APLIKASI MATRIKS DAN ARITMATIKA MODULAR UNTUK PENYANDIAN MENGGUNAKAN METODE *HILL CIPHER* DAN *CAESAR CIPHER*

SKRIPSI

UIN SUNAN AMPEL
S U R A B A Y A

Disusun Oleh:

ARINATUL KHOIRIYAH

NIM: H92214024

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN AMPEL

SURABAYA

2019

LEMBAR PERSETUJUAN PEMBIMBING

Skripsi oleh

NAMA : ARINATUL KHOIRIYAH

NIM : H92214024

JUDUL : APLIKASI MATRIKS DAN ARITMATIKA MODULAR UNTUK PENYANDIAN MENGGUNAKAN *METODE HILL* CIPHER DAN *CAESAR CIPHER*

Ini telah diperiksa dan disetujui untuk diujikan.

Surabaya, 27 Desember 2019

Dosen Pembimbing 1	Dosen Pembimbing 2
Aris Fanani,M.Kom	Dr.Moh.Hafiyusholeh,M.Si,M.P.Mat
NIP. 198701272014031002	NIP. 198002042014031001

PENGESAHAN TIM PENGUJI

Skripsi Oleh

Nama : Arinatul Khoiriyah

NIM : H92214024

Judul : Aplikasi Matriks dan Aritmatika Modular untuk Penyandian Menggunakan Metode *Hill Cipher* dan *Caesar Cipher*.

Telah dipertahankan di depan tim penguji skripsi

Pada hari Selasa Tanggal 31 Desember 2019

Mengesahkan,
Tim Penguji

Penguji I

Arris Fanani, M.Kom
NIP. 198701272014031002

Penguji II

Dr.Moh.Hafiyusholeh,M.Si,M.P.Mat
NIP. 198002042014031001

Penguji III

Nurissaidah Ulinnuha,M.Kom
NIP. 199011022014032004

Penguji IV

Wika Dianita Utami,M.Sc
NIP. 199206102018012003

Mengetahui,
Dekan Fakultas Sains dan Teknologi
UIN Sunan Ampel Surabaya

Dr.Hj. Eni Purwati, M.Ag
NIP. 196512211990022001

PERNYATAAN KEASLIAN

Saya yang bertanda tangan dibawah ini,

Nama : Arinatul Khoiriyah

NIM : H92214024

Program Studi : Matematika

Angkatan : 2014

Manyatakan bahwa saya tidak melakukan plagiat dalam penulisan skripsi saya yang berjudul: "APLIKASI MATRIKS DAN ARITMATIKA MODULAR UNTUK PENYANDIAN MENGGUNAKAN METODE HILL CIPHER DAN CAESAR CIPHER". Apabila nanti saya terbukti melakukan plagiat, maka saya bersedia menerima sanksi yang telah di tetapkan.

Demikian pernyataan keaslian ini saya buat dengan sebenar-benarnya.

Surabaya, Desember 2019

Yang menyatakan,

METERAI TEMPEL

959F0AFF409835116

6000

ENAM RIBU RUPIAH

(Arinatul Khoiriyah)

NIM. H92214024

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA
PERPUSTAKAAN
Jl. Jend. A. Yani 117 Surabaya 60237 Telp. 031-8431972 Fax.031-8413300
E-Mail: perpus@uinsby.ac.id

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika UIN Sunan Ampel Surabaya, yang bertanda tangan di bawah ini, saya:

Nama : ARINATUL KHOIRIYAH
NIM : H92214024
Fakultas/Jurusan : SAINTEK/MATEMTKA
E-mail address : arina.khoiriya@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Perpustakaan UIN Sunan Ampel Surabaya, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah :
☑ Sekripsi ☐ Tesis ☐ Desertasi ☐ Lain-lain (.....)
yang berjudul :
APLIKASI MATRIKS DAN ARITMATIKA MODULAR UNTUK PENYANDIAN MENGGUNAKAN METODE *HILL CIPHER* DAN *CAESAR CIPHER*

beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Ekslusif ini Perpustakaan UIN Sunan Ampel Surabaya berhak menyimpan, mengalih-media/format-kan, mengelolanya dalam bentuk pangkalan data (database), mendistribusikannya, dan menampilkan/mempublikasikannya di Internet atau media lain secara ***fulltext*** untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan UIN Sunan Ampel Surabaya, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini yang saya buat dengan sebenarnya.

Surabaya, Januari 2020

Penulis

(Arinatul Khoiriyah)

ABSTRAK

APLIKASI MATRIKS DAN ARITMATIKA MODULAR UNTUK PENYANDIAN MENGGUNAKAN METODE *HILL CIPHER* DAN *CAESAR CIPHER*

Berkembangnya teknologi informasi saat ini memudahkan manusia untuk saling bertukar informasi satu sama lain sehingga keamanan dari informasi juga rawan terjadi penyadapan. Informasi atau data dibagi menjadi dua jenis yaitu data yang bersifat rahasia dan data yang bersifat tidak rahasia. Untuk data yang bersifat rahasia tentu akan sangat dijaga kerahasiaannya agar tidak semua orang dapat mengetahui data tersebut. Data disini bisa berupa pesan. Untuk menjaga sebuah pesan rahasia agar tidak mudah diketahui yaitu dengan cara melakukan penyandian terhadap pesan tersebut. Penyandian adalah proses pengubahan pesan menjadi bentuk kode-kode tertentu agar tidak mudah dibaca oleh orang yang tidak mengetahui kuncinya. Cabang ilmu matematika yang mempelajari tentang penyandian disebut kriptografi. Dalam penelitian ini akan dilakukan penyandian dengan mengaplikasikan konsep-konsep matematika dalam hal ini adalah matriks dan aritmatika modular. Metode kriptografi yang digunakan dalam penelitian ini adalah metode hill cipher dan caesar cipher. Konsep matriks dan aritmatika modular digunakan untuk melakukan proses enkripsi dan dekripsi terhadap sebuah pesan rahasia. Dalam penelitian ini metode hill cipher dan caesar cipher berhasil meakukan proses enkripsi dan dekripsi.

Kata Kunci: enkripsi, dekripsi, hill cipher, caesar cipher.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

ABSTRACT

APPLICATION OF MODULAR MATRIX AND ARITHMATICS FOR ADMINISTRATION USINGMETHODS *HILL CIPHER* AND *CAESAR CIPHER*

The development of information technology today makes it easy for humans to exchange information with each other so that the security of information is also prone to eavesdropping. Information or data is divided into two types, namely confidential data and non-confidential data. Confidentiality of confidential data will certainly be maintained so that not everyone can find out the data. Data here can be in the form of messages. To protect a secret message so that it is not easily known by encoding the message. Encoding is the process of converting a message into a form of certain codes so that they are not easily read by people who do not know the key. The branch of mathematics that studies encoding is called cryptography. In this study coding will be done by applying mathematical concepts in this case are matrix and modular arithmetic. The cryptographic method used in this study is the hill cipher and caesar cipher method. The concept of matrix and modular arithmetic is used to process the encryption and decryption of a secret message. In this research the hill cipher and caesar cipher method succeeded in doing the encryption and decryption process.

Keywords: encryption, decryption, hill cipher, caesar cipher.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

DAFTAR ISI

Halaman Judul..... ii

Lembar Persetujuan Pembimbing iii

Lembar Pengesahan iv

Pernyataan Keaslian..... v

Motto..... vi

Halaman Persembahan..... vii

Kata Pengantar..... viii

Abstrak..... x

Abstract..... xi

Daftar Isi..... xii

BAB I PENDAHULUAN..... 1

1.1 Latar Belakang..... 1

1.2 Rumusan Masalah..... 4

1.3 Tujuan Penelitian..... 4

1.4 Manfaat Penelitin..... 4

1.5 Batasan Penelitian..... 5

1.6 Sistematika Penulisan..... 5

BAB II KAJIAN PUSTAKA..... 7

2.1 Kriptografi.....7

2.1.1 Sejarah Kriptografi.....7

2.1.2 Defnisi Kriptografi.....8

2.1.3 Tujuan Kriptografi.....9

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

2.1.4 Komponen Kriptografi.....10

2.2 Hill Cipher..... 12

2.3 Caesar Cipher..... 14

2.4 Matriks..... 17

2.4.1 Definisi Matriks..... 18

2.4.2 Operasi Matriks 18

2.4.3 Invers Matriks..... 19

2.4.4 Transpose Matriks..... 20

2.5 Aritmatika Modular..... 21

2.5.1 Aritmatika Modular dan Sandi Bergeser..... 22

2.5 Integrasi Keislaman..... 23

BAB III METODE PENELITIAN..... 25

3.1 Jenis Penelitian..... 25

3.2 Data dan Sumber Data..... 25

3.3 Pengolahan Data..... 25

BAB IV PEMBAHASAN..... 28

4.1 Proses Enkripsi dan Dekripsi Hill Cipher..... 28

4.2 Proses Enkripsi dan Dekripsi Caesar Cipher..... 34

4.3 Proses Enkripsi dan Dekripsi Gabungan Hill Cipher dan Caesar Cipher..... 40

BAB V PENUTUP..... 47

5.1 Kesimpulan..... 47

5.2 Saran..... 48

Daftar Pustaka..... 49

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Semakin berkembangnya teknologi informasi saat ini memudahkan manusia untuk saling berkomunikasi dengan dunia luar. Hal ini semakin mempermudah manusia untuk saling bertukar data ataupun informasi satu sama lain. Semakin mudahnya pertukaran informasi ini sehingga keamanan dari data yang dikirimkan ke orang lain menjadi rawan terjadi penyadapan.

Dalam melakukan komunikasi data dibagi menjadi dua jenis, yaitu data yang bersifat rahasia dan data yang bersifat tidak rahasia. Data yang bersifat rahasia akan sangat dijaga dan diperhatikan agar tidak mudah bagi orang lain untuk menggandakannya. Sedangkan data yang bersifat tidak rahasia akan kurang diperhatikan sehingga sangat mudah bagi orang lain untuk menggandakannya.

Pada saat mengirimkan pesan yang bersifat rahasia kepada orang lain, tentu semua orang menginginkan agar pesan yang dikirimkan tersebut aman dari orang-orang yang tidak berkepentingan dan tidak bertanggung jawab. Oleh karena itu, diperlukan suatu teknik untuk menyandikan pesan tersebut agar tetap aman. Seperti halnya didalam pramuka, untuk melakukan permainan dengan sebuah misi rahasia maka petunjuk-petunjuk yang diberikan tidak menggunakan bahasa sehari-hari melainkan menggunakan bahasa sandi, seperti sandi morse, sandi cacing, sandi rumput, dan sebagainya. Hal tersebut dimaksudkan agar petunjuk-petujuk tersebut tidak mudah untuk dipecahkan

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

kecuali oleh orang-orang yang mengetahui dan memahami kunci dari sandi tersebut.

Namun sandi-sandi dalam pramuka kurang efektif untuk menjaga kerahasiaan suatu pesan rahasia, karena cukup mudah untuk dipecahkan dan banyak orang yang mengetahuinya. Untuk itu dalam ilmu matematika terdapat pembelajaran mengenai matriks dan aritmatika modular yang terapannya dapat digunakan untuk penyandian. Ilmu yang mempelajari tentang penyandian disebut kriptografi. Dalam kriptografi terdapat beberapa algoritma yang berfungsi untuk mengamankan pesan, salah duanya adalah *hill cipher* dan *caesar cipher*.

Ada beberapa penelitian pengenai penyandian yang sebelumnya pernah dilakukan, seperti penelitian yang dilakukan Muhammad Fadhlan dan Hardiansa (2017) dengan judul Rekayasa Aplikasi Kriptografi dengan Penerapan Kombinasi Algoritma Knapsack Merkle dan Affine Cipher. Dalam penelitian ini peneliti mengkombinasikan metode Affine Cipher dan Knapsack Merkle Heliman untuk melakukan enkripsi dan dekripsi data teks. Affine cipher merupakan pengembangan dari caesar cipher. Affine cipher merupakan suatu sistem yang mengenkripsi huruf plainteks secara matematis dengan menggunakan perkalian dikombinasikan dengan penambahan, modulo m, dimana m adalah bulat dalam membuat subtitusi campuran. Data akan dienkripsi terlebih dahulu menggunakan affine cipher, kemudian hasilnya akan dienkripsi lagi menggunakan merkle hellman. Pada tahap dekripsi data akan didekripsi menggunakan merkle hellman kemudian didekripsi lagi menggunakan affine cipher. Pengkombinasian ini dilakukan untuk

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

menyulitkan dan memperkecil kemungkinan pihak-pihak yang tidak berkepentingan untuk mengetahui data rahasia tersebut sehingga lebih memperkuat keamanan sebuah data rahasia.

Muhammad Hilman Adiwibawa, Rini Marwati dan Ririn Sispiyati (2018) melakukan penelitian dengan judul pengimplementasian modifikasi kriptografi Hill Cipher dengan Matriks Sirkulan. Dalam penelitian ini peneliti menggunakan metode kriptografi yang menggunakan matriks sirkulan untuk membangkitkan matriks kunci publik dan pemilihan kunci privat, sehingga kunci yang simetris berubah menjadi kunci asimetris. Kemudian dibuat program aplikasi kriptografi agar pengguna lebih mudah dalam menggunakan modifikasi kripstografi tersebut.

Aida Halimatusadiah dan Entik Insanudin (2016) melakukan penelitian dengan judul Implementasi Kriptografi Metode Caesar Cipher pada Chating Berbasis Web. Niken Prima Puspita dan Nurdin Bahtiar (2010) melakukan penelitian dengan judul Kriptografi Hill Cipher dengan Menggunakan Operasi Matriks.

Metode Hill Cipher dan Caesar Cipher termasuk dalam Algoritma Kriptografi Klasik. Peneliti memilih algoritma tersebut karena untuk mengetahui konsep-konsep kriptografi yang menggunkan aplikasi matriks dan aritmatika modular.

Berdasarkan latar belakang tersebut maka dalam penelitian ini peneliti akan melakukan penyandian dan penguraian sandi dengan menggunakan matriks dan aritmatika modular dengan mengambil judul “APLIKASI

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

MATRIKS DAN ARITMATIKA MODULAR UNTUK PENYANDIAN MENGGUNAKAN METODE *HILL CIPHER* DAN *CAESAR CIPHER*"

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang yang telah dipaparkan tersebut maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana enkripsi dan deskripsi *hill cipher* menggunakan matriks dan aritmatika modular?
2. Bagaimana enkripsi dan deskripsi *caesar cipher* menggunakan matriks dan aritmatika modular?
3. Bagaimana enkripsi dan deskripsi gabungan *hill cipher* dan *caesar cipher* menggunakan matriks dan aritmatika modular?

1.3 TUJUAN PENELITIAN

Berdasarkan rumusan masalah penelitian tersebut maka tujuan penelitian ini adalah sebagai berikut:

1. Untuk mengetahui bagaimana enkripsi dan dekripsi *hill cipher* menggunakan matriks dan aritmatika modular.
2. Untuk mengetahui bagaimana enkripsi dan deskripsi *caesar cipher* menggunakan matriks dan aritmatika modular.
3. Untuk mengetahui bagaimana enkripsi dan deskripsi *hill cipher* dan *caesar cipher* menggunakan matriks dan aritmatika modular.

1.4 MANFAAT PENELITIAN

Hasil dari penelitian ini diharapkan mampu memberikan beberapa manfaat sebagai berikut:

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

1. Dapat menambah wawasan peneliti tentang penyandian dalam kriptografi khususnya metode hill cipher dan caesar chiper.
2. Dapat digunakan sebagai bahan perbandingan ataupun referensi mengenai terapan matriks dan aritmatika modular dalam penyandian untuk penelitian selanjutnya.

1.5 BATASAN MASALAH

Permasalahan yang dibahas dalam penelitian ini supaya tidak meluas maka dalam penelitian ini diberikan batasan masalah yaitu: Pada metode Hill Cipher hanya akan membahas hasil yang menggunakan matriks 3 x 3. Karena dalam metode hill cipher ukuran matriks yang digunakan adalah n x n.

1.6 SISTEMATIKA PENULISAN

Dalam proposal penelitian ini sitematika penulisannya terdiri dari tiga bab dan masing-masing bab terdapat beberapa subbab dengan rumusan sebagai berikut:

1. BAB I Pendahuluan, dalam pendahuluan ini berisi tentang latar belakang penelitian, rumusan masalah penelitian, tujuan penelitian, manfaat penelitian, batasan masalah dalam penelitian, dan sitematika penulisan.
2. BAB II Kajian Teori, berisi tentang teori-teori yang digunakan dalam penelitian ini, yaitu kriptografi, metode hill cipher, metode caesar chiper, matriks, aritmatika modular.
3. BAB III Metode Penelitian, berisi tentang alur jalannya penelitian antara lain, jenis penelitian, data yang digunakan, tahapan-tahapan dalam penelitian, tahapan-tahapan mengenai metode hill cipher dan caesar cipher.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

4. BAB IV Pembahasan, berisi tentang proses enkripsi dan dekripsi menggunakan hill cipher, caesar cipher, dan gabungan hill cipher dan caesar cipher.
5. BAB V Penutup, berisi tentang kesimpulan dari hasil dan pembahasan serta saran.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB II

KAJIAN PUSTAKA

2.1 KRIPTOGRAFI

2.1.1 Sejarah Kriptografi

Sejarah Kriptografi tertua dapat ditemukan pada peradaban mesir kuno sekitar tahun 3000 SM. Bangsa mesir kuno menggunakan ukiran rahasia yang disebut dengan *heiroglyhpics* untuk menyampaikan pesan kepada orang-orang yang berhak. Pada tahun 400 SM tentara sparta di Yunani menggunakan cipher transposisi dengan alat yang disebut *scytale* yaitu sebuah kertas panjang dari daun *papyrus* yang diilitkan pada sebuah silinder. Selain itu raja Yunani kuno bernama Julius Caesar tercatat paling awal menggunaka *subtitution cipher* yaitu dengan mengganti setiap karakter dalam alfabet dengan karakter yang terletak pada tiga posisi berikutnya.

Pada abad abad ke-17 Ratu Skotlandia yaitu Queen Mary yang merupakan seorang korban hukuman pancung setelah ditemukan surat rahasia miliknya di balik penjara yaitu surat terenkripsi yang berisi tentang rencana pembunuhan terhadap Ratu Elizabeth I.

Pada abad ke-15 Leon Battista Alberti menemukan Kode Roda (*Wheel Cipher*) yang terdiri dari dua potong silendris, yaitu silendris dalam dan silendris luar yang disebut *cipher disk*. Masing-masing silendris memiliki seluruh label alphabet dengan susunan yang tidak harus terurut dan sama.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Pada abad ke-20 kriptografi banyak digunakan kalangan militer. Pada perang dunia II, Nazi Jerman membuat mesin enkripsi bernama *enigma* yang menggunakan beberapa rotor (roda berputar) dan melakukan enkripsi yang sangat rumit. Mesin *enigma* yang digunakan Nazi Jerman dapat mengenkripsi satu pesan dengan 15 milyar kemungkinan. *Enigma* merupakan kriptografi berbasis *rotor* yang dibangun dan dipatenkan oleh beberapa penemu dari beberapa negara yang berbeda sejak tahun 1917 hingga 1921, antara lain Edward Hung Heben (Amerika), Arthur Scherbius (Jerman), Alexander Koch (Belanda) dan Arvid Gehard Damm (Swedia).

Pada tahun 1976 dimana Whitfield Diffie dan Martin Hellman mempublikasikan tesis berjudul *New Direction in Cryptography* yang memperkenalka konsep kunci publik kriptografi yang revolisioner dan metode baru dalam pertukaran kunci, yaitu keamanan berdasarkan algoritma diskrit. Selanjutnya pada tahun 1978 Rivest, Shamir, dan Adlean menemukan enkripsi kunci publik pertama yang dikenal sebagai RSA (*Rivest, Shamir, and Adleman*) (Nurdin A. P., 2017).

2.1.2 Definisi Kriptografi

Kriptografi berasal dari berasal dari Bahasa Yunani "*cryptos*" artinya "*secret*" (rahasia) dan "*graphein*" artinya "*writing*" (tulisan). Jadi kriptografi berarti tulisan rahasia. Terdapat beberapa definisi kriptografi. Pada era 80-an ada yang menyatakan bahwa kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan. Sedangkan dalam buku-buku terbaru menyatakan bahwa kriptografi adalah ilmu mengenai metode untuk mengirimkan pesan secara

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

rahasia sehingga hanya penerima yang dimaksud yang dapat membaca, memahami dan menghapus pesan tersebut (Munir, Bahan Kuliah IF4020 Kriptografi, 2018).

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

Selain itu ada yang menyatakan bahwa kriptografi adalah ilmu yang mepelajari teknik-teknik matematis yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentikasi data. Kriptografi tidak hanya memberikan keamanan informasi saja, namun lebih ke arah teknik-tekniknya (Komputer, 2010).

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

2.1.3 Tujuan Kriptografi

Terdapat empat tujuan mendsar dalam kriptografi, yaitu:

1. Kerahasiaan

   Kriptografi dimaksudkan untuk memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan data atau informasi dengan teknik enkripsi.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

2. Integritas data

   Kriptografi dimaksudkan untuk memberikan jaminan bahwa setiap bagian dari informasi tidak mengalami perubahan dari saat dibuat atau dikirim hingga saat informasi tersebut dibuka.

3. Penyangkalan

   Memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang bila ia mencoba menyangkal telah memiliki dokumen tersebut.

4. Autentikasi

   Kriptografi memberikan dua bentuk layanan, pertama adalah mengidentifikasi keaslian suatu pesan dan memberikan jaminan keotentikannya, dan kedua adalah untuk menguji identitas seseorang apabila ia akan memasuki sebuah sistem.

   (Nisak, 2015)

2.1.4 Komponen Kriptografi

Pada dasarnya kriptografi terdiri dari beberapa komponen berikut:

1. *Enkripsi*

   Enkripsi merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya. Pesan asli diubah menjadi kode-kode yang tidak dimengerti. *Enkripsi* bisa diartikan sebagai *cipher* atau kode. Untuk mengubah teks biasa ke bentuk teks kode dapat kita gunakan algoritma yang mengodekan data yang diinginkan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

2. *Dekripsi*

   Dekripsi merupakan kebalikan dari enkripsi. Pesan yand telah dienkripsi dikemalikan kebentuk aslinya. Algoritma yaang digunakan tentu berbeda dengan enkripsi.

3. Kunci

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

4. *Ciphertext*

   Ciphertext merupakan suatu pesan yang telah melalui proses enkripsi. Pesan yang ada pada teks kode ini tidak bisa dibaca karena berupa karakter-karakter yang tidak memiliki makna.

5. *Plaintext*

   Plaintext atau sering disebut dengan *cleartext*. Teks biasa ini merupakan pesan yang ditulis atau diketik yang memiliki makna. Pesan inlah yang akan diproses menggunakan algoritma kriptografi untuk menjadi *ciphertext* (teks kode).

6. Pesan dapat berupa data atau informasi yang dikirim atau disimpan dalam media perekaman.

7. *Cryptanalysis*

   Cryptanalysis adalah suatu ilmu untuk mendapatkan teks asli tanpa harus mengetahui kunci yang sah secara wajar. Jika suatu teks kode berhasil diubah menjadi teks asli tanpa menggunakan kunci yang sah, proses

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

tersebut dinamakan *breaking code*. Hal ini dilakukan oleh kriptanalis. Analisis kode juga dapat menemukan kelemahan dari suatu algoritma kriptografi dan akhirnya dapat menemukan kunci atau teks asli dari teks kode yang dienkripsu dengan algoritma tertentu. (Nisak, 2015)

2.2 HILL CIPHER

Hill cipher 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 (Yuliandru, 2016).

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.

Algoritma Enkripsi Hill Cipher

1. Tentukan Plaintext (pesan) selanjutnya, susun plaintext dalam bentuk blok matriks (2x1 jika ordo kunci 2x2, 3x1 jika ordo kunci 3x3). Jika panjang dari karakter plainteks bukan kelipatan dari panjang blok matriks, maka

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

ditambahkan karakter *dummy* (sebarang huruf) supaya semua blok matriks terisi.

2. Tentukan Matriks Kunci dengan persyaratan nilai determinasi matriks kunci harus nilai bilangan ganjil positif atau negatif.
3. Lakukan proses enkripsi dengan rumus:

   $C = M_k * M_p$

   Keterangan:

   C = Ciphertext

   M_k = Matriks kunci

   M_p = Matriks Plaintext

Algoritma Dekripsi Hill Cipher:

Terlebih dahulu menentukan kunci matriks yang akan digunakan, dengan cara sebagai berikut:

1. Menentukan nilai determinan matriks kunci

   $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \rightarrow \det A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11}a_{22} - a_{12}a_{21}$

2. tentukan nilai invers modulo

   $a_{ij}{a_{ij}}^{-1} = 1(mod\ 26)$ atau $\left(\det \mathrm{A} * \mathrm{b_{ij}}\right)\ mod\ 26 = 1$

   Keterangan:

   ${a_{ij}}^{-1}$ dan det A : Nilai determinan matriks kunci (M_k)

   a_{ij} dan b_{ij} : Bilangan bulat positif atau negatif

   mod (modulo atau modulus) : sisa bagi

   Untuk mencari nilai a_{ij} atau b_{ij} gunakan rumus berikut:

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

$\frac{26\,(k)+1}{\det A}$

Menentukan nilai "k" menggunakan bilangan bulat posiitif atau negatif. Lakukan perhitungan menggunakan rumus sampai hasil perhitungannya mendapatkan nilai bilangan bulat positif atau negatif, maka hasil perhitungan rumus tersebut adalah hasil untuk nilai invers modulo, hindari bilangan pecahan.

3. Tentukan Matriks Invers Matriks Kunci (M_k)

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \rightarrow \; A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

4. Tentukan Kunci dekripsi Hill Cipher (${M_k}^{-1}$)

   Nilai Invers modulo $\times$ Invers Matriks Kunci

5. Rumus Dekripsi Hill Cipher

   $P = {M_k}^{-1} * M_c$

   Keterangan:

   P = Plaintext

   ${M_k}^{-1}$ = Matriks Kunci Invers

   M_c = Matriks Ciphertext

   (Caesar, 2016)

2.3 CAESAR CIPHER

Dalam dunia penyandian subtitusi kode pertama terjadi pada masa pemerintahan Julius Caesar yang dikenal dengan kode kaisar. Penyandian

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

dilakukan dengan mengganti posisi huruf awal dari alphabet atau disebut juga dengan algoritma ROT3 (Nisak, 2015).

Penyandian menggunakan caesar cipher dilakukan dengan cara mengganti posisi huruf awal alfabet 3 huruf digeser ke kanan.

Plainteks: 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

Cipherteks: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Contoh:

Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX

Cipherteks: DZDVL DVWHULA GDQ WHPDQQBA REHOLA

Supaya lebih aman maka cipherteks dapat dikelompokkan kedalam n-huruf atau dengan membuang semua spasi tujuannya agar kriptanalis menjadi lebih sulit.

Secara matematis, caesar cipher dirumuskan:

Enkripsi: $C = E(P) = (P + 3)\ mod\ 26$

Dekripsi: $P = E(C) = (C - 3)\ mod\ 26$

Keterangan:

P = Karakter Plainteks

C = Karakter Cipherteks

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Misalkan:

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

Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX

Maka enkripsinya adalah sebagai berikut:

$P_1 =' A' = 0 \rightarrow C_1 = E(0) = (0+3) mod\ 26 = 3 = 'D'$

$P_2 =' W = 22 \rightarrow C_2 = E(22) = (22+3) mod\ 26 = 25 = 'Z'$

$P_3 =' A' = 0 \rightarrow C_3 = E(0) = (0+3) mod\ 26 = 3 = 'D'$

$P_4 =' S' = 18 \rightarrow C_4 = E(18) = (18+3) mod\ 26 = 21 = 'V'$

$P_5 = 'I' = 8 \rightarrow C_5 = E(8) = (8+3) mod\ 26 = 11 = 'L'$

Dan seterusnya....

Sehingga diperoleh cipherteks sebagai berikut:

DZDVL DVWHULA GDQ WHPDQQBA REHOLA

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Dan dekripsinya adaah sebagai berikut:

Cipherteks: DZDVL DVWHULA GDQ WHPDQQBA REHOLA

$C_1 =' D' = 3 \rightarrow P_1 = D(3) = (3-3) mod\ 26 = 0 = 'A'$

$C_2 =' Z' = 25 \rightarrow P_2 = D(25) = (25-3) mod\ 26 = 22 = 'W'$

$C_3 =' D' = 3 \rightarrow P_3 = D(3) = (3-3) mod\ 26 = 0 = 'A'$

.....

$C_{12} =' A' = 0 \rightarrow P_{12} = D(0) = (0-3) mod\ 26 = -3\ mod\ 26 = 23 = 'X'$

Untuk -3 mod 26 dihitung dengan cara |-3| mod 26 = 3, sehingga -3 mod 26 = 26 – 3 = 23.

Sehingga diperoleh plainteks sebagai berikut:

AWASI ASTERX DAN TEMANNYA OBELIX

Dalam proses enkripsi dan dekripsi, jika pergeseran huruf sejauh k, maka:

Enkripsi: $C = E(P) = (P + k) mod\ 26$ (2.1)

Dekripsi: $P = D(C) = (C - k) mod\ 26$ (2.2)

dimana k = kunci rahasia

(Munir, Diktat Kuliah IF4020 Kriptografi , 2019)

2.4 MATRIKS

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Dalam sub bab ini akan mendefinisikan operasi-operasi aritmatika untuk matriks ditijau dari sifat-sifat aljabarnya.

2.4.1 Definisi Matriks

Matriks adalah susunan segi empat siku-siku dari bilangan-bilangan atau skalar-skalar atau fungsi yang dibatasi dengan tanda kurung. Bilangan-bilangan tersebut dinamakan entri atau elemen matriks.

Bentuk umum dari matriks A_{mxn}adalah:

$$A_{mxn} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

Definisi 2.2: (Kesamaan Matriks)

Dua matriks dikatakan sama jika kedua matriks tersebut mempunyai ukuran yang sama dan entri-entri yang bersesuaian dalam kedua matris tersebut sama.

Contoh:

Jika $A = \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$ dan $B = \begin{bmatrix} 2 & 1 \\ 3 & 5 \end{bmatrix}$ maka A=B

(Nisak, 2015)

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

2.4.2 Operasi Matriks

Definisi 2.3 (Penjumlahan Matriks)

Jika $A = [a_{ij}]$ dan $B = [b_{ij}]$ adalah sebarang dua matriks yang berukuran sama, misalkan $m\ x\ n$, maka jumlah matriks A dan B adalah matriks yang diperoleh dengan menambahkan bersama-sama entri yng bersesuaian dalam kedua matriks tersebut.

$$A_{mxn} + B_{mxn} = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{2m} + b_{2m} & \dots & a_{mn} + b_{mn} \end{bmatrix}$$

Definisi 2.4 (Perkalian Matriks)

Jika A adalah matriks mxr dan B adalah matrik rxn, maka hasil dari AB adalah matriks mxn yang entri-entrinya ditentukan sebagai berikut. Untuk mencari entri dalam baris i dan kolom j dari AB, dipilih baris i dari matriks A dan kolom j dari matriks B,entri-entri yang bersesuaian dari baris dan kolom tersebut dikalikan bersama-sama dan kemudian ditambahkan hasil kali yang diperoleh (Nisak, 2015).

2.4.3 Invers Matriks

Definisi 2.5 (Invers Matriks)

Misalkan A merupakan suatu matriks kuadrat dengan n baris dan n kolom dan I_n suatu matriks identitas. Apabila ada *square* matriks A^{-1} sedemikian rupa sehingga

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

berlaku hubungan sebagai berikut: $AA^{-1} = A^{-1}A = I$, maka A^{-1} ini disebut *invers matriks*.

Contoh:

$B = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$ invers dari $A = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix}$

karena $AB = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

dan $BA = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

(Nisak, 2015)

2.4.4 Transpose Matriks

Jika diberikan suatu matriks A berorde $m \times n$, sering kali adalah berguna untuk membentuk matriks baru berukuran $m \times n$ yang kolom-kolomnya adalah baris-baris A.

Definisi 2.6 (Transpose Matriks)

Transpose dari suatu matriks A berorde $m \times n$ adalah matriks B berorde $m \times n$ yang didefinisikan oleh:

$$b_{ij} = a_{ij} \tag{2.3}$$

untuk j = 1,2,...,n dan i = 1,2,...,m.

Transpose dari A dinyatakan dengan A^T.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Sebagai akibat dari persamaan (2.1) bahwa baris ke-j dari A^T memiliki entri-entri yang sama dengan entri-entri dari kolom ke-j dari A, dan kolom ke-i dari A^T memiliki entrientri yang sama dengan entri-entri dari baris ke-i dari A.

Contoh:

Jika $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ maka transpose dari A adalah $A^T = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$

Jika $B = \begin{bmatrix} -3 & 2 & 1 \\ 4 & 3 & 2 \\ 1 & 2 & 5 \end{bmatrix}$ maka transpose dari B adalah $B^T = \begin{bmatrix} -3 & 4 & 1 \\ 2 & 3 & 2 \\ 1 & 2 & 5 \end{bmatrix}$

(Leon, 2001)

2.5 Aritmatika Modular

Aritmatika modular merupkan salah satu cabang ilmu matematika yang memegang peran penting dalam komputasi salah satunya pada aplikasi kriptografi. (Kurniadi, 2017) Sebuah operasi yang menghasilkan sisa pebagian dari suatu bilangan terhadap bilangan lainnya disebut aritmatika modular. Berikut definisi dari operasi modulo:

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi $a\ mod\ m$ menberikan sisa jika a dibagi dengan m. Dengan kata lain, $a\ mod\ m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$.

Atau dapat dituliskan sebagai, untuk sembarang bilangan bulat a modulus m, misal

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

$$R = sisa\ bagi\ dari\ \frac{|a|}{m}$$

Maka r disebut sebagai residu yang merupkan hasil dari $a\ mod\ m$ adalah

$$r = \begin{Bmatrix} R,\ \ untuk\ \ a\ \geq 0 \\ m - R,\ \ untuk\ \ a < 0\ dan\ R \neq 0 \\ 0,\ \ untuk\ a < 0\ dan\ \ R = 0 \end{Bmatrix}$$

Dalam aritmatika modulo juga dikenal dengan kekongruenan atau *equivalent*. Jika m adalah bilangan bulat positif dan a serta b adalah bilangan bulat, maka dikatakan a kongruen terhadap b dalam modulus m, jika $a - b$ adalah kelipatan bulat dari m.

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

Modulo juga memiliki bailikan modulo (invers modulo) yaitu jika a dan m relatif prima dan $m > 1$, maka terdapat suatu bilangan yang merupakan balikan atau inversi yang dilambangkan dengan a^{-1} yang memenuhui

$$aa^{-1} \equiv 1(mod\ m)$$

(Pasaribu, 2012)

2.5.1 Arimatika modular dan sandi bergeser

Sandi Caesar berfungsi dengan menggeser setiap huruf dalam alfabet sejumlah huruf tetap.

Shift cipher dengan shift k mengambil huruf plaintext sesuai dengan nomor p dan menugaskannya ke huruf ciphertext yang sesuai dengan angka $p + k\ mod\ 26$.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Bagaimana penggunaan aritmatika modular, dalam hal ini modulo 26, menyederhanakan dekripsi shift cipher. Jumlah shift berfungsi baik sebagai kinci enkripsi dan dekripsi. Enkripsi diberikan oleh formula:

(Ciphertext Letter) ≡ (Plaintext Letter) + (Secret Key) (mod 26),

Dan dekripsi bekerja dengan arah berlawanan

(Plaintext Letter) ≡ (Chiphertext Letter) - (Secret Key) (mod 26)

(Jeffrey Hoffstein, 2008)

2.6 Integrasi Keislaman dalam Penyandian pesan

Penyandian biasanya digunakan untuk mengamankan data yang bersifat rahasia dan hanya orang tertentu yang berhak mengetahui. Kriptografi adalah bagian dari ilmu matematika yang membahas tentang penyandian.

Setiap manusia tentu memiliki sesuatu yang disebunyikan, entah itu bersifat positif maupun negatif, hal itulah yang disebut dengan rahasia. Rahasia yang disimpan manusia bisa jadi hanya berkaitan dengan kepentingan pribadi dan keluarga, teman dan mungkin rahasia negara. Bahkan Allah SWT juga menentukan nasib hamba-Nya tanpa diketahui oleh siapapun, semua menjadi Rahasia Allah SWT.

Semua hal yang bersifat rahasia harus disimpan baik-baik agar tidak diketahui oleh orang yang tidak berhak mengetahuinya. Islam juga menganjurkan untuk menyimpan rahasia, sebagaimana dijeaskan dalam Al-Quran surat Al-Anfal ayat 27 yang berbunyi:

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

يَـٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَخُونُواْ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓاْ أَمَـٰنَـٰتِكُمۡ وَأَنتُمۡ تَعۡلَمُونَ

"Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui."(QS al-Anfal/8:27)

Di dalam hadits al-Hasan dari samurah, disebutkan bahwa Rasuluoh SAW telah bersada yang artinya:

"sampaikanlah amanat itu kepada orang yang mempercayaimu, dan janganah kamu berkhianat kepada orang yang berkhianat kepadamu."

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB III

METODE PENELITIAN

3.1 JENIS PENELITIAN

Penelitian aplikasi matriks dan aritmatika modular untuk penyandian menggunakan metode hill cipher dan caesar cipher merupakan jenis penelitian deskriptif kuantitatif. Dilihat dari aspek fungsinya penelitian ini merupakan penelitian terapan, dengan membuat kunci pada pesan berupa teks kemudian dilakukan proses enkripsi dan dekripsi menggunakan hill cipher dan caesar cipher.

3.2 DATA DAN SUMBER DATA

Dalam penelitian ini data berupa pesan teks yang akan diubah menjadi cipherteks dengan menggunakan kata sandi sehingga tidak mudah dibaca oleh orang lain.

3.3 PENGOLAHAN DATA

Hal pertama yang dilakukan dalam penelitian ini adalah menentukan teks yang akan disandikan. Kemudian pesan tersebut dienkripsi dan didekripsi menggunakan Hill Cipher, Caesar cipher, dan gabungan Hill Cipher dan Caesar Cipher.

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

1. Mengubah huruf-huruf dalam pesan menjadi bentuk numerik sesuai tabel kunci.
2. Menentukan matriks kunci untuk proses enkripsi

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

3. Mengelompokkan huruf-huruf pesan yang telah diubah dalam bentuk numerik menjadi matriks-matriks.
4. Mengalikan Matriks kunci dan matriks plainteks kemudian dimodulokan 26.
5. Hasilnya kemudian dikonversikan menjadi huruf-huruf alfabet sesuai tabel kunci.
6. Selanjutnya yaitu proses dekripsi. Mengubah cipherteks menjadi numerik.
7. Mencari invers matriks modulo dari matriks kunci enkripsi untuk dijadikan matriks kunci dekripsi.
8. Mengelopokkan angka-angka cipherteks menjadi matriks-matriks.
9. Mengalikan matriks cipherteks dan matriks kunci kemudian dimodulokan 26.
10. Hasilnya kemudian dikonversi kebentuk alfabet sesuai tabel kunci.

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

1. Mengkonversikan alfabet dalam numerik.
2. Menentukan kunci enkripsi dan dekripsi dengan menggeser alfabet sejauh k.
3. Melakukan enkripsi dengan menggunakan persamaan (2.1) dan dekripsi dengan persamaan (2.2).

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

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

1. Mengkonversikan alfabet ke dalam bentuk numerik dan melakukan penggeseran posisi alfabet sejauh k (sesuai dengan algoritma caesar cipher) dan digunakan sebagai tabel kunci ekripsi dan dekripsi.
2. Mengubah huruf-huruf dalam pesan menjadi bentuk numerik sesuai tabel kunci.
3. Melakukan proses enkripsi dan dekripsi sesuai algoritma Hill Cipher.
4. Menentukan matriks kunci untuk proses enkripsi.
5. Mengelompokkan huruf-huruf pesan yang telah diubah dalam bentuk numerik menjadi matriks-matriks.
6. Mengalikan Matriks kunci dan matriks plainteks kemudian dimodulokan 26.
7. Hasilnya kemudian dikonversikan menjadi huruf-huruf alfabet sesuai tabel kunci.
8. Selanjutnya yaitu proses dekripsi. Mengubah cipherteks menjadi numerik.
9. Mencari invers matriks modulo dari matriks kunci enkripsi untuk dijadikan matriks kunci dekripsi.
10. Mengelopokkan angka-angka cipherteks menjadi matriks-matriks.
11. Mengalikan matriks cipherteks dan matriks kunci kemudian dimodulokan 26.
12. Hasilnya kemudian dikonversi kebentuk alfabet sesuai tabel kunci.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB IV

PEMBAHASAN

4.1 Proses Enkripsi dan Dekripsi Hill Cipher

Sebelum melakukan proses penyandian (enkripsi) dan penguraian sandi (dekripsi) terlebih dahulu akan dibuat tabel kunci yaitu tabel konversi antara huruf-huruf alfabet ke dalam bentuk numerik. Angka yang digunakan adalah 0 sampai dengan N-1.

Tabel 4.1. Tabel Kunci Enkripsi dan Dekripsi Hill Cipher

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

Proses Enkripsi Hill Cipher

Sebelum melakukan enkripsi maka terlebih dahulu harus dibuat pesan asli atau dalam bahasa kriptografi disebut *plaintext* terlebih dahulu.

Dalam hal ini akan digunakan pesan berikut sebagai *plaintext*:

“HARI INI HARUS LEBIH BAIK DARI HARI KEMARIN”

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Setelah membuat pesan asli atau plaintext, kemudian huruf-huruf dari pesan tersebut dikonversikan kedalam bentuk sesuai tabel kunci yaitu Tabel 4.1.

H	A	R	I	I	N	I	H	A	R	U	S	L	E	B	I	H	B	A	I	K
7	0	17	8	8	13	8	7	0	17	20	18	11	4	1	8	7	1	0	8	10
D	A	R	I	H	A	R	I	K	E	M	A	R	I	N						
3	0	17	8	7	0	17	8	10	4	12	0	17	8	13						

Menentukan matriks kunci, matriks yang digunakan sebagai kunci yaitu matriks sebarang yang memiliki invers karena invers dari matriks kuncilah yang nanti akan digunakan sebagai matriks kunci dalam proses penguraian sandi (dekripsi). Hal ini dimaksudkan agar pesan yang telah disandikan dapat diurai menjadi pesan asli. Berikut ini adalah matriks kuncinya:

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

Karena matriks kunci berukuran 3x3, maka pesan yang telah dikonversikan dalam bentuk angka harus dikelompokkan dengan masing-masing kelompok beranggotakan tiga karakter antara lain:

$[7 \quad 0 \quad 17]$ $[8 \quad 8 \quad 13]$ $[8 \quad 7 \quad 0]$ $[17 \quad 24 \quad 18]$ $[11 \quad 4 \quad 1]$ $[8 \quad 7 \quad 1]$

$[0 \quad 8 \quad 10]$ $[3 \quad 0 \quad 17]$ $[8 \quad 7 \quad 0]$ $[17 \quad 8 \quad 10]$ $[4 \quad 12 \quad 0]$ $[17 \quad 8 \quad 13]$

Setelah dikelompokkan, kemudian lakukan proses penyandian (enkripsi) dengancara mengalikan matriks-matriks tersebut dengan matriks kunci yang telah ditentukan sebelumnya lalu dimodulokan dan hasilnya dikonversikan lagi dalam bentuk alfabet sesuai tabel awal. Berikut perhitungannya:

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 4\\5 & 6 & 0\end{bmatrix}\begin{bmatrix}7\\0\\17\end{bmatrix}=\begin{bmatrix}58\\68\\35\end{bmatrix}mod26=\begin{bmatrix}6\\16\\9\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}G\\Q\\J\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 4\\5 & 6 & 0\end{bmatrix}\begin{bmatrix}8\\8\\13\end{bmatrix}=\begin{bmatrix}63\\60\\88\end{bmatrix}mod26=\begin{bmatrix}11\\8\\10\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}L\\I\\K\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 4\\5 & 6 & 0\end{bmatrix}\begin{bmatrix}8\\7\\0\end{bmatrix}=\begin{bmatrix}22\\7\\82\end{bmatrix}mod26=\begin{bmatrix}22\\7\\4\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}W\\H\\E\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 4\\5 & 6 & 0\end{bmatrix}\begin{bmatrix}17\\20\\18\end{bmatrix}=\begin{bmatrix}111\\92\\205\end{bmatrix}mod26=\begin{bmatrix}7\\14\\23\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}H\\O\\X\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 4\\5 & 6 & 0\end{bmatrix}\begin{bmatrix}11\\4\\1\end{bmatrix}=\begin{bmatrix}22\\8\\79\end{bmatrix}mod26=\begin{bmatrix}22\\8\\1\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}W\\I\\B\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 4\\5 & 6 & 0\end{bmatrix}\begin{bmatrix}8\\7\\1\end{bmatrix}=\begin{bmatrix}25\\11\\82\end{bmatrix}mod26=\begin{bmatrix}25\\11\\4\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}Z\\L\\E\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 4\\5 & 6 & 0\end{bmatrix}\begin{bmatrix}0\\8\\10\end{bmatrix}=\begin{bmatrix}46\\48\\48\end{bmatrix}mod26=\begin{bmatrix}20\\22\\23\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}U\\W\\X\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 4\\5 & 6 & 0\end{bmatrix}\begin{bmatrix}3\\0\\17\end{bmatrix}=\begin{bmatrix}54\\68\\35\end{bmatrix}mod26=\begin{bmatrix}2\\16\\15\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}C\\Q\\P\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 4\\5 & 6 & 0\end{bmatrix}\begin{bmatrix}8\\7\\0\end{bmatrix}=\begin{bmatrix}22\\7\\82\end{bmatrix}mod26=\begin{bmatrix}22\\7\\4\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}W\\H\\E\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 4\\5 & 6 & 0\end{bmatrix}\begin{bmatrix}17\\8\\10\end{bmatrix}=\begin{bmatrix}63\\48\\133\end{bmatrix}mod26=\begin{bmatrix}11\\22\\3\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}L\\W\\D\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 4\\5 & 6 & 0\end{bmatrix}\begin{bmatrix}4\\12\\0\end{bmatrix}=\begin{bmatrix}28\\12\\92\end{bmatrix}mod26=\begin{bmatrix}2\\12\\14\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}C\\M\\O\end{bmatrix}$$

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 4\\5 & 6 & 0\end{bmatrix}\begin{bmatrix}17\\8\\13\end{bmatrix} = \begin{bmatrix}72\\60\\133\end{bmatrix} mod26 = \begin{bmatrix}20\\8\\3\end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix}U\\I\\D\end{bmatrix}$$

Setelah diakukan proses penyandian (enkripsi) maka didapatkan teks sandi atau yang sering disebut dengan *ciphertext* sebagai berikut:

"GQJLIKWHEHOXWIBZLEUWXCQPWHELWDCMOUID"

Proses Dekripsi Hill Cipher

Proses dekripsi merupakan proses penguraian teks sandi atau dalam bahasa kriptografi disebut sebagai *ciphertext*. Disini teks sandi (*ciphertext*) yang telah didapatkan dari proses enkripsi akan dikembalikan lagi menjadi teks asli atau *plaintext*.

Dalam proses dekripsi ini terlebih dahulu mengkonversikan teks sandi (*ciphertext*) ke dalam bentuk numerik.

G	Q	J	L	I	K	W	H	E	H	O	X	W	I	B	Z	L	E	U	W	X
6	16	9	11	8	10	22	7	4	7	14	23	22	8	1	25	11	4	20	22	23
C	Q	P	W	H	E	L	W	D	C	M	O	U	I	D						
2	16	15	22	7	4	11	22	3	2	12	14	20	8	3						

Untuk penguraikan sandi diperlukan invers matriks modulo dari matriks yang telah digunakan untuk melakukan penyandian yaitu matriks A.

$$A = \begin{bmatrix}1 & 2 & 3\\0 & 1 & 4\\5 & 6 & 0\end{bmatrix} \qquad A^{-1} = \begin{bmatrix}-24 & 18 & 5\\20 & -15 & -4\\-5 & 4 & 1\end{bmatrix} mod\ 26 = \begin{bmatrix}2 & 18 & 5\\20 & 11 & 22\\21 & 4 & 1\end{bmatrix}$$

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Maka diperoleh matriks $A^{-1} = \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix}$ sebagai matriks kunci untuk melakukan proses penguraian sandi.

Karena ukuran matriks kuncinya 3x3 maka *ciphertext* yang sudah dikonversikan dalam bentuk numerik dikelompokkan dengan masing-masing kelompok terdiri dari tiga huruf sehingga terbentuk menjadi sebuah matriks berukuran 3x1, sebagai berikut:

$$\begin{bmatrix} 6 \\ 16 \\ 9 \end{bmatrix} \begin{bmatrix} 11 \\ 8 \\ 10 \end{bmatrix} \begin{bmatrix} 22 \\ 7 \\ 4 \end{bmatrix} \begin{bmatrix} 7 \\ 14 \\ 23 \end{bmatrix} \begin{bmatrix} 22 \\ 8 \\ 1 \end{bmatrix} \begin{bmatrix} 25 \\ 11 \\ 4 \end{bmatrix} \begin{bmatrix} 20 \\ 22 \\ 22 \end{bmatrix} \begin{bmatrix} 2 \\ 16 \\ 15 \end{bmatrix} \begin{bmatrix} 22 \\ 7 \\ 4 \end{bmatrix} \begin{bmatrix} 11 \\ 22 \\ 3 \end{bmatrix} \begin{bmatrix} 2 \\ 12 \\ 14 \end{bmatrix} \begin{bmatrix} 20 \\ 8 \\ 3 \end{bmatrix}$$

Setelah terbentuk matriks-matriks seperti diatas, kemudian dilakukan proses penguraian sandi yaitu dengan mengalikan matriks *ciphertext* dengan matriks A^{-1} lalu hasilnya dimodulo 26 kemudian hasilnya dikonversikan kebentuk alfabet sesuai dengn tabel kunci tabel 4.1. berikut hasil perhitungan dari proses dekripsi:

$$\begin{bmatrix} 6 \\ 16 \\ 9 \end{bmatrix} \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 345 \\ 494 \\ 199 \end{bmatrix} mod26 = \begin{bmatrix} 7 \\ 0 \\ 17 \end{bmatrix} \text{sehingga diperoleh} \begin{bmatrix} H \\ A \\ R \end{bmatrix}$$

$$\begin{bmatrix} 11 \\ 8 \\ 10 \end{bmatrix} \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 216 \\ 528 \\ 273 \end{bmatrix} mod26 = \begin{bmatrix} 8 \\ 8 \\ 13 \end{bmatrix} \text{sehingga diperoleh} \begin{bmatrix} I \\ I \\ N \end{bmatrix}$$

$$\begin{bmatrix} 22 \\ 7 \\ 4 \end{bmatrix} \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 190 \\ 605 \\ 494 \end{bmatrix} mod26 = \begin{bmatrix} 8 \\ 7 \\ 0 \end{bmatrix} \text{sehingga diperoleh} \begin{bmatrix} I \\ H \\ A \end{bmatrix}$$

$$\begin{bmatrix} 7 \\ 14 \\ 23 \end{bmatrix} \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 381 \\ 800 \\ 226 \end{bmatrix} mod26 = \begin{bmatrix} 17 \\ 20 \\ 18 \end{bmatrix} \text{sehingga diperoleh} \begin{bmatrix} R \\ U \\ S \end{bmatrix}$$

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

$$\begin{bmatrix}22\\8\\1\end{bmatrix}\begin{bmatrix}2 & 18 & 5\\20 & 11 & 22\\21 & 4 & 1\end{bmatrix}=\begin{bmatrix}193\\550\\495\end{bmatrix}mod26=\begin{bmatrix}11\\4\\1\end{bmatrix}\text{ sehingga diperoleh}\begin{bmatrix}L\\E\\B\end{bmatrix}$$

$$\begin{bmatrix}25\\11\\4\end{bmatrix}\begin{bmatrix}2 & 18 & 5\\20 & 11 & 22\\21 & 4 & 1\end{bmatrix}=\begin{bmatrix}268\\709\\537\end{bmatrix}mod26=\begin{bmatrix}8\\7\\1\end{bmatrix}\text{ sehingga diperoleh}\begin{bmatrix}I\\H\\B\end{bmatrix}$$

$$\begin{bmatrix}20\\22\\22\end{bmatrix}\begin{bmatrix}2 & 18 & 5\\20 & 11 & 22\\21 & 4 & 1\end{bmatrix}=\begin{bmatrix}546\\1126\\530\end{bmatrix}mod26=\begin{bmatrix}0\\8\\10\end{bmatrix}\text{ sehingga diperoleh}\begin{bmatrix}A\\I\\K\end{bmatrix}$$

$$\begin{bmatrix}2\\16\\15\end{bmatrix}\begin{bmatrix}2 & 18 & 5\\20 & 11 & 22\\21 & 4 & 1\end{bmatrix}=\begin{bmatrix}367\\546\\121\end{bmatrix}mod26=\begin{bmatrix}3\\0\\17\end{bmatrix}\text{ sehingga diperoleh}\begin{bmatrix}D\\A\\R\end{bmatrix}$$

$$\begin{bmatrix}22\\7\\4\end{bmatrix}\begin{bmatrix}2 & 18 & 5\\20 & 11 & 22\\21 & 4 & 1\end{bmatrix}=\begin{bmatrix}190\\605\\494\end{bmatrix}mod26=\begin{bmatrix}8\\7\\0\end{bmatrix}\text{ sehingga diperoleh}\begin{bmatrix}I\\H\\A\end{bmatrix}$$

$$\begin{bmatrix}11\\22\\3\end{bmatrix}\begin{bmatrix}2 & 18 & 5\\20 & 11 & 22\\21 & 4 & 1\end{bmatrix}=\begin{bmatrix}433\\528\\322\end{bmatrix}mod26=\begin{bmatrix}17\\8\\10\end{bmatrix}\text{ sehingga diperoleh}\begin{bmatrix}R\\I\\K\end{bmatrix}$$

$$\begin{bmatrix}2\\12\\14\end{bmatrix}\begin{bmatrix}2 & 18 & 5\\20 & 11 & 22\\21 & 4 & 1\end{bmatrix}=\begin{bmatrix}290\\480\\104\end{bmatrix}mod26=\begin{bmatrix}4\\12\\0\end{bmatrix}\text{ sehingga diperoleh}\begin{bmatrix}E\\M\\A\end{bmatrix}$$

$$\begin{bmatrix}20\\8\\3\end{bmatrix}\begin{bmatrix}2 & 18 & 5\\20 & 11 & 22\\21 & 4 & 1\end{bmatrix}=\begin{bmatrix}199\\554\\455\end{bmatrix}mod26=\begin{bmatrix}17\\8\\13\end{bmatrix}\text{ sehingga diperoleh}\begin{bmatrix}R\\I\\N\end{bmatrix}$$

Setelah diakukan proses penguraian sandi (dekripsi), maka diperoleh teks asli (*plaintext*) sebagai berikut:

"HARI INI HARUS LEBIH BAIK DARI HARI KEMARIN"

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

4.2 Proses Enkripsi dan Dekripsi Caesar Cipher

Teknik penyandian dan penguraian sandi dengan metode caesar cipher merupakan teknik penyandian yang cukup sederhana yaitu dengan cara menggeser huruf-huruf alfabet dengan menggunakan kunci berupa kata yang sudah ditentukan dengan syarat tidak ada pengulangan huruf. Berikut tabel kunci yang akan digunakan untuk proses enkripsi dan dekripsi:

Tabel 4.2 Tabel Kunci Enkripsi dan Dekripsi Caesar Cipher

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

Proses Enkripsi Caesar Cipher

Teks asli (*Plaintext*) : HARI INI HARUS LEBIH BAIK DARI HARI KEMARIN

Sesuai dengan tabel kunci diatas maka diperoleh:

H	A	R	I	I	N	I	H	A	R	U	S	L	E	B	I	H	B	A	I	K
7	0	17	8	8	13	8	7	0	17	20	18	11	4	1	8	7	1	0	8	10
D	A	R	I	H	A	R	I	K	E	M	A	R	I	N						
3	0	17	8	7	0	17	8	10	4	12	0	17	8	13						

Kemudian diakukan penggeseran sesuai keingina. Disini huruf alfabet akan digeser sejauh k, dimana k = 5.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Berikut perhitungannya:

$P_1 = 'H' = 7 \rightarrow C_1 = E(7) = (7+5) mod\ 26 = 12$ berdasarkan tabel kunci diperoleh 12 = ‘M’

$P_2 = 'A' = 0 \rightarrow C_2 = E(0) = (0+5) mod\ 26 = 5$ berdasarkan tabel kunci diperoleh 5 = ‘F’

$P_3 = 'R' = 17 \rightarrow C_3 = E(17) = (17+5) mod\ 26 = 22$ berdasarkan tabel kunci diperoleh 22 = ‘W’

$P_4 = 'I' = 8 \rightarrow C_4 = E(8) = (8+5) mod\ 26 = 13$ berdasarkan tabel kunci diperoleh 13 = ‘N’

$P_5 = 'I' = 8 \rightarrow C_5 = E(8) = (8+5) mod\ 26 = 13$ berdasarkan tabel kunci diperoleh 13 = ‘N’

$P_6 = 'N' = 13 \rightarrow C_6 = E(13) = (13+5) mod\ 26 = 18$ berdasarkan tabel kunci diperoleh 18 = ‘S’

$P_7 = 'I' = 8 \rightarrow C_7 = E(8) = (8+5) mod\ 26 = 13$ berdasarkan tabel kunci diperoleh 13 = ‘N’

$P_8 = 'H' = 7 \rightarrow C_8 = E(7) = (7+5) mod\ 26 = 12$ berdasarkan tabel kunci diperoleh 12 = ‘M’

$P_9 = 'A' = 0 \rightarrow C_9 = E(0) = (0+5) mod\ 26 = 5$ berdasarkan tabel kunci diperoleh 5 = ‘F’

$P_{10} = 'R' = 17 \rightarrow C_{10} = E(17) = (17+5) mod\ 26 = 22$ berdasarkan tabel kunci diperoleh 22 = ‘W’

$P_{11} = 'U' = 20 \rightarrow C_{11} = E(20) = (20+5) mod\ 26 = 25$ berdasarkan tabel kunci diperoleh 25 = ‘Z’

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

$P_{12} = 'S' = 18 \rightarrow C_{13} = E(18) = (18 + 5) mod\ 26 = 23$ berdasarkan tabel kunci diperoleh 23 = ‘X’

$P_{13} = 'L' = 11 \rightarrow C_{13} = E(11) = (11 + 5) mod\ 26 = 16$ berdasarkan tabel kunci diperoleh 16 = ‘Q’

$P_{14} = 'E' = 4 \rightarrow C_{14} = E(4) = (4 + 5) mod\ 26 = 9$ berdasarkan tabel kunci diperoleh 9 = ‘J’

$P_{15} = 'B' = 1 \rightarrow C_{15} = E(1) = (1 + 5) mod\ 26 = 6$ berdasarkan tabel kunci diperoleh 6 = ‘G’

$P_{16} = 'I' = 8 \rightarrow C_{16} = E(8) = (8 + 5) mod\ 26 = 13$ berdasarkan tabel kunci diperoleh 13 = ‘N’

$P_{17} = 'H' = 7 \rightarrow C_{17} = E(7) = (7 + 5) mod\ 26 = 12$ berdasarkan tabel kunci diperoleh 12 = ‘M’

$P_{18} = 'B' = 1 \rightarrow C_{18} = E(1) = (1 + 5) mod\ 26 = 6$ berdasarkan tabel kunci diperoleh 6 = ‘G’

$P_{19} = 'A' = 0 \rightarrow C_{19} = E(0) = (0 + 5) mod\ 26 = 5$ berdasarkan tabel kunci diperoleh 5 = ‘F’

$P_{20} = 'I' = 8 \rightarrow C_{20} = E(8) = (8 + 5) mod\ 26 = 13$ berdasarkan tabel kunci diperoleh 13 = ‘N’

$P_{21} = 'K' = 10 \rightarrow C_{21} = E(10) = (10 + 5) mod\ 26 = 15$ berdasarkan tabel kunci diperoleh 15 = ‘P’

$P_{22} = 'D' = 3 \rightarrow C_{22} = E(3) = (3 + 5) mod\ 26 = 8$ berdasarkan tabel kunci diperoleh 8 = ‘I’

$P_{23} = 'A' = 0 \rightarrow C_{23} = E(0) = (0 + 5) mod\ 26 = 5$ berdasarkan tabel kunci diperoleh 5 = ‘F’

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

$P_{24} = 'R' = 17 \rightarrow C_{24} = E(17) = (17 + 5) mod\ 26 = 22$ berdasarkan tabel kunci diperoleh 22 = ‘W’

$P_{25} = 'I' = 8 \rightarrow C_{25} = E(8) = (8 + 5) mod\ 26 = 13$ berdasarkan tabel kunci diperoleh 13 = ‘N’

$P_{26} = 'H' = 7 \rightarrow C_{26} = E(7) = (7 + 5) mod\ 26 = 12$ berdasarkan tabel kunci diperoleh 12 = ‘M’

$P_{27} = 'A' = 0 \rightarrow C_{27} = E(0) = (0 + 5) mod\ 26 = 5$ berdasarkan tabel kunci diperoleh 5 = ‘F’

$P_{28} = 'R' = 17 \rightarrow C_{28} = E(17) = (17 + 5) mod\ 26 = 22$ berdasarkan tabel kunci diperoleh 22 = ‘W’

$P_{29} = 'I' = 8 \rightarrow C_{29} = E(8) = (8 + 5) mod\ 26 = 13$ berdasarkan tabel kunci diperoleh 13 = ‘N’

$P_{30} = 'K' = 10 \rightarrow C_{30} = E(10) = (10 + 5) mod\ 26 = 15$ berdasarkan tabel kunci diperoleh 15 = ‘P’

$P_{31} = 'E' = 4 \rightarrow C_{31} = E(4) = (4 + 5) mod\ 26 = 9$ berdasarkan tabel kunci diperoleh 9 = ‘J’

$P_{32} = 'M' = 12 \rightarrow C_{32} = E(12) = (12 + 5) mod\ 26 = 17$ berdasarkan tabel kunci diperoleh 17 = ‘R’

$P_{33} = 'A' = 0 \rightarrow C_{33} = E(0) = (0 + 5) mod\ 26 = 5$ berdasarkan tabel kunci diperoleh 5 = ‘F’

$P_{34} = 'R' = 17 \rightarrow C_{34} = E(17) = (17 + 5) mod\ 26 = 22$ berdasarkan tabel kunci diperoleh 22 = ‘W’

$P_{35} = 'I' = 8 \rightarrow C_{35} = E(8) = (8 + 5) mod\ 26 = 13$ berdasarkan tabel kunci diperoleh 13 = ‘N’

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

$P_{36} = 'N' = 13 \rightarrow C_{36} = E(13) = (13 + 5) mod\ 26 = 18$ berdasarkan tabel kunci diperoleh 18 = 'S'

Teks sandi(*Ciphertext*):

"MFWNNSNMFWZXQJGNUGFNPIFWNMFWNPJRFWNS"

Proses Dekripsi Caesar Cipher

Teks Sandi(*Ciphertext*):

MFWNNSNMFWZXYJGNUGFNPIFWNMFWNPJRFWNS

Sesuai dengan tabel kunci diatas maka diperoleh:

M	F	W	N	N	S	N	M	F	W	Z	X	Q	J	G	N	M	G	F	N	P
12	5	22	13	13	18	13	12	5	22	25	23	16	9	6	13	12	6	5	13	15
I	F	W	N	M	F	W	N	P	J	R	F	W	N	S						
8	5	22	13	12	5	22	13	15	9	17	5	22	13	18						

Disini huruf alfabet akan digeser sejauh k, dimana k = 5.

Berikut perhitungannya:

$$C_1 =' M' = 12 \rightarrow P_1 = D(12) = (12 - 5)\ mod\ 26 = 7 = 'H'$$

$$C_2 =' F' = 5 \rightarrow P_2 = D(5) = (5 - 5)\ mod\ 26 = 0 = 'A'$$

$$C_3 =' W' = 22 \rightarrow P_3 = D(22) = (22 - 5)\ mod\ 26 = 17 = 'R'$$

$$C_4 =' N' = 13 \rightarrow P_4 = D(13) = (13 - 5)\ mod\ 26 = 8 = 'I'$$

$$C_5 =' N' = 13 \rightarrow P_5 = D(13) = (13 - 5)\ mod\ 26 = 8 = 'I'$$

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

$C_6 =' S' = 18 \rightarrow P_6 = D(18) = (18 - 5)\ mod\ 26 = 13 = 'N'$

$C_7 =' N' = 13 \rightarrow P_7 = D(13) = (13 - 5)\ mod\ 26 = 8 = 'I'$

$C_8 =' M' = 12 \rightarrow P_8 = D(12) = (12 - 5)\ mod\ 26 = 7 = 'H'$

$C_9 =' F' = 5 \rightarrow P_9 = D(5) = (5 - 5)\ mod\ 26 = 0 = 'A'$

$C_{10} =' W' = 22 \rightarrow P_{10} = D(22) = (22 - 5)\ mod\ 26 = 17 = 'R'$

$C_{11} =' Z' = 25 \rightarrow P_{11} = D(25) = (25 - 5)\ mod\ 26 = 20 = 'U'$

$C_{12} =' X' = 23 \rightarrow P_{12} = D(23) = (24 - 5)\ mod\ 26 = 18 = 'S'$

$C_{13} =' Q' = 16 \rightarrow P_{13} = D(16) = (16 - 5)\ mod\ 26 = 11 =' L'$

$C_{15} =' J' = 9 \rightarrow P_{15} = D(9) = (9 - 5)\ mod\ 26 = 17 = 'E'$

$C_{16} =' G' = 6 \rightarrow P_{16} = D(6) = (6 - 5)\ mod\ 26 = 1 = 'B'$

$C_{17} =' N' = 13 \rightarrow P_{17} = D(13) = (13 - 5)\ mod\ 26 = 8 =' I'$

$C_{18} =' M' = 12 \rightarrow P_{18} = D(12) = (12 - 5)\ mod\ 26 = 7 = 'H'$

$C_{19} =' G' = 6 \rightarrow P_{19} = D(6) = (6 - 5)\ mod\ 26 = 1 = 'B'$

$C_{20} =' F' = 5 \rightarrow P_{20} = D(5) = (5 - 5)\ mod\ 26 = 0 = 'A'$

$C_{21} =' N' = 13 \rightarrow P_{21} = D(13) = (13 - 5)\ mod\ 26 = 8 = 'I'$

$C_{22} =' P' = 15 \rightarrow P_{22} = D(15) = (15 - 5)\ mod\ 26 = 10 = 'K'$

$C_{23} =' I' = 8 \rightarrow P_{23} = D(8) = (8 - 5)\ mod\ 26 = 3 = 'D'$

$C_{24} =' F' = 5 \rightarrow P_{24} = D(5) = (5 - 5)\ mod\ 26 = 0 = 'A'$

$C_{25} =' W' = 22 \rightarrow P_{25} = D(22) = (22 - 5)\ mod\ 26 = 17 = 'R'$

$C_{26} =' N' = 13 \rightarrow P_{26} = D(13) = (13 - 5)\ mod\ 26 = 8 = 'I'$

$C_{27} =' M' = 12 \rightarrow P_{27} = D(12) = (12 - 5)\ mod\ 26 = 7 = 'H'$

$C_{28} =' F' = 5 \rightarrow P_{28} = D(5) = (5 - 5)\ mod\ 26 = 0 = 'A'$

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

$C_{29} =' W' = 22 \rightarrow P_{29} = D(22) = (22 - 5)\ mod\ 26 = 17 = 'R'$

$C_{29} =' N' = 13 \rightarrow P_{29} = D(13) = (13 - 5)\ mod\ 26 = 8 = 'I'$

$C_{30} =' P' = 15 \rightarrow P_{30} = D(15) = (15 - 5)\ mod\ 26 = 10 = 'K'$

$C_{31} =' J' = 9 \rightarrow P_{31} = D(9) = (9 - 5)\ mod\ 26 = 17 = 'E'$

$C_{32} =' R' = 17 \rightarrow P_{32} = D(17) = (17 - 5)\ mod\ 26 = 12 = 'M'$

$C_{33} =' F' = 5 \rightarrow P_{33} = D(5) = (5 - 5)\ mod\ 26 = 0 = 'A'$

$C_{34} =' W' = 22 \rightarrow P_{34} = D(22) = (22 - 5)\ mod\ 26 = 17 = 'R'$

$C_{35} =' N' = 13 \rightarrow P_{35} = D(13) = (13 - 5)\ mod\ 26 = 8 = 'I'$

$C_{36} =' S' = 18 \rightarrow P_{36} = D(18) = (18 - 5)\ mod\ 26 = 13 = 'N'$

Teks Asli (*Plaintext*): HARI INI HARUS LEBIH BAIK DARI HARI KEMARIN

4.3 Proses Enkripsi dan Dekripsi Gabungan Hill Cipher dan Caesar Cipher

Disini kita akan akan melakukan proses penyandian (enkripsi) dan penguraian sandi (dekripsi) dengan menggabungkan antara Hill Cipher dan Caesar Cipher. Sebelum melakukan enkripsi dan dekripsi perlu membuat tabel kunci terlebih dahulu. Tabel kunci tersebut merupakan tabel konversi antara huruf-huruf alfabet kedalam bentuk numerik, angka-angka yang digunakan adalah 0 sampai dengan N-1. Karena ini merupakan gabungan dari Hill Cipher dan Caesar Cipher maka yang sebelumnya A = 0, B = 1, C = 2, dan seterusnya, akan digeser sehingga A = 11, B = 12, sampai angka N-1, kemudian kembali lagi ke angka 0,1,2,3, dan seterusnya. Karena jumlah huruf alfabet ada 26 maka setelah angaka N-1 = 25 akan kembali ke 0, 1, 2, dan seterusnya. Untuk lebih mudahnya lihat Tabel 4.3:

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Tabel 4.3 Tabel Kunci Enkripsi dan Dekripsi Gabungan Hill Cipher dan Caesar Cipher

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

Proses Enkripsi Gabungan Hill Cipher dan Caesar Cipher

Enkripsi (penyandian) adalah proses pengubahan teks asli (*plaintext*) kedalam bentuk teks sandi (*ciphertext*). Jadi hal pertama yang harus dilakukan untuk melakukan proses enkripsi adalah menentukan kalimat apa yang akan disandikan. Disini akan menggunakan kalimat berikut sebagai teks asli (*plainteks*):

"HARI INI HARUS LEBIH BAIK DARI HARI KEMARIN"

Setelah mengetahui kalimat atau *plaintext* yang akan disandikan kemudian ubahlah teks/kalimat tersebut ke dalam bentuk numerik sesuai dengan tabel kunci yaitu Tabel 4.3.

Berikut hasilnya:

H	A	R	I	I	N	I	H	A	R	U	S	L	E	B	I	H	B	A	I	K

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

18	11	2	19	19	24	19	18	11	2	5	3	22	15	12	19	18	12	11	19	21
D	A	R	I	H	A	R	I	K	E	M	A	R	I	N						
14	11	2	19	18	11	2	19	21	15	23	11	2	19	24						

Setelah huruf-huruf tersebut dikonversikan dalam bentuk numerik, kemudian tentukan sebuah matriks yang akan dijadikan sebagai matriks kunci dalam proses penyandian (enkripsi). Matriks yang digunakan sebagai matriks kunci harus matriks yang memiliki invers, karena invers dari matriks kunci yang digunakan dalam proses enkripsi akan digunakan untuk proses penguraian sandi (dekripsi) sehingga kalimat tersebut dapat terbaca kembali.

Dalam proses ini akan menggunakan matriks berukuran 3x3 sebagai berikut untuk dijadikan matriks kunci:

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

Karena matriks kuncinya berukuran 3x3 maka teks yang sudah diubah menjadi bentuk numerik tersebut dipecah menjadi beberapa kelompok sehingga membentuk matriks-matriks berukuran 3x1 sebagai berikut:

$$\begin{bmatrix} 18 \\ 11 \\ 2 \end{bmatrix} \begin{bmatrix} 19 \\ 19 \\ 24 \end{bmatrix} \begin{bmatrix} 19 \\ 18 \\ 11 \end{bmatrix} \begin{bmatrix} 2 \\ 5 \\ 3 \end{bmatrix} \begin{bmatrix} 22 \\ 15 \\ 12 \end{bmatrix} \begin{bmatrix} 19 \\ 18 \\ 12 \end{bmatrix} \begin{bmatrix} 11 \\ 19 \\ 2 \end{bmatrix} \begin{bmatrix} 14 \\ 11 \\ 2 \end{bmatrix} \begin{bmatrix} 19 \\ 18 \\ 11 \end{bmatrix} \begin{bmatrix} 2 \\ 19 \\ 21 \end{bmatrix} \begin{bmatrix} 15 \\ 23 \\ 11 \end{bmatrix} \begin{bmatrix} 2 \\ 19 \\ 24 \end{bmatrix}$$

Setelah *plaintext* berubah menjadi bentuk matriks berukuran 3x1, kemudian lakukan proses penyandian (enkripsi) dengan cara mengalikan matriks kunci dengan matriks *plaintext* setelah itu hasilnya dimodulokan 26 kemudian

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

hasilnya dikonversikan ke dalam bentuk alfabet sesuai tabel kunci 4.3. Berikut hasil perhitungannya:

$$\begin{bmatrix} 3 & 2 & 1 \\ -1 & 2 & 4 \\ 5 & 1 & -3 \end{bmatrix} \begin{bmatrix} 18 \\ 11 \\ 2 \end{bmatrix} = \begin{bmatrix} 78 \\ 12 \\ 95 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 0 \\ 12 \\ 17 \end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix} P \\ B \\ G \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 & 1 \\ -1 & 2 & 4 \\ 5 & 1 & -3 \end{bmatrix} \begin{bmatrix} 19 \\ 19 \\ 24 \end{bmatrix} = \begin{bmatrix} 119 \\ 115 \\ 42 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 15 \\ 11 \\ 16 \end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix} E \\ A \\ F \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 & 1 \\ -1 & 2 & 4 \\ 5 & 1 & -3 \end{bmatrix} \begin{bmatrix} 19 \\ 18 \\ 11 \end{bmatrix} = \begin{bmatrix} 104 \\ 61 \\ 80 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 0 \\ 9 \\ 2 \end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix} P \\ Y \\ R \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 & 1 \\ -1 & 2 & 4 \\ 5 & 1 & -3 \end{bmatrix} \begin{bmatrix} 2 \\ 5 \\ 3 \end{bmatrix} = \begin{bmatrix} 19 \\ 20 \\ 6 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 19 \\ 20 \\ 6 \end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix} I \\ J \\ V \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 & 1 \\ -1 & 2 & 4 \\ 5 & 1 & -3 \end{bmatrix} \begin{bmatrix} 22 \\ 15 \\ 12 \end{bmatrix} = \begin{bmatrix} 108 \\ 56 \\ 89 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 4 \\ 4 \\ 11 \end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix} T \\ T \\ A \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 & 1 \\ -1 & 2 & 4 \\ 5 & 1 & -3 \end{bmatrix} \begin{bmatrix} 19 \\ 18 \\ 12 \end{bmatrix} = \begin{bmatrix} 105 \\ 65 \\ 77 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 1 \\ 13 \\ 25 \end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix} Q \\ C \\ O \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 & 1 \\ -1 & 2 & 4 \\ 5 & 1 & -3 \end{bmatrix} \begin{bmatrix} 11 \\ 19 \\ 21 \end{bmatrix} = \begin{bmatrix} 92 \\ 111 \\ 11 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 14 \\ 7 \\ 11 \end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix} D \\ W \\ A \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 & 1 \\ -1 & 2 & 4 \\ 5 & 1 & -3 \end{bmatrix} \begin{bmatrix} 14 \\ 11 \\ 2 \end{bmatrix} = \begin{bmatrix} 66 \\ 16 \\ 75 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 14 \\ 16 \\ 23 \end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix} D \\ F \\ M \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 & 1 \\ -1 & 2 & 4 \\ 5 & 1 & -3 \end{bmatrix} \begin{bmatrix} 19 \\ 18 \\ 11 \end{bmatrix} = \begin{bmatrix} 104 \\ 61 \\ 80 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 0 \\ 9 \\ 2 \end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix} P \\ Y \\ R \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 & 1 \\ -1 & 2 & 4 \\ 5 & 1 & -3 \end{bmatrix} \begin{bmatrix} 2 \\ 19 \\ 21 \end{bmatrix} = \begin{bmatrix} 65 \\ 121 \\ -34 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 13 \\ 17 \\ 8 \end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix} C \\ G \\ X \end{bmatrix}$$

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

$$\begin{bmatrix} 3 & 2 & 1 \\ -1 & 2 & 4 \\ 5 & 1 & -3 \end{bmatrix} \begin{bmatrix} 15 \\ 23 \\ 11 \end{bmatrix} = \begin{bmatrix} 102 \\ 75 \\ 65 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 24 \\ 23 \\ 13 \end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix} N \\ M \\ C \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 & 1 \\ -1 & 2 & 4 \\ 5 & 1 & -3 \end{bmatrix} \begin{bmatrix} 2 \\ 19 \\ 24 \end{bmatrix} = \begin{bmatrix} 68 \\ 120 \\ -43 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 16 \\ 16 \\ 17 \end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix} F \\ F \\ G \end{bmatrix}$$

Berdasarkan hasil perhitungan dalam proses penyandian (enkripsi) di atas maka diperoleh teks sandi atau dalam bahasa kriptografi disebut sebagai *ciphertext* sebagai berikut:

"PPGEAFPYRIJVTTAQCODWADFMPYRCGXNMCFFG"

Proses Dekripsi Gabungan Hill Cipher dan Caesar Cipher

Dekripsi merupakan proses penguraian teks sandi (*ciphertext*) menjadi teks asli (*plaintext*) kembali agar teks dapat terbaca oleh penerima pesan. Dalam proses ini teks sandi (*ciphertext*) yang akan diuraikan adalah sebagai berikut:

"PBGEAFPYRIJVTTAQCODWADFMPYRCGXNMCFFG"

Sebelum melakukan penguraian sandi (dekripsi) maka *ciphertext* harus dirubah terlebih dahulu kedalam bentuk numerik sesuai tabel kuncinya yaitu tabel 4.3.

Berikut hasil konversi *ciphertext* dalam bentuk numerik:

P	B	G	E	A	F	P	Y	R	I	J	V	T	T	A	Q	C	O	D	W	A
0	12	17	15	11	16	0	9	2	19	20	6	4	4	11	1	13	25	14	7	11
D	F	M	P	Y	R	C	G	X	N	M	C	F	F	G						
14	16	23	0	9	16	0	17	2	19	20	13	16	16	17						

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Langkah berikutnya adalah menentukan matriks kunci, yaitu invers modulo dari matriks kunci yang sudah digunakan untuk melakukan proses enkripsi.

$$A = \begin{bmatrix} 3 & 2 & 1 \\ -1 & 2 & 4 \\ 5 & 1 & -3 \end{bmatrix} \quad A^{-1} = \begin{bmatrix} \frac{10}{7} & -1 & \frac{-6}{7} \\ \frac{-17}{7} & 2 & \frac{13}{7} \\ \frac{11}{7} & -1 & \frac{-8}{7} \end{bmatrix} mod\ 26 = \begin{bmatrix} 20 & 25 & 20 \\ 5 & 2 & 13 \\ 9 & 25 & 10 \end{bmatrix}$$

Setelah diketahui bentuk invers matriks modulonya maka matriks tersebutlah yang akan dijadikan sebagai matriks kunci dalam proses penguraian sandi (dekripsi).

Selanjutnya kelompokkan teks sandi (*ciphertext*) yang telah dikonversikan kedalam bentuk numerik menjadi matriks-matriks berukuran 3x1 karena matriks kuncinya berukuran 3x3. Berikut *ciphertext* yang telah dikelompokkan menjadi matriks-matriks:

$$\begin{bmatrix} 0 \\ 12 \\ 17 \end{bmatrix} \begin{bmatrix} 15 \\ 11 \\ 16 \end{bmatrix} \begin{bmatrix} 0 \\ 9 \\ 2 \end{bmatrix} \begin{bmatrix} 19 \\ 20 \\ 6 \end{bmatrix} \begin{bmatrix} 4 \\ 4 \\ 11 \end{bmatrix} \begin{bmatrix} 1 \\ 13 \\ 25 \end{bmatrix} \begin{bmatrix} 14 \\ 7 \\ 11 \end{bmatrix} \begin{bmatrix} 14 \\ 16 \\ 23 \end{bmatrix} \begin{bmatrix} 0 \\ 9 \\ 2 \end{bmatrix} \begin{bmatrix} 13 \\ 16 \\ 18 \end{bmatrix} \begin{bmatrix} 24 \\ 23 \\ 13 \end{bmatrix} \begin{bmatrix} 16 \\ 2 \\ 9 \end{bmatrix}$$

Setelah *ciphertext* dibentuk menjadi matriks-matriks dan matriks kuncinya sudah diketahui maka selanjutnya adalah proses perhitungan dalam penguraian sandi dengan mengalikan matriks-matriks *ciphertext* dengan matriks kunci lalu hasilnya dimodulokan 26 kemudian hasil akhirnya dikonversi kebentuk huruf alfabet sesuai dengan tabel kunci 4.3. Berikut hasil perhitungan proses dekripsi:

$$\begin{bmatrix} 0 \\ 12 \\ 17 \end{bmatrix} \begin{bmatrix} 20 & 25 & 14 \\ 5 & 2 & 13 \\ 9 & 25 & 10 \end{bmatrix} = \begin{bmatrix} 538 \\ 245 \\ 470 \end{bmatrix} mod 26 = \begin{bmatrix} 18 \\ 11 \\ 2 \end{bmatrix} \text{ sehingga diperoleh } \begin{bmatrix} H \\ A \\ R \end{bmatrix}$$

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

$$\begin{bmatrix}15\\11\\16\end{bmatrix}\begin{bmatrix}20 & 25 & 14\\5 & 2 & 13\\9 & 25 & 10\end{bmatrix}=\begin{bmatrix}799\\305\\570\end{bmatrix}mod26=\begin{bmatrix}19\\19\\24\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}I\\I\\N\end{bmatrix}$$

$$\begin{bmatrix}0\\9\\2\end{bmatrix}\begin{bmatrix}20 & 25 & 14\\5 & 2 & 13\\9 & 25 & 10\end{bmatrix}=\begin{bmatrix}253\\44\\245\end{bmatrix}mod26=\begin{bmatrix}19\\18\\11\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}L\\H\\A\end{bmatrix}$$

$$\begin{bmatrix}19\\20\\6\end{bmatrix}\begin{bmatrix}20 & 25 & 14\\5 & 2 & 13\\9 & 25 & 10\end{bmatrix}=\begin{bmatrix}964\\213\\731\end{bmatrix}mod26=\begin{bmatrix}2\\5\\3\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}R\\U\\S\end{bmatrix}$$

$$\begin{bmatrix}4\\4\\11\end{bmatrix}\begin{bmatrix}20 & 25 & 14\\5 & 2 & 13\\9 & 25 & 10\end{bmatrix}=\begin{bmatrix}334\\171\\246\end{bmatrix}mod26=\begin{bmatrix}22\\15\\12\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}L\\E\\B\end{bmatrix}$$

$$\begin{bmatrix}1\\13\\25\end{bmatrix}\begin{bmatrix}20 & 25 & 14\\5 & 2 & 13\\9 & 25 & 10\end{bmatrix}=\begin{bmatrix}695\\356\\584\end{bmatrix}mod26=\begin{bmatrix}19\\18\\12\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}I\\H\\B\end{bmatrix}$$

$$\begin{bmatrix}14\\7\\11\end{bmatrix}\begin{bmatrix}20 & 25 & 14\\5 & 2 & 13\\9 & 25 & 10\end{bmatrix}=\begin{bmatrix}609\\227\\411\end{bmatrix}mod26=\begin{bmatrix}11\\19\\21\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}A\\I\\K\end{bmatrix}$$

$$\begin{bmatrix}14\\16\\23\end{bmatrix}\begin{bmatrix}20 & 25 & 14\\5 & 2 & 13\\9 & 25 & 10\end{bmatrix}=\begin{bmatrix}1002\\401\\756\end{bmatrix}mod26=\begin{bmatrix}14\\11\\2\end{bmatrix}\text{ sehingga diperloeh }\begin{bmatrix}D\\A\\R\end{bmatrix}$$

$$\begin{bmatrix}0\\9\\2\end{bmatrix}\begin{bmatrix}20 & 25 & 14\\5 & 2 & 13\\9 & 25 & 10\end{bmatrix}=\begin{bmatrix}253\\44\\245\end{bmatrix}mod26=\begin{bmatrix}19\\18\\11\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}I\\H\\A\end{bmatrix}$$

$$\begin{bmatrix}13\\16\\18\end{bmatrix}\begin{bmatrix}20 & 25 & 14\\5 & 2 & 13\\9 & 25 & 10\end{bmatrix}=\begin{bmatrix}912\\331\\921\end{bmatrix}mod26=\begin{bmatrix}2\\19\\21\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}R\\I\\K\end{bmatrix}$$

$$\begin{bmatrix}24\\23\\13\end{bmatrix}\begin{bmatrix}20 & 25 & 14\\5 & 2 & 13\\9 & 25 & 10\end{bmatrix}=\begin{bmatrix}1237\\335\\921\end{bmatrix}mod26=\begin{bmatrix}15\\23\\11\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}E\\M\\A\end{bmatrix}$$

$$\begin{bmatrix}16\\2\\9\end{bmatrix}\begin{bmatrix}20 & 25 & 14\\5 & 2 & 13\\9 & 25 & 10\end{bmatrix}=\begin{bmatrix}496\\201\\284\end{bmatrix}mod26=\begin{bmatrix}2\\19\\24\end{bmatrix}\text{ sehingga diperoleh }\begin{bmatrix}R\\I\\N\end{bmatrix}$$

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Berdasarkan dari hasil perhitungan diatas, teks sandi (*ciphertext*) telah diuraikan sehingga menjadi teks asli (*plaintext*) kembali. Berikut ini adalah hasil penguraian sandi (dekripsi) yang telah diakukan.

"HARI INI HARUS LEBIH BAIK DARI HARI KEMARIN"

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan pada bab sebelumnya maka dapat disimpulkan bahwa:

1. Pada proses enkripsi Hill Cipher dengan menggunakan matriks kunci berukuran 3x3 pesan dapat disandikan sehingga diperoleh cipherteks "GQJLIKWHEHOXWIBZLEUWXCQPWHELWDCMOUID" dan pada proses dekripsi pesan dapat kembali kebentuk semula yaitu "HARI INI HARUS LEBIH BAIK DARI HARI KEMARIN". Hal ini menunjukkan bahwa algoritma tersebut berhasil melakukan proses enkripsi dan dekripsi.
2. Pada proses enkripsi Caesar Cipher dengan menggunakan kunci geser k=5 pesan dapat disandikan sehingga diperoleh cipherteks "MFWNNSNMFWZXQJGNUGFNPIFWNMFWNPJRFWNS" dan pada proses dekripsi pesan dapat kembali kebentuk semula yaitu "HARI INI HARUS LEBIH BAIK DARI HARI KEMARIN". Hal ini menunjukkan bahwa algoritma tersebut berhasil melakukan enkripsi dan dekripsi.
3. Pada metode gabungan Caesar Cipher dan Hill Cipher, dimana caesar cipher digunakan untuk menggeser kunci sejauh k=10 kemudian proses pengenkripsiannya menggunakan Hill Cipher dengan matriks kunci berukuran 3x3 pesan dapat disandikan sehingga diperoleh cipherteks "PPGEAFPYRIJVTTAQCODWADFMPYRCGXNMCFFG" dan pada proses dekripsi pesan dapat kembali kebentuk semula yaitu "HARI INI

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

HARUS LEBIH BAIK DARI HARI KEMARIN". Hal ini menunjukkan bahwa algoritma tersebut berhasil melakukan enkripsi dan dekripsi.

5.2 Saran

Dalam penelitian ini, peneliti menyadari bahwa masih banyak terdapat kekurangan sehingga masih banyak yang harus diperbaiki. Untuk penelitian selanjutnya disarankan untuk menggunakan metode kriptografi yang lain seperti Affine Cipher, Knapsack dan sebagainya serta menggunakan aplikasi komputer.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

DAFTAR PUSTAKA

Caesar, V. (2016). Penggunaan Transformasi Matriks dalam Enkripsi dan Dekripsi. Bandung: Sekolah Tinggi Elektro dan Informatika.

Jeffrey Hoffstein, J. P. (2008). An Introduction to Mathematical Cryptography. USA: Brown University.

Komputer, W. (2010). The Best Encryption Tools. Elek Media Komputindo.

Kurniadi, V. I. (2017). Aplikasi Teori Biangan dalam Algoritma Kriptografi. Bandung: Sekolah Teknik Elektro dan informatika,ITB.

Leon, S. J. (2001). Aljabar Linear dan Aplikasinya Edisi Kelima. Jakarta: Penerbit Erlangga.

Munir, R. (2018). Bahan Kuliah IF4020 Kriptografi. Bandung: Insitut Teknologi Bandung.

Munir, R. (2019). Diktat Kuliah IF4020 Kriptografi . Bandung: Sekolah Tinggi Elektro dan Informatika.

Munir, R. Diktat Kuliah IF5054 Kriptografi. Prodi Teknik Informatika STEI.

Nisak, K. (2015). Penyandian Kriptografi Metode Hill Cipher dan Caesar Cipher Menggunakan Appiventor .

Nurdin, A. P. (2017). Anaisa dan Ipleentasi Kriptografi pada Pesan Rahasia Menguunakan Algoritma Cipher Transposition. Jurnal Elektronik dan Sistem Informasi , Vol.3 No.1.

Nurdin, A. P. (2017). Analisa dan Implementasi Kriptografi pada Pesan Rahasia Menggunaka Algoritma Cipher Transpositon . Jurnal Elektronik Sistem Informasi dan Komputer , 1-10 Vol.3 No.1.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Pasaribu, E. S. (2012). Penerapan Arimatika Modulo dan Matriks dalam Cipher Hill. Bandung: Sekolah Tinggi Elektro dan Informatika ITB.

Sadikin, R. (2012). Kriptografi untuk Keamana Jaringan. Penerbit Andi.

Yuliandru, A. R. (2016). Teknik Kriptografi Hill Cipher Menggunakan Matriks. Bandung: Sekolah Teknik Elektro dan Informatika .

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id