

**PENYANDIAN SUPER ENKRIPSI MENGGUNAKAN *COLUMNAR*
TRANSPOSITION DAN MODIFIKASI *HILL CIPHER* DENGAN INVERS
KIRI MATRIKS PERSEGI PANJANG**

SKRIPSI

**OLEH
FIKA WAHYUNI
NIM 17610050**



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

**PENYANDIAN SUPER ENKRIPSI MENGGUNAKAN *COLUMNAR*
TRANSPOSITION DAN MODIFIKASI *HILL CIPHER* DENGAN INVERS
KIRI MATRIKS PERSEGI PANJANG**

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
FIKA WAHYUNI
NIM. 17610050**

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

**PENYANDIAN SUPER ENKRIPSI MENGGUNAKAN *COLUMNAR*
TRANSPOSITION DAN MODIFIKASI *HILL CIPHER* DENGAN INVERS
KIRI MATRIKS PERSEGI PANJANG**

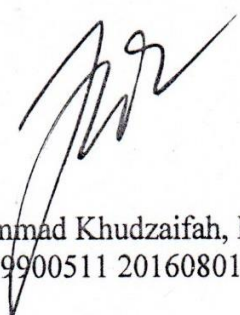
SKRIPSI


**OLEH
FIKA WAHYUNI
NIM. 17610050**

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 15 November 2021

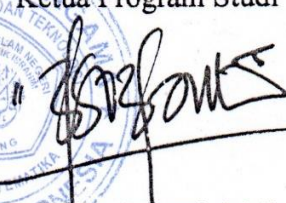

Pembimbing I,

Pembimbing II,


Muhammad Khudzaifah, M.Si
NIDT. 19900511 20160801 1 057


Muhammad Nafie Jauhari, M.Si
NIDT. 19870218 20160801 1 056

Mengetahui,
Ketua Program Studi



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

**PENYANDIAN SUPER ENKRIPSI MENGGUNAKAN COLUMNAR
TRANSPOSITION DAN MODIFIKASI HILL CIPHER DENGAN INVERS
KIRI MATRIKS PERSEGI PANJANG**

SKRIPSI

**OLEH
FIKA WAHYUNI
NIM. 17610050**

Telah Dipertahankan di Depan Dewan Penguji Skripsi
Dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
Untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 06 Desember 2021

Penguji Utama : Juhari, M.Si
Ketua Penguji : Hisyam Fahmi, M.Kom
Sekretaris Penguji : Muhammad Khudzaifah, M.Si
Anggota Penguji : Muhammad Nafie Jauhari, M.Si

.....
.....
.....
.....

Mengetahui,
Ketua Program Studi



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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertandatangan di bawah ini:

Nama : Fika Wahyuni

NIM : 17610050

Jurusan : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Penyandian Super Enkripsi Menggunakan Columnar
Transposition dan Modifikasi Hill Cipher dengan Invers Kiri
Matriks Persegi Panjang

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

Malang, 28 Oktober 2021

Yang membuat pernyataan,



Fika Wahyuni

NIM. 17610050

MOTO

“Selalu berusaha melakukan yang lebih baik dari hari kemarin”

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:

Bapak dan Ibu tercinta, yang senantiasa mendo'akan, mendukung baik moral maupun materiil, memberi nasihat, semangat dan kasih sayang yang tak ternilai, serta adik-adik tersayang yang selalu memberi semangat dan dukungan penuh kepada penulis. Teman-temanku yang selalu mensupport dan membantu penulis dalam menyelesaikan skripsi ini.

KATA PENGANTAR

Assalamu'alaikum arahmatullahi Wabarakatuh

Segala puji bagi Allah SWT, atas rahmat, taufik serta hidayah-Nya, sehingga penulis mampu menyelesaikan penyusunan skripsi sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang matematika di Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Dalam proses penyusunan skripsi ini, penulis banyak mendapat bimbingan dan arahan dari beberapa pihak. Untuk itu ucapan terimakasih yang sebesar-besarnya dan penghargaan yang setinggi-tingginya penulis sampaikan terutama kepada:

1. Muhammad Khudzaifah, M.Si, selaku dosen pembimbing I yang telah memberikan arahan, nasihat, motivasi dan berbagi pengalaman yang berharga bagi penulis.
2. Muhammad Nafie Jauhari, M.Si, selaku dosen pembimbing II yang telah memberi banyak arahan dan berbagi ilmunya kepada penulis.
3. Juhari, M.Si, selaku penguji utama yang telah memberikan banyak saran yang sangat bermanfaat untuk tugas akhir ini bagi penulis.
4. Hisyam Fahmi, M.Kom, selaku ketua penguji yang telah memberikan masukan yang sangat berarti bagi penulis untuk tugas akhir ini.
5. Segenap sivitas akademika Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang terutama kepada seluruh dosen yang telah memberikan ilmunya
6. Bapak dan Ibu serta saudara-saudara tercinta yang selalu memberikan doa, semangat dan motivasi kepada penulis sampai saat ini.
7. Sahabat-sahabat terbaik penulis, yang selalu menemani, membantu dan memberikan dukungan sehingga penulis dapat menyelesaikan skripsi ini.
8. Seluruh teman-teman di Jurusan Matematika angkatan 2017, terimakasih atas kenang-kenangan indah yang dirajut bersama.
9. Semua pihak yang tidak dapat disebutkan satu persatu yang telah membantu penulis dalam menyelesaikan skripsi ini.

Semoga Allah SWT, melimpahkan rahmat dan kaunia-Nya kepada kita semua. Akhirnya penulis berharap semoga dengan rahmat dan izin-Nya skripsi ini bermanfaat bagi penulis dan pembaca. Aamiin.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Malang. 28 Oktober 2021

Penulis

DAFTAR ISI

| | |
|--|-------|
| HALAMAN JUDUL | |
| HALAMAN PENGAJUAN | |
| HALAMAN PERSETUJUAN | |
| HALAMAN PENGESAHAN | |
| HALAMAN PERNYATAAN KEASLIAN TULISAN | |
| HALAMAN MOTO | |
| HALAMAN PERSEMBAHAN | |
| KATA PENGANTAR..... | viii |
| DAFTAR ISI..... | x |
| DAFTAR TABEL | xii |
| DAFTAR GAMBAR..... | xiii |
| ABSTRAK | xiv |
| ABSTRACT | xv |
| ملخص..... | xvi |
| BAB I PENDAHULUAN..... | 1 |
| 1.1 Latar Belakang..... | 1 |
| 1.2 Rumusan Masalah | 4 |
| 1.3 Tujuan Penelitian | 4 |
| 1.4 Batasan Masalah | 4 |
| 1.5 Manfaat Penelitian | 5 |
| 1.6 Metode Penelitian | 5 |
| 1.7 Sistematika Penulisan | 6 |
| BAB II KAJIAN PUSTAKA | 8 |
| 2.1 Himpunan | 8 |
| 2.2 Fungsi (Pemetaan) | 9 |
| 2.3 Fungsi Komposisi | 11 |
| 2.4 Matriks..... | 12 |
| 2.5 Operasi Matriks | 13 |
| 2.5.1 Penjumlahan Matriks..... | 13 |
| 2.5.2 Perkalian Matriks..... | 14 |
| 2.5.3 Transpose Matriks, Transpose Konjugat dan Hermitian..... | 14 |
| 2.5.4 Invers Matriks..... | 16 |
| 2.5.5 Invers Matriks Tergeneralisasi | 17 |

| | | |
|---------------------------------|--|-----------|
| 2.6 | Aritmatika Modulo | 18 |
| 2.6.1 | Kekongruenan..... | 19 |
| 2.6.2 | Invers Modulo | 22 |
| 2.6.3 | Invers Matriks Modulo | 22 |
| 2.7 | Struktur Aljabar | 22 |
| 2.8 | Kriptografi | 25 |
| 2.8.1 | Sejarah Kriptografi | 25 |
| 2.8.2 | Algoritma Kriptografi..... | 26 |
| 2.8.3 | Kriptografi Klasik dan Modern | 29 |
| 2.9 | Super Enkripsi | 30 |
| 2.10 | Columnar Transposition | 30 |
| 2.11 | Hill Cipher | 32 |
| 2.12 | Kriptografi dalam Kajian Keislaman..... | 34 |
| BAB III PEMBAHASAN | | 35 |
| 3.1 | Proses Penyandian Super Enkripsi Menggunakan <i>Columnar Transposition</i> dan Modifikasi <i>Hill Cipher</i> dengan Invers Kiri Matriks Persegi Panjang | 35 |
| 3.1.1 | Teknik Penyandian Algoritma <i>Columnar Transposition</i> | 35 |
| 3.1.2 | Teknik Modifikasi <i>Hill Cipher</i> dengan Invers Kiri Matriks Persegi Panjang | 38 |
| 3.1.3 | Teknik Penyandian Super Enkripsi Menggunakan <i>Columnar Transposition</i> dan Modifikasi <i>Hilll Cipher</i> dengan Invers Kiri Matriks Persegi Panjang | 54 |
| 3.2 | Kajian Keislaman | 63 |
| BAB IV PENUTUP | | 65 |
| 4.1 | Kesimpulan..... | 65 |
| 4.2 | Saran | 66 |
| DAFTAR PUSTAKA | | 67 |
| RIWAYAT HIDUP | | |

DAFTAR TABEL

| | |
|---|----|
| Tabel 2.1 Contoh Enkripsi <i>Columnar Transposition</i> | 31 |
| Tabel 3.1 Enkripsi Berdasarkan Urut Kunci | 36 |
| Tabel 3.2 Enkripsi Berdasarkan Urut Angka | 37 |
| Tabel 3.3 Dekripsi Berdasarkan Urut Angka | 37 |
| Tabel 3.4 Dekripsi Berdasarkan Urut Kunci | 38 |
| Tabel 3.5 Konversi Modifikasi <i>Hill Cipher</i> | 47 |
| Tabel 3.6 Enkripsi Super Enkripsi Terurut Kunci | 57 |
| Tabel 3.7 Enkripsi Super Enkripsi Terurut Angka | 57 |
| Tabel 3.8 Dekripsi Super Enkripsi Terurut Angka | 62 |
| Tabel 3.9 Dekripsi Super Enkripsi Terurut Kunci | 63 |

DAFTAR GAMBAR

| | |
|---|----|
| Gambar 2.1 Fungsi f Memetakan Himpunan X ke Y | 9 |
| Gambar 2.2 Contoh Fungsi f Surjektif..... | 10 |
| Gambar 2.3 Fungsi Injektif | 10 |
| Gambar 2.4 Fungsi Bijektif..... | 11 |
| Gambar 2.5 Fungsi Komposisi..... | 12 |

ABSTRAK

Wahyuni, Fika. 2021. **Penyandian Super Enkripsi Menggunakan *Columnar Transposition* dan Modifikasi *Hill Cipher* dengan Invers Kiri Matriks Persegi Panjang**. Skripsi. Jurusan Matematika Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si. (II) Muhammad Nafie Jauhari, M.Si.

Kata Kunci: Enkripsi, Dekripsi, Super Enkripsi, *Columnar Transposition*, *Hill Cipher*

Perkembangan zaman dan teknologi saat ini berkembang begitu cepat sehingga saat ini banyak komputer terhubung ke internet untuk penyampaian data dari satu pihak ke pihak yang lain, termasuk perusahaan, lembaga keuangan, lembaga pemerintahan dan lain-lain. Karenanya, diperlukan suatu keamanan pada proses penyampaian pesan. Enkripsi merupakan suatu proses mengubah pesan yang dapat dibaca (*plaintext*) menjadi suatu pesan acak yang tidak dapat dibaca (*ciphertext*), sedangkan dekripsi merupakan proses kebalikan dari enkripsi. Pada penelitian ini, proses enkripsi dan dekripsi menggunakan dua algoritma dan dua kunci rahasia guna untuk meningkatkan tingkat keamanan suatu pesan yang dienkripsi menggunakan metode super enkripsi. Super enkripsi merupakan suatu metode kriptografi yang mengkombinasikan dua algoritma kriptografi atau lebih yang merupakan algoritma metode substitusi dan transposisi. Pada penelitian ini, digunakan algoritma *columnar transposition* sebagai metode transposisi dan modifikasi algoritma *hill cipher* dengan invers kiri matriks persegi panjang sebagai metode substitusi. Penyandian pesan menggunakan metode super enkripsi dengan algoritma *columnar transposition* dan modifikasi algoritma *hill cipher* dengan invers kiri matriks persegi panjang menghasilkan pesan akhir yang tidak mengubah, menambah maupun mengurangi pesan awal, sehingga dapat diimplementasikan pada pesan dengan baik. Penyandian ini melipat gandakan keamanan suatu pesan, dimana keamanan pertama terletak pada enkripsi pesan dengan *columnar transposition* dan keamanan yang kedua terletak pada algoritma *hill cipher* yang telah dimodifikasi, sehingga membuat pesan akan semakin sulit untuk dipecahkan. Hasil dari penelitian ini dapat dijadikan sebagai tambahan pustaka mengenai kriptografi serta solusi bagi pihak yang menggunakan teknologi informasi dan komunikasi untuk dapat melakukan pengiriman pesan dengan aman.

ABSTRACT

Wahyuni, Fika. 2021. **On The Super Encryption Using Columnar Transposition and Modified Hill Cipher with Left Inverse Rectangle Matrix**. Thesis. Department of Mathematics, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University, Malang. Supervisor: (I) Muhammad Khudzaifah, M.Si. (II) Muhammad Nafie Jauhari, M.Si.

Keywords: Encryption, Decryption, Super Encryption, Columnar Transposition, Hill Cipher

The development of the times and technology is fast that currently many computers are connected to the internet for transmitting data from one party to another, including companies, financial institutions, government institutions and others. Therefore, we need a security in the process of delivering messages. Encryption is a process of converting a readable message (plaintext) into a random message that cannot be read (ciphertext), while decryption is the reverse process of encryption. In this study, the encryption and decryption process uses two algorithms and two secret keys in order to increase the security level of a message that is encrypted using the super encryption method. Super encryption is a cryptographic method that combines two or more cryptographic algorithms which are substitution and transposition method algorithms. In this study, the columnar transposition algorithm is used as a transposition method and a modification of the hill cipher algorithm with the left inverse of the rectangular matrix as the substitution method. Message encoding using a super encryption method with a columnar transposition algorithm and a modified hill cipher algorithm with a left inverse rectangular matrix produces a final message that does not change, add or reduce the initial message, so that it can be implemented in the message properly. This encryption doubles the security of a message, where the first security lies in encrypting the message with columnar transposition and the second security lies in the hill cipher algorithm that has been modified, thus making the message more difficult to the decipher. The results of this study can be used as an additional library on cryptography as well as solutions for those who use information and communication technology to be able to send messages safely.

ملخص

وحيوني. فيكا. ٢٠٢١. التشفير الفائق باستخدام عمود النقل وشفرة التل المعدلة مع مصفوفة المستطيل الأيسر. مقالة. قسم الرياضيات، كلية العلوم والتكنولوجيا. جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف: (١) محمد خديفة الماجستير، (٢) محمد نافع جوهرى الماجستير.

الكلمات الأساسية: التشفير (*Enkripsi*)، فك التشفير (*Dekripsi*)، التشفير الفائق (*Super*)
(*Enkripsi*)، نقل الكولومنار (*Columnar Transposition*)، تشفير هيل (*Hill Cipher*)

إن تطور الزمان والتكنولوجيا في هذا العصر متطور بسرعة مما يجعل معظم الحاسوب في هذا اليوم يتصل بالإنترنت لتبليغ البيانات من شخص واحد إلى شخص آخر، منها الشركة، المؤسسة النقودية، المؤسسة الجمهورية وغيرها. وهذا التطور يحتاج إلى الأمن في عملية إرسال الرسالة. فعملية التشفير هي عملية تغيير الرسالة المقروءة (*plaintext*) لتصبح الرسالة العشوائية غير المقروءة (*ciphertext*). وأما فك التشفير هو عملية عكس التشفير. وكان في هذا البحث، استخدمت عملية التشفير و فك التشفير نوعين من الخوارزمية (*algoritma*) ونوعين من مفتاح المؤمن لأجل ترقية درجة الأمن من الرسالة المرموزة باستخدام طريقة التشفير الفائق. التشفير الفائق هو طريقة التشفير (*kriptografi*) التي تختلط خطوتين من الخوارزمية التشفيرية أو أكثر مما هو من خوارزمية طريقة التبديل (*substitusi*) والتحويل (*transposisi*). واستخدم هذا البحث خوارزمية نقل الكولومنار (*columnar transposition*) كطريقة التحويل وتغيير خوارزمية تشفير هيل (*hill cipher*) بإنعكاس يسار المنشأ المستطيل كطريقة التبديل. فعملية ترميز الرسالة باستخدام طريقة التشفير الأعلى خوارزمية نقل الكولومنار وتغيير خوارزمية تشفير هيل بإنعكاس يسار المنشأ المستطيل يستطيع أن يطبقها في الرسالة بصورة جيدة. ويعمل هذا الترميز بإضعاف أمن الرسالة حيث أن الأمن الأول يقع في تشفير الرسالة نقل الكولومنار والأمن الثاني يقع في خوارزمية تشفير هيل المتغيرة، فأصبحت الرسالة صعبة لبحثها. فتكون نتائج هذا البحث مرجعا عن التشفير ومع الحل لمن يستخدم التكنولوجيا والمعلومات والاتصالات لإرسالة الرسالة بالأمن.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dewasa ini perkembangan teknologi begitu pesat dan cepat termasuk dalam perkembangan teknologi komunikasi dan informasi. Teknologi informasi banyak menawarkan kemudahan dalam berkomunikasi serta saling bertukar informasi atau data. Karena banyak menawarkan kemudahan, saat ini teknologi informasi telah menjadi bagian yang sangat penting di berbagai aspek kehidupan manusia. Seiring dengan kemajuan pada teknologi informasi, maka sangat diperlukan keamanan terhadap kerahasiaan dalam sebuah pertukaran informasi, terlebih lagi jika data tersebut terhubung dalam satu jaringan komputer dengan jaringan yang lainnya. Hal tersebut tentu saja menimbulkan risiko yang besar apabila informasi yang disampaikan bersifat berharga dan sensitif apabila di akses oleh orang lain yang tidak bertanggung jawab. Sehingga, keamanan dalam proses pengiriman pesan yang berisi data-data tertentu sangat diperlukan.

Menjaga kerahasiaan suatu pesan termasuk dalam amanah yang harus dijaga dengan sebaik-baiknya. Dalam Al-Quran telah ditetapkan mengenai pentingnya dalam menjaga amanah, yaitu pada surat An-Nisa' ayat 58:

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

Salah satu cara dan usaha yang dapat digunakan untuk mempertahankan kerahasiaan suatu informasi atau pesan adalah dengan melakukan penyandian pada pesan, pesan yang akan dikirimkan tersebut disandikan menjadi kode-kode yang hanya dapat dipahami oleh pihak pengirim dan penerima pesan, sehingga pihak

ketiga tidak dapat mengetahui pesan tersebut. Untuk memperkuat keamanan kerahasiaan pesan tersebut maka dibutuhkan suatu teknik metode yang digunakan untuk mengamankan pesan tersebut. Selanjutnya kriptografi adalah salah satu solusi yang dapat digunakan untuk menyelesaikan permasalahan di atas.

Saat ini kriptografi sudah banyak digunakan untuk mengamankan suatu data informasi maupun pesan yang penting dan telah diimplementasikan dalam berbagai bidang aspek kehidupan. Semakin sulit algoritma kriptografi yang digunakan maka semakin sulit juga bagi pihak ketiga untuk memecahkan algoritmanya. Sehingga semakin rumit algoritma kriptografi maka semakin tinggi keamanannya. Salah satu cara yang dapat digunakan untuk membuat algoritma yang memiliki tingkat kesulitan yang tinggi adalah dengan memodifikasi algoritma kriptografi ataupun dengan mengkombinasikan dua atau lebih metode algoritma kriptografi.

Metode yang mengkombinasikan dua atau lebih metode algoritma kriptografi yaitu dengan teknik substitusi dan transposisi disebut dengan super enkripsi. Karena pada super enkripsi mengkombinasikan beberapa algoritma maka super enkripsi ini sulit untuk dipecahkan, sehingga keamanan pada suatu pesan atau informasi dapat terjaga. Pada super enkripsi dapat dilakukan algoritma teknik substitusi terlebih dahulu kemudian algoritma teknik transposisi dan dapat juga dilakukan sebaliknya.

Pada penelitian sebelumnya telah dibahas modifikasi maupun kombinasi dari algoritma kriptografi. Kaur (2019) melakukan penelitian pada modifikasi algoritma *hill cipher* dengan matriks persegi panjang pada kunci yang digunakannya guna meningkatkan keamanan komunikasi menjadi lebih baik. Pada penelitiannya tersebut, Ravinder Kaur menggunakan matriks persegi panjang pada

proses enkripsinya, sedangkan invers kiri dari matriks persegi panjang tersebut digunakan untuk proses dekripsi. *Ciphertext* yang dihasilkan dari modifikasi *hill cipher* dengan invers kiri matriks persegi panjang ini lebih panjang dari *plaintext* sehingga dapat menambah keamanan suatu pesan. Namun pada penelitian ini algoritma yang digunakan hanya modifikasi dari algoritma *hill cipher* sehingga penyandian pesan hanya dilakukan satu kali.

Selanjutnya Reswan dkk (2018) melakukan penelitian dengan super enkripsi pada implementasi kompilasi algoritma kriptografi transposisi columnar dan RSA untuk mengamankan pesan rahasia. Proses enkripsi dilakukan menggunakan transposisi columnar terlebih dahulu kemudian di enkripsi kembali menggunakan algoritma RSA. Transposisi columnar digunakan untuk menambah kerumitan penyandian suatu pesan, sehingga dapat mengamankan pesan lebih kuat.

Berdasarkan masalah diatas, salah satu solusi yang dapat dilakukan untuk mengamankan pesan agar lebih kuat adalah dengan mengkombinasikan dua algoritma kriptografi yang dinamakan dengan metode super enkripsi. Super enkripsi merupakan salah satu cara yang dapat digunakan untuk meningkatkan kerumitan suatu algoritma karena menggunakan dua metode kriptografi, yaitu dengan mengkombinasikan teknik substitusi dan transposisi. Pada penelitian ini akan dilakukan penyandian pesan menggunakan super enkripsi dimana teknik substitusi yang digunakan pada penyandian ini ialah modifikasi algoritma *hill cipher* dengan invers matriks persegi, sedangkan teknik transposisinya menggunakan transposisi columnar. Penyandian dilakukan menggunakan *columnar transposition* terlebih dahulu kemudian modifikasi *hill cipher*, hal tersebut dilakukan karena apabila penyandian menggunakan modifikasi *hill cipher* terlebih dahulu maka akan

menghasilkan pesan akhir yang memiliki penambahan karakter. Penyandian dengan menggunakan kombinasi kedua algoritma tersebut diharapkan mampu mengamankan pesan karena terdapat pengamanan ganda, yaitu dari algoritma *hill cipher* yang dimodifikasi dan super enkripsi.

1.2 Rumusan Masalah

Berdasarkan dari latar belakang tersebut, maka rumusan masalah penelitian ini adalah bagaimana proses penyandian super enkripsi menggunakan *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, tujuan penelitian ini adalah untuk mengetahui proses penyandian super enkripsi menggunakan *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang.

1.4 Batasan Masalah

Dari latar belakang di atas, agar pembahasan tidak terlalu luas maka dibutuhkan pembatasan masalah sebagai berikut:

1. Hanya mengenkripsi pesan teks alphabet dan spasi.
2. Kunci yang digunakan dalam proses enkripsi pada modifikasi algoritma *hill cipher* dengan invers kiri matriks persegi panjang merupakan matriks berukuran 3×2 .
3. Proses penyandian menggunakan modulo 53.
4. Proses enkripsi dilakukan menggunakan *columnar transposition* terlebih dahulu kemudian modifikasi *hill cipher*, sedangkan untuk proses dekripsi adalah sebaliknya.

1.5 Manfaat Penelitian

Penulis berharap bahwa manfaat yang diperoleh dalam penelitian ini adalah sebagai berikut:

1. Dapat menambah wawasan tentang kriptografi khususnya pada metode super enkripsi menggunakan *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang.
2. Menambah bahan kepustakaan serta informasi mengenai kriptografi
3. Memperkaya sumber pengetahuan tentang kriptografi dan solusi bagi pihak-pihak yang menggunakan teknologi informasi dan komunikasi untuk dapat melakukan pengiriman pesan dengan aman.

1.6 Metode Penelitian

Metode penelitian yang dilakukan dalam penelitian ini adalah studi kepustakaan (*library research*) dengan mengkaji dan menelaah beberapa buku, jurnal serta referensi lain yang berkaitan dengan topik enkripsi dan dekripsi metode super enkripsi, *columnar transposition*, dan *hill cipher*.

Adapun langkah-langkah yang dilakukan dalam penelitian ini adalah:

1. Melakukan proses penyandian *columnar transposition*.
2. Melakukan proses penyandian modifikasi *hill cipher* dengan invers kiri matriks persegi panjang.
3. Melakukan proses penyandian super enkripsi *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang.
 - a. Enkripsi menggunakan super enkripsi *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang
 - 1) Menentukan pesan (*plaintext*).

- 2) Menentukan kunci *columnar transposition*.
 - 3) Melakukan perhitungan pada pesan teks bersandi dengan *columnar transposition*.
 - 4) Menentukan kunci matriks 3 x 2 untuk algoritma modifikasi *hill cipher* dengan invers matriks persegi panjang.
 - 5) Melakukan penyandian dengan modifikasi algoritma *hill cipher* dengan invers kiri matriks persegi panjang.
 - 6) Mendapatkan pesan teks yang telah disandikan (*ciphertext*).
- b. Dekripsi menggunakan super enkripsi menggunakan *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang.
- 1) Memasukkan pesan yang telah disandikan (*ciphertext*).
 - 2) Menentukan invers dari kunci matriks yang digunakan sebelumnya
 - 3) Melakukan dekripsi dengan modifikasi algoritma *hill cipher* dengan invers kiri matriks persegi panjang.
 - 4) Menentukan kunci *columnar transposition*.
 - 5) Melakukan perhitungan dengan *columnar transposition*.
 - 6) Mendapatkan teks asli (*plaintext*).

1.7 Sistematika Penulisan

Sistematika penulisan pada penelitian ini terdiri dari empat bab, yaitu:

Bab I Pendahuluan

Pada bab ini diuraikan mengenai latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, metode penelitian dan sistematika penulisan.

Bab II Kajian Pustaka

Bab ini memaparkan tentang gambaran umum dari teori yang mendasari pembahasan. Diantaranya yaitu tentang Matriks, Aritmatika Modulo, Kriptografi, Super enkripsi, *Columnar transposition* dan *Hill cipher*.

Bab III Pembahasan

Bab ini merupakan inti dari penulisan penelitian ini yang berisi tentang penyelesaian masalah.

Bab IV Penutup

Bab ini berisi kesimpulan dari hasil dan pembahasan yang telah diperoleh, serta dilengkapi saran yang berkaitan dengan penelitian yang dilakukan.

BAB II

KAJIAN PUSTAKA

2.1 Himpunan

Himpunan adalah kumpulan dari objek-objek tertentu yang didefinisikan secara jelas. Objek-objek dalam himpunan tersebut disebut dengan anggota himpunan, unsur himpunan ataupun elemen himpunan. Suatu himpunan dinotasikan dengan huruf-huruf besar (kapital) sedangkan anggota-anggota dari himpunan dinotasikan dengan huruf kecil dan ditulis diantara dua kurung kurawal. Untuk mendefinisikan suatu himpunan dapat dilakukan dengan beberapa cara, yaitu:

1. Menuliskan elemen-elemennya

Cara dengan menuliskan elemen-elemennya yaitu dengan menuliskan semua elemennya, sehingga elemen yang tidak terdapat dalam daftar tersebut bukan termasuk elemen himpunan. Untuk menuliskan suatu himpunan yang memiliki banyak elemen dapat menuliskan semua elemennya diwakili dengan "...". misalkan $X = \{1, 2, 3, \dots\}$

2. Menggunakan notasi syarat pembentukan elemen himpunan

Dengan cara ini cukup dengan menuliskan syarat dari anggota himpunan yang harus dipenuhi, sehingga suatu objek yang memenuhi syarat tersebut termasuk dalam elemen himpunan. Misalkan $A = \{x | 2 \leq x < 8\}$ (Soebagio dan Sukirman, 1999).

Keanggotaan suatu himpunan dapat dinyatakan dengan notasi \in , sedangkan untuk menyatakan suatu objek bukan termasuk suatu himpunan dinotasikan dengan \notin .

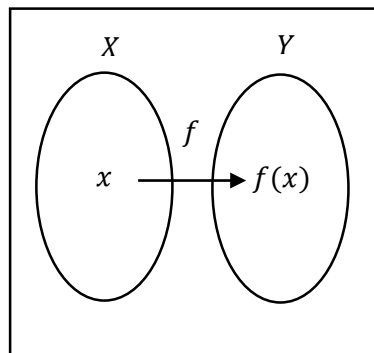
2.2 Fungsi (Pemetaan)

Fungsi f didefinisikan dengan korespondensi yang menghubungkan setiap elemen dari dua himpunan. Misalkan terdapat himpunan tak kosong X dan Y maka fungsi merupakan suatu korespondensi yang menghubungkan setiap elemen $x \in X$ ke $y \in Y$. Suatu fungsi atau pemetaan dari X ke Y dinotasikan dengan:

$$f: X \rightarrow Y.$$

Elemen x dari X terhubung dengan elemen $f(x)$ dari Y , elemen-elemen dari X disebut dengan domain (daerah asal) sedangkan elemen $f(x)$ dari Y disebut dengan kodomain (daerah hasil) (Raisinghanian dan Aggarwal, 1980).

Suatu fungsi f yang memetakan X ke Y dapat direpresentasikan dengan gambar sebagai berikut:



Gambar 2.1 Fungsi f Memetakan Himpunan X ke Y

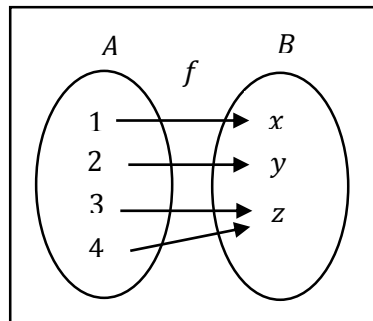
Dilihat dari elemen-elemen pada himpunan X yang direlasikan pada suatu fungsi terhadap elemen-elemen dari himpunan Y , maka terdapat tiga sifat fungsi yaitu :

a. Fungsi Surjektif (Onto)

Jika terdapat suatu fungsi f yang memetakan himpunan A ke himpunan B $f: A \rightarrow B$ dan setiap $b \in B$ memiliki pasangan di himpunan A sehingga $f(a) = b$, maka fungsi tersebut disebut dengan fungsi surjektif.

Contoh:

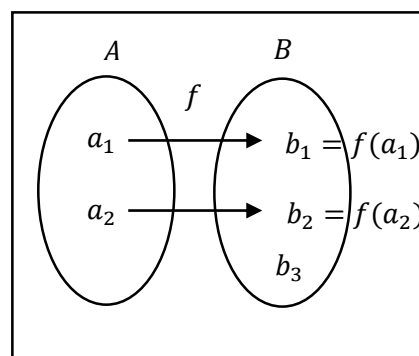
Misalkan terdapat suatu himpunan $A = \{1,2,3,4\}$ dan himpunan $B = \{x, y, z\}$ yang didefinisikan oleh fungsi $f = \{(1, x), (2, y), (3, z), (4, z)\}$ maka fungsi $f: A \rightarrow B$ merupakan fungsi surjektif karena daerah hasil sama dengan daerah asal, jika digambarkan pada sebuah diagram panah maka



Gambar 2.2 Contoh Fungsi f Surjektif.

b. Fungsi Injektif (Satu-satu)

Misalkan terdapat suatu himpunan A dan himpunan B yang didefinisikan oleh suatu fungsi dan setiap elemen A memiliki pasangan yang berbeda di B , maka fungsi tersebut disebut dengan fungsi injektif atau fungsi satu-satu, dengan kata lain untuk setiap $a_1, a_2 \in A$ dan $a_1 \neq a_2$ berlaku $f(a_1) \neq f(a_2)$.



Gambar 2.3 Fungsi Injektif

Contoh:

Misalkan terdapat suatu fungsi $f: \mathbb{Z} \rightarrow \mathbb{Z}$ dimana f didefinisikan dengan $f(a) = 2 - a$, maka ambil sembarang $f(a), f(b) \in \mathbb{Z}$ dengan $f(a) = f(b)$ sehingga

$$f(a) = f(b)$$

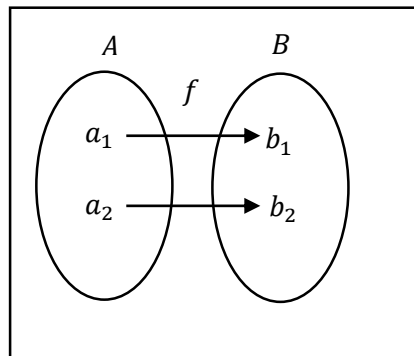
$$2 - a = 2 - b$$

$$a = b$$

Sehingga $f: \mathbb{Z} \rightarrow \mathbb{Z}$ dengan $f(a) = 2 - a$ bersifat injektif.

c. Fungsi Bijektif

Jika suatu fungsi $f: A \rightarrow B$ sedemikian sehingga f bersifat surjektif dan injektif maka f bijektif atau korespondensi satu-satu. Dengan kata lain setiap b elemen dari B berpasangan dan memiliki satu pasangan di A .



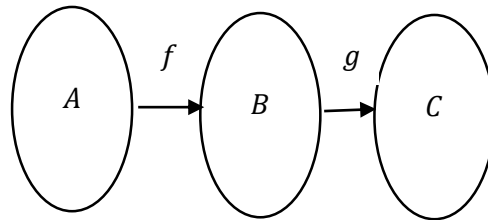
Gambar 2.4 Fungsi Bijektif

2.3 Fungsi Komposisi

Fungsi komposisi merupakan penggabungan operasi dan fungsi secara berurutan sehingga menghasilkan sebuah fungsi baru.

Definisi 1

Misalkan f merupakan fungsi dari himpunan A ke himpunan B dan g merupakan fungsi dari himpunan B ke himpunan C dimana B merupakan daerah hasil dari fungsi f . Jika diilustrasikan maka



Gambar 2.5 Fungsi Komposisi

Ilustrasi tersebut dinotasikan dengan $(g \circ f)$ atau $g(f)$. Jika terdapat $f: A \rightarrow B$ dan $g: B \rightarrow C$ maka kita definisikan fungsi $(g \circ f)(a) \equiv g(f(a))$.

2.4 Matriks

Matriks merupakan susunan bujur sangkar atau persegi panjang dari bilangan-bilangan yang diatur dalam baris dan kolom ditulis antara dua tanda kurung, yaitu $()$ atau $[]$ (Gazali, 2005)

Penulisan matriks disimbolkan dengan huruf kapital, sedangkan entri dalam matriks disimbolkan dengan huruf kecil. Sebagai contoh misalkan A adalah sebuah matriks, maka entri dalam matriks dapat disimbolkan dengan a_{ij} di mana i merupakan baris dalam matriks dan j merupakan kolom dalam matriks $i = 1, 2, 3, \dots, m$ dan $j = 1, 2, 3, \dots, n$. Banyaknya baris dalam matriks dinotasikan dengan m sedangkan banyaknya kolom dalam matriks dinotasikan dengan n sehingga sebuah matriks memiliki ordo atau ukuran $m \times n$. Secara umum matriks ditulis dengan

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Contoh sebuah matriks adalah

$$A = \begin{pmatrix} 4 & 7 \\ 6 & 3 \\ 1 & 2 \end{pmatrix}.$$

Dari contoh di atas, A merupakan matriks berordo $m \times n$ di mana $m = 3$ dan $n = 2$.

2.5 Operasi Matriks

Operasi yang digunakan pada penelitian ini meliputi penjumlahan matriks dan perkalian matriks.

2.5.1 Penjumlahan Matriks

Penjumlahan dua matriks didefinisikan jika terdapat sebuah matriks $A = [a_{ij}]$ dan $B = [b_{ij}]$ adalah matriks-matriks $m \times n$, maka jumlah $A + B$ adalah matriks $m \times n$ dengan

$$A + B = [a_{ij} + b_{ij}]$$

Di mana

$$[a_{ij} + b_{ij}] = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{bmatrix}.$$

Sehingga $A + B$ merupakan matriks $m \times n$ yang diperoleh dengan menambahkan entri-entri yang seletak dari A dan B jika $A + B = C = [c_{ij}]$, maka $c_{ij} = a_{ij} + b_{ij}$ untuk $i = 1, 2, \dots, m$ dan $j = 1, 2, \dots, n$ (Marjono, 2012).

Contoh

$$\begin{bmatrix} 2 & 6 \\ 3 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 5 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 6 \\ 8 & 5 \end{bmatrix}.$$

2.5.2 Perkalian Matriks

Definisi 2 (Perkalian Matriks dengan Skalar)

Jika $A = [a_{ij}]$ adalah matriks $m \times n$ dan c adalah skalar, maka perkalian skalar dari A dengan c adalah matriks $m \times n$ yang didefinisikan dengan

$$cA = [ca_{ij}] = \begin{bmatrix} ca_{11} & ca_{12} & \dots & ca_{1n} \\ ca_{21} & ca_{22} & \dots & ca_{2n} \\ \vdots & \vdots & & \vdots \\ ca_{m1} & ca_{m2} & \dots & ca_{mn} \end{bmatrix}.$$

Dengan kata lain, $cA = [ca_{ij}]$ adalah matriks yang diperoleh dengan mengalikan setiap entri dari A dengan c . Jika $cA = B = [b_{ij}]$, maka $b_{ij} = ca_{ij}$ untuk $i = 1, 2, \dots, m$ dan $j = 1, 2, \dots, n$ (Marjono, 2012)

Definisi 3 (Perkalian Matriks)

Jika $A = [a_{ij}]$ matriks $m \times n$ dan $B = [b_{ij}]$ matriks $n \times p$, maka hasil kali AB adalah matriks $m \times p$

$$AB = [c_{ij}]$$

Di mana untuk setiap i dan j ,

$$c_{ij} = \sum_{k=1}^n a_{ik}b_{kj} + a_{i2}b_{2j} + \dots + a_{in}b_{nj}$$

Dengan demikian, entri ke- ij dari AB adalah hasil kali titik (*dot product*) baris ke- i dari A dengan kolom ke- j dari B . Jika banyak kolom dari A sama dengan jumlah baris dari B , maka A dan B dikatakan *compatible* terhadap perkalian. (Marjono, 2012)

2.5.3 Transpose Matriks, Transpose Konjugat dan Hermitian

Transpose matriks merupakan perubahan kolom menjadi baris dan baris menjadi kolom pada matriks. Misalkan A sebuah matriks maka transpose matriks

dinotasikan dengan A^T, A^t atau A' . Jika matriks $A = (a_{ij})$ dengan $i = 1, 2, 3, \dots, n$ dan $j = 1, 2, 3, \dots, m$ berorde $m \times n$ maka transpose dari A yaitu $A^T = (b_{ij})$ berorde $n \times m$ sehingga $b_{ij} = a_{ji}$. Contoh :

$$A = \begin{pmatrix} 3 & 5 \\ 6 & 4 \\ 1 & 5 \end{pmatrix}, \text{ maka } A^T = \begin{pmatrix} 3 & 6 & 1 \\ 5 & 4 & 5 \end{pmatrix}.$$

Beberapa sifat transpose matriks adalah sebagai berikut:

1. $(A \pm B)^T = A^T \pm B^T$ di mana A dan B merupakan matriks yang berorde sama.
2. Jika α merupakan suatu skalar dan A adalah matriks maka $(\alpha A)^T = \alpha A^T$.
3. $(A^n)^T = (A^T)^n$ di mana A merupakan matriks bujur sangkar.
4. $(A^T)^T = A$
5. $(AB)^T = B^T A^T$ (Ruminta, 2014)

Definisi 4

Bilangan kompleks merupakan bilangan yang berbentuk $a + bi$ dengan a dan b merupakan bilangan real. Untuk setiap bilangan kompleks $x = a + bi$ maka konjugat dari bilangan x yaitu $\bar{x} = a - bi$

Definisi 5

Konjugat transpose yang dinotasikan dengan $A^* := \bar{A}^T$ merupakan konjugat dari entri ke i, j yaitu $\bar{a}_{j,i}$ dari matriks A . Matriks A dikatakan Hermitian jika $A^* = A$

Contoh:

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

Maka,

$$A^T = \begin{bmatrix} 1-2i & 1+i \\ 4 & 2-2i \\ 5+2i & 3 \end{bmatrix} \quad \text{dan} \quad A^* = \begin{bmatrix} 1+2i & 1-i \\ 4 & 2+2i \\ 5-2i & 3 \end{bmatrix}.$$

2.5.4 Invers Matriks

Jika A dan B adalah sebuah matriks persegi yang berordo sama, dan jika dikalikan menghasilkan sebuah matriks identitas I , yaitu $AB = BA = I$ maka A merupakan invers dari B atau B adalah invers dari A , atau dapat juga dinyatakan dengan $B = A^{-1}$ sehingga $AA^{-1} = I$.

Misalkan A sebuah matriks berordo $m \times n$. Jika B merupakan matriks berordo $n \times m$ yang memenuhi sifat $BA = I_m$, maka B disebut dengan invers kiri dari matriks A , sedangkan apabila C merupakan matriks berordo $n \times m$ yang memenuhi sifat $AC = I_n$ maka C disebut dengan invers kanan dari matriks A (Anton, 2000).

Jika A merupakan suatu matriks yang berukuran $n \times n$, c_{ij} merupakan kofaktor dari a_{ij} sehingga matriksnya ialah

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{nn} \end{pmatrix}$$

Dinamakan dengan matriks kofaktor A . Dan transpose dari matriks ini merupakan *adjoin* A , sehingga jika A merupakan matriks yang dapat dibalik, maka

$$A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$$

Contoh:

Misalkan matriks $A = \begin{pmatrix} i & 3 \\ 4 & 2+i \end{pmatrix}$ sehingga $B = A^{-1} = \begin{pmatrix} -2+i & 3 \\ 2 & -2-i \end{pmatrix}$

karena $AB = \begin{pmatrix} i & 3 \\ 4 & 2+i \end{pmatrix} \begin{pmatrix} -2+i & 3 \\ 2 & -2-i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$

dan $BA = \begin{pmatrix} -2+i & 3 \\ 2 & -2-i \end{pmatrix} \begin{pmatrix} i & 3 \\ 4 & 2+i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$

2.5.5 Invers Matriks Tergeneralisasi

Invers matriks tergenarilasi (*Generalized Inverse of Matrix*) adalah untuk menggenarilasi dari pengertian invers matriks. Invers dari matriks $A_{m \times n}$ dapat diselesaikan dengan invers matriks tergeneralisasi.

Definisi 6

Misalkan A suatu matriks berukuran $m \times n$, jika dapat ditunjukkan $x = A^-y$ dari solusi persamaan linear $Ax = y$ maka matriks A^- yang berukuran $n \times m$ merupakan matriks invers tergeneralisasi (*g - invers*) dari matriks A .

Definisi 7

Diberikan suatu matriks A atas *field*, maka suatu matriks B disebut *pseudo-invers* (*p-invers*) atau invers matriks tergeneralisasi dari matriks A apabila memenuhi sifat-sifat dibawah ini

1. $BAB = B$
2. $ABA = A$
3. $(BA)^* = BA$
4. $(AB)^* = AB$

Teorema 1

Jika $\text{rank } A = n \leq m$,

$$A^- = (A^*A)^{-1}A^*$$

Jika $\text{rank } A = m \leq n$

$$A^- = A^*(AA^*)^{-1}$$

2.6 Aritmatika Modulo

Definisi modulo ialah misalkan a adalah bilangan bulat dan m adalah bilangan bulat lebih dari 0. Operasi $a \bmod m$ (a modulo m) memberikan sisa jika r dibagi dengan m dengan kata lain, $a \bmod m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$ (Munir, 2002).

Aritmatika modulo (*modular arithmetic*) memainkan peranan penting dalam perhitungan bilangan bulat, khususnya pada aplikasi kriptografi. Operator yang digunakan pada aritmatika modulo adalah *mod*. Operator *mod* memberikan sisa pembagian. Misalnya 43 dibagi 5 memberikan hasil 8 dan sisa 3. Sehingga ditulis $43 \bmod 5 = 3$ (Munir, 2006).

Aritmatika modulo sangat berperan dalam kriptografi karena banyak digunakan dalam algoritma enkripsi, baik algoritma enkripsi simetri maupun asimetri. Dalam aritmatika modulo, konsep faktor persekutuan terbesar (FPB) antara lain digunakan untuk operasi invers. Selain FPB, konsep lain seperti kongruensi modulo sangat penting dalam kriptografi. FPB suatu bilangan a dan b dapat dinotasikan dengan $\text{FPB}(a, b)$ dan menghasilkan suatu bilangan d maka $\text{FPB}(a, b) = d$, sedemikian sehingga $d|a$ dan $d|b$ (Kromodimoeljo, 2010).

Contoh penggunaan aritmatika modulo dalam kriptografi adalah untuk penyandian alphabet "A" sampai "Z" kedalam angka dengan memetakan huruf alphabet $\{A, \dots, Z\}$ ke $\{0, \dots, 25\}$. Aritmatika modulo digunakan dalam penyandian ini bertujuan agar penyandian selalu bernilai $\{0, \dots, 25\}$ sehingga hasil penyandian selalu memiliki pasangan simbol.

2.6.1 Kekongruenan

Misalkan a dan b merupakan suatu bilangan bulat, dan m adalah bilangan bulat positif yang lebih besar dari satu, jika m membagi habis $(a - b)$ maka a dikatakan kongruen dengan b modulo m yang ditulis dengan $a \equiv b \pmod{m}$. Kekongruenan dapat dituliskan dengan suatu hubungan $a = b + km$ dimana k merupakan suatu bilangan bulat tertentu (Irawan, dkk, 2014).

Contoh:

- a. $12 \equiv 6 \pmod{3}$
- b. $60 \equiv 20 \pmod{5}$
- c. $25 \equiv 10 \pmod{3}$

Teorema 2

Jika a, b, c, d dan m adalah bilangan bulat dengan m adalah bilangan asli, maka berlaku

- 1. Refleksi $a \equiv a \pmod{m}$
- 2. Simetris, jika $a \equiv b \pmod{m}$ maka $b \equiv a \pmod{m}$
- 3. Transitif, jika $a \equiv b \pmod{m}$ dan $b \equiv c \pmod{m}$ maka $a \equiv c \pmod{m}$

Bukti:

- 1. Jika $m \neq 0$ maka $m|0$ sehingga $m|a - a$, maka berdasarkan definisi kongruensi berlaku $a \equiv a \pmod{m}$ untuk setiap $m \neq 0$

2. $a \equiv b \pmod{m}$ berdasarkan definisi maka $m|a - b$ sehingga dapat dinyatakan $a - b = km$

$$a - b = km$$

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

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

Sehingga $b \equiv a \pmod{m}$

3. Menurut definisi kongruensi $a \equiv b \pmod{m}$ maka $m|a - b$ dan $b \equiv c \pmod{m}$ maka $m|b - c$ sehingga

$$m|a - b \text{ dapat dinyatakan } a - b = k_1m$$

$$m|b - c \text{ dapat dinyatakan } b - c = k_2m$$

$$(a - b) + (b - c) = k_1m + k_2m$$

$$a - c = (k_1 + k_2)m$$

Maka berdasarkan definisi $a \equiv c \pmod{m}$

Teorema 3

Jika a, b, c, d dan m adalah bilangan bulat dengan $m > 0$ sedemikian hingga $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$ maka:

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $ac \equiv bd \pmod{m}$

Bukti:

1. Berdasarkan definisi kongruensi $a \equiv b \pmod{m}$ maka $m|a - b$ dan $c \equiv d \pmod{m}$ maka $m|c - d$ sehingga

$$m|(a - b) + (c - d)$$

$$m|[(a + c) - (b + d)]$$

$$a + c \equiv b + d \pmod{m}$$

2. Berdasarkan definisi kongruensi $a \equiv b \pmod{m}$ maka $m|a - b$ dan $c \equiv d \pmod{m}$ maka $m|c - d$ sehingga

$$m|(a - b) - (c - d)$$

$$m|[(a - c) - (b - d)]$$

$$a - c \equiv b - d \pmod{m}$$

3. Berdasarkan definisi kongruensi $a \equiv b \pmod{m}$ maka $m|a - b$ dan $c \equiv d \pmod{m}$ maka $m|c - d$. Terdapat suatu x dan y sehingga $xm = a - b$ dan $ym = c - d$. Kemudian

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= c(a - b) + b(c - d) \\ &= cxm + bym \\ &= m(cx - by) \end{aligned}$$

Sehingga, $m|ac - bd$ atau $ac \equiv bd \pmod{m}$

Teorema 4

$$a \pmod{m} + b \pmod{m} = (a + b) \pmod{m}$$

Bukti:

Berdasarkan pada definisi dari kongruensi m maka

$a \pmod{m}$ berarti $mk_1 + a$ dan $b \pmod{m}$ berarti $mk_2 + b$ sehingga

$$\begin{aligned} a \pmod{m} + b \pmod{m} &= mk_1 + a + mk_2 + b \\ &= mk_1 + mk_2 + a + b \\ &= m(k_1 + k_2) + (a + b) \\ &= (a + b) \pmod{m} \end{aligned}$$

2.6.2 Invers Modulo

Modulo juga memiliki balikan modulo (invers modulo), adapun menurut teorema yaitu:

Teorema 5

Bilangan bulat a mempunyai invers modulo M jika dan hanya jika $\text{FPB}(a, M) = 1$ (Ariyus, 2008).

Bukti:

Jika $\text{FPB}(a, M) = 1$ maka terdapat bilangan m dan n sedemikian sehingga $ma + nM = 1$ yang memiliki arti bahwa $ma + nM \equiv 1 \pmod{M}$. Karena $nM \equiv 0 \pmod{M}$ maka $ma \equiv 1 \pmod{M}$ yang berarti bahwa m adalah invers dari a modulo M .

2.6.3 Invers Matriks Modulo

Jika A dan B adalah matriks berordo $n \times n$ dari bilangan-bilangan bulat, dan $AB \pmod{m} \equiv BA \pmod{m} \equiv I \pmod{m}$ dengan I adalah matriks identitas berordo n , maka B dikatakan invers dari A modulo m (Irawan, dkk, 2014).

Contoh:

$$\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 10 \\ 10 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{5}.$$

Sehingga dapat dilihat bahwa $\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$ merupakan invers dari matriks

$$\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} \pmod{5}.$$

2.7 Struktur Aljabar

Definisi 8 (grup)

Misalkan suatu operasi biner $*$ didefinisikan untuk suatu elemen dari himpunan G , maka $(G, *)$ merupakan grup apabila memenuhi syarat-syarat dibawah ini:

1. G bersifat tertutup terhadap operasi biner, yaitu untuk $x \in G$ dan $y \in G$ maka $x * y$ terdapat di G
2. $*$ bersifat asosiatif, untuk setiap $x, y, z \in G$, $x * (y * z) = (x * y) * z$
3. G memiliki elemen identitas e . Terdapat e di G sedemikian sehingga $x * e = e * x = x$ untuk setiap $x \in G$
4. Semua elemen G memiliki invers. Untuk setiap $a \in G$ maka terdapat $b \in G$ sedemikian sehingga $a * b = b * a = e$

Kemudian apabila grup $(G, *)$ dan $*$ komutatif yaitu $x * y = y * x$ untuk setiap $x, y \in G$ maka G disebut dengan grup komutatif atau grup abelian (Soebagio dan Sukirman, 1993)

Definisi 9 (ring)

Misalkan R suatu himpunan dengan operasi biner penjumlahan $(+)$ dan perkalian (\cdot) . Maka R disebut suatu ring apabila memenuhi kondisi-kondisi dibawah ini

1. R tertutup terhadap penjumlahan: $x \in R$ dan $y \in R$ maka $x + y \in R$
2. Penjumlahan di R bersifat asosiatif: $x + (y + z) = (x + y) + z$ untuk setiap x, y, z di R
3. R memiliki identitas 0 terhadap penjumlahan: $x + 0 = 0 + x = x$ untuk setiap $x \in R$
4. R memiliki invers penjumlahan: untuk setiap x di R maka terdapat $-x$ di R , sedemikian sehingga $x + (-x) = (-x) + x = 0$
5. Penjumlahan di R bersifat komutatif: $x + y = y + x$ untuk setiap $x, y \in R$
6. R tertutup terhadap perkalian: $x \in R$ dan $y \in R$ maka $x \cdot y \in R$

7. Perkalian di R bersifat asosiatif: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ untuk setiap x, y, z di R
8. Bersifat distributive: $x \cdot (y + z) = x \cdot y + x \cdot z$ dan $(x + y) \cdot z = x \cdot z + y \cdot z$ untuk setiap $x, y, z \in R$

Dengan alternatif definisi ring yang lain, ring adalah R suatu himpunan dengan operasi biner penjumlahan $(+)$ dan perkalian (\cdot) dengan memenuhi kondisi:

1. R merupakan grup abelian terhadap penjumlahan
2. R tertutup dan asosiatif terhadap perkalian
3. Bersifat distributif: $x \cdot (y + z) = x \cdot y + x \cdot z$ dan $(x + y) \cdot z = x \cdot z + y \cdot z$ untuk setiap $x, y, z \in R$ (Soebagio dan Sukirman, 1993)

Definisi (Ring dengan unitas, Ring Komutatif)

Misalkan R merupakan ring. Jika terdapat suatu elemen e di R sedemikian sehingga $x \cdot e = e \cdot x = x$ untuk setiap x di R , maka e disebut dengan unitas dan R adalah ring dengan unitas. Jika perkalian di R bersifat komutatif maka R disebut dengan ring komutatif (Soebagio dan Sukirman, 1993).

Definisi 10 (*field*)

Misalkan F adalah suatu ring. Maka F merupakan *field* apabila memenuhi kondisi:

1. F merupakan ring komutatif
2. F memiliki unitas e , dan $e \neq 0$
3. Setiap elemen tak nol dari F memiliki invers terhadap perkalian

Teorema 6

\mathbb{Z}_n adalah field jika dan hanya jika n prima

Bukti:

Jika n bukan prima, maka n memiliki $n = ab$. Pada kasus ini, elemen b tidak memiliki invers terhadap perkalian. Karena $bc \equiv 1 \pmod{n}$ kemudian $abc \equiv a \pmod{n}$, $0 \equiv a \pmod{n}$ sehingga kontradiksi terhadap faktorisasi dari n , sehingga jika n bukan prima maka \mathbb{Z}_n bukan field.

Untuk n apabila prima maka diberikan elemen $0 < a < n$, karena prima maka kita punya $FPB(n, a) = 1$ sehingga terdapat $s \cdot n + t \cdot a = 1$ yaitu $t \cdot 1 \equiv 1 \pmod{n}$ dan $t = a^{-1} \pmod{n}$ sehingga \mathbb{Z}_n memiliki invers maka \mathbb{Z}_n dengan n prima merupakan *field*.

2.8 Kriptografi

Kriptografi berasal dari Bahasa Yunani, *cypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu yang mempelajari tentang bagaimana cara menjaga keamanan pesan saat dikirimkan dari suatu tempat ke tempat lain (Ariyus, 2006).

Pengertian lain dari kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas (Sadikin, 2012).

Secara umum kriptografi adalah teknik pengamanan informasi di mana informasi diubah dengan kunci tertentu melalui enkripsi sehingga menjadi informasi yang baru yang tidak dapat dimengerti oleh orang yang tidak berhak menerimanya dan informasi tersebut hanya dapat diubah oleh orang yang berhak menerimanya melalui dekripsi (Nurdin A. P., 2017)

2.8.1 Sejarah Kriptografi

Kriptografi mempunyai sejarah yang sangat menarik dan panjang. Kriptografi sudah digunakan 4000 tahun yang lalu, diperkenalkan oleh orang-

orang Mesir untuk mengirim pesan ke pasukan militer yang berada di lapangan agar pesan tersebut tidak terbaca oleh pihak musuh walaupun kurir pembawa pesan tertangkap oleh musuh. Dikisahkan, pada zaman Romawi kuno pada suatu saat, ketika Julius Caesar ingin mengirimkan pesan rahasia kepada seorang jenderal di medan perang. Pesan tersebut harus dikirimkan melalui seorang kurir, karena pesan tersebut bersifat rahasia, Julius Caesar tidak ingin pesan rahasia tersebut sampai terbuka di jalan. Julius Caesar kemudian memikirkan bagaimana mengatasinya, ia kemudian mengacak pesan tersebut hingga menjadi suatu pesan yang tidak dapat dipahami oleh siapapun terkecuali oleh jenderal saja. Tentu sang jenderal telah diberi tahu sebelumnya bagaimana cara membaca pesan yang teracak tersebut, yang dilakukan Julius Caesar adalah mengganti semua susunan alphabet dari a, b, c menjadi susunan a menjadi d, b menjadi e, c menjadi f, dan seterusnya (Ariyus, 2006).

Saat ini perkembangan teknologi terus mengalami perkembangan, karena hal itu metode kriptografi juga terus berkembang dan semakin beragam, keberagaman kriptografi yang berkembang saat ini dapat terlihat dari algoritma-algoritma yang digunakan pada konsep kriptografi yaitu pada proses enkripsi dan dekripsinya. Enkripsi merupakan proses mengubah teks biasa (*plaintext*) menjadi teks kode (*ciphertext*) sedangkan dekripsi yaitu proses mengubah teks kode (*ciphertext*) menjadi teks biasa (*plaintext*) agar dapat dibaca oleh penerima pesan. (Ariyus, 2006)

2.8.2 Algoritma Kriptografi

Algoritma merupakan urutan atau langkah-langkah untuk menyelesaikan masalah yang disusun secara sistematis. Algoritma kriptografi adalah langkah-

langkah bagaimana cara menyembunyikan pesan dari orang-orang yang berhak menerima pesan tersebut (Ariyus, 2008).

Dalam kriptografi terdapat istilah penting yang mendasari algoritma kriptografi, yaitu:

1. Enkripsi

Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Keuntungan dari enkripsi adalah kode asli kita tidak dapat dibaca oleh orang lain (Munir, 2006).

2. Dekripsi

Dekripsi adalah proses mengembalikan suatu informasi dengan cara tertentu dan sesuai dengan algoritma enkripsi yang dipakai. Dekripsi merupakan proses kebalikan dari proses enkripsi, mengubah *ciphertext* kembali ke dalam bentuk *plaintext* (Munir, 2006).

3. Key yaitu kunci yang digunakan dalam proses enkripsi dan dekripsi. Kunci yang digunakan tersusun dari alphabet, angka, symbol ataupun barisan bilangan biner. Dalam kriptografi terdapat dua macam kunci yaitu kunci *private* dan kunci *public*.

Berdasarkan kuncinya, algoritma kriptografi dibedakan menjadi tiga jenis (Ariyus, 2008) yaitu:

1. Algoritma Simetri

Algoritma simetri disebut juga dengan algoritma kunci rahasia. Merupakan algoritma kriptografi yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsinya. Karena hanya menggunakan kunci yang sama

maka si pengirim dan penerima pesan harus menjaga kerahasiaan kunci tersebut. Apabila kunci jatuh ke tangan orang lain, maka orang tersebut dapat mengenkripsi dan mendekripsi pesan. Untuk menjaga keamanannya maka setiap melakukan enkripsi dan dekripsi kuncinya harus sering diubah. Contoh algoritma simetri adalah Caesar cipher, vigenere cipher, hill cipher dan lain sebagainya.

2. Algoritma Asimetri

Algoritma asimetri disebut juga dengan algoritma kunci publik. Kriptografi kunci publik memiliki dua buah kunci yang berbeda pada proses enkripsi dan dekripsi. Kunci yang digunakan pada proses enkripsi adalah kunci publik sedangkan pada proses dekripsinya menggunakan *private key* sehingga kunci yang digunakan pada proses enkripsi dan dekripsi berbeda (Kamil, 2016).

3. Hash Function

Fungsi hash sering disebut dengan fungsi satu arah (*one-way function*), *message digest*, *fingerprint*, fungsi kompre dan *massage authentication code* (MAC). Hal ini merupakan fungsi matematika yang mengambil input panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap. Fungsi hash biasanya diperlukan bila ingin membuat sidik jari suatu pesan.

Dasar matematis yang mendasari kriptografi pada proses enkripsi adalah relasi antara dua himpunan yaitu antara himpunan *plaintext* dan himpunan *ciphertext*. Misalkan P menyatakan *plaintext* dan C menyatakan *chipertext*, maka fungsi enkripsi E memetakan P ke C ,

$$E(P) = C$$

Sedangkan fungsi dekripsi D memetakan C ke P

$$D(C) = P$$

Karena proses enkripsi dilanjutkan dengan dekripsi yaitu mengembalikan pesan rahasia ke pesan asal, maka persamaan berikut haruslah benar

$$D(E(P)) = P$$

Yang artinya, algoritma bersifat bijektif sehingga ciphertext dapat dikembalikan ke plaintext (Munir: 2019)

2.8.3 Kriptografi Klasik dan Modern

Berdasarkan jenisnya kriptografi dibagi menjadi dua, yaitu kriptografi klasik dan modern (Ariyus, 2008)

1. Kriptografi Klasik

Kriptografi Klasik merupakan algoritma yang menggunakan satu kunci untuk mengamankan data. Teknik ini merupakan teknik klasik dan sudah digunakan berabad-abad yang lalu, dua teknik dasar yang digunakan dalam kriptografi klasik yaitu:

a) Teknik Substitusi

Yaitu teknik dengan cara penggantian pada setiap karakter teks biasa (*plaintext*) dengan karakter lain.

b) Teknik Transposisi

Yaitu teknik yang menggunakan permutasi karakter.

2. Kriptografi Modern

Kriptografi modern merupakan suatu algoritma yang digunakan pada zaman sekarang, yang mana kriptografi modern mempunyai kerumitan yang sangat kompleks. (Ariyus, 2006).

2.9 Super Enkripsi

Super enkripsi (*multiple encryption*) merupakan salah satu teknik kriptografi yang menggabungkan dua atau lebih teknik substitusi dan *cipher* permutasi untuk mendapatkan *cipher* yang lebih kuat dan susah untuk dipecahkan (Ariyus, 2006)

Untuk melakukan teknik super enkripsi, harus terlebih dahulu memahami teknik substitusi dan transposisi. Dalam melakukan teknik super enkripsi, teks asli (*plaintext*) dienkripsi terlebih dahulu menggunakan teknik substitusi kemudian dienkripsi lagi menggunakan teknik transposisi atau sebaliknya sehingga didapatkan teks kode (*ciphertext*) yang selanjutnya didekripsikan dengan teknik transposisi kemudian dekripsi lagi menggunakan teknik substitusi atau sebaliknya.

2.10 Columnar Transposition

Columnar transposition merupakan *cipher* yang termasuk dalam teknik transposisi. Enkripsi yang digunakan dalam teknik transposisi adalah permutasi, teknik ini bekerja dengan mengacak posisi urutan huruf untuk menyembunyikan pesan yang dikirim. Model algoritma *columnar transposition* mirip dengan anagram namun dengan struktur yang lebih mudah.

Pada *columnar transposition* pesan ditulis dalam bentuk barisan dan dengan panjang yang tetap yang kemudian cara membacanya dari kolom demi kolom, banyaknya kolom ditentukan oleh panjang kunci yang digunakan. Baris pertama

pada tabel dituliskan urutan kunci, dan urutan pada kunci dituliskan berdasarkan urutan alphabet dari kunci tersebut. Misalkan penyandian dengan *plaintext* “INI ADALAH PESAN RAHASIA” dengan kunci ZEBRA, kunci dengan menggunakan kata ZEBRA dari urutan berdasarkan huruf alphabet maka urutannya adalah 6 3 2 4 1 5, dimana huruf A merupakan huruf awal pada urutan alphabet sehingga urutan pada kunci dengan kata ZEBRA bernilai 1, kemudian urutannya yang kedua adalah B dan yang ketiga adalah huruf E karena huruf E memiliki urutan lebih awal dibandingkan huruf yang lainnya pada kata ZEBRA, dan begitu pula seterusnya sehingga urutan dari kunci dengan kata ZEBRA ialah 6 3 2 4 1 5. Maka, penyandiannya adalah sebagai berikut:

Plainteks : INI ADALAH PESAN RAHASIA

Kunci : ZEBRA → 6 3 2 4 1 5

Tabel 2.1 Contoh Enkripsi Columnar Transposition

| | | | | | |
|---|---|---|---|---|---|
| 6 | 3 | 2 | 4 | 1 | 5 |
| I | N | I | | A | D |
| A | L | A | H | | P |
| E | S | A | N | | R |
| A | H | A | S | I | A |

Panjang kunci yang digunakan pada contoh diatas berukuran 6 sehingga banyaknya kolom adalah 6. Kemudian permutasi ditentukan menurut urutan alphabet huruf pada kunci. Dalam hal ini kata kunci adalah ZEBRA sehingga urutannya “6 3 2 4 1 5” yang kemudian untuk mendapatkan teks berkodenya ditulis berurutan dari kolom 1 dan seterusnya. Sehingga didapatkan hasil teks berkode “A IIAAANLSH HNSDPRAIAEA”. (Sinaga, dkk, 2018)

2.11 Hill Cipher

Hill cipher merupakan teknik kriptografi yang menerapkan aritmatika modulo. Teknik kriptografi ini menggunakan matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. *Hill cipher* diciptakan oleh Lester S. Hill pada tahun 1929. Maksud diciptakannya *hill cipher* adalah untuk menciptakan sebuah *cipher* yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. Dalam *hill cipher*, setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya. Sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya sehingga sangat sulit dipecahkan oleh kriptanalisis apabila dilakukan hanya dengan mengetahui berkas cipherteks saja (Forouzan, 2008).

Kunci yang digunakan pada teknik *hill cipher* adalah matriks A yang berukuran $n \times n$ dengan n adalah ukuran bloknya, matriks A yang digunakan untuk kunci hill cipher haruslah matriks yang memiliki *invertible* atau invers A^{-1} , karena kunci invers tersebut akan digunakan untuk proses dekripsi. Berikut ini proses enkripsi *hill cipher* yang ditulis secara matematis yaitu:

$$\begin{bmatrix} c1 \\ c2 \\ \vdots \\ cn \end{bmatrix} = A \begin{bmatrix} p1 \\ p2 \\ \vdots \\ pn \end{bmatrix} \text{mod } a$$

di mana

A = kunci matriks berukuran $n \times n$ yang memiliki invers

$c1, c2, \dots, cn$ = *ciphertext*

$p1, p2, \dots, pn$ = *plaintext*

a = ukuran karakter yang digunakan pada proses enkripsi dan dekripsi

Adapun algoritma enkripsi menggunakan teknik *hill cipher* adalah sebagai berikut:

1. Pilih sebuah matriks A berordo $n \times n$ yang memiliki invers untuk digunakan sebagai kunci.
2. Pilih *plaintext* yang akan dienkripsi, kemudian bagi *plaintext* dalam blok yang sesuai dengan ukuran kunci matriks nya.
3. Lakukan perhitungan, yaitu *plaintext* dalam bentuk blok masing-masing dikalikan dengan kunci matriks A . Sehingga didapatkan teks yang bersandi (*ciphertext*).

Sedangkan untuk proses dekripsi dengan teknik *hill cipher* pada dasarnya sama dengan proses enkripsi, namun kunci yang digunakan adalah invers modulo dari matriks kunci yang digunakan pada proses enkripsi. Secara matematis perhitungan dekripsi pada *hill cipher* adalah sebagai berikut:

$$\begin{bmatrix} p1 \\ p2 \\ \vdots \\ pn \end{bmatrix} = A^{-1} \begin{bmatrix} c1 \\ c2 \\ \vdots \\ cn \end{bmatrix} \text{mod } a$$

Adapun algoritma dekripsi menggunakan teknik *hill cipher* adalah sebagai berikut:

1. Hitung invers modulo dari matriks kunci yang dipakai pada proses enkripsi.
2. Cipherteks yang didapat pada proses enkripsi dibagi dalam blok yang sesuai dengan ukuran kunci matriks sebelumnya.
3. Lakukan perhitungan, yaitu *ciphertext* dikalikan dengan invers modulo dari matriks kunci A dengan modulo a , sehingga didapatkan kembali *plaintext* nya. (Setyaningsih, 2010)

2.12 Kriptografi dalam Kajian Keislaman

Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan. Pengamanan dilakukan dengan menyandi pesan tersebut dengan suatu kunci khusus. Penyandian pesan dengan suatu kunci khusus tersebut harus memiliki keamanan yang kuat dan tidak mudah disadap menggunakan transformasi pesan yang mudah dipahami oleh orang lain.

Amanat berarti dipercaya atau terpercaya, sehingga amanah berkaitan tentang menjaga suatu kepercayaan yang telah dititipkan oleh pemberi amanah. Amanah dapat berupa suatu benda, perkataan, perbuatan maupun pesan. Sehingga kerahasiaan suatu pesan termasuk dalam amanah yang harus dijaga dengan sebaik-baiknya. Amanah-amanah yang diberikan harus disampaikan kepada yang berhak menerimanya. Rasulullah SAW juga menghendaki setiap umatnya untuk bersikap amanah dalam segala apapun termasuk dalam menyampaikan suatu pesan informasi serta tidak berkhianat terhadap amanah yang telah diberikannya dan apabila berkhianat maka termasuk kepada orang-orang yang munafik, yang mana telah disampaikan pada salah satu Hadits:

Dari Abu Hurairah, bahwa Nabi SAW bersabda, “tanda-tanda orang yang munafik itu ada tiga: jika berbicara dia berdusta, jika berjanji dia mengingkari, dan jika diberi amanah dia berkhianat (HR. Al-Bukhari)

Menjaga amanah pada hakikatnya juga termasuk menjaga diri sendiri, karena dengan menjaga amanah maka dapat menjaga kepercayaan orang lain terhadap diri kita sendiri. Memiliki kepercayaan dari orang lain dapat membawa keberuntungan-keberuntungan didunia untuk diri kita sendiri.

BAB III PEMBAHASAN

Pada bab ini penulis membahas tentang bagaimana proses enkripsi dan dekripsi super enkripsi menggunakan algoritma *columnar transposition* dan modifikasi algoritma *hill cipher* dengan invers kiri matriks persegi panjang.

3.1 Proses Penyandian Super Enkripsi Menggunakan *Columnar*

***Transposition* dan Modifikasi *Hill Cipher* dengan Invers Kiri Matriks Persegi Panjang**

Berikut ini merupakan proses dari penyandian super enkripsi menggunakan *columnar transposition* dan modifikasi *Hill cipher* dengan invers kiri matriks persegi panjang.

3.1.1 Teknik Penyandian Algoritma *Columnar Transposition*

Algoritma *columnar transposition* merupakan algoritma simetri yaitu menggunakan kunci yang sama pada proses enkripsi dan dekripsinya. Pada metode super enkripsi ini, algoritma *columnar transposition* digunakan untuk menambah kerumitan penyandian pesan.

Algoritma *columnar transposition* telah diakui bahwa algoritma tersebut telah memenuhi syarat suatu sifat algoritma enkripsi, yaitu fungsi yang memetakan *plaintext* ke *ciphertext* bersifat bijektif sehingga *ciphertext* dapat dikembalikan ke *plaintext*.

Berikut ini merupakan algoritma dari proses enkripsi dan dekripsi menggunakan *columnar transposition*:

1. Menentukan kunci *columnar transposition*

2. Menuliskan *plaintext* dalam sebuah tabel dari baris pertama dan seterusnya dengan banyaknya kolom sesuai panjang kunci
3. Mengurutkan kolom sesuai urutan angka
4. Mendapatkan pesan teks yang telah disandikan (*ciphertext*)

Sedangkan proses dekripsi pesan menggunakan *columnar transposition* adalah dengan tahapan berikut ini:

1. Menentukan kunci *columnar transposition* yang digunakan pada proses enkripsinya
2. Menuliskan *ciphertext* dalam sebuah tabel dari kolom pertama dan seterusnya dengan banyaknya baris sesuai dengan panjang *ciphertext* dibagi dengan panjang kuncinya
3. Mengurutkan kolom sesuai urutan kunci
4. Mendapatkan teks asli (*plaintext*)

Adapun contoh implementasinya adalah sebagai berikut:

Misalkan dengan *plaintext*: UIN Maulana Malik Ibrahim

Kunci: PARIS → 3 1 4 2 5

Untuk mendapatkan *ciphertext* nya, maka tulislah *plaintext* dalam sebuah tabel dengan banyaknya kolom sesuai panjang kunci. Dalam hal ini kuncinya adalah PARIS dengan panjang kunci 5, sehingga:

Tabel 3.1 Enkripsi Berdasarkan Urut Kunci

| 3 | 1 | 4 | 2 | 5 |
|---|---|---|---|---|
| U | I | N | | M |
| a | u | l | a | n |
| a | | M | a | l |
| i | k | | I | b |
| r | a | h | i | m |

Kemudian tulis huruf-huruf yang ada dalam kolom sesuai dengan urutan angka pada baris pertama, sehingga:

Tabel 3.2 Enkripsi Berdasarkan Urut Angka

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| I | | U | N | M |
| u | a | a | l | n |
| | a | a | M | l |
| k | I | i | | b |
| a | i | r | h | m |

Dari tabel di atas didapatkan *ciphertext* nya yaitu “**Iu ka aaIiUaaIrNIMhMnlbm**”

Sedangkan untuk proses dekripsi algoritma *columnar transposition* di mana untuk mengembalikan pesan yang bersandi menjadi pesan yang sebenarnya adalah sebagai berikut:

Ciphertext yang didapat dari proses enkripsi yaitu “Iu ka aaIiUaaIrNIMhMnlbm”. Kemudian hitung panjang *ciphertext*, yang mana *ciphertext* diatas memiliki panjang 25, kemudian bagi panjang *ciphertext* dengan panjang kunci yang di gunakan pada proses enkripsi, sehingga banyak baris adalah $\frac{25}{5} = 5$.

Petakan *ciphertext* ke dalam tabel

Tabel 3.3 Dekripsi Berdasarkan Urut Angka

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| I | | U | N | M |
| u | a | a | l | n |
| | a | a | M | l |
| k | I | i | | b |
| a | i | r | h | m |

Kemudian diurutkan berdasarkan kunci, dalam hal ini kuncinya yaitu PARIS dengan urutan “3 1 4 2 5”. Sehingga

Tabel 3.4 Dekripsi Berdasarkan Urut Kunci

| 3 | 1 | 4 | 2 | 5 |
|---|---|---|---|---|
| U | I | N | | M |
| a | u | l | a | n |
| a | | M | a | l |
| i | k | | I | b |
| r | a | h | i | m |

Selanjutnya, tulis setiap teks per baris yaitu dari baris pertama sampai baris terakhir, sehingga di dapatkan kembali *plaintext*-nya yaitu **“UIN Maulana Malik Ibrahim”**

3.1.2 Teknik Modifikasi *Hill Cipher* dengan Invers Kiri Matriks Persegi

Panjang

Modifikasi algoritma *Hill cipher* dengan invers kiri yaitu dengan memodifikasi kunci yang digunakan pada proses penyandiannya. Dalam algoritma *Hill cipher* tradisional, kunci yang digunakan adalah matriks persegi $n \times n$. Sedangkan kunci yang digunakan pada modifikasi *Hill cipher* ini adalah matriks persegi panjang $m \times n$ di \mathbb{Z}_{53} .

Pada pembahasan ini, penulis mengambil data-data yang berupa huruf dikonversikan terlebih dahulu kedalam angka pada suatu himpunan \mathbb{Z}_{53} , sehingga perhitungannya dengan modulo 53. Setiap *plaintext* yang disandikan menggunakan metode ini dapat dikembalikan dengan baik ke *plaintext*-nya, maka akan dibuktikan bahwa *ciphertext* dapat kembali ke *plaintext*.

Misalkan x_1, x_2, \dots, x_n merupakan huruf *plaintext* dan y_1, y_2, \dots, y_n adalah *ciphertext*. Misalkan ambil sembarang suatu huruf *plaintext* $x_1, x_2 \in \mathbb{Z}_{53}$.

Kemudian ambil suatu kunci matriks persegi panjang 3×2 maka terdapat

$$A = \begin{bmatrix} a & b \\ c & d \\ e & f \end{bmatrix} \in M_{3 \times 2}(\mathbb{Z}_{53})$$

Implementasi terhadap rumus penyandian hill cipher yaitu

$$C = KP \text{ mod } n.$$

Sehingga,

$$P = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

$$C = \begin{bmatrix} a & b \\ c & d \\ e & f \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \text{ mod } 53$$

$$C = \begin{bmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \\ ex_1 + fx_2 \end{bmatrix} \text{ atau } \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \\ ex_1 + fx_2 \end{bmatrix}$$

Sehingga didapatkan persamaan

$$ax_1 + bx_2 \equiv y_1 \text{ modulo } 53 \quad (3.1)$$

$$cx_1 + dx_2 \equiv y_2 \text{ modulo } 53 \quad (3.2)$$

$$ex_1 + fx_2 \equiv y_3 \text{ modulo } 53 \quad (3.3)$$

Misalkan $a, b, c, d, e, f, x_1, x_2, y_1, y_2, y_3$ dan suatu n merupakan bilangan bulat elemen \mathbb{Z}_{53} dengan $n = 53$, sedemikian sehingga $(\Delta, n) = 1$ dengan $\Delta = ad - bc, \Delta = af - be, \Delta = cf - de$.

a) Kongruensi (1) dan (2)

Dengan menggunakan sistem kongruensi, kalikan kongruensi pertama dengan d dan yang kedua dengan b maka diperoleh

$$adx_1 + bdx_2 \equiv dy_1 \text{ modulo } 53$$

$$bcx_1 + bdx_2 \equiv by_2 \text{ modulo } 53$$

$$(ad - bc)x_1 \equiv dy_1 - by_2 \pmod{53}$$

$\Delta = ad - bc$, maka

$$\Delta x_1 \equiv dy_1 - by_2 \pmod{53}$$

Kemudian kalikan kedua ruas dengan $\bar{\Delta}$ yang merupakan invers dari Δ , sehingga diperoleh

$$x_1 \equiv \bar{\Delta}(dy_1 - by_2) \pmod{53}.$$

Dengan cara yang sama, kalikan kongruensi (1) dengan c dan kongruensi (2) dengan a maka diperoleh

$$acx_1 + adx_2 \equiv ay_2 \pmod{53}$$

$$acx_1 + bcx_2 \equiv cy_1 \pmod{53}$$

$$(ad - bc)x_2 \equiv ay_2 - cy_1 \pmod{53}$$

$$\Delta x_2 \equiv ay_2 - cy_1 \pmod{53}$$

Kemudian kalikan kedua ruas dengan $\bar{\Delta}$ yang merupakan invers dari Δ , sehingga diperoleh

$$x_2 \equiv \bar{\Delta}(ay_2 - cy_1) \pmod{53}.$$

Untuk mengecek bahwa x_1, x_2 adalah penyelesaian, maka

$$\begin{aligned} ax_1 + bx_2 &\equiv a\bar{\Delta}(dy_1 - by_2) \pmod{53} + b\bar{\Delta}(ay_2 - cy_1) \pmod{53} \\ &\equiv \bar{\Delta}(ady_1 - aby_2) \pmod{53} + \bar{\Delta}(aby_2 - bcy_1) \pmod{53} \\ &\equiv \bar{\Delta}(ady_1 - aby_2 + aby_2 - bcy_1) \pmod{53} \\ &\equiv \bar{\Delta}(ad - bc)y_1 \pmod{53} \\ &\equiv \bar{\Delta}\Delta y_1 \pmod{53} \end{aligned}$$

$$\equiv y_1(mod\ 53)$$

Selanjutnya

$$\begin{aligned} cx_1 + dx_2 &\equiv c\bar{\Delta}(dy_1 - by_2)(mod\ 53) + d\bar{\Delta}(ay_2 - cy_1)(mod\ 53) \\ &\equiv \bar{\Delta}(cdy_1 - bcy_2)(mod\ 53) + \bar{\Delta}(ady_2 - cdy_1)(mod\ 53) \\ &\equiv \bar{\Delta}(cdy_1 - bcy_2 + ady_2 - cdy_1)(mod\ 53) \\ &\equiv \bar{\Delta}(ad - bc)y_2(mod\ 53) \\ &\equiv \bar{\Delta}\Delta y_2(mod\ 53) \\ &\equiv y_2(mod\ 53) \end{aligned}$$

b) Kongruensi (1) dan (3)

Dengan menggunakan sistem kongruensi, kalikan kongruensi (1) dengan f dan kongruensi (3) dengan b maka diperoleh

$$afx_1 + bfx_2 \equiv fy_1 \text{ modulo } 53$$

$$bex_1 + bfx_2 \equiv by_3 \text{ modulo } 53$$

$$(af - be)x_1 \equiv fy_1 - by_3(mod\ 53)$$

$\Delta = af - be$, maka

$$\Delta x_1 \equiv fy_1 - by_3(mod\ 53)$$

Kemudian kalikan kedua ruas dengan $\bar{\Delta}$ yang merupakan invers dari Δ , sehingga diperoleh

$$x_1 \equiv \bar{\Delta}(fy_1 - by_3)(mod\ 53).$$

Dengan cara yang sama, kalikan kongruensi (1) dengan e dan kongruensi (3) dengan a maka diperoleh

$$aex_1 + afx_2 \equiv ay_3(mod\ 53)$$

$$aex_1 + bex_2 \equiv ey_1(mod\ 53)$$

$$(af - be)x_2 \equiv ay_3 - ey_1(mod\ 53)$$

$$\Delta x_2 \equiv ay_3 - ey_1 \pmod{53}$$

Kemudian kalikan kedua ruas dengan $\bar{\Delta}$ yang merupakan invers dari Δ , sehingga diperoleh

$$x_2 \equiv \bar{\Delta}(ay_3 - ey_1) \pmod{53}.$$

Untuk mengecek bahwa x_1, x_2 adalah penyelesaian, maka

$$\begin{aligned} ax_1 + bx_2 &\equiv a\bar{\Delta}(fy_1 - by_3) \pmod{53} + b\bar{\Delta}(ay_3 - ey_1) \pmod{53} \\ &\equiv \bar{\Delta}(afy_1 - aby_3) \pmod{53} + \bar{\Delta}(aby_3 - bey_1) \pmod{53} \\ &\equiv \bar{\Delta}(afy_1 - aby_3 + aby_3 - bey_1) \pmod{53} \\ &\equiv \bar{\Delta}(af - be)y_1 \pmod{53} \\ &\equiv \bar{\Delta}\Delta y_1 \pmod{53} \\ &\equiv y_1 \pmod{53} \end{aligned}$$

Selanjutnya

$$\begin{aligned} ex_1 + fx_2 &\equiv e\bar{\Delta}(fy_1 - by_3) \pmod{53} + f\bar{\Delta}(ay_3 - ey_1) \pmod{53} \\ &\equiv \bar{\Delta}(efy_1 - bey_3) \pmod{53} + \bar{\Delta}(afy_3 - efy_1) \pmod{53} \\ &\equiv \bar{\Delta}(efy_1 - bey_3 + afy_3 - efy_1) \pmod{53} \\ &\equiv \bar{\Delta}(af - be)y_3 \pmod{53} \\ &\equiv \bar{\Delta}\Delta y_3 \pmod{53} \\ &\equiv y_3 \pmod{53} \end{aligned}$$

c) Kongruensi (2) dan (3)

Dengan menggunakan sistem kongruensi, kalikan kongruensi (2) dengan f dan kongruensi (3) dengan d maka diperoleh

$$cfx_1 + dfx_2 \equiv fy_2 \pmod{53}$$

$$dex_1 + dfx_2 \equiv dy_3 \pmod{53}$$

$$(cf - de)x_1 \equiv fy_2 - dy_3 \pmod{53}$$

$\Delta = cf - de$, maka

$$\Delta x_1 \equiv fy_2 - dy_3 \pmod{53}$$

Kemudian kalikan kedua ruas dengan $\bar{\Delta}$ yang merupakan invers dari Δ , sehingga diperoleh

$$x_1 \equiv \bar{\Delta}(fy_2 - dy_3) \pmod{53}.$$

Dengan cara yang sama, kalikan kongruensi (2) dengan e dan kongruensi (3) dengan c maka diperoleh

$$cex_1 + cfx_2 \equiv cy_3 \pmod{53}$$

$$cex_1 + dex_2 \equiv ey_2 \pmod{53}$$

$$(cf - de)x_2 \equiv cy_3 - ey_2 \pmod{53}$$

$$\Delta x_2 \equiv cy_3 - ey_2 \pmod{53}$$

Kemudian kalikan kedua ruas dengan $\bar{\Delta}$ yang merupakan invers dari Δ , sehingga diperoleh

$$x_2 \equiv \bar{\Delta}(cy_3 - ey_2) \pmod{53}.$$

Untuk mengecek bahwa x_1, x_2 adalah penyelesaian, maka

$$\begin{aligned} cx_1 + dx_2 &\equiv c\bar{\Delta}(fy_2 - dy_3) \pmod{53} + d\bar{\Delta}(cy_3 - ey_2) \pmod{53} \\ &\equiv \bar{\Delta}(cfy_2 - cdy_3) \pmod{53} + \bar{\Delta}(cdy_3 - dey_2) \pmod{53} \\ &\equiv \bar{\Delta}(cfy_2 - cdy_3 + cdy_3 - dey_2) \pmod{53} \\ &\equiv \bar{\Delta}(cf - de)y_2 \pmod{53} \\ &\equiv \bar{\Delta}\Delta y_2 \pmod{53} \\ &\equiv y_2 \pmod{53} \end{aligned}$$

Selanjutnya

$$\begin{aligned} ex_1 + fx_2 &\equiv e\bar{\Delta}(fy_2 - dy_3) \pmod{53} + f\bar{\Delta}(cy_3 - ey_2) \pmod{53} \\ &\equiv \bar{\Delta}(efy_2 - dey_3) \pmod{53} + \bar{\Delta}(cfy_3 - efy_2) \pmod{53} \end{aligned}$$

$$\begin{aligned}
&\equiv \bar{\Delta}(efy_2 - dey_3 + cfy_3 - efy_2)(mod\ 53) \\
&\equiv \bar{\Delta}(cf - de)y_3(mod\ 53) \\
&\equiv \bar{\Delta}\Delta y_3(mod\ 53) \\
&\equiv y_3(mod\ 53)
\end{aligned}$$

Maka terbukti bahwa x_1 dan x_2 yang merupakan *plaintext* kemudian dioperasikan sehingga menghasilkan y_1, y_2, y_3 yang merupakan hasil *ciphertextnya*, dapat dikembalikan ke huruf *plaintext* menggunakan inversnya. Karena n pada \mathbb{Z}_{53} merupakan prima maka menurut teorema \mathbb{Z}_{53} merupakan *field*, sehingga teori-teori yang telah dibahas dapat berlaku.

Berdasarkan pada torema 1, maka akan dibuktikan bahwa jika rank $A = n \leq m$ maka $A^- = (A^*A)^{-1}A^*$ dan rank $A = m \leq n$ maka $A^- = A^*(AA^*)^{-1}$

Bukti:

a) Akan dibuktikan bahwa untuk rank $A = n \leq m$ maka $A^- = (A^*A)^{-1}A^*$ memenuhi kondisi dari definisi 7 maka

Kondisi 1 ($BAB = B$)

$$\begin{aligned}
A^-AA^- &= ((A^*A)^{-1}A^*)A((A^*A)^{-1}A^*) \\
&= (A^*A)^{-1}(A^*A)(A^*A)^{-1}A^* \\
&= (A^*A)^{-1}IA^* \\
&= (A^*A)^{-1}A^* \\
&= A^-
\end{aligned}$$

Kondis 2 ($ABA = A$)

$$\begin{aligned}
AA^-A &= A((A^*A)^{-1}A^*)A \\
&= A(A^*A)^{-1}(A^*A) \\
&= AI
\end{aligned}$$

$$= A$$

Kondisi 3 $(BA)^* = BA$

$$\begin{aligned} (A^-A)^* &= (((A^*A)^{-1}A^*)A)^* \\ &= ((A^*A)^{-1}A^*)^*A^* \\ &= ((A^*A)^{-1})^*(A^*)^*A^* \\ &= (A^*A)^{-1}(A^*A) \\ &= ((A^*A)^{-1}A^*)A \\ &= A^-A \end{aligned}$$

Kondisi 4 $(AB)^* = AB$

$$\begin{aligned} (AA^-)^* &= (A((A^*A)^{-1}A^*))^* \\ &= A^*((A^*A)^{-1}A^*)^* \\ &= AA^- \end{aligned}$$

Dari pembuktian diatas, untuk rank $A = n \leq m$ artinya rank A haruslah rank kolom penuh untuk membentuk A^*A berukuran $n \times n$.

b) Akan dibuktikan bahwa untuk rank $A = m \leq n$ maka $A^- = A^*(AA^*)^{-1}$ memenuhi kondisi dari definisi 7, maka

Kondisi 1 $(BAB = B)$

$$\begin{aligned} A^-AA^- &= (A^*(AA^*)^{-1})A(A^*(AA^*)^{-1}) \\ &= A^*(AA^*)^{-1}(AA^*)(AA^*)^{-1} \\ &= A^*(AA^*)^{-1}I \\ &= A^*(AA^*)^{-1} \\ &= A^- \end{aligned}$$

Kondisi 2 $(ABA = A)$

$$AA^-A = A(A^*(AA^*)^{-1})A$$

$$\begin{aligned}
&= (AA^*)(AA^*)^{-1}A \\
&= IA \\
&= A
\end{aligned}$$

Kondisi 3 $(BA)^* = BA$

$$\begin{aligned}
(A^-A)^* &= ((A^*(AA^*)^{-1})A)^* \\
&= (A^*)^*((AA^*)^{-1})^*A^* \\
&= A^*(AA^*)^{-1}A \\
&= (A^*(AA^*)^{-1})A \\
&= A^-A
\end{aligned}$$

Kondisi 4 $(AB)^* = AB$

$$\begin{aligned}
(AA^-)^* &= (A(A^*(AA^*)^{-1}))^* \\
&= (AA^*(AA^*)^{-1})^* \\
&= I^* \\
&= I \\
&= AA^*(AA^*)^{-1} \\
&= AA^-
\end{aligned}$$

Maka, dari pembuktian diatas apabila diberikan suatu matriks persegi panjang A berukuran $m \times n$ untuk $\text{rank } A = n \leq m$ maka $A^- = (A^*A)^{-1}A^*$ sedangkan jika $\text{rank } A = m \leq n$ maka $A^- = A^*(AA^*)^{-1}$. Untuk memenuhi syarat injektif maka panjang *plaintext* haruslah lebih kecil atau sama dengan panjang *ciphertext*, sehingga untuk rank A haruslah $\text{rank } A = n \leq m$ yaitu rank kolom penuh rank $A = n$ maka $A^- = (A^*A)^{-1}A^*$. Karena perhitungan di $\mathbb{Z}_{53} \in \mathbb{Z}_p$ maka $A^* = A^T$. Sehingga

Untuk $\text{rank } A = n \leq m$ didapatkan

$$A^- = (A^T A)^{-1} A^T$$

Pada modifikasi algoritma hill cipher dengan matriks persegi panjang ini dengan $n = 53$ sehingga $\mathbb{Z}_{53} \in \mathbb{Z}_p$, dengan $n \leq m$ maka $P = (\mathbb{Z}_{53})^n$ dan $C = (\mathbb{Z}_{53})^m$ dimana $K = \{k \in K_{m \times n}(\mathbb{Z}_{53}) | \text{rank}(K) = n\}$. Sehingga untuk suatu $k \in K$ dan $x = (x_1, x_2, \dots, x_n) \in P, y = (y_1, y_2, \dots, y_n) \in C$ maka didapatkan

$$E_k(x) = Kx$$

dan

$$D_k(y) = K^- y$$

Dengan $K^- = (A^T A)^{-1} A^T$

Proses penyandian pada modifikasi algoritma *Hill cipher* dengan invers kiri dibutuhkan konversi alphabet ke dalam angka, maka digunakan tabel konversi berikut ini untuk proses enkripsi dan dekripsi.

Tabel 3. 5 Konversi Modifikasi Hill Cipher

| | | | | | |
|--------|--------|--------|--------|------------|--------|
| A = 0 | B = 1 | C = 2 | D = 3 | E = 4 | F = 5 |
| G = 6 | H = 7 | I = 8 | J = 9 | K = 10 | L = 11 |
| M = 12 | N = 13 | O = 14 | P = 15 | Q = 16 | R = 17 |
| S = 18 | T = 19 | U = 20 | V = 21 | W = 22 | X = 23 |
| Y = 24 | Z = 25 | a = 26 | b = 27 | c = 28 | d = 29 |
| e = 30 | f = 31 | g = 32 | h = 33 | i = 34 | j = 35 |
| k = 36 | l = 37 | m = 38 | n = 39 | o = 40 | p = 41 |
| q = 42 | r = 43 | s = 44 | t = 45 | u = 46 | v = 47 |
| w = 48 | x = 49 | y = 50 | z = 51 | Spasi = 52 | |

Algoritma pada proses enkripsi menggunakan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang adalah sebagai berikut:

1. Menentukan matriks kunci yang memiliki invers untuk enkripsi pada modifikasi *hill cipher*

2. Membagi *plaintext* $p = x_1x_2x_3 \dots x_i$ menjadi matriks berorde $n \times 1$ dengan modulo 53 yang telah disebutkan dalam tabel sebelumnya sehingga

$$P = P_1P_2P_3 \dots P_i$$

dimana

$$P_1 = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \text{mod } 53, P_2 = \begin{bmatrix} x_{n+1} \\ x_{n+2} \\ \vdots \\ x_{2n} \end{bmatrix} \text{mod } 53 \dots P_i = \begin{bmatrix} x_{(i-1)n+1} \\ x_{(i-1)n+2} \\ \vdots \\ x_{in} \end{bmatrix} \text{mod } 53$$

3. Enkripsi kedua kunci K_e , panjang matriks dari orde $m \times n (m > n)$ akan diaplikasikan pada setiap P_i untuk mendapat kolom matrik C_i dari peningkatan orde m

$$C_i = (K_e P_i) \text{mod } 53 = (A P_i) \text{mod } 53$$

$$C = C_1C_2 \dots C_i$$

4. Mengkonversi matriks C kedalam huruf sehingga didapatkan *ciphertext* nya

$$C = y_1y_2 \dots$$

Sedangkan algoritma pada proses dekripsi menggunakan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang adalah sebagai berikut:

1. Menentukan invers kiri dari matriks kunci yang digunakan pada enkripsi
2. Ekspresikan cipher teks kedalam matriks kolom berorde m dan mengkonversi setiap karakter dalam matriks sebagai kode nomor menggunakan table konversi 3.5

$$C = C_1C_2 \dots C_i$$

3. Dekripsi dengan kunci $K_d = B$, lebar matriks berorde $n \times m (n < m)$ yang mana invers kiri A diaplikasikan pada setiap C_i dengan mod 53 untuk mendapatkan pesan dekripsi pertama P

$$P = P_1P_2 \dots P_i$$

4. Mengkonversi Matriks P kedalam huruf sehingga didapatkan kembali teks aslinya (*plaintext*)

Contoh enkripsi dan dekripsi:

Contoh 1

Misalkan *plaintext* yang akan digunakan adalah “UIN”

Sehingga proses enkripsinya yaitu:

Sebelumnya kita harus menentukan matriks kunci untuk enkripsi, misalkan dengan kunci

$$K_e = A = \begin{bmatrix} 0 & 4 \\ 9 & 0 \\ 0 & 3 \end{bmatrix}.$$

Kemudian, mengubah *plaintext* $P = UIN$ menjadi matriks 2×1 karena kunci

matriks berukuran 3×2 . Sehingga, $P = P_1 P_2 = \begin{bmatrix} U \\ I \end{bmatrix} \begin{bmatrix} N \end{bmatrix}$ di mana $P_1 = \begin{bmatrix} 20 \\ 8 \end{bmatrix}$ dan

$$P_2 = \begin{bmatrix} 13 \\ 52 \end{bmatrix}.$$

Selanjutnya mengenkripsi setiap P dengan kunci matriks yang sudah ditentukan,

menggunakan rumus penyandian *hill cipher* asli. Sehingga, Kalikan kunci

matriks dengan P_1 dan P_2 dengan perkalian modulo 53 untuk mendapat $C = C_1 C_2$

dimana

$$K_e = A = \begin{bmatrix} 0 & 4 \\ 9 & 0 \\ 0 & 3 \end{bmatrix}$$

$$C_1 = (K_e P_1) \bmod 53$$

$$C_2 = (K_e P_2) \bmod 53$$

maka

$$C_1 = \left(\begin{bmatrix} 0 & 4 \\ 9 & 0 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 20 \\ 8 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 32 \\ 180 \\ 24 \end{bmatrix} \bmod 53 = \begin{bmatrix} 32 \\ 21 \\ 24 \end{bmatrix}$$

$$C_2 = \left(\begin{bmatrix} 0 & 4 \\ 9 & 0 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 13 \\ 52 \end{bmatrix} \right) \text{mod } 53 = \begin{bmatrix} 208 \\ 117 \\ 156 \end{bmatrix} \text{mod } 53 = \begin{bmatrix} 49 \\ 11 \\ 50 \end{bmatrix}$$

$$C = \begin{bmatrix} 32 \\ 21 \\ 24 \end{bmatrix} \begin{bmatrix} 49 \\ 11 \\ 50 \end{bmatrix} = \begin{bmatrix} g \\ V \\ Y \end{bmatrix} \begin{bmatrix} x \\ L \\ y \end{bmatrix}$$

Maka didapatkan *ciphertext* $C = gVYxLy$

Dekripsi:

Di sini kita akan mendekripsi pesan yang sebelumnya telah dienkripsi, yaitu dengan *ciphertext* “ $gVYxLy$ ”.

Maka proses dekripsinya adalah sebagai berikut:

Untuk mendekripsi pesan tersebut kita harus mencari invers dari matriks kunci yang digunakan pada proses enkripsi, dimana pada proses enkripsi matriks kunci yang digunakan adalah

$$K_e = A = \begin{bmatrix} 0 & 4 \\ 9 & 0 \\ 0 & 3 \end{bmatrix}.$$

Maka akan dicari invers dari kunci matriks dengan $K^- = (A^T A)^{-1} A^T$

$$K^- = \left(\begin{bmatrix} 0 & 9 & 0 \\ 4 & 0 & 3 \end{bmatrix} \begin{bmatrix} 0 & 4 \\ 9 & 0 \\ 0 & 3 \end{bmatrix} \right)^{-1} \begin{bmatrix} 0 & 9 & 0 \\ 4 & 0 & 3 \end{bmatrix} (\text{mod } 53)$$

$$K^- = \left(\begin{bmatrix} 81 & 0 \\ 0 & 25 \end{bmatrix} \right)^{-1} \begin{bmatrix} 0 & 9 & 0 \\ 4 & 0 & 3 \end{bmatrix} (\text{mod } 53)$$

$$K^- = \frac{1}{2025} \begin{bmatrix} 25 & 0 \\ 0 & 81 \end{bmatrix} \begin{bmatrix} 0 & 9 & 0 \\ 4 & 0 & 3 \end{bmatrix} (\text{mod } 53)$$

$$K^- = 29 \begin{bmatrix} 25 & 0 \\ 0 & 28 \end{bmatrix} \begin{bmatrix} 0 & 9 & 0 \\ 4 & 0 & 3 \end{bmatrix} (\text{mod } 53)$$

$$K^- = \begin{bmatrix} 725 & 0 \\ 0 & 812 \end{bmatrix} \begin{bmatrix} 0 & 9 & 0 \\ 4 & 0 & 3 \end{bmatrix} (\text{mod } 53)$$

$$K^- = \begin{bmatrix} 0 & 6 & 0 \\ 15 & 0 & 51 \end{bmatrix} (\text{mod } 53)$$

$$K_d = B = \begin{bmatrix} 0 & 6 & 0 \\ 15 & 0 & 51 \end{bmatrix}$$

Mengekspresikan *ciphertext* “***bTH sn***” $C = bTH sn$ maka

$$C = \begin{bmatrix} g \\ V \\ Y \end{bmatrix} \begin{bmatrix} x \\ L \\ y \end{bmatrix} = \begin{bmatrix} 32 \\ 21 \\ 24 \end{bmatrix} \begin{bmatrix} 49 \\ 11 \\ 50 \end{bmatrix} = C_1 C_2$$

Selanjutnya, aplikasikan kunci dekripsi $K_d = \begin{bmatrix} 0 & 6 & 0 \\ 15 & 0 & 51 \end{bmatrix}$ dengan perhitungan dekripsi *hill cipher* asli pada C untuk mendapatkan P_1 dan P_2

$$P_1 = K_d C_1 \text{ mod } 53$$

$$P_2 = K_d C_2 \text{ mod } 53$$

Sehingga didapatkan dekripsi

$$P_1 = \left(\begin{bmatrix} 0 & 6 & 0 \\ 15 & 0 & 51 \end{bmatrix} \begin{bmatrix} 32 \\ 21 \\ 24 \end{bmatrix} \right) \text{ mod } 53 = \begin{bmatrix} 126 \\ 1704 \end{bmatrix} \text{ mod } 53 = \begin{bmatrix} 20 \\ 8 \end{bmatrix}$$

$$P_2 = \left(\begin{bmatrix} 0 & 6 & 0 \\ 15 & 0 & 51 \end{bmatrix} \begin{bmatrix} 49 \\ 11 \\ 50 \end{bmatrix} \right) \text{ mod } 53 = \begin{bmatrix} 66 \\ 3285 \end{bmatrix} \text{ mod } 53 = \begin{bmatrix} 13 \\ 52 \end{bmatrix}$$

$$P = \begin{bmatrix} 20 \\ 8 \end{bmatrix} \begin{bmatrix} 13 \\ 52 \end{bmatrix}$$

Kemudian dikonversikan pada alphabet menggunakan tabel yang telah tertera sehingga didapatkan teks asli

$$P = P_1 P_2 = \begin{bmatrix} 20 \\ 8 \end{bmatrix} \begin{bmatrix} 13 \\ 52 \end{bmatrix} = \begin{bmatrix} U \\ I \end{bmatrix} \begin{bmatrix} N \end{bmatrix}$$

Maka didapat teks asli “**UIN**”

Contoh 2

Misalkan plaintext nya yaitu “**Malang**”, dan ambil sebuah kunci matriks 3×2 yaitu:

$$K_e = A = \begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 1 & 5 \end{bmatrix}$$

Kemudian, mengubah *plaintext* $P = \text{Malang}$ menjadi matriks 2×1 karena kunci matriks berukuran 3×2 . Sehingga, $P = P_1 P_2 P_3 = \begin{bmatrix} M \\ a \end{bmatrix} \begin{bmatrix} l \\ a \end{bmatrix} \begin{bmatrix} n \\ g \end{bmatrix}$ di mana $P_1 = \begin{bmatrix} 12 \\ 26 \end{bmatrix}$, $P_2 = \begin{bmatrix} 37 \\ 26 \end{bmatrix}$ dan $P_3 = \begin{bmatrix} 39 \\ 32 \end{bmatrix}$.

Selanjutnya mengenkripsi setiap P dengan kunci matriks yang sudah ditentukan, menggunakan rumus penyandian *hill cipher* asli. Sehingga, kalikan kunci matriks dengan P_1 , P_2 dan P_3 dengan perkalian modulo 53 untuk mendapat $C = C_1 C_2 C_3$ dimana

$$C_1 = (K_e P_1) \bmod 53$$

$$C_2 = (K_e P_2) \bmod 53$$

$$C_3 = (K_e P_3) \bmod 53$$

Sehingga,

$$C_1 = \left(\begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 12 \\ 26 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 26 \\ 76 \\ 90 \end{bmatrix} \bmod 53 = \begin{bmatrix} 26 \\ 23 \\ 37 \end{bmatrix}$$

$$C_2 = \left(\begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 37 \\ 26 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 26 \\ 126 \\ 115 \end{bmatrix} \bmod 53 = \begin{bmatrix} 26 \\ 20 \\ 9 \end{bmatrix}$$

$$C_3 = \left(\begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 39 \\ 32 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 32 \\ 142 \\ 135 \end{bmatrix} \bmod 53 = \begin{bmatrix} 32 \\ 36 \\ 29 \end{bmatrix}$$

$$C = \begin{bmatrix} 26 \\ 23 \\ 37 \end{bmatrix} \begin{bmatrix} 26 \\ 20 \\ 9 \end{bmatrix} \begin{bmatrix} 32 \\ 36 \\ 29 \end{bmatrix} = \begin{bmatrix} a \\ X \\ l \end{bmatrix} \begin{bmatrix} a \\ U \\ J \end{bmatrix} \begin{bmatrix} g \\ k \\ d \end{bmatrix}$$

Maka didapatkan *ciphertext* $C = \mathbf{aXlaUJgkd}$.

Kemudian proses dekripsinya adalah sebagai berikut

Untuk mendekripsi pesan tersebut kita harus mencari invers dari matriks kunci yang digunakan pada proses enkripsi, dimana pada proses enkripsi matriks kunci yang digunakan adalah

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

Maka akan dicari invers dari kunci matriks dengan $K^- = (A^T A)^{-1} A^T$

$$K^- = \left(\begin{bmatrix} 0 & 2 & 1 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 1 & 3 \end{bmatrix} \right)^{-1} \begin{bmatrix} 0 & 2 & 1 \\ 1 & 2 & 3 \end{bmatrix} \pmod{53}$$

$$K^- = \left(\begin{bmatrix} 5 & 7 \\ 7 & 14 \end{bmatrix} \right)^{-1} \begin{bmatrix} 0 & 2 & 1 \\ 1 & 2 & 3 \end{bmatrix} \pmod{53}$$

$$K^- = \frac{1}{21} \begin{bmatrix} 14 & -7 \\ -7 & 5 \end{bmatrix} \begin{bmatrix} 0 & 2 & 1 \\ 1 & 2 & 3 \end{bmatrix} \pmod{53}$$

$$K^- = 48 \begin{bmatrix} 14 & 46 \\ 46 & 5 \end{bmatrix} \begin{bmatrix} 0 & 2 & 1 \\ 1 & 2 & 3 \end{bmatrix} \pmod{53}$$

$$K^- = \begin{bmatrix} 672 & 2208 \\ 2208 & 240 \end{bmatrix} \begin{bmatrix} 0 & 2 & 1 \\ 1 & 2 & 3 \end{bmatrix} \pmod{53}$$

$$K^- = \begin{bmatrix} 35 & 36 & 35 \\ 28 & 20 & 13 \end{bmatrix} \pmod{53}$$

Sehingga,

$$P_1 = (K^- C_1) \pmod{53}$$

$$P_2 = (K^- C_2) \pmod{53}$$

$$P_3 = (K^- C_3) \pmod{53}$$

$$P_1 = \left(\begin{bmatrix} 35 & 36 & 35 \\ 28 & 20 & 13 \end{bmatrix} \begin{bmatrix} 26 \\ 23 \\ 37 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 3033 \\ 1669 \end{bmatrix} \pmod{53} = \begin{bmatrix} 12 \\ 26 \end{bmatrix}$$

$$P_2 = \left(\begin{bmatrix} 35 & 36 & 35 \\ 28 & 20 & 13 \end{bmatrix} \begin{bmatrix} 26 \\ 20 \\ 9 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 1945 \\ 1245 \end{bmatrix} \pmod{53} = \begin{bmatrix} 37 \\ 26 \end{bmatrix}$$

$$P_3 = \left(\begin{bmatrix} 35 & 36 & 35 \\ 28 & 20 & 13 \end{bmatrix} \begin{bmatrix} 32 \\ 36 \\ 29 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 3431 \\ 1993 \end{bmatrix} \pmod{53} = \begin{bmatrix} 39 \\ 32 \end{bmatrix}$$

$$P = \begin{bmatrix} 12 \\ 26 \end{bmatrix} \begin{bmatrix} 37 \\ 26 \end{bmatrix} \begin{bmatrix} 39 \\ 32 \end{bmatrix}$$

Kemudian dikonversikan pada alphabet menggunakan tabel yang telah tertera sehingga didapatkan teks asli

$$P = P_1 P_2 P_3 = \begin{bmatrix} 12 \\ 26 \end{bmatrix} \begin{bmatrix} 37 \\ 26 \end{bmatrix} \begin{bmatrix} 39 \\ 32 \end{bmatrix} = \begin{bmatrix} M \\ a \end{bmatrix} \begin{bmatrix} l \\ a \end{bmatrix} \begin{bmatrix} n \\ g \end{bmatrix}$$

Maka didapat teks asli **“Malang”**

3.1.3 Teknik Penyandian Super Enkripsi Menggunakan *Columnar*

Transposition dan Modifikasi *Hill Cipher* dengan Invers Kiri Matriks

Persegi Panjang

Pada proses enkripsi dan dekripsi menggunakan super enkripsi ini, enkripsi dan dekripsi dilakukan dua kali yang bertujuan supaya pesan teks sulit untuk dipecahkan. Sehingga kerahasiaan dan keamanan suatu pesan dapat terjaga dengan baik. Untuk melakukan suatu penyandian pesan maka harus dipastikan bahwa pesan yang disandikan dapat kembali ke pesan asalnya, sehingga untuk memastikan hal tersebut akan dibuktikan bahwa penggabungan dua algoritma ini bersifat bijektif.

Lemma

Apabila terdapat pemetaan $f: A \rightarrow B$ dan $g: B \rightarrow C$ keduanya bersifat bijektif maka $g \circ f: A \rightarrow C$ juga bersifat bijektif

Bukti:

Diberikan suatu $f: A \rightarrow B$ bersifat bijektif

maka f bersifat surjektif dan injektif

dan diberikan $g: B \rightarrow C$ bijektif

maka g juga bersifat surjektif dan injektif

kita definisikan $h = g \circ f: A \rightarrow C$

akan dibuktikan bahwa $h = g \circ f: A \rightarrow C$ bersifat bijektif

a) Akan dibuktikan bahwa $h = g \circ f: A \rightarrow C$ surjektif

Karena f dan g surjektif maka dapat diketahui bahwa $f(A) = B$ dan $g(B) = C$ sedemikian sehingga

$$\begin{aligned}
 h(A) &= (g \circ f)(A) \\
 &= \{c \in C \mid (g \circ f)(a) = c, \text{ untuk suatu } a \in A\} \\
 &= \{c \in C \mid g(f(a)) = c, \text{ untuk suatu } a \in A\} \\
 &= \{c \in C \mid g(b) = c, \text{ untuk suatu } b \in B\} \\
 &= g(f(A)) \\
 &= g(B) \\
 &= C
 \end{aligned}$$

Maka terbukti bahwa h surjektif

b) Selanjutnya akan dibuktikan bahwa h injektif, maka akan ditunjukkan bahwa $h(a_1) = h(a_2)$ sehingga kita harus memiliki $a_1 = a_2$. Karena f dan g injektif maka

$$\begin{aligned}
 h(a_1) &= h(a_2) \\
 g(f(a_1)) &= g(f(a_2)) \\
 f(a_1) &= f(a_2) \\
 a_1 &= a_2
 \end{aligned}$$

Sehingga terbukti bahwa h juga injektif

Karena $h = g \circ f: A \rightarrow C$ bersifat surjektif dan injektif maka h bersifat bijektif, sehingga terbukti bahwa h injektif

Karena telah terbukti bahwa penggabungan dua fungsi bijektif bersifat bijektif maka penggabungan dua algoritma antara *columnar transposition* dan modifikasi *hill cipher* dapat dilakukan. Berikut ini proses enkripsi dan dekripsi

pada super enkripsi *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi.

a. Enkripsi

Adapun algoritma dari enkripsi pada metode super enkripsi pada suatu pesan adalah sebagai berikut:

1. Menentukan kunci *columnar transposition*
2. Menuliskan *plaintext* dalam sebuah tabel dari baris pertama dan seterusnya dengan banyaknya kolom sesuai panjang kunci
3. Mengurutkan kolom sesuai urutan angka
4. Mendapatkan pesan teks yang telah disandikan (*ciphertext*)
5. Menentukan matriks kunci yang memiliki invers untuk enkripsi pada modifikasi *hill cipher*
6. Membagi *plaintext* $p = x_1x_2x_3 \dots x_i$ menjadi matriks berorde $n \times 1$ dengan modulo 53 yang telah disebutkan dalam tabel sebelumnya sehingga

$$P = P_1P_2P_3 \dots P_i$$

dimana

$$P_1 = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \text{mod } 53, P_2 = \begin{bmatrix} x_{n+1} \\ x_{n+2} \\ \vdots \\ x_{2n} \end{bmatrix} \text{mod } 53 \dots P_i = \begin{bmatrix} x_{(i-1)n+1} \\ x_{(i-1)n+2} \\ \vdots \\ x_{in} \end{bmatrix} \text{mod } 53$$

7. Enkripsi kedua kunci K_e , panjang matriks dari orde $m \times n (m > n)$ akan diaplikasikan pada setiap P_i untuk mendapat kolom matrik C_i dari peningkatan orde m

$$C_i = (K_e P_i) \text{mod } 53 = (A P_i) \text{mod } 53$$

$$C = C_1 C_2 \dots C_i$$

8. Mengkonversi matriks C kedalam huruf sehingga didapatkan *ciphertext* nya

$$C = y_1 y_2 \dots$$

Berikut ini contoh penerapan enkripsi dengan algoritma super enkripsi *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang dengan pesan yang berisi “Jurusan Matematika”:

1. Misalkan kunci pada *columnar transposition* adalah “Melati”. Sehingga panjang kunci adalah 6 dengan urutan “5 2 4 1 6 3”
2. Menyusun *plaintext* dalam tabel secara mendatar dengan kolom tabel sebanyak 6, karena panjang kunci 6

Tabel 3.6 Enkripsi Super Enkripsi Terurut Kunci

| 5 | 2 | 4 | 1 | 6 | 3 |
|---|---|---|---|---|---|
| J | u | r | u | s | a |
| n | | M | a | t | e |
| m | a | t | i | k | a |

3. Mengurutkan tabel berdasarkan pada urutan baris pertama diikuti seluruh kolomnya dimulai dari urutan satu

Tabel 3.7 Enkripsi Super Enkripsi Terurut Angka

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| u | u | a | r | J | s |
| a | | e | M | n | t |
| i | a | a | t | m | k |

4. Sehingga didapatkan *chipertext* pertama yaitu “uuiu aaearMtJnmstk” yang merupakan *plaintext* untuk enkripsi pada modifikasi *hill cipher*
5. Menentukan matriks kunci untuk enkripsi pada modifikasi *hill cipher*, misalkan matriks kunci yang digunakan adalah

$$K_e = A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix}$$

6. Menyusun *plaintext* “uauu aaearMtJnmstk” dalam matriks $n \times 1$ dengan modulo 53 pada tabel 3.6 sehingga

$$P = P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 = \begin{bmatrix} u \\ a \end{bmatrix} \begin{bmatrix} i \\ u \end{bmatrix} \begin{bmatrix} \\ a \end{bmatrix} \begin{bmatrix} a \\ e \end{bmatrix} \begin{bmatrix} a \\ r \end{bmatrix} \begin{bmatrix} M \\ t \end{bmatrix} \begin{bmatrix} J \\ n \end{bmatrix} \begin{bmatrix} m \\ s \end{bmatrix} \begin{bmatrix} t \\ k \end{bmatrix}$$

Di mana

$$P_1 = \begin{bmatrix} u \\ a \end{bmatrix} = \begin{bmatrix} 46 \\ 26 \end{bmatrix}$$

$$P_6 = \begin{bmatrix} M \\ t \end{bmatrix} = \begin{bmatrix} 12 \\ 45 \end{bmatrix}$$

$$P_2 = \begin{bmatrix} i \\ u \end{bmatrix} = \begin{bmatrix} 34 \\ 46 \end{bmatrix}$$

$$P_7 = \begin{bmatrix} J \\ n \end{bmatrix} = \begin{bmatrix} 9 \\ 39 \end{bmatrix}$$

$$P_3 = \begin{bmatrix} \\ a \end{bmatrix} = \begin{bmatrix} 52 \\ 26 \end{bmatrix}$$

$$P_8 = \begin{bmatrix} m \\ s \end{bmatrix} = \begin{bmatrix} 38 \\ 44 \end{bmatrix}$$

$$P_4 = \begin{bmatrix} a \\ e \end{bmatrix} = \begin{bmatrix} 26 \\ 30 \end{bmatrix}$$

$$P_9 = \begin{bmatrix} t \\ k \end{bmatrix} = \begin{bmatrix} 45 \\ 36 \end{bmatrix}$$

$$P_5 = \begin{bmatrix} a \\ r \end{bmatrix} = \begin{bmatrix} 26 \\ 43 \end{bmatrix}$$

7. Menerapkan matriks kunci K_e pada setiap P_i untuk mendapatkan *ciphertext*

$C = C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8 C_9$, dimana $C_i = (K_e P_i) \bmod 53$ sehingga:

$$C_1 = \left(\begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 46 \\ 26 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 92 \\ 78 \\ 184 \end{bmatrix} \bmod 53 = \begin{bmatrix} 39 \\ 25 \\ 25 \end{bmatrix}$$

$$C_2 = \left(\begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 34 \\ 46 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 68 \\ 138 \\ 136 \end{bmatrix} \bmod 53 = \begin{bmatrix} 15 \\ 32 \\ 30 \end{bmatrix}$$

$$C_3 = \left(\begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 52 \\ 26 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 104 \\ 78 \\ 208 \end{bmatrix} \bmod 53 = \begin{bmatrix} 51 \\ 25 \\ 49 \end{bmatrix}$$

$$C_4 = \left(\begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 26 \\ 30 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 52 \\ 90 \\ 104 \end{bmatrix} \bmod 53 = \begin{bmatrix} 52 \\ 37 \\ 51 \end{bmatrix}$$

$$C_5 = \left(\begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 26 \\ 43 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 52 \\ 129 \\ 104 \end{bmatrix} \bmod 53 = \begin{bmatrix} 52 \\ 23 \\ 51 \end{bmatrix}$$

$$C_6 = \left(\begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 12 \\ 45 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 24 \\ 135 \\ 48 \end{bmatrix} \bmod 53 = \begin{bmatrix} 24 \\ 29 \\ 48 \end{bmatrix}$$

$$C_7 = \begin{pmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 9 \\ 39 \end{bmatrix} \end{pmatrix} \text{mod } 53 = \begin{bmatrix} 18 \\ 117 \\ 36 \end{bmatrix} \text{mod } 53 = \begin{bmatrix} 18 \\ 11 \\ 36 \end{bmatrix}$$

$$C_8 = \begin{pmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 38 \\ 44 \end{bmatrix} \end{pmatrix} \text{mod } 53 = \begin{bmatrix} 76 \\ 132 \\ 152 \end{bmatrix} \text{mod } 53 = \begin{bmatrix} 23 \\ 26 \\ 46 \end{bmatrix}$$

$$C_9 = \begin{pmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 45 \\ 36 \end{bmatrix} \end{pmatrix} \text{mod } 53 = \begin{bmatrix} 90 \\ 108 \\ 180 \end{bmatrix} \text{mod } 53 = \begin{bmatrix} 37 \\ 2 \\ 21 \end{bmatrix}$$

8. Mengkonversi matriks C kedalam huruf sehingga didapatkan *ciphertext* nya

$$C = y_1 y_2 \dots$$

$$C = \begin{bmatrix} 39 \\ 25 \\ 25 \end{bmatrix} \begin{bmatrix} 15 \\ 32 \\ 30 \end{bmatrix} \begin{bmatrix} 51 \\ 25 \\ 49 \end{bmatrix} \begin{bmatrix} 52 \\ 37 \\ 51 \end{bmatrix} \begin{bmatrix} 52 \\ 23 \\ 51 \end{bmatrix} \begin{bmatrix} 24 \\ 29 \\ 48 \end{bmatrix} \begin{bmatrix} 18 \\ 11 \\ 36 \end{bmatrix} \begin{bmatrix} 23 \\ 26 \\ 46 \end{bmatrix} \begin{bmatrix} 37 \\ 2 \\ 21 \end{bmatrix}$$

$$= \begin{bmatrix} n \\ Z \\ Z \end{bmatrix} \begin{bmatrix} P \\ g \\ e \end{bmatrix} \begin{bmatrix} z \\ Z \\ x \end{bmatrix} \begin{bmatrix} l \\ l \\ z \end{bmatrix} \begin{bmatrix} X \\ X \\ z \end{bmatrix} \begin{bmatrix} Y \\ d \\ w \end{bmatrix} \begin{bmatrix} S \\ L \\ k \end{bmatrix} \begin{bmatrix} X \\ a \\ u \end{bmatrix} \begin{bmatrix} l \\ B \\ V \end{bmatrix}$$

Sehingga *ciphertext* nya adalah “**nZZPgezZx lz XzYdwSLkXaulBV**”

a. Dekripsi

Kemudian dari proses enkripsi sebelumnya, pesan bersandi akan didekripsi dengan algoritma super enkripsi *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang dengan pesan atau *ciphertext* yang didapat dari proses enkripsi sebelumnya yaitu

“ nZZPgezZx lz XzYdwSLkXaulBV”.

Adapun algoritma dari proses dekripsi menggunakan metode tersebut adalah sebagai berikut:

1. Menentukan kunci *columnar transposition* yang digunakan pada proses enkripsinya

2. Menuliskan *ciphertext* dalam sebuah tabel dari kolom pertama dan seterusnya dengan banyaknya baris sesuai dengan panjang *ciphertext* dibagi dengan panjang kuncinya
3. Mengurutkan kolom sesuai urutan kunci
4. Mendapatkan teks asli (*plaintext*)
5. Menentukan invers kiri dari matriks kunci yang digunakan pada enkripsi
6. Ekspresikan cipher teks kedalam matriks kolom berorde m dan mengkonversi setiap karakter dalam matriks sebagai kode nomor menggunakan table konversi 3.5

$$C = C_1 C_2 \dots C_i$$

7. Dekripsi dengan kunci $K_d = B$, lebar matriks berorde $n \times m$ ($n < m$) yang mana invers kiri A diaplikasikan pada setiap C_i dengan mod 53 untuk mendapatkan pesan dekripsi pertama P

$$P = P_1 P_2 \dots P_i$$

8. Mengkonversi Matriks P kedalam huruf sehingga didapatkan kembali teks aslinya (*plaintext*).

sehingga dari proses enkripsi sebelumnya maka dekripsinya adalah sebagai berikut:

1. Menentukan invers dari matriks kunci, dimana matriks kuncinya adalah

$$K_e = A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix}$$

Maka akan dicari invers dari kunci matriks dengan $K^- = (A^T A)^{-1} A^T$

$$K^- = \left(\begin{bmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \right)^{-1} \begin{bmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \end{bmatrix} \pmod{53}$$

$$K^- = \left(\begin{bmatrix} 20 & 0 \\ 0 & 9 \end{bmatrix} \right)^{-1} \begin{bmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \end{bmatrix} \pmod{53}$$

$$K^- = \frac{1}{180} \begin{bmatrix} 20 & 0 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \end{bmatrix} \pmod{53}$$

$$K^- = 48 \begin{bmatrix} 9 & 0 \\ 0 & 20 \end{bmatrix} \begin{bmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \end{bmatrix} \pmod{53}$$

$$K^- = \begin{bmatrix} 432 & 0 \\ 0 & 960 \end{bmatrix} \begin{bmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \end{bmatrix} \pmod{53}$$

$$K^- = \begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \pmod{53}$$

2. Mengekspresikan *ciphertext* “ **nZZPgezZx lz XzYdwSLkXaulBV**”

kedalam matriks kolom berorde m sehingga

$$\begin{aligned} C &= \begin{bmatrix} n \\ Z \\ Z \end{bmatrix} \begin{bmatrix} P \\ g \\ e \end{bmatrix} \begin{bmatrix} Z \\ Z \\ x \end{bmatrix} \begin{bmatrix} l \\ l \\ z \end{bmatrix} \begin{bmatrix} X \\ X \\ z \end{bmatrix} \begin{bmatrix} Y \\ d \\ w \end{bmatrix} \begin{bmatrix} S \\ L \\ k \end{bmatrix} \begin{bmatrix} X \\ a \\ u \end{bmatrix} \begin{bmatrix} l \\ B \\ V \end{bmatrix} \\ &= \begin{bmatrix} 39 \\ 25 \\ 25 \end{bmatrix} \begin{bmatrix} 15 \\ 32 \\ 30 \end{bmatrix} \begin{bmatrix} 51 \\ 25 \\ 49 \end{bmatrix} \begin{bmatrix} 52 \\ 37 \\ 51 \end{bmatrix} \begin{bmatrix} 52 \\ 23 \\ 51 \end{bmatrix} \begin{bmatrix} 24 \\ 29 \\ 48 \end{bmatrix} \begin{bmatrix} 18 \\ 11 \\ 36 \end{bmatrix} \begin{bmatrix} 23 \\ 26 \\ 46 \end{bmatrix} \begin{bmatrix} 37 \\ 2 \\ 21 \end{bmatrix} \\ &= C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8 C_9 \end{aligned}$$

3. Mendekripsi dengan kunci dekripsi $K_d = B$ pada setiap C_i dengan mod 53

untuk mendapat P dimana $P_1 = (K_d C_i) \pmod{53}$ sehingga

$$P_1 = \left(\begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 39 \\ 25 \\ 25 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 1424 \\ 450 \end{bmatrix} \pmod{53} = \begin{bmatrix} 46 \\ 26 \end{bmatrix}$$

$$P_2 = \left(\begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 15 \\ 32 \\ 30 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 1200 \\ 576 \end{bmatrix} \pmod{53} = \begin{bmatrix} 34 \\ 46 \end{bmatrix}$$

$$P_3 = \left(\begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 51 \\ 25 \\ 49 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 2384 \\ 450 \end{bmatrix} \pmod{53} = \begin{bmatrix} 52 \\ 26 \end{bmatrix}$$

$$P_4 = \left(\begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 52 \\ 37 \\ 51 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 2464 \\ 666 \end{bmatrix} \pmod{53} = \begin{bmatrix} 26 \\ 30 \end{bmatrix}$$

$$P_5 = \left(\begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 52 \\ 23 \\ 51 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 2464 \\ 414 \end{bmatrix} \pmod{53} = \begin{bmatrix} 26 \\ 43 \end{bmatrix}$$

$$P_6 = \left(\begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 24 \\ 29 \\ 48 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 1920 \\ 522 \end{bmatrix} \bmod 53 = \begin{bmatrix} 12 \\ 45 \end{bmatrix}$$

$$P_7 = \left(\begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 18 \\ 11 \\ 36 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 1440 \\ 198 \end{bmatrix} \bmod 53 = \begin{bmatrix} 9 \\ 39 \end{bmatrix}$$

$$P_8 = \left(\begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 23 \\ 26 \\ 46 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 1840 \\ 468 \end{bmatrix} \bmod 53 = \begin{bmatrix} 38 \\ 44 \end{bmatrix}$$

$$P_9 = \left(\begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 37 \\ 2 \\ 21 \end{bmatrix} \right) \bmod 53 = \begin{bmatrix} 1264 \\ 36 \end{bmatrix} \bmod 53 = \begin{bmatrix} 45 \\ 36 \end{bmatrix}$$

4. Mengkonversi Matriks P kedalam huruf sehingga didapatkan kembali teks aslinya (*plaintext*)

$$P = \begin{bmatrix} 46 \\ 26 \end{bmatrix} \begin{bmatrix} 34 \\ 46 \end{bmatrix} \begin{bmatrix} 52 \\ 26 \end{bmatrix} \begin{bmatrix} 26 \\ 30 \end{bmatrix} \begin{bmatrix} 26 \\ 43 \end{bmatrix} \begin{bmatrix} 12 \\ 45 \end{bmatrix} \begin{bmatrix} 9 \\ 39 \end{bmatrix} \begin{bmatrix} 38 \\ 44 \end{bmatrix} \begin{bmatrix} 45 \\ 36 \end{bmatrix}$$

$$= \begin{bmatrix} u \\ a \end{bmatrix} \begin{bmatrix} i \\ u \end{bmatrix} \begin{bmatrix} \\ a \end{bmatrix} \begin{bmatrix} a \\ e \end{bmatrix} \begin{bmatrix} a \\ r \end{bmatrix} \begin{bmatrix} M \\ t \end{bmatrix} \begin{bmatrix} J \\ n \end{bmatrix} \begin{bmatrix} m \\ s \end{bmatrix} \begin{bmatrix} t \\ k \end{bmatrix}$$

Sehingga didapatkan hasil dekripsi dari modifikasi *hill cipher* yaitu **“uuiu
aaearMtJnmstk”**

5. Hasil dekripsi dari modifikasi *hill cipher* didekripsikan kembali menggunakan *columnar transposition* dengan kunci “Melati” sehingga panjang kunci 6 dengan urutan “5 2 4 1 6 3”

6. Memetakan *ciphertext* kedalam tabel, panjang *ciphertext* yaitu 18 sehingga

$\frac{18}{6} = 3$ maka banyaknya baris pada tabel adalah 3 sedangkan banyak

kolomnya 6 karena panjang kunci yaitu

Tabel 3.8 Dekripsi Super Enkripsi Terurut Angka

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| u | u | a | r | J | s |
| a | | e | M | n | t |
| i | a | a | t | m | k |

7. Mengurutkan sesuai urutan kunci yaitu “5 2 4 1 6 3”

Tabel 3.9 Dekripsi Super Enkripsi Terurut Kunci

| 5 | 2 | 4 | 1 | 6 | 3 |
|---|---|---|---|---|---|
| J | u | r | u | s | a |
| n | | M | a | t | e |
| m | a | t | i | k | a |

8. Sehingga didapatkan hasil dekripsi sesuai *plaintextnya* yaitu “**Jurusan Matematika**”.

3.2 Kajian Keislaman

Seiring dengan berkembangnya zaman serta kemajuan teknologi semakin banyak hal yang mudah dilakukan salah satunya menyampaikan pesan. Namun, ketika pesan dikirimkan ke tempat lain maka terdapat kemungkinan bahwa pesan diambil atau diakses oleh pihak-pihak yang tidak bertanggung jawab, oleh karenanya dilakukan penyandian terhadap pesan tersebut. Penyandian pesan bertujuan untuk melindungi suatu pesan dari orang yang tidak berhak menerimanya. Sebagaimana yang telah disampaikan sebelumnya bahwa menjaga kerahasiaan suatu pesan termasuk dalam amanah yang harus dijaga dengan sebaik-baiknya yaitu disampaikan kepada orang yang berhak menerimanya. Sebagaimana tercantum dalam Al-Quran mengenai pentingnya dalam menjaga amanah, yaitu pada surat An-Nisa’ ayat 58:

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

Berdasarkan pada surat An-Nisa’ ayat 58, agar pesan dapat disampaikan kepada orang yang berhak menerimanya maka dilakukan penyandian terhadap

pesan tersebut. Untuk memperkuat keamanan pada pesan, dapat dilakukan penyandian dengan mengkombinasikan dua metode penyandian atau dapat disebut juga dengan super enkripsi. Dalam hal ini, pada penelitian ini digunakan metode *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang pada penyandian pesan sehingga pesan dapat terjaga keamanannya.

Kemudian, karena begitu pentingnya menjaga sebuah amanah maka apabila berkhianat terhadap amanah yang telah diberikan tergolong orang-orang yang munafik. sebagaimana menurut sabda Rasulullah SAW dalam sebuah hadits yang diriwayatkan oleh Bukhari bahwa ciri-ciri orang yang munafik itu ada tiga dan salah satunya ialah orang yang apabila diberi amanah dia berkhianat. Adapun hadits tersebut berbunyi:

Dari Abu Hurairah, bahwa Nabi SAW bersabda, “tanda-tanda orang yang munafik itu ada tiga: jika berbicara dia berdusta, jika berjanji dia mengingkari, dan jika diberi amanah dia berkhianat (HR. Al-Bukhari)

BAB IV PENUTUP

4.1 Kesimpulan

Berdasarkan pembahasan di atas, dapat disimpulkan bahwa penyandian super enkripsi menggunakan *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang menghasilkan pesan akhir yang tidak mengubah, menambah maupun mengurangi pesan awal, sehingga dapat diimplementasikan pada pesan dengan baik. Penyandian dengan metode *hill cipher* dapat dimodifikasi menggunakan matriks persegi panjang pada kunci yang digunakannya, dimana pada metode *hill cipher* klasik matriks yang digunakan pada kunci ialah matriks persegi yang memiliki invers. Modifikasi *hill cipher* dengan invers kiri matriks persegi panjang ini menyebabkan *ciphertext* yang dihasilkan pada proses enkripsi lebih panjang dari *plaintextnya*, hal ini dapat menambah keamanan penyandian karena panjang *plaintext* tidak sama dengan *ciphertext* nya. Sehingga dengan menggunakan super enkripsi yang mengkombinasikan *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang didapatkan keamanan ganda. Keamanan pertama terletak pada keamanan menggunakan *columnar transposition* kemudian yang kedua ialah pada *hill cipher* yang telah dimodifikasi menggunakan invers kiri matriks persegi panjang. Dari algoritma *hill cipher* juga telah memiliki keamanan yang tinggi, karena *hill cipher* yang digunakan pada super enkripsi ini merupakan *hill cipher* yang telah dimodifikasi.

4.2 Saran

Penelitian ini membahas mengenai super enkripsi yang mengkombinasikan algoritma *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi. Pada penelitian selanjutnya di sarankan menggunakan kombinasi lain.

DAFTAR PUSTAKA

- Al-Bukhary, Muhammad bin Ismail bin Ibrahim bin alMughirah, *al-Jami as-Sahih al-Musnad min hadis Rasulullah saw wasunnatih wa ayatih* Sahih Bukhari, juz. 1. Hal.58
- Ariyus, D. 2008. *Pengantar Ilmu Kriptografi*. Yogyakarta: C.V Andi Offset.
- Ariyus, D. 2006. *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu.
- Anton, Howard. 2000. *Penerapan Aljabar Linear*. Jakarta: Erlangga.
- Departemen Agama RI. *Al-Quran dan Terjemahannya*. Juz 1-30. Bandung: PT. Cordoba Internasional Indonesia
- Forouzan, Behrouz. 2008. *Cryptography and Network Security*. McGraw-Hill.
- Gazali, Wikaria. 2005. *Matriks & Transformasi Linear*. Yogyakarta: Graha Ilmu.
- Irawan, W.H, dkk. 2014. *Pengantar Teori Bilangan*. Malang: UIN Maliki Press.
- Kamil, F. 2016. *Implementasi Kriptografi dengan Menggunakan Algoritma Advanced Encryption Standard (AES 256) dan Lempel Ziv Welech (LZW)*. Tangerang: STMIK Raharja.
- Kaur, Ravinder. 2019. *Rectangular Matrix with Left Inverse For variation in Hill Cipher: Communication Safe Guard*. 1234-1240 Vol. 21 Issue 8
- Kromodimoeljo, S. 2010. *Teori dan Aplikasi Kriptografi*. Jakarta: SPK IT Consuling
- Marjono, Marsudi. 2012. *Aljabar Linear*. Malang: Tim UB Press.
- Munir, Rinaldi. 2019. *Kriptografi*. Bandung: Penerbit Informatika
- Munir, Rinaldi. 2006. *Diktat Kuliah IF 2153 Matematika Diskrit*, Edisi Keempat Departemen Teknik Informatika, Institut Teknologi Bandung.
- Munir, Rinaldi. 2002. *Matematika Diskrit (Revisi kelima)*. Bandung: Informatika.
- Nurdin, A. P. 2017. *Analisa dan Implementasi Kriptografi pada pesan Rahasia Menggunakan Algoritma Cipher Transposition*. *Jurnal Elektronik Sistem Informasi dan Komputer*, 1-10 Vol.3 N0.1
- Raisinghania, M.D., & Aggarwal, R.S. 1980. *Modern Algebra*. New Delhi: S.Chand & Company Ltd.

- Reswan, Yuza dkk. 2018. *Implementasi Kompilasi Algoritma Kriptografi Transposisi Columnar dan RSA untuk Pengamanan Pesan Rahasia*. 194-202 Vol. 4 No. 2
- Ruminta. 2014. *Matriks Persamaan Linier dan Pemrograman Linier*. Bandung: Rekayasa Sains
- Sadikin, R. (2012). *Kriptografi untuk Keamanan Jaringan*. Penerbit Andi.
- Setyaningsih, Emy. 2010. *Konsep Super Enkripsi untuk Penyandian Citra Warna Menggunakan Kombinasi Hill Cipher dan Playfair Cipher*. 38-48 Vol. 6 No.1
- Sinaga, Daurat dkk. 2018. *Teknik Super Enkripsi Menggunakan Transposisi Kolom Berbasis Vigenere Cipher Pada Citra Digital*. 57-64 Vol 14
- Soebagio A. Suharti dan Sukirman. 1993. *Struktur Aljabar*. Jakarta: Universitas Terbuka

RIWAYAT HIDUP



Fika Wahyuni, lahir di Indramayu pada tanggal 15 Mei 1998. Bertempat tinggal di Sukra Kabupaten Indramayu, Jawa Barat. Merupakan anak pertama dari Bapak Sarmanto dan Ibu Oom Romziah.

Perempuan yang akrab disapa Fika ini telah menempuh pendidikan formal mulai dari SD Negeri Tegaltaman I dan lulus pada tahun 2010. Kemudian menempuh pendidikan di SMP Islam Al-Ishlah Boarding School lulus pada tahun 2013. Melanjutkan pendidikan SMA di MAN Yogyakarta III lulus pada tahun 2016. Selanjutnya ditahun berikutnya tahun 2017 menempuh kuliah di Universitas Islam Negeri Maulana Malik Ibrahim Malang Jurusan Matematika.

Selama menjadi mahasiswa aktif mengikuti kegiatan organisasi serta komunitas yang ada di dalam dan di luar kampus, seperti menjadi pengurus HMJ Matematika UIN Malang (2017-2019). Anggota Koperasi Mahasiswa (KOPMA) Padang Bulan UIN Malang. Anggota GenBI Malang (2018-2020).



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 : Fika Wahyuni
NIM : 17610050
Fakultas/ Jurusan : Sains dan Teknologi/ Matematika
Judul Skripsi : Penyandian Super Enkripsi menggunakan Columnar Transposition dan Modifikasi Hill Cipher dengan Invers Kiri Matriks Persegi Panjang
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Muhammad Nafie Jauhari, M.Si

| No | Tanggal | Hal | Tanda Tangan |
|----|-------------------|-----------------------------------|--------------|
| 1 | 09 Maret 2021 | Konsultasi Bab I & II & III | 1. |
| 2 | 16 Maret 2021 | Revisi Bab I & II & III | 2. |
| 3 | 22 Maret 2021 | Konsultasi Kajian Agama Bab I | 3. |
| 4 | 24 Maret 2021 | Revisi Kajian Agama Bab I | 4. |
| 5 | 25 Maret 2021 | Konsultasi Kajian Agama Bab II | 5. |
| 6 | 26 Maret 2021 | ACC untuk diseminarkan | 6. |
| 7 | 04 Mei 2021 | Konsultasi Bab III | 7. |
| 8 | 25 Mei 2021 | Revisi Bab III | 8. |
| 9 | 08 September 2021 | Konsultasi Bab III | 9. |
| 10 | 02 Oktober 2021 | Revisi Bab III | 10. |
| 11 | 02 Oktober 2021 | Konsultasi Kajian Agama Bab III | 11. |
| 12 | 06 Oktober 2021 | Revisi Kajian Agama Bab III | 12. |
| 13 | 19 Oktober 2021 | Konsultasi Bab IV & Abstrak | 13. |
| 14 | 22 Oktober 2021 | ACC Keseluruhan untuk disidangkan | 14. |

Malang, 06 Desember 2021

Mengetahui,

Ketua Program Studi Matematika



Dr. Elly Susanti, M.Sc.

NIP. 19741129 200012 2 005