ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN METODE *VIGENERE CIPHER* DAN *ROUTE CIPHER*

SKRIPSI

OLEH
ZULFATUL AUFIA
NIM. 17610109

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

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN METODE *VIGENERE CIPHER* DAN *ROUTE CIPHER*

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

ZULFATUL AUFIA

NIM. 17610109

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

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN METODE *VIGENERE CIPHER* DAN *ROUTE CIPHER*

SKRIPSI

OLEH

ZULFATUL AUFIA

NIM. 17610109

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal, 8 September 2021

Pembimbing I,

Prof. Dr. H. Turmudi, M.Si., Ph.D
NIP. 1957005 198203 1 006

Pembimbing II,

Evawati Alisah, M.Pd
NIP. 19720604 199903 2 001

Mengetahui,
Ketua Program Studi Matematika

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

ENKRISPI DAN DEKRIPSI PESAN MENGGUNAKAN METODE *VIGENERE CIPHER* DAN *ROUTE CIPHER*

SKRIPSI

Oleh
Zulfatul Aufia
NIM. 17610109

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

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

Mengetahui,
Ketua Program Studi Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Zulfatul Aufia

NIM : 17610109

Jurusan : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Enkripsi dan Dekripsi Pesan Menggunakan Metode *Vigenere Cipher* dan *Route Cipher*

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

Malang, 08 Juli 2021

Yang membuat pernyataan,

Zulfatul Aufia

NIM. 17610109

MOTO

“Sukses itu melewati banyak proses bukan banyak protes”

PERSEMBAHAN

Dengan rasa syukur penulis mempersembahkan skripsi ini kepada kedua orang tua, Abd Hamid dan Luluk Zunaidah yang dengan senantiasa selalu menyelipkan nama saya di dalam doanya dan kepada kakak saya Syauqi Machrus Ilham terimakasih atas dukungan dan motivasinya.

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakaatuh

Segala puji bagi Allah Swt. yang telah melimpahkan rahmat, taufik serta hidayah-Nya sehingga penulis mampu menyelesaikan skripsi dengan judul "*Enkripsi dan Dekripsi Pesan Menggunakan Metode Vigenere Cipher dan Route Cipher*" dengan baik sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang matematika di Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Sholawat serta salam tetap tercurahkan kepada junjungan Nabi Muhammad Saw. yang telah membimbing dari zaman kegelapan menuju zaman yang terang yakni agama Islam.

Dalam proses penyusunan skripsi ini tidak lepas dari bimbingan, dukungan serta bantuan dari berbagai pihak. Untuk itu ucapan terima kasih yang sebesar-besarnya penulis sampaikan kepada:

1. Prof. Dr. H. Turmudi. M.Si., Ph.D selaku dosen pembimbing I yang telah memberikan banyak arahan mengenai permasalahan skripsi ini dan telah meluangkan waktunya untuk memberikan bimbingan sehingga penulis dapat menyelesaikan skripsi ini.
2. Evawati Alisah, M.Pd selaku dosen pembimbing II yang telah memberikan nasihat, motivasi serta telah meluangkan waktunya.
3. Muhammad Khudzaifah, M.Si selaku penguji utama yang telah meluangkan waktunya untuk menguji serta memberikan arahan dan masukan.
4. Juhari, M.Si selaku ketua penguji yang telah meluangkan waktunya untuk menguji dan memberikan masukan.

Akhir kata, semoga skripsi ini dapat memberikan manfaat dan menambah wawasan keilmuan bagi pembaca dan penulis.

Wassalamu'alaikum Warahmatullahi Wabarakaatuh

Malang, 22 Oktober 2021

Penulis

DAFTAR ISI

DAFTAR TABEL

ABSTRAK

Aufia, Zulfatul. 2021. **Enkripsi dan Dekripsi Pesan Menggunakan Metode *Vigenere Cipher* dan *Route Cipher*.** Skripsi. Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Prof. Dr. H. Turmudi, M.Si., Ph. D (II) Evawati Alisah, Mp.Pd.

Kata Kunci: Kriptografi, Super Enkripsi, Enkripsi, Dekripsi, *Vigenere Cipher*, *Route Cipher*

Kriptografi merupakan ilmu yang mempelajari tentang cara menjaga kerahasiaan pesan. Terdapat dua proses dalam kriptografi yaitu enkripsi dan dekripsi. Enkripsi yaitu merubah pesan asli (*plainteks*) menjadi pesan acak (*cipherteks*). Dekripsi merupakan proses merubah pesan acak menjadi pesan asli. Penelitian ini menggunakan metode super enkripsi yang mana merupakan gabungan dari dua metode yang terdiri dari metode subtitusi dan metode transposisi. Metode subtitusi yang digunakan adalah *vigenere cipher* dan metode transposisi yang digunakan adalah *route cipher*. Terdapat tiga variasi kunci dari metode *vigenere cipher* yaitu, full *vigenere cipher*, auto-key *vigenere cipher* dan running-key *vigenere cipher*. Adapun tujuan dari penelitian ini yaitu untuk mengetahui proses beserta hasil dari enkripsi dan dekripsi menggunakan super enkripsi dengan metode *vigenere cipher* dan *route cipher*. Adapun proses enkripsi adalah dengan melakukan enkripsi menggunakan metode *vigenere cipher* dan selanjutnya dienkripsi lagi menggunakan metode *route cipher*. Metode *vigenere cipher* terdiri dari tiga variasi, sehingga setiap variasinya dienkripsi satu persatu yang kemudian dienkripsi lagi dengan metode *route cipher*. Adapun proses dekripsi adalah dengan melakukan dekripsi menggunakan metode *route cipher* dan dilanjut dengan metode *vigenere cipher*. Rumus yang digunakan metode *vigenere cipher* pada proses enkripsi adalah $C_i = (P_i + K_i) mod\ 26$ sedangkan pada proses dekripsi $P_i = (C_i - K_i) mod\ 26$. Hasil dari penelitian ini yaitu didapatkannya cipherteks pada proses enkripsi dan plainteks pada proses dekripsi yang menggunakan metode *vigenere cipher* dengan 3 variasi dan metode *route cipher.*

ABSTRACT

Aufia, Zulfatul. 2021. **Encryption and Decryption Messages Using the *Vigenere Cipher* and *Route Cipher* Methods**. Thesis. Department of Mathematics, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University Malang. Advisor: (I) Prof. Dr. H. Turmudi, M.Sc., Ph. D (II) Evawati Alisah, Mp.Pd.

Keywords: Cryptography, Super Encryption, Encryption, Decryption, Vigenere Cipher, Route Cipher

Cryptography is the study of how to maintain the confidentiality of messages. There are two processes in cryptography, namely encryption and decryption. Encryption is changing the original message (plaintext) into a random message (ciphertext). Decryption is the process of converting random messages into the original messages. This study uses a super encryption method which is a combination of two methods consisting of the substitution method and the transposition method. The substitution method used is the Vigenere cipher and the transposition method used is the Route cipher. There are three key variations of the vigenere cipher method, that is full vigenere cipher, auto-key vigenere cipher and running-key vigenere cipher. This purpose of this research is to determine the process of encryption and decryption using super encryption with vigenere cipher and route cipher methods. The encryption process is to encrypt using the vigenere cipher method and then encrypted again using the route cipher method. The Vigenere cipher method consists of three variations, each variation is encrypted one by one which is then encrypted again with the route cipher method. The decryption process is to decrypt using the route cipher method and continued with the Vigenere cipher method. The formula used by the vigenere cipher method in the encryption process is $C_i = (P_i + K_i) mod\ 26$ while in the decryption process $P_i = (C_i - K_i) mod\ 26$. The result of this research is that the ciphertext is obtained in the encryption process and the plaintext in the decryption process using the vigenere cipher method with theree variations and the route cipher method.

ملخص

الأوفيا، زلفة٢٠٢١. **التشفير و وصف طرق تشفير *Vigenere Cipher* وتشفير *Route Cipher***. البحث العلمى. قسم الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم مالانج.المشرف :(١) البروفيسور الدكتور الحاج ترمودي الماجستير، (٢) إيفاوتي أليسة، المجستير.

الكلمات المفتاحية : كيريفتوكيرفي، التشفير الفائق، التشفير ، وصف، *Vigenere Cipher* ، *Route Cipher*.

علم التشفير هو دراسة كيفية إبقاء الرسائل سرية. هناك عمليتان في التشفير، وهما التشفير و فك التشفير. يعمل التشفير على تغيير الرسالة الأصلية نص عادي (*plainteks*) إلى رسالة عشوائية نص مشفر (*cipherteks*). الوصف هو عملية تحويل الرسائل العشوائية إلى رسائل أصلية. تستخدم هذه الدراسة طريقة التشفير الفائق وهي مزيج من طريقتين التي تتكوين من طريقة الاستبدال وطريقة التحويل. طريقة الاستبدال المستخدمة هي تشفير فيكينيري جيفير (*vigenere cipher*) وطريقة التحويل المستخدمة هي تشفير روي جيفير (*route cipher*). هناك ثلاثة اختلافات رئيسية لطريقة التشفير فيكينيري جيفير (*vigenere cipher*) ، وهي: فول فيكينيري جيفير (*full vigenere cipher*) ، و أوت فيكينيري جيفير (*auto-key vigenere cipher*) ورنيغ فيكينيري جيفير (*running-key vigenere cipher*) . تهدف هذه الدراسة إلى تحديد عملية التشفير ووصف باستخدام طريقة التشفير الفائقة مع طريقة تشفير فيكينيري جيفير (*vigenere cipher*) ، تشفير روي جيفير (*route cipher*). عملية التشفير هي التشفير باستخدام طريقة تشفير فيكينيري جيفير (*vigenere cipher*) ثم إعادة تشفيرها باستخدام طريقة تشفير روي جيفير (*route cipher*) تتكون طريقة تشفير فيكينيري جيفير (*vigenere cipher*) جيفير من ثلاثة اختلافات، بحيث تشفير كل شكل واحدًا ا التشفير الآخر ثم يتم تشفيره مرة أخرى باستخدام طريقة روي جيفير. عملية وصف هي وصف التشفير باستخدام طريقة تشفير روي جيفير (*route cipher*) متبوعة بطريقة التشفير فيكينيري جيفير (*vigenere cipher*). الصيغة المستخدمة بواسطة طريقة التشفير فيكينيري جيفير (*vigenere cipher*) في عملية التشفير هي $C_i = (P_i + K_i) \ mod \ 26$ أثناء عملية وصف $P_i = (C_i - K_i) \ mod \ 26$. تُظهر النتائج أن الحصول على نص مشفر في عملية التشفير ونص عادي في

عملية وصف التشفير باستخدام طريقة التشفير **فيكينيري جيفير**(*vigenere cipher*) مع ٣ اختلافات وطريقة تشفير **روي جيفير** (*route cipher*).

BAB I

PENDAHULUAN

1.1. Latar Belakang

Di era modern seperti saat ini, perkembangan teknologi yang semakin pesat memudahkan dalam pertukaran pesan. Meningkatnya kebutuhan terhadap pertukaran pesan yang semakin tinggi, sehingga aspek keamanan sangat dibutuhkan. Dalam hal ini, dibutuhkan suatu pengamanan sehingga pesan tersebut tidak terbaca oleh pihak lain yang bukan merupakan tujuan dari pesan tersebut. Untuk menangani permasalahan tersebut, maka diperlukan kunci untuk membukanya, yang mana kunci tersebut hanya dimiliki orang yang berhak membuka pesan tersebut.

Menjaga keamanan pesan merupakan sebuah amanah yang harus dijaga karena hal ini merupakan suatu yang sangat penting. Hal ini telah dijelaskan dalam Al-Qur'an yaitu tentang amanat yang tercantum dalam surat Al-Anfal ayat 27:

Artinya:

Wahai orang-orang yang beriman! Janganlah kamu mengkhianati Allah dan Rasul dan (juga) janganlah kamu mengkhianati amanah yang dipercayakan kepadamu, sedangkan kamu mengentahui. (QS. Al-Anfal:27)

Ayat tersebut menjelaskan bahwa amanah merupakan suatu yang harus dijaga dan disampaikan kepada yang berhak menerimanya. Hal ini berhubungan dengan konsep kriptografi, dimana pesan tersebut hanya dapat dibuka oleh seorang yang membuat dan penerima yang mengetahui kunci tersebut, sehingga pesan tersebut tetap terjaga keamanannya.

Kriptografi merupakan teknologi keamanan pesan yang sering digunakan. Metode yang digunakan adalah *vigenere cipher* sebagai metode subtitusi dan *route cipher* sebagai metode transposisi. Dalam penyelesaiaanya menggunakan proses super enkripsi dimana metode ini merupakan kombinasi dari subtitusi dan

transposisi, karena kombinasi dari keduanya menghasilkan keamanan informasi yang tidak mudah dilacak.

Pada penelitian sebelumnya yang telah dilakukan oleh Surya Darma Nasution, Muhammad Syahrizal, Guidio Leonarde Ginting dan Robbi Rahim (2017) berjudul Data Security Using Vigenere Cipher and Goldbach Codes Algorithm yang membahas proses enkripsi dan dekripsi menggunakan metode *vigenere cipher* dan kode *goldbach*. Untuk mencapai cipherteksnya yaitu dengan melakukan enkripsi menggunakan metode *vigenere cipher* dan setelah didapatkan hasilnya (cipherteks) dilanjut dengan enkripsi menggunaan kode *goldbach*. Sedangkan untuk proses dekripsinya yaitu dengan melakukan dekripsi menggunkan kode *godbach* dan setelah didapatkan hasilnya (plainteks) dilanjut dengan dekripsi menggunakan metode *vigenere cipher*. Maksud penggabungan 2 metode ini untuk mengatasi kelemahan dari metode *vigenere cipher* yang dapat dilacak dengan metode kasiski. Kode *goldbach* merupakan algoritma yang dapat mengatasi kelemahan pada *vigenere cipher*. Shanny Avelina Halim (2007) berjudul Super Enkripsi Dengan Menggunakan Cipher Subtitusi dan Cipher Transposisi membahas tentang proses enkripsi dan dekripsi menggunakan metode subtitusi dan transposisi dimana metode subtitusi yang digunakan hanya menggunakan 1 kunci yang sama untuk semua karakter dan metode transposisinya menggunakan susunan blok namun metode ini dapat dipecahkan dengan menggunakan metode *brut force* yaitu mencoba semua kemungkinan yang ada. Selanjutnya telah dilakukan penelitian oleh Nova Fitri (2019) berjudul Perancangan Aplikasi Penyandian File Teks Meggunakan Algoritma Route Cipher Berbasis Dekstop yang membahas proses enkripsi dan dekripsi menggunakan metode *Route cipher* beserta implementasinya. Rute yang digunakan

pada metode ini yaitu berbentuk spiral. Rute spiral searah jarum jam digunakan pada proses enkripsi dan untuk proses dekripsi dengan mengisi kolom kosong dari kanan atas ke bawah berbentuk spiral searah jarum jam. Berdasarkan penelitian yang telah dilakukan oleh beberapa peneliti tersebut, sehingga peneliti berharap dapat melakukan suatu penelitian baru berjudul "Enkripsi dan Dekripsi Pesan Menggunakan Metode *Vigenere cipher* dan *Route cipher*", dimana *vigenere cipher* merupakan algoritma dengan menggunakan teknik subtitusi polyalfabetik dan *route cipher* merupakan algoritma dengan menggunakan transposisi yang memiliki susunan berbentuk spiral.

1.2. Rumusan Masalah

Berdasarkan latar belakang tersebut maka rumusan masalah penelitian ini adalah:

1. Bagaimana proses enkripsi pesan menggunakan metode *vigenere cipher* dan *route cipher*?
2. Bagaimana proses dekripsi pesan menggunakan *vigenere cipher* dan *route cipher*?

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, maka tujuan penelitian ini adalah:

1. Untuk mengetahui proses enkripsi pesan menggunakan metode *vigenere cipher* dan *route chiper*.
2. Untuk mengetahui proses dekripsi pesan menggunakan *vigenere cipher* dan *route cipher*.

1.4. Manfaat Penelitian

Beberapa manfaat yang dapat diambil dari penelitian ini, antara lain:

1. Bagi penulis

   Mendapatkan cara untuk mengamankan pesan teks dan dapat memperbanyak literatur terkait kriptografi khususnya algoritma *vigenere cipher* dan *route cipher*, sehingga nantinya dapat bermanfaat untuk menjaga keamanan data dan dapat diimplementasikan.

2. Bagi pembaca

   Mendapatkan tambahan wawasan yang nantinya dapat digunakan sebagai bahan referensi.

3. Bagi lembaga

   Dapat menambah bahan kepustakaan terutama untuk mata kuliah yang berhubungan dengan kriptografi.

1.5. Metode Penelitian

Metode yang digunakan pada penelitian ini yaitu *library research* atau kajian kepustakaan dengan mempelajari, mengumpulkan, menelaah dan mengolah bahan penelitian dari beberapa buku, artikel, makalah dan lain sebagainya yang berkaitan dengan pengertian, contoh-contoh proses enkripsi dan dekripsi menggunakan satu metode atau lebih yang berhubungan dengan peneltian ini. Berdasarkan tujuan penelitian, maka diperlukan langkah-langkah untuk mengetahui proses enkripsi dan dekripsi untuk mengamankan pesan.

Proses enkripsi menggunakan metode *vigenere cipher* dan *route cipher*

1. Membuat pesan teks (plainteks)
2. Menentukan kunci yang digunakan pada *vigenere cipher*
3. Melakukan perhitungan dengan *vigenere cipher* menggunakan rumus $C_i = (P_i + K_i)\ mod\ 26$
4. Mendapatkan hasil enkripsi *vigenere cipher*
5. Menentukan kunci yang digunakan pada metode transposisi *route cipher*
6. Menyusun hasil ekripsi *vigenere cipher* sesuai kunci *route cipher* dari kiri ke kanan secara horizontal
7. Menyusun hasil enkripsi *route cipher* dari kanan atas ke bawah berbentuk spiral searah jarum jam
8. Mendapatkan hasil enkripsi *route cipher* (cipherteks).

Proses dekripsi menggunakan metode *vigenere cipher* dan *route cipher*

1. Menentukan cipherteks *route cipher*
2. Menentukan kunci *route cipher* (jumlah karakter cipherteks dibagi kunci pada proses enkripsi)
3. Memasukkan pesan yang sudah disandikan (cipherteks) dan menyusun karakter dari kiri atas ke bawah berbentuk spiral berlawanan dengan arah jarum jam
4. Menyusun plainteks *route cipher* secara horizontal dari kanan ke kiri
5. Mendapatkan hasil dekripsi *route cipher*
6. Menyusun cipherteks *vigenere cipher* ke dalam tabel konversi
7. Menentukan kunci *vigenere cipher*

8. Melakukan perhitungan *vigenere cipher* dengan menggunakan rumus $P_i = (C_i - K_i)\ mod\ 26$
9. Mendapatkan pesan asli *vigenere cipher* (plainteks) .

1.6. Sistematika Penulisan

BAB 1 PENDAHULUAN

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

BAB II KAJIAN PUSTAKA

Kajian pustaka berisi teori-teori yang mendukung pembahasan. Teori-teori ini berisi kongruensi, pengertian kriptografi, macam-macam kriptografi, kriptografi klasik dan modern, *vigenere cipher*, *route cipher*, super enkripsi, dan keamanan data.

BAB III PEMBAHASAN

Bab ini berisi uraian secara keseluruhan langkah-langkah yang terdapat pada metode penelitian dan menjawab semua rumusan masalah.

BAB IV PENUTUP

Bab ini berisi tentang kesimpulan penelitian dan saran untuk penelitian selanjutnya.

BAB II

KAJIAN PUSTAKA

2.1. Kriptografi

2.1.1. Pengertian Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu *Kripto* dan *Grafia*. *Kripto* berasal dari bahasa *secret* (rahasia) dan *Grafia* berarti *writing* (tulisan). Menurut terminology, Kriptografi mencakup penelitian tentang bagaimana menjaga kerahasiaan pesan yang dikirim dari pihak pertama kepihak lain. (Ariyus, 2006) Dengan kata lain, kriptografi dapat diartikan sebagai ilmu yang memiliki hubungan dengan keamanan informasi diantaranya sebagai kerahasiaan data dan verifikasi.

Komponen dari algoritma kriptografi yaitu metode enkripsi dan metode dekripsi. Metode enkripsi adalah proses mengubah pesan asli menjadi pesan acak yang tidak mudah dipahami atau biasa disebut cipherteks. Sedangkan metode dekripsi adalah mengembalikan pesan terenkripsi ke bentuk aslinya atau yang disebut plainteks.

Beberapa komponen yang terdapat dalam kriptografi yaitu sebagai berikut:

1. *Enkripsi* adalah perubahan pesan asli (plainteks) menjadi sandi yang cukup sulit dimengerti. Dengan kata lain, enkripsi disebut sebagai cipherteks atau pesan acak.
2. *Dekripsi* adalah kebalikan dari enkripsi, dimana pesan terenkripsi dikembalikan kepesan asli. Cara mengembalikannya tentu menggunkan cara yang berbeda dengan proses asli.
3. *Kunci* adalah kunci yang digunakan dalam proses enkripsi dan dekripsi.

4. *Cipherext* adalah suatu pesan yang telah acak atau telah dienkripsi. Pesan yang telah dienkripsi tidak mudah terbaca karena merupakan karakter yang tidak memiliki arti.
5. *Plainteks* atau sering disebut *cleartext* merupakakn teks asli yang belum melalui proses apapun dan teks ini mudah dipahami karena mengandung makna.
6. *Pesan* dapat berupa data atau informasi yang dikirim atau yang disimpan di dalam media perekaman.
7. *Cryptanalysis* diartikan sebagai seseorang yang dapat membaca teks yang telah dienkripsi tanpa harus mengetahui kunci dari pemilik informasi. (Ariyus, 2006)

Adapun tujuan dari ilmu kriptografi yaitu:

1. Kerahasiaan merupakan suatu hal yang harus dijaga keamanan isinya dari informasi yang telah disandi.
2. Integritas data
3. Autentikasi adalah hubungan indentifikasi, baik seluruh informasi maupun informasi sendiri
4. Non-repudiasi atau penyangkalan adalah cara untuk mencegah perilaku tidak teratur dalam pengiriman informasi kepada pengirim. (Asnawati, Erfandi dan Yupiyanti, 2014)

2.1.2. Kriptografi Klasik dan Modern

Sama halnya dengan algoritma simetri, kriptografi klasik juga menggunakan kunci yang sama pada proses enkripsi dan dekripsinya. Kriptografi klasik telah ada selama berabad-abad. Algoritma ini memiliki dua teknik dasar, yaitu sebagai berikut:

1. Teknik subtitusi: merubah setiap karakter dengan karakter lain.
2. Teknik transposisi (permutasi): dilakukan dengan penggelompokkan dan permutasi.

Salah satu enkripsi menggunakan kunci simentri adalah teknik subtitusi. Terdapat 4 istilah subtitusi kode, antara lain:

1. *Monoalphabet*, setiap karakter teks kode menggantikan salah satu karakter teks asli.
2. *Polyalphabet*, setiap karakter teks kode dapat menggantikan lebih dari satu macam karakter teks asli.
3. *Monograf*, satu enkripsi dilakukan terhadap satu karakter teks asli.
4. *Polygraph*, satu enkripsi dilakukan terhadap lebih dari satu karakter teks asli. (Ariyus, 2006)

Kriptografi modern merupakan perbaikan dari kriptografi klasik. Pada kriptografi modern, keamanan informasi yang dikirim melalui jaringan komputer sehingga mempunyai kerumitan yang sangat kompleks dibanding kriptografi klasik. (Ariyus, 2008)

2.2. Aritmatika Modulo Dalam Kriptografi

Aritmatika modulo merupakan angka sisa dari hasil pembagian dua angka lainnya.

Misalkan a dan m bilangan bulat dengan $m > 0$. Operasi $a\ modulo\ m$ atau $a\ mod\ m$. Akan memberikan sisa pembagian jika a dibagi m, atau dapat ditulis:

$$a\ mod\ m = r$$

m disebut modulo atau modulus, dan hasil aritmatika modulo m terletak didalam himpunan $\{0,1,2,3, \dots, m-1\}$

Contoh:

1. 23 mod 5 = 3, karena 23 = 5·4 3
2. 0 mod 12 = 0, karena 0 = 12·0 0
3. -41 mod 9 = 4, karena a negatif, bagi $|a|$ dengan m mendapatkan sisa r^1. Maka a mod $m = m - r^1$ bila $r^1 \neq 0$. Jadi $|-41| mod\ 9 = 5$, sehingga 41 mod 9 = 9 – 5 = 4

(Wardani, 2016)

2.3. Kongruensi Dalam Kriptografi

Misalkan a, b dan m adalah bilangan bulat, dengan $m > 0$. Bilangan a dikatakan kongruen dengan b modulo m jika $m|(a - b)$ dan ditulis

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

Dalam kalimat yang sederhana bisa dianggap bila a dibagi m akan bersisa b

Dalil tentang pembagian:

- $n|n$ = setiap bilang bulat membagi dirinya sendiri
- $d|n$ dan $n|m \rightarrow d|m$ = prinsip transitif
- $d|n$ dan $d|m \rightarrow d|an + bm$ = $\forall\ a, b \in Z$, prinsip linear
- $d|n \rightarrow ad|an$ = prinsip multiplikatif
- $ad|an \rightarrow d|n\ \forall a \neq 0$ = prinsip pembatalan
- $1|n$ = angka 1 membagi setiap bilangan bulat
- $n|1 \rightarrow n = \pm 1$
- $d|0$ $\forall d$ adalah bilangan bulat
- Jika d dan n bilangan bulat positif yang bulat dan $d|n \rightarrow d \leq n$
- Jika $d|n$ dan $\rightarrow d|m$ maka dalam keadaan khusus $d|n + m$ dan $d|n - m$ merupakan prinsip kombinasi linear. (Tong, 2008)

Teorema 1

Misalkan a, b dan c bilangan bulat dan m bilangan asli, maka berlaku:

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

   $b \equiv a \ (mod\ m)$ dan $a - b \equiv 0 \ (mod\ m)$ adalah pernyataan yang ekuivalen
3. Transitif, jika $a \equiv b \ (mod\ m)$ dan $b \equiv c \ (mod\ m)$ maka:

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

Bukti:

1. Jika $m \neq 0$ maka $m|0$ yang dapat dituliskan sebagai $m|a - a$.

   Menurut definisi berlaku $a \equiv a(mod\ m)$, $\forall$ bilangan bulat a dan $m \neq 0$.
2. $a \equiv b(mod\ m)$ berarti $m|a - b$, menurut definisi 1 ada keterbagian bilangan bulat t sehingga:

   $m|a - b$ dapat dinyatakan $a - b = tm$

   $\leftrightarrow -(a - b) = -tm$

   $\leftrightarrow b - a = (-t)m$

   Menurut definisi, ini berarti $b \equiv a(mod\ m)$.

   $a \equiv b(mod\ m)$ berarti $m|a - b$, menurut definisi ada bilangan bulat t sehingga $m|a - b$ dapat dinyatakan $a - b = tm$, $\forall\ (a - b) - 0 = tm$ maka $(a - b) \equiv 0(mod\ m)$
3. $a \equiv b(mod\ m)$ berarti $m|a - b$ (menurut definisi)

   $b \equiv c(mod\ m)$ berarti $m|b - c$ (menurut definisi)

   Menurut definisi 1 pada keterbagian ada bilangan bulat t_1 dan t_2 sehingga:

   $m|a - b$ dinyatakan dengan $a - b = t_1 m$

   $m|b - c$ dinyatakan dengan $b - c = t_2 m$

Kedua persamaan dijumlahkan sehingga diperoleh

$$a - c = (t_1 + t_2)m$$

Hal ini sesuai dengan definisi sehingga $a \equiv c(mod\ m)$

Teorema 2

Jika $a \equiv b\ (mod\ m)$, maka $a + c \equiv b + c\ (mod\ m)$

Bukti:

$a \equiv b(mod\ m)$ berarti $m|a - b$ (definisi)

Menurut definisi pada keterbagian ada bilangan bulat t sehingga:

$m|a - b$ dapat dinyatakan $a - b = tm$

$\leftrightarrow (a - b) + 0 = tm$

$\leftrightarrow (a - b) + (c - c) = tm$

$\leftrightarrow (a + c) - (b + c) = tm$

Sesuai definisi maka diperoleh $a + c \equiv b + c(mod\ m)$

Teorema 3

Misalkan a, b, c adalah bilangan bulat dan m bilangan asli. Jika $a = -b\ (mod\ m)$, maka $a + c \equiv b + d\ (mod\ m)$

Bukti

$a \equiv b\ (mod\ m)$, berarti $m|a - b$ (menurut definisi)

Menurut definisi pada keterbagian ada bilangan bulat t sehingga:

$m|a - b$ dapat dinyatakan $a - b = tm$

$\leftrightarrow (a - b)c = (tm)c$

$\leftrightarrow ac - bc = (tc)m$

Sesuai definisi maka diperoleh $ac \equiv bc(mod\ m)$

Teorema 4

Misalkan a, b, c, d adalah bilangan bulat dan m, bilangan asli, jika $a \equiv b \ (mod\ m)$ dan $c \equiv d(mod\ m)$, maka $a - c \equiv b - d \ (mod\ m)$.

Bukti

$a \equiv b(mod\ m)$ berarti $m|a - b$ (i)

$c \equiv d(mod\ m)$ berarti $m|c - d$ (ii)

Menurut definisi 1 pada keterbagian ada bilangan bulat t_1 dan t_2 sehingga:

$m|a - b$ dapat dinyatakan $a - b = t_1 m$

$m|c - d$ dapat dinyatakan $c - d = t_2 m$

Persamaan (i) dan (ii) dijumlahkan menjadi

$(a + c) - (b + d) = (t_1 + t_2)m$

Ini berarti sesuai definisi $a + c \equiv b + d \ (mod\ m)$

Teorema 5

Jika $a \equiv b \ (mod\ m)$ dan $d|m, d > 0$, maka $a \equiv b \ (mod\ m)$.

Bukti

$a \equiv b \ (mod\ m)$ berarti $m|a - b$ (i)

Dan $c \equiv d \ (mod\ m)$ berarti $m|c - d$ (ii)

Menurut definisi 1 pada keterbagian ada bilangan bulat t_1 dan t_2 sehingga:

$m|a - b$ dapat dinyatakan $a - b = t_1 m$

$m|c - d$ dapat dinyatakan $\underline{c - d = t_2 m}$

Kedua persamaan (i) dan (ii) dikurangkan menjadi

$(a - c) - (b - d) = (t_1 - t_2)m$

Ini berarti $a - c \equiv b - d(mod\ m)$

(Habibi, Hijriyah dan Irawan, 2014)

2.4. Vigenere Cipher

2.4.1. Sejarah dan Pengertian Vigenere Cipher

Algoritma ini dipublikasikan oleh Blaise de Vigenere pada tahun 1586 diabad ke-16. Namun sebenarnya, kode tersebut ditemukan oleh Giovan Batista Belaso pada tahun 1553 dan dimasukkan ke dalam buku *La Cifta del Sig*. Algoritma tersebut menyebar sejak 200 tahun yang kemudian diberi nama kode *vigenere*. Vigenere merupakan penyebab terjadinya peperangan di Amerika Serikat dan sandinya telah digunakan oleh Tentara Sekutu. (Ariyus, 2008)

Keamanan sandi *vigenere* tergantung pada banyaknya kunci yang digunakan. Namun beberapa ahli telah mengungkapkan kelemahan dari metode ini, Friedrich Kasiski melakukan uji Kasiski pada sandi *vigenere* pada tahun 1863 dan menemukan kelemahan metode tersebut yaitu dapat diketahui panjang kunci dan nilai kunci *vigenere.* (Sadikin, 2012)

Vigenere cipher merupakan pengembangan dari *caesar cipher.* Pada *caesar cipher,* setiap huruf teks digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alphabet sedangkan *vigenere cipher* terdiri dari beberapa sandi *caesar* dengan nilai geser yang berbeda. Sehingga *vigenere cipher* merupakan algoritma klasik yang menggunakan metode subtitusi abjad-majemuk (*Polyalphabetic Subsitution Cipher*). Metode ini mengubah teks asli menjadi teks yang susah dimengerti dengan teknik subtitusi.

2.4.2. Variasi Vigenere Cipher

Kekurangan utama dari *vigenere cipher* adalah adanya pengulangan susunan huruf yang disebabkan oleh kunci yang diulang sepanjang plainteks. Untuk

mengurangi kekurangan tersebut sehingga muncul beberapa variasi dari *vigenere cipher*. Beberapa variasi tersebut sebagai berikut:

1. *Full vigenere cipher*

   Pada varian ini, setiap baris di dalam tabel tidak menyatakan pergeseran huruf, tetapi merupakan permutasi huruf-huruf alphabet.

2. *Auto-key vigenere cipher*

   Idealnya kunci tidak digunakan secara berulang. Pada *auto-key vigenere cipher*, jika panjang kunci lebih pendek dari panjang plainteks, maka kunci disambung dengan plainteks tersebut. Cara kerja dari *auto-key vigenere cipher* adalah karakter plainteks-nya digunakan sebagai kunci. Kemudian kunci yang dimasukkan akan digunakan sebagai karakter awal kunci. Apabila plainteks yang digunakan lebih panjang plainteks tersebut akan dimasukkan sebagai kunci. (Safei, 2012)

3. *Running-key vigenere cipher*

   Pada varian ini, kunci bukan karakter pendek yang diulang secara periodik seperti pada *vigenere cipher* standar, tetapi kunci adalah karakter yang sangat panjang yang diambil dari teks yang bermakna (misalnya naskah proklamasi, naskah Pembukaan UUD 1945, dan lain-lain).

Secara matematis, rumus enkripsi dan dekripsi *vigenere cipher* adalah sebagi berikut:

Enkripsi : $C_i = (P_i + k_i)\ mod\ 26$

Dekripsi : $P_i = (C_i - k_i)\ mod\ 26$

Dimana,

P_i : Nilai karakter plainteks ke-i

C_i : Nilai karakter cipherteks ke-i

K_i : Nilai karakter kunci ke-i

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

(Munir, 2019)

2.4.3. Proses Enkripsi

Plainteks yang digunakan adalah **"THE DOG WENT ROUND THE HYDRANT THE CAT INTO THE HIGHEST SPOT HE COULD FIND"**. Berikut ini enkripsi menggunakan varian *vigenere cipher*.

1. *Full vigenere cipher*

   Kunci: SCRAM

Plainteks	T	H	E	D	O	G	W	E	N	T
Kunci	S	C	R	A	M	S	C	R	A	M
Plainteks	R	O	U	N	D	T	H	E	H	Y
Kunci	S	C	R	A	M	S	C	R	A	M
Plainteks	D	R	A	N	T	T	H	E	C	A
Kunci	S	C	R	A	M	S	C	R	A	M
Plainteks	T	I	N	T	O	T	H	E	H	I
Kunci	S	C	R	A	M	S	C	R	A	M
Plainteks	G	H	E	S	T	S	P	O	T	H
Kunci	S	C	R	A	M	S	C	R	A	M
Plainteks	E	C	O	U	L	D	F	I	N	D
Kunci	S	C	R	A	M	S	C	R	A	M

Cipherteks: “LJV DAY YVNF JQLNP LJV HKVTRNF LJV CML KETA LJV HUYJVSF KRFT TW EFUXV HZNP”

2. *Auto-key vigenere cipher*

   Dengan menggunakan kata kunci “SCRAM” yang digabungkan dengan sebagaian plainteks.

   Kunci: “SCRAMTHEDOGWENTROUNDTHEHYDRANTTHEC ATINTOTHEHIGHESTSPOTHECOULD”

Plainteks	T	H	E	D	O	G	W	E	N	T
Kunci	S	C	R	A	M	T	H	E	D	O
Plainteks	R	O	U	N	D	T	H	E	H	Y
Kunci	G	W	E	N	T	R	O	U	N	D
Plainteks	D	R	A	N	T	T	H	E	C	A
Kunci	T	H	E	H	Y	D	R	A	N	T
Plainteks	T	I	N	T	O	T	H	E	H	I
Kunci	T	H	E	C	A	T	I	N	T	O
Plainteks	G	H	E	S	T	S	P	O	T	H
Kunci	T	H	E	H	I	G	H	E	S	T
Plainteks	E	C	O	U	L	D	F	I	N	D
Kunci	S	P	O	T	H	E	C	O	U	L

   Cipherteks: “LJV DAZ DIQH XKYAW KVY UBWYEUR WYE PTM PRVO MPR AWZOIZB YWSL AW RCNSH HWHO”

3. *Running-key vigenere cipher*

   Kunci: “KERAKYATAN YANG DIPIMPIN OLEH HIKMAT KEBIJAKSANAAN DALAM PERMUSYAWA”

Plainteks	T	H	E	D	O	G	W	E	N	T
Kunci	K	E	R	A	K	Y	A	T	A	N
Plainteks	R	O	U	N	D	T	H	E	H	Y
Kunci	Y	A	N	G	D	I	P	I	M	P
Plainteks	D	R	A	N	T	T	H	E	C	A
Kunci	I	N	O	L	E	H	H	I	K	M
Plainteks	T	I	N	T	O	T	H	E	H	I
Kunci	A	T	K	E	B	I	J	A	K	S
Plainteks	G	H	E	S	T	S	P	O	T	H
Kunci	A	N	A	A	N	D	A	L	A	M
Plainteks	E	C	O	U	L	D	F	I	N	D
Kunci	P	E	R	M	U	S	Y	A	W	A

Cipherteks: “DLV DYE WXNG POHTG BWM TNLEOYX AOM MMT BXXP BQE RAGUESG VPZT TT GFGF BIJD”

2.4.4. Proses Dekripsi

Berikut merupakan proses dekripsi menggunakan 3 variasi metode *vigenere cipher.*

1. *Full vigenere cipher*

   Cipherteks: “LJV DAY YVNF JQLNP LJV HKVTRNF LJV CML KETA LJV HUYJVSF KRFT TW EFUXV HZNP”

   Kunci: “SCRAM”

Plainteks	L	J	V	D	A	Y	Y	V	N	F
Kunci	S	C	R	A	M	S	C	R	A	M
Plainteks	J	Q	L	N	P	L	J	V	H	K

Kunci	S	C	R	A	M	S	C	R	A	M
Plainteks	V	T	R	N	F	L	J	V	C	M
Kunci	S	C	R	A	M	S	C	R	A	M
Plainteks	L	K	E	T	A	L	J	V	H	U
Kunci	S	C	R	A	M	S	C	R	A	M
Plainteks	Y	J	V	S	F	K	R	F	T	T
Kunci	S	C	R	A	M	S	C	R	A	M
Plainteks	W	E	F	U	X	V	H	Z	N	P
Kunci	S	C	R	A	M	S	C	R	A	M

Sehingga didapatkan plainteks “THE DOG WENT ROUND THE HYDRANT THE CAT INTO THE HIGHEST SPOT HE COULD FIND”.

2. *Auto-key vigenere cipher*

Cipherteks: “LJV DAZ DIQH XKYAW KVY UBWYEUR WYE PTM PRVO MPR AWZOIZB YWSL AW RCNSH HWHO”

Kunci: “SCRAMTHEDOGWENTROUNDTHEHYDRANTTHECATI NTOTHEHIGHESTSPOTHECOULD”

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

Plainteks	Z	O	I	Z	B	Y	W	S	L	A
Kunci	T	H	E	H	I	G	H	E	S	T
Plainteks	W	R	C	N	S	H	H	W	H	O
Kunci	S	P	O	T	H	E	C	O	U	L

Sehingga didapatkan plainteks “THE DOG WENT ROUND THE HYDRANT THE CAT INTO THE HIGHEST SPOT HE COULD FIND”.

3. *Running-key vigenere cipher*

Cipherteks: “DLV DYE WXNG POHTG BWM TNLEOYX AOM MMT BXXP BQE RAGUESG VPZT TT GFGFV BIJD”

Kunci: “KERAKYATAN YANG DIPIMPIN OLEH HIKMATKEBIJAK SANAAN DALAM PERMUSYAWA”

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

Sehingga didapatkan plainteks “THE DOG WENT ROUND THE HYDRANT THE CAT INTO THE HIGHEST SPOT HE COULD FIND”.

2.5. Route Cipher

Route cipher adalah cipher transposisi dimana kuncinya adalah rute mana yang akan diikuti saat membaca cipherteks dari blok yang dibuat dengan plainteks. Plainteks ditulis dalam kotak, lalu dibaca mengikuti rute yang dipilih. Adapun langkah penyelesaian menggunakan enkripsi dan dekripsi adalah sebagai berikut.

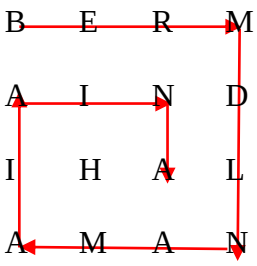
2.5.1. Proses Enkripsi

Enkripsi pesan merupakan proses mengubah pesan asli menjadi pesan yang susah dimengerti. Langkah pertama pada proses enkripsi metode *route cipher* adalah menuliskan plainteks di blok ukuran yang wajar untuk plainteks. Bagian dari kunci adalah grid. Sehingga menentukan sejumlah kolom atau sejumlah baris sebelum memulai. Begitu plainteks tertulis di grid, *route* yang ditugaskan berputar ke dalam dari sudut kanan atas searah jarum jam atau berlawanan jarum jam.

Contoh:

Plainteks : BERMAIN DI HALAMAN

Kunci : 4



Sehingga didapatkan cipherteks BERMDLNAMAIAINAH

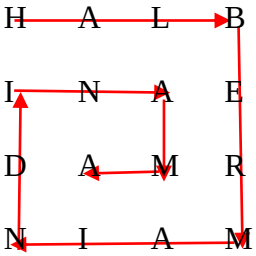
2.5.2. Proses Dekirpsi

Untuk mendekripsikan pesan yang diterima yang telah dikodekan dengan *route cipher*, rute yang digunakan yaitu lebar dan tinggi grid. Kemudian menyusun cipherteks dengan rute spiral berlawanan dengan arah jarum jam dari kanan atas.

Contoh:

Cipherteks : BERMAIN DI HALAMAN

Kunci : 4



Sehingga didapat plainteks BERMAIN DI HALAMAN. (Fitri, 2019)

Algoritma *route cipher* dapat dikatakan mempunyai proses enkripsi yang rumit. Hal tersebut dikarenakan *key* yang lebih membuat proses enkripsi dan dekripsi menjadi fleksibel. Bila panjang karakter tidak habis dibagi dengan panjang karakter, maka penambahan karakter secara *dummy* saat pengenkripsian. (Girsang, Siagian, Santoso, Wahyudi dan Sitorus, 2019)

2.6. Super Enkripsi

Super enkripsi merupakan suatu konsep yang menggunakan kombinasi dari dua atau lebih teknik subtitusi dan permutasi untuk mendapatkan suatu algoritma yang lebih andal (sulit dipecahkan). Teknik dari super enkripsi mudah dilakukan asal sudah memahami teknik subtitusi dan permutasi. Langkah-langkah yang perlu dilakukan adalah melakukan enkripsi pesan dengan menggunakan teknik subtitusi

dan teks kode yang dapat dienkripsi lagi menggunakan teknik transposisi (permutasi). (Ariyus, 2008)

2.6.1. Proses Enkripsi

Super enkripsi yang dapat dilakukan dengan melaukan enkripsi dengan menggunakan kedua cipher tersebut secara berurutan. Misalnya ada sebuah plainteks sebagai berikut:

Cipherteks : SAYA BERADA DI BANDUNG

Kunci : 3

Mula-mula lakukan enkripsi dengan menggunakan cipher subtitusi sehingga akan didapatkan cipherteks sebagai berikut:

"VDBD EHUDGD GL EDQGXQJ"

Selanjutnya enkripsi kembali cipherteks tersebut dengan menggunakan cipher transposisi dengan panjang kunci yang sama, yaitu 3 sehingga akan didapatkan hasil sebagai berikut:

V	D	B
D	E	H
U	D	G
D	G	L
E	D	Q
J	X	X

Pada akhir kolom ditambahkan dua buah karakter tambahan, yaitu 2 buah huruf X. Huruf X dipilih karena untuk mengisi kolom yang kosong. Karena cipherteks tersebut didapatkan juga dengan menggunakan cipher subtitusi, pemilihan huruf X dapat menyulitkan kriptanalis untuk memecahkan cipherteks

tersebut. Selanjutnya hanya perlu membaca blok-blok diatas dan akan didapat cipherteks akhir sebagai berikut:

VDUDEJDEDGDXBHGLQX

2.6.2. Proses Dekripsi

Untuk mengembalikan cipherteks tersebut menjadi plainteks yang memiliki mana, kita hanya perlu melakukan deskrip secara berurutan dengan menggunakan cipher subtitusi dan cipher transposisi namun urutannya ditukar. Mula-mula lakukan dekripsi dengan menggunakan cipher transposisi dengan jumlah kolom adalah 21 dibagi 3, yaitu 7 sehingga akan didapatkan blok-blok sebagai berikut:

V	D	U	D	E	G	J
D	E	D	G	D	X	X
B	H	G	L	Q	Q	X

Berdasarkan blok yang ada diatas, akan didapatkan cipherteks baru sebagai berikut:

VDBDEHUDGDGLEDQGXQJXX

Karena X dalam cipherteks tersebut tidak diketahui apakah merupakan tambahan atau karakter asli sehingga karakter tersebut tidak bisa langsung dihilangkan. Selanjutnya cipherteks tersebut didekripsi sekali lagi menggunakan cipher subtitusi dengan panjang kunci k=3 sehingga didapatkan plainteks sebagai berikut:

SAYABERADADIBANDUNGUU

Setelah didapatkan hasilnya, U merupakan karakter tambahan karena kata tersebut tidak memiliki makna yang bersesuaian dengan isi plainteks lain

sehingga kita bisa menghilangkannya. Setelah karakter tersebut dihapus sehingga susunan tersebut memiliki makna sebagai berikut:

SAYABERADADIBANDUNG

(Halim, 2007)

2.7. Pesan

Pesan dalam bahasa Prancis adalah *message*, berasal dari Bahasa latin "*missus*" artinya mengirim. Kata *message* digunakan sejak abad ke XI oleh para penutur atau partisipan komunikasi untuk mengatakan sesuatu yang kita kirimkan. Pesan pada dasarnya adalah komunikator yang disampaikan kepada komunikan (publik) baik secara langsung maupun melalui media. Pesan terdiri atas sekumpulan tanda-tanda yang dikelola berdasarkan kode-kode tertentu yang dipertukarkan antara komunikator dan komunikan melalui saluran. (Purwasito, 2017)

2.8. Integrasi Agama dalam Ilmu Kriptografi

Amanah menurut kamus besar bahasa Indonesia memiliki arti sesuatu yang dititipkan, sesuatu yang dipercayakan kepada orang lain. Sedangkan menurut Darimis, Amanah adalah sesuatu yang benar-benar bisa dipercaya. Dapat dipercaya disini memiliki maksud bahwasannya manusia yang diberi atau mendapat titipan sebuah amanah harus mampu melaksanakan dengan sungguh-sungguh dan dilaksanakan sesuai dengan apa yang sudah diamanahkan. Sedangkan menurut M. Quraish Shihab, amanah merupakan sesuatu yang diserahkan kepada pihak lain untuk dipelihara dan dikembalikan bila tiba saatnya atau bila diminta oleh pemiliknya.

Menjaga keamanan pesan merupakan sebuah amanah yang harus dijaga karena hal ini merupakan suatu yang sangat penting. Hal ini telah diterangkan dalam Al-Qur'an yaitu tentang amanah yang tercantum dalam surat An-anfal ayat 27:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَخُوْنُوا اللّٰهَ وَالرَّسُوْلَ وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ

Artinya:

Hai orang-orang yang beriman, janganlah kamu memgkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu menghianati amanat-amanat yang dipercayakan kepadamu.

Menurut Abu Ja'far, ayat tersebut membahas tentang bahwasannya Allah melarang orang-orang yang beriman mengkhianati Allah, Rasul-nya, dan amanah yang diamanatkan kepada mereka. Menurut Al mutsanna وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ memiliki penafsiran bahwa amanah adalah amal-amal yang diamanahkan Allah kepada para hambanya maksudnya yaitu kewajiban yang telah diberikan kepada hambanya. Sedangkan menurut Ali bin Daud,يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَخُوْنُوا اللّٰهَ memiliki penafsiran amanah adalah amal-amal.

Sikap tanggung jawab dan dapat dipercaya merupakan komponen-komponen amanah yang dapat dilihat dalam kehidupan seseorang dalam bermasyarakat. Amanah dapat menunjukkan kualitas dan derajat keimanan seseorang. Dengan mengimplementasikan amanah yang sesuai dengan perintah dan larangan dari Allah, maka manusia akan terselamatkan kehidupannya, baik didunia maupun diakhirat. Manusia yang menjalankan amanah Allah maka disebut manusia yang beriman sedangkan manusia yang tidak menjalankan amanah terhadap perintah dan larangan Allah maka disebut khianat. (Somad, Abdul, Hamdani, Yusuf dan Taslim, 2008)

Dalam hadist lain Rasulullah memberikan penegasan tentang amanah dan pengkhianatan:

فَإِذَا ضُيِّعَتْ الأَمَانَةُ فَانْتَظِرْ السَّاعَةَ قَالَ كَيْفَ إِضَاعَتُهَا قَالَ إِذَا وُسِّدَ الأَمْرُ إِلَى غَيْرِ أَهْلِهِ فَانْتَظِرْ السَّاعَة

Artinya:

Apabila sudah hilang amanah maka tunggulah terjadinya kiamat. Mereka bertanya:"Bagaimana hilangnya amanah itu?" Nabi SAW menjawab:"Jika urusan. diserahkan bukan kepada ahlinya, maka tunggulah terjadinya kiamat".(H.R. Bukhari)

Manusia sebagai makhluk yang mendapatkan amanah dalam kenyataannya tidak selalu dapat menjaga dan menjalankan amanah tersebut. Banyak manusia yang menyia-nyiakan kepercayaan yang telah diberikan kepadanya. Namun, karena hal tersebut sering dan biasa dilakukan sehingga manusia menganggapnya sebuah perbuatan yang wajar seakan-akan bukanlah suatu hal yang melanggar amanah padahal menjaga amanah tetaplah bersumber dari hidayah dan bimbingan Allah. (Ahmad, Hermawan dan Suhartini, 2020)

BAB III

PEMBAHASAN

Bab ini berisi proses enkripsi dan dekripsi pesan menggunakan dua metode atau biasa disebut dengan metode super enkripsi yang mana pada proses ini menggunakan metode subtitusi dan transposisi. Metode yang digunakan pada penelitian ini yaitu *vigenere cipher* yang merupakan metode subtitusi dan *route cipher* sebagai metode transposisi. Adapun langkah-langkah yang digunakan pada proses enkripsi yaitu melakukan enkripsi menggunaan metode *vigenere cipher*, setelah mendapatkan hasil enkripsinya dilanjut enkripsi menggunakan metode *route cipher*. Langkah-langkah proses dekripsi yaitu dengan melakukan dekripsi menggunakan metode *route cipher*, setelah mendapatkan hasil dekripsinya dilanjut melakukan dekripsi menggunakan metode *vigenere cipher*.

3.1. Proses Enkripsi Pesan Menggunakan Metode *Vigenere Cipher* dan *Route Cipher*

Berikut ini merupakan langkah-langkah pada proses enkripsi pesan menggunakan metode *vigenere cipher* dan *route cipher*. Langkah awal pada proses enkripsi pesan ini yaitu mengenkripsi pesan menggunakan metode *vigenere cipher*.

a. Enkripsi menggunakan varian *full vigenere cipher*

1. Menentukan pesan asli (plainteks).

   Pesan asli yang digunakan adalah “JOMBANG KOTA BERIMAN”. Pesan tersebut terdiri dari 18 karakter. Berikut ini pesan asli (plainteks) yang telah dikodekan sesuai konversi alphabet

Tabel 3. 1 Nilai Setiap Karakter Plainteks Variasi Full Vigenere Vipher

P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}
J	O	M	B	A	N	G	K	O	T	A
9	14	12	1	0	13	6	10	14	19	0

P_{12}	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}
B	E	R	I	M	A	N
1	4	17	8	12	0	13

Keterangan:

P_i = Plainteks

2. Menentukan kunci variasi *full vigenere cipher*.

   Kunci yang digunakan adalah "ZFTL". Berikut ini adalah kunci dari setiap karakter pesan asli.

Tabel 3. 2 Nilai Karakter Kunci Full Vigenere Cipher

K_1	K_2	K_3	K_4
Z	F	T	L
25	5	19	11

Tabel 3. 3 Kunci dari Setiap Karakter Plainteks Full Vigenere Cipher

K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
J	O	M	B	A	N	G	K	O	T	A
Z	F	T	L	Z	F	T	L	Z	F	T

K_{12}	K_{13}	K_{14}	K_{15}	K_{16}	K_{17}	K_{18}
B	E	R	I	M	A	N
L	Z	F	T	L	Z	F

3. Melakukan perhitungan menggunakan rumus $C_i = (P_i + K_i)\ mod\ 26$ dengan kunci K= ZFTL.

   $C_1\ (J, Z) = (P_1 + K_1)\ mod\ 26 = (9 + 25)\ mod\ 26 = 34\ mod\ 26 = 8$

$C_2\ (O,F) = (P_2 + K_2)\ mod\ 26 = (14 + 5)\ mod\ 26 = 19\ mod\ 26 = 19$

$C_3\ (M,T) = (P_3 + K_3)\ mod\ 26 = (12 + 19)\ mod\ 26 = 31\ mod\ 26 = 5$

$C_4\ (B,L) = (P_4 + K_4)\ mod\ 26 = (1 + 11)\ mod\ 26 = 12\ mod\ 26 = 12$

$C_5\ (A,Z) = (P_5 + K_5)\ mod\ 26 = (0 + 25)\ mod\ 26 = 25\ mod\ 26 = 25$

$C_6\ (N,F) = (P_6 + K_6)\ mod\ 26 = (13 + 5)\ mod\ 26 = 18\ mod\ 26 = 18$

$C_7\ (G,T) = (P_7 + K_7)\ mod\ 26 = (6 + 19)\ mod\ 26 = 25\ mod\ 26 = 25$

$C_8\ (K,L) = (P_8 + K_8)\ mod\ 26 = (10 + 11)\ mod\ 26 = 21\ mod\ 26 = 21$

$C_9\ (O,Z) = (P_9 + K_9)\ mod\ 26 = (14 + 25)\ mod\ 26 = 39\ mod\ 26 = 13$

$C_{10}\ (T,F) = (P_{10} + K_{10})\ mod\ 26 = (19 + 5)\ mod\ 26 = 24\ mod\ 26 =$
24

$C_{11}\ (A,T) = (P_{11} + K_{11})\ mod\ 26 = (0 + 19)\ mod\ 26 = 19\ mod\ 26 =$
19

$C_{12}\ (B,L) = (P_{12} + K_{12})\ mod\ 26 = (1 + 11)\ mod\ 26 = 12\ mod\ 26 =$
12

$C_{13}\ (E,Z) = (P_{13} + K_{13})\ mod\ 26 = (4 + 25)\ mod\ 26 = 29\ mod\ 26 = 3$

$C_{14}\ (R,F) = (P_{14} + K_{14})\ mod\ 26 = (17 + 5)\ mod\ 26 = 22\ mod\ 26 =$
22

$C_{15}\ (I,T) = (P_{15} + K_{15})\ mod\ 26 = (8 + 19)\ mod\ 26 = 27\ mod\ 26 = 1$

$C_{16}\ (M,L) = (P_{16} + K_{16})\ mod\ 26 = (12 + 11)\ mod\ 26 = 23\ mod\ 26 =$
23

$C_{17}\ (A,Z) = (P_{17} + K_{17})\ mod\ 26 = (0 + 25)\ mod\ 26 = 25\ mod\ 26 =$
25

$C_{18}\ (N,F) = (P_{18} + K_{18})\ mod\ 26 = (13 + 5)\ mod\ 26 = 18\ mod\ 26 =$
18

4. Mendapatkan hasil enkripsi variasi *full vigenere cipher*.

   Berdasarkan hasil enkripsi menggunakan metode *vigenere cipher*, sehingga didapatkan cipherteks "ITFMZSZVNYTMDWBXZS" dan berikut ini konversi cipherteks ke dalam tabel.

Tabel 3. 4 Konversi Nilai Proses Enkripsi Metode Subtitusi Variasi Full

C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}
9	6	3	9	0	5	23	18	14	11	17
I	T	F	M	Z	S	Z	V	N	Y	T

C_{12}	C_{13}	C_{14}	C_{15}	C_{16}	C_{17}	C_{18}
9	4	9	25	20	0	5
M	D	W	B	X	Z	S

Setelah melakukan enkripsi menggunakan metode *vigenere cipher* maka selanjutnya mengenkripsi pesan menggunakan metode *route cipher*. Berikut langkah-langkah proses enkripsi menggunakan metode *route cipher*.

1. Menentukan kunci *route cipher*

   Pada proses ini kunci yang digunakan adalah K=3.

2. Menyusun hasil enkripsi *vigenere cipher* sesuai kunci *route cipher* secara horizontal.

I T F

M Z S

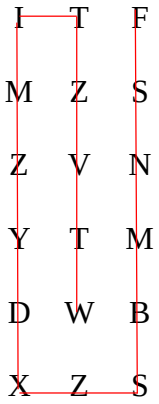
Z V N

Y T M

D W B

X Z S

3. Menyusun hasil enkripsi dari kanan atas ke bawah berbentuk spiral searah jarum jam.



4. Sehingga didapatkan hasil enkripsi (cipherteks) dari metode *route cipher* "FSNMBSZXDYZMITZVTW".

b. Enkripsi menggunakan varian *auto-key vigenere cipher*

1. Menentukan pesan asli (plainteks).

   Pesan asli yang digunakan adalah "JOMBANG KOTA BERIMAN" . Pesan tersebut terdiri dari 18 karakter. Berikut ini pesan asli (plainteks) yang telah dikodekan sesuai konversi alphabet.

Tabel 3. 5 Nilai Karakter Plainteks Variasi Auto-key

P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}
J	O	M	B	A	N	G	K	O	T	A
9	14	12	1	0	13	6	10	14	19	0

P_{12}	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}
B	E	R	I	M	A	N
1	4	17	8	12	0	13

Keterangan:

P_i = Plainteks

2. Menentukan kunci *variasi auto-key vigenere cipher*

   Kunci yang digunakan adalah "ZFTLJOMBANGJOTABER" yang kemudian disambung dengan plainteks. Berikut ini adalah kunci dari setiap karakter pesan asli.

Tabel 3. 6 Nilai Karakter Kunci Auto-key

K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
Z	F	T	L	J	O	M	B	A	N	G
25	5	11	19	9	14	12	1	0	13	6

K_{12}	K_{13}	K_{14}	K_{15}	K_{16}	K_{17}	K_{18}
K	O	T	A	B	E	R
10	14	19	0	1	4	17

Tabel 3. 7 Kunci dari Setiap Karakter Plainteks Variasi Auto-key

K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
J	O	M	B	A	N	G	K	O	T	A
Z	F	T	L	J	O	M	B	A	N	G

K_{12}	K_{13}	K_{14}	K_{15}	K_{16}	K_{17}	K_{18}
B	E	R	I	M	A	N
K	O	T	A	B	E	R

3. Melakukan perhitungan menggunakan rumus $C_i = (P_i + K_i)\ mod\ 26$ dengan kunci K= ZFTLJOMBANGKOTABER.

   $C_1\ (J, Z) = (P_1 + K_1)\ mod\ 26 = (9 + 25)\ mod\ 26 = 34\ mod\ 26 = 8$

   $C_2\ (O, F) = (P_2 + K_2)\ mod\ 26 = (14 + 5)\ mod\ 26 = 19\ mod\ 26 = 19$

   $C_3\ (M, T) = (P_3 + K_3)\ mod\ 26 = (12 + 19)\ mod\ 26 = 31\ mod\ 26 = 5$

   $C_4\ (B, L) = (P_4 + K_4)\ mod\ 26 = (1 + 11)\ mod\ 26 = 12\ mod\ 26 = 12$

   $C_5\ (A, J) = (P_5 + K_5)\ mod\ 26 = (0 + 9)\ mod\ 26 = 9\ mod\ 26 = 9$

$C_6\ (N, O) = (P_6 + K_6)\ mod\ 26 = (13 + 14)\ mod\ 26 = 27\ mod\ 26 = 1$

$C_7\ (G, M) = (P_7 + K_7)\ mod\ 26 = (6 + 12)\ mod\ 26 = 18\ mod\ 26 = 18$

$C_8\ (K, B) = (P_8 + K_8)\ mod\ 26 = (10 + 1)\ mod\ 26 = 11\ mod\ 26 = 11$

$C_9\ (O, A) = (P_9 + K_9)\ mod\ 26 = (14 + 0)\ mod\ 26 = 14\ mod\ 26 = 14$

$C_{10}\ (T, N) = (P_{10} + K_{10})\ mod\ 26 = (19 + 13)\ mod\ 26 = 32\ mod\ 26 = 6$

$C_{11}\ (A, G) = (P_{11} + K_{11})\ mod\ 26 = (0 + 6)\ mod\ 26 = 6\ mod\ 26 = 6$

$C_{12}\ (B, K) = (P_{12} + K_{12})\ mod\ 26 = (1 + 10)\ mod\ 26 = 11\ mod\ 26 = 11$

$C_{13}\ (E, O) = (P_{13} + K_{13})\ mod\ 26 = (4 + 14)\ mod\ 26 = 18\ mod\ 26 = 18$

$C_{14}\ (R, T) = (P_{14} + K_{14})\ mod\ 26 = (17 + 19)\ mod\ 26 = 36\ mod\ 26 = 10$

$C_{15}\ (I, A) = (P_{15} + K_{15})\ mod\ 26 = (8 + 0)\ mod\ 26 = 8\ mod\ 26 = 8$

$C_{16}\ (M, B) = (P_{16} + K_{16})\ mod\ 26 = (12 + 1)\ mod\ 26 = 13\ mod\ 26 = 13$

$C_{17}\ (A, E) = (P_{17} + K_{17})\ mod\ 26 = (0 + 4)\ mod\ 26 = 4\ mod\ 26 = 4$

$C_{18}\ (N, R) = (P_{18} + K_{18})\ mod\ 26 = (13 + 17)\ mod\ 26 = 30\ mod\ 26 = 4$

4. Mendapatkan hasil enkripsi variasi *auto-key vigenere cipher*.

   Berdasarkan hasil enkripsi menggunakan metode *vigenere cipher*, sehingga didapatkan cipherteks “ITFMJBSLOGGLSKINEE” dan berikut ini konversi cipherteks ke dalam tabel.

Tabel 3. 8 Konversi Nilai Proses Enkripsi Metode Subtitusi Variasi Auto-key

C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}
9	6	3	9	9	1	18	11	14	6	6
I	T	F	M	J	B	S	L	O	G	G

C_{12}	C_{13}	C_{14}	C_{15}	C_{16}	C_{17}	C_{18}
11	18	10	8	13	4	4
L	S	K	I	N	E	E

Setelah melakukan enkripsi menggunakan metode *vigenere cipher* maka selanjutnya mengenkripsi pesan menggunakan metode *route cipher*. Berikut langkah-langkah proses enkripsi menggunakan metode *route cipher*.

1. Menentukan kunci *route cipher*.

   Pada proses ini kunci yang digunakan adalah K=3.

2. Menyusun hasil enkripsi *vigenere cipher* sesuai kunci *route cipher* secara horizontal.

I T F

M J B

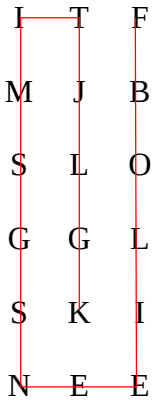
S L O

G G L

S K I

N E E

3. Menyusun hasil enkripsi dari kanan atas ke bawah berbentuk spiral searah jarum jam.



4. Sehingga didapatkan hasil enkripsi (cipherteks) dari metode *route cipher* "FBOLIEENSGSMITJLGK".

c. Enkripsi menggunaka variasi *running-key vigenere cipher*

1. Menentukan pesan asli (plainteks).

   Pesan asli yang digunakan adalah "JOMBANG KOTA BERIMAN" . Pesan tersebut terdiri dari 18 karakter. Berikut ini pesan asli (plainteks) yang telah dikodekan sesuai alphabet.

Tabel 3. 9 Nilai Karakter Plainteks Variasi Running-key

P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}
J	O	M	B	A	N	G	K	O	T	A
9	14	12	1	0	13	6	10	14	19	0

P_{12}	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}
B	E	R	I	M	A	N
1	4	17	8	12	0	13

Keterangan:

P_i = Plainteks

2. Menentukan kunci

Kunci yang digunakan adalah Pancasila sila ke 5 yang berbunyi "KEADILAN SOSIAL BAGI". Berikut ini adalah kunci dari setiap karakter pesan asli.

Tabel 3. 10 Nilai Karakter Kunci Variasi Running-key

K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
K	E	A	D	I	L	A	N	S	O	S
10	4	0	3	8	11	0	13	18	14	18

K_{12}	K_{13}	K_{14}	K_{15}	K_{16}	K_{17}	K_{18}
I	A	L	B	A	G	I
8	0	11	8	0	6	8

Tabel 3. 11 Kunci dari Setiap Karakter Plainteks Variasi Running-key

K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
J	O	M	B	A	N	G	K	O	T	A
K	E	A	D	I	L	A	N	S	O	S

K_{12}	K_{13}	K_{14}	K_{15}	K_{16}	K_{17}	K_{18}
B	E	R	I	M	A	N
I	A	L	B	A	G	I

3. Melakukan perhitungan menggunakan rumus $C_i = (P_i + K_i)\ mod\ 26$ dengan kunci K= KEADILANSOSIALBAGI.

$C_1\ (J, K) = (P_1 + K_1)\ mod\ 26 = (9 + 10)\ mod\ 26 = 19\ mod\ 26 = 19$

$C_2\ (O, E) = (P_2 + K_2)\ mod\ 26 = (14 + 4)\ mod\ 26 = 18\ mod\ 26 = 18$

$C_3\ (M, A) = (P_3 + K_3)\ mod\ 26 = (12 + 0)\ mod\ 26 = 12\ mod\ 26 = 12$

$C_4\ (B, D) = (P_4 + K_4)\ mod\ 26 = (1 + 3)\ mod\ 26 = 4\ mod\ 26 = 4$

$C_5\ (A, I) = (P_5 + K_5)\ mod\ 26 = (0 + 8)\ mod\ 26 = 8\ mod\ 26 = 8$

$C_6\ (N, L) = (P_6 + K_6)\ mod\ 26 = (13 + 11)\ mod\ 26 = 24\ mod\ 26 = 24$

$C_7\ (G, A) = (P_7 + K_7)\ mod\ 26 = (6 + 0)\ mod\ 26 = 6\ mod\ 26 = 6$

$C_8\ (K, N) = (P_8 + K_8)\ mod\ 26 = (10 + 13)\ mod\ 26 = 23\ mod\ 26 = 23$

$C_9\ (O, S) = (P_9 + K_9)\ mod\ 26 = (14 + 18)\ mod\ 26 = 32\ mod\ 26 = 6$

$C_{10}\ (T, O) = (P_{10} + K_{10})\ mod\ 26 = (19 + 14)\ mod\ 26 = 33\ mod\ 26 = 7$

$C_{11}\ (A, S) = (P_{11} + K_{11})\ mod\ 26 = (0 + 18)\ mod\ 26 = 18\ mod\ 26 = 18$

$C_{12}\ (B, I) = (P_{12} + K_{12})\ mod\ 26 = (1 + 8)\ mod\ 26 = 9\ mod\ 26 = 9$

$C_{13}\ (E, A) = (P_{13} + K_{13})\ mod\ 26 = (4 + 0)\ mod\ 26 = 4\ mod\ 26 = 4$

$C_{14}\ (R, L) = (P_{14} + K_{14})\ mod\ 26 = (17 + 11)\ mod\ 26 = 28\ mod\ 26 = 2$

$C_{15}\ (I, B) = (P_{15} + K_{15})\ mod\ 26 = (8 + 1)\ mod\ 26 = 9\ mod\ 26 = 9$

$C_{16}\ (M, A) = (P_{16} + K_{16})\ mod\ 26 = (12 + 0)\ mod\ 26 = 12\ mod\ 26 = 12$

$C_{17}\ (A, G) = (P_{17} + K_{17})\ mod\ 26 = (0 + 6)\ mod\ 26 = 6\ mod\ 26 = 6$

$C_{18}\ (N, I) = (P_{18} + K_{18})\ mod\ 26 = (13 + 8)\ mod\ 26 = 21\ mod\ 26 = 21$

4. Mendapatkan hasil enkripsi

   Berdasarkan hasil enkripsi menggunakan metode *vigenere cipher*, sehingga didapatkan cipherteks “TSMEIYGXGHSJECJMGV” dan berikut ini konversi cipherteks ke dalam tabel.

Tabel 3. 12 Konversi Nilai Enkripsi Metode Subtitusi Variasi Running-key

C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}
19	18	12	4	8	24	6	23	6	7	18
T	S	M	E	I	Y	G	X	G	H	S

C_{12}	C_{13}	C_{14}	C_{15}	C_{16}	C_{17}	C_{18}
9	4	2	9	12	6	21
J	E	C	J	M	G	V

Setelah melakukan enkripsi menggunakan metode *vigenere cipher* maka selanjutnya mengenkripsi pesan menggunakan metode *route cipher*. Berikut langkah-langkah proses enkripsi menggunakan metode *route cipher*.

1. Menentukan kunci *route cipher*.

   Pada proses ini kunci yang digunakan adalah K=3.

2. Menyusun hasil enkripsi *vigenere cipher* sesuai kunci *route cipher* secara horizontal.

T S M

E I Y

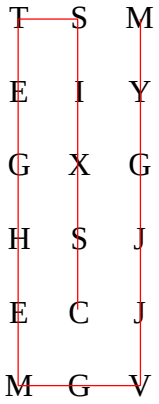
G X G

H S J

E C J

M G V

3. Menyusun hasil enkripsi dari kanan atas ke bawah berbentuk spiral searah jarum jam.



4. Sehingga didapatkan hasil enkripsi (cipherteks) dari metode *route cipher* "MYGJJVGMEHGETSIXSC".

Berdasarkan proses enkripsi menggunakan super enkripsi dengan metode *vigenere cipher* variasi *full vigenere cipher* dan *route cipher* didapatkan hasil enkripsi "DFOJZFAUELXJJGASRJ", hasil enkripsi dari metode *vigenere cipher* variasi *auto-key vigenere cipher* dan *route cipher* adalah "DBOLIEENSGSJJGJLGK" dan hasil enkripsi dari metode *vigenere cipher* variasi *running-key vigenere cipher* dan *route cipher* adalah "MYGJJVGMEHGETSIXSC".

3.2. Proses Dekripsi Menggunakan Super Enkripsi Metode *Vigenere Cipher* dan *Route Cipher*

Berikut ini merupakan langkah-langkah pada proses dekripsi pesan menggunakan metode *vigenere cipher* dan *route cipher*. Langkah awal yang dilakukan adalah dekripsi menggunakan metode *route cipher* yang dilanjut dengan metode *vigenere cipher*. Adapun langkah-langkahnya adalah sebagai berikut.

a. Langkah awal pada proses dekripsi pesan ini yaitu mendekripsi pesan menggunakan metode *route cipher* kemudian dilanjut dengan metode

vigenere cipher dengan variasi kunci *full vigenere cipher*. Berikut ini langkah-langkah dekripsi menggunakan metode *route cipher*.

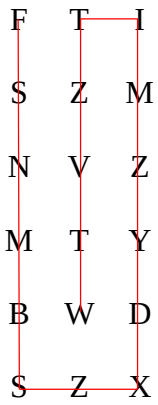
1. Menentukan cipherteks.

   Cipherteks dari metode *vigenere cipher* variasi full *vigenere cipher* dan metode *route cipher* adalah “FSNMBSZXDYZMITZVTW”.

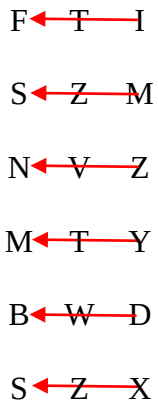
2. Menentukan kunci *route cipher*.

   Kunci yang digunakan pada proses dekripsi yaitu K=6.

3. Memasukkan cipherteks dan menyusun karater dari kiri atas ke bawah berbentuk spiral berlawanan dengan arah jarum jam.



4. Menyusun cipherteks secara horizontal dari kanan ke kiri.



Sehingga didapatkan plainteks *route cipher* “ITFMZSZVNYTMDWBXZS”

Setelah melakukan proses dekripsi menggunakan metode *route cipher*, langkah selanjutnya yaitu melakukan dekripsi menggunakan metode *vigenere cipher* variasi *full vigenere cipher*.. Berikut ini langkah-langkah dekripsi pesan menggunakan metode *vigenere cipher* variasi kunci full *vigenere cipher*

1. Menyusun cipherteks ke dalam tabel konversi

Tabel 3. 13 Nilai Karakter Cipherteks Variasi Full Vigenere Cipher

C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}
I	T	F	M	Z	S	Z	V	N	Y	T	M
8	19	5	12	25	18	25	21	13	24	19	12

C_{13}	C_{14}	C_{15}	C_{16}	C_{17}	C_{18}
D	W	B	X	Z	S
3	22	1	23	25	18

2. Menentukan kunci variasi *full vigenere cipher*.

   Kunci = “ZFTL”.

   Berikut ini adalah kunci beserta kode setiap karakter cipherteks.

Tabel 3. 14 Kunci Setiap Karakter Cipherteks Variasi Full Vigenere Cipher

K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
I	T	F	M	Z	S	Z	V	N	Y	T
Z	F	T	L	Z	F	T	L	Z	F	T

K_{12}	K_{13}	K_{14}	K_{15}	K_{16}	K_{17}	K_{18}
M	D	W	B	X	Z	S
L	Z	F	T	L	Z	F

3. Melakukan perhitungan menggunakan rumus $P_i = (C_i - K_i)\ mod\ 26$

$C_1\ (I, Z) = (P_1 - K_1)\ mod\ 26 = (8 - 25)\ mod\ 26 = -17\ mod\ 26 = 26 - (|-17|) mod\ 26 = 26 - 17\ mod\ 26 = 9\ \ mod\ 26 = 9$

$C_2\ (T, F) = (P_2 - K_2)\ mod\ 26 = (19 - 5)\ mod\ 26 = 14\ mod\ 26 = 14$

$C_3\ (F, T) = (P_3 - K_3)\ mod\ 26 = (5 - 19)\ mod\ 26 = -14\ mod\ 26 = 26 - (|-14|) mod\ 26 = 26 - 14\ mod\ 26 = 12\ mod\ 26 = 12$

$C_4\ (M, L) = (P_4 - K_4)\ mod\ 26 = (12 - 11)\ mod\ 26 = 1\ mod\ 26 = 1$

$C_5\ (Z, Z) = (P_5 - K_5)\ mod\ 26 = (25 - 25)\ mod\ 26 = 0\ mod\ 26 = 0$

$C_6\ (S, F) = (P_6 - K_6)\ mod\ 26 = (18 - 5)\ mod\ 26 = 13\ mod\ 26 = 13$

$C_7\ (Z, T) = (P_7 - K_7)\ mod\ 26 = (25 - 19)\ mod\ 26 = 6\ mod\ 26 = 6$

$C_8\ (V, L) = (P_8 - K_8)\ mod\ 26 = (21 - 11)\ mod\ 26 = 10\ mod\ 26 = 10$

$C_9\ (N, Z) = (P_9 - K_9)\ mod\ 26 = (13 - 25)\ mod\ 26 = -12\ mod\ 26 = 26 - (|-12|) mod\ 26 = 26 - 12\ mod\ 26 = 14\ mod\ 26 = 14$

$C_{10}\ (Y, F) = (P_{10} - K_{10})\ mod\ 26 = 24 - 5\ mod\ 26 = 19\ mod\ 26 = 19$

$C_{11}\ (T, T) = (P_{11} - K_{11})\ mod\ 26 = (19 - 19)\ mod\ 26 = 0\ mod\ 26 = 0$

$C_{12}\ (M, L) = (P_{12} - K_{12})\ mod\ 26 = (12 - 11)\ mod\ 26 = 1\ mod\ 26 = 1$

$C_{13}\ (D, Z) = (P_{13} - K_{13})\ mod\ 26 = (3 - 25)\ mod\ 26 = -22\ mod\ 26 = 26 - (|-22|) mod\ 26 = 26 - 22\ mod\ 26 = 4\ mod\ 26 = 4$

$C_{14}\ (W, F) = (P_{14} - K_{14})\ mod\ 26 = (22 - 5)\ mod\ 26 = 17\ mod\ 26 = 17$

$C_{15}\ (B, T) = (P_{15} - K_{15})\ mod\ 26 = (1 - 19)\ mod\ 26 = -18\ mod\ 26 = 26 - (|-18|) mod 26 = 26 - 18\ mod\ 26 = 8\ mod\ 26 = 8$

$C_{16}\ (X, L) = (P_{16} - K_{16})\ mod\ 26 = (23 - 11)\ mod\ 26 = 12\ mod\ 26 = 12$

$C_{17}\ (Z, Z) = (P_{17} - K_{17})\ mod\ 26 = (25 - 25)\ mod\ 26 = 0\ mod\ 26 = 0$

$C_{18}\ (S, F) = (P_{18} - K_{18})\ mod\ 26 = 18 - 5\ mod\ 26 = 13\ mod\ 26 = 13$

4. Mendapatkan hasil dekripsi metode *vigenere cipher* variasi *full vigenere cipher.*

Berdasarkan hasil dekripsi menggunakan metode *vigenere cipher*, sehingga didapatkan plainteks "JOMBANG KOTA BERIMAN" dan berikut ini konversi plainteks ke dalam tabel.

Tabel 3. 15 Konversi dari Proses Dekripsi Variasi Full Vigenere Cipher

P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}
9	14	12	1	0	13	6	10	14	19	0
J	O	M	B	A	N	G	K	O	T	A

P_{12}	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}
B	E	R	I	M	A	N
1	4	17	8	12	0	13

b. Langkah awal pada proses dekripsi pesan ini yaitu mendekripsi pesan menggunakan metode *route cipher* kemudian dilanjut dengan metode *vigenere cipher* dengan variasi kunci *auto-key vigenere cipher*. Berikut ini langkah-langkah dekripsi menggunakan metode *route cipher*.

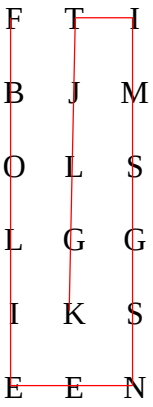
1. Menentukan cipherteks.

Cipherteks dari metode *vigenere cipher* variasi auto-key *vigenere cipher* dan metode *route cipher* adalah "FBOLIEENSGSMITJLGK".

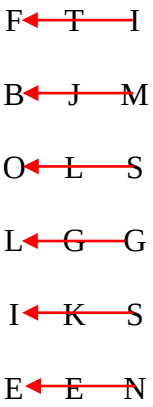
2. Menentukan kunci *route cipher*.

   Kunci yang digunakan pada proses dekripsi yaitu K= 6.

3. Memasukkan cipherteks dan menyusun karater dari kiri atas ke bawah berbentuk spiral berlawanan dengan arah jarum jam.



4. Menyusun cipherteks secara horizontal dari kanan ke kiri.



Sehingga didapatkan plainteks *route cipher* “ITFMJBSLOGGSLSKINEE”.

Setelah melakukan proses dekripsi menggunakan metode *route cipher*, langkah selanjutnya yaitu melakukan dekripsi menggunakan metode *vigenere cipher* variasi auto-key *vigenere cipher* menggunakan plainteks dari metode *vigenere cipher*.

Berikut ini langkah-langkah dekripsi pesan menggunakan metode *vigenere ciphe*

1. Menyusun cipherteks ke dalam tabel

Tabel 3. 16 Nilai Karakter Cipherteks Metode Subtitusi Variasi Auto-key

C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}
I	T	F	M	J	B	S	L	O	G	G	L
9	6	3	9	9	1	18	11	14	6	6	11

C_{13}	C_{14}	C_{15}	C_{16}	C_{17}	C_{18}
S	K	I	N	E	E
18	10	8	13	4	4

2. Menentukan kunci

Kunci = “ZFTLJOMBANGKOTABER”.

Berikut ini adalah kunci beserta kode setiap karakter cipherteks.

Tabel 3. 17 Kunci Dari Setiap Karakter Cipherteks Variasi Auto-key

K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
I	T	F	M	J	B	S	L	O	G	G
Z	F	T	L	J	O	M	B	A	N	G
25	5	19	11	9	14	12	1	0	13	6

K_{12}	K_{13}	K_{14}	K_{15}	K_{16}	K_{17}	K_{18}
L	S	K	I	N	E	E
K	O	T	A	B	E	R
10	14	19	0	1	4	17

3. Melakukan perhitungan menggunakan rumus $P_i = (C_i - K_i)\ mod\ 26$

$C_1\ (I, Z) = (P_1 - K_1)\ mod\ 26 = (8 - 25)\ mod\ 26 = -17\ mod\ 26 =$

$26 - (|-17|mod\ 26) = 26 - 17\ mod\ 26 = 9\ mod\ 26 = 9$

$C_2\ (T,F) = (P_2 - K_2)\ mod\ 26 = (19 - 5)\ mod\ 26 = 14\ mod\ 26 = 14$

$C_3\ (F,T) = (P_3 - K_3)\ mod\ 26 = (5 - 19)\ mod\ 26 = -14\ mod\ 26 =$

$26 - (|-14|mod\ 26) = 26 - 14\ mod\ 26 = 12\ mod\ 26 = 12$

$C_4\ (M,L) = (P_4 - K_4)\ mod\ 26 = (12 - 11)\ mod\ 26 = 1\ mod\ 26 = 1$ \

$C_5\ (J,J) = (P_5 - K_5)\ mod\ 26 = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0$

$C_6\ (B,O) = (P_6 - K_6)\ mod\ 26 = (1 - 14)\ mod\ 26 = -13\ mod\ 26 =$

$26 - (|-13|mod\ 26) = 26 - 13\ mod\ 26 = 13\ mod\ 26 = 13$

$C_7\ (S,M) = (P_7 - K_7)\ mod\ 26 = (18 - 12)\ mod\ 26 = 6\ mod\ 26 = 6$

$C_8\ (L,B) = (P_8 - K_8)\ mod\ 26 = (11 - 1)\ mod\ 26 = 10\ mod\ 26 = 10$

$C_9\ (O,A) = (P_9 - K_9)\ mod\ 26 = (14 - 0)\ mod\ 26 = 14\ mod\ 26 = 14$

$C_{10}\ (G,N) = (P_{10} - K_{10})\ mod\ 26 = (6 - 13)\ mod\ 26 = -7\ mod\ 26 =$

$26 - (|-7|mod\ 26) = 26 - 7\ mod\ 26 = 19\ mod\ 26 = 19$

$C_{11}\ (G,G) = (P_{11} - K_{11})\ mod\ 26 = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0$

$C_{12}\ (L,K) = (P_{12} - K_{12})\ mod\ 26 = (11 - 10)\ mod\ 26 = 1\ mod\ 26 = 1$

$C_{13}\ (S,O) = (P_{13} - K_{13})\ mod\ 26 = (18 - 14)\ mod\ 26 = 4\ mod\ 26 = 4$

$C_{14}\ (K,T) = (P_{14} - K_{14})\ mod\ 26 = (10 - 19)\ mod\ 26 = -9\ mod\ 26 =$

$26 - (|-9|mod\ 26) = 26 - 9\ mod\ 26 = 17\ mod\ 26 = 17$

$C_{15}\ (I,A) = (P_{15} - K_{15})\ mod\ 26 = (8 - 0)\ mod\ 26 = 8\ mod\ 26 = 8$

$C_{16}\ (N,B) = (P_{16} - K_{16})\ mod\ 26 = (13 - 1)\ mod\ 26 = 12\ mod\ 26 =$

12

$C_{17}\ (E,E) = (P_{17} - K_{17})\ mod\ 26 = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0$

$C_{18}\ (E,R) = (P_{18} - K_{18})\ mod\ 26 = (4 - 17)\ mod\ 26 = -13\ mod\ 26 =$

$26 - (|-13|)\ mod\ 26 = 26 - 13\ mod\ 26 = 13\ mod\ 26 = 13$

4. Mendapatkan hasil dekripsi metode *vigenere cipher* variasi *auto-key vigenere cipher*.

Berdasarkan hasil dekripsi menggunakan metode *vigenere cipher*, sehingga didapatkan plainteks "JOMBANG KOTA BERIMAN" dan berikut ini konversi plainteks ke dalam table.

Tabel 3. 18 Konversi Dari Proses Dekripsi Variasi Auto-key

P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}
9	14	12	1	0	13	6	10	14	19	0
J	O	M	B	A	N	G	K	O	T	A

P_{12}	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}
1	4	17	8	12	0	13
B	E	R	I	M	A	N

c. Langkah awal pada proses dekripsi pesan ini yaitu mendekripsi pesan *vigenere cipher* menggunakan metode *route cipher* kemudian dilanjut dengan metode *vigenere cipher* dengan variasi kunci *running-key vigenere cipher*. Berikut ini langkah-langkah dekripsi menggunakan metode *route cipher*.

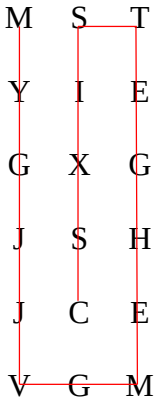
1. Menentukan cipherteks.

   Cipherteks dari metode *vigenere cipher* variasi *running-key vigenere cipher* dan *route cipher* adalah "MYGJJVGMEHGETSIXSC".

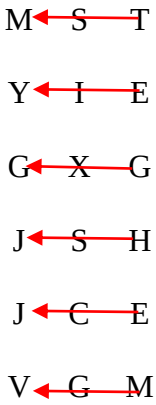
2. Menentukan kunci.

   Kunci yang digunakan pada proses dekripsi yaitu K=6.

3. Memasukkan cipherteks dan menyusun karater dari kiri atas ke bawah berbentuk spiral berlawanan dengan arah jarum jam.



4. Menyusun cipherteks secara horizontal dari kanan ke kiri.



Sehingga didapatkan plainteks *route cipher* “TSMEIYGXGHSJECJMGV”.

Setelah melakukan proses dekripsi menggunakan metode *route cipher*, langkah selanjutnya yaitu melakukan dekripsi menggunakan metode *vigenere cipher* variasi *running-key vigenere cipher* menggunakan plainteks dari metode *vigenere cipher*.

Berikut ini langkah-langkah dekripsi pesan menggunakan metode *vigenere cipher*.

1. Menyusun cipherteks ke dalam tabel konversi

Tabel 3. 19 Nilai Karakter Cipherteks

C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}
T	S	M	E	I	Y	G	X	G	H	S	J
12	18	19	24	11	4	6	23	6	9	18	7

C_{13}	C_{14}	C_{15}	C_{16}	C_{17}	C_{18}
E	C	J	M	G	V
9	2	4	21	9	12

2. Menentukan kunci

Kunci = “KEADILANSOSIALBAGI”.

Berikut ini adalah kunci beserta kode setiap karakter cipherteks.

Tabel 3. 20 Kunci Dari Setiap Karakter Cipherteks

K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
T	S	M	E	I	Y	G	X	G	H	S
K	E	A	D	I	L	A	N	S	O	S
10	4	0	3	8	11	0	13	18	14	18

K_{12}	K_{13}	K_{14}	K_{15}	K_{16}	K_{17}	K_{18}
J	E	C	J	M	G	V
I	A	L	B	A	G	I
8	0	11	1	0	6	8

3. Melakukan perhitungan menggunakan rumus $P_i = (C_i - K_i)\ mod\ 26$

$C_1\ (T, K) = (P_1 - K_1)\ mod\ 26 = (19 - 10)\ mod\ 26 = 9\ mod\ 26 = 9$

$C_2\ (S,E) = (P_2 - K_2)\ mod\ 26 = (18-4)\ mod\ 26 = 14\ mod\ 26 = 14$

$C_3\ (M,A) = (P_3 - K_3)\ mod\ 26 = (12-0)\ mod\ 26 = 12\ mod\ 26 = 12$

$C_4\ (E,D) = (P_4 - K_4)\ mod\ 26 = (4-3)\ mod\ 26 = 1\ mod\ 26 = 1$ \

$C_5\ (I,I) = (P_5 - K_5)\ mod\ 26 = (0-0)\ mod\ 26 = 0\ mod\ 26 = 0$

$C_6\ (Y,L) = (P_6 - K_6)\ mod\ 26 = (24-11)\ mod\ 26 = 13\ mod\ 26 = 13$

$C_7\ (G,A) = (P_7 - K_7)\ mod\ 26 = (6-0)\ mod\ 26 = 6\ mod\ 26 = 6$

$C_8\ (X,N) = (P_8 - K_8)\ mod\ 26 = (23-13)\ mod\ 26 = 10\ mod\ 26 = 10$

$C_9\ (G,S) = (P_9 - K_9)\ mod\ 26 = (6-18)\ mod\ 26 = -12\ mod\ 26 =$

$26 - (|-12|mod\ 26) = 26 - 12\ mod\ 26 = 14\ mod\ 26 = 14$

$C_{10}\ (H,O) = (P_{10} - K_{10})\ mod\ 26 = (7-14)\ mod\ 26 = -7\ mod\ 26 =$

$26 - (|-7|mod\ 26) = 26 - 7\ mod\ 26 = 19\ mod\ 26 = 19$

$C_{11}\ (S,S) = (P_{11} - K_{11})\ mod\ 26 = (0-0)\ mod\ 26 = 0\ mod\ 26 = 0$

$C_{12}\ (J,I) = (P_{12} - K_{12})\ mod\ 26 = (9-1)\ mod\ 26 = 1\ mod\ 26 = 1$

$C_{13}\ (E,A) = (P_{13} - K_{13})\ mod\ 26 = (4-0)\ mod\ 26 = 4\ mod\ 26 = 4$

$C_{14}\ (C,L) = (P_{14} - K_{14})\ mod\ 26 = (2-11)\ mod\ 26 = -9\ mod\ 26 =$

$26 - (|-9|mod\ 26) = 26 - 9\ mod\ 26 = 17\ mod\ 26 = 17$

$C_{15}\ (J,B) = (P_{15} - K_{15})\ mod\ 26 = (9-1)\ mod\ 26 = 8\ mod\ 26 = 8$

$C_{16}\ (M,A) = (P_{16} - K_{16})\ mod\ 26 = (12-0)\ mod\ 26 = 12\ mod\ 26 =$

12

$C_{17}\ (G,G) = (P_{17} - K_{17})\ mod\ 26 = (0-0)\ mod\ 26 = 0\ mod\ 26 = 0$

$C_{18}\ (V,I) = (P_{18} - K_{18})\ mod\ 26 = (21-8)\ mod\ 26 = -13\ mod\ 26 =$

$26 - (|-13|)\ mod\ 26 = 26 - 13\ mod\ 26 = 13\ mod\ 26 = 13$

4. Mendapatkan hasil dekripsi metode *vigenere cipher* variasi *running-key vigenere cipher*.

   Berdasarkan hasil dekripsi menggunakan metode *vigenere cipher*, sehingga didapatkan plainteks "JOMBANG KOTA BERIMAN" dan berikut ini konversi plainteks ke dalam tabel.

Tabel 3. 21 Konversi Dari Proses Dekripsi

P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}
9	14	12	1	0	13	6	10	14	19	0
J	O	M	B	A	N	G	K	O	T	A

P_{12}	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}
1	4	17	8	12	0	13
B	E	R	I	M	A	N

Berdasarkan proses dekripsi menggunakan super enkripsi dengan metode *vigenere cipher* variasi *full vigenere cipher, auto-key vigenere cipher dan running-key vigenere cipher* dengan *route cipher* didapatkan hasil dekripsi "JOMBANGKOTABERIMAN".

3.3. Integrasi Agama dengan Kriptografi

Amanah merupakan kepercayaan yang telah diberikan kepada seseorang dan harus dijaga. Penyampain pesan tidaklah boleh berkurang sedikit pun dengan pesan yang telah disampaikan kepadanya. Sebagai manusia, hendaknya kita menjaga amanah yang telah diberikan karena amanah tersebut nantinya akan dipertanggungjawabkan diakhirat kelak. Adapun hadist yang menjelaskan ciri-ciri orang munafik, diantaranya yaitu:

1. Apabila berkata berdusta
2. Apabila berjanji mengingkari
3. Dan apabila dipercaya khianat.

Sama halnya dengan kriptografi, yang mana pesan yang telah disampaikan tidak berbeda dengan pesan awal yang telah disampaikan kepadanya.

BAB IV

PENUTUP

4.1. Kesimpulan

Berdasarkan hasil pembahasan, dapat ditarik kesimpulan sebagai berikut:

1. Pada proses enkripsi pesan menggunakan super enkripsi yang dilakukan menggunakan dua metode yaitu *vigenere cipher* dan *route cipher*. Proses enkripsi dengan metode *vigenere cipher* dilakukan sebanyak 3 kali sesuai dengan variasi yang digunakan yang kemudian setiap variasi tersebut dienkripsi lagi menggunakan *route cipher*. Menyiapkan plainteks, menentukan kunci, melakukan perhitungan menggunakan rumus $C_i = (P_i + k_i)\ mod\ 26$, setelah mendapatkan hasil enkripsi dilanjut dengan mengenkripsi menggunakan metode kedua yaitu *route cipher*. Karena proses enkripsi menggunakan 3 variasi, maka prosesnya yaitu dengan mengenkripsi variasi pertama kemudian dienkripsi lagi menggunakan *route cipher* sehingga didapatkan cipherteks, begitupun seterusnya sampai dengan variasi ketiga. Berdasarkan proses enkripsi menggunakan super enkripsi dengan metode *vigenere cipher* variasi *full vigenere cipher* dan *route cipher* didapatkan hasil enkripsi "DFOJZFAUELXJJGASRJ", hasil enkripsi dari metode *vigenere cipher* variasi *auto-key vigenere cipher* dan *route cipher* adalah "DBOLIEENSGSJJGJLGK" dan hasil enkripsi dari metode *vigenere cipher* variasi *running-key vigenere cipher* dan *route cipher* adalah "MYGJJVGMEHGETSIXSC".
2. Untuk mengembalikan cipherteks kebentuk pesan asli (plainteks) maka dengan melakukan dekripsi menggunakan metode *route cipher* dan kemudian

dilanjut dengan metode *vigenere cipher*. Sama halnya dengan proses enkripsi, metode *vigenere cipher* didekripsi sebanyak tiga kali sesuai dengan variasi yang digunakan. Adapun rumus proses dekripsi *vigenere cipher* $P_i = (C_i - k_i)\ mod\ 26$. Proses dekripsinya yaitu dengan mendekripsi menggunakan *route cipher* kemudian menggunakan variasi *vigenere cipher* yang pertama sehingga mendapatkan plainteks. Begitu seterusnya hingga variasi ketiga. Berdasarkan ketiga variasi tersebut, didapatkan hasil dekripsi "JOMBANG KOTA BERIMAN" sesuai dengan plainteks awal.

4.2. Saran

Untuk penelitian selanjutnya disarankan untuk menggunakan kunci dan karakter yang lebih bervariasi. Sedangkan untuk metode *route cipher* disarankan untuk menggunakan rute yang lebih bervariasi.

DAFTAR PUSTAKA

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

Ahmad, Nurwadjah, Hermawan, Iwan dan Suhartini, Andewi. 2020. "Konsep Amanah dalam Perspektif Pendidikan Islam." *Qalamuna - Jurnal Pendidikan, Sosial, dan Agama* 12 (2): 141-152.

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

Ariyus, Dony. 2008. *Pengantar ilmu kriptografi : Teori, analisis dan implementasi.* Yogyakarta: CV. Andi Offset.

Asnawati, Efrandi, dan Yupiyanti. 2014. "Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher." *Jurnal Media Infotama*. 10 (2): 120-128.

Fitri, Nova. 2019. Perancangan Aplikasi Penyandian File Teks Menggunakan Algoritma Route Cipher Berbasis Desktop. *Jurnal Pelita Informatika*. 8(1)

Girsang, Nardianti Dewi, Siagian, Heldawaty, Santoso, Hamdani M., Wahyudi, Agung dan Sitorus, Bunaya Arthavia. 2019. "Kombinasi Algoritma Kriptografi Transposisi Rail Fence Cipher dan Route Cipher." *Prosiding Seminar Nasional Teknologi Informatika*. 2 (1): 48-53.

Habibi, Azwar Riza, Hijriyah, Nurul dan Irawan, Wahyu Henky. 2014. *Pengantar Teori Bilangan.* Malang: UIN_MALIKI PRESS.

Halim, S. A. 2007. Super Enkripsi Dengan Menggunakan Cipher Subtitusi dan Cipher Transposisi. *Makalah F5054-2007-A-080*.

Munir, Rinaldi. 2019. *Kriptografi.* Bandung: Informatika.

Nasution, Darma Surya, Syahrizal, Muhammad, Ginting, Guidio Leonarde dan Rahim, Robbi. 2017. "Data Security Using Vigenere Cipher and Goldbach Codes Algorithm." *International Journal of Engineering Research & Technology (IJERT)* 6 (01): 360-363.

Purwasito, Andrik. 2017. "Analisis Pesan". *Journal The Messenger*. 9(1): 103-105.

Sadikin, Rifqi. 2012. *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java.* Yogyakarta: CV. Andi Offset.

Safei, Timotius Triputra. 2012. "Pengukuran dan Pengujian Kekuatan Algoritma Auto-key Vegenere Cipher." *Makalah IF3058* 1-6.

Somad, Abdul, Hamdani, Yusuf & Taslim, Anshari. 2008. *Tafsir Ath-Thabari.* Jakarta: Pustaka Azam

Tong, Koe Yao. 2008. *Memahami Teori Bilangan Dengan Mudah dan Menarik.* Jakarta: PT. Grasindo.

Wardani, Ayu Sasmita. 2016. “Aritmatika Modulo, Kongruen dan Balikan Modulo.”

RIWAYAT HIDUP

Zulfatul Aufia lahir di Jombang pada tanggal 16 Agustus 1998. Biasa dipanggil Zulfa atau Fia, namun kebanyakan dipanggil Zulfa. Tinggal di Dusun Buduran RT 003 RW 001, Desa Jogoloyo, Kecamatan Sumobito, Kabupaten Jombang. Anak bungsu dari dua bersaudara dari pasangan Bapak Abd Hamid dan Ibu Luluk Zunaidah. Pendidikan awal dimulai di RA Al-Ihsan yang lulus pada tahun 2005, menempuh pendidikan madrasah di MI Al-ihsan I Sawahan yang lulus pada tahun 2011, setelah itu melanjutkan pendidikan menengah pertama di MTsN Rejoso yang lulus pada tahun 2014. Kemudian melanjutkan pendidikan menengah atas di SMA Darul Ulum I Unggulan BPPT Jombang yang lulus pada tahun 2017. Setelah menempuh bangku SMA, pendidikannya dilanjutkan di Universitas Islam Negeri Maulana Malik Ibrahim Malang dan mengambil jurusan Matematika.

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

BUKTI KONSULTASI SKRIPSI

Nama : Zulfatul Aufia
NIM : 17610109
Fakultas/Prodi : Sains dan Teknologi/Matematika
Judul Skripsi : Enkripsi dan Dekripsi Pesan Menggunakan Metode *Vigenere Cipher* dan *Route Cipher*
Pembimbing : Prof. Dr. H. Turmudi, M.Si.,Ph.D
Pembimbing II : Evawati Alisah, M.Pd

No	Tanggal	Hal	Tanda Tangan
1	22 Maret 2021	Konsultasi Agama Bab 1	1.
2	25 Maret 2021	Konsultasi Daftar Isi dan Bab 1	2.
3	01 April 2021	Revisi Daftar Isi dan Bab 1	3.
4	06 April 2021	Revisi Daftar Isi, Kajian Pustaka dan Rumusan Masalah	4.
5	14 April 2021	Konsultasi Bab 3	5.
6	22 April 2021	Penambahan Defini Operasioanl	6.
7	29 April 2021	ACC Bab 1-3 oleh Dosen Pembimbing 1	7.
8	4 Mei 2021	ACC Bab 1-3 oleh Dosen Pembimbing 2	8.
9	19 Juni 2021	Konsultasi Revisi Seminar Proposal dengan Dosen Pembimbing 1	9.
10	23 Juni 2021	Penambahan Variasi dari Metode Vigenere Cipher	10.
11	26 Juni 2021	Revisi Bab 3	11.
12	27 Juni 2021	Konsultasi Revisi Seminar Proposal dengan Dosen Pembimbing 2	12.
13	19 Juli 2021	Konsultasi Bab 3	13.

14	4 Agustus 2021	ACC Keseluruhan oleh Dosen Pembimbing 1	14.
15	8 September 2021	ACC Keseluruhan oleh Dosen Pembimbing 2	15.

Malang, 29 September 2021
Mengetahui,
Ketua Program Studi Matematika

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