilakukan adalah penelitian kualitatif yaitu penelitian yang menghasilkan penemuan-penemuan yang tidak dapat diperoleh dengan menggunakan prosedur-prosedur statistik atau cara-cara lain dari kuantifikasi (pengukuran). Penelitian kualitatif antara lain bertujuan untuk memperoleh pemahaman yang lebih mendalam dan mengembangkan teori. Penelitian ini menggunakan studi literatur yang berkaitan dengan apa yang diteliti, seperti buku, skripsi dan artikel jurnal.

3.2 Pra Penelitian

Sebelum melakukan penelitian, peneliti terlebih dahulu mencari literatur utama yang melandasi penelitian. Yaitu skripsi tentang penerapan kriptografi hibrida menggunakan algoritma *Hill Cipher* dan *Rivest Shamir Adleman (RSA)* pada pengamanan pesan teks oleh Fatimatuzzahro pada tahun 2021 dan artikel jurnal yang ditulis oleh Tika Khairani, Kiswara Agung Santoso, Ahmad Kamsyakawuni pada tahun 2021 tentang pengkodean monoalphabetic menggunakan *Affine Cipher* dengan kunci *Diffie-Hellman*. Dari rujukan tersebut, peneliti mencari referensi dan memahami materi terkait seperti matriks, aritmatika modular, keprimaan, kriptografi, proses pertukaran kunci, *Diffie-Hellman* dan *Hill Cipher*.

3.3 Tahapan Penelitian

Untuk mencapai tujuan dari penelitian dan menjawab masalah yang telah dirumuskan dalam penelitian, peneliti menggunakan tahapan-tahapan sebagai berikut :

1. Karakteristik matriks yang lebih efektif digunakan dalam kriptografi *Diffie-Hellman.*

   Mengidentifikasi karakteristik matriks yang dapat digunakan untuk melakukan proses enkripsi dan dekripsi dengan cara membuktikan bahwa determinan dari dua matriks yang digunakan sebagai kunci tidak boleh sama dengan nol. Dalam hal ini matriks yang digunakan yaitu matriks ukuran 3×3.

2. Proses enkripsi kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher.*

   a. Menentukan algoritma.

   b. Melakukan simulasi proses enkripsi.

      i. Matriks kunci yang telah sesuai dengan karakteristik akan ditukarkan melalui proses pertukaran kunci *Diffie-Hellman*. Karena kunci yang digunakan berbentuk matriks, maka pertukaran kunci *Diffie-Hellman* diaplikasikan dengan melakukan perkalian pada kedua matriks kunci.

      ii. Menentukan plainteks yang akan digunakan dalam proses enkripsi.

      iii. Mengubah plainteks ke dalam bentuk angka, yang dimulai dari 0 untuk huruf A sampai 53 untuk spasi. Selanutnya plainteks tersebut

akan dikelompokkan menjadi beberapa blok. Dan dilakukan proses dekripsi.

iv. Hasil dari proses enkripsi dikonversi ke dalam bentuk huruf.

3. Proses dekripsi kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher*.

   a. Pembuktian fungsi dekripsi.

   b. Melakukan simulasi proses dekripsi.

      i. Mencari invers dari matriks kunci.

      ii. Melakukan proses dekripsi dengan terlebih dahulu mengkonversikan huruf ke bentuk angka.

      iii. Jika proses dekripsi yang dilakukan benar, maka cipherteks akan kembali ke bentuk plainteks.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Karakteristik Matriks Yang Lebih Efektif Digunakan Dalam Pertukaran Kunci Kriptografi *Diffie-Hellman*

Matriks yang digunakan dalam pertukaran kunci kriptografi *Diffie-Hellman* sangat berkaitan dengan algoritma *Hill Cipher*. Syarat dari keberhasilan proses dekripsi dipengaruhi oleh karakteristik matriks yang digunakan sebagai kunci dimana matriks kunci tersebut harus memiliki invers. Dengan demikian, tidak semua matriks bisa digunakan pada proses dekripsi. Proses penentuan matriks akan membutuhkan waktu yang lama jika ciri-ciri matriks yang memiliki invers tidak diketahui. Oleh karena itulah, selanjutnya ditetapkan karakteristik dari matriks 3×3 yang lebih efektif digunakan pada pertukaran kunci kriptografi *Diffie-Hellman.*

Dalam menentukan karakteristik matriks, determinan dari matriks memiliki peran yang penting. Agar matriks bisa digunakan dalam proses dekripsi, matriks yang akan dijadikan kunci harus memiliki invers, dimana nilai determinan matriks tidak boleh sama dengan nol. Karakteristik dari matriks yang memiliki invers adalah determinannya tidak boleh sama dengan 0. Pada proses enkripsi dan dekripsi *Hill Cipher* yang melibatkan pertukaran kunci *Diffie-Hellman* akan dibuktikan bahwa karakteristik perkalian dari dua matriks yang memiliki invers adalah tidak sama dengan nol pada salah satu matriksnya.

Misal $A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$ dan $B = \begin{bmatrix} j & k & l \\ m & n & o \\ p & q & r \end{bmatrix}$, dengan entri-entri matriks A dan B adalah anggota bilangan prima.

Maka det $(A) = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = (aei + bfg + cdh) - (gec + hfa + idb)$

dan det $(B) = \begin{bmatrix} j & k & l \\ m & n & o \\ p & q & r \end{bmatrix} = (jnr + kop + lmq) - (pnl + qoj + rmk)$

Perkalian matriks AB adalah sebagai berikut :

$$AB = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} j & k & l \\ m & n & o \\ p & q & r \end{bmatrix}$$

Determinan dari matriks AB yaitu

$$\big[\big((aj + bm + cp)(dk + en + fq)(gl + ho + ir)\big) + \big((ak + bn + cq)(dl + eo + fr)(gj + hm + ip)\big) + \big((al + bo + cr)(dj + em + fp)(gk + hn + iq)\big)\big] - \big[\big((gj + hm + ip)(dk + en + fq)(al + bo + cr)\big) + \big((gk + hn + iq)(dl + eo + fr)\big) + \big((gl + ho + ir)(dj + em + fp)(ak + bn + cq)\big)\big]$$

Adapun proposisi yang terkait dengan determinan matriks yang dihasilkan dari penelitian ini adalah :

1. Jika det $(A) \neq 0$ dan det $(B) \neq 0$, maka det $(AB) \neq 0$
2. Jika det $(A) = 0$ dan det $(B) \neq 0$, maka det $(AB) = 0$
3. Jika det $(A) = 0$ dan det $(B) = 0$, maka det $(AB) = 0$
4. Jika det $(A) \neq 0$ dan det $(B) = 0$, maka det $(AB) = 0$

Pembuktian proposisi :

1. Jika det $A \neq 0$ dan det $B \neq 0$, maka det $A \neq$ det B.

   Tujuan pembuktian :

   $$\begin{aligned}&\big[\big((aj+bm+cp)(dk+en+fq)(gl+ho+ir)\big)+\big((ak+bn+\\&cq)(dl+eo+fr)(gj+hm+ip)\big)+\big((al+bo+cr)(dj+em+\\&fp)(gk+hn+iq)\big)\big]\\ \neq\ &\big[\big((gj+hm+ip)(dk+en+fq)(al+bo+cr)\big)+\big((gk+\\&hn+iq)(dl+eo+fr)(aj+bm+cp)\big)+\big((gl+ho+\\&ir)(dj+em+fp)(ak+bn+\\&cq)\big)\big]\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(*)\end{aligned}$$

   Pembuktian menggunakan kontradiksi :

   Andaikan det $A =$ det B, maka

   $$\begin{aligned}&\big[\big((aj+bm+cp)(dk+en+fq)(gl+ho+ir)\big)+\big((ak+bn+\\&cq)(dl+eo+fr)(gj+hm+ip)\big)+\big((al+bo+cr)(dj+em+\\&fp)(gk+hn+iq)\big)\big]\\ =\ &\big[\big((gj+hm+ip)(dk+en+fq)(al+bo+cr)\big)+\big((gk+\\&hn+iq)(dl+eo+fr)(aj+bm+cp)\big)+\big((gl+ho+\\&ir)(dj+em+fp)(ak+bn+cq)\big)\big]\end{aligned}$$

   Jadi, didapatkan persamaan berikut :

   $$\begin{aligned}&(ajdkgl+ajdkho+ajdkir+ajengl+ajenho+ajenir+ajfqgl+\\&ajfqho+ajffqir+bmdkgl+bmdkho+bmdkir+bmengl+\\&bmenho+bmenir+bmfqgl+bmfqho+bmfqir+cpdkgl+\\&cpdkho+cpdkir+cpengl+cpenho+cpenir+cpfqgl+cpfqho+\\&cpfqir)+(akdlgj+akdlhm+akdlip+akeogj+akeohm+\\&akeoip+akfrgj+akfrhm+akfrip+bndlgj+bndlhm+\\&bndlip+bneogj+bneohm+bneoip+bnfrgj+bnfrhm+\\&bnfrip+cqdlgj+cqdlhm+cqdlip+cqeogj+cqeohm+cqeoip+\end{aligned}$$

$$cqfrgj + cqfrhm + cqfrip) + (aldjgk + aldjhn + aldjiq + alemgk + alemhn + alemiq + alfpgk + alfphn + alfpiq + bodjgk + bodjhn + bodjiq + boemgk + boemhn + boemiq + bofpgk + bofphn + bofpiq + crdjgk + crdjhn + crdjiq + cremgk + cremhn + cremiq + crfpgk + crfphn + crfpiq)$$

$$= (gjdkal + gjdkbo + gjdkcr + gjenal + gjenbo + gjencr + gjfqal + gjfqbo + gjfqcr + hmdkal + hmdkbo + hmdkcr + hmenal + hmenbo + hmencr + hmfqal + hmfqbo + hmfqcr + ipdkal + ipdkbo + ipdkcr + ipenal + ipenbo + ipencr + ipfqal + ipfqbo + ipfqcr) + (gkdlaj + gkdlbm + gkdlcp + gkeoaj + gkeobm + gkeocp + gkfraj + gkfrbm + gkfrcp + hndlaj + hndlbm + hndlcp + hneoaj + hneobm + hneocp + hnfraj + hnfrbm + hnfrcp + iqdlaj + iqdlbm + iqdlcp + iqeoaj + iqeobm + iqeocp + iqfraj + iqfrbm + iqfrcp) + (gldjak + gldjbn + gldjcq + glemak + glembn + glemcq + glfpak + glfpbn + glfpcq + hodjak + hodjbn + hodjcq + hoemak + hoembn + hoemcq + hofpak + hofpbn + hofpcq + irdjak + irdjbn + irdjcq + iremak + irembn + iremcq + irfpak + irfpbn + irfpcq)$$

Pencoretan yang dilakukan bertujuan untuk mengeliminasi elemen yang sama antara ruas kanan dan ruas kiri.

$$(\cancel{ajdkgl + ajdkho + ajdkir + ajengl + ajenho} + ajenir + \cancel{ajfqgl} + ajfqho + \cancel{ajffqir} + \cancel{bmdkgl + bmdkho} + bmdkir + \cancel{bmengl + bmenho + bmenir} + bmfqgl + \cancel{bmfqho + bmfqir} + \cancel{cpdkgl} + cpdkho + \cancel{cpdkir} + cpengl + \cancel{cpenho + cpenir + cpfqgl + cpfqho + cpfqir}) + (\cancel{akdlgj + akdlhm + akdlip + akeogj + akeohm} + akeoip + \cancel{akfrgj} + akfrhm + \cancel{akfrip + bndlgj + bndlhm} + bndlip + \cancel{bneogj + bneohm} + \cancel{bneoip} + bnfrgj + \cancel{bnfrhm + bnfrip + cqdlgj} + cqdlhm + \cancel{cqdlip} + cqeogj + \cancel{cqeohm + cqeoip + cqfrgj + cqfrhm + cqfrip}) + (\cancel{aldjgk + aldjhn + aldjiq +}$$

$$\begin{aligned}
&\cancel{alemgk + alemhn} + alemiq + \cancel{alfpgk} + alfphn + \cancel{alfpiq + bodjgk + bodjhn} + bodjiq + \cancel{boemgk + boemhn + boemiq} + \\
&bofpgk + \cancel{bofphn + bofpiq + crdjgk} + crdjhn + \cancel{crdjiq} + \\
&cremgk + \cancel{cremhn + cremiq + crfpgk + crfphn + crfpiq}) \\
=\quad &(\cancel{gjdkal + gjdkbo + gjdkcr + gjenal + gjenbo} + gjencr + \\
&\cancel{gjfqal} + gjfqbo + \cancel{gjfqcr + hmdkal} + \cancel{hmdkbo} + \\
&hmdkcr + \cancel{hmenal + hmenbo + hmencr} + hmfqal + \\
&\cancel{hmfqbo + hmfqcr + ipdkal} + ipdkbo + \cancel{ipdkcr} + ipenal + \\
&\cancel{ipenbo + ipencr + ipfqal + ipfqbo + ipfqcr}) + (\cancel{gkdlaj + gkdlbm + gkdlcp + gkeoaj + gkeobm} + gkeocp + \cancel{gkfraj} + \\
&gkfrbm + \cancel{gkfrcp + hndlaj + hndlbm} + hndlcp + \cancel{hneoaj + hneobm + hneocp} + hnfraj + \cancel{hnfrbm + hnfrcp + iqdlaj} + \\
&iqdlbm + \cancel{iqdlcp} + iqeoaj + \cancel{iqeobm + iqeocp + iqfraj + iqfrbm + iqfrcp}) + (\cancel{gldjak + gldjbn + gldjcq + glemak + glembn} + glemcq + \cancel{glfpak} + glfpbn + \cancel{glfpcq} + \cancel{hodjak + hodjbn} + hodjcq + \cancel{hoemak + hoembn + hoemcq} + \\
&hofpak + \cancel{hofpbn + hofpcq + irdjak} + irdjbn + \cancel{irdjcq} + \\
&iremak + \cancel{irembn + iremcq + irfpak + irfpbn + irfpcq})
\end{aligned}$$

$$\begin{aligned}
&ajenir + ajfqho + bmdkir + bmfqgl + cpdkho + cpengl + akeoip + \\
&akfrhm + bnfrgj + bndlip + cqdlhm + cqeogj + alemiq + \\
&alfphm + bodjiq + bofpgk + crdjhn + cremgk \\
=\quad &gjencr + gjfqbo + hmdkcr + hmfqal + ipdkbo + ipenal + \\
&gkeocp + gkfrbm + hndlcp + hnfraj + iqdlbm + iqeoaj + \\
&glemcq + glfpbn + hodjcq + hofpak + irdjbn + iremak
\end{aligned}$$

$$\begin{aligned}
&ajenir + akeoip + alemiq + bnfrgj + bofpgk + bmfqgl + \\
&cpdkho + cqdlhm + crdjhn - gjencr - gkeocp - glemcq - \\
&hmfqal - hnfraj - hofpak - ipdkbo - iqdlbm - irdjbn \\
=\quad &ipenal + iqeoaj + iremak + gjfqbo + gkfrbm + glfpbn + \\
&hmdkcr + hndlcp + hodjcq - cpengl - cqeogj - cremgk - \\
&ajfqho - akfrhm - alfphn - bmdkir - bndlip - bodjiq
\end{aligned}$$

$[(aei + bfg + cdh) - (gec + hfa + idb)](jnr + kop + lmq) =$
$[(aei + bfg + cdh) - (gec + hfa + idb)](pnl + qoj + rmk)$

Dengan menggunakan penyederhanaan persamaan, di dapatkan :

$jnr + kop + lmq = pnl + qoj + rmk$ ……(∗∗)

Berdasarkan persamaan (∗∗) maka det $(B) = 0$. Hal ini kontradiksi dengan yang diketahui bahwa det $(B) \neq 0$. Jadi pengandaian bernilai salah.Oleh karena itu pernyataan bernilai benar.

2. Jika det $(A) = 0$ dan det $(B) \neq 0$, maka det $(AB) = 0$

   Pembuktian :

   $\big[\big((aj + bm + cp)(dk + en + fq)(gl + ho + ir)\big) + \big((ak + bn + cq)(dl + eo + fr)(gjhm + ip)\big) + \big((al + bo + cr)(dj + em + fp)(gk + hn + iq)\big)\big]$
   $= \big[\big((gj + hm + ip)(dk + en + fq)(al + bo + cr)\big) + \big((gk + hn + iq)(dl + eo + fr)(aj + bm + cp)\big) + \big((gl + ho + ir)(dj + em + fp)(ak + bn + cq)\big)\big]$

   $(ajdkgl + ajdkho + ajdkir + ajengl + ajenho + ajenir + ajfqgl + ajfqho + ajffqir + bmdkgl + bmdkho + bmdkir + bmengl + bmenho + bmenir + bmfqgl + bmfqho + bmfqir + cpdkgl + cpdkho + cpdkir + cpengl + cpenho + cpenir + cpfqgl + cpfqho + cpfqir) + (akdlgj + akdlhm + akdlip + akeogj + akeohm + akeoip + akfrgj + akfrhm + akfrip + bndlgj + bndlhm + bndlip + bneogj + bneohm + bneoip + bnfrgj + bnfrhm + bnfrip + cqdlgj + cqdlhm + cqdlip + cqeogj + cqeohm + cqeoip + cqfrgj + cqfrhm + cqfrip) + (aldjgk + aldjhn + aldjiq + alemgk + alemhn + alemiq + alfpgk + alfphn + alfpiq +$

$$bodjgk + bodjhn + bodjiq + boemgk + boemhn + boemiq + bofpgk + bofphn + bofpiq + crdjgk + crdjhn + crdjiq + cremgk + cremhn + cremiq + crfpgk + crfphn + crfpiq)$$

$$= (gjdkal + gjdkbo + gjdkcr + gjenal + gjenbo + gjencr + gjfqal + gjfqbo + gjfqcr + hmdkal + hmdkbo + hmdkcr + hmenal + hmenbo + hmencr + hmfqal + hmfqbo + hmfqcr + ipdkal + ipdkbo + ipdkcr + ipenal + ipenbo + ipencr + ipfqal + ipfqbo + ipfqcr) + (gkdlaj + gkdlbm + gkdlcp + gkeoaj + gkeobm + gkeocp + gkfraj + gkfrbm + gkfrcp + hndlaj + hndlbm + hndlcp + hneoaj + hneobm + hneocp + hnfraj + hnfrbm + hnfrcp + iqdlaj + iqdlbm + iqdlcp + iqeoaj + iqeobm + iqeocp + iqfraj + iqfrbm + iqfrcp) + (gldjak + gldjbn + gldjcq + glemak + glembn + glemcq + glfpak + glfpbn + glfpcq + hodjak + hodjbn + hodjcq + hoemak + hoembn + hoemcq + hofpak + hofpbn + hofpcq + irdjak + irdjbn + irdjcq + iremak + irembn + iremcq + irfpak + irfpbn + irfpcq)$$

Pencoretan yang dilakukan bertujuan untuk mengeliminasi elemen yang sama antara ruas kanan dan ruas kiri.

$$(\cancel{ajdkgl + ajdkho + ajdkir + ajengl + ajenho} + ajenir + \cancel{ajfqgl} + ajfqho + \cancel{ajffqir} + \cancel{bmdkgl + bmdkho} + bmdkir + \cancel{bmengl + bmenho + bmenir} + bmfqgl + \cancel{bmfqho + bmfqir} + \cancel{cpdkgl} + cpdkho + \cancel{cpdkir} + cpengl + \cancel{cpenho + cpenir + cpfqgl + cpfqho + cpfqir}) + (\cancel{akdlgj + akdlhm + akdlip + akeogj + akeohm} + akeoip + \cancel{akfrgj} + akfrhm + \cancel{akfrip + bndlgj + bndlhm} + bndlip + \cancel{bneogj + bneohm} + \cancel{bneoip} + bnfrgj + \cancel{bnfrhm + bnfrip + cqdlgj} + cqdlhm + \cancel{cqdlip} + cqeogj + \cancel{cqeohm + cqeoip + cqfrgj + cqfrhm + cqfrip}) + (\cancel{aldjgk + aldjhn + aldjiq + alemgk + alemhn} + alemiq + \cancel{alfpgk} + alfphn + \cancel{alfpiq +}$$

$$\begin{aligned}
&\cancel{bodjgk + bodjhn} + bodjiq + \cancel{boemgk + boemhn + boemiq} + \\
&bofpgk + \cancel{bofphn + bofpiq + crdjgk} + crdjhn + \cancel{crdjiq} + \\
&cremgk + \cancel{cremhn + cremiq + crfpgk + crfphn + crfpiq}) \\
=\ &(\cancel{gjdkal + gjdkbo + gjdkcr + gjenal + gjenbo} + gjencr + \\
&\cancel{gjfqal} + gjfqbo + \cancel{gjfqcr + hmdkal} + \cancel{hmdkbo} + \\
&hmdkcr + \cancel{hmenal + hmenbo + hmencr} + hmfqal + \\
&\cancel{hmfqbo + hmfqcr + ipdkal} + ipdkbo + \cancel{ipdkcr} + ipenal + \\
&\cancel{ipenbo + ipencr + ipfqal + ipfqbo + ipfqcr}) + \\
&(\cancel{gkdlaj + gkdlbm + gkdlcp + gkeoaj + gkeobm} + \\
&gkeocp + \cancel{gkfraj} + gkfrbm + \cancel{gkfrcp + hndlaj + hndlbm} + \\
&hndlcp + \cancel{hneoaj + hneobm + hneocp} + hnfraj + \cancel{hnfrbm + \\
&hnfrcp + iqdlaj} + iqdlbm + \cancel{iqdlcp} + iqeoaj + \cancel{iqeobm + \\
&iqeocp + iqfraj + iqfrbm + iqfrcp}) + (\cancel{gldjak + gldjbn + \\
&gldjcq + glemak + glembn} + glemcq + \cancel{glfpak} + glfpbn + \\
&\cancel{glfpcq} + \cancel{hodjak + hodjbn} + hodjcq + \cancel{hoemak + hoembn + \\
&hoemcq} + hofpak + \cancel{hofpbn + hofpcq + irdjak} + irdjbn + \\
&\cancel{irdjcq} + iremak + \cancel{irembn + iremcq + irfpak + irfpbn + \\
&irfpcq})
\end{aligned}$$

$$\begin{aligned}
&ajenir + akeoip + alemiq + bnfrgj + bofpgk + bmfqgl + \\
&cpdkho + cqdlhm + crdjhn - gjencr - gkeocp - glemcq - \\
&hmfqal - hnfraj - hofpak - ipdkbo - iqdlbm - irdjbn \\
=\ &ipenal + iqeoaj + iremak + gjfqbo + gkfrbm + \\
&glfpbn + hmdkcr + hndlcp + hodjcq - cpengl - \\
&cqeogj - cremgk - ajfqho - akfrhm - alfphn - \\
&bmdkir - bndlip - bodjiq
\end{aligned}$$

$$\begin{aligned}
&[(aei + bfg + cdh) - (gec + hfa + idb)](jnr + kop + lmq) = \\
&[(aei + bfg + cdh) - (gec + hfa + idb)](pnl + qoj + rmk) \\
&[(aei + bfg + cdh) - (gec + hfa + idb)](jnr + kop + lmq) - \\
&[(aei + bfg + cdh) - (gec + hfa + idb)](pnl + qoj + rmk)
\end{aligned}$$

$[(aei + bfg + cdh) - (gec + hfa + idb)][(jnr + kop + lmq) - (pnl + qoj + rmk)]$

$= 0.[(jnr + kop + lmq) - (pnl + qoj + rmk)] = 0$

3. Jika det $(A) = 0$ dan det $(B) = 0$, maka det $(AB) = 0$

   Pembuktian :

   $\big[\big((aj + bm + cp)(dk + en + fq)(gl + ho + ir)\big) + \big((ak + bn + cq)(dl + eo + fr)(gjhm + ip)\big) + \big((al + bo + cr)(dj + em + fp)(gk + hn + iq)\big)\big]$

   $= \big[\big((gj + hm + ip)(dk + en + fq)(al + bo + cr)\big) + \big((gk + hn + iq)(dl + eo + fr)(aj + bm + cp)\big) + \big((gl + ho + ir)(dj + em + fp)(ak + bn + cq)\big)\big]$

   $(ajdkgl + ajdkho + ajdkir + ajengl + ajenho + ajenir + ajfqgl + ajfqho + ajffqir + bmdkgl + bmdkho + bmdkir + bmengl + bmenho + bmenir + bmfqgl + bmfqho + bmfqir + cpdkgl + cpdkho + cpdkir + cpengl + cpenho + cpenir + cpfqgl + cpfqho + cpfqir) + (akdlgj + akdlhm + akdlip + akeogj + akeohm + akeoip + akfrgj + akfrhm + akfrip + bndlgj + bndlhm + bndlip + bneogj + bneohm + bneoip + bnfrgj + bnfrhm + bnfrip + cqdlgj + cqdlhm + cqdlip + cqeogj + cqeohm + cqeoip + cqfrgj + cqfrhm + cqfrip) + (aldjgk + aldjhn + aldjiq + alemgk + alemhn + alemiq + alfpgk + alfphn + alfpiq + bodjgk + bodjhn + bodjiq + boemgk + boemhn + boemiq + bofpgk + bofphn + bofpiq + crdjgk + crdjhn + crdjiq + cremgk + cremhn + cremiq + crfpgk + crfphn + crfpiq)$

   $= (gjdkal + gjdkbo + gjdkcr + gjenal + gjenbo + gjencr + gjfqal + gjfqbo + gjfqcr + hmdkal + hmdkbo + hmdkcr + hmenal + hmenbo + hmencr + hmfqal + hmfqbo + hmfqcr + ipdkal + ipdkbo + ipdkcr + ipenal +$

$$ipenbo + ipencr + ipfqal + ipfqbo + ipfqcr) + (gkdlaj + gkdlbm + gkdlcp + gkeoaj + gkeobm + gkeocp + gkfraj + gkfrbm + gkfrcp + hndlaj + hndlbm + hndlcp + hneoaj + hneobm + hneocp + hnfraj + hnfrbm + hnfrcp + iqdlaj + iqdlbm + iqdlcp + iqeoaj + iqeobm + iqeocp + iqfraj + iqfrbm + iqfrcp) + (gldjak + gldjbn + gldjcq + glemak + glembn + glemcq + glfpak + glfpbn + glfpcq + hodjak + hodjbn + hodjcq + hoemak + hoembn + hoemcq + hofpak + hofpbn + hofpcq + irdjak + irdjbn + irdjcq + iremak + irembn + iremcq + irfpak + irfpbn + irfpcq)$$

Pencoretan yang dilakukan bertujuan untuk mengeliminasi elemen yang sama antara ruas kanan dan ruas kiri.

$$(\cancel{ajdkgl + ajdkho + ajdkir + ajengl + ajenho} + ajenir + \cancel{ajfqgl} + ajfqho + \cancel{ajffqir} + \cancel{bmdkgl + bmdkho} + bmdkir + \cancel{bmengl + bmenho + bmenir} + bmfqgl + \cancel{bmfqho + bmfqir} + \cancel{cpdkgl} + cpdkho + \cancel{cpdkir} + cpengl + \cancel{cpenho + cpenir + cpfqgl + cpfqho + cpfqir}) + (\cancel{akdlgj + akdlhm + akdlip + akeogj + akeohm} + akeoip + \cancel{akfrgj} + akfrhm + \cancel{akfrip + bndlgj + bndlhm} + bndlip + \cancel{bneogj + bneohm} + \cancel{bneoip} + bnfrgj + \cancel{bnfrhm + bnfrip + cqdlgj} + cqdlhm + \cancel{cqdlip} + cqeogj + \cancel{cqeohm + cqeoip + cqfrgj + cqfrhm + cqfrip}) + (\cancel{aldjgk + aldjhn + aldjiq + alemgk + alemhn} + alemiq + \cancel{alfpgk} + alfphn + \cancel{alfpiq + bodjgk + bodjhn} + bodjiq + \cancel{boemgk + boemhn + boemiq} + bofpgk + \cancel{bofphn + bofpiq + crdjgk} + crdjhn + \cancel{crdjiq} + cremgk + \cancel{cremhn + cremiq + crfpgk + crfphn + crfpiq})$$

$$= (\cancel{gjdkal + gjdkbo + gjdkcr + gjenal + gjenbo} + gjencr + \cancel{gjfqal} + gjfqbo + \cancel{gjfqcr + hmdkal} + \cancel{hmdkbo} + hmdkcr + \cancel{hmenal + hmenbo + hmencr} + hmfqal + \cancel{hmfqbo + hmfqcr + ipdkal} + ipdkbo + \cancel{ipdkcr} + ipenal +$$

$$\begin{aligned}
&\cancel{ipenbo + ipencr + ipfqal + ipfqbo + ipfqcr}) + \\
&(\cancel{gkdlaj + gkdlbm + gkdlcp + gkeoaj + gkeobm} + \\
&gkeocp + \cancel{gkfraj} + gkfrbm + \cancel{gkfrcp + hndlaj + hndlbm} + \\
&hndlcp + \cancel{hneoaj + hneobm + hneocp} + hnfraj + \cancel{hnfrbm + \\
&hnfrcp + iqdlaj} + iqdlbm + \cancel{iqdlcp} + iqeoaj + \cancel{iqeobm + \\
&iqeocp + iqfraj + iqfrbm + iqfrcp}) + (\cancel{gldjak + gldjbn + \\
&gldjcq + glemak + glembn} + glemcq + \cancel{glfpak} + glfpbn + \\
&\cancel{glfpcq} + \cancel{hodjak + hodjbn} + hodjcq + \cancel{hoemak + hoembn + \\
&hoemcq} + hofpak + \cancel{hofpbn + hofpcq + irdjak} + irdjbn + \\
&\cancel{irdjcq} + iremak + \cancel{irembn + iremcq + irfpak + irfpbn + \\
&irfpcq})
\end{aligned}$$

$$\begin{aligned}
&ajenir + ajfqho + bmdkir + bmfqgl + cpdkho + cpengl + akeoip + \\
&akfrhm + bnfrgj + bndlip + cqdlhm + cqeogj + alemiq + \\
&alfphm + bodjiq + bofpgk + crdjhn + cremgk \\
=\quad &gjencr + gjfqbo + hmdkcr + hmfqal + ipdkbo + ipenal + \\
&gkeocp + gkfrbm + hndlcp + hnfraj + iqdlbm + iqeoaj + \\
&glemcq + glfpbn + hodjcq + hofpak + irdjbn + iremak
\end{aligned}$$

$$\begin{aligned}
&ajenir + ajfqho + bmdkir + bmfqgl + cpdkho + cpengl + akeoip + \\
&akfrhm + bnfrgj + bndlip + cqdlhm + cqeogj + alemiq + \\
&alfphm + bodjiq + bofpgk + crdjhn + cremgk - gjencr - \\
&gjfqbo - hmdkcr - hmfqal - ipdkbo - ipenal - gkeocp - \\
&gkfrbm - hndlcp - hnfraj - iqdlbm - iqeoaj - glemcq - \\
&glfpbn - hodjcq - hofpak - irdjbn - iremak = 0
\end{aligned}$$

$$\begin{aligned}
&[(aei + bfg + cdh) - (gec + hfa + idb)](jnr + kop + lmq) - \\
&[(aei + bfg + cdh) - (\ gec + hfa + idb)](pnl + qoj + rmk) = 0 \\
&[(aei + bfg + cdh) - (gec + hfa + idb)](jnr + kop + lmq) = \\
&[(aei + bfg + cdh) - (\ gec + hfa + idb)](pnl + qoj + \quad rmk)
\end{aligned}$$

$[(aei + bfg + cdh) - (gec + hfa + idb)](jnr + kop + lmq) -$
$[(aei + bfg + cdh) - (\ gec + hfa + idb)](pnl + qoj + rmk)$

$[(aei + bfg + cdh) - (gec + hfa + idb)][(jnr + kop + lmq) -$
$(pnl + qoj + rmk)] = 0.0 = 0$

4. Jika det $(A) \neq 0$ dan det $(B) = 0$, maka det $(AB) = 0$

   Pembuktian :

   $\big[\big((aj + bm + cp)(dk + en + fq)(gl + ho + ir)\big) + \big((ak + bn +$
   $cq)(dl + eo + fr)(gjhm + ip)\big) + \big((al + bo + cr)(dj + em +$
   $fp)(gk + hn + iq)\big)\big]$

   $= \quad \big[\big((gj + hm + ip)(dk + en + fq)(al + bo + cr)\big) +$
   $\big((gk + hn + iq)(dl + eo + fr)(aj + bm + cp)\big) +$
   $\big((gl + ho + ir)(dj + em + fp)(ak + bn + cq)\big)\big]$

   $(ajdkgl + ajdkho + ajdkir + ajengl + ajenho + ajenir + ajfqgl +$
   $ajfqho + ajffqir + bmdkgl + bmdkho + bmdkir + bmengl +$
   $bmenho + bmenir + bmfqgl + bmfqho + bmfqir + cpdkgl +$
   $cpdkho + cpdkir + cpengl + cpenho + cpenir + cpfqgl + cpfqho +$
   $cpfqir) + (akdlgj + akdlhm + akdlip + akeogj + akeohm +$
   $akeoip + akfrgj + akfrhm + akfrip + bndlgj + bndlhm +$
   $bndlip + bneogj + bneohm + bneoip + bnfrgj + bnfrhm +$
   $bnfrip + cqdlgj + cqdlhm + cqdlip + cqeogj + cqeohm + cqeoip +$
   $cqfrgj + cqfrhm + cqfrip) + (aldjgk + aldjhn + aldjiq +$
   $alemgk + alemhn + alemiq + alfpgk + alfphn + alfpiq +$
   $bodjgk + bodjhn + bodjiq + boemgk + boemhn + boemiq +$
   $bofpgk + bofphn + bofpiq + crdjgk + crdjhn + crdjiq +$
   $cremgk + cremhn + cremiq + crfpgk + crfphn + crfpiq)$

   $= \quad (gjdkal + gjdkbo + gjdkcr + gjenal + gjenbo + gjencr +$
   $gjfqal + gjfqbo + gjfqcr + hmdkal + hmdkbo +$
   $hmdkcr + hmenal + hmenbo + hmencr + hmfqal +$

$$hmfqbo + hmfqcr + ipdkal + ipdkbo + ipdkcr + ipenal + ipenbo + ipencr + ipfqal + ipfqbo + ipfqcr) + (gkdlaj + gkdlbm + gkdlcp + gkeoaj + gkeobm + gkeocp + gkfraj + gkfrbm + gkfrcp + hndlaj + hndlbm + hndlcp + hneoaj + hneobm + hneocp + hnfraj + hnfrbm + hnfrcp + iqdlaj + iqdlbm + iqdlcp + iqeoaj + iqeobm + iqeocp + iqfraj + iqfrbm + iqfrcp) + (gldjak + gldjbn + gldjcq + glemak + glembn + glemcq + glfpak + glfpbn + glfpcq + hodjak + hodjbn + hodjcq + hoemak + hoembn + hoemcq + hofpak + hofpbn + hofpcq + irdjak + irdjbn + irdjcq + iremak + irembn + iremcq + irfpak + irfpbn + irfpcq)$$

Pencoretan yang dilakukan bertujuan untuk mengeliminasi elemen yang sama antara ruas kanan dan ruas kiri.

$$(\cancel{ajdkgl + ajdkho + ajdkir + ajengl + ajenho} + ajenir + \cancel{ajfqgl} + ajfqho + \cancel{ajffqir} + \cancel{bmdkgl + bmdkho} + bmdkir + \cancel{bmengl + bmenho + bmenir} + bmfqgl + \cancel{bmfqho + bmfqir} + \cancel{cpdkgl} + cpdkho + \cancel{cpdkir} + cpengl + \cancel{cpenho + cpenir + cpfqgl + cpfqho + cpfqir}) + (\cancel{akdlgj + akdlhm + akdlip + akeogj + akeohm} + akeoip + \cancel{akfrgj} + akfrhm + \cancel{akfrip + bndlgj + bndlhm} + bndlip + \cancel{bneogj + bneohm} + \cancel{bneoip} + bnfrgj + \cancel{bnfrhm + bnfrip + cqdlgj} + cqdlhm + \cancel{cqdlip} + cqeogj + \cancel{cqeohm + cqeoip + cqfrgj + cqfrhm + cqfrip}) + (\cancel{aldjgk + aldjhn + aldjiq + alemgk + alemhn} + alemiq + \cancel{alfpgk} + alfphn + \cancel{alfpiq + bodjgk + bodjhn} + bodjiq + \cancel{boemgk + boemhn + boemiq} + bofpgk + \cancel{bofphn + bofpiq + crdjgk} + crdjhn + \cancel{crdjiq} + cremgk + \cancel{cremhn + cremiq + crfpgk + crfphn + crfpiq})$$

$$= (\cancel{gjdkal + gjdkbo + gjdkcr + gjenal + gjenbo} + gjencr + \cancel{gjfqal} + gjfqbo + \cancel{gjfqcr + hmdkal} + \cancel{hmdkbo} + hmdkcr + \cancel{hmenal + hmenbo + hmencr} + hmfqal +$$

$$\begin{aligned}
&\cancel{hmfqbo + hmfqcr + ipdkal} + ipdkbo + \cancel{ipdkcr} + ipenal + \\
&\cancel{ipenbo + ipencr + ipfqal + ipfqbo + ipfqcr}) + \\
&(\cancel{gkdlaj + gkdlbm + gkdlcp + gkeoaj + gkeobm} + \\
&gkeocp + \cancel{gkfraj} + gkfrbm + \cancel{gkfrcp + hndlaj + hndlbm} + \\
&hndlcp + \cancel{hneoaj + hneobm + hneocp} + hnfraj + \cancel{hnfrbm + \\
&hnfrcp + iqdlaj} + iqdlbm + \cancel{iqdlcp} + iqeoaj + \cancel{iqeobm + \\
&iqeocp + iqfraj + iqfrbm + iqfrcp}) + (\cancel{gldjak + gldjbn + \\
&gldjcq + glemak + glembn} + glemcq + \cancel{glfpak} + glfpbn + \\
&\cancel{glfpcq} + \cancel{hodjak + hodjbn} + hodjcq + \cancel{hoemak + hoembn + \\
&hoemcq} + hofpak + \cancel{hofpbn + hofpcq + irdjak} + irdjbn + \\
&\cancel{irdjcq} + iremak + \cancel{irembn + iremcq + irfpak + irfpbn + \\
&irfpcq})
\end{aligned}$$

$$\begin{aligned}
&ajenir + ajfqho + bmdkir + bmfqgl + cpdkho + cpengl + akeoip + \\
&akfrhm + bnfrgj + bndlip + cqdlhm + cqeogj + alemiq + \\
&alfphm + bodjiq + bofpgk + crdjhn + cremgk \\
=\ &gjencr + gjfqbo + hmdkcr + hmfqal + ipdkbo + ipenal + \\
&gkeocp + gkfrbm + hndlcp + hnfraj + iqdlbm + iqeoaj + \\
&glemcq + glfpbn + hodjcq + hofpak + irdjbn + iremak
\end{aligned}$$

$$\begin{aligned}
&ajenir + akeoip + alemiq + bnfrgj + bofpgk + bmfqgl + crdjhn + \\
&cpdkho + cqdlhm - ipenal - iqeoaj - iremak - glfpbn - gjfqbo - \\
&gkfrbm - hndlcp - hodjcq - hmdkcr \\
=\ &gjencr + gkeocp + glemcq + hnfraj + hofpak + hmfqal + \\
&irdjbn + ipdkbo + iqdlbm - cpengl - cqeogj - cremgk - \\
&alfphn - ajfqho - akfrhm - bndlip - bodjiq - bmdkir
\end{aligned}$$

$$\begin{aligned}
&[(jnr + kop + lmq) - (pnl + qoj + rmk)](aei + bfg + cdh) \\
&= [(jnr + kop + lmq) - (pnl + qoj + rmk)](gec + hfa + idb) \\
&[(jnr + kop + lmq) - (pnl + qoj + rmk)](aei + bfg + cdh) - \\
&[(jnr + kop + lmq) - (pnl + qoj + rmk)](gec + hfa + idb)
\end{aligned}$$

$$[(jnr + kop + lmq) - (pnl + qoj + rmk)][(aei + bfg + cdh) - (gec + hfa + idb)]$$

$$0.[(aei + bfg + cdh) - (gec + hfa + idb)] = 0$$

Sesuai dengan pembuktian dari proposisi yang telah dilakukan, didapatkan bahwa karakteristik dari matriks yang akan dijadikan sebagai kunci dalam proses enkripsi dan dekripsi adalah matriks yang determinannya tidak boleh sama dengan nol. Sehingga bisa dicari invers dari matriks tersebut. Adapun ciri dari mariks yang memiliki determinan sama dengan nol telah ditunjukkan dalam subbab 2.1.5 pada sifat-sifat determinan matriks. Namun, karakteristik tersebut tidak cukup untuk menjamin bahwa matriks kunci yang digunakan memiliki invers dan bisa digunakan dalam proses ini. Sesuai dengan definisi 2.10 pada subbab 2.1.4 tentang sistem reduksi modulo m. Dari definisi 2.10 dapat diaplikasikan pada penelitian kali ini. Dimana jika hasil dari determinan matriks kunci relatif prima dengan modulo 53, maka dapat dipastikan bahwa terdapat satu anggota dari determinan matriks kunci yang kongruen modulo 53.

4.2 Proses Enkripsi Pada Protokol Pertukaran Kunci Kriptografi *Diffie-Hellman* Dengan Menggunakan Algoritma *Hill Cipher*

4.2.1 Menentukan Algoritma

Pada protokol pertukaran kunci kriptografi *Diffie-Hellman* algoritma yang digunakan yaitu algoritma *Hill Cipher*. Sesuai dengan penjelasan pada subbab 2.5, nilai g pada kriptografi *Diffie-Hellman* akan digantikan oleh matriks kunci yang akan digunakan pada proses enkripsi dan dekripsi sesuai algoritma *Hill Cipher.*

Adapun algoritma *Hill Cipher* yang digunakan pada kriptografi *Diffie-Hellman* yaitu sebagai berikut :

1. Pengirim dan penerima menyepakati nilai n dan matriks g. Dimana n adalah bilangan prima, g adalah sebuah matriks yang memiliki entri-entri bilangan prima.
2. Pengirim membangkitkan bilangan prima yaitu x dan mengirim hasil perhitungan berikut kepada penerima :

$$X = g^x \ mod \ n$$

3. Penerima membangkitkan bilangan prima yaitu y dan mengirim hasil perhitungan berikut kepada pengirim :

$$Y = g^y \ mod \ n$$

4. Penerima menghitung

$$K = Y^x \ mod \ n$$

5. Pengirim menghitung

$$K' = X^y \ mod \ n$$

Jika $K = K'$ maka perhitungan yang dilakukan pengirim dan penerima adalah benar.

6. Setelah didapatkan matriks kunci yang sama antara pengirim dan penerima, selanjutnya akan dipastikan bahwa matriks kunci memiliki invers.
7. Matriks kunci yang didapatkan dari proses *Diffie-Hellman* akan digunakan pada proses enkripsi dengan mengunakan algoritma *Hill Cipher.*
8. Invers dari matriks kunci akan digunakan pada proses dekripsi dengan menggunakan algoritma *Hill Cipher.*

4.2.2 Melakukan Simulasi Proses Enkripsi

1. Matriks kunci yang telah sesuai dengan karakteristik akan digunakan melalui proses pertukaran kunci kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher*. Karena kunci yang digunakan berbentuk matriks, maka pertukaran kunci kriptografi Diffie-Hellman diaplikasikan dengan mengganti bilangan prima g dengan matriks yang entri-entrinya adalah bilangan prima.

   Contoh :

   Misalkan Sean dan Sion menyepakati $n = 53$ dan $g = \begin{bmatrix} 2 & 3 & 5 \\ 7 & 11 & 2 \\ 3 & 13 & 5 \end{bmatrix}$

   Sean memilih $x = 1$ dan menghitung :

   $$A = \begin{bmatrix} 2 & 3 & 5 \\ 7 & 11 & 2 \\ 3 & 13 & 5 \end{bmatrix}^{x} \ mod\ 53 = \begin{bmatrix} 2 & 3 & 5 \\ 7 & 11 & 2 \\ 3 & 13 & 5 \end{bmatrix}^{1} \ mod\ 53 = \begin{bmatrix} 2 & 3 & 5 \\ 7 & 11 & 2 \\ 3 & 13 & 5 \end{bmatrix}$$

   Sion memilih $y = 3$ dan menghitung :

   $$B = \begin{bmatrix} 2 & 3 & 5 \\ 7 & 11 & 2 \\ 3 & 13 & 5 \end{bmatrix}^{y} \ mod\ 53 = \begin{bmatrix} 2 & 3 & 5 \\ 7 & 11 & 2 \\ 3 & 13 & 5 \end{bmatrix}^{3} \ mod\ 53$$

   $$= \begin{bmatrix} 931 & 1797 & 613 \\ 1571 & 3010 & 1156 \\ 1941 & 3581 & 1324 \end{bmatrix} \text{mod } 53 = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix}$$

Sean menghitung kunci simetri K,

$$K = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix}^{x} \ mod\ n = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix}^{1} \ mod\ 53$$

$$= \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix}$$

Sion menghitung kunci simetri K',

$$K' = \begin{bmatrix} 2 & 3 & 5 \\ 7 & 11 & 2 \\ 3 & 13 & 5 \end{bmatrix}^{y} \ mod\ n = \begin{bmatrix} 2 & 3 & 5 \\ 7 & 11 & 2 \\ 3 & 13 & 5 \end{bmatrix}^{3} \ mod\ 53$$

$$= \begin{bmatrix} 931 & 1797 & 613 \\ 1571 & 3010 & 1156 \\ 1941 & 3581 & 1324 \end{bmatrix} \text{mod } 53 = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix}$$

Jadi, Sean dan Sion sekarang sudah mempunyai kunci enkripsi yang sama, yaitu $K' = K = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix}$

2. Menentukan plainteks yang akan digunakan dalam proses enkripsi.

   Plainteks yang digunakan adalah :

   Kekuatan algoritma Diffie-Hellman adalah pada sulitnya melakukan perhitungan logaritma diskrit

3. Mengubah plainteks ke dalam bentuk angka, yang dimulai dari 0 untuk huruf A sampai 53 untuk karakter spasi yang akan ditunjukkan dalam tabel berikut :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

a	b	c	d	e	f	g	h	i	j	k	l	m
26	27	28	29	30	31	32	33	34	35	36	37	38

n	o	p	q	r	s	t	u	v	w	x	y	z	Spasi
39	40	41	42	43	44	45	46	47	48	49	50	51	52

Tabel 4.1 Konversi Huruf ke Angka

Selanjutnya plainteks tersebut akan dikelompokkan menjadi beberapa blok. Dalam hal ini dikarenakan matriks yang berukuran 3×3, sehingga masing-masing matriks memiliki entri 3×1. Jika dalam pengelompokan plainteks tidak memiliki entri 3×1 maka kekurangan dari karakter matriks akan ditambah dengan spasi. Selanjutnya akan dilakukan proses enkripsi pesan dengan rumus :

$C \equiv KP \bmod 53$

$$\begin{bmatrix} K \\ e \\ k \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 10 \\ 30 \\ 36 \end{bmatrix} = \begin{bmatrix} 2820 \\ 3148 \\ 3102 \end{bmatrix} \bmod 53 = \begin{bmatrix} 11 \\ 21 \\ 28 \end{bmatrix} = \begin{bmatrix} L \\ V \\ c \end{bmatrix}$$

$$\begin{bmatrix} u \\ a \\ t \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 46 \\ 26 \\ 45 \end{bmatrix} = \begin{bmatrix} 3978 \\ 4591 \\ 4638 \end{bmatrix} \bmod 53 = \begin{bmatrix} 3 \\ 33 \\ 27 \end{bmatrix} = \begin{bmatrix} D \\ h \\ b \end{bmatrix}$$

$$\begin{bmatrix} a \\ n \\ Spasi \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 26 \\ 39 \\ 52 \end{bmatrix} = \begin{bmatrix} 4212 \\ 4758 \\ 4732 \end{bmatrix} \bmod 53 = \begin{bmatrix} 25 \\ 41 \\ 15 \end{bmatrix} = \begin{bmatrix} Z \\ p \\ P \end{bmatrix}$$

$$\begin{bmatrix} a \\ l \\ g \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 26 \\ 37 \\ 32 \end{bmatrix} = \begin{bmatrix} 3516 \\ 3814 \\ 3632 \end{bmatrix} \bmod 53 = \begin{bmatrix} 18 \\ 51 \\ 28 \end{bmatrix} = \begin{bmatrix} S \\ z \\ c \end{bmatrix}$$

$$\begin{bmatrix} o \\ r \\ i \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 40 \\ 43 \\ 34 \end{bmatrix} = \begin{bmatrix} 4284 \\ 4628 \\ 4378 \end{bmatrix} \bmod 53 = \begin{bmatrix} 44 \\ 17 \\ 32 \end{bmatrix} = \begin{bmatrix} s \\ R \\ g \end{bmatrix}$$

$$\begin{bmatrix} t \\ m \\ a \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 45 \\ 38 \\ 26 \end{bmatrix} = \begin{bmatrix} 3954 \\ 4244 \\ 3977 \end{bmatrix} \bmod 53 = \begin{bmatrix} 32 \\ 4 \\ 2 \end{bmatrix} = \begin{bmatrix} g \\ E \\ C \end{bmatrix}$$

$$\begin{bmatrix} spasi \\ D \\ i \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 52 \\ 3 \\ 34 \end{bmatrix} = \begin{bmatrix} 2724 \\ 3356 \\ 3574 \end{bmatrix} \bmod 53 = \begin{bmatrix} 21 \\ 17 \\ 23 \end{bmatrix} = \begin{bmatrix} V \\ R \\ X \end{bmatrix}$$

$$\begin{bmatrix} f \\ f \\ i \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 31 \\ 31 \\ 34 \end{bmatrix} = \begin{bmatrix} 3438 \\ 3818 \\ 3721 \end{bmatrix} \bmod 53 = \begin{bmatrix} 46 \\ 2 \\ 11 \end{bmatrix} = \begin{bmatrix} u \\ C \\ L \end{bmatrix}$$

$$\begin{bmatrix} e \\ H \\ e \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 30 \\ 7 \\ 30 \end{bmatrix} = \begin{bmatrix} 2136 \\ 2604 \\ 2760 \end{bmatrix} \bmod 53 = \begin{bmatrix} 16 \\ 7 \\ 4 \end{bmatrix} = \begin{bmatrix} Q \\ H \\ E \end{bmatrix}$$

$$\begin{bmatrix} l \\ l \\ m \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 37 \\ 37 \\ 38 \end{bmatrix} = \begin{bmatrix} 4026 \\ 4446 \\ 4307 \end{bmatrix} \bmod 53 = \begin{bmatrix} 51 \\ 47 \\ 14 \end{bmatrix} = \begin{bmatrix} z \\ v \\ O \end{bmatrix}$$

$$\begin{bmatrix} a \\ n \\ spasi \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 26 \\ 39 \\ 52 \end{bmatrix} = \begin{bmatrix} 4212 \\ 4758 \\ 4732 \end{bmatrix} \bmod 53 = \begin{bmatrix} 25 \\ 41 \\ 15 \end{bmatrix} = \begin{bmatrix} Z \\ p \\ P \end{bmatrix}$$

$$\begin{bmatrix} a \\ d \\ a \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 26 \\ 29 \\ 26 \end{bmatrix} = \begin{bmatrix} 2952 \\ 3220 \\ 3080 \end{bmatrix} \bmod 53 = \begin{bmatrix} 37 \\ 40 \\ 6 \end{bmatrix} = \begin{bmatrix} l \\ o \\ G \end{bmatrix}$$

$$\begin{bmatrix} l \\ a \\ h \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 37 \\ 26 \\ 33 \end{bmatrix} = \begin{bmatrix} 3348 \\ 3769 \\ 3717 \end{bmatrix} \bmod 53 = \begin{bmatrix} 9 \\ 6 \\ 7 \end{bmatrix} = \begin{bmatrix} J \\ G \\ H \end{bmatrix}$$

$$\begin{bmatrix} spasi \\ p \\ a \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 52 \\ 41 \\ 26 \end{bmatrix} = \begin{bmatrix} 4308 \\ 4608 \\ 4298 \end{bmatrix} \bmod 53 = \begin{bmatrix} 15 \\ 50 \\ 5 \end{bmatrix} = \begin{bmatrix} P \\ y \\ F \end{bmatrix}$$

$$\begin{bmatrix} d \\ a \\ spasi \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 29 \\ 26 \\ 52 \end{bmatrix} = \begin{bmatrix} 3678 \\ 4314 \\ 4441 \end{bmatrix} \bmod 53 = \begin{bmatrix} 21 \\ 21 \\ 42 \end{bmatrix} = \begin{bmatrix} V \\ V \\ q \end{bmatrix}$$

$$\begin{bmatrix} s \\ u \\ l \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 44 \\ 46 \\ 37 \end{bmatrix} = \begin{bmatrix} 4638 \\ 5019 \\ 4756 \end{bmatrix} \bmod 53 = \begin{bmatrix} 27 \\ 37 \\ 39 \end{bmatrix} = \begin{bmatrix} b \\ l \\ n \end{bmatrix}$$

$$\begin{bmatrix} i \\ t \\ n \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 34 \\ 45 \\ 39 \end{bmatrix} = \begin{bmatrix} 4350 \\ 4723 \\ 4500 \end{bmatrix} \bmod 53 = \begin{bmatrix} 4 \\ 6 \\ 48 \end{bmatrix} = \begin{bmatrix} E \\ G \\ w \end{bmatrix}$$

$$\begin{bmatrix} y \\ a \\ spasi \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 50 \\ 26 \\ 52 \end{bmatrix} = \begin{bmatrix} 4308 \\ 5028 \\ 5134 \end{bmatrix} \bmod 53 = \begin{bmatrix} 15 \\ 46 \\ 46 \end{bmatrix} = \begin{bmatrix} P \\ u \\ u \end{bmatrix}$$

$$\begin{bmatrix} m \\ e \\ l \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 38 \\ 30 \\ 37 \end{bmatrix} = \begin{bmatrix} 3690 \\ 4143 \\ 4078 \end{bmatrix} \bmod 53 = \begin{bmatrix} 33 \\ 9 \\ 50 \end{bmatrix} = \begin{bmatrix} h \\ J \\ y \end{bmatrix}$$

$$\begin{bmatrix} a \\ k \\ u \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 26 \\ 36 \\ 46 \end{bmatrix} = \begin{bmatrix} 3888 \\ 4374 \\ 4330 \end{bmatrix} \bmod 53 = \begin{bmatrix} 19 \\ 28 \\ 37 \end{bmatrix} = \begin{bmatrix} T \\ c \\ l \end{bmatrix}$$

$$\begin{bmatrix} k \\ a \\ n \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 36 \\ 26 \\ 39 \end{bmatrix} = \begin{bmatrix} 3498 \\ 3993 \\ 3996 \end{bmatrix} \bmod 53 = \begin{bmatrix} 0 \\ 18 \\ 21 \end{bmatrix} = \begin{bmatrix} A \\ S \\ V \end{bmatrix}$$

$$\begin{bmatrix} spasi \\ p \\ e \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 52 \\ 41 \\ 30 \end{bmatrix} = \begin{bmatrix} 4428 \\ 4780 \\ 4506 \end{bmatrix} \bmod 53 = \begin{bmatrix} 29 \\ 10 \\ 1 \end{bmatrix} = \begin{bmatrix} d \\ K \\ B \end{bmatrix}$$

$$\begin{bmatrix} r \\ h \\ i \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 43 \\ 33 \\ 34 \end{bmatrix} = \begin{bmatrix} 3894 \\ 4310 \\ 4177 \end{bmatrix} \bmod 53 = \begin{bmatrix} 25 \\ 17 \\ 43 \end{bmatrix} = \begin{bmatrix} Z \\ R \\ r \end{bmatrix}$$

$$\begin{bmatrix} t \\ u \\ n \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 45 \\ 46 \\ 39 \end{bmatrix} = \begin{bmatrix} 4728 \\ 5139 \\ 4893 \end{bmatrix} \bmod 53 = \begin{bmatrix} 11 \\ 51 \\ 17 \end{bmatrix} = \begin{bmatrix} L \\ z \\ R \end{bmatrix}$$

$$\begin{bmatrix} g \\ a \\ n \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 32 \\ 26 \\ 39 \end{bmatrix} = \begin{bmatrix} 3378 \\ 3857 \\ 3864 \end{bmatrix} \bmod 53 = \begin{bmatrix} 39 \\ 41 \\ 48 \end{bmatrix} = \begin{bmatrix} n \\ p \\ w \end{bmatrix}$$

$$\begin{bmatrix} spasi \\ l \\ o \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 52 \\ 37 \\ 40 \end{bmatrix} = \begin{bmatrix} 4536 \\ 5042 \\ 4906 \end{bmatrix} \bmod 53 = \begin{bmatrix} 31 \\ 7 \\ 30 \end{bmatrix} = \begin{bmatrix} f \\ H \\ e \end{bmatrix}$$

$$\begin{bmatrix} g \\ a \\ r \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 32 \\ 26 \\ 43 \end{bmatrix} = \begin{bmatrix} 3498 \\ 4029 \\ 4072 \end{bmatrix} \bmod 53 = \begin{bmatrix} 0 \\ 1 \\ 44 \end{bmatrix} = \begin{bmatrix} A \\ B \\ s \end{bmatrix}$$

$$\begin{bmatrix} i \\ t \\ m \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 34 \\ 45 \\ 38 \end{bmatrix} = \begin{bmatrix} 4320 \\ 4680 \\ 4448 \end{bmatrix} \bmod 53 = \begin{bmatrix} 27 \\ 16 \\ 49 \end{bmatrix} = \begin{bmatrix} b \\ Q \\ x \end{bmatrix}$$

$$\begin{bmatrix} a \\ spasi \\ d \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 26 \\ 52 \\ 29 \end{bmatrix} = \begin{bmatrix} 4146 \\ 4315 \\ 3926 \end{bmatrix} \bmod 53 = \begin{bmatrix} 12 \\ 22 \\ 4 \end{bmatrix} = \begin{bmatrix} M \\ W \\ E \end{bmatrix}$$

$$\begin{bmatrix} i \\ s \\ k \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 34 \\ 44 \\ 36 \end{bmatrix} = \begin{bmatrix} 4212 \\ 4552 \\ 4314 \end{bmatrix} \bmod 53 = \begin{bmatrix} 25 \\ 47 \\ 21 \end{bmatrix} = \begin{bmatrix} Z \\ v \\ V \end{bmatrix}$$

$$\begin{bmatrix} r \\ i \\ t \end{bmatrix} = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} \begin{bmatrix} 43 \\ 34 \\ 45 \end{bmatrix} = \begin{bmatrix} 4272 \\ 4825 \\ 4779 \end{bmatrix} \bmod 53 = \begin{bmatrix} 32 \\ 2 \\ 9 \end{bmatrix} = \begin{bmatrix} g \\ C \\ J \end{bmatrix}$$

4. Hasil dari proses enkripsi dikonversi ke dalam bentuk huruf. Berikut adalah cipherteks yang dihasilkan dari proses enkripsi :

   LVcDhbhZpPSzcsRggECVRXuCLQHEzvOZpPloGJGHPyFVVqblnEGwP

   uuhJyTclASVdKBZRrLZRnpwfHeABsbQxMWEZvVgCJ

4.3 Proses Dekripsi Pada Protokol Pertukaran Kunci Kriptografi *Diffie-Hellman* dengan Menggunakan Algoritma *Hill Cipher*

4.3.1 Pembuktian fungsi dekripsi

Sebelum melakukan dekripsi pada cipherteks yang telah diperoleh pada proses enkripsi, terlebih dahulu akan diberikan pembuktian tentang fungsi dekripsi. Adapun fungsi dekripsi algoritma *Hill Cipher* yang digunakan dalam kriptografi *Diffie-Hellman* yaitu :

$C \equiv KP \bmod 53$

dengan : C = cipherteks yang dihasilkan dari proses enkripsi

K = kunci matriks yang digunakan dalam proses enkripsi dan

dekripsi

P = Plainteks yang akan diperoleh dari proses enkripsi

Berikut adalah pembuktian fungsi dekripsi :

$\mathrm{C} \equiv \mathrm{KP} \bmod 53$	(definisi kongruensi)
$\Leftrightarrow \mathrm{KP} \equiv \mathrm{C} \bmod 53$	(relasi kongruensi, simetris)
$\Leftrightarrow \mathrm{K}^{-1}\mathrm{KP} \equiv \mathrm{K}^{-1}\mathrm{C} \bmod 53$	(kedua ruas dikalikan dengan K^{-1})
$\Leftrightarrow \mathrm{IP} \equiv \mathrm{K}^{-1}\mathrm{C} \bmod 53$	(definisi invers dari suatu matriks)
$\Leftrightarrow \mathrm{P} \equiv \mathrm{K}^{-1}\mathrm{C} \bmod 53$	(sifat matriks satuan, identitas perkalian)

∴ Terbukti

4.3.2 Melakukan Simulasi Proses Dekripsi

1. Mencari invers dari matriks kunci.

   Setelah Sean dan Sion memiliki matriks kunci yang digunakan untuk proses enkripsi, selanjutnya akan dicari invers dari matriks kunci tersebut.

$$K = \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix}, \det = 164232 - 165144 = -912 \; mod \; 53$$

$$= 42 \; mod \; 53 = 42$$

   Invers matriks $K = |K|^{-1} \; adj \; (K)$

$$\text{Adjoin } K = \begin{pmatrix} \begin{bmatrix} 42 & 43 \\ 30 & 52 \end{bmatrix} - \begin{bmatrix} 34 & 43 \\ 33 & 52 \end{bmatrix} \begin{bmatrix} 34 & 42 \\ 33 & 30 \end{bmatrix} \\ - \begin{bmatrix} 48 & 30 \\ 30 & 52 \end{bmatrix} \begin{bmatrix} 30 & 30 \\ 33 & 52 \end{bmatrix} - \begin{bmatrix} 30 & 48 \\ 33 & 30 \end{bmatrix} \\ \begin{bmatrix} 48 & 30 \\ 42 & 43 \end{bmatrix} - \begin{bmatrix} 30 & 30 \\ 34 & 43 \end{bmatrix} \begin{bmatrix} 30 & 48 \\ 34 & 42 \end{bmatrix} \end{pmatrix}$$

$$= \begin{bmatrix} 894 & -349 & -366 \\ -1596 & 570 & 684 \\ 804 & -270 & -372 \end{bmatrix} = \begin{bmatrix} 894 & -349 & -366 \\ -1596 & 570 & 684 \\ 804 & -270 & -372 \end{bmatrix}^{T}$$

$$= \begin{bmatrix} 894 & 47 & 804 \\ 22 & 570 & 48 \\ 5 & 684 & 52 \end{bmatrix}$$

Invers matriks $K = K^{-1} = 42^{-1}\ mod\ 53 \begin{bmatrix} 894 & 47 & 804 \\ 22 & 570 & 48 \\ 5 & 684 & 52 \end{bmatrix}$

$$= 24 \begin{bmatrix} 894 & 47 & 804 \\ 22 & 570 & 48 \\ 5 & 684 & 52 \end{bmatrix} mod\ 53$$

$$= \begin{bmatrix} 21456 & 1128 & 19296 \\ 528 & 13680 & 1152 \\ 120 & 16416 & 1248 \end{bmatrix} mod\ 53$$

$$= \begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}$$

Bukti :

$$\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \begin{bmatrix} 30 & 48 & 30 \\ 34 & 42 & 43 \\ 33 & 30 & 52 \end{bmatrix} = \begin{bmatrix} 1962 & 2862 & 2173 \\ 3021 & 3870 & 3816 \\ 2703 & 3180 & 3605 \end{bmatrix} mod\ 53$$

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

2. Melakukan proses dekripsi dengan terlebih dahulu mengkonversikan huruf ke bentuk angka.

   Rumus Dekripsi : $P \equiv K^{-1}C \bmod 53$

$$\begin{bmatrix} L \\ V \\ c \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \right] \begin{bmatrix} 11 \\ 21 \\ 28 \end{bmatrix} = \begin{bmatrix} 911 \\ 1779 \\ 1785 \end{bmatrix} \bmod 53 = \begin{bmatrix} 10 \\ 30 \\ 36 \end{bmatrix} = \begin{bmatrix} K \\ e \\ k \end{bmatrix}$$

$$\begin{bmatrix} D \\ h \\ b \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \right] \begin{bmatrix} 3 \\ 33 \\ 27 \end{bmatrix} = \begin{bmatrix} 735 \\ 1404 \\ 2112 \end{bmatrix} \bmod 53 = \begin{bmatrix} 46 \\ 26 \\ 45 \end{bmatrix} = \begin{bmatrix} u \\ a \\ t \end{bmatrix}$$

$$\begin{bmatrix} Z \\ p \\ P \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \right] \begin{bmatrix} 25 \\ 41 \\ 15 \end{bmatrix} = \begin{bmatrix} 1775 \\ 2106 \\ 2384 \end{bmatrix} \bmod 53 = \begin{bmatrix} 26 \\ 39 \\ 52 \end{bmatrix} = \begin{bmatrix} a \\ n \\ spasi \end{bmatrix}$$

$$\begin{bmatrix} S \\ z \\ c \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 18 \\ 51 \\ 28 \end{bmatrix} = \begin{bmatrix} 1669 \\ 2316 \\ 3053 \end{bmatrix} \bmod 53 = \begin{bmatrix} 26 \\ 37 \\ 32 \end{bmatrix} = \begin{bmatrix} a \\ l \\ g \end{bmatrix}$$

$$\begin{bmatrix} s \\ R \\ g \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 44 \\ 17 \\ 32 \end{bmatrix} = \begin{bmatrix} 2319 \\ 3594 \\ 2207 \end{bmatrix} \bmod 53 = \begin{bmatrix} 40 \\ 43 \\ 34 \end{bmatrix} = \begin{bmatrix} o \\ r \\ i \end{bmatrix}$$

$$\begin{bmatrix} g \\ E \\ C \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 32 \\ 4 \\ 2 \end{bmatrix} = \begin{bmatrix} 1476 \\ 1734 \\ 662 \end{bmatrix} \bmod 53 = \begin{bmatrix} 45 \\ 38 \\ 26 \end{bmatrix} = \begin{bmatrix} t \\ m \\ a \end{bmatrix}$$

$$\begin{bmatrix} V \\ R \\ X \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 21 \\ 17 \\ 23 \end{bmatrix} = \begin{bmatrix} 1271 \\ 2070 \\ 1624 \end{bmatrix} \bmod 53 = \begin{bmatrix} 52 \\ 3 \\ 34 \end{bmatrix} = \begin{bmatrix} spasi \\ D \\ i \end{bmatrix}$$

$$\begin{bmatrix} u \\ C \\ L \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 46 \\ 2 \\ 11 \end{bmatrix} = \begin{bmatrix} 2098 \\ 2787 \\ 1041 \end{bmatrix} \bmod 53 = \begin{bmatrix} 31 \\ 31 \\ 34 \end{bmatrix} = \begin{bmatrix} f \\ f \\ i \end{bmatrix}$$

$$\begin{bmatrix} Q \\ H \\ E \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 16 \\ 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 825 \\ 1014 \\ 613 \end{bmatrix} \bmod 53 = \begin{bmatrix} 30 \\ 7 \\ 30 \end{bmatrix} = \begin{bmatrix} e \\ H \\ e \end{bmatrix}$$

$$\begin{bmatrix} z \\ v \\ O \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 51 \\ 47 \\ 14 \end{bmatrix} = \begin{bmatrix} 3005 \\ 3429 \\ 2953 \end{bmatrix} \bmod 53 = \begin{bmatrix} 37 \\ 37 \\ 38 \end{bmatrix} = \begin{bmatrix} l \\ l \\ m \end{bmatrix}$$

$$\begin{bmatrix} Z \\ p \\ P \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 25 \\ 41 \\ 15 \end{bmatrix} = \begin{bmatrix} 1775 \\ 2106 \\ 2384 \end{bmatrix} \bmod 53 = \begin{bmatrix} 26 \\ 39 \\ 52 \end{bmatrix} = \begin{bmatrix} a \\ n \\ spasi \end{bmatrix}$$

$$\begin{bmatrix} l \\ o \\ G \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 37 \\ 40 \\ 6 \end{bmatrix} = \begin{bmatrix} 2252 \\ 2361 \\ 2252 \end{bmatrix} \bmod 53 = \begin{bmatrix} 26 \\ 29 \\ 26 \end{bmatrix} = \begin{bmatrix} a \\ d \\ a \end{bmatrix}$$

$$\begin{bmatrix} J \\ G \\ H \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 9 \\ 6 \\ 7 \end{bmatrix} = \begin{bmatrix} 514 \\ 768 \\ 563 \end{bmatrix} \bmod 53 = \begin{bmatrix} 37 \\ 26 \\ 33 \end{bmatrix} = \begin{bmatrix} l \\ a \\ h \end{bmatrix}$$

$$\begin{bmatrix} P \\ y \\ F \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 15 \\ 50 \\ 5 \end{bmatrix} = \begin{bmatrix} 1430 \\ 1260 \\ 2305 \end{bmatrix} \bmod 53 = \begin{bmatrix} 52 \\ 41 \\ 26 \end{bmatrix} = \begin{bmatrix} spasi \\ p \\ a \end{bmatrix}$$

$$\begin{bmatrix} V \\ V \\ q \end{bmatrix} = \begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \begin{bmatrix} 21 \\ 21 \\ 42 \end{bmatrix} = \begin{bmatrix} 1407 \\ 2835 \\ 2331 \end{bmatrix} \bmod 53 = \begin{bmatrix} 29 \\ 26 \\ 52 \end{bmatrix} = \begin{bmatrix} d \\ a \\ spasi \end{bmatrix}$$

$$\begin{bmatrix} b \\ l \\ n \end{bmatrix} = \begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \begin{bmatrix} 27 \\ 37 \\ 39 \end{bmatrix} = \begin{bmatrix} 1899 \\ 3120 \\ 2952 \end{bmatrix} \bmod 53 = \begin{bmatrix} 44 \\ 46 \\ 37 \end{bmatrix} = \begin{bmatrix} s \\ u \\ l \end{bmatrix}$$

$$\begin{bmatrix} E \\ G \\ w \end{bmatrix} = \begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \begin{bmatrix} 4 \\ 6 \\ 48 \end{bmatrix} = \begin{bmatrix} 458 \\ 2112 \\ 1682 \end{bmatrix} \bmod 53 = \begin{bmatrix} 34 \\ 45 \\ 39 \end{bmatrix} = \begin{bmatrix} i \\ t \\ n \end{bmatrix}$$

$$\begin{bmatrix} P \\ u \\ u \end{bmatrix} = \begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \begin{bmatrix} 15 \\ 46 \\ 46 \end{bmatrix} = \begin{bmatrix} 1534 \\ 2835 \\ 3338 \end{bmatrix} \bmod 53 = \begin{bmatrix} 50 \\ 26 \\ 52 \end{bmatrix} = \begin{bmatrix} y \\ a \\ spasi \end{bmatrix}$$

$$\begin{bmatrix} h \\ J \\ y \end{bmatrix} = \begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \begin{bmatrix} 33 \\ 9 \\ 50 \end{bmatrix} = \begin{bmatrix} 1787 \\ 3687 \\ 2263 \end{bmatrix} \bmod 53 = \begin{bmatrix} 38 \\ 30 \\ 37 \end{bmatrix} = \begin{bmatrix} m \\ e \\ l \end{bmatrix}$$

$$\begin{bmatrix} T \\ c \\ l \end{bmatrix} = \begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \begin{bmatrix} 19 \\ 28 \\ 37 \end{bmatrix} = \begin{bmatrix} 1404 \\ 2580 \\ 2431 \end{bmatrix} \bmod 53 = \begin{bmatrix} 26 \\ 36 \\ 46 \end{bmatrix} = \begin{bmatrix} a \\ k \\ u \end{bmatrix}$$

$$\begin{bmatrix} A \\ S \\ V \end{bmatrix} = \begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \begin{bmatrix} 0 \\ 18 \\ 21 \end{bmatrix} = \begin{bmatrix} 354 \\ 927 \\ 1311 \end{bmatrix} \bmod 53 = \begin{bmatrix} 36 \\ 26 \\ 39 \end{bmatrix} = \begin{bmatrix} k \\ a \\ n \end{bmatrix}$$

$$\begin{bmatrix} d \\ K \\ B \end{bmatrix} = \begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \begin{bmatrix} 29 \\ 10 \\ 1 \end{bmatrix} = \begin{bmatrix} 1430 \\ 1578 \\ 825 \end{bmatrix} \bmod 53 = \begin{bmatrix} 52 \\ 41 \\ 30 \end{bmatrix} = \begin{bmatrix} spasi \\ p \\ e \end{bmatrix}$$

$$\begin{bmatrix} Z \\ R \\ r \end{bmatrix} = \begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \begin{bmatrix} 25 \\ 17 \\ 43 \end{bmatrix} = \begin{bmatrix} 1527 \\ 3054 \\ 2260 \end{bmatrix} \bmod 53 = \begin{bmatrix} 43 \\ 33 \\ 34 \end{bmatrix} = \begin{bmatrix} r \\ h \\ i \end{bmatrix}$$

$$\begin{bmatrix} L \\ z \\ R \end{bmatrix} = \begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \begin{bmatrix} 11 \\ 51 \\ 17 \end{bmatrix} = \begin{bmatrix} 1317 \\ 1530 \\ 2636 \end{bmatrix} \bmod 53 = \begin{bmatrix} 45 \\ 46 \\ 39 \end{bmatrix} = \begin{bmatrix} t \\ u \\ n \end{bmatrix}$$

$$\begin{bmatrix} n \\ p \\ w \end{bmatrix} = \begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix} \begin{bmatrix} 39 \\ 41 \\ 48 \end{bmatrix} = \begin{bmatrix} 2523 \\ 4107 \\ 3537 \end{bmatrix} \bmod 53 = \begin{bmatrix} 32 \\ 26 \\ 39 \end{bmatrix} = \begin{bmatrix} g \\ a \\ n \end{bmatrix}$$

$$\begin{bmatrix} f \\ H \\ e \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 31 \\ 7 \\ 30 \end{bmatrix} = \begin{bmatrix} 1589 \\ 2793 \\ 1577 \end{bmatrix} \bmod 53 = \begin{bmatrix} 52 \\ 37 \\ 40 \end{bmatrix} = \begin{bmatrix} spasi \\ l \\ o \end{bmatrix}$$

$$\begin{bmatrix} A \\ B \\ s \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 0 \\ 1 \\ 44 \end{bmatrix} = \begin{bmatrix} 191 \\ 1722 \\ 1315 \end{bmatrix} \bmod 53 = \begin{bmatrix} 32 \\ 26 \\ 43 \end{bmatrix} = \begin{bmatrix} g \\ a \\ r \end{bmatrix}$$

$$\begin{bmatrix} b \\ Q \\ x \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 27 \\ 16 \\ 49 \end{bmatrix} = \begin{bmatrix} 1624 \\ 3384 \\ 2423 \end{bmatrix} \bmod 53 = \begin{bmatrix} 34 \\ 45 \\ 38 \end{bmatrix} = \begin{bmatrix} i \\ t \\ m \end{bmatrix}$$

$$\begin{bmatrix} M \\ W \\ E \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 12 \\ 22 \\ 4 \end{bmatrix} = \begin{bmatrix} 874 \\ 900 \\ 1142 \end{bmatrix} \bmod 53 = \begin{bmatrix} 26 \\ 52 \\ 29 \end{bmatrix} = \begin{bmatrix} a \\ d \\ i \end{bmatrix}$$

$$\begin{bmatrix} Z \\ v \\ V \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 25 \\ 47 \\ 21 \end{bmatrix} = \begin{bmatrix} 1889 \\ 2376 \\ 2792 \end{bmatrix} \bmod 53 = \begin{bmatrix} 34 \\ 44 \\ 36 \end{bmatrix} = \begin{bmatrix} s \\ k \\ r \end{bmatrix}$$

$$\begin{bmatrix} g \\ C \\ J \end{bmatrix} = \left[\begin{bmatrix} 44 & 15 & 4 \\ 51 & 6 & 39 \\ 14 & 39 & 29 \end{bmatrix}\right]\begin{bmatrix} 32 \\ 2 \\ 9 \end{bmatrix} = \begin{bmatrix} 1474 \\ 1995 \\ 787 \end{bmatrix} \bmod 53 = \begin{bmatrix} 43 \\ 34 \\ 45 \end{bmatrix} = \begin{bmatrix} i \\ t \\ spasi \end{bmatrix}$$

3. Jika proses dekripsi yang dilakukan benar, maka cipherteks akan Kembali ke bentuk plainteks.

   Adapun plainteks yang didapatkan dari proses dekripsi tersebut adalah:

   Kekuatan algoritma Diffie-Hellman adalah pada sulitnya melakukan perhitungan logaritma diskrit

4.4 Amanah dalam Kriptografi

Amanah adalah sesuatu yang wajib dijaga. Kriptografi sama halnya dengan amanah. Kriptografi berkaitan dengan proses enkripsi dan dekripsi pesan. Dimana pesan antara pengirim dan penerima harus benar-benar dijaga kerahasiaannya. Rahasia yang dimaksud berarti tidak boleh diketahui oleh orang lain.

Pada proses enkripsi, pesan akan diubah menjadi cipherteks. Meskipun cipherteks tidak mudah dibaca, bukan berarti kerahasiaannya tidak dijaga. Karena dalam kriptografi, cipherteks bisa diterjemahkan melalui proses kriptanalis. Menjaga kerahasiaan cipherteks, kunci yang digunakan, maupun komponen lain yang berperan harus tetap dilakukan hingga pesan yang dikirim bisa tersampaikan dengan baik kepada penerima. Jika pesan yang dikirimkan diketahui oleh selain pengirim dan penerima maka amanah yang ada di dalamnya tidak dapat dijaga.

Seperti telah dijelaskan dalam subbab 2.2, banyak ayat-ayat Al-Qur'an yang menjelaskan tentang Amanah, salah satunya sebagaimana perintah Allah untuk menyampaikan amanah kepada yang berhak menerimanya yang disebutkan dalam Al-Qur'an surat An-Nisa' ayat 58. Menjaga kerahasiaan data atau informasi sampai diterima oleh mereka yang berhak harus dilaksanakan dengan sebaik-baiknya. Agar tidak ada dampak negatif yang ditimbulkan dari kebocoran data yang kemudian akan disalahgunakan pada hal-hal yang merugikan banyak orang.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan dan pembahasan yang dijelaskan dapat diambil tiga kesimpulan :

1. Karakteristik matriks yang efektif digunakan dalam pertukaran kunci kriptografi *Diffie-Hellman* dengan modulo 53 adalah matriks non singular dimana determinan dari matriks tersebut harus relatif prima dengan modulo 53.
2. Proses enkripsi kriptografi *Diffie-Hellman* dengan menggunakan algoritma *Hill Cipher* pertama-tama dilakukan dengan mengganti bilangan prima g pada algoritma *Diffie-Hellman* dengan matriks 3×3 yang memiliki entri bilangan prima. Hasil dari perhitungan dengan menggunakan algoritma *Diffie-Hellman* adalah matriks kunci K yang digunakan dalam proses enkripsi dan dekripsi sesuai dengan algoritma *Hill Cipher*.
3. Pada proses dekripsi kriptografi Diffie-Hellman dengan menggunakan algoritma Hill Cipher, invers matriks kunci K yang telah didapatkan pada pembahasan rumusan masalah ke-2 digunakan sebagai matriks kunci untuk proses dekripsi sesuai dengan algoritma Hill Cipher. Hasil dari proses dekripsi ini adalah cipherteks yang kembali kedalam bentuk plainteks. Adapun fungsi dekripsi algoritma *Hill Cipher* yang digunakan dalam kriptografi *Diffie-Hellman* yaitu :

   $\mathrm{C} \equiv \mathrm{KP} \bmod 53$

5.2 Saran

Untuk penelitian selanjutnya, dapat menggunakan algoritma lain sehingga bisa mengetahui algoritma mana yang lebih aman digunakan dalam mengirimkan pesan. Selain itu, bisa juga menggunakan ukuran matriks kunci yang lebih besar dari 3×3 dan karakter ASCII agar kunci yang digunakan dan proses enkripsi dekripsi yang dilakukan lebih bervariasi.

DAFTAR PUSTAKA

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

Andari, A. (2017). *Aljabar Linear Elementer*. Malang: UB Press.

Andika, T., Taquyuddin, M., & Admizal, I. (2020). Amanah Dan Khianat Dalam Al_Qur"An Menurut Quraish Shihab. *Jurnal Ilmu Al-Quran Dan Tafsir (5), 02*, 183-184.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi.* Yogyakarta: Andi.

Basyir, H. (2011). *At-Tafsir Al-Muyassar*. Solo: An-Naba'.

Fatimatuzzahro'. (2021). *Penerapan Kriptografi Hibrida Menggunakan Algoritma Hill Cipher dan Rivest Shamir Adleman (RSA) Pada Pengamanan Pesan Teks.* Malang: UIN Malang.

Febri Dwinata Yonathan, Helfi Nasution, Heri Priyanto. (2021). Aplikasi Pengaman Dokumen Digital Menggunakan Algoritma Kriptografi Hybrid dan Algoritma Kompresi Huffman. *Jurnal Edukasi dan Penelitian Informatika,* 183.

Ginting, V. S. (2020). Penerapan Algoritma Vigenere Cipher Dan Hill Cipher Mengggunakan Satuan Massa. *Jurnal Teknologi Informasi, 4*(2), 242.

'Imrona, M. (2009). *Aljabar Linear Dasar.* Jakarta: Penerbit Erlangga.

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

Khairani, T., Santoso, K. A., & Kamsyakawuni, A. (2021). Pengkodean Monoalphabetic Menggunakan Affine Cipher dengan Kunci Diffie-Hellman. *PRISMA, Prosiding Seminar Nasional Matematika , 4*, 553-559.

Mulyadi. (2019). Aplikasi Kriptografi Pesan Teks Menggunakan Algoritma Advanced Encryption Standard 256 Bit(Aes-256) Dan Diffie-Hellman. *Jurnal Sistem Informasi*, 29.

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

Pratama, H. J., Ali, E. P., Nurvia, M., & Harahap, E. (2021). Aplikasi Penjumlahan dan Perkalian Matriks Pada Microsoft Excel. *Matematika*, 18.

Sadikin, R. (2012). *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java.* Yogyakarta: C. V Andi Offset.

Sembiring, M. B. (2015). Elliptic Curve Cryptography (Ecc) Pada Proses Pertukaran Kunci Publik Diffie-Hellman. *Vol IV*(1), 28.

Yusfrizal. (2019). Rancang Bangun Aplikasi Ktiptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android. *Jurnal Teknik Informatika Kaputama (JTIK)*, 30.

RIWAYAT HIDUP

Sri Widati Eka Kapti, lahir di kabupaten Gresik pada tanggal 18 Desember 1999, biasa dipanggil Eka. Penulis tinggal di desa Cerme Lor, kecamatan Cerme, kabupaten Gresik. Anak satu-satunya dari pasangan bapak Santoso dan Ibu Jumaroh.

Pendidikan dasar ditempuh di SD YPI Darussalam (2006 - 2012), kemudian melanjutkan pendidikan menengah pertama di SMPN 1 Cerme (2012 - 2015), kemudian Pendidikan menengah atas di SMAN 1 Cerme (2015 - 2018) dan tahun 2018 penulis mulai menempuh kuliah di Universitas Islam Negeri Maulana Malik Ibrahim Malang mengambil program studi matematika.

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	: Sri Widati Eka Kapti
NIM	: 18610010
Fakultas / Program Studi	: Sains dan Teknologi / Matematika
Judul Skripsi	: Proses Pertukaran Kunci Kriptografi *Diffie-Hellman* Dengan Menggunakan Algoritma *Hill Cipher*
Pembimbing I	: Muhammad Khudzaifah, M.Si
Pembimbing II	: Erna Herawati, M.Pd

No	Tanggal	Hal	Tanda Tangan
1.	20 Januari 2022	Konsultasi Bab I	1.
2.	25 Januari 2022	Konsultasi Revisi Bab I	2.
3.	15 Februari 2022	Konsultasi Bab II dan III	3.
4.	13 Maret 2022	Konsultasi Revisi Bab II dan III	4.
5.	14 Maret 2022	Konsultasi Kajian Agama	5.
6.	16 April 2022	ACC untuk Seminar Proposal	6.
7.	20 April 2022	Konsultasi Bab IV dan V	7.
8.	5 Juni 2022	Konsultasi Revisi Bab IV dan V	8.
9.	8 September 2022	Konsultasi Kajian Agama	9.
10.	23 September 2022	ACC untuk Seminar Hasil	10.
11.	14 Oktober 2022	ACC Matriks Revisi Seminar Hasil	11.
12.	31 Oktober 2022	ACC untuk Sidang Skripsi	12.
13.	2 November 2022	Konsultasi Revisi Kajian Agama	13.
14.	9 Desember 2022	Konsultasi Abstrak Arab	14.
15.	10 Desember 2022	Konsultasi Revisi Bab IV	15.
16.	14 Desember 2022	ACC Keseluruhan	16.

Malang, 14 Desember 2022
Mengetahui,
Ketua Program Studi Matematika

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