MODIFIKASI CAESAR HILL CIPHER DENGAN BILANGAN BINER DAN MATRIKS SIRKULER PADA KEAMANAN TEKS DATA

SKRIPSI

OLEH
M.A. HARISMA EXCEL SP
NIM. 17610103

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

MODIFIKASI CAESAR HILL CIPHER DENGAN BILANGAN BINER DAN MATRIKS SIRKULER PADA KEAMANAN TEKS DATA

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
M.A. Harisma Excel SP
NIM. 17610103

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

MODIFIKASI CAESAR HILL CIPHER
DENGAN BILANGAN BINER DAN MATRIKS SIRKULER
PADA KEAMANAN TEKS DATA

SKRIPSI

OLEH
M.A. HARISMA EXCEL SP
NIM. 17610103

Telah diperiksa dan disetujui untuk diuji
Tanggal 11 Juni 2021

Pembimbing I	Pembimbing II
Prof.Dr. H. Turmudi,M.Si.Ph.D	Muhammad Khudzaifah,M.Si.
NIP. 195710051982031006	NIDT. 19900511201608011057

Mengetahui,
Ketua Program Studi Matematika

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

MODIFIKASI CAESAR HILL CIPHER
DENGAN BILANGAN BINER DAN MATRIKS SIRKULER
PADA KEAMANAN TEKS DATA

SKRIPSI

Oleh
M.A. Harisma Excel SP
NIM. 17610103

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 15 Desember 2021

Penguji Utama	: Juhari, M.Si	.....
Ketua Penguji	: Evawati Alisah, M.Pd	.....
Sekretaris Penguji	: Prof. Dr. H. Turmudi, M.Si, Ph.D	.....
Anggota Penguji	: Muhammad Khudzaifah,M.Si	.....

Mengetahui,
Ketua Program Studi Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : M.A. Harisma Excel SP

NIM : 17610103

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Modifikasi Caesar Hill Cipher Dengan Bilangan Biner dan Matriks Sirkuler pada Keamanan Teks Data

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

Malang,15 Desember 2021

Yang membuat pernyataan,

M.A. Harisma Excel SP

NIM. 17610103

MOTO

“Kegagalan terjadi bila kita menyerah” (Lessing, Philosof German)

“dan barangsiapa yang berjihad, maka sesungguhnya jihadnya itu adalah untuk dirinya sendiri. Sesungguhnya Allah benar-benar Maha Kaya (tidak memerlukan sesuatu) dari semesta alam” (QS. Al-Ankabut/29:06)

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:
Ibu Uswatun Hasanah dan ayah Rokimin yang kata-katanya selalu memberikan semangat yang berarti bagi penulis dan keluarga penulis yang telah memberikan do'a dan semangat kepada penulis.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah SWT atas rahmat, taufik serta hidayah-Nya, sehingga penulis dapat menyelesaikan penyusunan skripsi ini sebagai syarat untuk memperoleh gelar pada bidang matematika di Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.Ucapan terima kasih yang sebesar-besarnya penulis sampaikan kepada semua pihak yang telah memberikan bimbingan dan arahan terutama kepada:

1. Prof. Dr. H. M. Zainuddin, MA, 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. Dr. Elly Susanti, M.Sc, selaku ketua Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Prof. Dr. H. Turmudi, M.Si., Ph.D, selaku dosen pembimbing I yang telah memberikan nasihat, dan arahan kepada penulis.
5. Muhammad Khudzaifah,M.Si, selaku pembimbing II yang telah memberikan arahan dan ilmunya kepada penulis.
6. Ayah dan Ibu yang selalu memberikan doa, semangat, serta motivasi kepada penulis sampai saat ini.

Semoga Allah SWT melimpahkan seluruh rahmat-Nya kepada kita semua skripsi ini bermanfaat bagi peniliti dan pagi pembaca dan mudah-mudahan skripsi ini dapat bermanfaat bagi peniliti dan pembaca.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, 14 Desember 2021

Peneliti

DAFTAR ISI

BAB III METODE PENELITIAN

BAB IV HASIL DAN PEMBAHASAN

BAB V PENUTUP

LAMPIRAN

RIWAYAT HIDUP

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

Syahputra, M.A. Harisma Excel. 2021. **Modifikasi *Caesar Hill Cipher* dengan Bilangan Biner dan Matriks Sirkuler untuk Keamanan Teks Data**. Skripsi. Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing (1) : Prof. Dr. H. Turmudi , Pembimbing (2) : M. Khudzaifah M.Si.

Kata Kunci : Modifikasi, Caesar, Hill, Biner, Matriks.

Kriptografi adalah salah satu metode untuk mengamankan data dari serangan pihak yang tidak berhak. Dengan adanya serangan kriptografi menyebabkan munculnya pihak lain selain pemilik asli data yang dapat menyalahgunakan data tersebut. Oleh karena itu, perlu dipastikan bahwa setiap data yang ada di suatu sistem aman dan terlindungi dari pihak yang tidak bertanggungjawab.Pada penelitian ini dibahas mengenai proses modifikasi Caesar Cipher dan Hill Cipher dengan bilangan biner dan matriks sirkuler untuk keamanan teks data. Sehingga diharapkan teks data tersebut dapat diamankan dari penggunaan ilegal oleh pihak yang tidak bertanggungjawab.

Tujuan dari penelitian ini adalah untuk mengetahui modifikasi algoritma Caesar Cipher dan Hill Cipher untuk mengamankan teks data. Hasil yang didapat dari penelitian ini adalah suatu algoritma kriptografi baru dari proses modifikasi algortima kriptografi Caesar Cipher dan Hill Cipher yang dapat diterapkan untuk mengamankan suatu data yang berbentuk teks. Dengan menerapkan modifikasi Caesar Cipher dan Hill Cipher pada suatu plainteks, diperoleh cipherteks yang berbeda dari cipherteks dari Caesar Cipher dan Hill Cipher sebelum dimodifikasi. Perbedaan Caesar Cipher dan Hill Cipher terletak pada modifikasinya dengan bilangan biner dan matriks sirkuler. Sehingga cipherteks yang didapat dari proses enkripsi modifikasi Caesar Hill Cipher menjadi lebih rumit dan lebih susah dipecahkan oleh kriptanalis.

ABSTRACT

Syahputra, M.A. Harisma Excel. 2021. **Caesar Hill Cipher Modification with Binary and Circulant Matrix for Data Text Security**. Thesis Department of Mathematics, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University . Advisor : (1) : Prof. Dr. H. Turmudi , Advisor (2) : M. Khudzaifah M.Si.

Kata Kunci : Modification, Caesar, Hill, Binary, Matrix.

Cryptography is one method to secure data from attacks by unauthorized parties. Cryptographic attacks cause the emergence of parties other than the owner of the data who can misuse the data. Therefore, it is necessary to ensure that every data in a system is safe and protected from irresponsible parties. This study discusses the modification process of Caesar Cipher and Hill Cipher with binary numbers and circular matrices for text data security. So it is hoped that the text of the data can be secured from illegal use by irresponsible parties.

The purpose of this study is to determine the modification of the Caesar Cipher and Hill Cipher algorithms to secure data text. The results obtained from this study are a new cryptographic algorithm from the modification process of the Caesar Cipher and Hill Cipher cryptographic algorithms that can be applied to secure data in the form of text. By applying the modification of Caesar Cipher and Hill Cipher on a plaintext, obtained ciphertext that is different from the ciphertext of Caesar Cipher and Hill Cipher before being modified. The difference between Caesar Cipher and Hill Cipher lies in its modification with binary numbers and circular matrices. So that the ciphertext obtained from the modified Caesar Hill Cipher encryption process becomes more complicated for cryptanalysts to crack.

مستخلص البحث

سياح بوترا، م. أ. هاريسما إكسل. ٢٠٢١. **تعديل قيصر هيل شفرة (*Caesar Hill Cipher*) بأرقام ثنائية ومصفوفة دائرية لأمن البيانات النصية**. البحث العلمي. قسم الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف (١): البروفيسور الدكتور الحاج تورمودي، المشرف (٢): محمد خذيفة الماجستير.

الكلمات الرئيسية: تعديل، قيصر، هيل، ثنائية، ومصفوفة.

التشفير (Kriptografi) هو إحدى الطرق لتأمين البيانات من الهجمات التي تشنها جهات غير مصرح لها. مع هجمات التشفير التي تتسبب في ظهور أطراف أخرى غير المالك الأصلي للبيانات الذين يمكنهم إساءة استخدام البيانات. لذلك، من الضروري التأكد من أن كل بيانات في النظام آمنة ومحمية من الأطراف غير المسؤولة. تناقش هذه الدراسة عملية تعديل قيصر الشفرة و هيل الشفرة بأرقام ثنائية ومصفوفة دائرية لأمن البيانات النصية. لذلك من المأمول أن يتم تأمين نص البيانات من الاستخدام غير القانوني من قبل أطراف غير مسؤولة.

كان الغرض من هذه الدراسة هو لمعرفة تعديل خوارزميات قيصر الشفرة و هيل الشفرة لتأمين البيانات النصية. النتائج من هذه الدراسة هو عبارة عن خوارزمية تشفير جديدة من عملية تعديل خوارزميات التشفير قيصر الشفرة و هيل الشفرة التي يمكن تطبيقها لتأمين البيانات في شكل نص. من خلال تطبيق تعديل قيصر الشفرة و هيل الشفرة على نص عادي، تم الحصول على نص مشفر يختلف عن النص المشفر في قيصر الشفرة و هيل الشفرة قبل تعديله. يكمن الاختلاف بين قيصر الشفرة و هيل الشفرة في تعديلها بأرقام ثنائية ومصفوفات دائرية. بحيث يصبح النص المشفر الذي تم الحصول عليه من عملية تشفير قيصر الشفرة و هيل الشفرة المعدلة أكثر تعقيدًا وأصعب على محللي التشفير.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kriptografi adalah salah satu metode untuk mengamankan data dari serangan orang yang tidak berhak. Dengan adanya serangan kriptografi menyebabkan munculnya pihak lain selain pemilik asli data yang dapat menyalahgunakan data tersebut. Oleh karena itu, perlu dipastikan bahwa setiap data yang ada di suatu sistem aman dan terlindungi dari pihak yang tidak bertanggungjawab. Hal ini sesuai dengan konsep amanah yang terdapat dalam Al-Qur'an.

Amanah itu merupakan sifat yang diperintahkan Allah SWT agar dimiliki dan dipelihara oleh kaum muslimin. Amanah itu memenuhi hak-haknya Allah SWT dan hak-haknya hamba Allah SWT. Sebab menjaga amanah adalah perintah Allah SWT yang terdapat dalam Al-Qur'an Surah Al-Anfal ayat 27

Artinya:

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

Salah satu perintah Allah SWT dalam Al-Qur'an Surah Al-Anfal ayat 27 adalah jangan mengkhianati amanah yang diberikan. Amanah yang diberikan dapat berupa data pribadi, dokumen rahasia milik negara, dan lain-lain. Kriptografi adalah salah satu cara yang dapat digunakan untuk mengamankan data tersebut.

Seiring dengan berkembangnya ilmu kriptografi, berbagai jenis serangan kriptografi juga ikut berkembang. Dalam penelitian *Combination of Hill Cipher*

Algorithm and Caesar Cipher Algorithm for Exam Data Security oleh Agung Susilo Yuda Irawan, Nono Heryana, dan Arip Solehudin (Agung Susilo Yuda Irawan, Nono Heryana, Arip Solehudin,2020) Hill Cipher dan Caesar Cipher yang dimodifikasi dengan bilangan biner dan digabungkan. Akan tetapi, kunci enkripsi dan dekripsi algortima kriptografi tersebut hanya ada satu sehingga dapat dengan mudah diingat maupun dipecahkan oleh kriptanalis. Dalam penelitian *A Modified Hill Cipher Based on Circulant Matrices* oleh Adinarayana Reddy K , Vishnuvardhan B , Madhuviswanatham , dan Krishna A. V. N.(Adinarayana Reddy K , Vishnuvardhan B , Madhuviswanatham , Krishna A. V. N.,2012) kunci algoritma Hill Cipher dimodifikasi menjadi kunci publik (*public key*) dan kunci rahasia (*secret key*). Akan tetapi, kunci rahasia dari modifikasi algoritma Hill Cipher dibangun dari kunci publik sehingga mudah dipecahkan oleh kriptanalis apabila kunci publiknya sudah diketahui. Dalam *Improved Classical Cipher for Healthcare Applications* oleh Maya Mohan ,M.K.Kavithadevi ,dan Jeevan Prakash V(Maya Mohan ,M.K.Kavithadevi ,Jeevan Prakash V,2016) algoritma Hill Cipher digunakan untuk mengamankan data fasilitas kesehatan. Akan tetapi, pemodifikasiannya hanya dengan menambahkan angka, tidak hanya alfabet a sampai z, namun angka 1 sampai 0, sehingga proses enkripsinya sama dengan algoritma Hill Cipher sebelum dimodifikasi. Kedua penelitian Hill Cipher menggunakan kunci yang berupa matriks sehingga dapat ditebak algoritma kriptografi yang digunakan yaitu Hill Cipher.

Dengan adanya penelitian-penelitian sebelumnya mengenai modifikasi algoritma kriptografi, algoritma tersebut menjadi lebih susah dipecahkan oleh kriptanalis. Jadi algoritma kriptografi tersebut dapat digunakan untuk

mengamankan suatu sistem. Akan tetapi algoritma kriptografi tersebut haruslah diperbarui untuk mencegah kemungkinan terjadinya serangan-serangan dari pihak yang tidak bertanggungjawab. Oleh karena itu, peneliti tertarik untuk memodifikasi algoritma yang sudah ada untuk menjadikannya lebih efisien dalam menjaga suatu sistem.

Dalam penelitian ini Caesar Cipher dan Hill Cipher dimodifikasi berdasarkan penelitian sebelumnya mengenai modifikasi algortima kriptografi tersebut. Dengan adanya pembaruan algoritma kriptografi, algoritma tersebut menjadi lebih susah dipecahkan oleh kriptanalis. Untuk Caesar Cipher, peneliti merujuk proses modifikasi dari penelitian *Combination of Hill Cipher Algorithm and Caesar Cipher Algorithm for Exam Data Security*. Proses modifikasi tersebut yaitu dengan mengubah plainteks ke dalam bentuk bilangan biner 8-bit, lalu menggeser bilangan biner sebanyak kunci (k) digit. Untuk Hill Cipher, peneliti merujuk pada *A Modified Hill Cipher Based on Circulant Matrices* dan *Improved Classical Cipher for Healthcare Applications*. Proses modifikasi tersebut yaitu dengan menggunakan matriks sirkuler sebagai kunci enkripsi dan menggunakan tidak hanya alfabet a sampai z, namun angka 1 sampai 0 juga digunakan dalam proses enkripsinya. Dengan menggabungkan kedua modifikasi algoritma Caesar Cipher dan Hill Cipher, maka algoritma baru yang akan dihasilkan menjadi lebih sulit dipecahkan oleh kriptanalis karena cipherteks yang dihasilkan akan berupa karakter berbentuk bilangan biner 8-bit dan juga telah melalui proses enkripsi dua kali yaitu Caesar Cipher dan Hill Cipher.

Peneliti memilih untuk memodifikasi algoritma Caesar Cipher dan Hill Cipher karena algoritma tersebut mudah dipahami sehingga untuk

pengembangannya masih terdapat banyak ruang. Dengan menggabungkan kedua modifikasi algoritma tersebut, maka diperoleh suatu algoritma baru yang lebih susah dipecahkan oleh kriptanalis. Sehingga dalam penelitian ini Modifikasi Caesar Hill Cipher dengan Bilangan Biner dan Matriks Sirkuler, dapat diterapkan dalam suatu sistem untuk mengamankan data yang ada.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, dapat diambil rumusan masalah yaitu

1. Bagaimana modifikasi algoritma kriptografi Caesar Cipher dengan bilangan biner?
2. Bagaimana modifikasi algoritma kriptografi Hill Cipher berdasarkan matriks sirkuler?
3. Bagaimana penggabungan modifikasi algoritma Caesar Hill Cipher pada keamanan teks data?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini yaitu

1. Untuk mengetahui modifikasi algoritma kriptografi Caesar Cipher dengan bilangan biner.
2. Untuk mengetahui modifikasi algoritma kriptografi Hill Cipher berdasarkan matriks sirkuler.
3. Untuk mengetahui penggabungan modifikasi algoritma Caesar Cipher dan Hill Cipher untuk mengamankan teks data.

1.4 Manfaat Penelitian

Adapun manfaat dari penelitian modifikasi algoritma kriptografi Caesar Cipher dan Hill Cipher ini adalah

1. Sebagai referensi untuk pemodifikasian algoritma kriptografi Caesar Cipher dan Hill Cipher.
2. Dapat digunakan sebagai acuan dalam meningkatkan keamanan data dalam suatu sistem.

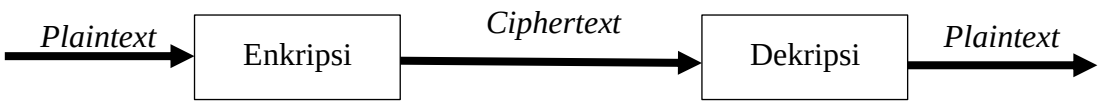
BAB II

TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa yunani yang terdiri dari dua suku kata yaitu kripto dan graphia. Kripto berarti menyembunyikan, sedangkan graphia memiliki arti tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, integritas data, serta autentikasi data.(Riyanto, 2007). Contoh kriptografi dalam kehidupan sehari-hari diantaranya adalah transaksi melalui ATM, pay television, komunikasi dengan telepon selular, *barcode* dan sebagainya. (Munir, 2004).

Fungsi-fungsi mendasar dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan asli (*plaintext*) menjadi suatu pesan dalam bahasa sandi (*ciphertext*). Enkripsi bisa diartikan dengan cipher atau kode, dimana pesan asli (*plaintext*) diubah menjadi kode-kode tersendiri sesuai metode yang disepakati kedua belah pihak, baik pengirim maupun penerima (Prerna et al, 2014). Sedangkan dekripsi adalah proses mengubah pesan dalam suatu bahasa sandi (*ciphertext*) menjadi pesan asli (*plaintext*) kembali. Urutan proses kriptografi dapat dilihat pada Gambar 2.1 berikut :



Gambar 2.1 Urutan Proses Kriptografi (Widyartono, A. 2011).

Sistem kriptografi adalah algoritma, seluruh kemungkinan plaintext, ciphertext dan kunci. P adalah notasi yang digunakan untuk plaintext, C adalah ciphertext, E adalah fungsi enkripsi dan D adalah fungsi dekripsi (Schneier, 1996). Sedangkan untuk kunci dapat dinotasikan sebagai K.

Berdasarkan kunci yang dipakai, algoritma kriptografi dibagi menjadi tiga, yaitu algoritma simetri (menggunakan satu kunci untuk enkripsi dan dekripsi), algoritma asimetri (menggunakan kunci yang berbeda untuk enkripsi dan dekripsi) dan fungsi hash (Ariyus, 2008).

Selain berdasarkan kunci yang dipakai, karakteristik kriptografi juga dibagi berdasarkan tipe operasi yang dipakai untuk enkripsi dan dekripsi serta berdasarkan tipe pengolahan pesan (Sadikin, 2012).

2.1.1 Algoritma Kriptografi

Algoritma kriptografi atau yang sering disebut dengan *cipher* adalah suatu fungsi matematis yang digunakan untuk melakukan *encipher* dan *decipher* (Riyanto, 2007). Secara umum algoritma kriptografi dibagi menjadi 2 jenis yaitu algoritma kunci rahasia dan algoritma kunci publik (Markovski, dkk., 1997). Algoritma kriptografi modern tidak lagi mengandalkan keamanannya pada kerahasiaan algoritma tetapi pada kerahasiaan kunci (Budiono, 2004). *Plaintext* yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan ciphertext yang berbeda pula.

Enkripsi (*encryption*) adalah proses yang dilakukan untuk mengamankan sebuah pesan (disebut *plaintext*) menjadi pesan yang tersembunyi dan tidak dapat dibaca (disebut *ciphertext*). Menurut ISO 7498-2, terminologi yang lebih tepat

digunakan adalah encipher. Dekripsi (*decryption*) adalah proses untuk mengubah *ciphertext* menjadi *plaintext*. Menurut IS) 7498-2, terminology yang tepat untuk proses ini adalah decipher. (S. Aprilia, 2005).

Algoritma kunci rahasia atau biasa disebut algoritma simetris adalah algoritma kriptografi yang menggunakan kunci yang sama untuk proses encipher dan deciphernya. Keamanan algoritma konvensional tergantung pada kunci (Riyanto, 2007). Membocorkan kunci sama artinya dengan memberikan kesempatan bagi pihak tak berwenang untuk melakukan encipher dan decipher pada *plaintext* (Ochodkova, 2001). Algoritma kriptografi yang termasuk dalam algoritma konvensional diantaranya adalah :

1. *Substitution Cipher*

   Substitution cipher adalah algoritma yang mengganti setiap karakter dari *plaintext* dengan karakter lain dalam susunan abjad tanpa adanya perubahan pada susunan abjad asli. Contoh algoritma ini diantaranya *Caesar cipher* dan *vigenere cipher*.

2. *Transposition Cipher*

   Transposition cipher adalah algoritma yang mengubah susunan karakter dari *plaintext* tanpa mengganti karakter yang ada dengan karakter lain. Contoh algoritma ini adalah *rail fence*.

3. *Block Cipher*

   Block cipher adalah algoritma yang membagi karakter pada *plaintext* menjadi blok dengan ukuran tertentu yang mana setiap blok dikodekan dengan menggunakan kunci yang sama. Empat mode operasi yang lazim diterapkan

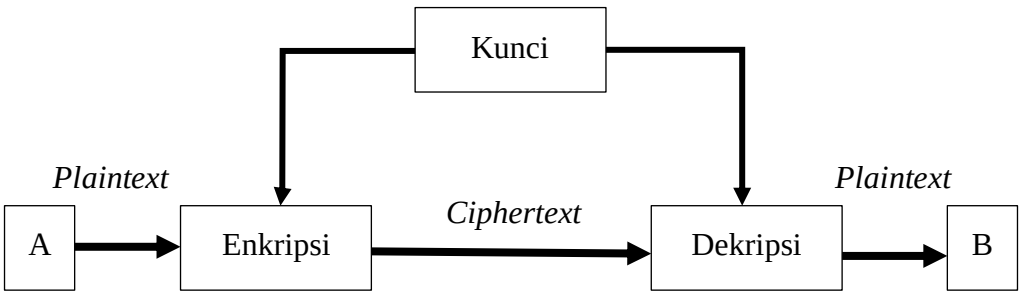
pada algoritma ini adalah *Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFC) dan Output Feedback (OFB).*

4. *Stream Cipher*

Stream cipher adalah algoritma yang mengkodekan karakter persatuan karakter seperti bit, byte, nible, dan sebagainya. Pada tipe pengkodean satu satuan karakter digunakan kunci yang dibangkitkan dari kunci sebelumnya.

2.1.2 Algoritma Simetris

Algoritma simetris adalah algoritma yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya (Kromodimoeljo, 2010). Istilah lain untuk algoritma simetris adalah kriptografi kunci privat (private key cryptography) atau kriptografi konvensional (conventional cryptography). Skema Algoritma Simetri dapat dilihat pada Gambar 2.2

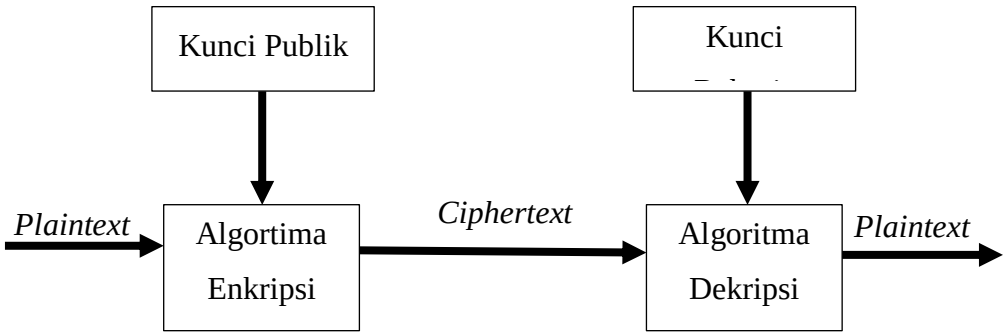


Gambar 2.2 Skema Algoritma Simetris (Halim, A. 2013)

2.1.3 Algoritma Asimetris

Algoritma asimetris disebut juga dengan kriptografi kunci publik karena algoritma ini memiliki kunci yang berbeda untuk enkripsi dan dekripsi, dimana enkripsi menggunakan public key dan untuk dekripsinya menggunakan private key. Public key dan private key harus saling berpasangan secara matematis. Dengan memberikan publickey, pembuat kunci berhak memberikan dan

mendapatkan public key agar pesan aman dan hanya bisa dibaca oleh si pembuat kunci. Dalam kriptografi kunci asimetri, hampirsemua algoritma kriptografinya menggunakan konsep kunci publik, seperti Rivest Shamir-Adleman (RSA), El-Gamal, Rabin dan sebagainya (Harahap, 2014). Skema kriptografi asimetris ditunjukkan secara umum pada Gambar 2.3.



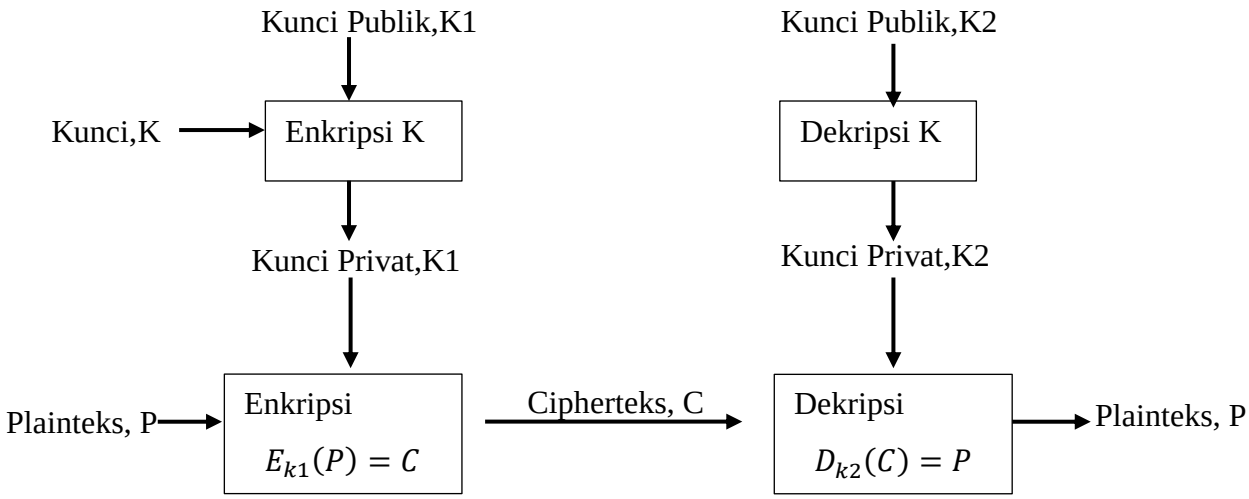
Gambar 2.3 Skema Algoritma Asimetris (Halim, A. 2013)

Kriptografi asimetri ini dapat dianalogikan seperti kotak surat yang terkunci dan memiliki lubang untuk memasukan surat. Setiap orang dapat memasukkan surat ke dalam kotak surat tersebut, tetapi hanya pemilik surat yang memiliki kunci dan yang dapat membuka kotak surat. Kunci publik dapat dikirim ke penerima melalui saluran yang sama dengan saluran yang digunakan untuk mengirim pesan, tidak perlu takut, karena pihak yang tidak berkepentingan tidak akan dapat mendekripsi pesan tersebut, karena tidak memiliki kunci privat.

2.1.4 Algoritma Hybrid

Kriptografi hybrid adalah suatu penggabungan antara kriptografi simetris dan kriptografi asimetris bentuk tulisan rahasia yang memperhatikan keseimbangan dan menggunakan syarat-syarat tertentu yang telah ditetapkan dan juga tetap pada kerahasiaan sampai kepada si penerimaKelebihan kriptografi simetris adalah pada segi kecepatan untuk proses enkripsi dan dekripsi yang

tinggi, namun memiliki kelemahan dalam segi pendistribusian kuncinya. Sedangkan kelebihan kriptografi asimetris adalah kemudahan dalam pertukaran kunci, namun lemah dalam segi kecepatannya. Untuk mengatasi kelemahan masing-masing algoritma kriptografi tersebut, maka dipadukan kedua sistem algoritma kriptografi tersebut. Perpaduan atau penggabungan sistem ini disebut kriptografi hybrid. Skema kriptografi hybrid dapat dilihat pada Gambar 2.4.



Gambar 2.4 Skema Algoritma Hybrid

2.2 *Data Text*

Menurut Inmon (2005) Data adalah sebuah rekaman dari fakta-fakta, konsep-konsep, atau instruksiinstruksi pada media penyimpanan untuk komunikasi perolehan, dan pemrosesan dengan cara otomatis dan presentasi sebagai informasi yang dapat dimengerti oleh manusia. Sedangkan menurut Bernard (2012 : 130) data adalah fakta kasar mengenai orang, tempat, kejadian dan sesuatu yang penting diorganisasikan. Menurut Williams dan Sawyer (2007 : 25) data terdiri dari fakta-fakta dan angka-angka yang diolah menjadi informasi.

Hariyanto (2004) mengatakan, bahwa data merupakan sebuah rekaman dari fakta, konsep, atau instruksi yang harus diproses untuk menjadi sebuah informasi

yang dapat dimengerti oleh manusia. Tempat penyimpanan data bisa di media penyimpanan berupa media komputer yang bisa menyimpan data berupa video, gambar, suara, dan teks. Maka dari itu pengertian data pada era ini dapat diperluas menjadi data berupa fakta, konsep, instruksi, grafik, suara, serta video.Berdasarkan beberapa pengertian diatas, maka dapat ditarik kesimpulan bahwa data adalah fakta ataupun angka yang dapat diolah dan dapat berupa file yang memuat konsep, instruksi, grafik, dan suara.

2.2.1 Keamanan Data

Masalah keamanan dan kerahasiaan data merupakan hal yang sangat sangat penting dalam suatu organisasi maupun untuk pribadi. Keamanan secara umum diartikan sebagai "*quality or state of being secure-to be free from danger*". Keamanan informasi adalah bagaimana kita dapat mencegah penipuan (cheating) atau paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik (Ramadhani A., 2018). Berdasarkan masalah yang terkait dengan keamanan data dalam suatu sistem, Whitman dan Mattord (2011) berpendapat bahwa tinjauan keamanan terbagi menjadi 5 yaitu:

1. *Physical Security* yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
2. *Personal Security* yang overlap dengan „phisycal security' dalam melindungi orang-orang dalam organisasi.

3. *Operation Security* yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
4. *Communications Security* yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.
5. *Network Security* yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

2.2.2 Aspek Keamanan Data

Protection atau perlindungan pada data dilakukan untuk memenuhi aspek keamanan data. Aspek-aspek tersebut perlu diperhatikan, dikontrol dan diterapkan untuk mencapai keamanan data. Whitman dan Mattord (2011) menyebutkan beberapa aspek yang terkait dengan keamanan data, yaitu:

a. *Privacy*

Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi adalah dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. Privacy menjamin keamanan data bagi pemilik informasi dari orang lain.

b. *Identification*

Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali penggunaannya. Identifikasi adalah langkah pertama dalam memperoleh hak

akses ke informasi yang diamankan. Identifikasi umumnya dilakukan dengan penggunaan user name dan user ID. 10

c. *Authentication*

Autentikasi terjadi pada saat sistem dapat membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas yang di klaim.

d. *Authorization*

Setelah identitas pengguna diautentikasi, sebuah proses yang disebut autorisasi memberikan jaminan bahwa pengguna (manusia dan komputer) telah mendapatkan autorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari informasi.

e. *Accountability*

Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktivitas terhadap informasi yang telah dilakukan, dan siapa yang melakukan aktivitas itu.

Menurut (Schneier B., 1996) ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi, yaitu :

1. Kerahasiaan, adalah aspek yang digunakan untuk menjaga isi informasi dari siapapun kecuali orang yang memiliki wewenang untuk mengetahuinya. Terdapat banyak sekali pendekatan yang dapat digunakan untuk merahasiakan data, termasuk membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit dibaca dan dipahami.
2. Integritas data, adalah aspek yang berhubungan untuk penjagaan dari perubahan data secara tidak sah. Untuk menjamin integritas data,seseorang atau sistem harus memiliki kemampuan untuk mendeteksi manipulasi data

oleh pihak-pihak yang tidak memiliki wewenang. Bentuk dari manipulasi data antara lain menyisipkan, menghapus, dan mensubtitusikan data lain kedalam data yang sebenarnya.

3. Auntentikasi, adalah aspek yang berhubungan dengan identifikasi, baik autentifikasi pihak-pihak yang terlibat dalam pengiriman data maupun autentifikasi keaslian data. Kedua pihak yang terlibat dalam komunikasi harus mengenalkan diri satu sama lain. Informasi yang dikirim harus terbukti keasliannya meliputi asal usulnya, tanggal asal, isi informasi, tanggal pengiriman dan sebagainya.
4. Non-repudiation, adalah usaha untuk mencegah terjadinya penyangkalan terhadap tanggung jawab atau tindakan pengiriman suatu informasi, dengan kata lain jika pihak pengirim menyangkal telah mengirim suatu pesan, maka harus bisa dibuktikan bahwa pesan yang dikirim berasal dari pengirim tersebut.

2.3 Pengkodean Data

Data disimpan di dalam komputer pada main memory untuk diproses. Sebuah karakter data disimpan dalam main memory menempati posisi 1 byte. Komputer generasi pertama, 1 byte terdiri dari 4 bit, komputer generasi kedua, 1 byte terdiri dari 6 bit dan komputer generasi sekarang, 1 byte terdiri dari 8 bit. Suatu karakter data yang disimpan di main memory diwakili dengan kombinasi dari digit binary (binary digit atau bit) suatu kode biner dapat digunakan untuk mewakili suatu karakter.

Suatu komputer yang berbeda menggunakan kode biner yang berbeda untuk mewakili suatu karakter. Komputer yang 2 byte terdiri dari 4 bit, menggunakan kode

binari yang berbentuk kombinasi 4 bit, yaitu Binary coded decimal (BCD). Komputer yang menggunakan 6 bit untuk 1 bytenya, menggunakan kode biner yang terdiri dari 6 kombinasi yaitu Standard Binary Coded Decimal (SBCDK). Komputer yang 1 byte terdiri 8 bit, menggunakan kode Decimal Interchange Code (DIC) atau American Standard Code of Information Interchange (ASCII). Berikut merupakan beberapa bentuk kode biner:

1. Binary Coded Decimal (BCD)

   BCD merupakan kode biner yang digunakan hanya untuk mewakili nilai digit desimal saja, yaitu angka 0 samapai dengan 9. BCD menggunakan kombinasi dari 4 bit, sehingga sebanyak 16 (2 pangkat 4 = 16) kemungkinan kombinasi yang dapat diperoleh dan hanya 10 kombinasi yang digunakan. Kode BCD yang orisinil sudah jarang dipergunakan untuk komputer generasi sekarang karena tidak dapat mewakili huruf atau simbol-simbol karakter khusus.

2. Standard Binary Coded Decimal Interchange Code (SBCDIC)

   SBCDIC merupakan kode biner perkembangan dari BCD. BCD dianggap tanggung, karena masih ada 6 kombinasi yang tidak dipergunakan, 6 kombinasi yang tersebut tidak dapat digunakan untuk mewakili karakter yang lainnya. SBCDIC menggunakan kombinasi 6 bit, sehingga lebih banyak kombinasi yang bisa dihasilkan, sebanyak 64 kombinasi kode, yaitu 10 kode untuk digit angka, 26 kode untuk huruf alphabet dan sisanya karakter-karakter khusus yang dipilih. Posisi bit di SBCDIC dibagi menjadi 2 area, yaitu 2 bit pertama disebut dengan alphabet position dan 4 bit berikutnya disebut dengan numeric bit position.

3. Extended Binary Coded Decimal Interchange Code (EBCDIC)

EBCDIC terdiri dari kombinasi 8 bit yang memungkinkan untuk mewakili karakter sebanyak 256 kombinasi karakter. Pada EBCDIC, high order bits atau 4 bit pertama disebut dengan zone bit dan low order bits atau 4 bit kedua disebut dengan numeric bits.

4. American Standard Code For Information Interchange (ASCII) 7 bit

   Kode ASCII yang standar menggunakan kombinasi 7 bit, dengan kombinasi sebanyak 127 dari 128 kemungkinan kombinasi. Kode ASCII 7 bit terdiri dari dua bagian, yaitu control characters dan information characters. Control characters merupakan karakter-karakter yang digunakan untuk mengontrol pengiriman atau transmisi dari data, sedangkan information characters merupakan karakter-karakter yang mewakili data.

5. American Standard Code For Information Interchange (ASCII) 8 bit

   Karakter-karakter grafik yang tidak dapat diwakili oleh ASCII 7 bit, dapat diwakili dengan ASCII 8 bit karena lebih banyak memberikan kombinasi karakter.

2.4 Keterbagian

Keterbagian merupakan salah satu pokok bahasan dari Teori Bilangan yang berkaitan dengan sifat pembagian dalam matematika. Penjelasan mengenai definisi dan teorema yang berkaitan dengan keterbagian telah diberikan oleh banyak buku dengan berbagai bahasa yang berbeda. Berikut beberapa definisi dan teorema yang menjelaskan tentang keterbagian.

Definisi Keterbagian

Untuk setiap $a, b \in \mathbb{Z}$, a dikatakan habis membagi b jika ada k yang memenuhi $a = k.b$, dan dinotasikan $a|b$.

Algoritma Keterbagian

Untuk setiap a, b ada tunggal bilangan q dan r sehingga $b = aq + r$, untuk $0 < r < q$.

Pada teorema tersebut, diketahui bilangan q disebut hasil bagi, bilangan r disebut sisa (residu), dan bilangan r selalu kurang dari a.(Wono Setya Budhi, 2006).

Teorema Keterbagian

Misalkan a, b, c, d, e merupakan bilangan bulat, dan $b, c \neq 0$, berlaku

1. Jika $b|a$ dan $c|b$, maka $c|a$.
2. Jika $b|a$, maka $bc|ac$.
3. Jika $c|d$ dan $c|e$, maka untuk suatu bilangan bulat m dan n, $c|dm + en$.
4. Jika b merupakan pembagi sejati dari a, maka $1 < b < |a|$. (Keng,1982:2)

2.5 Kekongruenan

Gagasan mengenai kongruensi/kekongruenan sering ditemui dan terjadi dalam kehidupan sehari-hari. Contohnya dalam hitungan hari dalam seminggu yang merupakan masalah kongruensi dengan modulus 7.

Definisi Kongruensi

Misalkan k dan m suatu bilangan bulat. Jika $a - b = km$, maka a dan b kongruen modulo m, dan ditulis $a - b \equiv 0 \ (mod\ m)$ atau $a \equiv b (mod\ m)$. Jika a dan b tidak kongruen modulo m dituliskan $a \not\equiv b (mod\ m)$ (Keng,1982:22).

Aritmatika Modular

Ambil a, b, c dan m bilangan bulat, maka:

1. Setiap a disebut kongruen b modulo m jika dan hanya jika ada bilangan a dan b dibagi m memiliki sisa(residu) yang sama.
2. $a \equiv a$. (sifat refleksif)
3. $a \equiv b(mod\ m)$ jika dan hanya jika $b \equiv a$. (sifat simetris)
4. Jika $a \equiv b$ dan $b \equiv c$, maka $a \equiv c$. (sifat transitif)(Julan Hernadi, 2013)

2.6 Caesar Cipher

Dalam dunia penyandian subtitusi kode pertama terjadi pada masa pemerintahan Julius Caesar yang dikenal dengan kode kaisar. Penyandian dilakukan dengan mengganti posisi huruf awal dari alphabet atau disebut juga dengan algoritma ROT3 (Nisak, 2015).

Kemudian pada perkembangannya algoritma kode caesar memberikan suatu gagasan baru untuk menggunakan kunci lain yang disebut *polyalphabetic*. Kunci bisa jadi nama, alamat atau apa saja yang diinginkan oleh pengirim pesan. Caesar Cipher dengan menggunakan satu kunci atau bisa disebut substitusi deret campur kata kunci, yang perlu diingat adalah tidak ada perulangan huruf (Ariyus, 2006:20).

Menurut Egar Dika Santosa (2015) sistematika enkripsi maupun dekripsi dalam Caesar Cipher adalah dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet). Misalnya, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan akjad. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu $k = 3$). Dengan mengkodekan setiap huruf abjad dengan bilangan bulat sebagai berikut: $A = 0, B = 1, \dots, Z = 25$,

maka secara matematis Caesar Chiper menyandikan plainteks p_i menjadi c_i dengan aturan:

$$c_i = E(p_i) = (p_i + k) mod\ 26$$

Dan dekripsi dengan aturan

$$p_i = D(c_i) = (c_i - k) mod\ 26.$$

2.7 Hill Cipher

Hill Cipher adalah algoritma cipher poligrafik berdasarkan transformasi linier dan ditemukan oleh Lester S. Hill pada tahun 1929. Hill Cipher adalah algoritma cipher blok dimana plainteks dibagi menjadi blok berukuran sama. Dalam Hill cipher kuncinya adalah matriks non-singular berukuran $n \times n$ dimana n adalah ukuran blok. Plainteks P dienkripsi sebagai $C = KP\ mod\ m$ dimana C adalah blok cipherteks dan K adalah matriks kunci. Dekripsi dari cipherteks C menghasilkan plainteks dimana $P = K^{-1}C\ mod\ m$.(Lester S. Hill, 1929).

Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas cipherteks saja. Namun, teknik ini bukan berarti tanpa cela, hill cipher dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas cipherteks dan potongan berkas plainteks. Teknik kriptanalisis ini disebut *known-plaintext attack*.

Hill Cipher yang merupakan *polyalphabetic cipher* dapat dikategorikan sebagai *block cipher* karena teks yang akan diproses akan dibagi menjadi blok blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula. (Behrouz Forouzan, 2008).

Dasar dari teknik Hill Cipher adalah aritmatika modulo terhadap matriks. Dalam penerapannya hill cipher menggunakan menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada Hill Cipher adalah matriks n x n dengan n merupakan ukuran blok. Matriks A yang menjadi kunci harus merupakan matriks yang invertible, yaitu memiliki multiplicative invers A^{-1} sehingga: $A.A^{-1} = A^{-1}.A = I$. Kunci harus memiliki invers karena matriks A^{-1} tersebut adalah kunci yang digunakan untuk melakukan dekripsi.

Menurut Egar Dika Santosa (2015) Ide dari Hill cipher adalah dengan mengambil m kombinasi linier dari m karakter alfabet dalam satu elemen *plaintext*, sehingga menghasilkan m alfabet karakter dalam satu elemen *plaintext*. Misalkan $m = 2$, maka dapat ditulis suatu elemen plaintext sebagai $x = (x_1, x_2)$ dan suatu elemen *ciphertext* sebagai $y = (y_1, y_2)$. Di sini, y_1, y_2 adalah kombinasi linier dari x_1 dan x_2.misalkan

$$y_1 = 11x_1 + 3x_2, y_2 = 8x_1 + 7x_2$$

maka dapat ditulis dalam notasi matriks sebagai berikut:

$$(y_1, y_2) = (x_1, x_2)\left[\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}\right]$$

Secara umum, dengan menggunakan matriks K $m \times m$ sebagai kunci. Jika elemen pada baris i dan kolom j dari matriks K adalah ki, j, maka dapat ditulis $K = (ki, j)$.

Untuk $x = (x1, \dots, xm) \in P$ dan $K \in K$, di hitung $y = eK(x) = (y1, \dots, ym)$ sebagai berikut:

$$(y_1, y_2, \dots, y_m) = (x_1, x_2, \dots, x_m)\left[\begin{pmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{pmatrix}\right]$$

Dengan kata lain $y = xK$ .Dikatakan bahwa ciphertext diperoleh dari plaintext dengan cara transformasi linier. Untuk melakukan dekripsi dengan menggunakan matriks invers K^{-1}. Jadi dekripsi dilakukan dengan rumus $x = yK^{-1}$.

2.8 Amanah

Kata amanah diambil dari kata amina yang memiliki arti " merasa aman" dan "percaya". Siapa saja yang dititipi amanat, maka yaitu berarti yang menitipkannya percaya kepadanya dan merasa aman bahwa sesuatu yang dititipkan itu dipelihara dan dijaga olehnya (Quraish Shihab:5, 2005). Semua saja yang berada ditangan manusia adalah sebuah amanat yang harus dilakukan. Seluruh yang ada didalam dunia ini termasuk amanat manusia yang harus dijaga kelestarian lingkungannya. Anak dan keluarga juga merupakan sebagai amanah Allah. Amanat Allah SWT wajib dipelihara dan dikembangkan. Amanat manusia terhadap manusia mencakup banyak hal, bukan hanya harta benda yang dititipkan atau ikatan perjanjian yang disepakati, tetapi termasuk juga rahasia yang dibisikkan. Barang siapa saja yang mendustakan tentang amanah berarti secara tidak langsung kita sudah mengkhianati amanah terhadap diri sendiri, amanah kepada manusia bahkan Amanah kepada Allah SWT. Tidak ada seorangpun yang memiliki akal yang akaan mendustakan amanat yang sudah dibebankan kepada dirinya.

Dalam Al-Qur'an surah An-Nisa' ayat 58 yang artinya:

Sesungguhnya Allah menyuruh kamu menyampaikan amanat-amanat kepada pemiliknya, dan apabila kamu menetapkan hukum diantara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah member pengajaran yang sebaik-baiknya kepada kamu. Sesungguhnya Allah Maha Mendengar lagi Maha Melihat (Q.S An Nisa': 58)

menjelaskan bahwa amanah yang diberikan atau yang diperintahkan Allah harus dilaksanakan kepada ahlinya (pemilik amanah). Oleh sebab itu, siapapun yang diberikan amanah varus dilaksanakan tanpa harus membedakan agama, ras dan budaya (Quraish Shihab:2, 2005).

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian Modifikasi Caesar Hill Cipher dengan Bilangan Biner dan Matriks Sirkuler menggunakan metode studi pustaka, yaitu penelitian yang dilakukan dengan cara mengumpulkan data dan informasi dengan bantuan berbagai macam referensi meliputi buku, catatan, dokumen, dan artikel yang berkaitan dengan pembahasan.

3.2 Definisi Operasional Penelitian

Definisi operasional variabel penelitian menurut Sugiyono (2015, h.38) adalah suatu atribut atau sifat atau nilai dari obyek atau kegiatan yang memiliki variasi tertentu yang telah ditetapkan oleh peneliti untuk dipelajari dan kemudian ditarik kesimpulannya. Dalam penelitian ini, definisi operasional variabelnya adalah sebagai berikut :

1. Kunci publik (k_p)

   Dalam penelitian ini kunci publik berupa matriks arnold dan digunakan pada modifikasi algortima Hill Cipher.

2. Kunci rahasia(k_s)

   Dalam penelitian ini kunci publik berupa matriks sirkuler dan digunakan pada modifikasi algortima Hill Cipher.

3. Matriks baris dari kunci rahasia (v^T)

Dalam penelitian ini matriks baris didapat dari kunci rahasia (k_s) dan digunakan pada modifikasi algortima Hill Cipher.

3.3 Tahapan Penelitian

Hal pertama yang dilakukan dalam penelitian ini adalah menentukan teks yang akan disandikan. Setelah itu, teks tersebut akan diubah menjadi pesan yang berbentuk bilangan biner atau bentuk desimalnya. Kemudian pesan tersebut dienkripsi dan didekripsi menggunakan modifikasi Hill Cipher, modifikasi Caesar cipher, dan gabungan dari modifikasi Hill Cipher dan Caesar Cipher.

3.3.1 Modifikasi Caesar Cipher

Pada penelitian ini langkah-langkah yang dilakukan dalam proses enkripsi dan dekripsi modifikasi Caesar Cipher, yaitu:

1. Menyiapkan plainteks (p) yang akan dienkripsi.
2. Menyiapkan bilangan bulat (k) sebagai kunci enkripsi.
3. Mengubah plainteks (p) ke dalam bentuk bilangan binernya menurut tabel ASCII.
4. Mengeblok sebanyak k digit dari bilangan biner (p_i) dan menggesernya ke depan atau belakang.
5. Mengubah kembali bilangan biner (p_i) ke dalam bentuk karakter atau simbolnya dan diperoleh cipherteks (c) proses enkripsi modifikasi Caesar Cipher.
6. Menyiapkan kunci dekripsi (k) dari kunci enkripsi.
7. Mengubah cipherteks (c) ke dalam bentuk bilangan binernya menurut tabel ASCII.

8. Mengeblok sebanyak k digit dari bilangan biner (c_i) dan menggesernya berlawanan arah dengan proses enkripsi.
9. Mengubah kembali bilangan biner (c_i) ke dalam bentuk karakter atau simbolnya dan diperoleh plainteks (p) proses dekripsi modifikasi Caesar Cipher.

3.3.2 Modifikasi Hill Cipher

Berikut ini langkah-langkah yang diakukan dalam proses enkripsi dan dekripsi modifikasi Hill Cipher:

1. Menyiapkan plainteks yang akan diproses.
2. Mengubah plainteks ke dalam bentuk bilangan desimalnya.
3. Membuat matriks (p) dari bentuk desimal plainteks.
4. Menyiapkan kunci publik (k_p) berupa matriks arnold.
5. Menyiapkan kunci rahasia (k_s) berupa matriks sirkuler prima dari matriks koefisien kunci publik (k_p).
6. Membangun kunci enkripsi dengan mengalikan kunci publik (k_p) dan kunci rahasia (k_s).

$$k = k_p \cdot k_s \cdot k_p^{-1}$$

7. Mengalikan kunci enkripsi (k) dengan matriks plainteks (p_i) dan menjumlahkan dengan transpose matriks baris dari kunci rahasia (v^T).

$$c_i = k \cdot p_i + v_i^T mod\ 256$$

8. Mengubah kembali matriks (c_i) ke dalam bentuk simbolnya dan didapat cipherteks.
9. Mengubah cipherteks ke dalam bentuk bilangan desimalnya.

10. Membuat matriks (c) dari bentuk desimal cipherteks.
11. Menyiapkan kunci dekripsi dari invers kunci enkripsi.

$$k^{-1} = k_p^{-1} \cdot k_s^{-1} \cdot k_p$$

12. Mengalikan kunci dekripsi dengan matriks cipherteks (c_i) yang dikurangi dengan transpose matriks baris dari kunci rahasia (v^T).

$$p_i = k^{-1} \cdot (c_i - v_i^T) mod\ 256$$

13. Mengubah kembali matriks (p_i) ke dalam bentuk simbolnya dan didapat plainteks.

3.3.3 Modifikasi Caesar Cipher dan Hill Cipher

Berikut ini langkah-langkah yang diakukan dalam proses enkripsi dan dekripsi menggunakan modifikasi Caesar Cipher dan Hill Cipher:

1. Proses enkripsi dengan Caesar Cipher yang dimodifikasi dengan bilangan biner 8 bit
   a. Menyiapkan plainteks (p) yang akan dienkripsi.
   b. Menyiapkan bilangan bulat (k) sebagai kunci enkripsi.
   c. Mengubah plainteks (p) ke dalam bentuk bilangan binernya menurut tabel ASCII.
   d. Mengeblok sebanyak k digit dari bilangan biner (p_i) dan menggesernya ke depan atau belakang.
   e. Mengubah kembali bilangan biner (p_i) ke dalam bentuk karakter atau simbolnya dan diperoleh cipherteks1 ($c1$) proses enkripsi modifikasi Caesar Cipher.

2. Proses enkripsi dengan Hill Cipher yang dimodifikasi dengan matriks kunci dan modulonya menggunakan seluruh karakter dari ASCII yaitu terdapat 256 karakter.
   a. Menyiapkan cipherteks1 ($c1$) dari proses enkripsi modifikasi Caesar Cipher.
   b. Mengubah cipherteks1 ($c1$) ke dalam bentuk bilangan desimalnya.
   c. Membuat matriks (p) dari bentuk desimal plainteks.
   d. Menyiapkan kunci publik (k_p) berupa matriks arnold.
   e. Menyiapkan kunci rahasia (k_s) berupa matriks sirkuler prima dari matriks koefisien kunci publik (k_p).
   f. Membangun kunci enkripsi dengan mengalikan kunci publik (k_p) dan kunci rahasia (k_s).

$$k = k_p \cdot k_s \cdot k_p^{-1}$$

   g. Mengalikan kunci enkripsi (k) dengan matriks plainteks (p) dan menambahkannya dengan transpose matriks baris dari kunci rahasia (v^T).

$$c_i = k \cdot p_i + v_i^T mod\ 256$$

   h. Mengubah kembali matriks (c_i) ke dalam bentuk simbolnya dan didapat cipherteks.

3. Proses dekripsi dengan Hill Cipher yang dimodifikasi dengan matriks kunci dan modulo dari seluruh karakter dari ASCII yaitu 256.
   a. Mengubah cipherteks ke dalam bentuk bilangan desimalnya.
   b. Membuat matriks (c) dari bentuk desimal cipherteks.

c. Menyiapkan kunci dekripsi dari invers kunci enkripsi.

$$k^{-1} = k_p^{-1} \cdot k_s^{-1} \cdot k_p$$

d. Mengalikan kunci dekripsi dengan matriks cipherteks (c) yang dikurangi dengan transpose matriks baris dari kunci rahasia (v^T).

$$p_i = k^{-1} \cdot (c_i - v_i^T) mod\ 256$$

e. Mengubah kembali matriks (p_i) ke dalam bentuk simbolnya dan didapat plainteks1 ($p1$) proses dekripsi Hill Cipher.

4. Proses dekripsi dengan Caesar Cipher yang dimodifikasi dengan kode biner ASCII 8 bit.
   a. Mengubah plainteks1 ($p1$) ke dalam bentuk bilangan binernya menurut tabel ASCII.
   b. Menyiapkan kunci dekripsi ($-k$) dari kunci enkripsi modifikasi caesar cipher.
   c. Mengeblok sebanyak k digit dari bilangan biner (c_i) dan menggesernya berlawanan arah dengan proses enkripsi.
   d. Mengubah kembali bilangan biner (c_i) ke dalam bentuk karakter atau simbolnya dan diperoleh plainteks.

BAB IV

HASIL DAN PEMBAHASAN

4. 1 Proses Enkripsi dan Dekripsi Modifikasi Caesar Cipher

Proses enkripsi dan dekripsi modifikasi algoritma Caesar Cipher adalah dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan bentuk bilangan binernya dalam ASCII, lalu urutan(order) dari bilangan biner tersebut digeser sebanyak kunci (k). Dengan mengkodekan setiap karakter dari plainteks menjadi bilangan biner dan kunci (k) yang digunakan berupa bilangan bulat, maka secara matematis proses enkripsi dapat dirumuskan menjadi

$$c_j = E(p) = p_{(i+k)\ mod\ 7}$$

Dan dekripsi dengan aturan

$$p_i = D(c) = c_{(j-k)\ mod\ 7}$$

Akan dibuktikan bahwa cipherteks pada modifikasi algoritma Caesar Cipher akan memenuhi fungsi enkripsi dekripsinya dapat menggunakan teorema keterbagian dan kongruensi. Berikut bukti fungsi enkripsi dekripsi:

$$c = E(p) = p_{(i+k)\ mod\ 7}$$

Menurut definisi kongruensi, maka

$$7|j-(i+k)$$

$$j-(i+k) = 7 \cdot a$$

$$-j+(i+k) = 7 \cdot (-a)$$

$$i+k-j = 7 \cdot (-a)$$

$$i-(j-k) = 7 \cdot (-a)$$

$$7|i-(j-k)$$

Menurut definisi keterbagian, maka

$$p_i = D(c) = c_{(j-k)\ mod\ 7}$$

Jadi terbukti bahwa cipherteks pada modifikasi algoritma Caesar Cipher memenuhi fungsi enkripsi dekripsinya. Berikut contoh penggunaan algoritma Caesar Cipher dan modifikasi algortima Caesar Cipher:

Misal diberikan Plainteks : MATRIX

Langkah-langkah dalam algortima Caesar Cipher yaitu

1. Proses enkripsi algortima Caesar Cipher:
   a. Ubah Plainteks $P = MATRIX$ menjadi bilangan bulat.

$$M = 12, A = 1, T = 19, R = 17, I = 8, X =.$$

   b. Jumlahkan setiap bilangan plainteks dengan kunci k, misal $k = 3$.

$$c_i = E(p_i) = (p_i + k) mod\ 26$$

$$c_1 = E(12) = (12 + 3) mod\ 26 = 15$$

$$c_2 = E(1) = (1 + 3) mod\ 26 = 4$$

$$c_3 = E(19) = (19 + 3) mod\ 26 = 22$$

$$c_4 = E(17) = (17 + 3) mod\ 26 = 20$$

$$c_5 = E(8) = (8 + 3) mod\ 26 = 11$$

$$c_6 = E(10) = (10 + 3) mod\ 26 = 13.$$

   c. Ubah kembali bilangan yang diperoleh menjadi bentuk alfabetnya dan didapat cipherteks.

$$15 = P, 4 = D, 22 = W, 20 = U, 11 = L,.$$

   d. Maka didapat $C = PDWULNV$ sebagai cipherteks dalam proses enkripsi Caesar Cipher.

2. Proses dekripsi algoritma Caesar Cipher:

   a. Ubah Cipherteks $C = PDWULNV$ menjadi bilangan bulat.

   $$P = 15, D = 4, W = 22, U = 20, L = 11, N = 13, V = 21.$$

   b. Kurangkan setiap bilangan cipherteks dengan kunci $k = 3$.

   $$p_i = D(c_i) = (c_i - k) mod\ 26.$$

   $$p_1 = D(15) = (15 - 3) mod\ 26 = 12$$

   $$p_2 = D(4) = (4 - 3) mod\ 26 = 1$$

   $$p_3 = D(22) = (22 - 3) mod\ 26 = 19$$

   $$p_4 = D(20) = (20 - 3) mod\ 26 = 17$$

   $$p_5 = D(11) = (11 - 3) mod\ 26 = 8$$

   $$p_6 = D(13) = (13 - 3) mod\ 26 = 10$$

   $$p_7 = D(21) = (21 - 3) mod\ 26 = 18$$

   c. Ubah kembali bilangan yang diperoleh menjadi bentuk alfabetnya dan didapat plainteks.

   $$12 = M, 1 = A, 19 = T, 17 = R, 8 = I, 10 = K, 18 = S.$$

   d. Maka didapat $P = MATRIKS$ sebagai plainteks dalam proses dekripsi Caesar Cipher.

Proses modifikasi dari algoritma Caesar Cipher adalah dengan menggunakan bilangan biner dari tabel ASCII dan dengan bilangan bulat (k) sebagai kuncinya.

Misal diberikan sebuah Plainteks : MATRIKS

Langkah-langkah dalam modifikasi Caesar Cipher yaitu:

1. Proses enkripsi modifikasi Caesar Cipher:

a. Ubah Plainteks $P = MATRIKS$ ke bentuk bilangan biner 8 bit.

$$M = 01001101$$

$$A = 01000001$$

$$T = 01010100$$

$$R = 01010010$$

$$I = 01001001$$

$$K = 01001011$$

$$S = 01010011$$

b. Geser bilangan biner (yang diblok merah) tersebut sebanyak kunci K, misal $K = 3$, dan ubah kembali menjadi bentuk simbolnya.

$$M = 01001\,101 \rightarrow 101\,01001 = ©$$

$$A = 01000\,001 \rightarrow 001\,01000 = (\,$$

$$T = 01010\,100 \rightarrow 100\,01010 = \check{S}$$

$$R = 01010\,010 \rightarrow 010\,01010 = J$$

$$I = 01001\,001 \rightarrow 001\,01001 =)$$

$$K = 01001\,011 \rightarrow 011\,01001 = i$$

$$S = 01010\,011 \rightarrow 011\,01010 = j$$

c. Maka didapat $C = ©(\check{S}J)ij$ sebagai cipherteks dalam proses enkripsi modifikasi Caesar Cipher dengan bilangan biner 8 bit

2. Proses dekripsi modifikasi Caesar Cipher:

a. Ubah Cipherteks $C = ©(\check{S}J)ij$ ke bentuk bilangan biner 8 bit

$$© = 10101001$$

$$(= 00101000$$

$$\check{S} = 10001010$$

$$J = 01001010$$

$$) = 00101001$$

$$i = 01101001$$

$$j = 01101010$$

b. Geser bilangan biner (yang diblok merah) tersebut sebanyak kunci dekripsi $K = -3$, dan ubah kembali menjadi bentuk simbolnya.

$$© = 101\ 01001 \rightarrow 01001\ 101 = M$$

$$(= 001\ 01000 \rightarrow 01000\ 001 = A$$

$$\check{S} = 100\ 01010 \rightarrow 01010\ 100 = T$$

$$J = 010\ 01010 \rightarrow 01010\ 010 = R$$

$$) = 001\ 01001 \rightarrow 01001\ 001 = I$$

$$i = 011\ 01001 \rightarrow 01001\ 011 = K$$

$$j = 011\ 01010 \rightarrow 01010\ 011 = S$$

c. Maka didapat $P = MATRIKS$ sebagai plainteks dalam proses dekripsi modifikasi Caesar Cipher dengan bilangan biner 8 bit

Pada tabel 4.1 ditunjukkan perbandingan proses enkripsi dekripsi algoritma Caesar Cipher sebelum dan sesudah dimodifikasi.

Tabel 4.1 Perbandingan Hasil Enkripsi Algoritma Caesar Cipher dan Modifikasi Caesar Cipher

Algoritma Kriptografi	Plainteks	Kunci Enkripsi	Cipherteks	Kunci Dekripsi	Plainteks
Caesar Cipher	$MATRIX$	3	$PDWULNV$	3	$MATRIX$
Modifikasi Caesar Cipher	$MATRIX$	3	$©(\check{S}J)ij$	3	$MATRIX$

4. 2 Proses Enkripsi dan Dekripsi Modifikasi Hill Cipher

Proses enkripsi dan dekripsi modifikasi Hill Cipher adalah dengan menggunakan kunci publik (k_p) berupa matriks arnold $\begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$ dan kunci rahasia (k_s) berupa matriks sirkuler prima dari matriks koefisien kunci publik (v). Dengan mengubah setiap huruf abjad(alfabet) menjadi bilangan bulat, maka secara matematis proses enkripsi dapat dirumuskan menjadi

$$C = k \cdot P \; mod \; 26$$

$$C = (k \cdot P) + v \; mod \; 26$$

Dan dekripsinya menjadi

$$P = k^{-1} \cdot C \; mod \; 26.$$

$$P = k^{-1} \cdot (C - v) \; mod \; 26.$$

Matriks kunci disebut dengan k, maka matriks k adalah sebagai berikut

$$k = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$$

Matriks k yang menjadi kunci ini adalah matriks arnold yang merupakan matriks invertible, yaitu memiliki multiplicative inverse k^{-1} sehingga :

k: Kunci Matriks

k^{-1}: Invers Kunci Matriks

$k \cdot k^{-1} = 1.$

Akan dibuktikan bahwa cipherteks pada modifikasi algoritma Hill Cipher akan memenuhi fungsi enkripsi dekripsinya dengan menggunakan teorema keterbagian dan kongruensi. Berikut bukti fungsi enkripsi dekripsi:

$$p_i = p_1, p_2, \dots, p_n$$

$$p_i = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix}, c_i = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$$

$$k = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ k_{m1} & k_{m2} & \cdots & k_{mn} \end{bmatrix}, v = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$$

$$\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \left(\begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ k_{m1} & k_{m2} & \cdots & k_{mn} \end{bmatrix} \cdot \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix} \right) + \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \; mod\ 26$$

$$\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} k_{11} \cdot p_1 + k_{12} \cdot p_2 + \cdots + k_{1n} \cdot p_n \\ k_{21} \cdot p_1 + k_{22} \cdot p_2 + \cdots + k_{2n} \cdot p_n \\ \vdots \\ k_{n1} \cdot p_1 + k_{n2} \cdot p_2 + \cdots + k_{nn} \cdot p_n \end{bmatrix} + \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} mod\ 26$$

$$\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} (k_{11} \cdot p_1 + k_{12} \cdot p_2 + \cdots + k_{1n} \cdot p_n) + v_1 \\ (k_{21} \cdot p_1 + k_{22} \cdot p_2 + \cdots + k_{2n} \cdot p_n) + v_2 \\ \vdots \\ (k_{n1} \cdot p_1 + k_{n2} \cdot p_2 + \cdots + k_{nn} \cdot p_n) + v_3 \end{bmatrix} mod\ 26$$

$$c_i = (k \cdot p_i) + v\ mod\ 26$$

$$26 \mid c_i \cdot (k \cdot p_i)^{-1} - v$$

$$c_i \cdot (k \cdot p_i)^{-1} - v = 26 \cdot a$$

$$c_i{}^{-1} \cdot c_i \cdot (k \cdot p_i)^{-1} - v + v = c_i{}^{-1} \cdot \big((26 \cdot a) + v\big)$$

$$(k \cdot p_i)^{-1} = c_i{}^{-1} \cdot \big((26 \cdot a) + v\big)$$

$$p_i^{-1} \cdot k^{-1} = c_i{}^{-1} \cdot \big((26 \cdot a) + v\big)$$

$$p_i^{-1} \cdot k^{-1} \cdot k = c_i{}^{-1} \cdot k^{-1} \cdot \big((26 \cdot a) + v\big)$$

$$p_i^{-1} = c_i{}^{-1} \cdot k^{-1} \cdot \big((26 \cdot a) + v\big)$$

$$(p_i^{-1})^{-1} = \Big(c_i{}^{-1} \cdot k \cdot \big((26 \cdot a) + v\big)\Big)^{-1}$$

$$p_i = k^{-1} \cdot c_i \cdot \big((26 \cdot a^{-1}) + v^{-1}\big)$$

$$p_i \cdot (k^{-1} \cdot c_i)^{-1} = (k^{-1} \cdot c_i) \cdot (k^{-1} \cdot c_i)^{-1} \cdot \big((26 \cdot a^{-1}) + v^{-1}\big)$$

$$p_i \cdot (k^{-1} \cdot c_i)^{-1} - v^{-1} = (26 \cdot a^{-1}) + v^{-1} - v^{-1}$$

$$p_i \cdot (k^{-1} \cdot c_i)^{-1} - v^{-1} = 26 \cdot (a^{-1})$$

$$26 \mid p_i \cdot (k^{-1} \cdot c_i)^{-1} - v^{-1}$$

$$p_i = k^{-1} \cdot (c_i - v^{-1}) \; mod \; 26$$

Jadi terbukti bahwa cipherteks pada algoritma Hill Cipher memenuhi fungsi enkripsi dekripsinya. Berikut contoh penggunaan algoritma Hill Cipher dan modifikasi algortima Hill Cipher:

Misal diberikan Plainteks : MATRIKS

Langkah-langkah dalam algortima Hill Cipher yaitu

1. Proses enkripsi algortima Hill Cipher:
   a. Ubah Plainteks $P = MATRIKS$ menjadi bilangan bulat.

   $$M = 12, A = 0, T = 19, R = 17, I = 8, K = 10, S = 18.$$

   b. Buat matriks (P) dari bentuk bilangan bulat plainteks.

   $$p_1 = \begin{bmatrix} 12 \\ 0 \end{bmatrix}$$

   $$p_2 = \begin{bmatrix} 19 \\ 17 \end{bmatrix}$$

   $$p_3 = \begin{bmatrix} 8 \\ 10 \end{bmatrix}$$

   $$p_4 = \begin{bmatrix} 18 \\ 26 \end{bmatrix}$$

   c. Kalikan matriks plainteks (p_i) dengan kunci k, misal $k = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix}$.

   $$C = k \cdot P \; mod \; 27$$

   $$c_1 = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 0 \end{bmatrix} \; mod \; 27 = \begin{bmatrix} 12 \\ 21 \end{bmatrix}$$

   $$c_2 = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 17 \end{bmatrix} \; mod \; 27 = \begin{bmatrix} 16 \\ 0 \end{bmatrix}$$

$$c_3 = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 10 \end{bmatrix} \ mod\ 27 = \begin{bmatrix} 11 \\ 1 \end{bmatrix}$$

$$c_4 = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \cdot \begin{bmatrix} 18 \\ 26 \end{bmatrix} \ mod\ 27 = \begin{bmatrix} 15 \\ 5 \end{bmatrix}$$

d. Ubah kembali matriks (c_i) ke dalam bentuk alfabetnya dan didapat cipherteks.

$$c_1 = \begin{bmatrix} 12 \\ 21 \end{bmatrix} = \begin{bmatrix} M \\ V \end{bmatrix}$$

$$c_2 = \begin{bmatrix} 16 \\ 0 \end{bmatrix} = \begin{bmatrix} Q \\ A \end{bmatrix}$$

$$c_3 = \begin{bmatrix} 11 \\ 1 \end{bmatrix} = \begin{bmatrix} L \\ A \end{bmatrix}$$

$$c_4 = \begin{bmatrix} 15 \\ 5 \end{bmatrix} = \begin{bmatrix} P \\ F \end{bmatrix}$$

e. Maka didapat $C = MVQALAPF$ sebagai cipherteks dalam proses enkripsi Hill Cipher.

2. Proses dekripsi algortima Hill Cipher:

a. Ubah Cipherteks $C = MVQALAPF$ menjadi bilangan bulat.

$M = 12, V = 21, Q = 16, A = 0, L = 11, A = 1, P = 15, F = 5.$

b. Buat matriks (C) dari bentuk bilangan bulat cipherteks.

$$c_1 = \begin{bmatrix} 12 \\ 21 \end{bmatrix}$$

$$c_2 = \begin{bmatrix} 16 \\ 0 \end{bmatrix}$$

$$c_3 = \begin{bmatrix} 11 \\ 1 \end{bmatrix}$$

$$c_4 = \begin{bmatrix} 15 \\ 5 \end{bmatrix}$$

c. Kalikan matriks cipherteks (c_i) dengan kunci dekripsi $k^{-1} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix}$.

$$P = k^{-1} \cdot C \ mod\ 27$$

$$p_1 = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 21 \end{bmatrix} \ mod\ 27 = \begin{bmatrix} 12 \\ 0 \end{bmatrix}$$

$$p_2 = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \cdot \begin{bmatrix} 16 \\ 0 \end{bmatrix} \ mod\ 27 = \begin{bmatrix} 19 \\ 17 \end{bmatrix}$$

$$p_3 = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \cdot \begin{bmatrix} 11 \\ 1 \end{bmatrix} \ mod\ 27 = \begin{bmatrix} 8 \\ 10 \end{bmatrix}$$

$$p_4 = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \cdot \begin{bmatrix} 15 \\ 5 \end{bmatrix} \ mod\ 27 = \begin{bmatrix} 18 \\ 26 \end{bmatrix}$$

d. Ubah kembali matriks (p_i) ke dalam bentuk alfabetnya dan didapat plainteks.

$$c_1 = \begin{bmatrix} 12 \\ 0 \end{bmatrix} = \begin{bmatrix} M \\ A \end{bmatrix}$$

$$c_2 = \begin{bmatrix} 19 \\ 17 \end{bmatrix} = \begin{bmatrix} T \\ R \end{bmatrix}$$

$$c_3 = \begin{bmatrix} 8 \\ 10 \end{bmatrix} = \begin{bmatrix} I \\ K \end{bmatrix}$$

$$c_4 = \begin{bmatrix} 18 \\ 26 \end{bmatrix} = \begin{bmatrix} S \\ \end{bmatrix}$$

e. Maka didapat $P = MATRIKS$ sebagai plainteks dalam proses dekripsi Hill Cipher.

Proses modifikasi dari algoritma Hill Cipher adalah dengan menggunakan matriks arnold sebagai kunci publik dan matriks sirkuler prima sebagai kunci rahasianya.

Misal diberikan sebuah Plainteks : MATRIKS.

Langkah-langkah dalam modifikasi Hill Cipher yaitu:

1. Proses enkripsi modifikasi Hill Cipher:

   a. Ubah Plainteks $P = MATRIKS$ ke bentuk desimalnya.

   $$M = 77, A = 65, T = 84, R = 82, I = 73, K = 75, S = 83$$

   b. Buat matriks (P) dari bentuk desimal plainteks.

   $$P_1 = \begin{bmatrix} M \\ A \end{bmatrix} = \begin{bmatrix} 77 \\ 65 \end{bmatrix}$$

   $$P_2 = \begin{bmatrix} T \\ R \end{bmatrix} = \begin{bmatrix} 84 \\ 82 \end{bmatrix}$$

   $$P_3 = \begin{bmatrix} I \\ K \end{bmatrix} = \begin{bmatrix} 73 \\ 75 \end{bmatrix}$$

   $$P_4 = \begin{bmatrix} S \end{bmatrix} = \begin{bmatrix} 83 \\ 0 \end{bmatrix}$$

   c. Siapkan kunci publik (k_p) berupa matriks arnold $\begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$.

   $$k_p = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix}$$

   d. Siapkan kunci rahasia (k_s) berupa matriks sirkuler prima dari matriks koefisien kunci publik (k_p).

   $$k_p = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix}. k_{pc} = \begin{bmatrix} 1 & 3 & 4 & 13 \\ 3 & 1 & 13 & 4 \\ 4 & 13 & 1 & 3 \\ 13 & 4 & 3 & 1 \end{bmatrix}$$

   $$k_s = \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}$$

   e. Bangun kunci enkripsi dengan mengalikan kunci publik (k_p) dan kunci rahasia (k_s).

   $$K = k_p \cdot k_s \cdot k_p^{-1} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix}^{-1} = \begin{bmatrix} 106 & -24 \\ 449 & -104 \end{bmatrix}$$

f. Kalikan kunci enkripsi (k) dengan matriks plainteks (p) dan jumlahkan dengan transpose matriks baris dari kunci rahasia (v^T).

$$C_i = K \cdot P_i + v_i^T mod\ 256$$

$$C_1 = \begin{bmatrix}106 & -24\\ 449 & -104\end{bmatrix} \cdot \begin{bmatrix}77\\ 65\end{bmatrix} + \begin{bmatrix}1\\ 3\end{bmatrix} mod\ 256 = \begin{bmatrix}203\\ 170\end{bmatrix}$$

$$C_2 = \begin{bmatrix}106 & -24\\ 449 & -104\end{bmatrix} \cdot \begin{bmatrix}84\\ 82\end{bmatrix} + \begin{bmatrix}3\\ 1\end{bmatrix} mod\ 256 = \begin{bmatrix}27\\ 77\end{bmatrix}$$

$$C_3 = \begin{bmatrix}106 & -24\\ 449 & -104\end{bmatrix} \cdot \begin{bmatrix}73\\ 75\end{bmatrix} + \begin{bmatrix}1\\ 3\end{bmatrix} mod\ 256 = \begin{bmatrix}51\\ 110\end{bmatrix}$$

$$C_4 = \begin{bmatrix}106 & -24\\ 449 & -104\end{bmatrix} \cdot \begin{bmatrix}83\\ 0\end{bmatrix} + \begin{bmatrix}3\\ 1\end{bmatrix} mod\ 256 = \begin{bmatrix}97\\ 210\end{bmatrix}$$

g. Ubah kembali matriks (c_i) ke dalam bentuk simbolnya dan didapat cipherteks.

$$C_1 = \begin{bmatrix}203\\ 170\end{bmatrix} = \begin{bmatrix}\ddot{E}\\ \underline{a}\end{bmatrix}$$

$$C_2 = \begin{bmatrix}27\\ 77\end{bmatrix} = \begin{bmatrix}ESC\\ M\end{bmatrix}$$

$$C_3 = \begin{bmatrix}51\\ 110\end{bmatrix} = \begin{bmatrix}3\\ n\end{bmatrix}$$

$$C_4 = \begin{bmatrix}97\\ 210\end{bmatrix} = \begin{bmatrix}a\\ \grave{O}\end{bmatrix}$$

h. Maka didapat $C = \ddot{E}\ \underline{a}\ ESC\ M3na\grave{O}$ sebagai cipherteks dalam proses enkripsi modifikasi Hill Cipher.

2. Proses dekripsi modifikasi Hill Cipher:

a. Ubah Cipherteks $C = \ddot{E}\ \underline{a}\ ESC\ M3na\grave{O}$ ke bentuk desimalnya.

$$\ddot{E} = 203, \underline{a} = 170, ESC = 27, M = 77, 3 = 51, n = 110, a = 97, \grave{O} = 210$$

b. Buat matriks (C) dari bentuk desimal cipherteks.

$$C_1 = \begin{bmatrix} \ddot{E} \\ \underline{a} \end{bmatrix} = \begin{bmatrix} 203 \\ 170 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} ESC \\ M \end{bmatrix} = \begin{bmatrix} 27 \\ 77 \end{bmatrix}$$

$$C_3 = \begin{bmatrix} 3 \\ n \end{bmatrix} = \begin{bmatrix} 51 \\ 110 \end{bmatrix}$$

$$C_4 = \begin{bmatrix} a \\ \grave{O} \end{bmatrix} = \begin{bmatrix} 97 \\ 210 \end{bmatrix}$$

c. Siapkan kunci dekripsi dari invers kunci enkripsi.

$$K^{-1} = \begin{bmatrix} 106 & -24 \\ 449 & -104 \end{bmatrix}^{-1} = \begin{bmatrix} 13 & -3 \\ 57.475 & -13.25 \end{bmatrix}$$

d. Kalikan kunci dekripsi dengan matriks cipherteks (c) yang dikurangi dengan transpose matriks baris dari kunci rahasia (v^T).

$$P_i = k^{-1} \cdot (c_i - v_i^T) mod\ 256$$

$$P_1 = \begin{bmatrix} 13 & -3 \\ 57.475 & -13.25 \end{bmatrix} \cdot \left(\begin{bmatrix} 203 \\ 170 \end{bmatrix} - \begin{bmatrix} 1 \\ 3 \end{bmatrix} \right) mod\ 256 = \begin{bmatrix} 77 \\ 65 \end{bmatrix}$$

$$P_2 = \begin{bmatrix} 13 & -3 \\ 57.475 & -13.25 \end{bmatrix} \cdot \left(\begin{bmatrix} 27 \\ 77 \end{bmatrix} - \begin{bmatrix} 3 \\ 1 \end{bmatrix} \right) mod\ 256 = \begin{bmatrix} 84 \\ 82 \end{bmatrix}$$

$$P_3 = \begin{bmatrix} 13 & -3 \\ 57.475 & -13.25 \end{bmatrix} \cdot \left(\begin{bmatrix} 51 \\ 110 \end{bmatrix} - \begin{bmatrix} 1 \\ 3 \end{bmatrix} \right) mod\ 256 = \begin{bmatrix} 73 \\ 75 \end{bmatrix}$$

$$P_4 = \begin{bmatrix} 13 & -3 \\ 57.475 & -13.25 \end{bmatrix} \cdot \left(\begin{bmatrix} 97 \\ 210 \end{bmatrix} - \begin{bmatrix} 3 \\ 1 \end{bmatrix} \right) mod\ 256 = \begin{bmatrix} 83 \\ 0 \end{bmatrix}$$

e. Mengubah kembali matriks (P_i) ke dalam bentuk simbolnya dan didapat plainteks.

$$P_1 = \begin{bmatrix} 77 \\ 65 \end{bmatrix} = \begin{bmatrix} M \\ A \end{bmatrix}$$

$$P_2 = \begin{bmatrix} 84 \\ 82 \end{bmatrix} = \begin{bmatrix} T \\ R \end{bmatrix}$$

$$P_3 = \begin{bmatrix} 73 \\ 75 \end{bmatrix} = \begin{bmatrix} I \\ K \end{bmatrix}$$

$$P_4 = \begin{bmatrix} 83 \\ 0 \end{bmatrix} = \begin{bmatrix} S \end{bmatrix}$$

f. Maka didapat $P = MATRIKS$ sebagai plainteks dalam proses dekripsi modifikasi Hill Cipher.

Pada tabel 4.2 ditunjukkan perbandingan proses enkripsi dekripsi algoritma Hill Cipher sebelum dan sesudah dimodifikasi.

Tabel 4.2 Perbandingan Hasil Enkripsi Algoritma Hill Cipher dan Modifikasi Hill Cipher

Algoritma Kriptografi	Plainteks	Kunci Enkripsi	Cipherteks	Kunci Dekripsi	Plainteks
Hill Cipher	$MATRIX$	$\begin{bmatrix}1 & 3\\4 & 13\end{bmatrix}$	$MVQALAPF$	$\begin{bmatrix}13 & -3\\-4 & 1\end{bmatrix}$	$MATRIX$
Modifikasi Hill Cipher	$MATRIX$	$k_p = \begin{bmatrix}1 & 3\\4 & 13\end{bmatrix}$ $k_s = \begin{bmatrix}1 & 3\\3 & 1\end{bmatrix}$	$\ddot{E}\ ^{a}\ ESC\ M3$ $naÒ$	$\begin{bmatrix}13 & -3\\57.475 & -13.25\end{bmatrix}$	$MATRIX$

4. 3 Proses Enkripsi dan Dekripsi Modifikasi Caesar Hill Cipher

Proses modifikasi dari metode metode Caesar Cipher dan Hill Cipher adalah dengan menggabungkan modifikasi dari dua modifikasi metode tersebut.

Misal diberikan sebuah Plainteks : MATRIKS

Langkah-langkah dalam modifikasi Caesar Cipher yaitu:

1. Proses enkripsi modifikasi Caesar Cipher:
   a. Ubah Plainteks $P = MATRIKS$ ke bentuk bilangan biner 8 bit.

$$M = 01001101$$

$$A = 01000001$$

$$T = 01010100$$

$$R = 01010010$$

$$I = 01001001$$

$$K = 01001011$$

$$S = 01010011$$

b. Geser bilangan biner (yang diblok merah) tersebut sebanyak kunci K, misal $K = 3$, dan ubah kembali menjadi bentuk simbolnya.

$$M = 01001\,101 \rightarrow 101\,01001 = ©$$

$$A = 01000\,001 \rightarrow 001\,01000 = (\,$$

$$T = 01010\,100 \rightarrow 100\,01010 = \check{S}$$

$$R = 01010\,010 \rightarrow 010\,01010 = J$$

$$I = 01001\,001 \rightarrow 001\,01001 =)$$

$$K = 01001\,011 \rightarrow 011\,01001 = i$$

$$S = 01010\,011 \rightarrow 011\,01010 = j$$

c. Maka didapat $C = ©(\check{S}J)ij$ sebagai cipherteks dalam proses enkripsi modifikasi Caesar Cipher.

2. Proses enkripsi modifikasi Hill Cipher:

a. Ubah Cipherteks dari proses enkripsi modifikasi Caesar Cipher $C = ©(\check{S}J)ij$ ke bentuk desimalnya.

$© = 169, (= 40, \check{S} = 138, J = 74,) = 41, i = 105, j = 106.$

b. Buat matriks (P) dari bentuk desimal cipherteks.

$$P_1 = \begin{bmatrix} © \\ (\end{bmatrix} = \begin{bmatrix} 169 \\ 40 \end{bmatrix}$$

$$P_2 = \begin{bmatrix} \check{S} \\ J \end{bmatrix} = \begin{bmatrix} 138 \\ 74 \end{bmatrix}$$

$$P_3 = \begin{bmatrix}) \\ i \end{bmatrix} = \begin{bmatrix} 41 \\ 105 \end{bmatrix}$$

$$P_4 = \begin{bmatrix} j \end{bmatrix} = \begin{bmatrix} 106 \\ 0 \end{bmatrix}$$

c. Siapkan kunci publik (k_p) berupa matriks arnold $\begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$.

$$k_p = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix}$$

d. Siapkan kunci rahasia (k_s) berupa matriks sirkuler prima dari matriks koefisien kunci publik (k_p).

$$k_p = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix}. k_{pc} = \begin{bmatrix} 1 & 3 & 4 & 13 \\ 3 & 1 & 13 & 4 \\ 4 & 13 & 1 & 3 \\ 13 & 4 & 3 & 1 \end{bmatrix}$$

$$k_s = \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}$$

e. Bangun kunci enkripsi dengan mengalikan kunci publik (k_p) dan kunci rahasia (k_s).

$$K = k_p \cdot k_s \cdot k_p^{-1} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix}^{-1} = \begin{bmatrix} 106 & -24 \\ 449 & -104 \end{bmatrix}$$

f. Kalikan kunci enkripsi (k) dengan matriks plainteks (p) dan jumlahkan dengan transpose matriks baris dari kunci rahasia (v^T).

$$C_i = K \cdot P_i + v_i^T mod\ 256$$

$$C_1 = \begin{bmatrix} 106 & -24 \\ 449 & -104 \end{bmatrix} \cdot \begin{bmatrix} 169 \\ 40 \end{bmatrix} + \begin{bmatrix} 1 \\ 3 \end{bmatrix} mod\ 256 = \begin{bmatrix} 59 \\ 198 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 106 & -24 \\ 449 & -104 \end{bmatrix} \cdot \begin{bmatrix} 138 \\ 74 \end{bmatrix} + \begin{bmatrix} 3 \\ 1 \end{bmatrix} mod\ 256 = \begin{bmatrix} 55 \\ 95 \end{bmatrix}$$

$$C_3 = \begin{bmatrix} 106 & -24 \\ 449 & -104 \end{bmatrix} \cdot \begin{bmatrix} 41 \\ 105 \end{bmatrix} + \begin{bmatrix} 1 \\ 3 \end{bmatrix} mod\ 256 = \begin{bmatrix} 35 \\ 222 \end{bmatrix}$$

$$C_4 = \begin{bmatrix} 106 & -24 \\ 449 & -104 \end{bmatrix} \cdot \begin{bmatrix} 106 \\ 0 \end{bmatrix} + \begin{bmatrix} 3 \\ 1 \end{bmatrix} mod\ 256 = \begin{bmatrix} 231 \\ 15 \end{bmatrix}$$

g. Ubah kembali matriks (c_i) ke dalam bentuk simbolnya dan didapat cipherteks.

$$C_1 = \begin{bmatrix} 59 \\ 198 \end{bmatrix} = \begin{bmatrix} ; \\ Æ \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 55 \\ 95 \end{bmatrix} = \begin{bmatrix} 7 \\ \_ \end{bmatrix}$$

$$C_3 = \begin{bmatrix} 35 \\ 222 \end{bmatrix} = \begin{bmatrix} \# \\ ß \end{bmatrix}$$

$$C_4 = \begin{bmatrix} 231 \\ 15 \end{bmatrix} = \begin{bmatrix} ç \\ \text{SI} \end{bmatrix}$$

h. Maka didapat $C =$; Æ7_#ßçSI sebagai cipherteks dalam proses enkripsi modifikasi Caesar Cipher dan Hill Cipher.

3. Proses dekripsi modifikasi Hill Cipher:

a. Ubah Cipherteks $C =$; Æ7_#ßçSI ke bentuk desimalnya.

$; = 59, Æ = 198, 7 = 55, \_ = 95, \# = 35, ß = 222, ç = 231, \text{SI} = 15.$

b. Buat matriks (C) dari bentuk desimal cipherteks.

$$C_1 = \begin{bmatrix} ; \\ Æ \end{bmatrix} = \begin{bmatrix} 59 \\ 198 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 7 \\ \_ \end{bmatrix} = \begin{bmatrix} 55 \\ 95 \end{bmatrix}$$

$$C_3 = \begin{bmatrix} \# \\ ß \end{bmatrix} = \begin{bmatrix} 35 \\ 222 \end{bmatrix}$$

$$C_4 = \begin{bmatrix} ç \\ \text{SI} \end{bmatrix} = \begin{bmatrix} 231 \\ 15 \end{bmatrix}$$

c. Siapkan kunci dekripsi dari invers kunci enkripsi.

$$K^{-1} = \begin{bmatrix} 106 & -24 \\ 449 & -104 \end{bmatrix}^{-1} = \begin{bmatrix} 13 & -3 \\ 57.475 & -13.25 \end{bmatrix}$$

d. Kalikan kunci dekripsi dengan matriks cipherteks (c) yang dikurangi dengan transpose matriks baris dari kunci rahasia (v^T).

$$P_i = K^{-1} \cdot (C_i - v_i^T) mod\ 256$$

$$P_1 = \begin{bmatrix} 13 & -3 \\ 57.475 & -13.25 \end{bmatrix} \cdot \left(\begin{bmatrix} 59 \\ 198 \end{bmatrix} - \begin{bmatrix} 1 \\ 3 \end{bmatrix} \right) mod\ 256 = \begin{bmatrix} 169 \\ 40 \end{bmatrix}$$

$$P_2 = \begin{bmatrix} 13 & -3 \\ 57.475 & -13.25 \end{bmatrix} \cdot \left(\begin{bmatrix} 55 \\ 95 \end{bmatrix} - \begin{bmatrix} 3 \\ 1 \end{bmatrix} \right) mod\ 256 = \begin{bmatrix} 138 \\ 74 \end{bmatrix}$$

$$P_3 = \begin{bmatrix} 13 & -3 \\ 57.475 & -13.25 \end{bmatrix} \cdot \left(\begin{bmatrix} 35 \\ 222 \end{bmatrix} - \begin{bmatrix} 1 \\ 3 \end{bmatrix} \right) mod\ 256 = \begin{bmatrix} 41 \\ 105 \end{bmatrix}$$

$$P_4 = \begin{bmatrix} 13 & -3 \\ 57.475 & -13.25 \end{bmatrix} \cdot \left(\begin{bmatrix} 231 \\ 15 \end{bmatrix} - \begin{bmatrix} 3 \\ 1 \end{bmatrix} \right) mod\ 256 = \begin{bmatrix} 106 \\ 0 \end{bmatrix}$$

e. Mengubah kembali matriks (P_i) ke dalam bentuk simbolnya dan didapat plainteks.

$$P_1 = \begin{bmatrix} © \\ (\end{bmatrix} = \begin{bmatrix} 169 \\ 40 \end{bmatrix}$$

$$P_2 = \begin{bmatrix} \check{S} \\ J \end{bmatrix} = \begin{bmatrix} 138 \\ 74 \end{bmatrix}$$

$$P_3 = \begin{bmatrix}) \\ i \end{bmatrix} = \begin{bmatrix} 41 \\ 105 \end{bmatrix}$$

$$P_4 = \begin{bmatrix} j \\ \ \end{bmatrix} = \begin{bmatrix} 106 \\ 0 \end{bmatrix}$$

f. Maka didapat $C = ©(\check{S}J)ij$ sebagai plainteks dalam proses dekripsi modifikasi Hill Cipher.

4. Proses dekripsi modifikasi Caesar Cipher:

a. Ubah Cipherteks $C = ©(\check{S}J)ij$ ke bentuk bilangan biner 8 bit

$$© = 10101001$$

$$(= 00101000$$

$$\check{S} = 10001010$$

$$J = 01001010$$

$$) = 00101001$$

$$i = 01101001$$

$$j = 01101010$$

b. Geser bilangan biner (yang diblok merah) tersebut sebanyak kunci dekripsi $K = -3$, dan ubah kembali menjadi bentuk simbolnya.

$$© = 101\ 01001 \rightarrow 01001\ 101 = M$$

$$(= 001\ 01000 \rightarrow 01000\ 001 = A$$

$$\check{S} = 100\ 01010 \rightarrow 01010\ 100 = T$$

$$J = 010\ 01010 \rightarrow 01010\ 010 = R$$

$$) = 001\ 01001 \rightarrow 01001\ 001 = I$$

$$i = 011\ 01001 \rightarrow 01001\ 011 = K$$

$$j = 011\ 01010 \rightarrow 01010\ 011 = S$$

c. Maka didapat $P = MATRIKS$ sebagai plainteks dalam proses dekripsi modifikasi Hill Cipher dan Caesar Cipher.

Berikut tabel perbandingan proses enkripsi dekripsi algoritma Caesar Cipher, Hill Cipher dan modifikasi Caesar Cipher dan Hill Cipher :

Tabel 4.3 Perbandingan Hasil Enkripsi Algoritma Caesar Cipher, Hill Cipher dan Modifikasi Caesar Hill Cipher

Algoritma Kriptografi	Plainteks	Kunci Enkripsi	Cipherteks	Kunci Dekripsi	Plainteks
Caesar Cipher	$MATRIKS$	3	$PDWULNV$	3	$MATRIX$
Hill Cipher	$MATRIX$	$\begin{bmatrix}1 & 3\\4 & 13\end{bmatrix}$	$MVQALAPF$	$\begin{bmatrix}13 & -3\\-4 & 1\end{bmatrix}$	$MATRIX$
Modifikasi Caesar Hill Cipher	$MATRIKS$	$k = 3$ $k_p = \begin{bmatrix}1 & 3\\4 & 13\end{bmatrix}$ $k_s = \begin{bmatrix}1 & 3\\3 & 1\end{bmatrix}$	;Æ7#ßçSI	$\begin{bmatrix}13 & -3\\57.475 & -13.25\end{bmatrix}$	$MATRIX$

4. 4 Bentuk Penerapan Amanah pada Pengamanan Data Text

Tujuan dari kriptografi salah satunya adalah untuk melindungi data dari penyalahgunaan data yang bersifat pribadi oleh pihak yang tidak bertanggungjawab maupun yang tidak berwenang. Seperti yang disebutkan sebelumnya, mengamankan data adalah salah satu cara menjaga amanah yang diberikan. Orang yang tidak bisa menjaga amanah dengan baik termasuk orang kafir dan tergolong munafik. Hal ini terdapat dalam Al-Qur'an Surah Al-Anfal ayat 27 yang menjelaskan bahwa amanah yang diberikan atau yang diperintahkan Allah harus dilaksanakan kepada ahlinya (pemilik amanah). Menjaga kerahasiaan data juga termasuk mengemban amanah yang diberikan dan harus dilaksanakan semaksimal mungkin. Salah satunya adalah dengan mencegah data tersebut disalahgunakan oleh pihak yang tidak bertanggungjawab maupun yang tidak berwenang. Oleh sebab itu, siapapun yang diberikan amanah harus dilaksanakan.

BAB V

PENUTUP

5. 1 Kesimpulan

Berdasarkan rumusan masalah dan pembahasan tersebut, dapat dismpulkan bahwa:

1. Proses modifikasi dari algoritma Caesar Cipher adalah dengan menggunakan bilangan biner dari tabel ASCII dan dengan bilangan bulat (k) sebagai kuncinya. Proses enkripsi pada modifikasi algoritma Caesar Cipher adalah dengan mengeblok sebanyak kunci (k) digit dari bilangan biner plainteks (p_i) dan menggesernya ke depan atau belakang. Sedangkan untuk proses dekripsinya adalah dengan mengeblok sebanyak kunci (k) digit dari bilangan biner cipherteks (c_i) dan menggesernya berlawanan arah dengan proses enkripsinya.
2. Proses modifikasi dari algoritma Hill Cipher adalah dengan menggunakan matriks arnold sebagai kunci publik (k_p) dan matriks sirkuler prima sebagai kunci rahasia (k_s). Proses enkripsi pada modifikasi algoritma Hill Cipher adalah dengan mengalikan kunci enkripsi (k) yang dibangun dari kunci publik (k_p) dan kunci rahasia (k_s) dengan matriks plainteks (p_i) dan menjumlahkan dengan transpose matriks baris dari kunci rahasia (v^T). Sedangkan untuk proses dekripsinya adalah dengan mengalikan kunci dekripsi (k^{-1}) dengan matriks cipherteks (c_i) yang dikurangi transpose matriks baris dari kunci rahasia (v^T).

3. Penggabungan dari dua modifikasi dari algoritma Caesar Cipher dan Hill Cipher adalah sebgai berikut:
    a. Dimulai dengan proses enkripsi dari modifikasi algortima Caesar Cipher dengan kunci (k), bilangan biner plainteks (p_i) digeser sebanyak kunci enkripsi Caesar Cipher (k) digit.
    b. Kemudian cipherteks dari proses enkripsi modifikasi Caesar Cipher dienkripsi oleh modifikasi Hill Cipher yaitu dengan mengalikan kunci enkripsi Hill Cipher (k) yang dibangun dari kunci publik (k_p) dan kunci rahasia (k_s) dengan matriks plainteks (p_i) dan menjumlahkan dengan transpose matriks baris dari kunci rahasia (v^T) dan diperoleh cipherteks dalam proses enkripsi modifikasi Caesar Cipher dan Hill Cipher.
    c. Untuk proses dekripsinya dimulai dengan proses dekripsi modifikasi Hill Cipher yaitu dengan mengalikan kunci dekripsi (k^{-1}) dengan matriks cipherteks (c_i) yang dikurangi transpose matriks baris dari kunci rahasia (v^T).
    d. Selanjutnya plainteks dari proses dekripsi modifikasi Hill Cipher didekripsi oleh modifikasi Caesar Cipher yaitu dengan mengeblok sebanyak kunci dekripsi Caesar Cipher (k) digit dari bilangan biner cipherteks dari (c_i) dan menggesernya berlawanan arah dengan proses enkripsinya dan diperoleh plainteks proses dekripsi modifikasi Caesar Cipher dan Hill Cipher.

5. 2 Saran

Penelitian ini membahas mengenai modifikasi algoritma Caesar Cipher dan Hill Cipher dengan menggunakan bilangan biner dan matriks sirkuler. Pada penelitian selanjutnya disarankan untuk membuat suatu modifikasi algoritma kriptografi dari proses modifikasi seperti menambahkan karakter baru atau menggunakan seluruh karakter ASCII pada proses enkripsi, menggeser atau

mengacak susunan bilangan biner dari plainteks, atau dengan perhitungan matriks yang lainnya. Kunci yang lebih rumit seperti kunci publik dan rahasia yang berbeda atau hanya memakai satu kunci tapi berbentuk suatu karakter dari ASCII yang sulit terbaca juga dapat meningkatkan tingkat keamanan sistem yang akan dilindungi.

DAFTAR PUSTAKA

Agung, A., Heryana, N., & Solehudin, A. .2020. Combination of Hill Cipher Algorithm and Caesar Cipher Algorithm for Exam Data Security. Buana Information Technology and Computer Sciences (BIT and CS), 1(2), 42-45.

Al-Quran Terjemahan. 2015. Departemen Agama RI. Bandung: CV Darus Sunnah.

Aprilia, S. 2005. Pengamanan Data Informasi menggunakan Kriptografi Klasik. *Jurnal Teknologi Informasi DINAMIK Volume X*, (3), pp.160-167.

Ariyus, Dony. 2008. Pengantar Ilmu Kriptografi. Yogyakarta: Penerbit Andi.

Bambang Hariyanto. 2004. Sistem Manajemen Basis Data. Informatika. Bandung.

Bernard, A. S. 2012. An Introduction to Enterprise Architecture. Bloomington: AuthorHouse.

Budiyono, A. 2004. Enkripsi Data Kunci Simetris dengan Algoritma Kriptografi LOKI97. Bandung : Program Studi Magister Teknologi Informasi Institut Teknologi Bandung.

Concise Oxford English dictionary. Oxford [England]: Oxford University Press.

Forouzan, Behrouz. 2008 Cryptography and Network Security. McGraw-Hill.

Golose, P.R. 2006. Perkembangan Cybercrime dan upaya Penanganannya di Indonesia oleh Polri. BULETIN HUKUM PERBANKAN DAN KEBANKSENTRALAN, Agustus 4(2):29-47.

Harahap, A.A. 2014. Implementasi Sistem Keamanan Data Menggunakan Steganografi Teknik Pemetaan Titik Hitam dengan Pencarian Sekuensial dan Rabin Cryptosystem. Skripsi. Universitas Sumatera Utara.

Hasugian, A.H. 2013. Implementasi Algoritma Hill Cipher Dalam Penyandian Data. *Pelita Informatika Budi Darma*, *4*(2), pp.115-122.

Hill, Lester, S. 1929, Cryptography in an Algebraic Alphabet: The American Mathematical Monthly, 36 (6), pp.306-312.

Inmon, William H. 2005. Building Data Warehouse. 3th Edition. Canada: John Wiley & Sons.

Jonaki B Ghosh. 2014. At Right Angles. Azim Premji Foundation. Vol. 3, No. 3, November 2014.

Kasgar, A.K., Dhariwal, M. K., Tantubay, N., & Malviya, H. 2013.A Review Paper of Message Digest 5 (MD5).International Journal of Modern Engineering & Management Research1(4): 29-35.

Keng, Hua Loo. 1982. Introduction to Number Theory. Berlin Heidelberg: Springer-Verlag.

Kromodimoeljo, S. 2010. "Teori dan Aplikasi Kriptografi". SPK IT Consulting.

Markovski,S., D.Glikoroski, dan S. Andonova. 1997. Using Quasigroups for Oneone Secure Encoding. Proceeding of VII-th Confrence for Logic and Computing-LIRA'97 page 1-6.

Mohan, M., Kavithadevi, M. K., & Prakash, V. J. 2016. Improved Classical Cipher for Healthcare Applications. Procedia Computer Science, 93, 742-750.

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

Nisak, Khoirun .2015., Penyandian kriptografi metode Hill Cipher dan Caesar Cipher dengan menggunakan appinventor.Undergraduate thesis, Universitas Islam Negeri Maulana Malik Ibrahim.

Ochodkova, E. dan V.Snasel. 2001. Using Quasigroups for Secure Encoding of File Sistem. Proceedings of The Confrence for Security and Protection of Information Page 175-181.

P. Parmar and N. Jindal. 2014. Image Security with Integrated Watermarking and Encryption 1 1 2, vol. 9, no. 3, pp. 24-29.

R. Sadikin, 2012, "Kriptografi Untuk Keamanan Jaringan", Andi, Yogyakarta.

Ramadhani, A., 2018. Keamanan Informasi. *Nusantara Journal of Information and Library Studies (N-JILS), 1*(1), pp.39-51.

Reddy, K. A., Vishnuvardhan, B., & Krishna, A. V. N. 2012. A modified hill cipher based on circulant matrices. Procedia Technology, 4, 114-118.

Rifki Sadikin. 2012. "Kriptografi untuk Keamanan Jaringan". Yogyakarta. Andi.

Riyanto, M. Z. 2007. Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Elgamal atas Group Pergandaan Zp*. Skripsi. Yogyakarta: Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Gadjah Mada Yogyakarta.

Santosa, E.D. 2015. Implementasi Algoritma Caesar Cipher dan Hill Cipher Pada Database Sistem Inventori TB Mita Jepara. *Dok. Karya Ilm. Progr. Stud. Tek. Inform. Univ. Dian Nuswantoro. Semarang*.

Schneier, Bruce. 1996. Applied Cryptography, Second Edition, John Wiley & Son, New York.

Shihab, M.Q., 2005. *Logika agama: Kedudukan wahyu & batas-batas akal dalam Islam*. Lentera Hati.

Sugiyono. 2015. Metode Penelitian Kombinasi (Mix Methods). Bandung: Alfabeta.

Widyartono, Agustinus, 2011, Algoritma Elagamal Untuk Enkripsi Data Menggunakan GNUPG, Jurnal Teknologi dan Informatika Vol.1 No.1 Januari 2011.

William dan Sawyer. 2007.Using Information Technologi.Yogyakarta:Andi

William J Buchanan. 2021. *Hill's Cipher*, Asecuritysite, from https://asecuritysite.com/Coding/hill

Witman, M. E., Mattord, H. J., 2011. Principles of Information security, 4th Edition. Atlanta: Cengage Learning.

LAMPIRAN

Lampiran 1. Tabel ASCII

DEC	BIN	Symbol	Description
0	00000000	NUL	Null char
1	00000001	SOH	Start of Heading
2	00000010	STX	Start of Text
3	00000011	ETX	End of Text
4	00000100	EOT	End of Transmission
5	00000101	ENQ	Enquiry
6	00000110	ACK	Acknowledgment
7	00000111	BEL	Bell
8	00001000	BS	Back Space
9	00001001	HT	Horizontal Tab
10	00001010	LF	Line Feed
11	00001011	VT	Vertical Tab
12	00001100	FF	Form Feed
13	00001101	CR	Carriage Return
14	00001110	SO	Shift Out / X-On
15	00001111	SI	Shift In / X-Off
16	00010000	DLE	Data Line Escape
17	00010001	DC1	Device Control 1 (oft. XON)
18	00010010	DC2	Device Control 2
19	00010011	DC3	Device Control 3 (oft. XOFF)
20	00010100	DC4	Device Control 4
21	00010101	NAK	Negative Acknowledgement
22	00010110	SYN	Synchronous Idle
23	00010111	ETB	End of Transmit Block
24	00011000	CAN	Cancel
25	00011001	EM	End of Medium
26	00011010	SUB	Substitute
27	00011011	ESC	Escape
28	00011100	FS	File Separator
29	00011101	GS	Group Separator
30	00011110	RS	Record Separator
31	00011111	US	Unit Separator
32	00100000		Space

DEC	BIN	Symbol	Description
33	00100001	!	Exclamation mark
34	00100010	"	Double quotes (or speech marks)
35	00100011	#	Number
36	00100100	$	Dollar
37	00100101	%	Per cent sign
38	00100110	&	Ampersand
39	00100111	'	Single quote
40	00101000	(	Open parenthesis (or open bracket)
41	00101001	)	Close parenthesis (or close bracket)
42	00101010	*	Asterisk
43	00101011	+	Plus
44	00101100	,	Comma
45	00101101	-	Hyphen
46	00101110	.	Period, dot or full stop
47	00101111	/	Slash or divide
48	00110000	0	Zero
49	00110001	1	One
50	00110010	2	Two
51	00110011	3	Three
52	00110100	4	Four
53	00110101	5	Five
54	00110110	6	Six
55	00110111	7	Seven
56	00111000	8	Eight
57	00111001	9	Nine
58	00111010	:	Colon
59	00111011	;	Semicolon
60	00111100	<	Less than (or open angled bracket)
61	00111101	=	Equals
62	00111110	>	Greater than (or close angled bracket)
63	00111111	?	Question mark
64	01000000	@	At symbol
65	01000001	A	Uppercase A
66	01000010	B	Uppercase B
67	01000011	C	Uppercase C

DEC	BIN	Symbol	Description
68	01000100	D	Uppercase D
69	01000101	E	Uppercase E
70	01000110	F	Uppercase F
71	01000111	G	Uppercase G
72	01001000	H	Uppercase H
73	01001001	I	Uppercase I
74	01001010	J	Uppercase J
75	01001011	K	Uppercase K
76	01001100	L	Uppercase L
77	01001101	M	Uppercase M
78	01001110	N	Uppercase N
79	01001111	O	Uppercase O
80	01010000	P	Uppercase P
81	01010001	Q	Uppercase Q
82	01010010	R	Uppercase R
83	01010011	S	Uppercase S
84	01010100	T	Uppercase T
85	01010101	U	Uppercase U
86	01010110	V	Uppercase V
87	01010111	W	Uppercase W
88	01011000	X	Uppercase X
89	01011001	Y	Uppercase Y
90	01011010	Z	Uppercase Z
91	01011011	[	Opening bracket
92	01011100	\	Backslash
93	01011101	]	Closing bracket
94	01011110	^	Caret - circumflex
95	01011111	_	Underscore
96	01100000	`	Grave accent
97	01100001	a	Lowercase a
98	01100010	b	Lowercase b
99	01100011	c	Lowercase c
100	01100100	d	Lowercase d
101	01100101	e	Lowercase e
102	01100110	f	Lowercase f

DEC	BIN	Symbol	Description
103	01100111	g	Lowercase g
104	01101000	h	Lowercase h
105	01101001	i	Lowercase i
106	01101010	j	Lowercase j
107	01101011	k	Lowercase k
108	01101100	l	Lowercase l
109	01101101	m	Lowercase m
110	01101110	n	Lowercase n
111	01101111	o	Lowercase o
112	01110000	p	Lowercase p
113	01110001	q	Lowercase q
114	01110010	r	Lowercase r
115	01110011	s	Lowercase s
116	01110100	t	Lowercase t
117	01110101	u	Lowercase u
118	01110110	v	Lowercase v
119	01110111	w	Lowercase w
120	01111000	x	Lowercase x
121	01111001	y	Lowercase y
122	01111010	z	Lowercase z
123	01111011	{	Opening brace
124	01111100	|	Vertical bar
125	01111101	}	Closing brace
126	01111110	~	Equivalency sign - tilde
127	01111111		Delete
128	10000000	€	Euro sign
129	10000001		
130	10000010	‚	Single low-9 quotation mark
131	10000011	ƒ	Latin small letter f with hook
132	10000100	„	Double low-9 quotation mark
133	10000101	…	Horizontal ellipsis
134	10000110	†	Dagger
135	10000111	‡	Double dagger
136	10001000	ˆ	Modifier letter circumflex accent
137	10001001	‰	Per mille sign

DEC	BIN	Symbol	Description
138	10001010	Š	Latin capital letter S with caron
139	10001011	‹	Single left-pointing angle quotation
140	10001100	Œ	Latin capital ligature OE
141	10001101		
142	10001110	Ž	Latin capital letter Z with caron
143	10001111		
144	10010000		
145	10010001	‘	Left single quotation mark
146	10010010	’	Right single quotation mark
147	10010011	“	Left double quotation mark
148	10010100	”	Right double quotation mark
149	10010101	•	Bullet
150	10010110	–	En dash
151	10010111	—	Em dash
152	10011000	˜	Small tilde
153	10011001	™	Trade mark sign
154	10011010	š	Latin small letter S with caron
155	10011011	›	Single right-pointing angle quotation mark
156	10011100	œ	Latin small ligature oe
157	10011101		
158	10011110	ž	Latin small letter z with caron
159	10011111	Ÿ	Latin capital letter Y with diaeresis
160	10100000		Non-breaking space
161	10100001	¡	Inverted exclamation mark
162	10100010	¢	Cent sign
163	10100011	£	Pound sign
164	10100100	¤	Currency sign
165	10100101	¥	Yen sign
166	10100110	¦	Pipe, Broken vertical bar
167	10100111	§	Section sign
168	10101000	¨	Spacing diaeresis - umlaut
169	10101001	©	Copyright sign
170	10101010	ª	Feminine ordinal indicator
171	10101011	«	Left double angle quotes
172	10101100	¬	Not sign

DEC	BIN	Symbol	Description
173	10101101		Soft hyphen
174	10101110	®	Registered trade mark sign
175	10101111	¯	Spacing macron - overline
176	10110000	°	Degree sign
177	10110001	±	Plus-or-minus sign
178	10110010	²	Superscript two - squared
179	10110011	³	Superscript three - cubed
180	10110100	´	Acute accent - spacing acute
181	10110101	µ	Micro sign
182	10110110	¶	Pilcrow sign - paragraph sign
183	10110111	·	Middle dot - Georgian comma
184	10111000	¸	Spacing cedilla
185	10111001	¹	Superscript one
186	10111010	º	Masculine ordinal indicator
187	10111011	»	Right double angle quotes
188	10111100	¼	Fraction one quarter
189	10111101	½	Fraction one half
190	10111110	¾	Fraction three quarters
191	10111111	¿	Inverted question mark
192	11000000	À	Latin capital letter A with grave
193	11000001	Á	Latin capital letter A with acute
194	11000010	Â	Latin capital letter A with circumflex
195	11000011	Ã	Latin capital letter A with tilde
196	11000100	Ä	Latin capital letter A with diaeresis
197	11000101	Å	Latin capital letter A with ring above
198	11000110	Æ	Latin capital letter AE
199	11000111	Ç	Latin capital letter C with cedilla
200	11001000	È	Latin capital letter E with grave
201	11001001	É	Latin capital letter E with acute
202	11001010	Ê	Latin capital letter E with circumflex
203	11001011	Ë	Latin capital letter E with diaeresis
204	11001100	Ì	Latin capital letter I with grave
205	11001101	Í	Latin capital letter I with acute
206	11001110	Î	Latin capital letter I with circumflex
207	11001111	Ï	Latin capital letter I with diaeresis

DEC	BIN	Symbol	Description
208	11010000	Đ	Latin capital letter ETH
209	11010001	Ñ	Latin capital letter N with tilde
210	11010010	Ò	Latin capital letter O with grave
211	11010011	Ó	Latin capital letter O with acute
212	11010100	Ô	Latin capital letter O with circumflex
213	11010101	Õ	Latin capital letter O with tilde
214	11010110	Ö	Latin capital letter O with diaeresis
215	11010111	×	Multiplication sign
216	11011000	Ø	Latin capital letter O with slash
217	11011001	Ù	Latin capital letter U with grave
218	11011010	Ú	Latin capital letter U with acute
219	11011011	Û	Latin capital letter U with circumflex
220	11011100	Ü	Latin capital letter U with diaeresis
221	11011101	Ý	Latin capital letter Y with acute
222	11011110	Þ	Latin capital letter THORN
223	11011111	ß	Latin small letter sharp s - ess-zed
224	11100000	à	Latin small letter a with grave
225	11100001	á	Latin small letter a with acute
226	11100010	â	Latin small letter a with circumflex
227	11100011	ã	Latin small letter a with tilde
228	11100100	ä	Latin small letter a with diaeresis
229	11100101	å	Latin small letter a with ring above
230	11100110	æ	Latin small letter ae
231	11100111	ç	Latin small letter c with cedilla
232	11101000	è	Latin small letter e with grave
233	11101001	é	Latin small letter e with acute
234	11101010	ê	Latin small letter e with circumflex
235	11101011	ë	Latin small letter e with diaeresis
236	11101100	ì	Latin small letter i with grave
237	11101101	í	Latin small letter i with acute
238	11101110	î	Latin small letter i with circumflex
239	11101111	ï	Latin small letter i with diaeresis
240	11110000	ð	Latin small letter eth
241	11110001	ñ	Latin small letter n with tilde
242	11110010	ò	Latin small letter o with grave

DEC	BIN	Symbol	Description
243	11110011	ó	Latin small letter o with acute
244	11110100	ô	Latin small letter o with circumflex
245	11110101	õ	Latin small letter o with tilde
246	11110110	ö	Latin small letter o with diaeresis
247	11110111	÷	Division sign
248	11111000	ø	Latin small letter o with slash
249	11111001	ù	Latin small letter u with grave
250	11111010	ú	Latin small letter u with acute
251	11111011	û	Latin small letter u with circumflex
252	11111100	ü	Latin small letter u with diaeresis
253	11111101	ý	Latin small letter y with acute
254	11111110	þ	Latin small letter thorn
255	11111111	ÿ	Latin small letter y with diaeresis

Lampiran 2. Tabel Konversi Caesar Cipher

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Letter	R	S	T	U	V	W	X	Y	Z
Number	17	18	19	20	21	22	23	24	25

Lampiran 3. Tabel Konversi Hill Cipher

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Letter	R	S	T	U	V	W	X	Y	Z
Number	17	18	19	20	21	22	23	24	25

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	#
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

William J Buchanan (2021), *Hill's Cipher*, Asecuritysite, from https://asecuritysite.com/Coding/hill

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25
.	**_**	**?**										
26	27	28										

Jonaki B Ghosh, 2014, At Right Angles, Azim Premji Foundation, Vol. 3, No. 3, November 2014

RIWAYAT HIDUP

Muhammad Agus Harisma Excel SyahPutra lahir di Banyuwangi pada tanggal 14 Agustus 1999. Memiliki nama panggilan Excel. Alamatnya berada di Dusun Talun RT/RW: 04/08 Desa Gambiran, Kecamatan Gambiran, Kabupaten Banyuwangi. Merupakan anak pertama dari Bapak Rokimin dan Ibu Uswatun Hasanah.

Pendidikan yang pernah ditempuh yaitu TK Khadijah 14, Tegalpare, Muncar. Kemudian melanjutkan sekolahnya di SDN 01 Genteng dan lulus pada tahun 2011. Menempuh pendidikan SMP di Sekolah Menengah Pertama Negeri 01 Genteng lulus pada tahun 2014. Melanjutkan pendidikan SMA di Sekolah Menengah Atas Negeri 01 Genteng lulus pada tahun 2017.

Tahun 2017 melanjutkan studi ke jenjang pendidikan strata 1 di Universitas Islam Negeri Maulana Malik Ibrahim Malang menempuh Program Studi Matematika, Fakultas Sains dan Teknologi. Aktif mengikuti kegiatan akademis dan organisasi yang ada di dalam kampus, seperti mengikuti organisasi HMJ sebagai Pengurus Divisi PNJ HMJ "Integral" Matematika UIN Malang (2018-2019), mengikuti PIONIR-IX cabang karya inovatif (2019), dan ICGT-XI sebagai presenter (2021).

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

BUKTI KONSULTASI SKRIPSI

Nama : M.A. Harisma Excel SP
NIM : 17610103
Fakultas/Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Modifikasi Caesar Hill Cipher Dengan Bilangan Biner dan Matriks Sirkuler pada Keamanan Teks Data
Pembimbing I : Prof. Dr. H. Turmudi, M.Si., Ph.D
Pembimbing II : Muhammad Khudzaifah,M.Si

No	Tanggal	Hal	Tanda Tangan
1	12 Februari 2021	Konfirmasi untuk Pembimbingan dan konsultasi proposal skripsi	1.
2	9 Maret 2021	Konfirmasi untuk Pembimbingan dan konsultasi proposal skripsi	2.
3	22 Maret 2021	Konsultasi Bab I,II, dan III	3.
4	30 Maret 2021	Revisi Bab I dan III	4.
5	6 April 2021	Konsultasi Kajian Keagamaan, konsultasi Bab IV, dan revisi Bab III	5.
6	14 April 2021	Revisi Bab I, Bab II, Bab III dan konsultasi Bab IV	6.
7	16 April 2021	Revisi Kajian Keagamaan pada Bab I	7.
8	22 April 2021	Revisi format kepenulisan Bab III dan Bab IV	8.
9	27 April 2021	Revisi format kepenulisan Bab III, dan Bab IV	9.
10	7 Mei 2021	Acc untuk ujian seminar proposal	10.
11	7 Mei 2021	Acc untuk ujian seminar proposal	11.

12	12 Juni 2021	Revisi Bab I, Bab II, Bab III dan konsultasi Bab IV	12.
13	15 Juni 2021	Revisi Bab I, Bab II, Bab III dan konsultasi Bab IV	13.
14	18 Juni 2021	Konsultasi Kajian Keagamaan & Kepenulisan pada Bab II	14.
15	5 Juli 2021	Revisi untuk format kepenulisan, revisi Bab V	15.
16	6 Agustus 2021	Acc dosen pembimbing skripsi	16.
17	13 Desember 2021	Revisi Keseluruhan	17.
18	15 Desember 2021	ACC Keseluruhan	18
19	15 Desember 2021	ACC Keseluruhan	19.

Malang, 15 Desember 2021
Mengetahui,
Ketua Program Studi Matematika

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