IMPLEMENTASI ALGORITMA SUPER ENKRIPSI (*HILL CIPHER* DAN TRANSPOSISI COLUMNAR) PADA PESAN TEKS

SKRIPSI

Oleh
NUR AZIZAH
NIM. 14610007

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

IMPLEMENTASI ALGORITMA SUPER ENKRIPSI (*HILL CIPHER* DAN TRANSPOSISI COLUMNAR) PADA PESAN TEKS

SKRIPSI

Diajukan kepada:
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk memenuhi Salah Satu persyaratan Dalam Memperoleh
Gelar Sarjana Matematika (S.Mat)

Oleh
Nur Azizah
NIM. 14610007

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

IMPLEMENTASI ALGORITMA SUPER ENKRIPSI (*HILL CIPHER* DAN TRANSPOSISI COLUMNAR) PADA PESAN TEKS

SKRIPSI

Oleh

Nur Azizah

NIM.14610007

Telah Diperiksa dan Disetujui untuk Diuji

Tanggal 24 Desember 2020

Pembimbing I,	Pembimbing II,
Muhammad Khudzaifah, M.Si	Mohammad Nafie Jauhari, M.Si
NIDT. 19900511 20160801 1 057	NIDT. 19870218 20160801 1 056

Mengetahui,
Ketua Jurusan Matematika

Dr. Usman Pagalay, M.Si
NIP.19650414 200312 1 001

IMPLEMENTASI ALGORITMA SUPER ENKRIPSI (*HILL CIPHER* DAN TRANSPOSISI COLUMNAR) PADA PESAN TEKS

SKRIPSI

Oleh

Nur Azizah

NIM.14610007

Telah Dipertahankan di Depan Dewan Penguji Skripsi
Dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
Untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 21 September 2020

Penguji Utama	: Dr. Hairur Rahman, M.Si	.....
Ketua Penguji	: Dr. Heni Widayani, M.Si	.....
Sekretaris Penguji	: Muhammad Khudzaifah, M.Si	.....
Anggota Penguji	: Mohammad Nafie Jauhari, M.Si	.....

Mengetahui,
Ketua Jurusan Matematika

Dr. Usman pagalay, M.Si
NIP.1965041420003121 1 001

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan dibawah ini:

Nama	: Nur Azizah
NIM	: 14610007
Jurusan	: Matematika
Fakultas	: Sains dan Teknologi
Judul Penelitian	: Implementasi Algoritma Super Enkripsi (Hill Cipher dan Transposisi Columnar pada Pesan Teks

Menyatakan dengan sebenar-benarnya bahwa hasil penelitian saya ini tidak memiliki unsur-unsur penjiplakan karya ilmiah yang pernah dilakukan atau dibuat oleh orang lain, kecuali yang terkutip dalam naskah ini dan disebutkan dalam sumber kutipan daftar pustaka. Apabila ternyata hasil penelitian ini terbukti terdapat unsur-unsur penjiplakan, maka saya bersedia untuk mempertangungjawabkan, serta diproes sesuai aturan yang berlaku.

Malang, 23 Maret 2021

Yang membuat pernyataan,

Nur Azizah

NIM. 14610007

MOTTO

“ Yen Pingin Mulyo, Kudu Wani Soro ”.

PERSEMBAHAN

Skripsi ini saya persembahkan untuk:

Ayahanda Sumi Harjono dan Ibu Muslichah yang senantiasa ikhlas dalam mendoakan, menasehati, menyemangati, dan memberi kasih sayang yang tak ternilaia, serta keluarga dan sahabat – sahabat yang telah menyemangati, menolong, dan menginspirasi bagi penulis.

KATA PENGANTAR

Segala puji dan syukur kepada Allah SWT yang telah memberikan segala rahmat, barokah dan nikmatnya berupa kesehatan, kesempatan, kekuatan, keinginan, serta kesabaran, sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Skripsi yang telah penulis susun ini berjudul "Implementasi Algoritma Super Enkripsi *(Hill Cipher dan* Transposisi Columnar*)* pada Pesan Teks". Sholawat serta salam penulis panjatkan kepada Rasulullah Muhammad SAW, yang telah menuntun manusia dari zaman jahiliyah menuju zaman yang terang benderang, yakni agama islam yang penuh dengan ilmu pengetahuan luar biasa saat ini.

Penulis menyadari bahwa penulisan skripsi ini tidak akan tersusun dengan baik tanpa adanya bantuan dari pihak-pihak yang terkait. Oleh karena itu, pada kesempatan ini penulis mengucapkan banyak terima kasih kepada semua pihak yang telah membantu penulis dalam penyusunan penulisan proposal skripsi ini.

Selanjutnya kami ucapkan terima kasih kepada :

1. Prof. Dr. H. Abd. Haris, M.Ag, selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Muhammad Khudzaifah, M.Si selaku dosen pembimbing I yang telah meluangkan waktu dan pikirannya untuk membimbing jalannnya proses penyelesaian skripsi ini.

4. Mohammad Nafie Jauhari, M. Si selaku dosen pembimbing II yang telah banyak memberikan arahan, nasihat, motivasi, dan berbagai pengalaman kepada penulis.
5. Dr. H. Turmudi, M.Si, Ph.D selaku dosen wali
6. Segenap sivitas akademika Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang terutama seluruh dosen, terima kasih atas segala ilmu dan bimbingannya.
7. Semua pihak yang ikut membantu dalam menyelesaikan skripsi ini terutama kepada Mariah lutfiyah sekeluarga yang telah berkontribusi dalam meminjamkan laptop selama proses pengerjaan skripsi ini.

Semoga skripsi ini dapat memberikan manfaat, tambahan ilmu, dan dapat menjadikan bahan pembelajaran untuk terus berinovasi kepada para pembaca. Amin Ya Robbal Alamin.

Malang, 03 Februari 2021

Penulis

DAFTAR ISI

ABSTRAK

Azizah, Nur. 2020**. Implementasi Algoritma Super Enkripsi (*Hill Cipher* dan Transposisi Columnar) Pada Pesan Teks.** Skripsi. Jurusan Matematika Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si. (II) Mohammad Nafie Jauhari, M.Si.

Kata kunci: Super enkripsi, *Hill cipher*, transposisi columnar, enkripsi, dekripsi.

Kriptografi adalah salah satu metode untuk mengamankan pesan untuk terjaga kerahasiannnya dengan mengimplementasikan enkripsi dan dekripsi pada pesan.Super enkripsi merupakan *cipher* substitusi dan *cipher*transposisi yang dikombinasikan untuk memperoleh *cipher*yang lebih kuat daripada hanya satu cipher saja.Tujuan dari penelitian ini adalah untuk mengetahui proses enkripsi dan dekripsi pada pesan teks menggunakan metode super enkripsi (*hill* cipher dan transposisi columnar). Proses super enkripsi merupakan gabungan proses enkripsi dan dekripsi kedua algoritma tersebut. *Hill* cipher termasuk algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis. Columnar merupakan kriptografi dengan konsep transposisi yang sangat mudah dipahami oleh pengirim maupun penerima pesan. *Hill* ciphermengenkripsi suatu *plaintext* yang disebut ciphertextlalu columnar mengenkripsi kembali hasil ciphertextnya. Hasil ciphertext tersebut merupakan plaintext columnar yang akan didekripsi oleh columnar dan didekripsikan kembali dengan *hill* cipher untuk mendapatkan plainteks seperti semula pesan terkirim.Hasil penelitian menunjukkan bahwa implementasi super enkripsi dengan proses enkripsi dan dekripsi pada algoritma *hill* cipher menggunakan kunci matriks 3×3 dengan operasi perkalian, penjumlahan, dan aritmatika modulo. Kunci pada algoritma transposisi columnar menyesuaikan dengan kunci cipher substitusinya. Menebak kunci tersebut membutuhkan beberapa pasangan elemen-elemen yang tepat untuk menghasilkan elemen yang sesuai. Selain itu, karakter plainteks yang sama tidak selalu meghasilkan karakter cipherteks yang sama sehingga tidak mudah menebak karakter sebenarnya. Hasil penelitian super enkripsi ini dapat diimplementasikan dengan menggunakan alat bantu program MAPLE yang dapat memudahkan jika menggunakan kunci matriks yang berordo lebih besar dan *plaintext*panjang.

ABSTRACT

Azizah, Nur. 2020. Implementation of Super Encryption Algorithms *(Hill Cipher* and Columnar Transposition) in Text Messaging. Essay. Department of Mathematics, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University of Malang. Advisor: (I) Muhammad Khudzaifah, M.Si. (II) Mohammad Nafie Jauhari, M.Si.

Key words: Super Encryption, *Hill cipher*, Columnar Transposition, Encryption, Decryption.

Cryptography is a method for securing messages to be kept secret by implementing encryption and decryption of messages. Super encryption is a substitution cipher and transposition cipher which are combined to obtain a cipher that is stronger than just one cipher. The purpose of this study was to determine the encryption and decryption process in text messages using super encryption methods (*hill* cipher and columnar transposition). The super encryption process is a combination of the encryption and decryption processes of the two algorithms. *Hill* cipher is a classic cryptographic algorithm that is very difficult to solve by cryptanalysts. Columnar is cryptography with a transposition concept that is very easy to understand by the sender and receiver of the message.*Hill* cipherencrypts a plaintext called ciphertext then columnar re-encrypts the ciphertext result. The result of the ciphertext is columnar plaintext which will be decrypted by the columnar and re-decrypted with the *hill* cipher to get the plaintextas originally the message was sent. The results showed that the implementation of super encryption with encryption and decryption processes in the *hill* cipher algorithm using a 3 × 3 matrix key with multiplication, addition, and modulo arithmetic operations. The key to the columnar transposition algorithm corresponds to the cipher key of the substitution. Guessing the key requires the correct number of pairs of elements to produce the correct element. In addition, the same *plaintext* characters do not always produce the same ciphertext characters so it is not easy to guess the real characters. The results of this super encryption research can be implemented using the MAPLE program tool which can make it easier if you use a matrix key with a larger order and a long *plaintext*.

ملخص

عزيزة ، نور ٢٠٢٠. **تنفيذ خوارزمية التشفير الفائق (تشفير التل والتبديل عمودي) في رسالة نصية** .مقال .قسم الرياضيات ، كلية العلوم والتكنولوجيا ، جامعة مولانا مالك إبراهيم مالانجالمشرف: (I) محمد خديفةالماجستير، م (II) . محمد نافع جوهري الماجستير، م.

الكلمات الرئيسية: التشفير الفائق ، تشفير التل ، التحويل العمودي ، النص العادي ، النص المشفركان الغرض.

التشفير هو طريقة لتأمين الرسائل التي يجب أن تظل سرية من خلال تنفيذ تشفير الرسائل وفك تشفيرها. التشفير الفائق هو تشفير بديل وشفرة تبديل يتم دمجها للحصول على تشفير أقوى (فائق) من تشفير واحد فقط. كان الغرض من هذه الدراسة هو تحديد عملية التشفير وفك التشفير في الرسائل النصية باستخدام طرق التشفير الفائقة (تشفير التل والتبديل العمودي). عملية التشفير الفائق عبارة عن مجموعة من عمليات التشفير وفك التشفير للخوارزميتين .هيلبتشفير هي خوارزمية تشفير كلاسيكية يصعب حلها بواسطة محللي التشفير. عمودي هو تشفير بمفهوم التحويل الذي يسهل فهمه من قبل المرسل والمستقبل للرسالة. يقوم تشفير التل بتشفير نص عادي يسمى النص المشفر ثم يقوم عمودي بإعادة تشفير نتيجة النص المشفر. نتيجة النص المشفر هي نص عادي عمودي سيتم فك تشفيره بواسطة عمودي وإعادة فك تشفيره باستخدام تشفير التل للحصول على النص العادي كما تم إرسال الرسالة في الأصل. أظهرت النتائج تنفيذ عمليات التشفير الفائق مع عمليات التشفير وفك التشفير في خوارزمية تشفير التل باستخدام مفتاح مصفوفة ٣ × ٣ مع عمليات حسابية للضرب والإضافة والنمط. يتوافق مفتاح خوارزمية التحويل العمودي مع مفتاح التشفير الخاص بالاستبدال. يتطلب تخمين المفتاح العدد الصحيح من أزواج العناصر لإنتاج العنصر الصحيح. بالإضافة إلى ذلك ، فإن نفس أحرف النص العادي لا تنتج دائمًا نفس أحرف النص المشفر ، لذلك ليس من السهل تخمين الأحرف الحقيقية. يمكن تنفيذ نتائج بحث التشفير الفائق هذا باستخدامنتائجالبحث.MAPLEالتي يمكن أن تسهل الأمر إذا كنت تستخدم مفتاح مصفوفة بترتيب أكبر ونص عادي طويل.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam kehidupan manusia sebagai makhluk sosial dibutuhkan suatu komunikasi antar sesama. Komunikasi bisa dilakukan dengan bertatap muka, lewat pesan, atau yang lainnya. Komunikasi lewat pesan atau berpesan atau beramanat tentunya hanya ditujukan kepada pihak tertentu sehingga pihak lain tidak akan mengetahuinya. Dengan demikian diperlukan suatu keamanan dalam menyampaikan pesan untuk menjamin kerahasiannya. Keamanan tersebut berupa kunci yang berguna untuk membuka pesan tersebut, dimana kunci hanya diketahui oleh pengirim dan penerima pesan.

Menjaga amanahmerupakan salah satu kewajiban dari merahasiakan data. Adapun Al-Quran yang berkaitan dengan pernyataan di atas telah dijelaskan dalam surah An-Nisa/ 4:58

إِنَّ اللَّهَ يَأْمُرُكُمْ أَنْ تُؤَدُّوا الْأَمَانَاتِ إِلَىٰ أَهْلِهَا وَإِذَا حَكَمْتُمْ بَيْنَ النَّاسِ أَنْ تَحْكُمُوا بِالْعَدْلِ ۚ إِنَّ اللَّهَ نِعِمَّا يَعِظُكُمْ بِهِ ۗ إِنَّ اللَّهَ كَانَ سَمِيعًا بَصِيرًا

Artinya: *"sesungguhnya Allah menyuruh kamu untuk menunaikan amanah kepada yang berhak menerimanya, dan (menyuruh kamu) apabila kalian menetapkan hukum diantara manusia supaya kamu menetapkannya dengan adil. Sesungguhnya Allah memberikan pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah maha mendengar lagi maha melihat" (Q.S An-Nisa/ 4: 58).*

Selain Al-Quran, berikut ini hadits yang berkaitan dengan kewajiban dalam menyampaikan pesan atau amana

أَدِّالْأَمَانَةَ إِلَى مَنِ ائْتَمَكَ وَلاَ تَخُنْ مَنْ خَانَكَ

Artinya :*"Tunaikan amanah kepada orang yang memberi amanah kepadamu, dan janganlah kamu menghianati orang yang menghianatimu"(diriwayatkan oleh Imam Ahmad dan Ahlussunan).*

Kriptografi adalah salah satu metode untuk mengamankan pesan untuk terjaga kerahasiannnya dengan mengimplementasikan enkripsi dan dekripsi pada pesan. Enkripsi adalah proses penyandian pesan asli (*plaintext*) menjadi pesan tersandi (*ciphertext*). Untuk proses mengembalikan *ciphertext* menjadi *plaintext* disebut dekripsi. Setiap proses enkripsi dan dekripsi membutuhkan parameter untuk transformasi yang dinamakan kunci (Munir, 2004).

Adapun fungsi matematika yang digunakan dalam proses enkripsi dan dekripsi disebut algoritma kriptografi (Kurniawan, 2008). Salah satu algoritma kriptografi yang dimanfaatkan adalah algoritma super enkripsi. Super enkripsi merupakan *cipher* substitusi dan *cipher* transposisi yang dikombinasikan untuk memperoleh *cipher*yang lebih kuat (super) daripada hanya satu *cipher* saja. Mula-mula *plaintex* dienkripsi dengan c*ipher* substitusi sederhana lalu dienkripsi lagi dengan *cipher* transposisi (atau bisa juga sebaliknya) (Munir, 2019).

Algoritma kriptografi klasik terdiri dari teknik substitusi dan teknik transposisi. Adapun teknik substitusi merupakan proses mensubstitusikan karakter-karakter yang terdapat pada *plaintext*. Sedangkan teknik tranposisi yaitu proses pertukaran karakter-karakter. Pada pembahasan ini digunakan algoritma *hill cipher* sebagai teknik substitusinya dan columnar sebagai teknik transposisinya. Algoritma *hill cipher* merupakan salah satu algoritma kriptografi

yang memanfaatkan aritmatika modulo dan matriks. Setiap karakter pada *plaintex* dan *ciphertext* dikonversikan kedalam angka. Proses enkripsi dilakukan dengan mengalikan matriks kunci dengan matriks *plaintext*, sedangkan proses dekripsi dengan mengalikan invers matriks kunci dengan *ciphertext*nya. Algoritma transposisi columnar merupakan salah satu algoritma kriptografi dimana pesan dituliskan berderet dari suatu panjang yang ditetapkan, lalu dibaca kembali secara perkolom dengan urutan pembacaan berdasarkan suatu kata kunci.Panjang deret ditentukan oleh panjang kata kunci juga. Urutan pembacaan kolom berdasarkan urutan kolomnya.

Berbagai metode kriptografi terus dikembangkan. Sebagaimana sebuah ilmu, kriptografi berkembang menjadi sesuatu yang jauh lebih kompleks.Penelitian sebelumnya yang digagas oleh Halim pada tahun 2017 mengenai proses super enkripsi dengan menggunakan *cipher* substitusi dan transposisi, dimana proses substitusinya menggunakan *caesar cipher* sedangkan transposisinya dengan cara mengubah susunan karakter menjadi kata baru yang tidak memiliki makna. Penelitian (Hidayat, dkk., 2013) menjelaskan tentang proses enkripsi dan dekripsi teks menggunakan *hill cipher* dengan kata kunci matriks persegi panjang. Penggunaan matriks persegi panjang menjadikan *ciphertext* lebih panjang dari *plaintext* sehingga menjadikan pesan lebih tersamarkan. Penelitian lain meneliti tentang implementasi kompilasi algoritma transposisi columnar dan RSA untuk pengamanan pesan rahasia. Penelitian (Reswan,dkk., 2018), hasil enkripsi didapatkan dari menyusun ulang karakter *plaintext* dengan posisi yang berbeda. Lalu *plaintext* ditulis dalam matriks dengan panjang kolom sesuai panjang karakter kuncinya. Setelah itu, *plaintext* ditulis

perbaris dari baris pertama. *Ciphertext* dihasilkan dari penyusunan ulang *plaintext* dengan menyusun kolom pertama sesuai urutan abjad.

Berdasarkan uraian diatas, maka peneliti ingin melakukan suatu kajian yang berjudul "Implementasi Algoritma Super Enkripsi (*Hill Cipher*dan Transposisi *Columnar*) pada Pesan Teks".

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka rumusan masalah penelitian ini sebagai berikut:

1. Bagaimana proses enkripsi pada pesan teks menggunakan metode super enkripsi (*Hill Cipher* dan Transposisi *Columnar*)?
2. Bagaimana proses dekripsi pada pesan teks menggunakan metode super
3. enkripsi (*Hill Cipher* dan Transposisi *Columnar*)?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan dalam penelitian ini adalah sebagai berikut:

1. Mengetahui proses enkripsi pada pesan teks menggunakan metode super enkripsi (*Hill Cipher* dan Transposisi *Columnar*).
2. Mengetahui proses dekripsi pada pesan teks menggunakan metode super enkripsi (*Hill Cipher* dan Transposisi *Columnar*).

1.4 Manfaat Penelitian

Adapun beberapa manfaat yang terdapat pada penelitian ini sebagai berikut:

1. Menghasilkan algoritma enkripsi kombinasi yang lebih aman.
2. Menghasilkan algoritma dekripsi kombinasi yang lebih aman.

1.5 Batasan Masalah

Adapun batasan masalah dalam penelitian ini sebagai berikut:

1. Meggunakan karakter berupa alfabet pada proses enkripsi dan dekripsi.
2. Kunci yang digunakan proses enkripsi dan dekripsi pada *hill cipher* matriks 3×3 yang memiliki invers. Sedangkan kunci columnar menggunakan tiga karakter.
3. Pesan yang diubah dalam bentuk matriks dengan jumlah baris sesuai dengan ukuran kunci matriksnya untuk *hill cipher*. Sedangkan untuk columnar, pesan dimasukkan ke dalam kolom sesuai dengan panjang karakter kunci, dengan jumlah baris menyesuaikan jumlah karakter *plaintext* nya.
4. Karakter spasi pada *plaintext* algoritma columnar disimbolkan dengan "#".
5. Pesanpada *hill cipher* terdapat 91 karakter ASCII antara 32 dan 122.
6. Proses enkripsi dan dekripsi pada super enkripsi dalam penelitian ini diimplementasikan pada software MAPLE.

1.6 Metode Penelitian

Penulisan ini dilakukan dengan cara studi literatur. Penulisan ini dimulai dengan mempelajari tugas akhir, artikel, dan buku-buku yang mendukung penelitian ini. Adapun langkah-langkah penelitian yang penulis gunakan adalah sebagai berikut:

Proses enkripsi dengan menggunakan metode super enkripsi:

1. Menentukan *plaintext*,
2. Mengubah *plaintext* ke dalam bentuk karakter ASCII dan bentuk matriks,
3. Menentukan kunci yang berbentuk matriks 3×3,

4. Mengalikan matriks kunci dengan matriks *plaintext* dan dimodulokan dengan 91,
5. Mengkonversi *ciphertext* menjadi karakter ASCII,
6. Mengenkripsi kembali *ciphertext* menggunakan columnar,
7. Menentukan kunci pada columnar,
8. Memasukkan semua karakter *ciphertext* ke kolom sesuai banyak karakter kunci yang dimulai dengan baris pertama ke baris lain secara horizontal, dan,
9. Membaca karakter perkolom sesuai urutan abjad secara vertikal sebagai *ciphertext*.

Proses Dekripsi dengan menggunakan metode super enkripsi:

1. Menentukan *chipertext* dari hasil pengenkripsian dengan columnar,
2. Menentukan kunci yang sama dengan proses enkripsi columnar,
3. Memasukkan *ciphertext* ke kolom sesuai nama kunci secara vertikal,
4. Mengkonversi hasil *plaintext* ke bilangan karakter ASCII,
5. Mengkonversi *plaintext* menjadi matriks berbentuk 3×7,
6. Menginverskan matriks kunci *hill cipher*,
7. Mengalikan matriks kunci dengan matriks *plaintext*,
8. Mengkonversi hasil perkalian ke karakter ASCII. 3 × 7,
9. Menemukan *plaintext* asli dari proses di atas.

1.7 Sistematika Penelitian

Dalam penulisan penelitian ini, peneliti menggunakan sistematika yang terdiri dari empat bab, dan masing-masing bab dibagi dalam sub-bab dengan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Menguraikan tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan yang menggambarkan secara singkat isi laporan penelitian ini.

Bab II Kajian Pustaka

Membahas tentang teori-teori penunjang atau gambaran umum dari teori yang mendasari pembahasan.

Bab III Pembahasan

Bab ini merupakan bab inti dari penulisan penelitian yang dilakukan berisi penyelesaian permasalahan.

Bab IV Penutup

Bab ini berisi kesimpulan dari pembahasan yang sesuai dengan hasil penelitian, yang selanjutnya dapat digunakan sebagai saran bagi pembaca dan peneliti selanjutnya.

BAB II

KAJIAN PUSTAKA

2.1 Matriks

Matriks merupakan susunan dari bilangan atau elemen yang disusun menurut baris dan kolom. Matriks yang mempunyai *m*baris dan *n* kolom disebut matriks berordo $m \times n$. Bilangan yang disusun pada matriks disebut entri pada matriks (Anton dan Rorres, 2010). Matriks disimbolkan dengan huruf kapital dan entrinya disimbolkan dengan huruf non kapital. Matriks A yang berordo $m \times n$ dapat ditulis dengan $A_{\mathrm{m} \times \mathrm{n}}$. Berikut merupakan bentuk umum matriks A dengan ordo m × n.

$$A_{\mathrm{m} \times \mathrm{n}} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Matriks yang hanya mempunyai satu baris disebut matriks baris, dan matriks yang hanya mempunyai satu kolom disebut matriks kolom (Anton dan Rorres, 2010). Matriks baris A ditulis dengan $A_{1 \times \mathrm{n}}$ dan matriks kolom A ditulis dengan $A_{\mathrm{m} \times 1}$. Berikut merupakan bentuk umum matriks baris A dan matriks kolom B:

$$\boldsymbol{A} = [\boldsymbol{a_{11}a_{12}} \ \ldots \ \boldsymbol{a_{1n}}] \text{ dan } \boldsymbol{B} = \begin{bmatrix} \boldsymbol{b_{11}} \\ \boldsymbol{b_{21}} \\ \vdots \\ \vdots \\ \boldsymbol{b_{m1}} \end{bmatrix}$$

Matriks yang memiliki banyak baris sama dengan banyak kolom dinamakan sebagai matriks persegi atau matriks bujur sangkar A berordo $m \times n$ maka $m = n$. Berikut merupakan bentuk umum matriks persegi A berordo $n \times n$:

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

Dalam aljabar, matriks dapat didefinisikan dengan beberapa operasi yang terdapat pada matriks, yaitu penjumlahan, pengurangan, perkalian matriks dengan skalar dan perkalian matriks dengan matriks.

2.1.1 Operasi Matriks

2.1.1.1. Perkalian Matriks

Jika A adalah matriks $m \times r$ dan B adalah matriks $r \times n$, maka hasil kali matrik AB adalah matriks $m \times r$ yang entri-entrinya ditentukan sebagai berikut. Untuk mencari entri pada baris i dan kolom j dari AB, pisahkan baris i dari matriks A dan kolom j dari matriks B. Lalu kalikan entri-entri yang bersesuaian dari baris dan kolom tersebut dan kemudian jumlahkan hasil yang diperoleh (Howard Anton, 2004:30).

Misal matriks A berordo $m \times r$ dan matriks B berordo $r \times n$, maka AB dapat ditulis: $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mr} \end{bmatrix}$ dan $B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{r1} & b_{r2} & \cdots & a_{rn} \end{bmatrix}$

Entri $(AB)_{ij}$ pada baris i dan kolom j dari AB diperoleh melalui

$$(AB)_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \cdots + a_{ir}b_{rj}$$

Untuk setiap $i = 1,2,3, \ldots, m$ dan $j = 1,2,3, \ldots, n$.

2.1.1.2 Perkalian Matriks dengan Skalar

Jika A adalah matriks sebarang dan c adalah skalar sebarang, maka hasil kalinya (*product*) cA adalah matriks yang diperoleh dari perkalian setiap entri

pada matriks A dengan bilangan c. Matriks cA disebut sebagai kelipatan skalar (*scalar multiple*) (Howard Anton, 2004:29).

Dalam notasi matriks, jika $A = [a_{ij}]$ maka

$$cA = c[a]_{ij} = [ca_{ij}] = \begin{bmatrix} ca_{11} & ca_{12} & \cdots & ca_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ ca_{m1} & ca_{m2} & \cdots & ca_{mn} \end{bmatrix}$$

2.1.1.3 Transpos Matriks

Jika A adalah matriks $m \times n$, maka transpos dari A (transpose of A), dinyatakan A^T, didefinisikan sebagai matriks $n \times m$ yang didapatkan dengan mempertularkan baris-baris dan kolom-kolom dari A, sehingga kolom pertama A^T adalah baris pertama dari A, kolom kedua dari A^T adalah baris kedua dari A dan seterusnya (Howard Anton,2004:36).

Misal matriks A berordo $m \times n$ adalah:

Jika $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$ maka $A^T = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nm} \end{bmatrix}$

Atau jika $A = [a_{ij}]$ maka $A^T = [a_{ji}]$.

2.1.1.4 Invers Matriks

Jika A adalah matriks persegi, dan jika terdapat matriks B yang ukurannya sama sedemikian rupa sehingga $AB = BA = I$, maka A disebut *invertible* (dapat dibalik) dan B disebut sebagai *invers* dari A. Jika matriks B tidak dapat didefinisikan, maka A dinyatakan sebagai matriks singular (Howard Anton, 2004:46).

Berikut ini pernyataan mengenai invers dari matriks yang dapat dibalik. Jika A dapat dibalik, maka inversnya akan dinyatakan dengan simbol A^{-1}, jadi:

$AA^{-1} = A^{-1}A = I$

Teorema 1:

Jika A dan B adalah matriks-matriks yang dapat dibalik dengan ukuran yang sama, maka AB dapat dibalik dan $(AB)^{-1} = B^{-1}A^{-1}$.

Bukti:

Contoh:

Misal matriks A dan B berordo 2×2

$A = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix}$ dan $B = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$, maka $AB = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix}\begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$ sedangkan $BA = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$.

2.1.2 Determinan Matriks

Determinan merupakan suatu matriks persegi. Fungsi determinan dinotasikan dengan $\det(A)$ sebagai jumlah dari semua hasil kali elementer bertanda dari A (Howard Anton, 2004:94).

Determinan dari matriks 2×2 adalah $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ dapat dibalik jika $a_{11}a_{22} - a_{12}a_{21} \neq 0$, disebut determinan dari matriks A dan dinyatakan sebagai $\det(A)$. Dengan notasi rumus untuk A^{-1}adalah $A^{-1} = \frac{1}{\det(A)}\begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}$.

2.1.3 Adjoin

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

Definisi : jika A sebarang matriks berordo $n \times n$ dan c_{ij} adalah kofaktor a_{ij}, maka matriks : $\begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{bmatrix}$ dinamakan matriks kofaktor dari A. Transpos matrik ini dinamakan adjoin dari A dan dinyatakan dengan adj(A) (Anton dan Rorres, 2010).

Contoh : misalkan matriks A berordo 3×3

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

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

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

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

2.2 Keterbagian

Teori bilangan merupakan teori yang mendasar dalam memahami algoritma kriptografi. Teori ini berkaitan dengan sifat-sifat dari bilangan bulat. Salah satu yang menjadi topik utama dalam teori bilangan adalah keterbagian. Beberapa sifat dan relasi lain seperti kekongruenan dikembangkan dari masalah keterbagian.

Definisi : misal a dan b adalah bilangan bulat dengan a $\neq 0$. Dikatakan $a$membagi a jika terdapat bilangan bulat c sedemikian hingga $b = ac$, dinotasikan dengan $a|b|$. Ketika a membagi $b$dikatakan a adalah faktor atau pembagi dari b, dan b adalah kelipatan dari a (Rosen, 2012).

Contoh : misal $a = 4$ dan $b = 20$ maka $4|20$, sehingga $20 = 4 \times 5$.

2.2.1 Aritmetika Modular

Aritmetika modular sangat berperan dalam kriptografi karena banyak digunakan dalam algoritma enkripsi, baik algoritma enkripsi simetri maupun asimetri. Dalam aritmetika modular, konsep faktor persekutuan terbesar (FPB) antara lain digunakan untuk operasi invers. Selain FPB konsep lain seperti kongruensi modulo sangat penting dalam kriptografi (Kromodimoeljo, 2010).

2.2.2. Faktor Persekutuan Terbesar (FPB)

Jika $a, b \in \mathbb{Z}$ yang tidak keduanya 0, maka faktor persekutuan terbesar (FPB) dari a dan b adalah bilangan asli g sedemikian hingga $g|a$, $g|b$, dan g adalah pembagi dari setiap persekutuan dari a dan b ditulis dengan $g = (a, b)$ dengan $a, b \in \mathbb{Z}$ dan yang tidak keduanya 0.

Contoh :

Himpunan semua faktor dari 15 adalah : $A = \{-15, -5, -3, -1, 1, 3, 5, 15\}$,

dan himpunan semua faktor dari 9 adalah: $B = \{-9, -3, -1, 1, 3, 9\}$.

Himpunan semua faktor persekutuan dari 18 dan 9 adalah $G = \{-3, -1, 1, 3\}$.

Karena unsur G yang terbesar adalah maka (15,9) = 3.

2.2.3 Relatif Prima

Bilangan bulat a dan b dikatakan relatif prima jika $(a, b) = 1$. Jika a dan b relatif prima, maka terdapat bilangan bulat m dan n,

sedemikian hingga $ma + nb = 1$ (Ariyus, 2008).

Contoh :

Himpunan semua faktor dari 12 adalah :

$$P = \{-12, -6, -3, -2, -1, 1, 2, 3, 6, 12\},$$

dan himpunan semua faktor dari 7 adalah :

$$Q = \{-7, -1, 1, 7\}.$$

Himpunan semua faktor persekutuan dari 12 dan 7 adalah : $G = \{-1,1\}$

Karena unsur G yang terbesar adalah 1, maka $(12,7) = 1$. Jadi 12 dan 7 relatif prima. Selain itu diperoleh $3 \cdot 12 + (-5) \cdot 3 = 1$, dengan $m = 3$ dan $n = -5$.

2.2.4 Kongruensi Modulo

Jika bilangan bulat M yang tidak nol, membagi selisih $a - b$, maka dikatakan a kongruen dengan b modulo M, dan dapat ditulis $a \equiv b(mod\ M)$ (Irawan, dkk, 2014).

Contoh :

$16 \equiv 4(mod\ 4)$ karena 4|(16-4) atau 4|12.

2.2.5 Invers Modulo

Teorema 2

Bilangan bulat a mempunyai invers modulo M jika dan hanya jika $(a, M) = 1$(Ariyus, 2008).

Bukti

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

2.2.6 Kongruensi Matriks

Jika A dan B adalah matriks $r \times n$ dengan entri-entrinya bilangan bulat, unsur ke (i, j) berturut-turut adalah a_{ij}dan b_{ij}. A dikatakan kongruensi dengan B modulo m, jika $a_{ij} \equiv b_{ij}(mod\ m)$untuk setiap pasang (i, j) dengan $1 \leq i \leq r$ dan $1 \leq j \leq n$ dan dinotasikan dengan $A \equiv B(mod\ m)$(Irawan, dkk, 2014).

Contoh : $\begin{bmatrix} 11 & 9 \\ 4 & 8 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ -3 & 1 \end{bmatrix} (mod\ 7)$

Maksud dari contoh tersebut adalah matriks $\begin{bmatrix} 11 & 9 \\ 4 & 8 \end{bmatrix}$merupakan hasil dari matriks $\begin{bmatrix} 4 & 2 \\ -3 & 1 \end{bmatrix}$ dimodulokan dengan 7.

2.2.7 Invers Matriks Modulo

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

Contoh: $\begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 4 & 10 \\ 10 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (mod\ 5)$

Dari contoh tersebut terlihat bahwa $\begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix}$ invers dari $\begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}$ modulo 5.

2.2.8 Invers Matriks Modulo dari Adjoin

Invers matriksmodulo berordo tinggi membutuhkan adjoin untuk mencari hasil invers matriks. Berikut teorema yang menggunakan adjoin untuk mencari invers matriks modulo berordo tinggi, yaitu:

Teorema 3

Jika A adalah matriks berordo $n \times n$ dengan unsur-unsurnya bilangan bulat dan m adalah bilangan bulat positif, sedemikian sehingga $(\det(A),\ m) = 1$ dan

$\det(A)^{-1}$adalah invers dari $\det(A)$ modulo m, maka invers dari A modulo m adalah $A^{-1} = \det(A)^{-1} adj(A)$ (Irawan, dkk, 2014).

Bukti

Jika $(\det(A), m) = 1$ maka $\det(A), \neq 0$ dan $A\ adj(A) = \det(A) I$.

Karena $(\det(A), m) = 1$, maka $\det(A)$ mempunyai invers $\det(A)^{-1}$ modulo m. Misal $A^{-1} = \det(A) I\ adj(A)$ maka $A \det(A)^{-1} adj(A) = A\ adj(A)$.

$\det(A)^{-1} = \det(A) I \det(A)^{-1}$ atau $\det(A) I \cdot \det(A)^{-1} I \equiv I (\mathrm{mod} m)$ dan $\det(A)^{-1} adj(A) A = \det(A)^{-1} A\ adj(A) = \det(A)^{-1} \det(A)$atau $\det(A) I \cdot \det(A)^{-1} \equiv I (\mathrm{mod}\ m)$ ini menunjukkan bahwa $(A)^{-1} = \det(A)^{-1} adj(A)$ adalah invers dari A modulo m.

2.3 Kriptografi

Kriptografi berasal dari bahasa Yunani yang terdiri dari dua kata yaitu *cryptos* yang artinya rahasia dan *graphien* yang artinya tulisan. Jadi kriptografi secara harfiah berarti tulisan rahasia. Definisi lama yang dipakai di dalam buku-buku sebelum tahun 1980-an menyatakan bahwa, kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dipahami lagi maknanya (Meyer,1982). Adapun pengertian kriptografi terus berkembang dan secara umumya makna dari kriptografi adalah ilmu yang mempelajari tentang bagaimana menjaga kerahasiaan suatu pesan, supaya isi pesan yang disampaikan tersebut aman sampai ke penerima pesan (Ariyus, 2008).

2.3.1 Pesan

Pesan (*message*) adalah data atau informasi yang dapat dibaca, dipersepsi, dan dapat dimengerti oleh seseorang. Pesan dapat berupa teks, citra (*image*), suara atau bunyi (audio), video, baik berbentuk digital maupun analog. Pesan berupa teks sering disebut juga *plaintext* atau teks-jelas (*cleartext*), pesan dalam bentuk gambar, audio, dan video masing-masing disebut *plain-image*, *plain-audio*, dan *plain-video*.

Pesan dapat dikirim atau disimpan. Pesan yang terkirim adalah informasi yang disampaikan ke penerima melalui media komunikasi (misalnya melalui pos, kurir, saluran telekomunikasi seperti kabel, gelombang radio, serat optik, dll). Pesan yang tersimpan adalah pesan yang disimpan di dalam memori sekunder atau media perekaman (*disk*, *hard-disk*, *flash-disk*, CD/DVD, kaset, dll). Pesan disimpan dalam format file ke dalam media perekaman tersebut. Baik pesan yang terkirim maupun yang tersimpan tidak hanya berupa teks, tetapi juga dapat berbentuk citra (*image*), suara/bunyi (audio), dan video, atau berkas biner lainnya.

Agar pesan tidak dapat dipahami isinya oleh pihak lain, maka pesan perlu disandikan menjadi pesan yang tidak dapat dimengerti lagi maknanya. Pesan teks yang tersandi disebut *ciphertext*, gambar tersandi disebut *cipher-image*, video tersandi dinamakan *cipher-video*, audio tersandi dinamakan *cipher-audio*. Pesan tersandi harus dikembalikan menjadi pesan semua agar bisa dibaca. Pesan teks dapat dibaca dengan jelas, tetapi pesan tersandi (*ciphertext*) sudah tidak dapat dipahami lagi isinya. Begitu juga untuk pesan berupa gambar dan video, gambar tersandinya tidak dapat lagi dipersepsi secara visual karena terlihat seperti gambar acak. Dengan cara menyandikan pesan menjadi bentuk tak bermakna, maka itu

berarti konten pesan sudah disamarkan sehingga kerahasiaan pesan terjamin. Dengan proses yang berkebalikan, pesan tersandi dapat dikembalikan menjadi pesan semula.

2.3.2 Pengirim dan Penerima

Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan. Pengirim atau penerima tidak harus berupa orang, tetapi juga dapat berupa mesin, robot, atau komputer. Jadi, orang bisa berkomunikasi dengan orang lain, orang berkomunikasi dengan mesin penjawab, atau mesin berkomunikasi dengan komputer, atau komputer *client* berkomunikasi dengan *server*.

2.3.3 Algoritma Kriptografi

Algoritma merupakan urutan atau langkah-langkah untuk menyelesaikan masalah yang disusun secara sistematis. Algoritma kriptografi adalah langkah-langkah bagaimana cara menyembunyikan pesandari orang-orang yang tidak berhak menerima pesan tersebut (Ariyus, 2008).

Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan kunci yang dipakainya:

1. Algoritma Simetri(menggunakan satu kunci untuk enkripsi dan dekripsi).
2.Algoritma Asimetri (menggunakan kunci berbeda untuk enkripsi dan dekripsi).
3. Fungsi Hash (Ariyus, 2008).

2.4 Super Enkripsi

Super enkripsi merupakan suatu konsep dengan menggunakan kombinasi dari dua atau lebih dari teknik substitusi dan transposisi cipher untuk mendapatkan suatu algoritma yang sulit dipecahkan oleh penyusup (Ariyus, 2006). Untuk menjalankan teknik super enkripsi, harus memahami teknik substitusi yang dapat melakukan enkripsi pesan dan teknik transposisi yang dapat mengubah chiperteks bisa dienkripsikan menjadi bentuk semula suatu pesan.

*Cipher*substitusi dan *cipher* transposisi dapat dikombinasikan untuk memperoleh *cipher* yang lebih kuat (super) daripada hanya satu *cipher* saja. Mula-mula *plaintext* dienkripsi dengan *cipher* seederhana (misalnya *cipher* alfabet-tunggal), lalu hasilnya dienkripsi lagi dengan *cipher* transposisi atau bisa juga sebaliknya. Algoritma kriptografi modern menerapkan prinsip super enkripsi untuk mendapatkan *ciphertext* yang kompleks.

Contoh :

Plaintext→hello world

*Plaintext*di atas dienkripsi dengan *caesar cipher* menjadi: KHOOR ZROUG. Kemudian hasil enkripsi ini dienkripsi kembali dengan *cipher* transposisi (kunci =4): maka hasilnya menjadi :

KHOO

RZRU

OGZZ

Ciphertext akhir adalah : KROHZGORZOUZ, dimana dibaca per kolom dari atas kiri.

2.5 Algoritma Hill Cipher

Hill cipher merupakan algoritma enkripsi-dekripsi yang menggunakan matriks transformasi. *Cipher* ini ditemukan pada tahun 1929. Adapun prinsip *hill cipher*adalah sebuah matriks yang dapatmentransformasikan *plaintext* menjadi *ciphertext*. Matriks transformasi merepresentasikan matriks kunci. Untuk melakukan dekripsi, penerima pesan perlu menghitung terlebih dahulu matriks balikan *(invers*) dari matriks kunci, karena invers dapat digunakan untuk mentransformasikan *ciphertext* menjadi *plaintext*. Matriks balikan hanya dapat dihitungjika mengetahui matriks kunci. Secara matematik, enkripsi *plaintext* $\boldsymbol{P}= (\boldsymbol{p_1}, \boldsymbol{p_2}, \dots, \boldsymbol{p_n})$dengan matriks kunci K= k_{ij} menghasilkan chiperteks $\boldsymbol{C}=(\boldsymbol{c_1}, \boldsymbol{c_2}, \dots, \boldsymbol{c_n})$ dinyatakan sebagai $\begin{pmatrix} \boldsymbol{c_1} \\ \boldsymbol{c_2} \\ \boldsymbol{c_n} \end{pmatrix} = \begin{pmatrix} k_{11} & \dots. & k_{1n} \\ : & k_{22} & : \\ k_{n1} & \dots. & k_{nn} \end{pmatrix} \begin{pmatrix} \boldsymbol{p_1} \\ \boldsymbol{p_2} \\ \boldsymbol{p_n} \end{pmatrix} mod\ 26$

Atau dalam bentuk sistem persamaan lanjar dalam modulus 26:

$$c_{1=}(k_{11}p_1+k_{12}p_2+\cdots+k_{1n}p_n) mod 26$$

$$c_{2=}(k_{21}p_1+k_{22}p_2+\cdots+k_{2n}p_n) mod 26$$

.....

$$c_{n=}(k_{n1}p_1+k_{n2}p_2+\cdots+k_{nn}p_n) mod 26$$

Atau dalam notasi *C=KP mod 26*

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

$$\begin{pmatrix} \boldsymbol{p_1} \\ \boldsymbol{p_2} \\ \boldsymbol{p_n} \end{pmatrix} = \begin{pmatrix} k_{11} & \dots. & k_{1n} \\ : & k_{22} & : \\ k_{n1} & \dots. & k_{nn} \end{pmatrix}^{-1} \begin{pmatrix} \boldsymbol{c_1} \\ \boldsymbol{c_2} \\ \boldsymbol{c_n} \end{pmatrix} mod\ 26$$

Atau dalam bentuk persamaan

$$p_{1=(k\prime_{11}c_1+k\prime_{12}c_2+\cdots+k\prime_{1n}c_n)mod26}$$

$$p_{2=(k\prime_{21}c_1+k\prime_{22}c_2+\cdots+k\prime_{2n}c_n)mod26}$$

.....

$$p_{n=(k\prime_{n1}c_1+k\prime_{n2}c_2+\cdots+k\prime_{nn}c_n)mod26}$$

Atau dalam notasi $P = K^{-1}C \ mod\ 26$.

Hal terpenting dalam *hill cipher* adalah bagaimana menghitung matriks balikan (K^{-1}) sedemikian hingga $KK^{-1} = 1$, dimana$I$ adalah matriks identitas. Menghitung matriks balikan dalam aritmetika modulo tidak boleh menghasilkan nilai negatif dan pecahan, karena operasi kriptografi hanya dalam bilangan bulattak-negatif. Jika ada perhitungan menghasilkan bilangan negatif, maka harus diganti dengan bilangan positif yang kongruen dalam modulo 26. Begitu juga bilangan berbentuk pecahan $\frac{1}{a} = a^{-1}$, maka a^{-1}diganti dengan balikan a dalam modulus 26. Metode menghitung matriks balikan sama seperti metode menghitung matriks balikan yang diajarkan di dalam materi aljabar lanjar.

Contoh :

Matriks enkripsi yang memiliki inverse pada Z_{26}:

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

Karena

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = \begin{pmatrix} 11\times 7+8\times 23 & 11\times 18+8\times 11 \\ 3\times 7+7\times 23 & 3\times 18+7\times 11 \end{pmatrix}$$

$$= \begin{pmatrix} 261 & 286 \\ 182 & 131 \end{pmatrix}$$

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

Semua operasi aritmetik diatas dilakukan pada modulo 26.

Contoh: untuk memberikan gambaran tentang enkripsi dan dekripsi dalam *hill cipher*.

Misalkan kunci yang dipakai adalah: $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

Dari perhitungan diatas diperoleh bahwa:

$$K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

Misalkan suatu pesan "JULY" akan dienkripsikan, sebelum itu dibagi menjadi dua elemen *plaintext* untuk dienkripsi:

--(9,20)→JU

--(11,24)→ LY

Kemudian melakukan perhitungan berikut:

$(9,20)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (99 + 60, 72 + 140) mod\ 26 = (3,4) \longrightarrow DE$

$(11,24)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (121 + \ 72, 192 + 168) = (11,22) LW$

Sehingga enkripsi untuk JULY adalah DELW.

Untuk mendekripsi, dilakukan dengan cara:

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

$(3,4)\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} mod 26$ =(21+92,72+44)=(113,116) =(9,12)→JU

$(11,22)\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} mod\ 26$ =(77+506,198+242)=(583,440)mod2

6 =(11,24)→LY

Dengan demikian didapatkan *plaintext* kembali seperti semula.

Adanya penjelasan tersebut menerangkan bahwa dekripsi hanya mungkin dilakukan jika matriks *K* memiliki invers. Suatu matriks *K* memiliki invers jika dan hanya jika determinannya tidak nol. Namun karena berdasarkan pada $\mathbb{Z}_{26}$,

maka matriks K memiliki invers modulo 26 jika dan hanya jika $gcd(det\ K, 26) = 1$.

2.6 Algoritma Transposisi Columnar

Transposisi columnar merupakan salah satu metode kriptografi dimana pesan dituliskan berderet dari suatu panjang yang ditetapkan,lalu dibaca kembali kolom per kolom dengan urutan pembacaan berdasarkan suatu kata kunci. Panjang deret ditentukan oleh panjang kata kunci. Urutan pembacaan kolom berdasarkan urutan abjad kata kunci.

Transposisi columnar ini termasuk dalam metode penyandian tranposisi dimana metodenya dilakukan dengan cara mengubah letak dari teks pesan yang disandikan. Adapun untuk membaca pesan aslinya kembali, cukup dengan mengembalikan letak dari pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati.

Transposisi columnar merupakan teknik kriptografi asimetri yang menggunakan duakunci berbeda dalam proses enkripsi dan dekripsi. Kedua kunci tersebut digunakan untuk enkripsi data (*private key*) dandigunakan untuk dekripsi data (*public key*).Salah satu kunci transposisi yang paling sederhana adalah kunci transposisi columnar. Kunci columnar dengan menulis karakter teks asli dengan orientasi baris dengan panjang karakter yang sama dan kemudian teks sandi didapatkan dengan menulis ulang dengan orientasi kolom. Urutan kolom disepakati sebelumnya untuk mempersulit analisis sandi.

2.6.1 Perancangan Modifikasi transposisi Columnar Fungsi Enkripsi

Adapun rancangan suatu fungsi enkripsi sederhana yang terdiri dari dua tahap:

1. Perancangan Modifikasi Transposisi Columnar Fungsi Dekripsi
   - Mengacak urutan huruf pada pesan. Pengacakan urutan huruf pada pesan dilakukan dengan aturan ganjil genap. Langkah-langkah implementasi aturan tersebut sebagai berikut:
   - Memisahkan huruf-huruf yang berada pada posisi ganjil dan genap.
   - Melakukan tahap sebelumnya terhadap huruf-huruf kelompok ganji dan genap menjadi kelompok ganjil-ganjil, ganjil-genap, genap-ganjil, dan genap-genap.
   - Menggabungkan kembali huruf-huruf yang telah terpisah menjadi 4 kelompok tersebut dengan aturan ganjil-ganjil, ganjil-genap, genap-ganjil, dan genap-genap.
2. Perancangan Modifikasi Transposisi Columnar Fungsi Dekripsi
   - Menginverskan urutan huruf dengan menuliskan posisi huruf dari yang paling akhir hingga ke paling awal
   - Mengacak urutan huruf setelah inverse dan mengembalikan posisi huruf ke posisi semula sebelum diacak menggunakan aturan ganjil-genap, diperinci dengan beberapa tahapan sebagai berikut
   - Membagi pesan menjadi dua bagian sama banyak.
   - Melakukan tahap sebelumnya terhadap huruf-huruf kelompok pertama dan kedua. Hasil pembagian pada kelompok pertama menjadi bagian 1 dan 2, sedangkan kelompok kedua menjadi bagian kelompok 3 dan 4.

- Menggabungkan keempat bagian yang telah terbentuk diatas pada posisi semula, dimana pada enkripsi bagian satu adalah kelompok ganjl-ganjil bagian dua adalah ganjil-genap, bagian tiga adalah genap-ganjil, bagian empat adalah genap-genap.

Misalnya terdapat *plaintext*SAHILA menjadi ”6 3 2 4 1 5’ dengan suatu permisalan pesan yang akan dikirim yaitu “ NAMA SAYA TITO akan dienkripsi menggunakan transposisi columnar dengan kata kunci HOI maka proses enkripsi akan menjadi seperti berikut:

HOI maka didapat pola 1 3 2

1	3	2
N	A	M
A	S	A
Y	A	T
I	T	O

Adapun hasil dari proses enkripsi columnar berupa*ciphertext*yaitu“NAYIMATO ASAT”. *Ciphertext* tersebut dari kolom pertama (secara veertikal) ke kolom berikutnya sesuai urutan pola angka 1-2-3.

Kunci dapat diperoleh dari kata yang mudah dibaca dan kemudian dikodekan menjadi bilangan. Sistem ini dinamakan Algoritma Transposisi columnar dengan kunci numerik. Misalnya:

Kata Sandi	S	A	N	T	A	N
Bilangan	5	1	3	6	2	4

Huruf A yang dobel diberikan nomor 1 dan 2, kemudian huruf yang dekat dengan A yaitu N, diberi nomor 3 dan 4 karena dobel, sedangkan huruf berikutnya diberi

angka 5 dan 6. Pesan dapat ditambahi padding bits yang merupakan bit-bit tambahan jika ukuran blok terakhir tidak mencukupi panjang blok.

Contoh:

Pesan: “nama saya tito” di enkripsi dengan kunci “polar”. Kunci polar memiliki 21345 sesuai urutan urutan abjad. Lalu dibuat kolom

2	**1**	**3**	**4**	**5**
N	A	M	A	S
A	Y	A	T	I
T	O	*R*	*A*	*B*

Sehingga di dapat *ciphertext*nya AYONATMARATASIB. Adapun huruf yang dicetak miring tersebut merupakan tambahan untuk mengisi kolom yang kosong disebut juga dengan *padding*.

2.7 Super Enkripsi

Super enkripsi merupakan salah satu kriptografi berbasis karakter yang menggabungkan *cipher* substitusi dan *cipher* transposisi. Adapun *cipher* substitusi dalam bahasan ini menggunakan algoritma *hill cipher* sedangkan *cipher* transposisinya menggunakan transposisi columnar. Hal ini bertujuan untuk mendapatkan *cipher* yang lebih kuat daripada hanya menggunakan satu *cipher* saja, sehingga tidak mudah untuk dipecahkan. Enkripsi dan dekripsinya dapat dilakukan dengan urutan *cipher* substitusi kemudian dilanjutkan *cipher* transposisi, atau sebaliknya. Super enkripsi dapat dilakukan dengan mengunakan kedua *cipher* tersebut secara berulang-ulang, namun dalam penelitian ini hanya

akan dibahas mengenai proses enkripsi dan dekripsi satu kali dengan menggunakan *cipher* substitusi dan satu kali dengan menggunakan *cipher* transposisi.

Adapun urutan dalam proses super enkripsi berikut ini

1. Mengenkripsi *plaintext* menggunakan algoritma *hill cipher* dan menjadi suatu *ciphertext*.
2. Mengenkripsi kembali*ciphertext* tersebut menggunakan transposisi columnar dan hasilnya masih disebut *ciphertext*.
3. Mendekripsi *ciphertext* dari hasil proses enkripsi columnar dengan transposisi columnar terlebih dahulu.
4. Mendekripsi kembali hasilproses dekripsi columnar tersebut dengan algoritma *hill cipher*.
5. Menghasilkan *plaintext* seperti semula pesan terkirim.

Proses super enkripsi bisa dilakukan dengan transposisi terlebih dulu dan dilanjut dengan substitusi. Proses super enkripsi sangat aman dankuat dalam mengirimkan suatu pesan yang akan sulit dipecahkan oleh pihak ketiga.

2.8 Kajian Keagamaan

Alquran merupakan mukjizat terbesar dari mukjizat-mukjizat lainnya yang diberikan Alloh SWT kepada para nabi sebelumnya. Mukjizat tersebut diberikan kepada hamba pilihan Allah yakni Muhammad SAW untuk disampaikan kepada seluruh umat manusia.Kemukjizatan Alquran bersifat universal dan abadi. Maka dari itu, makna dari pada Alquran akan tersampaikan kepada seluruh umat manusia dengan mempelajari dan memahaminya. Sehingga implementasi makna dari pada alquran dapat terealisasikan dengan baik.

Dalam Al-Qur'an terdapat beberapa ayat pada pembuka surat *(fawatihus suwar)*seperti *Alif Lam Mim, 'Ain Shin Qaf, Haa Mim, Kaf Ha Ya 'Ain Shad*, dan lainnya. Makna huruf-huruf tersebut hanya Alloh yang tahu. Sehingga makna dari ayat tersebut belum diketahui manusia. Ada yang berpendapat bahwa huruf-huruf tersebut merupakan nama surah dan ada yang pula berpendapat bahwa gunanya untuk menarik perhatian atau untuk mengisyaratkan bahwa al-quran itu diturunkan dalam bahasa arab yang tersusun dari huruf-huruf abjad.

ٱلَّذِينَ يَذْكُرُونَ ٱللَّهَ قِيَٰمًا وَقُعُودًا وَعَلَىٰ جُنُوبِهِمْ وَيَتَفَكَّرُونَ فِى خَلْقِ ٱلسَّمَٰوَٰتِ وَٱلْأَرْضِ رَبَّنَا مَا خَلَقْتَ هَٰذَا بَٰطِلًا سُبْحَٰنَكَ فَقِنَا عَذَابَ ٱلنَّارِ

Artinya : *"(yaitu) orang-orang yang mengingat Allah sambil berdiri atau duduk atau dalam keadan berbaring dan mereka memikirkan tentang penciptaan langit dan bumi (seraya berkata): "Ya Tuhan kami, tiadalah Engkau menciptakan ini dengan sia-sia, Maha Suci Engkau, maka peliharalah kami dari siksa neraka".(Ali-Imran: 191).*

Ayat di atas menjelaskan bahwa segala penciptaan Allah akan berguna bagi seluruh makhluk-Nya. Meskipun manusia tidak menyadarinya. Hal tersebut juga berlakupada ayat *fawatihus suwar*, yang mana makna dari ayat tersebut belum diketahui.Makna dari ayat tersebut masih menjadi rahasia Allah.

Pernyataan diatas berhubungan dengan pesan yang dapat dienkripsi dan didekripsikan. Suatu pesan yang akan dikirim akan terenkripsi dengan menggunakan suatu kunci. Penerima pesan akan mendekripsikan pesan tersebut dengan menggunakan kunci juga. enkripsi dan dekripsi dapat diimplementasikan pada seluruh ayat Al-Quran kecuali ayat fawatihul suwar. Salah satu impelementasi enkripsi dan dekripsi pada Al-Quran yakni pada proses mempelajarinya dengan menerjemahkan ke berbagai bahasa yang mana al-quran

terenkripsi secara bahasa arab. Ayat fawatihul suwar tidak dapat didekripsikan karena makna ayat tersebut masih menjadi rahasia.

BAB III

PEMBAHASAN

Pada pembahasan ini penulis akan membahas hasil dari analisis keamanan proses enkripsi dan dekripsi pesan menggunakan super enkripsi yaitu algoritma *hill cipher* dan columnar serta program yang digunakan untuk simulasi pada proses enkripsi dan dekripsi.

3.1 Analisis Keamanan Enkripsi dan Dekripsi *Hill Cipher* dan Columnar

3.1.1 Analisis Algoritma *Hill Cipher*

Dasar teori matriks yang digunakan dalam *hill cipher* adalah perkalian antar matriks dan melakukan invers pada matriks dengan aritmatika modulo. Algoritma *hill cipher* mempunyai salah satu parameter dalam proses enkripsi dekripsi sebagai kuncinya. Kunci pada hill cipher adalah matriks $n\ x\ n$ dengan n meerupakan ukuran blok. Jika matriks kunci tersebut sebut dengan K, maka matriks Ksebagai berikut: $K = \begin{bmatrix} k_{11} & k_{12} & \cdots k_{1n} \\ \vdots & \vdots & \ddots \ \vdots \\ k_{n1} & k_{n2} & \cdots k_{nn} \end{bmatrix}$,

Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible, yaitu memiliki *multiplicative inverse*K^{-1} sehingga : $K\ x\ K^{-1} = 1$

Kunci harus memiliki invers karena kunci matriks tersebut digunakan untuk melakukan proses dekripsi.

Proses enkripsi pada *hill cipher* dilakukan per blok plainteks. Ukuran blok tersebut sama dengan ukuran matriks kunci. Secara matematis, proses enkripsi pada *hill cipher* adalah: $C = K.P$

dengan: C = cipherteks, K = kunci, P= plainteks.

Proses dekripsi pada *hill cipher* pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (invers) terlebih dahulu. Secara matematis, proses dekripsi pada *hill cipher* dapat diturunkan dari:

$$C = K.P$$

$$K^{-1}.C = K^{-1}.K.P$$

$$K^{-1}.C = 1.P$$

Maka pesamaan proses dekripsi:

$$P = K^{-1}.C$$

Algoritma *hill cipher* terdapat beberapa parameter yangdigunakan untuk proses enkripsi dan dekripsi yaitu :

a. P (*plaintext*) merupakan pesan asli yang hanya diketahui oleh pengirim dan akan diketahui oleh penerima dengan proses dekripsi. Plainteks diubah ke dalam bilangan ASCII. Jadi $\boldsymbol{P_{1xa} = [p_1, p_2, p_3, p_4, \dots\dots, p_a]}$, dimana a merupakan banyaknya karakter pada plainteks$(a = 21)$.

b. Kemudian matriks P_{1xa} diubah menjadi matriks P_{nxm} yang ukurannya disesuaikan dengan ukuran matriks kunci yang digunakan.

   Jadi $P_{nxm} = \begin{bmatrix} p_{11} & p_{12} & \cdots p_{1m} \\ \vdots & \vdots & \ddots \ \vdots \\ p_{n1} & p_{n2} & \cdots k_{nm} \end{bmatrix}$ dimana $p_{11}, p_{12}, \dots\dots, p_{nxm} \in \mathbb{Z}$

c. K adalah parameter yang digunakan sebagai perkalian kunci matriks enkripsi dan dekripsi dengan pesan untuk memperoleh pesan kembali pada proses dekripsi maka $K_{n\times n}$ harus mempunyai invers dimana $(det\ (K_{n\times n}) \neq 0$ dan elemen-elemen pada kunci matriks $K_{n\times n}$ adalah bilangan bulat.

   Jadi $K_{n\times n} = \begin{bmatrix} k_{11} & k_{12} & \cdots k_{1n} \\ \vdots & \vdots & \ddots \ \vdots \\ k_{n1} & k_{n2} & \cdots k_{nn} \end{bmatrix}$, dimana $k_{11,}k_{12,}k_{13\dots\dots,}k_{nn} \in Z.$

d. Kemudian kunci matriks ($K_{n\times n}$) dikalikan dengan matriks (P_{nxm}) pada plainteks dan dimodulokan 91. Hasil perkalian tersebut disimbolkan dengan matriks

$$S_{n\times m} = \begin{bmatrix} k_{11} & k_{12} & \cdots k_{1n} \\ \vdots & \vdots & \ddots \ \vdots \\ k_{n1} & k_{n2} & \cdots k_{nn} \end{bmatrix} \begin{bmatrix} p_{11} & p_{12} & \cdots p_{1m} \\ \vdots & \vdots & \ddots \ \vdots \\ p_{n1} & p_{n2} & \cdots k_{nm} \end{bmatrix} (\text{mod } 91)$$

$$= \begin{bmatrix} s_{11} & s_{12} & \cdots s_{1m} \\ \vdots & \vdots & \ddots \ \vdots \\ s_{n1} & s_{n2} & \cdots s_{nm} \end{bmatrix}$$

Dengan $S_{11} = k_{11}.p_{11}+k_{12}.p_{21}+....+k_{1n}.p_{n1}$.

e. Kemudian matriks $S_{n\times m}$ diubah menjadi matriks baris (T).

$T_{1\times b} = [t_1\, t_2 t_3 \ \ldots t_b\,]$, dimana $b = \frac{a}{n}$ jika $n \mid a$ dan $b = \frac{(a+n-mod(a,n))}{n}$ jika $n \nmid a$. Dengan diketahui bahwa nilai $a = 21$ (panjang plainteks), $b = 3$, $c = 7$, $b \times c = 3 \times 7$ (ukuran matriks).

f. C ($chipertext$) merupakan pesan yang sudah dienkripsi atau pesan yang tersandikan oleh pengirim. $\boldsymbol{C_{1\times b} = [c_1\, c_2\, c_3\ \ldots c_b\,]}$.

g. $chipertext$ akan didekripsikan dengan mengonversi ke bentuk matriks baris berupa elemen-elemen nilai numerik yang ekuivalen. Matriks baris tersebut disimbolka dengan $\boldsymbol{D_{1\times b} = [d_1\, d_2\, d_3 \ldots d_b\,]}$.

h. Matriks $\boldsymbol{D}_{1\times b}$ diubah menjadi matriks yang berukuran sesuai dengan kunci matriks yang digunakan, disimbolkan dengan $\boldsymbol{E}_{n\times m} = \begin{bmatrix} e_{11} & e_{12} & \cdots e_{1m} \\ \vdots & \vdots & \ddots \ \vdots \\ e_{n1} & e_{n2} & \cdots e_{nm} \end{bmatrix}$

i. Mengalikan invers kunci matriks (K^{-1}), dengan matriks ($\boldsymbol{E}$)yang akan dimodulokan 91, dapat disimbolkan dengan

$$\boldsymbol{F}_{n\times m} = \begin{bmatrix} k^{-1}{}_{11} & k^{-1}{}_{12} & \cdots k^{-1}{}_{1n} \\ \vdots & \vdots & \ddots \ \vdots \\ k^{-1}{}_{n1} & k^{-1}{}_{n2} & \cdots k^{-1}{}_{nn} \end{bmatrix} \begin{bmatrix} e_{11} & e_{12} & \cdots e_{1m} \\ \vdots & \vdots & \ddots \ \vdots \\ e_{n1} & e_{n2} & \cdots e_{nm} \end{bmatrix} (mod\ 91)$$

$$= \begin{bmatrix} f_{11} & f_{12} & \cdots f_{1m} \\ \vdots & \vdots & \ddots \ \vdots \\ f_{n1} & f_{n2} & \cdots f_{nm} \end{bmatrix}$$

dengan $f_{11} = k^{-1}{}_{11} \,.\, e + k^{-1}{}_{12} \,.\, e_{21} + \ldots + k^{-1}{}_{1n} \,.\, e_{n1}$.

j. Matriks (***F***) diubah ke bentuk matriks baris untuk mendapatkan plainteks seperti semula. Hasil dari proses pendekripsian merupakan plainteks pada pesan yang akan dikirim.

k. m adalah 91, merupakan jumlah dari rentang 32 sampai 122 yang tertera pada lampiran tabel karakter ASCII. Sehingga untuk melakukan proses enkripsi dengan menggunakan rumus: dan proses dekripsi menggunakan rumus:

$$\boldsymbol{S}_{n\times m} = \boldsymbol{K}_{n\times m}\boldsymbol{P}_{n\times m} \ (mod\ 91)$$

an proses dekripsi menggunakan rumus:

$$\boldsymbol{F}_{n\times m} = K^{-1}{}_{n\times m}\boldsymbol{E}_{n\times m} \ (mod\ 91)$$

3.1.2 Keamanan Algoritma *Hill Cipher*

Keamanan algoritma *hill cipher* terletak pada kunci matriks yang dirahasiakan. Elemen-elemen kunci matriks ($K_{n\times n}$) adalah bilangan bulat dan (det $(K_{n\times n}), m) = \pm 1$, dengan m yaitu 91 (jumlah karakter ASCII) yang digunakan. Suatu kunci matriks pada algoritma *hill cipher* memiliki ukuran 3×3 dengan elemen yang terdiri dari bilangan bulat. Semakin banyak kombinasi elemen matriks yang meiliki nilai det(det $(K_{n\times n}), m) = \pm 1$ maka kunci matriks algoritma *hill cipher* dapat dianggap aman untuk menyandikan pesan. Kunci matriks yang bisa digunakan untuk menyandikan pesan dapat dibentuk dari elemen-elemen kunci matriks. Jika (det $(K_{n\times n}), m) = \pm 1$ maka $ad - bc = \pm 1$ jadi $ad = 1 \pm bc$

sehingga $a = \frac{1 \pm bc}{d}$. oleh karena itu, terdapat beberapa kemungkinan cara untuk memilih b, c, d sedemikian sehingga $a \epsilon \mathbb{Z}$ dengan memilih syarat-syarat tertentu, yaitu:

1. $d \neq 0$ maka d< 0 atau d>0.
2. $|1 \pm bc| \geq d$.
3. $1 \pm bc \equiv 0 \ (mod\ d)$.

Contoh: $a = \frac{1+bc}{d}$

Untuk $1 + bc = 32 \ \longrightarrow 9 \equiv 0(mod\ d)$

$$9 = kd + 0$$

$9 = kd$ dimana $k = 3, d = 3$

dan $k = 3, d = 3$ atau sebaliknya.

$bc = 8 \longrightarrow b = 1, c = 8\ dan\ b = 2, c = 4$ atau sebaliknya.

Dengan memilih $d = 3$, maka $a = \frac{1+bc}{d}$ untuk $a = \frac{1+8}{3} = \frac{9}{3} = 3$

Didapatkan, $a = 3$.

Sedemikian hingga $ad - bc = 1$, maka $3(3) - 8 = 1$

Dapat dilihat dari salah satu contoh diatas, bhawa jika banyaknya bilangan bulat sampai tak terhingga, maka banyaknya nilai $\det(K) = \pm 1$ juga tak terhingga. Jadi syarat (1), (2) dan (3) berlaku untuk $ad - bc \pm 1$.

3.1.3 Kontruksi Pembentukan Kunci Matriks Algoritma *Hill Cipher*.

Keamanan sistem kriptografi terletak pada kerahasiaan kunci matriks. Apabila pengirim pesan mengenkripsikan pesan menggunakan suatu kunci rahasia sehingga dapat menghasilkan *ciphertext* dan begitu sebaliknya penerima pesan dapat menghasilkan *plaintext* yang semula.

Kedua pihak harus melakukan suatu perjanjian untuk membentuk suatu kunci matriks, karena tidak semua kunci matriks dapat digunakan untuk melakukan proses enkripsi dan dekripsi. Oleh karena itu, syarat-syarat yang digunakan untuk mendapatkan kunci matriks tersebut adalah:

1. $\boldsymbol{K}_{n\times n}$ adalah kunci matriks peersegi terhadap operasi perkalian.
2. Elemen-elemen dari kunci matriks$\boldsymbol{K} \epsilon \mathbb{Z}$, Sehingga:
3. Invers dari kunci matriks $({K^{-1}}_{n\times n})$ akan mempunyai elemen-elemen yang berupa bilangan bulat jika determinannya dari matriks tersebut sama dengan 1 atau -1.
4. Kunci matriks *hill cipher* harus berupa matriksyang invertible yaitu memiliki *multiplicative inverse*${K^{-1}}_{n\times n}$ sehingga $\boldsymbol{K}_{n\times n}{K^{-1}}_{n\times n} = 1$.
5. Suatu matriks $\boldsymbol{K}_{n\times n}$ memiliki invers jika da hanya jika determinannya tidak nol.

3.1.4 Analisis Algoritma Transposisi Columnar

Proses mengenkripsi pesan dengan menggunakan columnar termasuk transposisi dengan memindahkan karakter-karakternya sesuai teori columnar. Cara kerja sandi transposisi columnar adalah dengan menulis karakter asli dengan bentuk orientasi baris dengan panjang karakter yang sama. Kemudian teks sandi didapatkan dengan menulis ulang bentuk orientasi kolom. Adapun urutan kolom telah disepakati sebelumnya oleh kedua belah pihak antara pengirim dan penerima untuk mempersulit sandi agar tetap terjaga keamanannya. Berikut ini merupakan beberapa tahap enkripsi dengan menggunakan Columnar :

a. Menuliskan *plaintext* dalam matriks dengan panjang kolom sesuai dengan panjang karakter kunci yang digunakan. Kolom yang disusun pertama adalah kolom yang berhubungan dengan karakter sesuai urutan abjad.
b. Menempatkan *plaintext* ditulis dari baris per baris yang dimulai dengan baris pertama.
c. Menyusun *plaintext* dimulai dari kolom yang berhubungan dengan karakter urutan pertama pada abjad. Adapun kata kunci dalam pembahasan ini yakni kata "YES" dimana "E" huruf abjad terawal lalu "S" lalu "Y", dimana sudah sesuai urutan abjad. Jadi "E"=1, "S"=2, "Y"=3.
d. Membagi setiap karakter dengan jumlah kolom yang ditentukan oleh banyak kata kunci.
e. Membaca hasil proses enkripsi ini secara vertikal atau per kolom sesuai urutan abjad pada karakter kuncinya.
f. Membagi chiperteks tersebut sesuai huruf pada kolom per kolom masing-masing.
g. Menyusun kembali *ciphertext* sesuai kunci yang bermakna.
h. Memasukkan ke tabel sesuai jumlah kata kuncinya secara vertikal atau perkolom secara keseluruhan.
i. Menemukan suatu *plaintext* seperti semula dengan membaca tabel tersebut secara perbaris atau horizontal. Dimulai dari baris awal sampai akhir dengan urutan kiri kanan sampai baris akhir.
j. Mendapatkan *plaintext* sesuai pesan semula terkirim.

3.2 Implementasi Enkripsi dan Dekripsi pada Algoritma *Hill Cipher* dan Columnar dengan Menggunakan Perhitungan Manual.

3.2.1 Implementasi Proses Enkripsi Pesan dengan *Hill Chiper*

Proses pengenkripsianini pengirim akan mengirimkan suatu pesan dengan kunci matriks ukuran $3 \times 3 (K_{3\times3})$. Berikut ini diambil sebuah contoh pesan dan kunci yang telah disepakati, yaitu:

P = "MATEMATIKA 2020 LULUS"

$$K_{3\times3} = \begin{bmatrix} 3 & 4 & 1 \\ 2 & 1 & 1 \\ 6 & 2 & 3 \end{bmatrix}$$

Pesan di atas menggunakan huruf kapital semua. Adapun suatu pesan dapat menggunakan semua karakter yang terdapat pada keyboard, dalam artian karakter tersebut masih bisa terbaca. Jika suatu pesan terdapat elemen-elemen matriks yang kosong maka dapat ditambahkan dengan sebarang huruf. Misalan dengan spasi, sehingga diperoleh seperti berikut ini:

1. $P_{1\times21} = [\text{MATEMATIKA 2020 LULUS }]$
2. kemudian mengkonversi P $(plaintext)$menjadi bentuk matriks 3×7 pada pesan asli menjadi karakter-karakter numerik sesuai dengan kode ASCII.

$$P_{3\times7} = \begin{bmatrix} 45 & 37 & 52 & 33 & 16 & 0 & 44 \\ 33 & 45 & 41 & 0 & 18 & 44 & 53 \\ 52 & 33 & 43 & 18 & 16 & 53 & 51 \end{bmatrix}$$

3. Menentukan suatu kunci enkripsi matriks $3 \times 3 \rightarrow K_{3\times3} = \begin{bmatrix} 3 & 4 & 1 \\ 2 & 1 & 1 \\ 6 & 2 & 3 \end{bmatrix}$
4. Mengalikan kunci matriks dengan matriks *plaintext* :

$$M = K_{3\times3}P_{3\times7}(mod\ 91) = \begin{bmatrix} 3 & 4 & 1 \\ 2 & 1 & 1 \\ 6 & 2 & 3 \end{bmatrix}\begin{bmatrix} 45 & 37 & 52 & 33 & 16 & 0 & 44 \\ 33 & 45 & 41 & 0 & 18 & 44 & 53 \\ 52 & 33 & 43 & 18 & 16 & 53 & 51 \end{bmatrix}(mod\ 91)$$

$$= \begin{bmatrix} 319 & 324 & 363 & 117 & 136 & 229 & 395 \\ 175 & 152 & 188 & 84 & 66 & 97 & 192 \\ 492 & 411 & 523 & 252 & 180 & 247 & 523 \end{bmatrix} mod\ 91$$

$$= \begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix}$$

Setelah itu, mengubah ke dalam bentuk matriks 1×21 seperti berikut ini:

[**46 84 37 51 61 47 90 6 68 26 84 70 45 66 89 47 6 65 31 10 68**]

$$C = NtES]Oz\&d{:}\ tfMbyO\&a?{*}\ d$$

5. Memperoleh suatu *ciphertext* "$NtES]Oz\&d{:}\ tfMbyO\&a?{*}\ d$ ".

3.2.2 Implementasi Proses Enkripsi Columnar

Plaintext akan dienkripsi menggunakan transposisi columnar sehingga menjadi *ciphertext*. Dalam proses mengenkripsi *plaintext* yang merupakan *ciphertext*-nya *hill chiper*, karakter spasi disimbolkandengan tanda"#". Proses mengimplementasikan enkripsi columnar pada pembahasan ini terdapat dua puluh satu karakter dan tiga karakter kunci. Jumlah karakter kunci disesuaikan dengan jumlah baris matriks kunci *hill cipher*

a. Membuat *plaintext* :MATEMATIKA#2020#LULUS
b. Menggunakan kunci " YES". Karakter-karakter kunci tersebut diurutkan sesuai urutan abjad dimana E menempati posisi pertama dalam urutan abjad dan Smenempati posisi kedua dan Y menempati posisi ketiga, sehingga format urutan 3-1-2.
c. Memasukkan karakter - karakter di atas pada tabel berikut sesuai jumlah kunci yakni tigakolom dan karakter tersebut diletakkansecara perbaris atau horizontal dari baris pertama ke berikutnya dengan formasi kiri ke kanan (berlaku sampai akhir karakter).

‘Y’	‘E’	‘S’
M	A	T
E	M	A
T	I	K
A	#	2
0	2	0
#	L	U
L	U	S

d. Menghasilkan *ciphertext*dengan membacanya secara vertikal sesuai urutan abjad nya diawali dengan huruf E, sehingga didapatkan seperti berikut : AMI#2LUTAK20USMETA0#L .

3.2.3 Implementasi Proses Dekripsi Columnar

Transposisi Columnar akan mendekripsi hasil enkripsi columnar dengan *mentranspose*-nya dan menggunakan kunci yang sama dengan proses enkripsi columnar. Terdapat perbedaan dalam pengurutan karakter kunci yang disesuaikan nama kuncinya. Berikut ini beberapa tahap proses dekripsi menggunakan columnar :

a. Mendapatkan *ciphertext* yang merupakan hasil dari proses enkripsi columnar yaitu : AMI#2LUTAK20USMETA0#L

b. Memasukkan karakter-karakter pada *ciphertext* tersebut ke dalam tabel yang sama persis dengan proses enkripsi columnar. Memasukkan karakter secara vertikal atau perkolom sesuai dengan kata kunci “YES”

c. Sebelum memasukkan beberapa karakter, menentukan anggota pada tiap bagian sesuai langkah proses enkripsi columnar. Jumlah *plaintext* terdapat dua puluh satu karakter yang dibagi dengan jumlah karakter kuncinya yaitu tiga maka anggota tiap bagian terdapattujuh karakter, seperti berikut :

- Bagian 1 (mewakili huruf 'E') : AMI#2LU
- Bagian 2 (mewakili huruf 'S') : TAK20US
- Bagian 3 (mewakili huruf 'Y') : META0#L

d. Menyusun bagian-bagian tersebut seperti berikut ini:

'Y'	'E'	'S'
M	A	T
E	M	A
T	I	K
A	#	2
0	2	0
#	L	U
L	U	S

e. Menghasilkan suatu *plaintext* dari tabel di atas dengan membaca secara horizontal atau baris perbaris yaitu MATEMATIKA#2020#LULUS

Dengan demikian, pesan tersebut sesuai dengan *plaintext*s emula dan memiliki makna sesuai maksud pengirim pesan.

3.2.4 Implementasi Proses Dekripsi *Hill Cipher*

Berikut adalah proses dekripsi pesan menggunakan algoritma *hill cipher* :

1. Mendapatkan kode *ciphertext* dari hasil enkripsi *hill cipher*:

$$C = NtES]Oz\&d{:}\ tfMbyO\&a?{*}\ d$$

2. Mendapatkan kunci invers : $K^{-1} = \begin{bmatrix} 1 & -10 & 3 \\ 0 & 3 & -1 \\ -2 & 18 & -5 \end{bmatrix}$

Dengan determinan: $|A| = aei + bfg + cdh - ceg - bdi - afh = 3.1.3 + 4.1.6 + 1.2.2 - 1.1.6 - 4.2.3 - 3.1.2 = 9 + 24 + 4 - 6 - 24 - 6 = 37 - 36 = 1$

Adjoin: $M_{11} = \begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} = 3 - 2 = 1,\quad M_{12} = \begin{vmatrix} 2 & 1 \\ 6 & 3 \end{vmatrix} = 6 - 6 = 0,\ M_{13} = \begin{vmatrix} 2 & 1 \\ 6 & 2 \end{vmatrix} = 4 - 6 = -2,\quad M_{21} = \begin{vmatrix} 4 & 1 \\ 2 & 3 \end{vmatrix} = 12 - 2 = 10,\ M_{22} = \begin{vmatrix} 3 & 1 \\ 6 & 3 \end{vmatrix} = 9 - 6 = 3, M_{23} = \begin{vmatrix} 3 & 4 \\ 6 & 2 \end{vmatrix} = 6 - 24 = -18,\ M_{31} = \begin{vmatrix} 4 & 1 \\ 1 & 1 \end{vmatrix} = 4 - 1 = 3, M_{32} = \begin{vmatrix} 3 & 1 \\ 2 & 1 \end{vmatrix} = 3 - 2 = 1,\ M_{33} = \begin{vmatrix} 3 & 4 \\ 2 & 1 \end{vmatrix} = 3 - 8 = -5$

Maka matriks kofaktor $C = \begin{bmatrix} 1 & 0 & -2 \\ 10 & 3 & -18 \\ 3 & 1 & -5 \end{bmatrix}, C^T = \begin{bmatrix} 1 & 10 & 3 \\ 0 & 3 & 1 \\ -2 & -18 & -5 \end{bmatrix},$

$\begin{bmatrix} 1 & -10 & 3 \\ 0 & 3 & -1 \\ -2 & 18 & -5 \end{bmatrix}$(dengan menggunakan aturan $\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$)

$$K^{-1} = \frac{1}{|A|}\begin{bmatrix} 1 & -10 & 3 \\ 0 & 3 & -1 \\ -2 & 18 & -5 \end{bmatrix} = \frac{1}{1}\begin{bmatrix} 1 & -10 & 3 \\ 0 & 3 & -1 \\ -2 & 18 & -5 \end{bmatrix} = \begin{bmatrix} 1 & -10 & 3 \\ 0 & 3 & -1 \\ -2 & 18 & -5 \end{bmatrix}$$

3. Mengubah karakter *ciphertext* ke dalam karakter bilangan kode ASCII sehingga menjadi matriks $F_{1\times 21}$

$F_{1\times 21}$

$= [46\ 84\ 37\ 51\ 61\ 47\ 90\ 6\ 68\ 26\ 84\ 70\ 45\ 66\ 89\ 47\ 6\ 65\ 31\ 10\ 68]$

4. Mengubah lagi menjadi matriks $G_{3\times 7}$ untuk disesuaikan dengan invers matriks kuncinya

$$G = \begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix}$$

5. Mengalikan invers matriks kunci dengan matriks *ciphertext* yang dimodulokan dengan 91.

$$K^{-1}{}_{3\times3} G_{3\times7} = \begin{bmatrix} 1 & -10 & 3 \\ 0 & 3 & -1 \\ -2 & 18 & -5 \end{bmatrix} \begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix} mod\ 91$$

6. Mengalikan antar matriks yang akan dimodulokan.

$$I_{3\times7} = \begin{bmatrix} -683 & -418 & 234 & -604 & -348 & 182 & 135 \\ 215 & 136 & -50 & 182 & 109 & -47 & -38 \\ 1235 & 761 & -412 & 1110 & 653 & -311 & -222 \end{bmatrix} mod\ 91$$

7. Berikut ini hasil setelah dimodulokan :

$$J_{3\times7} = \begin{bmatrix} 45 & 37 & 52 & 33 & 16 & 0 & 44 \\ 33 & 45 & 41 & 0 & 18 & 44 & 53 \\ 52 & 33 & 43 & 18 & 16 & 53 & 51 \end{bmatrix}$$

8. Setelah itu, diubah ke matriks 1×21

$$J_{3\times7} = [45\ 33\ 52\ 37\ 45\ 33\ 52\ 41\ 43\ 33\ 0\ 18\ 16\ 18\ 16\ 0\ 44\ 53\ 44\ 53\ 51].$$

10. dihasilkan *plaintext* seperti ini: $M\ A\ T\ E\ M\ A\ T\ I\ K\ A\ 2\ 0\ 2\ 0\ L\ U\ L\ U\ S$.

3.3 Super Enkripsi

Super enkripsi merupakan salah satu kriptografi berbasis karakter yang menggabungkan *cipher* substitusi dan *cipher* transposisi. Adapun *cipher* substitusi dalam bahasan ini menggunakan algoritma *hill cipher* sedangkan cipher transposisinya menggunakan transposisi columnar. Hal ini bertujuan untuk mendapatkan *cipher* yang lebih kuat daripada hanya menggunakan satu cipher saja, sehingga tidak mudah untuk dipecahkan. Enkripsi dan dekripsinya dapat dilakukan dengan urutan *cipher* substitusi kemudian dilanjutkan cipher

transposisi, atau sebaliknya. Super enkripsi dapat dilakukan dengan menggunakan kedua *chiper* tersebut secara berulang-ulang, namun dalam penelitian ini hanya akan dibahas mengenai proses enkripsi dan dekripsi satu kali dengan menggunakan *cipher* substitusi dan satu kali dengan menggunakan *cipher* transposisi.

3.3.1 Enkripsi dalam Proses Super Enkripsi

Super enkripsi dapat dilakukan dengan melakukan proses enkripsi dengan menggunakan kedua *cipher* tersebut secara berurutan. Pada Pembahasan diatas terdapat *plaintext* yang akan akan diproses sebagai berikut :

1. Dibuat matriks: $P_{1\times 21} = [\text{MATEMATIKA 2020 LULUS}]$
2. P adalah matriks 3×7 pada pesan asli yang dikonversi dalam bentuk elemen-elemen nilai numerik yang sesuai dengan kode ASCII

$$P_{3\times 7} = \begin{bmatrix} 45 & 37 & 52 & 33 & 16 & 0 & 44 \\ 33 & 45 & 41 & 0 & 18 & 44 & 53 \\ 52 & 33 & 43 & 18 & 16 & 53 & 51 \end{bmatrix}$$

3. Ditentukan sebuah kunci enkripsi matriks $3 \times 3 \rightarrow K_{3\times 3} = \begin{pmatrix} 3 & 4 & 1 \\ 2 & 1 & 1 \\ 6 & 2 & 3 \end{pmatrix}$
4. Mengalikan kunci matriks dengan matriks *plaintext*

$$M = K_{3\times 3}P_{3\times 7}(mod\ 91) = \begin{bmatrix} 3 & 4 & 1 \\ 2 & 1 & 1 \\ 6 & 2 & 3 \end{bmatrix}\begin{bmatrix} 45 & 37 & 52 & 33 & 16 & 0 & 44 \\ 33 & 45 & 41 & 0 & 18 & 44 & 53 \\ 52 & 33 & 43 & 18 & 16 & 53 & 51 \end{bmatrix}(mod\ 91)$$

$$= \begin{bmatrix} 319 & 324 & 363 & 117 & 136 & 229 & 395 \\ 175 & 152 & 188 & 84 & 66 & 97 & 192 \\ 492 & 411 & 523 & 252 & 180 & 247 & 523 \end{bmatrix} mod\ 91$$

$$= \begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix}$$

$$= [46\ 84\ 37\ 51\ 61\ 47\ 90\ 6\ 68\ 26\ 84\ 70\ 45\ 66\ 89\ 47\ 6\ 65\ 31\ 10\ 68]$$

$$C = NtES]Oz\&d{:}\,tfMbyO\&a?{*}\,d$$

5. Didapatkan hasil proses enkripsi dengan*hill chiper* berupa*ciphertext* sebagai berikut: $NtES]Oz\&d{:}\,tfMbyO\&a?{*}\,d$.

Selanjutnya, *ciphertext* tersebut dienkripsi kembali dengan menggunakan *cipher* transposisi columnar yang merupakan *plaintext* pada transposisi columnar. Dalam proses enkripsi terhadap transposisi columnar diperlukan panjang kunci yang sama dengan kunci pada *cipher* substitusinya, yaitu tiga kata kunci, sehingga akan didapatkan hasil sebagai berikut:

Plaintext : $NtES]Oz\&d{:}\,tfMbyO\&a?{*}\,d$

Kunci : YES→ 3-1-2

‘Y’	‘E’	‘S’
N	t	E
S	]	O
z	&	d
:	t	f
M	b	y
O	&	a
?	*	d

Hasil *ciphertext***:** = t]&tb&*EOdfyadNSz:MO?

Ciphertext didapatkan dengan membaca tiap kolom diatas sesuai urutan karakter kuncinya “YES” yang memiliki urutan 3-1-2, karakter E merupakan urutan pertama dalam abjad dengan berisikan karakter-karakter“t]&tb&*” dan S

yaitu“EOdfyad” dan Y yaitu “NSz:MO?”. Sehingga *ciphertext* dari proses enkripsi dengan transposisi columnar “ t]&tb&*EOdfyadNSz:MO? ”

3.3.2 Dekripsi dalam Proses Super Enkripsi

Untuk mengembalikan *ciphertext* tersebut menjadi *plaintext* yang memiliki makna sesungguhnya pada suatu pesan, diperlukan proses dekripsi secara berurutan dengan menggunakan *hill cipher* dan transposisi columnar, yang mana urutan dekripsinya ditukar dengan proses enkripsinya. Jadi dalam proses dekripsi yang pertama adalah transposisi columnar lalu *hill cipher*. Mengawali proses dekripsi yang menggunakan transposisi columnar dengan membagi jumlah *plaintext* dengan jumlah kata kunci sehingga didapatkan 21 dibagi 3 yaitu 7. Lalu dimasukkkan ke dalam kolom berikut ini:

Menggunakan ciphertext dari *hill cipher*: $C = t]\&tb\& * EOdfyad\ NSz{:}\ MO?$

dengan kunci =YES→3 1 2

“Y”	“E”	“S”
N	t	E
S	]	O
z	&	d
:	t	f
M	b	y
O	&	A
?	*	D

Maka didapatkan *plaintext* seperti diatas yakni : $NtES]Oz\&d{:}\ tfMbyO\&a?*\ d$ dimana *plaintext* tersebut dapat dibaca secara per baris dari kiri ke kanan yang

diawali dari kolom satu sampai kolom akhir kemudian *plaintext* tersebut diubah ke bilangan numerik yang sesuai dengan kode ASCII.

Untuk mengubah *plaintext*nya, dibutuhkan sebuah kunci yang dari awal disepakati kedua pihak yang kemudian diinverskan, seperti berikut ini:

1. Kunci matriks: $K^{-1} = \begin{bmatrix} 1 & -10 & 3 \\ 0 & 3 & -1 \\ -2 & 18 & -5 \end{bmatrix}$
2. Mengkonversi *plaintext* ke bilangan numerik dengan kode ASCII, seperti berikut ini: dengan memakai matriks 1×21

$$\boldsymbol{F_{1\times 21} = [46\ 84\ 37\ 51\ 61\ 47\ 90\ 6\ 68\ 26\ 84\ 70\ 45\ 66\ 89\ 47\ 6\ 65\ 31\ 10\ 68]}$$

3. Mengubah lagi menjadi matriks berukuran 3×7 untuk disesuaikan dengan kunci bermatriks berukuran 3×3

$$G = \begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix}$$

4. Mengalikan kunci bermatriks 3×3 dengan *plaintext* bermatriks 3×7 yang dimodulokan dengan 91.

$$H = \begin{bmatrix} 1 & -10 & 3 \\ 0 & 3 & -1 \\ -2 & 18 & -5 \end{bmatrix} \begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix} mod\ 91$$

$$I = \begin{bmatrix} -683 & -418 & 234 & -604 & -348 & 182 & 135 \\ 215 & 136 & -50 & 182 & 109 & -47 & -38 \\ 1235 & 761 & -412 & 1110 & 653 & -311 & -222 \end{bmatrix} mod\ 91$$

5. didapatkan hasil dari perkalian matriks tersebut sebagai berikut:

$$J = \begin{bmatrix} 45 & 37 & 52 & 33 & 16 & 0 & 44 \\ 33 & 45 & 41 & 0 & 18 & 44 & 53 \\ 52 & 33 & 43 & 18 & 16 & 53 & 51 \end{bmatrix}$$

6. Mengubah lagi menjadi *plaintext* bermatriks 1×21, dari perkolom-kolom diatas menjadi satu baris

$$\boldsymbol{J}$$

$$= [\mathbf{45\ 33\ 52\ 37\ 45\ 33\ 52\ 41\ 43\ 33\ 0\ 18\ 16\ 18\ 16\ 0\ 44\ 53\ 44\ 53\ 51}]$$

7. Mengkonversi bilangan numerik dengan kode ASCII tersebut ke *plaintext* asli. Sehingga didapatkan *Plaintext* berikut ini:

$$[MATEMATIKA\ 2020\ LULUS].$$

Proses super enkripsi diatas ditentukan dengan menggabungkan cipher substitusi dan cipher transposisi. Adapun cipher substitusinya yakni algoritma *hill* Cipher dan cipher transposisinya yakni transposisi columnar. Proses ini mengenkripsi suatu *plaintext* menggunakan algoritma *hill* cipher terlebih dahulu yang menghasilkan suatu *ciphertext*, kemudian hasil tersebut dienkripsikan kembali menggunakan transposisi columnar yang menghasilkan *ciphertext* juga. Kemudian hasil dari enkripsi dengan menggunakan transposisi columnar tersebut didekripsikan dengan proses algoritma transposisi columnar terlebih dulu, sehingga menghasilkan *plaintext* yang akan didekripsikan kembali menggunakan algoritma *hill cipher*. Dengan demikian, didapatkan hasil dari pendekripsian dari algoritma *hill cipher* yang merupakan pesan asli yang dapat terbaca oleh penerim pesan.

Pesan ini akan terbaca sesuai pesan yang telah dikirim oleh pengirim jika kedua pihak telah menyepakati suatu kunci pada pesan tersebut. Penggunaan super enkripsi ini sesuai dengan tujuannya untuk mendapatkan cipher yang lebih kuat daripada hanya menggunakan *satu chiper* saja, sehingga tidak mudah untuk dipecahkan. Penggabungan kedua algoritma ini juga untuk mengamankan pesan secara efektif, sehingga dapat dipastikan pesan yang ada tersebut tidak akan

diperoleh dan diketahui dengan muda oleh orang-orang yang tidak mempunyai kewenangan untuk itu.

3.4 Implementasi Enkripsi dan Dekripsi pada Super Enkripsi (Algoritma Hill Cipher dan Transposisi Columnar) dengan Menggunakan Maple

Prosesimplementasi enkripsi dan dekripsi super enkripsi ini menggunakan *coding* matriks untuk *cipher* substitusinya dan *coding* transpose untuk *cipher* transposisi pada aplikasi Maple. Pengcodingan kedua algoritma diperlukan untuk mencocokkan perhitungan manual dengan perhitungan aplikasi matematika.

3.4.1 Proses Enkripsi *Hill Cipher*dengan Menggunakan Aplikasi Maple

Untuk mengetahui implementasi suatu enkripsi akan diberikan suatu pesan *plaintext* yaitu: “MATEMATIKA 2020 LULUS”.

1. Susunan karakter *plaintext* dalam bentuk matriks diperoleh (Lampiran II)
2. Membuat matriks berukuran 3×7 karakter (Lampiran II)
3. Menentukan suatu kunci matriks enkripsi berukuran 3×3 (Lampiran II)
4. Mengalikan *plaintext* dengan kunci matriks: (Lampiran II)
5. Hasil dari perkalian akan dimodulo 91 dan ditambahkan dengan 32 (Lampiran II)
6. Mengkonversikan suatu matriks yang yang didapatkan sebagai hasil ke dalambentuk ASCII, dan hasil enkripsi (*ciphertext*) diperoleh:

(Lampiran II)

3.4.2 Proses Enkripsi Transposisi *Columnar* dengan Menggunakan Aplikasi Maple.

Pada proses enkripsi dan dekripsi columnar, *plaintext* yang digunakan merupakan hasil *ciphertext* hill cipher yang diubah ke bilangan ASCII terlebih dahulu dikarenakan pada aplikasi maple tidak akan terdefiniskan jika memasukkan kode selain abjad dan angka. Jika diteruskan menggunakan tanda lain seperti ":", " ; " , dan lainnya.

Berikut ini contoh kode yang terdefinisikan pada Maple

baris1 := NtE

baris1 := NtE

Proses columnar ini terbantu dengan panduan help pada Maple yakni menggunakan transpose

Berikut merupakan tahap pengcodingan enkripsi pada Maple :

1. Mengubah *ciphertext* hill cipher dengan cara mentranspos
   (Lampiran II)
2. Mendefinisikan bagian-bagian dari karakter kunci sesuai jumlah karakter kunci
   (Lampiran II)
3. Bagian-bagian tersebut digabungkansesuai urutan kata yang bermakna
   (Lampiran II)
4. Mentransformasi bagian bagian sesuai kunci yang berdasar urutan abjad
   (Lampiran II)

5. *Mentranspose* hasil transformasi di atas dan menghasilkan *ciphertext* dalam bentuk bilangan ASCII

   (Lampiran II)

6. Mengubah *ciphertext* dalam bentuk karakter ASCII

   (Lampiran II)

7. Menjumlahkan antara matriks *ciphertext* dengan matriks 32

   (Lampiran II)

8. Mengkonversikan hasil penjumlahan sehingga mendapatkan *ciphertext* dalam bentuk karakter ASCII :

   (Lampiran II)

3.4.3 Proses Dekripsi TransposisiColumnar dengan Menggunakan Aplikasi Maple

Proses dekripsi ini masih menggunakan *transpose* pada aplikasi Maple. Proses dekripsi hampir sama dengan enkripsi, namun perlu sedikit membalik beberapa proses dari enkripsinya. Berikut ini bebrapa tahapan pengcodingan proses dekripsi dengan menggunakan columnar :

1. Mengubah hasil enkripsi columnar menjadi bentuk matriks (pengganti tabel)

   (Lampiran II)

2. Mentransformasi kembali matriks sesuai karakter kunci berdasar urutan abjad

   (Lampiran II)

3. Mengubah hasil dari (langkah 10)ke dalam bentuk matriks berukuran 1×21

   (Lampiran II)

4. Mentransformasi kembalimatriks diatas menjadi matriks berukuran 3×7 untuk memudahkan dijadikan karakter ASCII.

   (Lampiran II)

5. Matriks berukuran 3×7 tersebut dijumlahkan dengan matriks 32 ukuran 3×7

   (Lampiran II)

6. Mengkonversi hasil penjumlahan tersebut ke dalam karakter ASCII

   (Lampiran II)

3.4.4 Proses Dekripsi *Hill Cipher* dengan Menggunakan Aplikasi Maple

Berikut ini merupakanpengcodingan pada proses dekripsi dengan menggunakan *hill cipher* :

1. Dalam proses dekripsi ini dianjurkan untuk menuliskan perintah “with linalg” karena berhubungan dengan matriks dan inversnya.
2. Menentukan invers dari kunci enkripsi terlebih dahulu.

   (Lampiran II)

3. Mendekripsi *ciphertext* (hasil dekripsicolumnar) menjadi suatu matriks.
4. Mengalikan matriks suatu *ciphertext* diatas dengan invers kunci matriksnya sehingga diperoleh:

   (Lampiran II)

5. Hasil perkalian tersebut dimodulokan 91 dan ditambah dengan matriks 32 untuk menjadi suatu karakter ASCII

   (Lampiran II)

6. Kemudian hasil diatas dikonversikan agar menjadi *plaintext* seperti semula

   (Lampiran II)

BAB 1V

PENUTUP

4.1 Kesimpulan

Berdasarkan pembahasan diatas dapat disimpulkan sebagai berikut :

1. Proses enkripsi super enkripsi merupakan gabungan proses enkripsi *hill cipher* dan proses enkripsi transposisi columnar. Proses pertama mengenkripsi *plaintext* dengan *hill cipher*. Proses kedua mengenkripsi kembali *ciphertext*-nya *hill cipher* menjadi *ciphertext* columnar.
2. Proses dekripsi super enkripsi merupakan proses mengembalikan *ciphertext* menjadi *plaintext* seperti semula. Proses dekripsi ini diawali dengan mendekripsikan *ciphertext* dengan menggunakan transposisi columnar. Hasil proses dekripsi columnar didekripsikan kembali menjadi *plaintext*oleh*hill cipher*.

4.2 Saran

Penelitian ini membahas implementasi algoritma super enkripsi (*hill cipher* dan transposisi *columnar*) pada pesan teks. Metode enkripsi dan dekripsinya yang digunakan adalah substitusi cipher pada algoritma *hill cipher* dan cipher transposisi pada transposisi *columnar*. Untuk pengembangan penelitian selanjutnya disarankan menggunakan algoritma lain bisa yang tradisional atau modern seperti *vignere cipher*, *caesar cipher*, ECB, RSA, *Elgamal*, dan lainnya.

DAFTAR RUJUKAN

Abdillah, Ikhwan Muji. 2019. *Penyandian Model Kriptografi Hill Cipher dengan menggunakan Metode Transposisi Matriks*. Skripsi Tidak Dipublikasikan. Malang: UIN Maulana Malik Ibrahim.

Anggriani, Ika. 2019. *ImplementasiAlgoritma Modifikasi Transposisi Columnar dalam Mengamankan data Teks*. JTIK: vol.3, no.1.

Anton, H dan Rorres, C. 2010. *Elementary Linear Algebra Aplications Version.* New Jersey: John Wiley & Sons, Inc.

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

Ariyus, D. 2008. *Pengantar Ilmu Kriptografi*. Jogjakarta: Andi.

Azlindah, Nur. 2018. *Aplikasi Kriptografi Enkripsi dan Dekripsi Menggunakan Algoritma Hill Cipher untuk Mengamankan Pesan.* Skripsi Tidak Dipublikasikan. Malang: UIN Maulana Malik Ibrahim.

Hidayat, Akik, dkk. 2013. *Enkripsi dan Dekripsi Teks Menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang*. Jurnal Matematika Integratif. Vol.9: 39-51.

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

Katsir, I. 2003. *Tafsir Ibnu Katsir Jilid 2*. Terjemahan M. Abdul Ghoffar E.M. Bogor: Pustaka Imam As-Syafi'i.

Kromodimoeljo, S. 2010.*Teori dan Aplikasi Kriptografi*. Jakarta: SPK IT Consuling.

Munir, R. 2004. *Sistem Kriptografi Kunci-Publik Diktat Kuliah*. Bandung: Departemen Teknik Informatika Institut Teknologi Bandung.

Prima Puspita, Nikken.2010. *Kriptografi Hill Cipher dengan menggunakan Operasi matriks.* UGM.article.

Reswan, Yuza,. dkk. 2018. *Implementasi Kompilasi Algoritma Kriptografi transposisi Columnar dan RSA untuk Pengamanan Pesan Rahasia*. Jurnal Informatika Upgris. Vol.4, no.2.

Rosen, K.H. 2012.*Discrete Mathematics and Its Aplications Seventh Edition*. New York: McGraw-Hill.

Wais, Al-Qorny. 2018. *Enkripsi dan Dekripsis Pesan Menggunakan Algoritma RSA dan Affine Cipher dengan Metode Matriks*. Skripsi Tidak Dipublikasikan. Malang: UIN Maulana Malik Ibrahim.

LAMPIRAN

Lampiran

Lampiran 1.

Tabel ASCII

Dec	Hex	HTML	Char	Description
0	00	&#0;	NUL	Null
1	01	&#1;	SOH	Start of Header
2	02	&#2;	STX	Start of Text
3	03	&#3;	ETX	End of Text
4	04	&#4;	EOT	End of Transmission
5	05	&#5;	ENQ	Enquiry
6	06	&#6;	ACK	Acknowledge
7	07	&#7;	BEL	Bell
8	08	&#8;	BS	Backspace
9	09		HT	Horizontal Tab
10	0A
LF	Line Feed
11	0B	&#11;	VT	Vertical Tab
12	0C		FF	Form Feed
13	0D
CR	Carriage Return
14	0E	&#14;	SO	Shift Out
15	0F	&#15;	SI	Shift In
16	10	&#16;	DLE	Data Link Escape
17	11	&#17;	DC1	Device Control 1
18	12	&#18;	DC2	Device Control 2
19	13	&#19;	DC3	Device Control 3
20	14	&#20;	DC4	Device Control 4
21	15	&#21;	NAK	Negative Acknowledge
22	16	&#22;	SYN	Synchronize
23	17	&#23;	ETB	End of Transmission Block
24	18	&#24;	CAN	Cancel
25	19	&#25;	EM	End of Medium
26	1A	&#26;	SUB	Substitute
27	1B	&#27;	ESC	Escape
28	1C	&#28;	FS	File Separator
29	1D	&#29;	GS	Group Separator
30	1E	&#30;	RS	Record Separator
31	1F	&#31;	US	Unit Separator
32	20		space	Space
33	21	!	!	Exclamation mark

34	22	&#34;	"	Double quote
35	23	&#35;	#	Number
36	24	&#36;	$	Dollar sign
37	25	&#37;	%	Percent
38	26	&#38;	&	Ampersand
39	27	&#39;	'	Single quote
40	28	&#40;	(	Left parenthesis
41	29	&#41;	)	Right parenthesis
42	2A	&#42;	*	Asterisk
43	2B	&#43;	+	Plus
44	2C	&#44;	,	Comma
45	2D	&#45;	-	Minus
46	2E	&#46;	.	Period
47	2F	&#47;	/	Slash
48	30	&#48;	0	Zero
49	31	&#49;	1	One
50	32	&#50;	2	Two
51	33	&#51;	3	Three
52	34	&#52;	4	Four
53	35	&#53;	5	Five
54	36	&#54;	6	Six
55	37	&#55;	7	Seven
56	38	&#56;	8	Eight
57	39	&#57;	9	Nine
58	3A	&#58;	:	Colon
59	3B	&#59;	;	Semicolon
60	3C	&#60;	<	Less than
61	3D	&#61;	=	Equality sign
62	3E	&#62;	>	Greater than
63	3F	&#63;	?	Question mark
64	40	&#64;	@	At sign
65	41	&#65;	A	Capital A
66	42	&#66;	B	Capital B
67	43	&#67;	C	Capital C
68	44	&#68;	D	Capital D
69	45	&#69;	E	Capital E
70	46	&#70;	F	Capital F
71	47	&#71;	G	Capital G
72	48	&#72;	H	Capital H

73	49	&#73;	I	Capital I
74	4A	&#74;	J	Capital J
75	4B	&#75;	K	Capital K
76	4C	&#76;	L	Capital L
77	4D	&#77;	M	Capital M
78	4E	&#78;	N	Capital N
79	4F	&#79;	O	Capital O
80	50	&#80;	P	Capital P
81	51	&#81;	Q	Capital Q
82	52	&#82;	R	Capital R
83	53	&#83;	S	Capital S
84	54	&#84;	T	Capital T
85	55	&#85;	U	Capital U
86	56	&#86;	V	Capital V
87	57	&#87;	W	Capital W
88	58	&#88;	X	Capital X
89	59	&#89;	Y	Capital Y
90	5A	&#90;	Z	Capital Z
91	5B	&#91;	[	Left square bracket
92	5C	&#92;	\	Backslash
93	5D	&#93;	]	Right square bracket
94	5E	&#94;	^	Caret / circumflex
95	5F	&#95;	_	Underscore
96	60	&#96;	`	Grave / accent
97	61	&#97;	a	Small a
98	62	&#98;	b	Small b
99	63	&#99;	c	Small c
100	64	&#100;	d	Small d
101	65	&#101;	e	Small e
102	66	&#102;	f	Small f
103	67	&#103;	g	Small g
104	68	&#104;	h	Small h
105	69	&#105;	i	Small i
106	6A	&#106;	j	Small j
107	6B	&#107;	k	Small k
108	6C	&#108;	l	Small l
109	6D	&#109;	m	Small m
110	6E	&#110;	n	Small n
111	6F	&#111;	o	Small o

112	70	p p	Small p
113	71	q q	Small q
114	72	r r	Small r
115	73	s s	Small s
116	74	t t	Small t
117	75	u u	Small u
118	76	v v	Small v
119	77	w w	Small w
120	78	x x	Small x
121	79	y y	Small y
122	7A	z z	Small z
123	7B	{ {	Left curly bracket
124	7C		|	Vertical bar
125	7D	} }	Right curly bracket
126	7E	~ ~	Tilde
127	7F	&#127; DEL	Delete

Lampiran II

Proses Enkripsi*Hill Cipher* menggunakan Aplikasi Maple

1. >*plaintekshillcipher* := *map*(*Ord*, *Explode*("MATEMATIKA 2020 LULUS"));

   Explode(*Ord*("MATEMATIKA 2020 LULUS"))

   1. *ENKRIPSI HILL CIPHER*

      1. *ENKRIPSI HILL CIPHER*

2. *matriksplaintekshillcipher* := *matrix*(3, 7, [45, 37, 52, 33, 16, 0, 44, 33, 45, 41, 0, 18, 44, 53, 52, 33, 43, 18, 16, 53, 51]);

$$\begin{bmatrix} 45 & 37 & 52 & 33 & 16 & 0 & 44 \\ 33 & 45 & 41 & 0 & 18 & 44 & 53 \\ 52 & 33 & 43 & 18 & 16 & 53 & 51 \end{bmatrix}$$

3. *kuncienkripsihill* := *matrix*(3, 3, [3, 4, 1, 2, 1, 1, 6, 2, 3]);

$$\begin{bmatrix} 3 & 4 & 1 \\ 2 & 1 & 1 \\ 6 & 2 & 3 \end{bmatrix}$$

4. *evalm*(*kuncienkripsihill*.*matriksplaintekshillcipher*);

$$\begin{bmatrix} 319 & 324 & 363 & 117 & 136 & 229 & 395 \\ 175 & 152 & 188 & 84 & 66 & 97 & 192 \\ 492 & 411 & 523 & 252 & 180 & 247 & 523 \end{bmatrix}$$

5. $$\begin{bmatrix} 319 & 324 & 363 & 117 & 136 & 229 & 395 \\ 175 & 152 & 188 & 84 & 66 & 97 & 192 \\ 492 & 411 & 523 & 252 & 180 & 247 & 523 \end{bmatrix} \bmod 91$$

$$\begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix}$$

mengubah hasil enkripsi di atas ke dalam bentuk karakter ASCII ,
sehingga diperlukan matriks berikut

mengubah hasil enkripsi di atas ke dalam bentuk karakter ASCII,
sehingga diperlukan matriks berikut

6. $d := matrix(3, 7, [32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32])$;

$$\begin{bmatrix} 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \end{bmatrix}$$

7. $$\begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix} + \begin{bmatrix} 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \end{bmatrix}$$

$$\begin{bmatrix} 78 & 83 & 122 & 58 & 77 & 79 & 63 \\ 116 & 93 & 38 & 116 & 98 & 38 & 42 \\ 69 & 79 & 100 & 102 & 121 & 97 & 100 \end{bmatrix}$$

8. $karakterasciihil : convert([78, 116, 69, 83, 93, 79, 122, 38, 100, 58, 116, 102, 77, 98, 121, 79, 38, 97, 63, 42, 100], 'bytes')$;

"NtES]Oz&d:tfMbyO&a?*d"

9. $HASILENKRIPSIHILLCIPHER :=$ "NtES]Oz&d:tfMbyO&a?*d"

"NtES]Oz&d:tfMbyO&a?*d"

Proses Enkripsi *Transposisi Columnar* Menggunakan Aplikasi Maple.

2. *ENKRIPSI COLUMNAR*

2. *ENKRIPSI COLUMNAR*

plainteks pada enkripsi columnar menggunakan hasil enkripsi hill cipher
plainteks pada enkripsi^2 columnar menggunakan hasil hill cipher

10. $columnar := \langle\langle 46, 51, 90, 26, 45, 47, 31\rangle|\langle 84, 61, 6, 84, 66, 6, 10\rangle|\langle 37, 47, 68, 70, 89, 65, 68\rangle\rangle$;

$$\begin{bmatrix} 46 & 84 & 37 \\ 51 & 61 & 47 \\ 90 & 6 & 68 \\ 26 & 84 & 70 \\ 45 & 66 & 89 \\ 47 & 6 & 65 \\ 31 & 10 & 68 \end{bmatrix}$$

11. *mendefinisikan tiap kolom di atas*

mendefinisikan tiap kolom di atas

$Y := \langle\langle 46, 51, 90, 26, 45, 47, 31\rangle\rangle;$

$$\begin{bmatrix} 46 \\ 51 \\ 90 \\ 26 \\ 45 \\ 47 \\ 31 \end{bmatrix}$$

$E := \langle\langle 84, 61, 6, 84, 66, 6, 10\rangle\rangle;$

$$E := \begin{bmatrix} 84 \\ 61 \\ 6 \\ 84 \\ 66 \\ 6 \\ 10 \end{bmatrix}$$

$S := \langle\langle 37, 47, 68, 70, 89, 65, 68\rangle\rangle;$

$$S := \begin{bmatrix} 37 \\ 47 \\ 68 \\ 70 \\ 89 \\ 65 \\ 68 \end{bmatrix}$$

12. $posisiberdasarkunci := \langle\langle Y\rangle|\langle E\rangle|\langle S\rangle\rangle;$

$$posisiberdasarkunciENKRIPSI := \begin{bmatrix} 46 & 84 & 37 \\ 51 & 61 & 47 \\ 90 & 6 & 68 \\ 26 & 84 & 70 \\ 45 & 66 & 89 \\ 47 & 6 & 65 \\ 31 & 10 & 68 \end{bmatrix}$$

13. $>prosesEnkripsi(kunci\ berdasar\ urutan\ abjad) := \langle\langle E\rangle|\langle S\rangle|\langle Y\rangle\rangle;$

$$prosesEnkripsi(kunci\ berdasar\ urutan\ abjad) := \begin{bmatrix} 84 & 37 & 46 \\ 61 & 47 & 51 \\ 6 & 68 & 90 \\ 84 & 70 & 26 \\ 66 & 89 & 45 \\ 6 & 65 & 47 \\ 10 & 68 & 31 \end{bmatrix}$$

14. $enkripsicolumnar := \langle\langle E\rangle|\langle S\rangle|\langle Y\rangle\rangle;$

$$enkripsicolumnar := \begin{bmatrix} 84 & 37 & 46 \\ 61 & 47 & 51 \\ 6 & 68 & 90 \\ 84 & 70 & 26 \\ 66 & 89 & 45 \\ 6 & 65 & 47 \\ 10 & 68 & 31 \end{bmatrix}$$

15. $enkripsicolumnar^{\%T};$

$$\begin{bmatrix} 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \\ 46 & 51 & 90 & 26 & 45 & 47 & 31 \end{bmatrix}$$

16. $c := \langle\langle 84, 61, 6\rangle|\langle 84, 66, 6\rangle| < 10, 37, 47 > |\langle 68, 70, 89\rangle| < 65, 68, 46 > |\langle 51, 90, 26\rangle|\langle 45, 47, 31\rangle\rangle;$

$$c := \begin{bmatrix} 84 & 84 & 10 & 68 & 65 & 51 & 45 \\ 61 & 66 & 37 & 70 & 68 & 90 & 47 \\ 6 & 6 & 47 & 89 & 46 & 26 & 31 \end{bmatrix}$$

$d := matrix(3, 7, [32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32]);$

$$d := \begin{bmatrix} 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \end{bmatrix}$$

17. $c + \begin{bmatrix} 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \end{bmatrix};$

$$\begin{bmatrix} 116 & 116 & 42 & 100 & 97 & 83 & 77 \\ 93 & 98 & 69 & 102 & 100 & 122 & 79 \\ 38 & 38 & 79 & 121 & 78 & 58 & 63 \end{bmatrix}$$

konversikeAscii := *convert*([116, 93, 38, 116, 98, 38, 42, 69, 79, 100, 102, 121, 97, 100, 78, 83, 122, 58, 77, 79, 63],'*bytes*');

konversikeAscii := "t]&tb&*EOdfyadNSz:MO?"

Proses Dekripsi *Transposisi Columnar*dengan Menggunakan Aplikasi Maple.

3. *DEKRIPSI COLUMNAR*

3. *DEKRIPSI COLUMNAR*

> *plainteksdekripsi* := ⟨⟨84, 61, 6, 84, 66, 6, 10⟩|⟨37, 47, 68, 70, 89, 65, 68⟩|⟨46, 51, 90, 26, 45, 47, 31⟩⟩;

$$plainteksdekripsi := \begin{bmatrix} 84 & 37 & 46 \\ 61 & 47 & 51 \\ 6 & 68 & 90 \\ 84 & 70 & 26 \\ 66 & 89 & 45 \\ 6 & 65 & 47 \\ 10 & 68 & 31 \end{bmatrix}$$

>*hasildekripsiberdasarkunciawal* := ⟨⟨*Y*⟩|⟨*E*⟩|⟨*S*⟩⟩;

$$hasildekripsiberdasarkunciawal := \begin{bmatrix} 46 & 84 & 37 \\ 51 & 61 & 47 \\ 90 & 6 & 68 \\ 26 & 84 & 70 \\ 45 & 66 & 89 \\ 47 & 6 & 65 \\ 31 & 10 & 68 \end{bmatrix}$$

>*maka hasil diatas ditranspose terlebih dulu agar bisa diubah ke suatu karakter ASCII*

maka hasil diatas ditranspose terlebih dulu agar bisa diubah ke suatu karakter ASCII

>$hasildekripsiberdasarkunciawal^{\%T}$;

$$\begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix}$$

> $\begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix} + \begin{bmatrix} 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \end{bmatrix};$

$$\begin{bmatrix} 78 & 83 & 122 & 58 & 77 & 79 & 63 \\ 116 & 93 & 38 & 116 & 98 & 38 & 42 \\ 69 & 79 & 100 & 102 & 121 & 97 & 100 \end{bmatrix}$$

> *HASILdekripsicolumnar* := *convert*([78, 116, 69, 83, 93, 79, 122, 38, 100, 58, 116, 102, 77, 98, 121, 79, 38, 97, 63, 42, 100],'*bytes*');

HASILdekripsicolumnar := "NtES]Oz&d:tfMbyO&a?*d"

Proses Dekripsi *Hill Cipher* Menggunakan Aplikasi Maple.

>4. *DEKRIPSI Hill CIPHER*

4. *DEKRIPSI Hill CIPHER*

>*with*(*linalg*);

[*BlockDiagonal*, *GramSchmidt*, *JordanBlock*, *LUdecomp*, *QRdecomp*, *Wronskian*, *addcol*, *addrow*, *adj*, *adjoint*, *angle*, *augment*, *backsub*, *band*, *basis*, *bezout*, *blockmatrix*, *charmat*, *charpoly*, *cholesky*, *col*, *coldim*, *colspace*, *colspan*, *companion*, *concat*, *cond*, *copyinto*, *crossprod*, *curl*, *definite*, *delcols*, *delrows*, *det*, *diag*, *diverge*, *dotprod*, *eigenvals*, *eigenvalues*, *eigenvectors*, *eigenvects*, *entermatrix*, *equal*, *exponential*, *extend*, *ffgausselim*, *fibonacci*, *forwardsub*, *frobenius*, *gausselim*, *gaussjord*, *geneqns*, *genmatrix*, *grad*, *hadamard*, *hermite*, *hessian*, *hilbert*, *htranspose*, *ihermite*, *indexfunc*, *innerprod*, *intbasis*, *inverse*, *ismith*, *issimilar*, *iszero*, *jacobian*, *jordan*, *kernel*, *laplacian*, *leastsqrs*, *linsolve*, *matadd*, *matrix*, *minor*, *minpoly*, *mulcol*, *mulrow*, *multiply*, *norm*, *normalize*, *nullspace*, *orthog*, *permanent*, *pivot*, *potential*, *randmatrix*, *randvector*, *rank*, *ratform*, *row*, *rowdim*, *rowspace*, *rowspan*, *rref*, *scalarmul*, *singularvals*, *smith*, *stackmatrix*, *submatrix*, *subvector*, *sumbasis*, *swapcol*, *swaprow*, *sylvester*, *toeplitz*, *trace*, *transpose*, *vandermonde*, *vecpotent*, *vectdim*, *vector*, *wronskian*]

>*det*(*kuncienkripsihill*);

1

>*adj*(*kuncienkripsihill*);

$$\begin{bmatrix} 1 & -10 & 3 \\ 0 & 3 & -1 \\ -2 & 18 & -5 \end{bmatrix}$$

>*inverse*(*kuncienkripsihill*);

$$\begin{bmatrix} 1 & -10 & 3 \\ 0 & 3 & -1 \\ -2 & 18 & -5 \end{bmatrix}$$

>$hasildekripsiberdasarkunciawal^{\%T}$;

$$\begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix}$$

> $plainteksdekripsiHill : \begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix}$

$$\begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix}$$

> $evalm(inverse(kuncienkripsihill).hasildekripsiberdasarkunciawal^{\%T})$;

$$\begin{bmatrix} -683 & -418 & 234 & -604 & -348 & 182 & 135 \\ 215 & 136 & -50 & 182 & 109 & -47 & -38 \\ 1235 & 761 & -412 & 1110 & 653 & -311 & -222 \end{bmatrix}$$

> $\begin{bmatrix} 1 & -10 & 3 \\ 0 & 3 & -1 \\ -2 & 18 & -5 \end{bmatrix} . \begin{bmatrix} 46 & 51 & 90 & 26 & 45 & 47 & 31 \\ 84 & 61 & 6 & 84 & 66 & 6 & 10 \\ 37 & 47 & 68 & 70 & 89 & 65 & 68 \end{bmatrix}$

$$\begin{bmatrix} -683 & -418 & 234 & -604 & -348 & 182 & 135 \\ 215 & 136 & -50 & 182 & 109 & -47 & -38 \\ 1235 & 761 & -412 & 1110 & 653 & -311 & -222 \end{bmatrix}$$

> $\begin{bmatrix} -683 & -418 & 234 & -604 & -348 & 182 & 135 \\ 215 & 136 & -50 & 182 & 109 & -47 & -38 \\ 1235 & 761 & -412 & 1110 & 653 & -311 & -222 \end{bmatrix} \bmod 91$

$$\begin{bmatrix} 45 & 37 & 52 & 33 & 16 & 0 & 44 \\ 33 & 45 & 41 & 0 & 18 & 44 & 53 \\ 52 & 33 & 43 & 18 & 16 & 53 & 51 \end{bmatrix}$$

> *mengubah hasil di atas ke suatu karakter*

mengubah hasil di atas ke suatu karakter

> $d := matrix(3, 7, [32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32])$;

$$d := \begin{bmatrix} 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \end{bmatrix}$$

> $\begin{bmatrix} 45 & 37 & 52 & 33 & 16 & 0 & 44 \\ 33 & 45 & 41 & 0 & 18 & 44 & 53 \\ 52 & 33 & 43 & 18 & 16 & 53 & 51 \end{bmatrix} + \begin{bmatrix} 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 \end{bmatrix}$;

$$\begin{bmatrix} 77 & 69 & 84 & 65 & 48 & 32 & 76 \\ 65 & 77 & 73 & 32 & 50 & 76 & 85 \\ 84 & 65 & 75 & 50 & 48 & 85 & 83 \end{bmatrix}$$

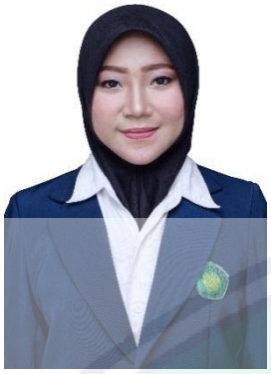
> *hasil di atas terbaca secara per kolom*

hasil di atas terbaca secara per kolom

```
> hasildekripsiHill := convert([77, 65, 84, 69, 77, 65, 84, 73, 75, 65, 32, 50, 48, 50, 48, 32, 76,
    85, 76, 85, 83],'bytes');
```

hasildekripsiHill := "MATEMATIKA 2020 LULUS"

RIWAYAT HIDUP



Nur Azizah dilahirkan di Sidoarjo pada tanggal 14 November 1996, biasa dipanggil zizah, merupakan anak kedua dari tiga bersaudara, pasangan bapak Sumi Harjono dan ibu Muslichah. Sekarang tinggal di Desa Kalidawir RT 11 RW 04, Kecamatan Tanggulangin Sidoarjo. Pendidikan dasarnya ditempuh di MI Islamiyah Kebonsari Malang yang ditamatkan pada tahun 2008. Pada tahun yang sama melanjutkan pendidikan menengah pertama di SMPN 12 Malang yang ditamatkan pada tahun 2011. Kemudian melanjutkan pendidikan menengah atas di SMAN 5 Malang yang ditamatkan pada tahun 2014. Pendidikan berikutnya ditempuh di Universitas Islam Negeri Maulana Malik Ibrahim Malang dengan mengambil Jurusan Matematika di Fakultas Sains dan Teknologi.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No. 50 Dinoyo Malang Telp./Fax. (0341)558933

BUKTI KONSULTASI SKRIPSI

Nama : Nur Azizah
NIM : 14610007
Fakultas/Jurusan : Sains dan Teknologi/Matematika
Judul Skripsi : Implementasi Algoritma Super Enkripsi (*Hill Cipher* dan Transposisi Columnar) Pada Pesan Teks

Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Muhammad Nafie Jauhari, M.Si

No	Tanggal	Hal	Tanda Tangan
1	17 Februari 2020	Konsultasi BAB I & II	1
2	12 Maret 2020	Konsul Keagamaan	2
3	27 April 2020	ACC Keagamaan	3
4	27 April 2020	ACC BAB I, II, & III	4
5	28 April 2020	Konsultasi BAB II & III	5
6	30 April 2020	Konsultasi Ayat	6
7	3 September 2020	Konsultasi BAB III	7
8	5 September 2020	Revisi BAB III	8
9	16 September 2020	Konsultas BAB III	9
10	9 Oktober 2020	Konsultasi BAB III & IV	10
11	10 Oktober 2020	Konsultasi Keagamaan	11
12	02 November 2020	ACC Keagamaan	12
13	17 Oktober 2020	ACC Keseluruhan	13

Malang, 18 Desember 2020
Mengtahui,
Ketua Jurusan Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001