PENERAPAN KRIPTOGRAFI HIBRIDA MENGGUNAKAN ALGORITMA *HILL CIPHER* DAN *RIVEST SHAMIR ADLEMAN* (RSA) PADA PENGAMANAN PESAN TEKS

SKRIPSI

OLEH
FATIMATUZZAHRO'
NIM. 16610100

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2021

PENERAPAN KRIPTOGRAFI HIBRIDA MENGGUNAKAN ALGORITMA *HILL CIPHER* DAN *RIVEST SHAMIR ADLEMAN* (RSA) PADA PENGAMANAN PESAN TEKS

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
FATIMATUZZAHRO'
NIM. 16610100

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2021

PENERAPAN KRIPTOGRAFI HIBRIDA MENGGUNAKAN ALGORITMA *HILL CIPHER* DAN RIVEST SHAMIR ADLEMAN (*RSA*) PADA PENGAMANAN PESAN TEKS

SKRIPSI

Oleh
FATIMATUZZAHRO'
NIM. 16610100

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 02 November 2021

Pembimbing I,	Pembimbing II,
Muhammad Khudzaifah, M. Si.	Juhari, M. Si.
NIDT. 19900511 20160801 1 057	NIDT. 19840209 20160801 1 055

Mengetahui,
Ketua Program Studi Matematika

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

PENERAPAN KRIPTOGRAFI HIBRIDA MENGGUNAKAN ALGORITMA *HILL CIPHER* DAN *RIVEST SHAMIR ADLEMAN* (RSA) PADA PENGAMANAN PESAN TEKS

SKRIPSI

Oleh
FATIMATUZZAHRO'
NIM. 16610100

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S, Mat)
Tanggal 18 November 2021

Penguji Utama	: Drs. H. Imam Sujarwo, M. Pd	.....
Ketua Penguji	: M. Nafie Jauhari, M. Si	.....
Sekretaris Penguji	: Muhammad Khudzaifah, M. Si	.....
Anggota Penguji	: Juhari, M. Si	.....

Mengetahui,
Ketua Program Studi Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama	: Fatimatuzzahro'
NIM	: 16610100
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi
Judul Penelitian	: Penerapan Kriptografi Hibrida Menggunakan Algoritma *Hill Cipher* Dan *Rivest Shamir Adleman* (RSA) Pada Pengamanan Pesan Teks

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

Malang, 01 November 2021
Yang membuat pernyataan,

Fatimatuzzahro'
NIM. 16610100

MOTO

“Allah memberi jalan atau cara yang berbeda kepada manusia untuk tujuan yang sama, jadi selalu syukuri apa yang telah kamu miliki**”**

PERSEMBAHAN

Skripsi ini penulis sembahkan untuk:

Kedua orang tua penulis ayah Inzrok dan ibu Lilis Eko Styowati, serta keluarga yang selalu memberikan doa, dukungan secara materil maupun non materil.

Teman-teman yang selalu memberikan semangan dan motivasi kepada penulis.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah Swt. yang telah melimpahkan rahmat, taufik, serta hidayah-Nya sehingga penulis mampu menyelesaikan penyusunan skripsi sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang Matematika Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Sholawat serta salam semoga senantiasa tercurahkan kepada junjungan nabi Muhammad SAW. yang telah membimbing manusia menuju jalan yang terang.

Dalam proses penyusunan skripsi ini, penulis banyak mendapat bimbingan dan arahan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih yang sebesar-besarnya dan penghargaan setinggi-tingginya terutama kepada:

1. Muhammad Khudzaifah, M. Si, selaku dosen pembimbing I yang telah memberikan solusi mengenai permasalahan dalam skripsi ini serta meluangkan waktunya untuk memberikan bimbingan dan arahan sehingga penulis dapat menyelesaikan skripsi ini dengan baik.
2. Juhari, M. Si, selaku dosen pembimbing II yang telah memberikan bimbingan, arahan, dan berbagi ilmu kepada penulis.
3. Dr. H. Imam Sujarwo, M. Pd, selaku penguji utama yang telah membantu dalam menyelesaikan tugas akhir.
4. M. Nafie jauhari, M. Si, selaku ketua penguji yang telah membantu dalam menyelesaikan tugas akhir.

Penulis berharap semoga skripsi ini dapat bermanfaat bagi pembaca dan penulis dalam menambah wawasan.

Wassalamu'alaikum Wr. Wb.

Malang, 10 Juni 2021

Penulis

DAFTAR ISI

DAFTAR GAMBAR

ABSTRAK

Fatimatuzzahro'. 2021. **Penerapan Kriptografi Hibrida menggunakan Algoritma *Hill Cipher* dan *Rivest Shamir Adleman* (RSA) pada Pengamanan Pesan Teks Melalui Contoh "berakhirnya masa pandemic COVID19".** Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing (I): M. Khudzaifah, M. Si, Pembimbing (II): Juhari, M. Si.

Kata Kunci: Kriptografi Hibrida, *Hill Cipher, Rivest Shamir Adleman* (RSA).

Penyandian pesan dilakukan untuk mengamankan pesan dari pihak yang tidak berhak mengetahui isi pesan. Penyandian pesan menggunakan kriptografi hibrida merupakan salah satu cara untuk mengamankan pesan teks. Kriptografi hibrida merupakan penggabungan dari dua algoritma yaitu algoritma simetri dengan metode *hill cipher* dan algoritma asimetri dengan metode *Rivest Shamir Adleman* (RSA). Metode *hill cipher* digunakan untuk mengamankan pesan teks dengan kekuatannya terletak pada kerahasiaan kunci pesan, sehingga untuk menjaga kerahasiaannya, kunci pesan diamankan dengan metode RSA yang kekuatannya terletak pada sulitnya pemfaktoran bilangan bulat menjadi dua bilangan prima. Penggabungan tersebut dapat menyulitkan penjahat untuk mendapatkakn pesan asli. Tujuan dari penelitian ini adalah untuk mengetahui proses dan hasil dari enkripsi dan dekripsi algoritma hibrida dengan metode *hill cipher* dan RSA sehingga dapat meningkatkan pengamanan yang lebih baik. Penelitian dilakukan dengan membuat pembangkit pasangan kunci oleh penerima pesan dengan menentukan sebarang nilai p dan q yang relatif prima sehingga didapatkan pasangan kunci publik (e,n) dan pasangan kunci privat (d,n). Kemudian pengirim pesan membuat sampel berupa pesan teks atau plainteks yang dikonversikan dalam bentuk ASCII dan menentukan kunci matriks yang akan dihitung dengan rumus *hill cipher*. Selanjutnya, pasangan kunci publik yang diberikan oleh penerima pesan digunakan untuk mengenkripsi kunci pesan menggunakan metode RSA. Setelah pesan dikirimkan, penerima pesan harus menemukan kunci asli menggunakan pasangan kunci privat untuk mendekripsi kunci pesan menggunakan metode RSA. Selanjutnya, penerima pesan harus mencari invers kunci pesan untuk mendapatkan pesan asli yang dihitung dengan rumus *hill cipher*, kemudian dikembalikan dalam bentuk teks menggunakan kode ASCII. Hasil penelitian dari penggabungan metode *hill cipher* dan RSA berupa peningkatan keamanan pesan dengan mengenkripsi keamanan *hill cipher* yang terletak pada kunci matriks menggunakan RSA yang memiliki kunci enkripsi dan dekripsi berbeda.

ABSTRACT

Fatimatuzzahro'. 2021. **Applying the Hybrid Cryptography using Hill Cipher and Rivest Shamir Adleman (RSA) Algorithm for Text Message Security**. Thesis. Study Program of Mathematics, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University Malang. Supervisor (I): Muhammad Khudzaifah, M. Si, Supervisor (II): Juhari, M. Si.

Keywords: Hybrid Cryptography, Hill Cipher, Rivest Shamir Adleman (RSA).

Message encoding is to secure messages from parties who are not entitled to know the contents of the message. Encrypting messages using hybrid cryptography is one way to secure text messages. Hybrid cryptography is a combination of two algorithms, namely the symmetric algorithm with the Hill cipher method and the asymmetric algorithm with the Rivest Shamir Adleman (RSA) method. The Hill cipher method is used to secure text messages with its strength lies in the confidentiality of the message key, so to maintain the confidentiality, the message key is secured by the RSA method whose strength lies in the difficulty of factoring integers into two prime numbers. The combination can make it difficult for criminals to get to the original message. The purposes of the research were to determine the process of encryption and decryption of hybrid algorithms with Hill cipher and RSA methods so as to improve better security. The research was conducted by generating a key pair generator by the recipient of the message by determining any relatively prime p and q values in order to obtain a public key pair (e, n) and a private key pair (d, n). Then the sender of the message made a sample in the form of a text message or plaintext which was converted in ASCII form and determined the key matrix to be calculated by the Hill cipher formula. Next, the public key pair that was provided by the recipient of the message was used to encrypt the message key using the RSA method. After the message was sent, the recipient of the message must find the original key using the private key pair to decrypt the message key using the RSA method. Next, the recipient of the message must look for the inverse of the message key to get the original message which was calculated by the hill cipher formula, then returned in text form using the ASCII code. The results of the combination of the Hill cipher and RSA methods were in the form of increasing message security by encrypting the security of the hill cipher located in the matrix key by using RSA which had different encryption and decryption keys.

مستخلص البحث

فاطمة الزهرة. 2021. **تطبيق التشفير الهجين *(Kriptografi Hibrida)* باستخدام خوارزمية*Hill Cipher* و *Rivest Shamir Adleman* لأمان الرسائل النصية**. بحث جامعي. قسم دراسة علم الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف الأول: محمد خذيفة، الماجستير، المشرف الثاني: جوحاري، الماجستير.

الكلمات المفتاحية: التشفير الهجين، *Hill Cipher* ، *Rivest Shamir Adleman*

تم تشفير الرسائل لتأمين الرسائل من الأطراف التي لا يحق لها معرفة محتويات الرسالة. يعد تشفير الرسائل باستخدام التشفير المختلط إحدى الطرق لتأمين الرسائل النصية. التشفير الهجين هو مزيج من خوارزميتين، وهما الخوارزمية المتماثلة باستخدام طريقة *hill cipher* والخوارزمية غير المتماثلة باستخدام طريقة *Rivest Shamir Adleman* . تُستخدم هذه طريقة *hill cipher* لتأمين الرسائل النصية حيث تكون قوتها في سرية مفتاح الرسائل، لذلك للتحفيظ على سريتها، يتم تأمين مفتاح الرسائل بواسطة طريقة *Rivest Shamir Adleman* التي تكون قوتها في صعوبة تحليل الأعداد الصحيحة إلى رقمين أوليين. يمكن أن يؤدي هذا المزيج إلى صعوبة وصول المجرمين إلى الرسائل الأصلية. كان الهدف من هذا البحث هو تحديد عملية تشفير وفك تشفير الخوارزميات الهجينة باستخدام طرق *hill cipher* وطرق *Rivest Shamir Adleman* لتحسين الأمن. تم إجراء هذا البحث عن طريق إنشاء مولد زوج المفاتيح بواسطة مستلم الرسائل عن طريق تحديد أي قيم p و q أولية نسبيا بحيث يتم الحصول على زوج من المفاتيح العامة (e,n) وزوج مفاتيح خاص(d,n) . ثم يقوم مرسل الرسائل بعمل عينة في شكل الرسالة النصية أو النص العادي يتم تحويلها في شكل ASCIIويحدد مصفوفة المفاتيح التي سيتم حسابها بواسطة صيغة*hill cipher* .و بعد ذلك، يتم استخدام زوج المفاتيح العمومي الذي يوفره مستلم الرسائل لتشفير مفتاح الرسائل باستخدام طريقة *Rivest Shamir Adleman*. ثم يجب أن يبحث مستلم الرسائل عن معكوس مفتاح (kunci matriks) الرسالة للحصول على الرسالة الأصلية التي يتم حسابها بواسطة صيغة *hill cipher* ، ثم يتم إرجاعها في شكل نص باستخدام رمز ASCII. تكون نتائج جمع الطريقة *hill cipher* و الطريقة *Rivest Shamir Adleman* في شكل زيادة أمان الرسائل عن طريق تشفير أمان *hill cipher* الموجود

في مفتاح المصفوفة باستخدام *Rivest Shamir Adleman* الذي يحتوي على مفاتيح التشفير وفك التشفير المختلفة.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan sistem informasi yang pesat memudahkan seseorang untuk mendapatkan suatu informasi. Hal tersebut dapat mengakibatkan proses pengiriman informasi menjadi tidak aman karena dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Masalah keamanan informasi menjadi aspek penting pada proses pengiriman informasi, banyak kejahatan *cyber* atau *hacker* yang memanfaatkan celah keamanan suatu sistem untuk memanipulasi informasi. Keamanan informasi meliputi banyak aspek, antara lain pencegahan dari pengaksesan informasi oleh pihak-pihak yang tidak berhak, melindungi kerahasiaan informasi yang bersifat privat, pencegahan dari usaha untuk mengubah informasi, dan lain-lain. Salah satu bentuk informasi yang dikirim dapat berupa pesan teks.

Pesan itu sendiri dapat disampaikan melalui media komunikasi. Perkembangan teknologi saat ini menjadikan lalu lintas pengiriman pesan semakin pesat. Pertukaran informasi yang pesat didukung oleh perkembangan komputer dan telepon genggam. Dimana akan memudahkan pihak yang tidak berkepentingan untuk mendapatkan pesan teks. Oleh karena itu, dibutuhkan suatu sistem keamanan pesan teks yang dapat menjaga kerahasiaan pesan teks tersebut.

Salah satu teknik yang dapat digunakan untuk menjaga keamanan pesan teks yaitu dengan menggunakan kriptografi. Kriptografi merupakan ilmu yang berperan penting dalam bidang keamanan informasi. Kriptografi digunakan untuk menjaga keamanan pesan atau informasi itu sendiri, baik informasi yang ditransmisikan

melalui saluran komunikasi maupun informasi yang disimpan dalam media penyimpanan (Munir, Kriptografi, 2019). Dalam kriptografi, informasi yang sangat rahasia akan disandikan sedemikian rupa sehingga informasi yang dicuri tidak dapat diketahui oleh pihak yang tidak berhak, karena informasi yang dicuri merupakan informasi yang sudah disandikan (Jamaludin, 2018).

Kriptografi memiliki banyak metode yang dapat digunakan untuk menyandikan pesan, namun pada dasarnya terdapat dua algoritma, yaitu algoritma simetri dan algoritma asimetri. Masing-masing dari algoritma tersebut memiliki kelebihan dan kekurangannya. Supaya dapat mengamankan suatu sistem dari pihak yang tidak berkepentingan maka diperlukan suatu metode untuk meningkatkan keamanan sistem tersebut. Oleh karena itu, salah satu solusi untuk meningkatkan keamanan pesan teks dengan menggabungkan dua algoritma yang disebut dengan algoritma hibrida.

Algoritma hibrida antara algoritma simetri dan algoritma asimetri dibutuhkan karena masalah keamanan kunci simetri. Algoritma asimetri mempunyai tingkat keamanan kunci lebih tinggi, tetapi kecepatan enkripsi maupun dekripsi yang dilakukakn algoritma asimetri lebih lama. Sehingga algoritma simetri dan asimetri digabung untuk memberikan perlindungan untuk kunci simetri serta meningkatkan kecepatan kriptografi kunci asimetri (Suhandinata & dkk, 2019). Dalam penggunaan algoritma hibrida, algoritma simetri adalah teknik enkripsi yang digunakan pada algoritma ini, dimana kunci dekripsi sama dengan kunci enkripsi. Untuk kriptografi *public key*, akan digunakan algoritma asimetri, dimana kunci dekripsi tidak sama dengan kunci enkripsi (Jamaludin, 2018). Kunci enkripsi pada algoritma asimetri dapat diketahui banyak orang atau bersifat umum, sedangkan

kunci dekripsinya hanya dapat dimiliki oleh pengirim dan penerima atau bersifat rahasia. Algoritma simetri sendiri memiliki banyak metode, salah satunya adalah *hill cipher* yang akan digabungkan dengan metode pada algoritma asimetri yaitu Rivest Shamir Adleman (*RSA).*

Algoritma *hill cipher* merupakan algoritma enkripsi-dekripsi yang menggunakan matriks transformasi. Cipher ini ditemukan oleh Lester Hill tahun 1929. Keamanan algoritma *hill cipher* terletak pada ukuran dan tingkat keamanan kunci matriks. *Hill cipher* termasuk algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui cipherteks saja. Namun, *hill cipher* dapat dipecahkan dengan cukup mudah jika kriptanalismemiliki cipherteks dan potongan plainteks dengan kunci yang sama.oleh karena itu, keamanan kunci harus diperkuat dengan menyandikan kunci matriks menggunakan algoritma RSA, dimana algoritma RSA merupakan algoritma kriptografi kunci-publik yang populer. Algorirma ini dibuat oleh tiga orang peneliti dari MIT (*Massachussets Institute of Technology*) pada tahun 1976, yaitu: Rivest, Shamir, dan Adleman. Algoritma RSA menggunakan kunci publik dan kunci privat, dimana kunci publik dapat diketahui banyak orang untuk mengenkripsi pesan, sedangkan kunci privat hanya dapat diketahui oleh pihak tertentu untuk mendekripsi pesan. Keamanan algoritma ini terletak pada sulitnya pemfaktoran bilangan bulat besar menjadi faktor-faktor prima. Pemfaktoran ini dilakukan untuk memperoleh kunci privat.

Terdapat beberapa penelitian terdahulu menggunakan kriptografi hibrida, yang pertama penelitian dilakukan oleh Sebastian Suhandinata, dkk (2019) yang berjudul "*Analisis Performa Kriptografi Hybrid Algoritma Blowfish dan Algoritma*

RSA". Penelitian tersebut bertujuan untuk mengukur tingkat kecepatan kriptografi *hybrid* yang terdiri dari algoritma simetri *blowfish* dan algoritma asimetri RSA pada beberapa tipe data diantaranya dokumen, foto, audio, dan video. Hasil dari penelitian tersebut adalah algoritma *hybrid* yang memiliki performa tidak jauh berbeda dari algoritma *blowfish* dan membuat proses enkripsi dan dekripsi data lebih aman dengan keunggulan dari algoritma RSA, dalam hal ini rata-rata kecepatan enkripsi algoritma hibrida lebih cepat dari pada rata-rata kecepatan dekripsi algoritma hibrida.

Penelitian yang kedua dilakukan oleh Ilham (2018) yang berjudul "*Analisis dan Desain Algoritma Hybrid Kriptografi untuk Manajemen Strategi Pengamanan Data Perusahaan*". Penelitian tersebut menggabungkan algoritma asimetri RSA dan *ElGamal* untuk membantu dalam menjaga keamanan dan kerahasiaan dokumen-dokumen penting, enkripsi dan dekripsi pada algoritma RSA menggunakan satu pasang kunci yaitu kunci publik dan kunci privat sehingga membantu proses pengamanan data dan algoritma *ElGamal* yang digunakan untuk *digital signature*. Hasil dari penelitian tersebut yaitu pengamanan dokumen yang memiliki keakuratan rata-rata sebesar 85,57%, hasil dari dokumen yang asli dan dokumen yang didekripsi terletak pada *margin* halaman dan gambar simbol *bullet list*.

Penelitian ketiga menggunakan metode yang sama yaitu algoritma simetri *hill cipher* dan algoritma asimetri RSA oleh Jamaludin (2018) dengan judul "*Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem*". Peneliti menggunakan *hybrid cryptosystem* dengan memanfaatkan keunggulan kecepatan pemrosesan data oleh algoritma simetri dan kemudahan

transfer kunci menggunakan algoritma asimetri untuk meningkatkan keamanan teks. Penelitian tersebut bertujuan untuk mengkombinasikan algoritma *hill cipher* dan RSA sehingga akan meningkatkan pengamanan yang lebih baik dari hasil kombinasi tersebut. Penelitian tersebut menggunakan kunci pesan dengan matriks (2×2) dan banyak karakter yang digunakan sebanyak 26 karakter. Hasil dari penelitian tersebut dapat diterapkan untuk meningkatkan keamanan pada pesan teks dimana plainteks yang dikirim dienkripsi oleh *hill cipher* serta pengamanan kunci oleh algoritma RSA.

Amanah merupakan hal penting dalam proses pengiriman pesan, apabila seseorang memiliki sifat amanah dalam dirinya maka pesan akan sampai kepada penerima dalam keadaan baik tanpa adanya perubahan isi pesan. Adapun ayat yang berkaitan dengan sifat amanah terdapat pada surat an-Nisa ayat 58, yang artinya:

"*Sungguh, Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan apabila menetapkan hukum diantara manusia hendaknya kamu menetapkannya dengan adil. Sungguh, Allah sebaik-baik yang memberi pengajaran kepadamu. Sungguh, Allah adalah Maha Mendengar, Maha Melihat.*"(an-Nisa'/4:58)

Yang mana pada ayat tersebut dijelaskan bahwa menunaikan amanah itu hukumnya wajib terutaman ketika orang yang berhak menuntutnya dan kalau didunia tidak ditunaikan, maka akan dituntut pertanggungjawabannya pada hari kiamat. Dalam hadist nabi dinyatakan melanggar amanah adalah kehancuran dan sifat *nifaq* melekat padanya. (Lajnah Pentashihan Mushaf Al-Qur'an, 2009)

Berdasarkan beberapa uraian diatas yang melatarbelakangi penulis melakukan penelitian dengan judul "Penerapan Kriptografi Hibrida Algoritma *Hill Cipher* dan *Rivest Shamir Adleman* (RSA) pada Pengamanan Pesan Teks". Penelitian ini dilakukan untuk mengetahui proses enkripsi dan dekripsi

menggunakan metode *hill cipher* dan RSA, serta dapat mengananlisis keamanan pesan teks. Diharapkan adanya penelitian ini dapat memberikan gambaran dan informasi sebagian tentang keamanan sistem informasi dan sekaligus membantu para perancang dan pengelola sistem informasi dalam mengamankan sistem informasinya.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka rumusan masalah dalam penelitian ini yaitu

1. Bagaimana proses dan hasil dari enkripsi algoritma hibrida menggunakan metode *hill cipher* dan metode *RSA*?
2. Bagaimana proses dan hasil dari dekripsi algoritma hibrida menggunakan metode *hill cipher* dan metode *RSA*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah sebelumnya, tujuan dari penelitian ini yaitu:

1. Dapat mengetahui proses dan hasil dari enkripsi algoritma hibrida menggunakan metode *hill cipher* dan metode *RSA.*
2. Dapat mengetahui proses dan hasil dari dekripsi algoritma hibrida menggunakan metode *hill cipher* dan metode *RSA.*

1.4 Manfaat Penelitian

Peneliti berharap bahwa dalam melakukan penelitian ini dapat memberi manfaat kepada orang lain sehingga dapat memperkaya sumber pengetahuan tentang kriptografi khususnya pada pengembangan proses penyandian secara

kompleks dengan menggabungkan metode *hill cipher* dan *RSA* dan dapat memperkuat keamanan pesan rahasia.

1.5 Batasan Masalah

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

1. Kunci matriks yang digunakan yaitu kunci matriks persegi yang memiliki invers.
2. Pesan yang diubah dalam bentuk matriks memiliki jumlah kolom yang sama dengan ukuran kunci matriksnya.
3. Pesan yang digunakan terdiri dari 127 karakter ASCII yang dimulai dari 32 sampai 159.
4. Entri untuk spasi pada matriks akan ditulis "*space*", simbol-simbol yang lain tetap seperti simbol aslinya dan setiap entri yang kosong pada matriks pesan akan diisi dengan huruf "X".

1.6 Metode Penelitian

Informasi yang telah diperoleh dari berbagai literatur kemudian dianalisis dan diolah dalam bentuk laporan penelitian kepustakaan. Berikut akan dijelasan langkah-langkah analisis untuk mengetahui proses enkripsi dan dekripsi algoritma hibrida mengunakan metode *hill cipher* dan metode RSA.

Sebelum melakukan enkripsi dan dekripsi, diperlukan pembangkit pasangan kunci terlebih dahulu, yang nantinya digunakan dalam proses pada metode RSA. Selanjutnya dapat melakukan proses denkripsi dan dekripsi sebagai berikut:

1. Proses enkripsi pesan menggunakan metode *hill cipher* dan enkripsi kunci pesan menggunakan metode RSA.
    a. Menentukan pesan yang akan dikirim.
    b. Menentukan kunci enkripsi dengan matriks 3×3.
    c. Membagi pesan dalam bentuk blok-blok dan mengkonversikan masing-masing karakter ke dalam bilangan ASCII.
    d. Mengalikan kunci matriks dengan karakter ASCII yang di modulo 127.
    e. Mengkonversi hasil perkalian sehingga didapatkan cipherteks.
    f. Pengirim pesan menerima pasangan kunci publik dari penerima pesan.
    g. Membagi kunci *hill cipher* dalam beberapa blok.
    h. Menentukan enkripsi dengan memangkatkan kunci *hill cipher* dengan kunci publik yang di modulo n.
    i. Hasil enkripsi dirubah dalam bentuk matriks dan diberikan kepada penerima pesan.
2. Proses dekripsi kunci pesan menggunakan metode RSA dan dekripsi pesan menggunakan metode *hill cipher*.
    a. Mendapatkan enkripsi kunci *hill cipher*.
    b. Mengubah enkripsi kunci *hill cipher* dalan bebeapa blok.
    c. Menentukan dekripsi dengan memangkatkan hasil enkripsi dengan kunci privat yang di modulo n.
    d. Mendapatkan kembali kunci *hill cipher*.
    e. Menerima pesan (cipherteks) dari pengirim pesan.
    f. Mencari invers kunci matriks 3×3.

g. Membagi pesan dalam bentuk blok-blok dan mengkonversikan masing-masing karakter ke dalam bilangan ASCII.
h. Mengalikan hasil invers dengan hasil konversi cipherteks sehingga diperoleh plainteks.
i. Didapatkan kembali plainteks (pesan rahasia).

1.7 Sistematika Penulisan

Sistematika penulisan dalam penelitian kali ini terbagi dalam 4 bab dan masing-masing terdiri dari beberapa subbab. Berikut rincian dari sistematika penulisan agar mempermudah pembaca untuk memahaminya.

Bab I Pendahuluan

Hal-hal yang dijelaskan pada bab ini meliputi latar belakang penelitian ini diambil, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, metode penelitian dan sistematika penelitian.

Bab II Kajian Pustaka

Teori-teori yang dijelaskan pada bab ini bersumber dari berbagai literatur seperti buku, jurnal ilmiah, serta penelitian terdahulu yang mendukung dalam pembahasan penelitian. Sehingga pada bab ini memuat penguraian tentang kriptografi hibrida dengan menggunakan metode *hill cipher* dan RSA serta terdapat kajian al-Qur’an yang berkaitan dengan masalah tersebut.

Bab III Pembahasan

Pembahasan kali ini berisi tentang penyelesaian prosen enkripsi dan dekripsi menggunakan metode *hill cipher* dan RSA serta hasil yang didapatkan dari proses tersebut.

Bab IV Penutup

Bab ini memberikan kesimpulan dari uraian pembahasan dan saran-saran yang mendukung dalam penelitian selanjutnya.

BAB II

KAJIAN PUSTAKA

2.1 Matriks

Matriks adalah susunan skalar elemen-elemen dalam bentuk baris dan kolom. Matriks A yang berukuran dari m baris dan n kolom $(m \times n)$ adalah (Munir, Matematika Diskrit, 2012):

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

Entri a_{ij} disebut elemen matriks pada baris ke-i dan kolom ke-j, dimana $i = 1, 2, 3, \ldots, n$ dan $j = 1, 2, 3, \ldots, m$. Jika $m = n$, maka matriks tersebut dinamakan juga matriks bujur sangkar *(square matrix)*. Menuliskan matriks dalam bentuk persegi panjang di atas adalah boros tempat, oleh karena itu kita lazim menulis matriks dengan notasi ringkas $A = [a_{ij}]$.

2.1.1 Determinan, Adjoin, dan Invers Matriks

1. Determinan matriks

   Secara umum determinan untuk sebarang matriks persegi berordo $n \times n$ didefinisikan sebagai berikut:

   Jika *A* adalah matriks bujur sangkar. *Fungsi determinan* dinyatakan dengan *det*, dan $\det(A)$ didefinisikan sebagai jumlah semua hasil kali elementer bertanda dari *A*. Angka $\det(A)$ disebut *determinan A* (Anton, 2000).

   Misalkan matriks $A_{n\times n} = [a_{ij}]$

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

Maka matriks $\det|A_{n\times n}| = [a_{ij}]$

$$\det|A| = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

Hasil kali elementer matriks A adalah hasil kali n buah unsur A tanpa ada pengambilan unsur dari baris maupun kolom. Sedangkan hasil kali elementer diberi tanda positif atau negatif sehingga dinamakan hasil kali elementer bertanda negatif atau positif didasarkan pada hasil permutasi.

Contoh:

$$A = \begin{bmatrix} 20 & 18 \\ 67 & 8 \end{bmatrix}$$

Maka

$$\det(A) = \begin{bmatrix} 20 & 18 \\ 67 & 8 \end{bmatrix} = 20 \times 8 - 18 \times 67 = -1046$$

2. Adjoin matriks

Jika A adalah sebarang matriks $n \times n$ dan C_{ij} adalah kofaktor dari a_{ij}, maka matriks

$$\begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ C_{n1} & C_{n2} & \cdots & C_{nn} \end{bmatrix}$$

disebut *matriks kofaktor* dari A. Transpos dari matriks ini disebut *adjoin A* dan dinyatakan oleh $adj(A)$ (Anton, 2000).

Misalkan $A_{n\times n} = [a_{ij}]$

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

Maka diperoleh M_{ij} dan C_{ij} dari matriks A

$$M_{11} = \begin{bmatrix} a_{22} & \cdots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

$$\vdots$$

$$M_{nn} = \begin{bmatrix} a_{11} & \cdots & a_{1,n-1} \\ \vdots & \ddots & \vdots \\ a_{-1,1} & \cdots & a_{n-1,n-1} \end{bmatrix}, C_{nn} = (-1)^{n+n} M_{nn}$$

Jika matriks kofaktor dari A ditranspos maka hasilnya disebut adjoin A.

Contoh:

Misalkan matriks A berordo 3×3

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

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

Matriks kofaktor A adalah

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

Dan adjoin A adalah

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

3. Invers matriks

Jika determinan matriks bujur sangkar, dan jika terdapat sebuah matriks B yang berukuran sama dapat ditentukan sedemikian sehingga $AB = BA = I$, maka A disebut *dapat dibalik* dan B disebut *invers* dari A (Anton, 2000).

Misalkan $A_{n\times n} = [a_{ij}]$

$$A_{n\times n} = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

$$A^{-1} = \frac{1}{\det A}\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

$$= \frac{[A_{ij}]^t}{|A|}, i = j = 1 = 1, n$$

Contoh:

Diketahui sebuah matriks

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

Maka determinan diperoleh

$\det A = det \begin{bmatrix} 1 & 2 & 3 \\ 0 & 2 & 1 \\ 3 & 2 & 1 \end{bmatrix} = -12$, jadi matriks non-singular dan mempunyai invers.

Kofaktor dari matriks A:

$$A_{ij} = (-1)^{i+j}\left|M_{ij}\right|$$

$$A_{11} = |M_{11}| = \begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix} = 0, A_{12} = -|M_{12}| = -\begin{vmatrix} 0 & 1 \\ 3 & 1 \end{vmatrix} = 3, A_{13} = |M_{13}|$$

$$= \begin{vmatrix} 0 & 2 \\ 3 & 2 \end{vmatrix} = -6$$

$$A_{21} = -|M_{21}| = -\begin{vmatrix} 2 & 3 \\ 2 & 1 \end{vmatrix} = 4, A_{22} = |M_{22}| = \begin{vmatrix} 1 & 3 \\ 3 & 1 \end{vmatrix} = -8, A_{23} = -|M_{23}|$$

$$= -\begin{vmatrix} 1 & 2 \\ 3 & 2 \end{vmatrix} = 4$$

$$A_{31} = |M_{31}| = \begin{vmatrix} 2 & 3 \\ 2 & 1 \end{vmatrix} = -4, A_{32} = -|M_{32}| = -\begin{vmatrix} 1 & 3 \\ 0 & 1 \end{vmatrix} = -1, A_{33} = |M_{33}|$$

$$= \begin{vmatrix} 1 & 2 \\ 0 & 2 \end{vmatrix} = 2$$

Jadi:

$$A^{-1} = \frac{(A_{ij})^t}{|A|} = -\frac{1}{12}\begin{bmatrix} 0 & 3 & -6 \\ 4 & -8 & 4 \\ -4 & -1 & 2 \end{bmatrix}^t = -\frac{1}{12}\begin{bmatrix} 0 & 4 & -4 \\ 3 & -8 & -1 \\ -6 & 4 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & -\frac{1}{3} & \frac{1}{3} \\ -\frac{1}{4} & \frac{2}{3} & \frac{1}{12} \\ \frac{1}{2} & -\frac{1}{3} & -\frac{1}{6} \end{bmatrix}$$

Perhatikan:

$$AA^{-1} = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 2 & 1 \\ 3 & 2 & 1 \end{bmatrix}\begin{bmatrix} 0 & -\frac{1}{3} & \frac{1}{3} \\ -\frac{1}{4} & \frac{2}{3} & \frac{1}{12} \\ \frac{1}{2} & -\frac{1}{3} & -\frac{1}{6} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I$$

Untuk semua matriks bujur sangkar berlaku $AA^{-1} = I$.

2.2 Teori Bilangan

2.2.1 Kongruensi

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

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

Jika $a - b$ tidak habis dibagi M, maka dapat dikatakan tidak kongruen dengan $b\ mod\ M$, dan dituliskan: $a \not\equiv b\ (mod\ M)$ (Irawan & dkk, 2014).

Contoh:

$27 \equiv 2(mod\ 5)$ karena $(27 - 2)$ terbagi oleh 5.

Definisi dan contoh tersebut dapat ditelaah sebagai berikut:

Jika $M > 0$ dan $M|(a - b)$ maka ada suatu bilangan bulat t sehingga $a - b = Mt$. Sehingga $a \equiv b(mod\ M)$ dapat dinyatakan juga 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. Menurut contoh $27 \equiv 2(mod\ 5)$ sama artinya dengan $27 = 5.5 + 2$.

Teorema. Andaikan a, b dan c adalah bilangan bulat dan m bilangan asli, maka berlaku (Irawan & dkk, 2014):

1. Refleksi $a \equiv a(mod\ m)$.
2. Simetris, jika $a \equiv b\ (mod\ m)$, maka:

$b \equiv a\ (mod\ m)$ dan $a - b \equiv 0(mod\ m)$ adalah pernyataan yang ekuivalen.

3. Transitif, jika $a \equiv b\ (mod\ m)$ dan $b \equiv c(mod\ m)$maka $a \equiv c\ (mod\ m)$.

2.2.2 Sistem Residu

Jika $x \equiv y\ (mod\ m)$, maka y disebut residu dari x modulo m. Himpunan $x_1, x_2, x_3, \dots, x_m$ dikatakan sistem residu lengkap modulo m, jika untuk setiap bilangan bulat y ada suatu dan hanya satu x_i sehingga $y \equiv x_i(mod\ m)$ (Irawan & dkk, 2014).

Berdasarkan definisi sebelumnya, jelas bahwa ada tak terhingga banyak sistem residu lengkap modulo m, seperti $0, 1, 2, \dots, m-1, m$. Himpunan m-buah bilangan bulat – bilangan bulat dikatakan membentuk residu lengkap modulo m jika dan hanya jika tidak ada dua bilangan bulat dalam himpunan tersebut yang kongruen modulo m.

Untuk suatu bilangan bulat a dan $m > 0$, sehingga himpunan semua bilangan bulat x yang memenuhi $x \equiv a\ (mod\ m)$ adalah bentuk barisan matematika:

$$\dots, a - 3m, a - 2m, a - m, a, a + m, a + 2m, a + 3m, \dots$$

Himpunan ini disebut kelas sisa atau kelas kongruensi modulo m.

2.2.3 Kongruensi Matriks

Definisi. Misalkan A dan B adalah matriks $n \times k$ dengan unsur-unsurnya bilangan bulat, unsur ke (i, j) berturut-turut adalah a_{ij} dan b_{ij}. A dikatakan kongruensi 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 $A \equiv B(mod\ m)$ jika A kongruensi B modulo m.

Contoh:

$$\begin{pmatrix} 15 & 3 \\ 8 & 12 \end{pmatrix} \equiv \begin{pmatrix} 4 & 3 \\ 3 & 1 \end{pmatrix} (mod\ 11)$$

Proposisi 2.1. Jika A dan B adalah matriks $n \times k$ dengan $A \equiv B(mod\ m)$, C adalah matriks $k \times p$ dan D adalah matriks $p \times n$, yang semua unsurnya bilangan bulat, maka $AC \equiv BC(mod\ m)$ dan $DA \equiv DB(mod\ m)$.

Perhatikan sistem kongruensi berikut ini:

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1(mod\ m)$$

$$a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2(mod\ m)$$

$$\vdots$$

$$a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \equiv b_n(mod\ m)$$

Dengan menggunakan notasi matriks, sistem kongruensi n ekuivalen dengan kongruensi matriks $AX \equiv B(mod\ m)$ dimana:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}, X = \begin{bmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{bmatrix} \text{ dan } B = \begin{bmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{bmatrix}$$

Contoh:

$$3x + 4y \equiv 5(mod\ 13)$$

$$2x + 5y \equiv 7(mod\ 13)$$

Ditulis dalam bentuk matriks sebagai berikut:

$$\begin{bmatrix}3 & 4\\ 2 & 5\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix} \equiv \begin{bmatrix}5\\ 7\end{bmatrix} (mod\ 13)$$

Sekarang kita kembangkan suatu metode penyelesaian kongruensi dari bentuk $AX \equiv B(mod\ m)$. Dasar dari metode ini adalah mencari invers dari matriks A yaitu $\bar{A}$ sedemikian sehingga $\bar{A}A \equiv I(mod\ m)$ dimana I adalah matriks identitas.

Definisi. Jika $\bar{A}$ dan A adalah matriks $n \times n$ dari bilangan-bilangan bulat, dan $\bar{A}A \equiv A\bar{A} \equiv I(mod\ m)$ dimana:

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

adalah matriks identitas berordo n, maka $\bar{A}$ dikatakan invers dari A modulo m.

Jika $\bar{A}$ invers dari A dan $B \equiv \bar{A}(mod\ m)$, maka B juga invers dari A. Hal ini mengikuti proposisi 2.1, karena $BA \equiv \bar{A}A \equiv I(mod\ m)$.

Sebaliknya, jika B_1 dan B_2 kedua invers dari A maka $B_1 \equiv B_2(mod\ m)$. Dengan menggunakan proposisi 2.1 dan kongruensi $B_1A \equiv B_2A \equiv I(mod\ m)$, kita peroleh $B_1AB_1 \equiv B_2AB_2\ (mod\ m)$. Karena $AB_1 \equiv I(mod\ m)$, maka kita simpulkan bahwa $B_1 \equiv B_2\ (mod\ m)$.

Contoh:

$$\begin{bmatrix}1 & 3\\ 2 & 4\end{bmatrix}\begin{bmatrix}3 & 4\\ 1 & 2\end{bmatrix} = \begin{bmatrix}6 & 10\\ 10 & 16\end{bmatrix} \equiv \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} (mod\ 5)$$

Dan

$$\begin{bmatrix}3 & 4\\1 & 2\end{bmatrix}\begin{bmatrix}1 & 3\\2 & 4\end{bmatrix} = \begin{bmatrix}11 & 25\\5 & 11\end{bmatrix} \equiv \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} (mod\ 5)$$

Kita lihat bahwa matriks $\begin{bmatrix}3 & 4\\1 & 2\end{bmatrix}$ adalah invers dari $\begin{bmatrix}1 & 3\\2 & 4\end{bmatrix} (mod\ 5)$

Proposisi berikut memberikan suatu metode yang mudah untuk mencari invers dari matriks 2×2.

Proposisi 2.2. Misalnya $A = \begin{bmatrix}a & b\\c & d\end{bmatrix}$ adalah matriks bilangan bulat sedemikian sehingga $\Delta = \det A = ad - bc$ adalah relatif prima terhadap bilangan bulat positif m. Maka, matriks

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

dimana $\bar{\Delta}$ adalah invers dari Δ modulo m, yang merupakan invers dari A modulo m.

Contoh:

Misalkan $\begin{bmatrix}3 & 4\\2 & 5\end{bmatrix}$. Karena 2 adalah invers dari $\det A = 7\ modulo\ 13$, diperoleh

$$\bar{A} = 2\begin{bmatrix}5 & -4\\-2 & 3\end{bmatrix} = \begin{bmatrix}10 & -8\\-4 & 6\end{bmatrix} \equiv \begin{bmatrix}10 & 5\\9 & 6\end{bmatrix} (mod\ 13)$$

Untuk menyusun rumus invers dari matriks $n \times n$ dimana n adalah bilangan bulat positif, kita perlu hasil dari aljabar linier (Rosen, 1986).

2.2.4 Bilangan Prima

Bilangan bulat positif p $(p > 1)$ disebut bilangan prima jika pembaginya hanya 1 dan p. Misalnya, 23 adalah bilangan prima karena ia hanya habis dibagi oleh 1 dan 23. Karena bilangan prima harus lebih besar dari 1, maka barisan prima

dimulai dari 2, yaitu $2, 3, 5, 7, 11, 13, ...$ Seluruh bilangan prima adalah bilangan ganjil, kecuali 2 yang merupakan bilangan genap. Bilang selain prima disebut bilangan komposit (*composite*). Misalkan 20 adalah bilangan komposit karena 20 dapat dibagi oleh 2, 4, 5, dan 10, selain 1 dan 20 sendiri (Munir, Kriptografi, 2019).

Di dalam Teori Bilangan terdapat sebuah teorema yang dapat digunakan untuk menguji keprimaan suatu bilangan bulat, yang terkenal dengan Teorema Fermat. Teorema Fermat menyatakan jika p adalah bilangan prima dan a adalah bilangan bulat yang tidak habis dibagi dengan p, yaitu pembagi bersama terbesar (PBB) $(a, p) = 1$, maka $a^{p-1} \equiv 1(mod\ p)$ (Munir, Kriptografi, 2019).

Contoh:

Kita akan menguji apakah 17 dan 21 bilangan prima atau bukan dengan Teorema Fermat. Di sini kita mengambil nilai $a = 2$ karena $\text{PBB}(17,2) = 1$ dan $\text{PBB}(21,2) = 1$. Untuk 17,

$$2^{17-1} = 65536 \equiv 1(mod\ 17)$$

Karena 17 habis membagi $65531 - 1 = 65535$ (yaitu, $65535 \div 17 = 3855$). Oleh karena itu, 17 adalah bilangan prima. Untuk 21,

$$2^{21-1} = 1048576 \not\equiv 1(mod\ 21)$$

Karena 21 tidak habis menbagi $1048576 - 1 = 1048575$. Oleh karena itu, 21 bukan bilangan prima.

2.2.5 Pembagi Bersama Terbesar (PBB)

Misalkan a dan b adalah bilangan bulat tidak nol. Pembagi Bersama Terbesar (PBB) atau *greatest common divisor (gcd)* dari a dan b adalah bilangan bulat terbesar d sedemikian sehingga $d|a$ dan $d|b$. Dalam hal ini dapat dinyatakan bahwa PBB$(a, b) = d$ (Munir, Kriptografi, 2019).

Sifat-sifat dari pembagi bersama terbesar dinyatakan pada teorema berikut:

Teorema. Misalkan a, b dan c adalah bilanga bulat.

a) Jika c adalah PBB dari a dan b, maka $c|(a + b)$
b) Jika c adalah PBB dari a dan b, maka $c|(a - b)$
c) Jika $c|a$, maka $c|ab$.

Teorema sebelumnya ingin menunjukkan bahwa PBB dari dua buah bilangan bulat sama dengan PBB salah satu bilangan bulat tersebut dengan sisa hasil pembaginya. Hal ini dinyatakan pada teorema berikut.

Teorema. Misalkan m dan n adalah dua buah bilangan bulat dengan syarat $n > 0$ sedemikian sehingga

$$m = nq + r \quad , 0 \leq r < n$$

maka PBB(m, n) = PBB(n, r) (Munir, Matematika Diskrit, 2012).

2.2.6 Fungsi Totient Euler ϕ

Fungsi totient Euler ϕ mendefinisikan $\phi(n)$ untuk $n \geq 1$ yang menyatakan jumlah bilangan bulat positif $< n$ yang relatif prima dengan n (Munir, Kriptografi, 2019).

Jika n prima, maka setiap bilangan bulat yang lebih kecil dari n relatif prima terhadap n. Dengan kata lain, $\phi(n) = n - 1$ hanya jika n prima. Misalkan, $\phi(3) = 2, \phi(5) = 4, \phi(7) = 6, \phi(11) = 10, \phi(13) = 12$, dst.

Tiga sifat fungsi totient Euler sebagai berikut (Munir, Kriptografi, 2019):

1. Jika $n = pq$ adalah bilangan komposit dengan p dan q prima, maka $\phi(n) = \phi(p).\phi(q) = (p-1).(q-1)$.

   Contohnya, karena 21=7.3, maka $\phi(21) = \phi(7).\phi(3) = 6.2 = 12$, yaitu ada buah bilangan bulat yang relatif prima terhadap 21, yaitu 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20.
2. Jika p bilangan prima dan $k > 0$, maka $\phi(p^k) = p^k - p^{k-1}$,

   Contohnya, karena $16 = 2^4$, maka $\phi(16) = \phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$, maka ada delapan buah bilangan bulat yang relatif prima terhadap 16, yaitu 1, 3, 5, 7, 11, 13, 15.
3. (*Euler's generalization of fermat theorem*). Jika $\text{PBB}(a, n) = 1$, maka $a^{\phi(n)} mod\ n = 1$ (atau $a^{\phi(n)} \equiv 1 (mod\ n)$).

2.3 Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: "*cryptós*" artinya "*secret*" (rahasia), sedangkan "*gráphein*" artinya "*writing*" (tulisan). Jadi, kriptografi secara harfiah berarti "*secret writing*" (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai pustaka, salah satunya adalah kutipan dari buku Meyer (1982) yang mengatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara

menyandikannya ke dalam bentuk yang tidak dapat dipahami lagi maknanya (Munir, Kriptografi, 2019).

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern, kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data, dan autentikasi entitas. Jadi pengertian kriptografi secara modern tidak hanya berurusan dengan penyandian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi (Sadikin, 2012).

Kriptografi merupakan ilmu yang berperan penting di dalam bidang keamanan informasi. Kriptografi digunakan untuk menjaga keamanan pesan atau informasi, baik informasi yang ditransmisikan melalui saluran komunikasi maupun informasi disimpan di dalam media penyimpanan (Munir, Kriptografi, 2019).

2.3.1 Istilah dalam Kriptografi

1. Pesan

   Pesan (*message*) adalah data atau informasi yang dapat dibaca, dipersepsi, dan dimengerti artinya. Pesan dapat berupa teks, citra (*image*), suara/bunyi (*audio*), video, atau bentuk-bentuk biner lainnya, baik berbentuk digital maupun analog.

2. Plainteks

   Plainteks merupakan pesan yang berupa teks asli atau teks biasa yang ditulis atau diketik dan memiliki makna, plainteks sering disebut juga dengan teks-jelas (*cleartext*).

3. Cipherteks

Cipherteks merupakan pesan yang disandikan menjadi pesan yang tidak dapat dimengerti lagi maknanya, sehingga tidak dapat dipahami oleh pihak lain karena pesan tersebut berupa karakter-karakter yang tidak mempunyai makna (arti).

4. Enkripsi

Enkripsi (*encryption*) atau *enciphering* merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya menggunakan proses penyandian plainteks menjadi cipherteks. Proses enkripsi menerima masukan berupa plainteks dan kunci, hasilnya berupa cipherteks.

5. Dekripsi

Dekripsi (*decryption*) atau *deciphering* merupakan proses mengembalikan cipherteks menjadi bentuk asal atau plainteks. Proses dekripsi menerima masukan berupa cipherteks dan kunci, hasilnya adalah plaintek.

6. Cipher, Kode, dan Kunci

Algoritma kriptografi untuk enkripsi dan dekripsi disebut juga cipher. Cipher dapat diartikan sebagai aturan untuk *enchipering* dan *dechipering*, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa cipher memerlukan algoritma yang berbeda untuk *enciphering* dan *deciphering*.

Kriptografi pada zaman modern mengatasi masalah tersebut dengan penggunakan kunci (*key*). Algoritma kriptografi tidak perlu rahasia, tetapi kunci harus rahasia. Kunci adalah parameter yang digunakan di dalam *enciphering* dan *dechipering*. Kunci umumnya berupa string yang pendek atau berupa deretan bilangan. Istilah cipher sering disalahpahami dengan kode (*code*), kedua

istilah ini tidaklah sama pengertiannya. Jika cipher adalah transformasi karakter-ke-karakter atau bit-ke-bit tanpa memperhatikan struktur bahasa pesan, maka kode sering diacu sebagai prosedur yang mengganti setiap plainteks dengan suatu kata kode. Kode juga dapat berupa deretan angka dan huruf yang tidak bermakna. Transformasi dari plainteks menjadi kode sering disebut *encoding*, sedangkan transformasi sebaliknya sering disebut *decoding*. Untuk melakukan *encoding* dan *decoding* digunakan dokumen yang disebut buku kode (*codebook*) (Munir, Kriptografi, 2019).

2.3.2 Cipher Blok

Cipher blok merupakan suatu algoritma enkripsi dengan membagi jumlah teks-asli (plainteks) menjadi ukuran tertentuk (disebut blok) yang ditentukan dengan panjang yang sama, tergantung dari keinginan pengirim pesan. Cipher blok juga dapat diartikan sebagai algoritma yang masukan dan keluarannya berupa satu blok dan setiap bloknya terdiri dari banyak karakter. Secara garis besar, cipher blok dapat dianggap sebagai sebuah algoritma substitusi terhadap sekumpulan karakter yang berjumlah banyak.

Setiap blok plainteks dienkripsi dengan kunci yang panjangnya sama dengan blok plainteks tersebut. Enkripsi menghasilkan blok cipherteks yang berukuran sama dengan blok plainteks. Dekripsi dilakukan dengan cara yang serupa seperti enkripsi, blok cipherteks dienkripsi dengan kunci yang sama. Pada umumnya, cipher blok memproses teks atau karakter dengan blok yang relative manjang, sehingga dapat mempersulit penggunaan pola-pola serangan yang ada untuk membongkat kunci.

Misalkan blok plainteks (P) yang berukuran n yang nantinya dirubah menjadi matriks $n \times 1$ dinyatakan sebagai vektor

$$P = (p_1, p_2, \dots, p_n)$$

Dan blok cipherteks (C) adalah

$$C = (c_1, c_2, \dots, c_n)$$

Untuk setiap blok plainteks P_i, penyusunannya dapat dinyatakan sebagai vektor

$$P_i = (p_{i1}, p_{i2}, \dots, p_{in})$$

(Munir, Kriptografi, 2019)

Coba perhatikan contoh di bawah ini:

Plainteks: "BANJIRMEREDAMJAKARTAHARTABAHANPOKOKNAIK"

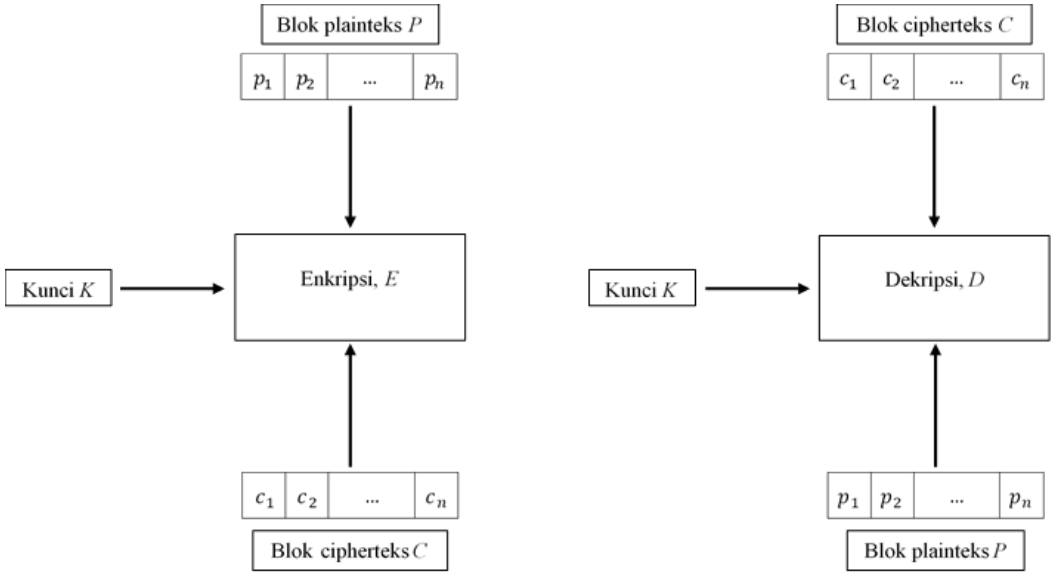
Plainteks tersebut dibagi menjadi 8 blok. Setiap blok berisi 6 karakter. Karena blok yang ketujuh tidak mencukupi maka ditambah dengan karakter "X" atau karakter lain yang diinginkan (Ariyus, 2008).

BANJIR	MEREDA	MJAKAR	TAHARG	ABAHAN	POKOKN	AIKXXX
Block 1	Block 2	Block 3	Block 4	Block 5	Block 6	Block 7

Enkripsi dan dekripsi blok P dengan kunci eksternal K dinyatakan berturut-turut dengan persamaan

$E_K(P) = C$ dan $D_K(C) = P$

Berikut gambaran proses enkripsi dan dekripsi dengan membagi teks kedalam bentuk blok-blok



Gambar 2. 1 Skema enkripsi dan dekripsi dengan pembagian blok

2.3.3 Algoritma-Algoritma Kriptografi

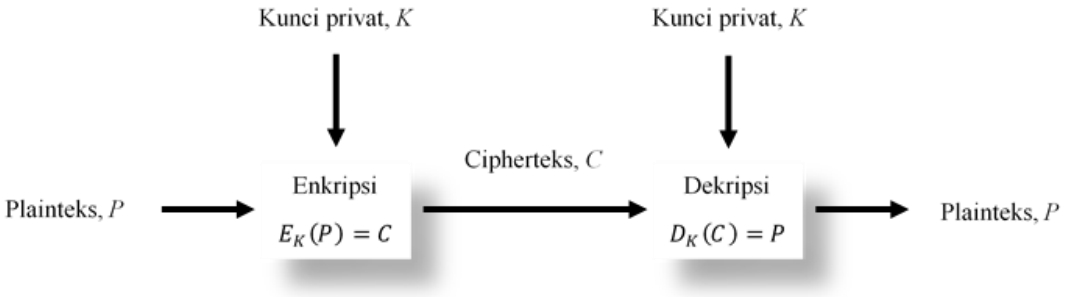
1. Algoritma Simetri

Algoritma ini sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi. Bila mengirim pesan dengan menggunakan algoritma ini, penerima pesan harus mengetahui kunci dari pesan tersebut agar bisa mendekripsikan pesan yang dikirim. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci. Jika kunci tersebut diketahui orang lain maka orang tersebut dapat melakukan enkripsi dan dekripsi terhadap pesan. Algoritma yang memakai kunci simetri diantaranya adalah (Ariyus, 2008):

1. Data Encryption Standard (DES),
2. Hill Cipher,
3. RC2, RC4, RC4, RC6,
4. International Data Encryption Algorithm (IDEA),

5. Advanced Encryption Standard (AES),
6. One Time Pad (OTP),
7. A5, dan lain sebagainya.

Kelemahan kriptografi simetri adalah penerima pesan harus memiliki kunci yang sama dengan pengirim pesan, sehingga pengirim pesan harus mencari cara yang aman untuk memberitahu kunci tersebut kepada penerima pesan.



Gambar 2. 2 Skema sistem kriptografi simetri

Analogi kriptografi simetri adalah dengan kotak, gembok, dan kunci gembok. Misalkan Alice hendak mengirim surat kepada Bob. Alice menyiapkan sebuah kotak dan gembok. Alice memiliki kunci gembok, Bob pun memiliki duplikatnya. Alice memasukkan suratnya ke dalam kotak, memasang gembok, lalu mengunci gembok dengan kunci yang dimilikinya. Menaruh surat ke dalam kotak yang terkunci sama artinya dengan menenkripsi surat tersebut. Tidak ada seorangpun yang dapat membaca surat karena kotak sudah terkunci. Kunci gembok yang digunakan Alice dianalogikan sebagai kunci rahasia. Kotak tersebut kemudian dikirim mengunakan kurir kepada Bob. Bob membuka gembok dengan kunci yang dimilikinya (duplikat kunci yang dimiliki Alice), lalu membaca surat di dalamnya. Membuka kotak dengan kunci gembok lalu membaca surat di dalamnya sama artinya dengan mendekripsi surat. Hanya Bob

yang dapat mendekripsi surat karena hanya Bob yang memiliki duplikat kunci gembok (Munir, Kriptografi, 2019).

2. Algoritma Asimetri

Algoritma asimetri sering juga disebut dengan algoritma kunci publik, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu (Ariyus, 2008):

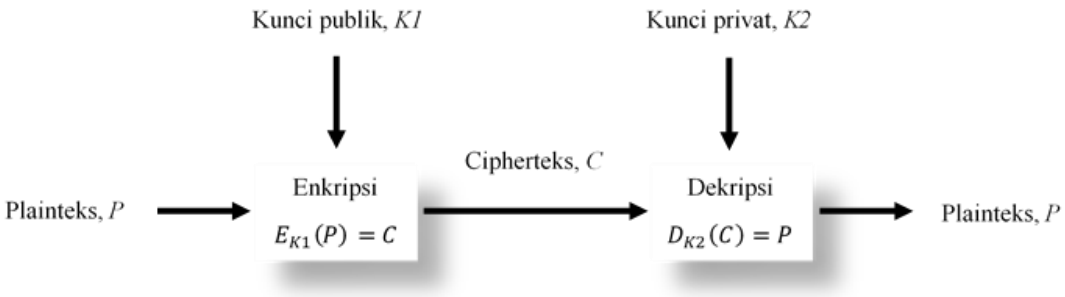
1. Kunci umum (*public key*): kunci yang boleh diketahui semua orang (dipublikasikan).
2. Kunci rahasia (*private key*): kunci yang dirahasiakan (hanya boleh diketahui satu orang).

Kunci-kunci tersebut berhubungan satu sama lain. Dengan kunci publik orang dapat mengenkripsi pesan tetapi tidak bisa mendekripsinya. Hanya orang yang memiliki kunci rahasia yang dapat mendekripsi pesan tersebut. Algoritma asimetri dapat mengirimkan pesan dengan lebih aman dari pada algoritma simetri. Algoritma yang memakai kunci publik diantaranya adalah (Ariyus, 2008):

1. Digital Signature Algorithm (DSA),
2. *RSA*,
3. Diffie-Hellman (DH),
4. Elliptic Curve Cryptography (ECC),
5. Kriptografi Quantum, dan lain sebagainya.

Keuntungan kriptografi asimetri ada dua. Pertama, tidak ada kebutuhan untuk mendistribusikan kunci rahasia (kunci privat) sebagaimana pada kriptografi simetri. Kunci publik dapat dikirim ke penerima melalui saluran yang sama dengan saluran yang digunakan untuk mengirim pesan. Saluran untuk mengirim pesan biasanya tidak aman.

Kedua, jumlah kunci dapat ditekan. Untuk berkomunikasi secara rahasia dengan banyak orang tidak perlu kunci privat sebanyak jumlah orang tersebut, cukup membuat dua buah kunci, yaitu kunci publik bagi para koresponden untuk mengenkripsi pesan yang hendak dikirim, dan kunci privat untuk mendekripsi pesan yang diterima.



Gambar 2. 3 Skema sistem kriptografi asimetri

Analogi kriptografi asimetri adalah seperti kotak surat yang terkunci dan memiliki lubang untuk memasukkan surat. Setiap orang dapat memasukkan surat ke dalam kotak surat tersebut, tetapi hanya pemilik kotak yang dapat membuka kotak dan membaca surat di dalamnya karena ia memiliki kunci. Dalam hal ini, kunci publik adalah alamat si pemilik kotak surat, alamat ini bersifat publik karena diketahui oleh siapapun. Kunci privat adalah kunci untuk membuka kotak surat, kunci ini disebut privat atau rahasia karena hanya pemilik kotak yang memilikinya (Munir, Kriptografi, 2019).

3. Fungsi Hash

Fungsi Hash sering disebut dengan fungsi Hash satu arah (*one-way function*), *message digest*, *fingerprint*, fungsi kompresi dan *message authentication code* (MAC), merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap. Fungsi Hash biasanya diperlukan bila ingin membuat sidik jari dari suatu pesan. Sidik jari pada pesan merupakan suatu tanda bahwa pesan tersebut benar-benar berasal dari orang yang diinginkan (Ariyus, 2008).

Fungsi Hash berguna untuk menguji integritas pesan. Dua pesan yang hanya berbeda satu bit menghasilkan pesan ringkas yang berbeda secara signifikan. Dua buah pesan dibandingkan pesan ringkasnya, jika pesan ringkasnya sama maka kedua pesan dianggap sama. Sebaliknya, jika pesan ringkasnya berbeda maka kedua pesan tidak sama (Munir, Kriptografi, 2019).

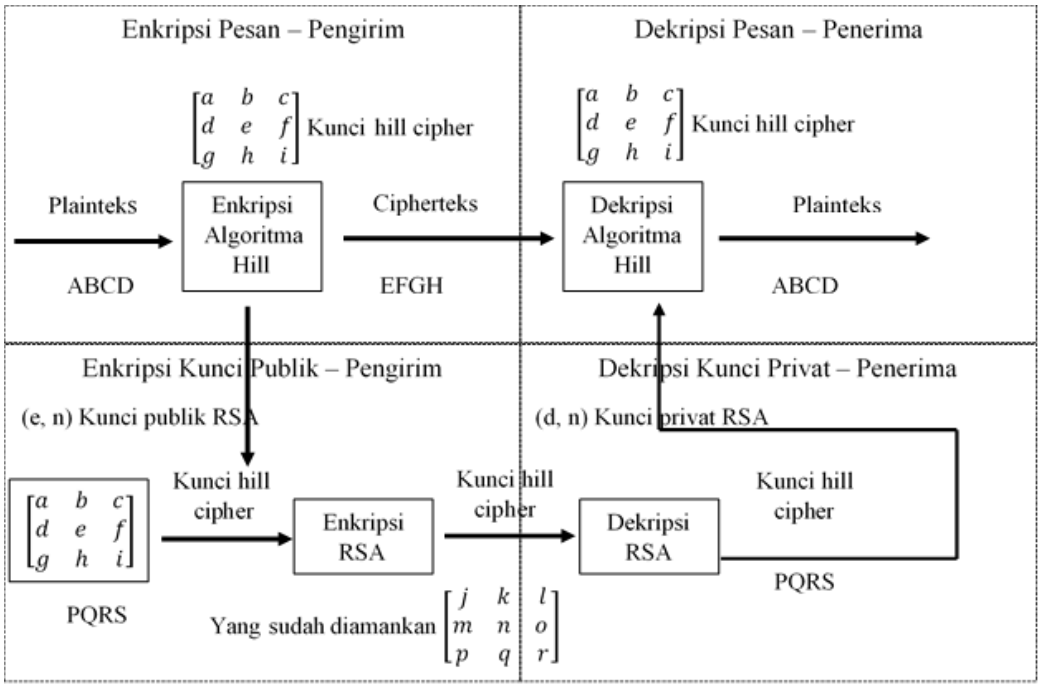
2.4 Kriptografi Hibrida

Kriptografi hibrida (*Hybrid Cryptosystem*) merupakan gabungan antara *cryptosystem* yang memakai *asymmetric cryptosystem* dan *cryptosystem* yang memakai *symmetric cryptosystem*. Dalam penggunaan algoritma hibrida, teknik enkripsi yang digunakan adalah enkripsi simetri dimana kunci dekripsi sama dengan kunci enkripsi. Untuk *public key cryptography*, diperlukan teknik enkripsi asimetri dimana kunci enkripsi tidak sama dengan kunci dekripsi (Jamaludin, 2018).

Algoritma hibrida adalah algoritma yang memanfaatkan dua tingkatan kunci, yaitu kunci rahasia (simetri) – yang disebut juga *session key* (kunci sesi) – untuk

enkripsi data dan pasangan kunci rahasia-kunci *public* untuk pemberian tanda tangan digital serta melindungi kunci simetri (Ariyus, 2008).

Pada sistem hibrida ini enkripsi atau dekripsi pesan menggunakan kriptografi kunci simetri, sedangkan kunci simetri di enkripsi atau dekripsi dengan menggunakan kunci *public*. Kunci simetri (yang disebut juga kunci sesi) dibangkitkan oleh salah satu pihak dan mengenkripsi pesan dengan kunci tersebut. Selanjutnya kunci sesi dienkripsikan dengan kunci *public* penerima lalu dikirim bersama-sama dengan pesan yang sudah dienkripsi. Penerima mula-mula mendekripsikan kunci sesi dengan kunci privatnya, lalu mendekripsikan pesan dengan kunci sesi tersebut. Kriptografi hibrida sering dipakai karena memanfaatkan keunggulan kecepatan pemrosesan data oleh algoritma simetri dan kemudahan transfer kunci menggunakan algoritma asimetri (Jamaludin, 2018).



Gambar 2. 4 Skema sistem kriptografi hibrida menggunakan algoritma hill cipher dan RSA

2.5 Algoritma *Hill Cipher*

Hill cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi.

Prinsip *hill cipher* adalah sebuah matriks dapat digunakan untuk mentransformasikan plainteks menjadi cipherteks. Matriks transformasi merepresentasikan matriks kunci. Untuk melakukan dekripsi, penerima pesan perlu menghitung terlebih dahulu matriks balikan (invers) dari matriks kunci, karena matriks balikan dapat digunakan untuk mentransformasikan cipherteks menjadi plainteks. Matriks balikan hanya dapat dihitung jika mengetahui kunci matriks (Munir, Kriptografi, 2019).

Algoritma enkripsi *hill cipher* diawali dengan menentukan plainteks terlebih dahulu kemudian dikorespondensikan abjad pada plainteks dengan numerik. Setelah itu tentukan kunci dimana kunci adalah sebarang matriks bujursangkar yang memiliki determinan dan invertibel yaitu memiliki *multiplicative inverse* atau K^{-1}. Matriks kunci harus memiliki determinan yang relatif prima dengan nilai modulonya (misalkan 256) atau $\text{PBB}(d, 256) = 1$, dimana 256 merupakan nilai modulo yang diambil dari banyaknya karakter ASCII, nilai modulo juga bisa diambil dari banyaknya huruf abjad (26), atau bisa juga sebagian dari karakter ASCII, seperti 95, 127,…, 256. Setelah itu masukkan plainteks yang kemudian ditranspose sesuai panjang plainteks dan ukuran kolom matriks kunci. Plainteks memiliki ukuran kolom yang sama dengan ukuran baris matriks kunci. Kemudian hitung cipherteks dengan ketentuan:

$$C = K.P \ mod \ N$$

Setelah proses enkripsi dilakukan proses dekripsi. Algoritma dekripsi *hill cipher* dilakukan dengan mengorespondenkan abjad dengan numerik. Langkah kedua cari invers dari matriks kunci dengan rumus:

$$K^{-1} = \bar{\Delta} \ (adj \ K)$$

(Pangaribuan, 2018)

Bila invers matriks kunci pecahan, konversikan kunci matriks menjadi integer. Langkah ketiga masukkan cipherteks, kemudian cipherteks ditranspose sesuai panjang pesan dan ukuran kolom invers matriks kunci. Langkah terakhir yaitu menghitung plainteks, rumus untuk mendapatkan plainteks kembali dapat diperoleh dengan cara sebagai berikut:

Diketahui rumus untuk menghitung cipherteks yaitu $C \equiv K.P \ mod \ N$ menurut definisi kongruensi dapat ditulis dengan $N|C - (K.P)$.

Ada keterbagian bilangan bulat t sehingga dapat dinyatakan dengan

$$C - (K.P) = tN$$

$$-\big(C - (K.P)\big) = -tN$$

$$(K.P) - C = (-t)N$$

Sehingga diperoleh $K.P \equiv C \ mod \ N$

Berdasarkan sifat $ac \equiv bc \ mod \ n$ dan sifat identitas $\bar{A}A \equiv A\bar{A} \equiv I \ mod \ m$, maka diperoleh

$$K^{-1}(K.P) \equiv K^{-1}C \ mod \ N$$

$$(K^{-1}K)P \equiv K^{-1}C \ mod \ N$$

$$I.P \equiv K^{-1}C \ mod \ N$$

Sehingga untuk mendapatkan plainteks kembali menggunakan rumus

$$P \equiv K^{-1}C \ mod \ N$$

Dimana: P = plainteks

C = cipherteks

K = matriks kunci

N = nilai modulo

K^{-1} = invers matriks kunci

$\bar{\Delta}$ = invers determinan K

Contoh

Misalkan pengirim pesan akan mengirim pesan "kirim uang" atau dalam bentuk numerik (spasi diabaikan) menjadi (10, 8, 17, 8, 12, 20, 0, 13, 6). Lakukan enkripsi untuk setiap blok 3-huruf, masing-masing (10, 8, 17), (8, 12, 20), (0, 13, 6). Misalkan $K = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$.

Blok pesan pertama, (10, 8, 17), dienkripsi sebagai

$$C = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 10 \\ 8 \\ 17 \end{pmatrix} mod \ 26 = \begin{pmatrix} 504 \\ 657 \\ 345 \end{pmatrix} mod \ 26 = \begin{pmatrix} 10 \\ 7 \\ 7 \end{pmatrix} = (K, H, H)$$

Blok pesan kedua, (8, 12, 20), dienkripsi sebagai

$$C = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 8 \\ 12 \\ 20 \end{pmatrix} mod\ 26 = \begin{pmatrix} 604 \\ 724 \\ 428 \end{pmatrix} mod\ 26 = \begin{pmatrix} 6 \\ 22 \\ 12 \end{pmatrix} = (G, W, M)$$

Blok pesan ketiga, (0, 13, 6), dienkripsi sebagai

$$C = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 13 \\ 6 \end{pmatrix} mod\ 26 = \begin{pmatrix} 289 \\ 310 \\ 220 \end{pmatrix} mod\ 26 = \begin{pmatrix} 3 \\ 24 \\ 12 \end{pmatrix} = (D, Y, M)$$

Jadi, pesan “kirim uang” dienkripsi menjadi “KHHGW MDYM”

Dekripsi dilakukan dengan persamaan

$$P = K^{-1} C\ mod\ 26$$

Mencari K^{-1} terlebih dahulu

$$\det(K) = 441$$

$$Kofaktor\ (K) = \begin{pmatrix} 70 & 5 & -99 \\ -343 & 70 & 378 \\ 224 & -47 & -216 \end{pmatrix}$$

$$adj(K) = \begin{pmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{pmatrix}$$

$$K^{-1} = \frac{1}{441} \begin{pmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{pmatrix} = 25 \begin{pmatrix} 1750 & 525 & 5600 \\ 125 & 1750 & 125 \\ 125 & 9450 & 450 \end{pmatrix} mod\ 26$$

$$= \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix}$$

Blok cipherteks pertama, (10, 7, 7), didekripsi sebagai

$$P = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 10 \\ 7 \\ 7 \end{pmatrix} mod\ 26 = \begin{pmatrix} 374 \\ 190 \\ 303 \end{pmatrix} mod\ 26 = \begin{pmatrix} 10 \\ 8 \\ 17 \end{pmatrix} = (k, i, r)$$

Blok pesan kedua, (6, 22, 12), didekripsi sebagai

$$P = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 6 \\ 22 \\ 12 \end{pmatrix} mod\ 26 = \begin{pmatrix} 762 \\ 350 \\ 618 \end{pmatrix} mod\ 26 = \begin{pmatrix} 8 \\ 12 \\ 20 \end{pmatrix} = (i, m, u)$$

Blok pesan ketiga, (3, 24, 12), didekripsi sebagai

$$P = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 3 \\ 24 \\ 12 \end{pmatrix} mod\ 26 = \begin{pmatrix} 780 \\ 351 \\ 633 \end{pmatrix} mod\ 26 = \begin{pmatrix} 0 \\ 13 \\ 6 \end{pmatrix} = (a, n, g)$$

Jadi, pesan “KHHGW MDYM” didekripsi kembali menjadi “kirim uang”

2.6 Algoritma RSA

Algoritma *RSA* adalah sebuah algoritma yang bekerja perblok data yang mengelompokkan plainteks menjadi blok-blok terebih dahulu sebelum dilakukan enkripsi sehingga menjadi cipherteks (Ilham, 2018).

Palanisamy mengatakan *RSA* melibatkan kunci publik dan sebuah kunci pribadi. Kunci publik dapat diketahui semua orang dan digunakan untuk mengenkripsi pesan. Kemudian pesan yang dienkripsi dengan kunci publik hanya dapat didekripsi kembali menggunakan kunci pribadi (Pangaribuan, 2018).

Keamanan algoritma *RSA* terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama belum ditemukan algoritma yang mangkus untuk memfaktorkan bilangan bulat yang besar menjadi faktor-faktor primanya, maka selama itu pula keamanan algoritma *RSA* masih tetap terjamin (Munir, Kriptografi, 2019).

Algoritma *RSA* memiliki besaran-besaran sebagai berikut (Munir, Kriptografi, 2019):

1. p dan q bilangan prima (rahasia)
2. $n = p.q$ (tidak rahasia)
3. $\phi(n) = (p-1)(q-1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)
6. m (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

Algoritma Enkripsi dan Dekripsi *RSA*

Algoritma enkripsi *RSA* dirumuskan oleh Paar diawali dengan mengambil kunci publik milik penerima pesan (n dan e). Lalu pecah plainteks menjadi blok-blok m_1, m_2, ... sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang $[0, n-1]$ (Pangaribuan, 2018).

Algoritma RSA didasarkan pada teorema Euler yang menyatakan bahwa

$$a^{\phi(n)} \equiv 1 \ (mod\ n)$$

Dengan syarat:

1. a harus relatif prima terhadap n
2. $\phi(n) = n(1-1/p_1)(1-1/p_2)\ \ldots(1-1/p_r)$, yang dalam hal ini $p_1, p_2, \ldots, p_r$ adalah faktor prima dari n. Fungsi $\phi(n)$ adalah fungsi totient Euler yang menentukan berapa banyak dari bilangan-bilangan $1,2,3, \ldots, n$ yang relatif prima terhadap n.

Berdasarkan sifat $a^k \equiv b^k \ (mod\ n)$ untuk k bilangan bulat ≥ 1, maka dapat ditulis menjadi

$$m^{k\phi(n)} \equiv 1^k (mod\ n)$$

atau

$$m^{k\phi(n)} \equiv 1\ (mod\ n)$$

Bila *a* diganti dengan plainteks *m*, maka dapat ditulis menjadi

$$m^{k\phi(n)+1} \equiv m\ (mod\ n)$$

Misalkan *e* dan *d* dipilih sedemikian sehingga

$$e \cdot d \equiv 1\ (mod\ \phi(n))$$

Atau dapat juga ditulis dalam bentuk kesamaan:

$$e \cdot d = k\phi(n) + 1$$

Masukkan persamaan tersebut kedalam persamaan $m^{k\phi(n)+1} \equiv m\ (mod\ n)$ menjadi :

$$m^{e \cdot d} \equiv m\ (mod\ n)$$

Dapat ditulis kembali menjadi

$$(m^e)^d \equiv m\ (mod\ n)$$

Yang artinya, perpangkatan m dengan e lalu diikuti dengan perpangkatan dengan d menghasilkan kembali P semula. Berdasarkan persamaan tersebut, maka fungsi enkripsi (E) dan fungsi

$$E_e\ (m) = c = m^e\ mod\ n$$

$$D_d\ (c) = m = c^e\ mod\ n$$

Karena $e \cdot d = d \cdot e$, maka enkripsi diikuti dengan dekripsi ekivalen dengan dekripsi diikuti enkripsi:

$$D_d\ (E_e\ (m)) = E_e\ (D_d\ (m)) = m^d\ mod\ n$$

Oleh karena $m^d \bmod n \equiv (m + jn)^d \bmod n$ untuk sembarang bilangan bulat j, maka tiap plainteks $m, m + n, m + 2n, \ldots$, menghasilkan cipherteks yang saman.dengan kata lain, transformasinya satu ke satu, maka m harus dibatasi dalam himpunan $\{0,1,2, \ldots, n - 1\}$ sehingga enkripsi dan dekripsi yang digunakan yaitu:

Enkripsi : $E_e\ (m) = c = m^e\ mod\ n$

Dekripsi : $D_d\ (c) = m = c^e\ mod\ n$

(Munir, Kriptografi, 2019).

Langkah-langkah yang digunakan untuk membangkitkan pasangan kunci di *RSA* dirumuskan oleh Paar yaitu:

1. Pilih dua buah bilangan prima sebarang p dan q. (Rahasiakan p dan q).
2. Hitung: $n = p \times q$, dengan $p \neq q$ dan n tidak rahasia.
3. Hitung $\phi(n) = (p - 1) \times (q - 1)$, dimana $n =$ hasil perkalian dua buah bilangan prima dan $\phi(n) =$ (bilangan prima pertama – 1) dikali (bilangan prima kedua – 1).
4. Pilih kunci publik e, yang relatif prima terhadap $\phi(n)$ atau PBB$\big(e, \phi(n)\big) = 1$, dimana $e \neq (p - 1), e \neq (q - 1)$.
5. Bangkitkan kunci privat d dengan kekongruenan $e.d \equiv 1(mod\ \phi(n))$.

Hasil dari langkah-langkah diatas adalah kunci publik (n, e) dan kunci privat (d, e) (Pangaribuan, 2018).

Perhatikan bahwa $e.d \equiv 1(mod\ \phi(n))$ sehingga d merupakan invers e dalam modulus $\phi(n)$. Cara lain menghitung d adalah dengan menyatakan kekongruenan $e.d \equiv 1(mod\ \phi(n))$ sebagai persamaan $e.d = 1 + k.\phi(n)$, sehingga secara sederhana d dapat dihitung dengan persamaan $d = \frac{1+k.\phi(n)}{e}$ (Munir, Kriptografi, 2019).

Contoh

Misalkan Receiver dan Sender ingin membangkitkan kunci publik dan kunci privatnya masing-masing. Receiver memilih $p = 47$ dan $q = 71$. Selanjutnya Receiver menghitung

$n = p.q = 3337$ dan $\phi(n) = (p-1)(q-1) = 3220$

Receiver memilih kunci publik $e = 79$, karena 79 relatif prima dengan 3220. Receiver mengumumkan nilai e dan n kepada publik. Selanjutnya Receiver menghitung kunci dekripsi d dari kekongruenan $e.d \equiv 1(mod\ \phi(n))$. Maka

$$d = \frac{1 + (k \times 3220)}{79}$$

Dengan mencoba nilai-nilai $k = 1, 2, 3, ...$, diperoleh nilai d yang bulat adalah 1019. Ini adalah kunci privat untuk mendekripsi pesan. Kunci privat ini harus dirahasiakan oleh Receiver. Jadi, perhitungan kunci ini menghasilkan pasangan kunci privat dan kunci publik Receiver:

Kunci publik Receiver: $(e = 79, n = 3337)$

Kunci privat Receiver : $(d = 1019)$

Di sisi lain, Sender memilih dua bilangan prima $p = 83$ dan $q = 61$ untuk membangkitkan kunci privat dan kunci publik miliknya. Sender menghitung

$n = p.q = 5063$ dan $\phi(n) = (p-1)(q-1) = 4920$.

Sender menetapkan $e = 187$, karena 187 relatif prima dengan 4920. Selanjutnya Sender menghitung kunci dekripsi d dari kekongruenan $e.d \equiv 1(mod(\phi(n))$, diperoleh $d = 763$. Jadi, perhitungan kunci ini menghasilkan pasangan kunci privat dan kunci publik Sender:

Kunci publik Sender : $(e = 187, n = 5063)$

Kunci privat Sender : $(d = 763)$

Baik Receiver dan Sender mengumumkan kunci publik mereka masing-masing agar dapat digunakan untuk mengenkripsi pesan yang ditujukan kepada mereka.

Misalkan Sender mengirim plainteks "m", dinyatakan sebagai *integer,* 2671 kepada Receiver (perhatikan bahwa 2671 masih berada didalam selang $[0, 3336]$. Di sisi Sender, enkripsi "m" menjadi ciperteks c sebagai berikut:

$c = m^e mod\ n = 2671^{79} mod\ 3337 \equiv 2081$

Di sisi Receiver, dekripsi c menjadi plainteks semula sebagai berikut:

$m = c^e mod\ n = 2081^{1019} mod\ 3337 \equiv 2671.$

2.7 Kajian Al-Qur'an

Kecurangan merupakan salah satu bentuk perampasan hak kepada orang lain. Larangan untuk melakukan kecurangan juga berlaku pada pengiriman pesan. Seperti yang dijelaskan pada al-Qur'an surat al-A'raf ayat 85, yang artinya:

"Sesungguhnya telah dating padamu bukti yang nyata dari Tuhanmu. Maka sempurnakanlah takaran dan timbangan dan janganlah kamu kurangkan bagi manusia barang-barang takaran dan timbangannya, dan janganlah kamu berbuat kerusakan di muka bumi sesudah Tuhan memperbaikinya. Yang demikian itu lebih baik bagimu jika betul-betul kamu orang yang beriman"(al-A'raf/8:85).

Ayat tersebut membahas mengenai annjuran untuk menjaga dan menyampaikan pesan dengan sebenar-benarnya, tanpa mengurangi ataupun menambah isi pesan memastikan pesan tersebut tersampaikan dengan baik kepada orang berhak menerimanya. Oleh karena itu, untuk menghindari kecurangan dalam menyampaikan pesan perlu digunakan teknik penyandian pesan seperti teknik kriptografi hibrida. Teknik kriptografi hibrida merupakan teknik penggabungan dari dua algoritma yaitu algoritma simetri menggunakan metode *hill cipher* yang akan digunakan untuk mengamankan pesan dengan mengubah pesan asli (plainteks) menjadi pesan yang tidak dapat dimengerti maknanya (cipherteks). Kemudian, algoritma asimetri menggunakan metode RSA yang akan digunakan untuk mengamankan kunci pesan dengan mengubah kunci pesan asli kedalam bentuk yang lain. Dengan penggabungan dua algoritma tersebut diharapkan dapat menjaga keamanan pesan dengan lebih baik, sehingga tetap terjaga keamanannya dari orang yang tidak berhak menerimanya.

BAB III

PEMBAHASAN

Kriptografi hibrida merupakan gabungan dari kriptografi simetri dan kriptografi asimetri, dimana pada penelitian ini metode yang akan digunakan adalah algoritma *hill cipher* dari kriptografi simetri yang kunci enkripsinya sama dengan kunci dekripsi dan algoritma RSA dari kriptografi asimetri yang kunci enkripsinya tidak sama dengan kunci dekripsi. Pada pembahsan kali ini akan diambil sampel berupa pesan teks untuk mengetahui keamanan suatu pesan. Peneliti akan menjabarkan proses kriptografi hibrida menggunakan metode *hill* cipher dan RSA dengan sampel pesan yang sudah ditentukan peneliti.

Perlu diketahui, sebelum membahas mengenai proses enkripsi dan dekripsi menggunakan algoritma *hill cipher* dan RSA. Diperlukan pembangkit pasangan kunci yang diberikan oleh pengirim pesan, yang nantinya akan digunakan oleh pengirim pesan untuk mengenkripsi kunci *hill cipher*. Pembangkit ini memiliki sifat umum (dapat diketahui semua orang) dan sifat rahasia yang hanya diketahui oleh orang tertentu atua penerima pesan. Langkah-langkah yang diperlukan untuk membangkitkan pasangan kunci diantaranya:

1. Menentukan dua buah sebarang bilangan prima yang bersifat rahasia.

   Misalkan: $p = 19$ dan $q = 23$

2. Menghitung nilai $n = p \times q$. (sebaiknya $p \neq q$, sebab jika $p = q$ maka $n = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n). nilai n tidak bersifat rahasia karena n diperlukan pada perhitungan enkripsi dan dekripsi.

Sehingga: $n = p \times q$.

$$= 19 \times 23 = 437$$

3. Menghitung nilai $\phi(n) = (\mathrm{p} - 1) \times (\mathrm{q} - 1)$, dimana $\phi(n)$ bersifat rahasia.

   Sehingga: $\phi(n) = (\mathrm{p} - 1) \times (\mathrm{q} - 1)$.

   $$= 18 \times 22 = 396$$

4. Memilih kunci publik yang relatif prima terhadap $\phi(n)$.

   Misalkan kunci publik = *e*, dimana e yang memenuhi $\phi(n)\ modulo\ e$ bersisa 1. Dapat ditulis dengan:

   $\mathrm{PBB}\big(e, \phi(n)\big) = 1, \qquad dimana\ 1 < e < \phi(n)$

   $\mathrm{PBB}(e, 396) = 1, \qquad 1 < e < 396$

   $396\ mod\ 5 = 1$

   Sehingga diperoleh nilai $e = 5$

5. Menghitung kunci privat (*d*) dengan kekongruenan $e.d\ mod\ \phi(n) = 1$ atau dengan $d = \frac{1+k.\phi(n)}{e}$.

   Dengan mencoba nilai-nilai $k = 1, 2, 3, \ldots$ diperoleh nilai d yang bulat adalah 317.

Maka, dari langkah-langkah tersebut akan didapatkan pasangan kunci publik $(e, n) = (5, 437)$ yang akan diumumkan kepada orang lain atau pengirim pesan dan pasangan kunci privat $(d, n) = (317, 437)$ yang akan dirahasiakan oleh penerima pesan.

3.1 Proses Enkripsi Algoritma *Hill Cipher* dan Enkripsi Kunci *Hill Cipher* Menggunakan Algoritma RSA.

1. Menentukan pesan (plainteks) yang akan dikirimkan kepada penerima.

   Yaitu: "**berakhirnya masa pandemi COVID19**"

2. *K* adalah parameter yang digunakan sebagai kunci matriks pada enkripsi pesan yang elemen-elemennya merupakan bilangan bulat dan memiliki invers untuk proses dekripsi pesan maka haruslah $\det(\boldsymbol{K}_{n\times n}) \neq 0$.

   $$\boldsymbol{K}_{n\times n} = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{bmatrix} \text{ dimana } k_{11}, k_{12}, k_{12}, \dots, k_{nn} \in \mathbb{Z}$$

   Sehingga ditentukan kunci enkripsi dengan matriks 3×3.

   $$K = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix}$$

3. Memasangkan plainteks sesuai dengan urutannya menjadi beberapa blok dimana panjang kolom dan baris tiap bloknya sama. Kemudian konversikan masing-masing karakter kedalam bilangan ASCII yang bersesuaian. Setiap blok terdiri dari 3 huruf yang disusun dalam bentuk matriks 3×1.

   $$\begin{pmatrix} b \\ e \\ r \end{pmatrix} = \begin{pmatrix} 98 \\ 101 \\ 114 \end{pmatrix}, \quad \begin{pmatrix} a \\ k \\ h \end{pmatrix} = \begin{pmatrix} 97 \\ 107 \\ 104 \end{pmatrix}, \quad \begin{pmatrix} i \\ r \\ n \end{pmatrix} = \begin{pmatrix} 105 \\ 114 \\ 110 \end{pmatrix},$$

   $$\begin{pmatrix} y \\ a \\ space \end{pmatrix} = \begin{pmatrix} 121 \\ 97 \\ 32 \end{pmatrix}, \quad \begin{pmatrix} m \\ a \\ s \end{pmatrix} = \begin{pmatrix} 109 \\ 97 \\ 115 \end{pmatrix}, \quad \begin{pmatrix} a \\ space \\ p \end{pmatrix} = \begin{pmatrix} 97 \\ 32 \\ 112 \end{pmatrix},$$

   $$\begin{pmatrix} a \\ n \\ d \end{pmatrix} = \begin{pmatrix} 97 \\ 110 \\ 100 \end{pmatrix}, \quad \begin{pmatrix} e \\ m \\ i \end{pmatrix} = \begin{pmatrix} 101 \\ 109 \\ 105 \end{pmatrix}, \quad \begin{pmatrix} space \\ C \\ O \end{pmatrix} = \begin{pmatrix} 32 \\ 67 \\ 79 \end{pmatrix},$$

   $$\begin{pmatrix} V \\ I \\ D \end{pmatrix} = \begin{pmatrix} 86 \\ 73 \\ 68 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 9 \\ X \end{pmatrix} = \begin{pmatrix} 49 \\ 57 \\ 88 \end{pmatrix}$$

4. S adalah hasil perkalian kunci matriks ($\boldsymbol{K}$) dengan tiap-tiap blok yang hasilnya dimodulo 127. Kemudian matriks $\boldsymbol{S}_{n\times m}$ ditambahkan dengan skalar 32.

   a. $\begin{pmatrix} b \\ e \\ r \end{pmatrix} \rightarrow \begin{pmatrix} 98 \\ 101 \\ 114 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 98 \\ 101 \\ 114 \end{pmatrix} = \begin{pmatrix} 427 \\ 936 \\ 708 \end{pmatrix} mod\ 127 \rightarrow$

   $\begin{pmatrix} 46 \\ 47 \\ 73 \end{pmatrix} + 32 = \begin{pmatrix} 78 \\ 79 \\ 105 \end{pmatrix} = \begin{pmatrix} N \\ O \\ i \end{pmatrix}$

   b. $\begin{pmatrix} a \\ k \\ h \end{pmatrix} \rightarrow \begin{pmatrix} 97 \\ 107 \\ 104 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 97 \\ 107 \\ 104 \end{pmatrix} = \begin{pmatrix} 412 \\ 914 \\ 706 \end{pmatrix} mod\ 127 \rightarrow$

   $\begin{pmatrix} 31 \\ 25 \\ 71 \end{pmatrix} + 32 = \begin{pmatrix} 63 \\ 57 \\ 103 \end{pmatrix} = \begin{pmatrix} ? \\ 9 \\ g \end{pmatrix}$

   c. $\begin{pmatrix} i \\ r \\ n \end{pmatrix} \rightarrow \begin{pmatrix} 105 \\ 114 \\ 110 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 105 \\ 114 \\ 110 \end{pmatrix} = \begin{pmatrix} 439 \\ 978 \\ 758 \end{pmatrix} mod\ 127 \rightarrow$

   $\begin{pmatrix} 58 \\ 89 \\ 123 \end{pmatrix} + 32 = \begin{pmatrix} 90 \\ 121 \\ 155 \end{pmatrix} = \begin{pmatrix} Z \\ y \\ \text{ø} \end{pmatrix}$

   d. $\begin{pmatrix} y \\ a \\ space \end{pmatrix} \rightarrow \begin{pmatrix} 121 \\ 97 \\ 32 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 121 \\ 97 \\ 32 \end{pmatrix} = \begin{pmatrix} 282 \\ 774 \\ 710 \end{pmatrix} mod\ 127 \rightarrow$

   $\begin{pmatrix} 28 \\ 12 \\ 75 \end{pmatrix} + 32 = \begin{pmatrix} 60 \\ 44 \\ 107 \end{pmatrix} = \begin{pmatrix} < \\ , \\ k \end{pmatrix}$

   e. $\begin{pmatrix} m \\ a \\ s \end{pmatrix} \rightarrow \begin{pmatrix} 109 \\ 97 \\ 115 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 109 \\ 97 \\ 115 \end{pmatrix} = \begin{pmatrix} 436 \\ 975 \\ 745 \end{pmatrix} mod\ 127 \rightarrow$

   $\begin{pmatrix} 55 \\ 86 \\ 110 \end{pmatrix} + 32 = \begin{pmatrix} 87 \\ 118 \\ 142 \end{pmatrix} = \begin{pmatrix} W \\ v \\ Ä \end{pmatrix}$

f. $\begin{pmatrix} a \\ space \\ p \end{pmatrix} \rightarrow \begin{pmatrix} 97 \\ 32 \\ 112 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 97 \\ 32 \\ 112 \end{pmatrix} = \begin{pmatrix} 353 \\ 788 \\ 564 \end{pmatrix} mod\ 127 \rightarrow$

$\begin{pmatrix} 99 \\ 26 \\ 56 \end{pmatrix} + 32 = \begin{pmatrix} 131 \\ 58 \\ 88 \end{pmatrix} = \begin{pmatrix} \hat{a} \\ : \\ X \end{pmatrix}$

g. $\begin{pmatrix} a \\ n \\ d \end{pmatrix} \rightarrow \begin{pmatrix} 97 \\ 110 \\ 100 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 97 \\ 110 \\ 100 \end{pmatrix} = \begin{pmatrix} 407 \\ 908 \\ 708 \end{pmatrix} mod\ 127 \rightarrow$

$\begin{pmatrix} 26 \\ 19 \\ 73 \end{pmatrix} + 32 = \begin{pmatrix} 58 \\ 51 \\ 105 \end{pmatrix} = \begin{pmatrix} : \\ 3 \\ i \end{pmatrix}$

h. $\begin{pmatrix} e \\ m \\ i \end{pmatrix} \rightarrow \begin{pmatrix} 101 \\ 109 \\ 105 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 101 \\ 109 \\ 105 \end{pmatrix} = \begin{pmatrix} 420 \\ 937 \\ 727 \end{pmatrix} mod\ 127 \rightarrow$

$\begin{pmatrix} 39 \\ 48 \\ 92 \end{pmatrix} + 32 = \begin{pmatrix} 71 \\ 80 \\ 124 \end{pmatrix} = \begin{pmatrix} G \\ P \\ \vert \end{pmatrix}$

i. $\begin{pmatrix} space \\ C \\ O \end{pmatrix} \rightarrow \begin{pmatrix} 32 \\ 67 \\ 79 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 32 \\ 67 \\ 79 \end{pmatrix} = \begin{pmatrix} 257 \\ 499 \\ 341 \end{pmatrix} mod\ 127 \rightarrow$

$\begin{pmatrix} 3 \\ 118 \\ 87 \end{pmatrix} + 32 = \begin{pmatrix} 35 \\ 150 \\ 119 \end{pmatrix} = \begin{pmatrix} \# \\ \hat{u} \\ w \end{pmatrix}$

j. $\begin{pmatrix} V \\ I \\ D \end{pmatrix} \rightarrow \begin{pmatrix} 86 \\ 73 \\ 68 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 86 \\ 73 \\ 68 \end{pmatrix} = \begin{pmatrix} 295 \\ 694 \\ 558 \end{pmatrix} mod\ 127 \rightarrow$

$\begin{pmatrix} 41 \\ 59 \\ 50 \end{pmatrix} + 32 = \begin{pmatrix} 73 \\ 91 \\ 82 \end{pmatrix} = \begin{pmatrix} I \\ [\\ R \end{pmatrix}$

k. $\begin{pmatrix} 1 \\ 9 \\ X \end{pmatrix} \rightarrow \begin{pmatrix} 49 \\ 57 \\ 88 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 49 \\ 57 \\ 88 \end{pmatrix} = \begin{pmatrix} 282 \\ 574 \\ 398 \end{pmatrix} mod\ 127 \rightarrow$

$\begin{pmatrix} 28 \\ 66 \\ 17 \end{pmatrix} + 32 = \begin{pmatrix} 60 \\ 98 \\ 49 \end{pmatrix} = \begin{pmatrix} < \\ b \\ 1 \end{pmatrix}$

5. Cipherteks ($\boldsymbol{C}$) merupakan pesan yang sudah dienkripsi dan dikonversikan kembali sesuai kode ASCII.

   Sehingga didapatkan hasil cipherteks.

   "**NOi?9gZyø<,kWvÄâ:X:3iGP|#ûwI[R<b1**"

6. Menerima pembangkit pasangan kunci publik dari penerima pesan untuk mengenkripsi kunci *hill cipher*, sehingga didapatkan kunci publik $(e, n) = (5, 437)$.

7. Membagi kunci *hill cipher* yang aslinya berbentuk matriks menjadi blok-blok m_1, m_2, ..., dan diubah menjadi bilangan bulat positif m_i sedemikian sehingga setiap blok m_i merepresentasikan nilai di dalam selang $[0, n-1]$.

   Disini pengirim akan membagi kunci *hill cipher* menjadi 3 blok.

   $m_1 = 112,$ $m_2 = 423,$ $m_3 = 421.$

8. Mengenkripsi setiap blok dengan memangkatkan kunci *hill cipher* dengan kunci publik (e) dimodulo dengan n, dapat juga dirumuskan dengan $h_i = m_i^e \ mod \ n$.

   Sehingga didapatkan:

   a) $h_1 = 112^5 \ mod \ 437 = 424$

   b) $h_2 = 423^5 \ mod \ 437 = 123$

   c) $h_3 = 421^5 \ mod \ 437 = 224$

9. Enkripsi kunci *hill cipher* yang didapatkan dari perhitungan sebelumnya dikembalikan lagi dalam bentuk matrik 3×3, menjadi:

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

Setelah mendapatkan hasil enkripsi pesan dalam bentuk cipherteks dan hasil enkripsi kunci *hill cipher* dalam bentuk matriks, kemudian hasil dari enkripsi tersebut dikirimkan kepada penerima pesan.

3.2 Proses Dekripsi Kunci *Hill Cipher* Menggunakan Algoritma RSA dan Dekripsi Algoritma *Hill Cipher*

1. Menerima enkripsi kunci *hill cipher* dari pengirim pesan.

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

2. Membagi kunci *hill cipher* yang aslinya berbentuk matriks menjadi blok-blok $h_1, h_2, ...$, dan diubah menjadi bilangan bulat positif h_i sedemikian sehingga setiap blok h_i merepresentasikan nilai di dalam selang $[0, n-1]$.

   Disini pengirim akan membagi kunci *hill cipher* menjadi 3 blok.

   $h_1 = 424,$ $h_2 = 123,$ $h_3 = 224.$

3. Mendapatkan kembali kunci *hill cipher* dengan memangkatkan setiap blok dari enkripsi kunci *hill cipher* dengan kunci privat (d) dimodulo dengan n, dapat juga dirumuskan dengan $m_i = h_i^d \ mod \ n$.

   Sehingga didapatkan:

   a) $m_1 = 424^{317} \ mod \ 437 = 112$

   b) $m_2 = 123^{317} \ mod \ 437 = 423$

   c) $m_3 = 224^{317} \ mod \ 437 = 421$

4. Didapatkan kembali kunci *hill cipher* dan diubah kembali dalam bentuk matriks 3×3..

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

5. Menerima pesan dalam bentuk cipherteks dari pengirim pesan yang berisi:

   "**NOi?9gZyø<,kWvÄâ:X:3iGP|#ûwI[R<b1**"

6. K adalah parameter yang digunakan sebagai kunci matriks pada enkripsi pesan dan untuk memperoleh pesan kembali pada proses dekripsi maka $K_{n\times n}$ harus mempunyai invers yang dilambangkan dengan K^{-1}, maka untuk mendapatkan invers matriks haruslah $\det(K_{n\times n}) \neq 0$ dan elemen-elemen invers kunci matriks K^{-1} adalah bilangan bulat.

   Berikut adalah proses untuk mendapatkan invers kunci matrks:

   $$K = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix}$$

   Misalkan $\det K = \Delta$, sehingga $invers \det K = \bar{\Delta}$

   Dengan rumus invers $K^{-1} = \bar{\Delta}\ [adj\ K]$, Maka diperlukan

   $$\det K = (2 + 12 + 16) - (16 + 6 + 4) = 30 - 26 = 4$$

   Mencari invers $\det K$ dengan rumus invers modulo $\Delta\bar{\Delta} \equiv 1\ (mod\ n)$, sehingga dengan $4\bar{\Delta} \equiv 1\ mod\ 127$

   Diperoleh $\bar{\Delta} = 32$

   Dengan $kofaktor\ K = \begin{bmatrix} -4 & 8 & 0 \\ 3 & -7 & 2 \\ -1 & 5 & -2 \end{bmatrix}$

   Maka diperoleh $adj\ K = \begin{bmatrix} -4 & 3 & -1 \\ 8 & -7 & 5 \\ 0 & 2 & -2 \end{bmatrix}$

   $$K^{-1} = 32\begin{bmatrix} -4 & 3 & -1 \\ 8 & -7 & 5 \\ 0 & 2 & -2 \end{bmatrix} = \begin{bmatrix} -128 & 96 & -32 \\ 256 & -224 & 160 \\ 0 & 64 & -64 \end{bmatrix} mod\ 127$$

   $$= \begin{bmatrix} 126 & 96 & 95 \\ 2 & 30 & 33 \\ 0 & 64 & 63 \end{bmatrix}$$

   Sehingga, dari proses tersebut didapatkan:

$$K^{-1} = \begin{bmatrix} 126 & 96 & 95 \\ 2 & 30 & 33 \\ 0 & 64 & 63 \end{bmatrix}$$

7. Memasangkan plainteks sesuai dengan urutannya menjadi beberapa blok, setiap blok terdiri dari 3 huruf yang disusun dalan bentuk matriks 3×1. Kemudian konversikan masing-masing karakter kedalam bilangan ASCII yang bersesuaian.

$\begin{pmatrix} N \\ O \\ i \end{pmatrix} = \begin{pmatrix} 78 \\ 79 \\ 105 \end{pmatrix}, \begin{pmatrix} ? \\ 9 \\ g \end{pmatrix} = \begin{pmatrix} 63 \\ 57 \\ 103 \end{pmatrix}, \quad \begin{pmatrix} Z \\ y \\ ø \end{pmatrix} = \begin{pmatrix} 90 \\ 121 \\ 155 \end{pmatrix},$

$\begin{pmatrix} ; \\ j \\ + \end{pmatrix} = \begin{pmatrix} 59 \\ 106 \\ 43 \end{pmatrix}, \begin{pmatrix} W \\ v \\ \ddot{A} \end{pmatrix} = \begin{pmatrix} 87 \\ 118 \\ 142 \end{pmatrix}, \quad \begin{pmatrix} C \\ 9 \\ W \end{pmatrix} = \begin{pmatrix} 67 \\ 57 \\ 87 \end{pmatrix},$

$\begin{pmatrix} ; \\ 3 \\ i \end{pmatrix} = \begin{pmatrix} 58 \\ 51 \\ 105 \end{pmatrix}, \begin{pmatrix} G \\ P \\ \vert \end{pmatrix} = \begin{pmatrix} 71 \\ 80 \\ 124 \end{pmatrix}, \quad \begin{pmatrix} b \\ \ddot{o} \\ u \end{pmatrix} = \begin{pmatrix} 98 \\ 148 \\ 117 \end{pmatrix},$

$\begin{pmatrix} I \\ [\\ R \end{pmatrix} = \begin{pmatrix} 73 \\ 91 \\ 82 \end{pmatrix}, \quad \begin{pmatrix} < \\ b \\ 1 \end{pmatrix} = \begin{pmatrix} 60 \\ 98 \\ 49 \end{pmatrix},$

8. $F_{n\times m}$ adalah matriks hasil pengurangan skalar 32 dari tiap-tiap blok. Kemudian mengalikan invers kunci matriks $K_{n\times n}^{-1}$ dengan matriks $F_{n\times m}$ dan hasilnya dimodulo 127.

a. $\begin{pmatrix} N \\ O \\ i \end{pmatrix} \rightarrow \begin{pmatrix} 78 \\ 79 \\ 105 \end{pmatrix} - 32 = \begin{pmatrix} 46 \\ 47 \\ 73 \end{pmatrix} \rightarrow \begin{pmatrix} 126 & 96 & 95 \\ 2 & 30 & 33 \\ 0 & 64 & 63 \end{pmatrix} \begin{pmatrix} 46 \\ 47 \\ 73 \end{pmatrix} mod\ 127 =$

$\begin{pmatrix} 17243 \\ 3911 \\ 7607 \end{pmatrix} mod\ 127 = \begin{pmatrix} 98 \\ 101 \\ 114 \end{pmatrix} = \begin{pmatrix} b \\ e \\ r \end{pmatrix}$

b. $\begin{pmatrix}?\\9\\g\end{pmatrix} \rightarrow \begin{pmatrix}63\\57\\103\end{pmatrix} - 32 = \begin{pmatrix}31\\25\\71\end{pmatrix} \rightarrow \begin{pmatrix}126 & 96 & 95\\2 & 30 & 33\\0 & 64 & 63\end{pmatrix}\begin{pmatrix}31\\25\\71\end{pmatrix} mod\ 127 =$

$\begin{pmatrix}13051\\3155\\6073\end{pmatrix} mod\ 127 = \begin{pmatrix}97\\107\\104\end{pmatrix} = \begin{pmatrix}a\\k\\h\end{pmatrix}$

c. $\begin{pmatrix}Z\\y\\ø\end{pmatrix} \rightarrow \begin{pmatrix}90\\121\\155\end{pmatrix} - 32 = \begin{pmatrix}58\\89\\123\end{pmatrix} \rightarrow \begin{pmatrix}126 & 96 & 95\\2 & 30 & 33\\0 & 64 & 63\end{pmatrix}\begin{pmatrix}58\\89\\123\end{pmatrix} mod\ 127 =$

$\begin{pmatrix}27537\\6845\\13445\end{pmatrix} mod\ 127 = \begin{pmatrix}105\\114\\110\end{pmatrix} = \begin{pmatrix}i\\r\\n\end{pmatrix}$

d. $\begin{pmatrix}<\\,\\k\end{pmatrix} \rightarrow \begin{pmatrix}60\\44\\107\end{pmatrix} - 32 = \begin{pmatrix}28\\12\\75\end{pmatrix} \rightarrow \begin{pmatrix}126 & 96 & 95\\2 & 30 & 33\\0 & 64 & 63\end{pmatrix}\begin{pmatrix}28\\12\\75\end{pmatrix} mod\ 127 =$

$\begin{pmatrix}11805\\2891\\5493\end{pmatrix} mod\ 127 = \begin{pmatrix}121\\97\\32\end{pmatrix} = \begin{pmatrix}y\\a\\space\end{pmatrix}$

e. $\begin{pmatrix}W\\v\\\ddot{A}\end{pmatrix} \rightarrow \begin{pmatrix}87\\118\\142\end{pmatrix} - 32 = \begin{pmatrix}55\\86\\110\end{pmatrix}\begin{pmatrix}126 & 96 & 95\\2 & 30 & 33\\0 & 64 & 63\end{pmatrix}\begin{pmatrix}55\\86\\110\end{pmatrix} mod\ 127 =$

$\begin{pmatrix}25636\\6320\\12434\end{pmatrix} mod\ 127 = \begin{pmatrix}109\\97\\115\end{pmatrix} = \begin{pmatrix}m\\a\\s\end{pmatrix}$

f. $\begin{pmatrix}\hat{a}\\:\\X\end{pmatrix} \rightarrow \begin{pmatrix}131\\58\\88\end{pmatrix} - 32 = \begin{pmatrix}99\\26\\56\end{pmatrix} \rightarrow \begin{pmatrix}126 & 96 & 95\\2 & 30 & 33\\0 & 64 & 63\end{pmatrix}\begin{pmatrix}99\\26\\56\end{pmatrix} mod\ 127 =$

$\begin{pmatrix}20290\\2826\\5192\end{pmatrix} mod\ 127 = \begin{pmatrix}97\\32\\112\end{pmatrix} = \begin{pmatrix}a\\space\\p\end{pmatrix}$

g. $\begin{pmatrix};\\3\\i\end{pmatrix} \rightarrow \begin{pmatrix}58\\51\\105\end{pmatrix} - 32 = \begin{pmatrix}26\\19\\73\end{pmatrix} \rightarrow \begin{pmatrix}126 & 96 & 95\\2 & 30 & 33\\0 & 64 & 63\end{pmatrix}\begin{pmatrix}26\\19\\73\end{pmatrix} mod\ 127 =$

$\begin{pmatrix}12035\\3031\\5815\end{pmatrix} mod\ 127 = \begin{pmatrix}97\\110\\100\end{pmatrix} = \begin{pmatrix}a\\n\\d\end{pmatrix}$

h. $\begin{pmatrix} G \\ P \\ | \end{pmatrix} \rightarrow \begin{pmatrix} 71 \\ 80 \\ 124 \end{pmatrix} - 32 = \begin{pmatrix} 39 \\ 48 \\ 92 \end{pmatrix} \rightarrow \begin{pmatrix} 126 & 96 & 95 \\ 2 & 30 & 33 \\ 0 & 64 & 63 \end{pmatrix} \begin{pmatrix} 39 \\ 48 \\ 92 \end{pmatrix} mod\ 127 =$

$\begin{pmatrix} 18262 \\ 4554 \\ 8868 \end{pmatrix} mod\ 127 = \begin{pmatrix} 101 \\ 109 \\ 105 \end{pmatrix} = \begin{pmatrix} e \\ m \\ i \end{pmatrix}$

i. $\begin{pmatrix} \# \\ \hat{u} \\ w \end{pmatrix} \rightarrow \begin{pmatrix} 35 \\ 150 \\ 19 \end{pmatrix} - 32 = \begin{pmatrix} 3 \\ 118 \\ 87 \end{pmatrix} \begin{pmatrix} 126 & 96 & 95 \\ 2 & 30 & 33 \\ 0 & 64 & 63 \end{pmatrix} \begin{pmatrix} 3 \\ 118 \\ 87 \end{pmatrix} mod\ 127 =$

$\begin{pmatrix} 19971 \\ 6417 \\ 13033 \end{pmatrix} mod\ 127 = \begin{pmatrix} 32 \\ 67 \\ 79 \end{pmatrix} = \begin{pmatrix} space \\ C \\ O \end{pmatrix}$

j. $\begin{pmatrix} I \\ [\\ R \end{pmatrix} \rightarrow \begin{pmatrix} 73 \\ 91 \\ 82 \end{pmatrix} - 32 = \begin{pmatrix} 41 \\ 59 \\ 50 \end{pmatrix} \rightarrow \begin{pmatrix} 126 & 96 & 95 \\ 2 & 30 & 33 \\ 0 & 64 & 63 \end{pmatrix} \begin{pmatrix} 41 \\ 59 \\ 50 \end{pmatrix} mod\ 127 =$

$\begin{pmatrix} 15580 \\ 3502 \\ 6926 \end{pmatrix} mod\ 127 = \begin{pmatrix} 86 \\ 73 \\ 68 \end{pmatrix} = \begin{pmatrix} V \\ I \\ D \end{pmatrix}$

k. $\begin{pmatrix} < \\ b \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} 60 \\ 98 \\ 49 \end{pmatrix} - 32 = \begin{pmatrix} 28 \\ 66 \\ 17 \end{pmatrix} \rightarrow \begin{pmatrix} 126 & 96 & 95 \\ 2 & 30 & 33 \\ 0 & 64 & 63 \end{pmatrix} \begin{pmatrix} 28 \\ 66 \\ 17 \end{pmatrix} mod\ 127 =$

$\begin{pmatrix} 11479 \\ 2597 \\ 5295 \end{pmatrix} mod\ 127 = \begin{pmatrix} 49 \\ 57 \\ 88 \end{pmatrix} = \begin{pmatrix} 1 \\ 9 \\ X \end{pmatrix}$

9. Hasil dari perkalian tersebut akan dikonversikan kedalam tabel ASCII sehingga didapatkan plainteks.

   "**berakhirnya masa pandemik COVID19**"

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan pembahasan sebelumnya, maka dapat diambil kesimpulan sebagai berikut:

1. Proses enkripsi menggunakan algoritma *hill cipher* dan RSA dimulai dengan proses penyandian pesan asli (plainteks) menjadi pesan yang berbeda maknanya (cipherteks) menggunakan algoritma *hill cipher*. Kemudian, dilanjutkan dengan proses penyandian kunci pesan menghasilkan kunci yang berbeda menggunakan algoritma RSA. Sehingga diperoleh cipherteks dan hasil enkripsi kunci pesan. Berdasarkan hasil dari proses enkripsi, diperoleh kesimpulan bahwa keamanan pesan terletak pada kerahasiaan kunci pesan, semakin besar ukuran kunci matriks yang digunakan maka waktu yang diperlukan semakin banyak. Sehingga untuk memperkuat keamanan pesan digunakan RSA untuk mengamankan kunci pesan, dimana RSA memiliki duakunci yaitu kunci publik dan kunci privat. Jumlah karakter yang digunakan proses enkripsi juga berpengaruh pada hasil enkripsi pesan. Semakin banyak karakter yang digunakan, maka karakter yang muncul pada hasil enkripsi semakin bervariasi.
2. Penerima pesan perlu menentukan pembangkit pasangan kunci yang menghasilkan kunci publik dan kunci privat, kunci publik bersifat umum atau dapat diketahui banyak orang yang akan digunakan pada proses enkrispi pesan, sedangkan kunci privat bersifat rahasia atau hanya dapat diketahui oleh penerima pesan yang akan digunakan pada proses dekripsi pesan.

Selanjutnya, pada proses dekripsi menggunakan algoritma *hill cipher* dan RSA dimulai dengan mengembalikan hasil enkripsi kunci pesan kedalam kunci pesan yang semula menggunakan algoritma RSA. Kemudian, menemukan invers kunci pesan yang digunakan untuk mendekripsi cipherteks agar dapat kembali kedalam bentuk pesan asli (plainteks) menggunkan algoritma *hill cipher*. Berdasarkan hasil dari proses dekripsi, dapat diambil kesimpulan bahwa keamanan enkripsikunci 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 semakin lama.

4.2 Saran

Pada penelitian ini membahas tentang kriptografi algoritma hibrida menggunakan metode *hill cipher* dan RSA serta implementasi kedalam suatu pesan. Adapun saran untuk penelitian selanjutnya yaitu dapat menggunakan metode penyandian yang lain sehingga dapat mengetahui metode atau cara penyandian pesan dengan tingkat keamanan yang berbeda. Bisa juga dengan memperkuat tingkat keamanan kunci pesan dengan memperbesar ukuran matriks dan nilai bilangan prima pada proses RSA sehingga dapat mempersulit untuk diketahui pesan aslinya.

DAFTAR PUSTAKA

Al-Qur'an Terjemah. (2015). *Departemen Agama RI*. Bandung: CV Darus Sunnah.

Anton, H. (2000). *Dasar-dasar Aljabar Linear*. Tangerang: Binarupa Aksara Publisher.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi.* Yogyakarta: CV. ANDI OFFSET.

Ilham. (2018). Analisis dan Desain Algoritma Hybrid Kriptografi untuk Manajemen Strategi Pengamanan Data Perusahaan. *Jurnal Teknologi Proses dan Inovasi Industri*, 51-56.

Irawan, W. H., & dkk. (2014). *Pengantar Teori Bilangan.* Malang: UIN-Maliki Press.

Jamaludin. (2018). Rancangan Bangun Kombinasi Hill Cipher dan RSA Mwnggunakan Metode Hybrid Cryptosystem. *Publikasi Jurnal & Penelitian Teknik Informatika*, 86-93.

Lajnah Pentashihan Mushaf Al-Qur'an. (2009). *Tafsir Al-Qur'an Tematik Jilid 3.* Jakarta: Kamil Pustaka.

Munir, R. (2012). *Matematika Diskrit.* Bandung: INFORMATIKA.

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

Pangaribuan, L. J. (2018). Kriptografi Hybrida Algoritma Hill Cipher dan Rivest Shamir Adleman (RSA) Sebagai Pengembangan Kriptografi Kunci Simetris. *Jurnal Teknologi Informasi dan Komunikasi*, 11-16.

Rosen, K. H. (1986). *Elementary Number Theory and Its Applications.* Canada: Addison-Wealey.

Sadikin, R. (2012). *Kriptografi untuk keamanan jaringan.* Yogyakarta: Penerbit ANDI.

Suhandinata, S., & dkk. (2019). Analisis Performa Kriptografi Hybrid Algoritma Blowfish dan Algoritma RSA. *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)*, 1-10.

LAMPIRAN

Lampiran 1. Tabel ASCII

ASCII control characters					
DEC	Binary	Simbol ASCII	DEC	Binary	Simbol ASCII
00	00000000	NULL	16	00010000	DLE
01	00000001	SOH	17	00010001	DC1
02	00000010	STX	18	00010010	DC2
03	00000010	ETX	19	00010011	DC3
04	00000100	EOT	20	00010100	DC4
05	00000101	ENQ	21	00010101	NAK
06	00000110	ACK	22	00010110	SYN
07	00000111	BEL	23	00010111	ETB
08	00001000	BS	24	00011000	CAN
09	00001001	HT	25	00011001	EM
10	00001010	LF	26	00011010	SUB
11	00001011	VT	27	00011011	ESC
12	00001100	FF	28	00011100	FS
13	00001101	CR	29	00011101	GS
14	00001110	SO	30	00011110	RS
15	00001111	SI	31	00011111	US

ASCII printable characters					
DEC	Binary	Simbol ASCII	DEC	Binary	Simbol ASCII
32	00100000	Space	80	01010000	P
33	00100001	!	81	01010001	Q
34	00100010	“	82	01010010	R
35	00100011	#	83	01010011	S
36	00100100	$	84	01010100	T
37	00100101	%	85	01010101	U

38	00100110	&	86	01010110	V
39	00100111	‘	87	01010111	W
40	00101000	(	88	01011000	X
41	00101001	)	89	01011001	Y
42	00101010	*	90	01011010	Z
43	00101011	+	91	01011011	[
44	00101100	,	92	01011100	\
45	00101101	-	93	01011101	]
46	00101110	.	94	01011110	^
47	00101111	/	95	01011111	_
48	00110000	0	96	01100000	`
49	00110001	1	97	01100001	a
50	00110010	2	98	01100010	b
51	00110011	3	99	01100011	c
52	00110100	4	100	01100100	d
53	00110101	5	101	01100101	e
54	00110110	6	102	01100110	f
55	00110111	7	103	01100111	g
56	00111000	8	104	01101000	h
57	00111001	9	105	01101001	i
58	00111010	:	106	01101010	j
59	00111011	;	107	01101011	k
60	00111100	<	108	01101100	l
61	00111101	=	109	01101101	m
62	00111110	>	110	01101110	n
63	00111111	?	111	01101111	o
64	01000000	@	112	01110000	p
65	01000001	A	113	01110001	q
66	01000010	B	114	01110010	r
67	01000011	C	115	01110011	s
68	01000100	D	116	01110100	t

69	01000101	E	117	01110101	u
70	01000110	F	118	01110110	v
71	01000111	G	119	01110111	w
72	01001000	H	120	01111000	x
73	01001001	I	121	01111001	y
74	01001010	J	122	01111010	z
75	01001011	K	123	01111011	{
76	01001100	L	124	01111100	|
77	01001101	M	125	01111101	}
78	01001110	N	126	01111110	~
79	01001111	O	127	01111111	DEL

Extended ASCII characters					
DEC	Binary	Simbol ASCII	DEC	Binary	Simbol ASCII
128	10000000	Ç	160	10100000	á
129	10000001	ü	161	10100001	í
130	10000010	é	162	10100010	ó
131	10000011	â	163	10100011	ú
132	10000100	ä	164	10100100	ñ
133	10000101	à	165	10100101	Ñ
134	10000110	ȧ	166	10100110	ª
135	10000111	ç	167	10100111	º
136	10001000	ê	168	10101000	¿
137	10001001	ë	169	10101001	®
138	10001010	è	170	10101010	¬
139	10001011	ï	171	10101011	½
140	10001100	î	172	10101100	¼
141	10001101	ì	173	10101101	¡
142	10001110	Ä	174	10101110	«
143	10001111	Å	175	10101111	»
144	10010000	É	176	10110000	▒

145	10010001	Æ	177	10110001	▒
146	10010010	Æ	178	10110010	▓
147	10010011	Ô	179	10110011	│
148	10010100	Ö	180	10110100	┤
149	10010101	Ò	181	10110101	Á
150	10010110	Û	182	10110110	Â
151	10010111	Ù	183	10110111	À
152	10011000	Ÿ	184	10111000	©
153	10011001	Ö	185	10111001	╣
154	10011010	Ü	186	10111010	║
155	10011011	Ø	187	10111011	╗
156	10011100	£	188	10111100	╝
157	10011101	Ø	189	10111101	¢
158	10011110	×	190	10111110	¥
159	10011111	*F*	191	10111111	┐

Extended ASCII characters					
DEC	Binary	Simbol ASCII	DEC	Binary	Simbol ASCII
192	11000000	└	224	11100000	Ó
193	11000001	┴	225	11100001	ß
194	11000010	┬	226	11100010	Ô
195	11000011	├	227	11100011	Ò
196	11000100	─	228	11100100	õ
197	11000101	┼	229	11100101	Õ
198	11000110	ã	230	11100110	µ
199	11000111	Ã	231	11100111	þ
200	11001000	╚	232	11101000	Þ
201	11001001	╔	233	11101001	Ú
202	11001010	╩	234	11101010	Û
203	11001011	╦	235	11101011	Ù
204	11001100	╠	236	11101100	ý

205	11001101	═	237	11101101	Ý
206	11001110	╬	238	11101110	¯
207	11001111	¤	239	11101111	´
208	11010000	ð	240	11110000	≡
209	11010001	Ð	241	11110001	±
210	11010010	Ê	242	11110010	‗
211	11010011	Ë	243	11110011	¾
212	11010100	È	244	11110100	¶
213	11010101	ı	245	11110101	§
214	11010110	í	246	11110110	÷
215	11010111	î	247	11110111	¸
216	11011000	ï	248	11111000	°
217	11011001	┘	249	11111001	¨
218	11011010	┌	250	11111010	·
219	11011011	█	251	11111011	¹
220	11011100	▄	252	11111100	³
221	11011101	¦	253	11111101	²
222	11011110	ì	254	11111110	■
223	11011111	▀	255	11111111	

RIWAYAT HIDUP

Fatimatuzzahro', lahir di kota Trenggalek pada tanggal 08 Oktober 1997. Memiliki nama panggilan Ema, tinggal di Dusun Taraan Desa Tegalrejo Kecamatan Merakuran Kabupaten Tuban. Merupakan anak pertama dari tiga bersaudara dari pasangan bapak Inzrok dan ibu Lilis Eko Styowati. Pendidikan formal pada tingkat dasar ditempuh di MIN Tuban dan lulus pada tahun 2010, setelah itu melanjutkan ke MTs Al-Multazam Mojokerto dan lulus pada tahun 2013. Kemudian melanjutkan pendidikan ke SMA Al-Multazam Mojokerto dan lulus pada tahun 2016. Selanjutnya, pada tahun 2016 menempuh kuliah di Universitas Islam Negeri Maulana Malik Ibrahim Malang mengambil Jurusan Matematika Fakultas Sains dan Teknologi. Selain menempuh pendidikan formal, dia juga menempuh pendidikan informal di pondok pesantren Al-Multazam Mojokerto mulai tahun 2010 hingga 2016.

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 : Fatimatuzzahro'
NIM : 16610100
Fakultas/Jurusan : Sains dan Teknologi/ Matematika
Judul Skripsi : Penerapan Algoritma Hibrida Menggunakan Metode *Hill Cipher* Dan *Rivest Shamir Adleman* (RSA) Pada Pengamankan Pesan Teks
Pembimbing I : Muhammad Khudzaifah,M. Si
Pembimbing II : Juhari, M. Si

No	Tanggal	Hal	Tanda Tangan
1.	04 Oktober 2020	Konsultasi Bab I, Bab II, dan Bab III	1.
2.	20 April 2021	Revisi Bab I, Bab II, dan Bab III	2.
3.	10 Juni 2021	Konsultasi Bab IV	3.
4.	12 Juni 2021	Konsultasi Kajian Keagamaan	4.
5.	25 Agustus 2021	ACC Kajian Keagamaan	5.
6.	03 September 2021	konsultasi Bab I, Bab II, Bab III, dan Bab IV	6.
7.	13 Oktober 2021	Revisi Bab I, Bab II, Bab III, dan Bab IV	7.
8.	28 Oktober 2021	ACC Bab I, Bab II, Bab III, dan Bab IV	8.
9.	15 Desember 2021	Revisi Keseluruhan	9.
10.	22 Desember 2021	ACC Keseluruhan	10.

Malang, 23 Desember 2021
Mengetahui,
Ketua Program Studi Matematika

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