MODIFIKASI ALGORITMA SUPER ENKRIPSI *CAESAR CIPHER* DAN *ROUTE CIPHER* UNTUK MENGAMANKAN PESAN

SKRIPSI

OLEH:
ALI MAHFUDZ
NIM. 18610107

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2022

MODIFIKASI ALGORITMA SUPER ENKRIPSI *CAESAR CIPHER* DAN *ROUTE CIPHER* UNTUK MENGAMANKAN PESAN

SKRIPSI

OLEH:
ALI MAHFUDZ
NIM. 18610107

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2022

MODIFIKASI ALGORITMA SUPER ENKRIPSI *CAESAR CIPHER* DAN *ROUTE CIPHER* UNTUK MENGAMANKAN PESAN

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
ALI MAHFUDZ
NIM. 18610107

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2022

MODIFIKASI ALGORITMA SUPER ENKRIPSI *CAESAR CIPHER* DAN *ROUTE CIPHER* UNTUK MENGAMANKAN PESAN

SKRIPSI

Oleh
Ali Mahfudz
NIM. 18610107

Telah Disetujui Untuk Diuji

Malang, 26 Desember 2022

Dosen Pembimbing I	Dosen Pembimbing II
Prof. Dr. H. Turmudi, M.Si., Ph.D	Ach. Nashichuddin, M.A
NIP. 19571005 198203 1 006	NIP. 19730705 200003 1 001

Mengetahui,
Ketua Program Studi Matematika

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

MODIFIKASI ALGORITMA SUPER ENKRIPSI *CAESAR CIPHER* DAN *ROUTE CIPHER* UNTUK MENGAMANKAN PESAN

SKRIPSI

Oleh
Ali Mahfudz
NIM. 18610107

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 28 Desember 2022

Ketua Penguji	: Dr. Elly Susanti, M.Sc	.....
Anggota Penguji I	: Intan Nisfulaila, M.Si	.....
Anggota Penguji II	: Prof. Dr. H. Turmudi, M.Si., Ph.D	.....
Anggota Penguji III	: Ach. Nashichuddin, M.A	.....

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	: Ali Mahfudz
NIM	: 18610107
Progran Studi	: Matematika
Fakultas	: Sains dan Teknologi
Judul Sripsi	: Modifikasi Algoritma Super Enkripsi Caesar Cipher dan Route Cipher untuk Mengamankan Pesan

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

Malang, 28 Desember 2022

Yang membuat pernyataan,

Ali Mahfudz

NIM. 18610107

MOTO

“Tidak ada cara mudah untuk mencapai bintang-bintang dari bumi”

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:
Kedua orang tua tercinta yaitu Bapak Supriyanto dan Ibu Nurul Hidayah yang selalu memberikan dukungan dan doa restu kepada penulis.
Adik saya yaitu Nur Rohman dan seluruh keluarga saya yang senantiasa memberikan dukungan. Serta sahabat dan teman-teman penulis yang memberikan semangat dan dukungannya kepada penulis dalam menyelesaikan skripsi ini.

KATA PENGANTAR

Assalamu 'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah yang selalu melimpahkan rahmat, taufik serta hidayah-Nya, sehingga penulis dapat menyelesaikan penyusunan skripsi ini yang mempunyai judul "Modifikasi Algoritma Super Enkripsi *Caesar Cipher* dan *Route Cipher* untuk Mengamankan Pesan" sebagai syarat untuk menyelesaikan Program Strata 1 (S1) Matematika di Fakultas Sains dan Teknologi Universitas Islam Maulana Malik Ibrahim Malang. Selanjutnya sholawat serta salam semoga tetap terlimpahkan kepada nabi kita Muhammad SAW yang telah menuntun kita dari zaman kebodohan menuju zaman yang dirahmati Allah SWT, yakni agama Islam. Semoga penulis serta pembaca termasuk golongan orang-orang yang akan selamat kelak di hari kiamat, aamiin.

Dalam proses penulisan skripsi ini, penulis banyak mendapat bimbingan serta arahan dari berbagai pihak. Oleh karena itu penulis mengucapkan banyak terima kasih dan penghargaan setinggi-tingginya terutama kepada:

1. Prof. Dr. H. M. Zainuddin, MA selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. Sri Harini, M.Si selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Elly Susanti, M.Sc, selaku ketua Program Studi Matematika Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Prof. Dr. H. Turmudi, M.Si., Ph.D, selaku dosen Pembimbing I yang telah memberikan arahan kepada penulis.

5. Ach. Nashichuddin, M.A, selaku dosen Pembimbing II yang telah memberikan arahan kepada penulis.
6. Dr. Elly Susanti, S.Pd., M.Sc, selaku Ketua Penguji dalam Ujian Skripsi.
7. Intan Nisfulaila, M.Si, selaku Anggota Penguji 1 dalam Ujian Skripsi.
8. Segenap bapak dan ibu dosen Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Maulana Malik Ibrahim Malang yang sudah memberikan ajarannya kepada penulis selama masa perkuliahan.
9. Bapak Supriyanto dan Ibu Nurul Hidayah selaku bapak dan ibu dari penulis yang senantiasa memberikan doa, dukungan, semangat, dan juga nasihat kepada penulis hingga detik ini.
10. Semua teman-teman yang telah membantu penulis menyelesaikan skripsi ini.

Penulis mengharapkan kritik dan saran dari kalian agar di lain kesempatan bisa menghasilkan karya tulis yang lebih baik. Penulis berharap skripsi ini bisa memberikan manfaat serta kontribusi positif bagi penulis secara pribadi maupun pembaca pada umumnya.

Wassalamu ‘alaikum Warahmatullai Wabarakatuh

Malang, 28 Desember 2022

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

ABSTRAK

Mahfudz, Ali. 2022. **Modifikasi Algoritma Super Enkripsi *Caesar Cipher* dan *Route Cipher* untuk Mengamankan Pesan.** Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Prof. Dr. H. Turmudi, M.Si., Ph.D. (II) Ach. Nashichuddin, M.A.

Kata Kunci : Enkripsi, Dekripsi, Super Enkripsi, Caesar Cipher, Route Cipher.

Keamanan suatu pesan merupakan hal yang penting untuk menjaga data agar tidak mudah dikenali oleh orang lain. Cara yang digunakan untuk mencapai tujuan tersebut adalah kriptografi. Pada penelitian ini menggunakan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher*. Tujuan penelitian ini yaitu untuk mengetahui proses enkripsi dan dekripsi serta keamanan dari algoritma super enkripsi *Caesar Cipher* dan *Route Cipher*. Tahapan dalam penelitian ini menggunakan pendekatan kualitatif dengan metode *library research*. Dalam proses enkripsi dengan algoritma *Caesar Cipher*, rumus yang dipakai adalah $E(x) \equiv ((x - 32 + 5)\ mod\ 95 + 32\ )$. Selanjtnya dalam proses enkripsi menggunakan algoritma *Route Cipher* pesan disusun secara vertikal dari atas ke bawah kemudian akan dibaca secara spiral dari kanan bawah dan searah jarum jam. Kebalikan dari proses enkripsi, pada proses dekripsi menggunakan algoritma *Route Cipher* cipherteks disusun secara spiral dari kanan bawah dan searah jarum jam kemudian akan dibaca secara vertikal ke bawah dari kiri atas. Selanjutnya dalam proses dekripsi menggunakan algoritma *Caesar Cipher* melakukan penghitungan dengan rumus $D(x) \equiv ((x - 32 - 5)\ mod\ 95 + 32)$. Hasil dari pesan yang diamankan menggunakan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher* memiliki tingkat keamanan yang lebih tinggi di banding pesan yang hanya menggunakan algoritma *Caesar Cipher*.

ABSTRACT

Mahfudz, Ali. 2022. **Modification of Caesar Cipher and Route Cipher Super Encryption Algorithms to Secure Messages**. Thesis. Mathematics Study Program, Sciens and Technology Faculty, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisor: (I) Prof. Dr. H. Turmudi, M.Si., Ph.D. (II) Ach. Nashichuddin, M.A.

Keyword: Encryption, Decryption, Super Encryption, Caesar Cipher, Route Cipher.

The security of a message is important to keep data from being easily recognized by others. The means used to achieve such goals are cryptography. In this study, it used a super encryption algorithm of Caesar Cipher and Route Cipher. The purpose of this study is to determine the encryption and decryption process as well as the security of the super encryption algorithms of Caesar Cipher and Route Cipher. The stages in this research use a qualitative approach with the library research method. In the process of encryption with the Caesar Cipher algorithm, the formula used is $E(x) \equiv ((x - 32 + 5) \ mod \ 95 + 32)$. In addition, the encryption process using the Route Cipher algorithm messages are arranged vertically from top to bottom and then will be read in a spiral from the bottom right and clockwise. In contrast to the encryption process, the decryption process used the Route Cipher algorithm ciphertext arranged in a spiral from the bottom right and clockwise and will then be read vertically downwards from the top left. Furthermore, in the decryption process using the Caesar Cipher algorithm, it performs calculations with the formula $D(x) \equiv ((x - 32 - 5) \ mod \ 95 + 32)$. The result of messages being secured using the super encryption algorithm Caesar Cipher and Route Cipher has a higher level of security than messages that only use the Caesar Cipher algorithm.

مستخلص البحث

محفوظ، علي.٢٠٢٢. **تعديل خوارزمية التشفير الفائق (*Caesar Cipher* و *Route Cipher*) لتأمين الرسائل.** البحث العلمي. قسم الرياضيات ، كلية العلوم والتكنولوجيا ، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف: (I) ،بروفسورالدكتور الترمودي ، الماجستير,الحاج (II) احمد ناصح الدين, الماجستير.

الكلمات المفتاحية : التشفير، فك التشفير، التشفيرالفائق، (*Caesar Cipher*، *Route Cipher*)

يعد أمان الرسالة أمرا مهما لمنع التعرف على البيانات بسهولة من قبل الآخرين. الوسائل المستخدمة لتحقيق هذه الأهداف هي التشفير. في هذه الدراسة ، استخدمت خوارزمية التشفير الفائقة *Caesar Cipher* و *Route Cipher*. الغرض من هذه الدراسة هو تحديد عملية التشفير وفك التشفير بالإضافة إلى أمان خوارزميات التشفير الفائقة لتشفير قيصر *وتشفير الطريق*. تستخدم المراحل في هذه الدراسة نهجا نوعيا مع منهج*البحث المكتبي*. في عملية التشفير باستخدام خوارزمية *Caesar Cipher* ، الصيغة المستخدمة هي$E(x) \equiv ((x - 32 + 5) \ mod \ 95 + 32)$. بالإضافة إلى ذلك ، يتم ترتيب عملية التشفير باستخدام رسائل خوارزمية *Route Cipher* عموديا من أعلى إلى أسفل ثم تتم قراءتها حلزونيا من أسفل اليمين وفي اتجاه عقارب الساعة. على عكس عملية التشفير ، في عملية فك التشفير باستخدام *خوارزمية Route Cipher* ، *يتم ترتيب النص المشفر* حلزونيا من أسفل اليمين وفي اتجاه عقارب الساعة ثم ستتم قراءته عموديا لأسفل من أعلى اليسار. ثم في عملية فك التشفير باستخدام خوارزمية *Caesar Cipher* ، يقوم بإجراء عملية الحسابية باستخدام الصيغة$D(x) \equiv ((x - 32 - 5) \ mod \ 95 + 32)$. نتيجة الرسائل التي يتم تأمينها باستخدام خوارزمية التشفير الفائق يتمتع *Caesar Cipher* و *Route Cipher* بمستوى أمان أعلى من الرسائل التي تستخدم خوارزمية *Caesar Cipher* فقط.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era teknologi informasi saat ini, pengiriman informasi selalu terjadi sehingga sangat penting untuk tetap menjaga kerahasiaan serta keamanan suatu informasi. Keamanan dan kerahasiaan data adalah hal yang penting pada pertukaran data atau informasi, supaya tujuan keamanan bersama dan keamanan pribadi dapat tercapai. Dikarenakan dalam pengiriman informasi sering terjadi pencurian informasi oleh orang yang tidak memiliki hak akan informasi tersebut. Oleh sebab itu dalam pengiriman dan penerimaan informasi, pengguna membutuhkan jaminan yang bisa membuat mereka yakin informasi yang diperoleh adalah benar dan aman.

Keamanan suatu pesan ataupun informasi merupakan hal yang penting untuk menjaga sebuah data agar tidak mudah dikenali oleh orang yang tidak berhak. Kriptografi adalah ilmu dan seni untuk menjaga pesan agar tetap aman. Kriptografi merupakan bidang pengetahuan yang memakai persamaan matematis untuk melakukan proses enkripsi dan dekripsi. Teknik ini untuk mengubah data ke bentuk kode-kode esklusif supaya informasi tidak bisa dibaca oleh siapapun kecuali orang yang memiliki hak. Contoh algoritma kriptografi yang biasa dipakai adalah algoritma simetris yang memakai sandi yang sama dalam melakukan enkripsi dan dekripsi sehingga informasi tidak mudah dimengerti artinya. Kriptografi mempunyai banyak teknik dalam menyandikan data, misalnya adalah algoritma *Caesar Cipher* dan *Route Cipher*.

Caesar Cipher ialah salah satu prosedur pemecahan atau algoritma tertua dan juga salah satu jenis *cipher* substitusi yang membentuk kode-kode dengan cara

melakukan penggeseran terhadap semua huruf pada pesan asli dengan melakukan penggeseran yang sama (Ariyus, 2008). *Caesar Cipher* mempunyai suatu kelemahan yaitu kita bisa memperoleh plainteks dengan menggunakan algoritma *Brute Force* serta presentasi frekuensi karakter yang paling banyak muncul dalam kalimat. *Brute Force* adalah sebuah pendekatan yang langsung untuk memecahkan suatu masalah (Santoso, Sundawa, & Azhari, 2016). *Brute Force* dilakukan dengan percobaan terhadap semua kunci. Agar tidak mudah dipecahkan, algoritma *Caesar Cipher* dapat digabungkan dengan algoritma lain atau bisa disebut Super Enkripsi. Super Enkripsi dilakukan untuk mendapatkan *cipher* yang lebih kuat sehingga tidak mudah untuk dipecahkan (Setyaningsih, Iswahyudi, & Widyastuti, 2011).

Contoh penelitian yang telah dilakukan adalah mengkombinasikan *Caesar Cipher* dengan algoritma *Rail Fence*. Dalam penelitian itu, proses penyandian plainteks dilakukan dengan menggunakan algoritma *Caesar Cipher* terlebih dahulu kemudian dilanjutkan pada cipherteks itu diterapkan algoritma *Rail Fence*. Hasil dari penelitian tersebut adalah cipherteks yang dihasilkan lebih sulit untuk dipecahkan, tidak dapat dengan mudah dilakukan rekontruksi, tidak bisa dibobol dengan *Brute Force* dan secara keseluruhan mengatasi kelemahan *Caesar Cipher* (Singh, Nandal, & Malik, 2012).

Peneliti kali ini melakukan penelitian dengan melakukan super enkripsi dengan mengkombinasikan algoritma *Caesar Cipher* dengan algoritma *Route Cipher*. *Route Cipher* sendiri merupakan salah satu jenis *cipher* transposisi. *Route Cipher* memiliki kunci berupa rute yang mana akan diikuti saat membaca cipherteks dari blok yang dibuat dengan plainteks. Plainteks ditulis dalam kotak lalu dibaca mengikuti rute yang dipilih (Wahyuni, 2019). Alasan penulis memilih algoritma ini

karena lebih sulit dibobol dikarenakan memiliki rute yang lebih beragam tergantung pengirim pesan. Pada penelitian kali ini juga akan dilakukan analisis keamanan untuk mengetahui apakah algoritma yang akan dipakai akan lebih aman atau tidak.

Dalam ajaran agama Islam juga terdapat sebuah konsep kriptografi yang berupa amanah. Hal tersebut dijelaskan dalam Al-Qur'an surah An-Nisa' ayat 58 yang berbunyi:

اِنَّ اللّٰهَ يَأْمُرُكُمْ اَنْ تُؤَدُّوا الْاَمٰنٰتِ اِلٰٓى اَهْلِهَاۙ وَاِذَا حَكَمْتُمْ بَيْنَ النَّاسِ اَنْ تَحْكُمُوْا
بِالْعَدْلِۗ اِنَّ اللّٰهَ نِعِمَّا يَعِظُكُمْ بِهٖۗ اِنَّ اللّٰهَ كَانَ سَمِيْعًاۢ بَصِيْرًا

"Sungguh, Allah menyuruhmu menyampaikan amanat kepada yang berhak menerimanya, dan apabila kamu menetapkan hukum di antara manusia hendaknya kamu menetapkannya dengan adil. Sungguh, Allah sebaik-baik yang memberi pengajaran kepadamu. Sungguh, Allah Maha Mendengar, Maha Melihat."(Q.S. An-Nisa'/4:58)

Dalam surat An-Nisa' ayat 58 menegaskan bahwa Allah menyuruh manusia untuk menyampaikan amanat kepada yang berhak menerimanya atau kepada yang dapat dipercaya dan menyuruh yang menyampaikan amanat apabila menetapkan hukum diantara manusia secara adil. Allah memberi pengajaran yang sebaik-baiknya kepada manusia dan Allah Maha Mendengar dan Maha Melihat (Andika, Taquyyudin, & Admizal, 2020).

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka penelitian ini mempunyai rumusan masalah dibawah ini:

1. Bagaimana proses enkripsi pada pesan dengan menggunakan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher*?
2. Bagaimana proses dekripsi pada pesan dengan menggunakan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher*?

3. Bagaimana analisis keamanan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, penelitian ini bertujuan untuk:

1. Mengetahui proses enkripsi pada pesan dengan menggunakan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher*.
2. Mengetahui proses dekripsi pada pesan dengan menggunakan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher*.
3. Mengetahui keamanan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher.*

1.4 Manfaat Penelitian

Ada beberapa manfaat yang dapat kita peroleh yaitu :

1. Untuk mengetahui keamanan pesan yang di enkripsi dengan memakai algoritma super enkripsi *Caesar Cipher* dan *Route Cipher*.
2. Untuk memperdalam pengetahuan tentang implementasi algoritma super enkripsi *Caesar Cipher* dan *Route Cipher*.

1.5 Batasan Masalah

Ada beberapa batasan yang perlu diperhatikan pada penelitian ini yang akan kita bahas yaitu :

1. Karakter yang akan digunakan berjumlah 95 yaitu karakter nomor 32 sampai karakter nomor 126 dalam tabel ASCII.
2. Dalam proses enkripsi dan dekripsi kunci yang dipakai untuk *Caesar Cipher* adalah 5 dan kunci yang dipakai untuk *Route Cipher* adalah 6 dengan rute spiral.

3. Algoritma yang dipakai dalam super enkripsi adalah *Caesar Cipher* dan *Route Cipher.*
4. Pada analisis keamanan memakai algoritma *Brute Force*.

1.6 Definisi Istilah

Berdasarkan rumusan masalah penelitian, maka uraian definisi istilah dalam penelitian ini adalah sebagai berikut:

1. Enkripsi

   Enkripsi merupakan plainteks atau pesan asli disandikan menjadi cipherteks yang tidak dimengerti.

2. Dekripsi

   Dekripsi adalah kebalikan dari enkripsi. Pesan yang sudah disandikan kemudian dikembalikan ke bentuk asalnya (plainteks).

3. Super Enkripsi

   Super enkripsi atau enkripsi super adalah sebuah gagasan yang mengkombinasikan dua teknik substitusi dan teknik transposisi agar memperoleh sebuah algoritma yang lebih aman atau tidak mudah dipecahkan. Algoritma yang akan dipakai adalah *Caesar Cipher* dan *Route Cipher.*

4. Algoritma *Caesar Cipher*

   Algoritma *Caesar Cipher* adalah algoritma sederhana yang melakukan penggeseran terhadap setiap huruf pada pesan asli dengan pergeseran yang sama.

5. Algoritma *Route Cipher*

   Algoritma *Route Cipher* ialah algoritma transposisi/permutasi yang cara baca dan kuncinya dapat ditentukan sesuai perjanjian penggunanya.

6. Algoritma Brute Force

Algoritma *Brute Force* adalah sebuah metode pemecahan masalah dengan cara mencoba semua kemungkinan solusi dan melakukan pengecekan apakah semua kemungkinan solusi yang diberikan dapat memenuhi syarat-syarat sebagai solusi atau tidak

BAB II

KAJIAN TEORI

2.1 Teori Pendukung

2.1.1 Kriptografi

Kata kriptografi berasal dari bahasa Yunani, yaitu *crypto* dan *graphia*. Kata *Crypto* mempunyai arti rahasia (*secret*) dan kata *graphia* yang berarti tulisan (*writing*). Sedangkan dalam terminologi, kriptografi berarti ilmu serta seni yang digunakan untuk menjamin keamanan informasi saat dikirim dari satu tempat ke tempat yang lain (Ariyus, 2008). Kriptografi klasik adalah kriptografi yang hanya memakai satu kunci dalam pengamanan data. Orang-orang telah menggunakan Teknik ini sejak beberapa ratus tahun yang lalu. Teknik dasar yang biasa dipakai dalam algoritma jenis ini ada dua yaitu sebagai berikut:

1. Teknik substitusi/pengganti yaitu mengganti semua huruf plainteks dengan teks lain. Contoh algoritma yang menggunakan teknik substitusi adalah *Caesar Cipher*.
2. Teknik transposisi/permutasi yaitu dilakukan dengan memakai transposisi/permutasi karakter. Contoh algoritma yang menggunakan teknik trasposisi adalah *Route Cipher* (Ariyus, 2008).

Kriptografi modern adalah suatu perbaikan yang mengacu dalam kriptografi klasik. Dalam kriptografi modern terdapat banyak sekali algoritma yang dimaksudkan dalam mengamankan informasi yang dikirim melalui jaringan komputer. Algoritma kriptografi modern terdiri dari 2 bagian yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris menggunakan kunci yang sama untuk enkripsi dan dekripsinya, sedangkan algoritma asimetris memiliki

pasangan kunci yang salah satunya digunakan untuk proses enkripsi dan yang satu lagi digunakan untuk proses dekripsi (Ariyus, 2008).

2.1.1.1 Masalah Keamanan

Masalah keamanan termasuk bagian yang penting dalam suatu sistem informasi. Tetapi, masalah keamanan sendiri jarang menerima perhatian saat pengelolaan sistem informasi. Masalah keamanan cukup sering menempati urutan belakang pada daftar hal-hal yang dianggap krusial. Jika ada gangguan pada kinerja sistem, masalah keamanan jarang dipedulikan atau bahkan diabaikan (Ariyus, 2008). Informasi menentukan hampir semua elemen dari kehidupan manusia. Informasi memiliki arti penting bagi kehidupan karena tanpa informasi hampir semua kegiatan tidak dapat dilakukan dengan baik. Hanya sedikit hal yang dapat dilakukan di dunia modern tanpa melibatkan pembuatan, penukaran, pengumpulan, atau penukaran informasi. Saat ini informasi sudah menjadi komoditas yang sangat penting.

Kemajuan sistem informasi memberikan banyak manfaat bagi kehidupan manusia. Akan tetapi, sistem informasi juga menimbulkan kerugian yang cukup banyak, diantaranya kejahatan pada komputer yang mencakup pemerasan, penipuan, pencurian, kompetisi, dan lain sebagainya. Tersebarnya informasi ke orang lain, seperti saingan dalam berbisnis, bisa menyebabkan kerugian bagi pemilik informasi tersebut. Contohnya banyak informasi milik perusahaan yang hanya boleh diketahui oleh orang dengan jabatan tertentu di perusahaan tersebut, misal informasi tentang detail produk yang sedang dikembangkan dan teknik yang dipakai untuk menghasilkan produk tersebut.

Oleh karena itu keamanan dari sistem informasi yang dipakai harus terjamin dalam batas tertentu.

2.1.1.2 Algoritma Kriptografi

Algoritma berasal dari nama seorang Ilmuan Arab yang bernama Abu Ja'far Muhammad Ibnu Musa Al Khuwarizmi penulis buku berjudul Al Jabar Wal Muqabala (Buku Pemugaran dan Pengurangan). Kata Al Khuwarizmi dibaca orang barat menjadi algorism yang kemudian lambat laun menjadi *Algorithm* dan diserap dalam Bahasa Indonesia menjadi Algoritma. Algoritma dapat diartikan sebagai urutan langkah-langkah terbatas untuk menyelesaikan suatu masalah (Nuraini, 2015).

Menurut terminologinya algoritma adalah urutan tahapan-tahapan logis dalam menyelesaikan suatu masalah yang tersusun secara sistematis. Algoritma kriptografi adalah langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak memiliki hak padapesan itu.

Algoritma kriptografi terdiri dari 3 fungsi dasar sebagai berikut:

1. Enkripsi

   Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak dimengerti atau tidak mudah dibaca. Dari definisi di atas dapat disimpulkan bahwa enkripsi adalah mengacak suatu kode menjadi kode lain sehingga tidak dapat diketahui kode aslinya.

2. Dekripsi

   Dekripsi adalah kebalikan dari enkripsi. Pesan yang telah disandikan dikembalikan ke pesan aslinya (plainteks), disebut dengan dekripsi pesan. Algoritma yang dipakai dalam dekripsi berbeda dengan algoritma yang dipakai dalam enkripsi.

3. Kunci

   Kunci yang dimaksud disini adalah kunci yang digunakan dalam melakukan enkripsi dan juga dekripsi.

2.1.1.3 Algorima Caesar Cipher

Salah satu contoh yang sederhana dari *cipher* substitusi adalah *Caesar Cipher,* yang digunakan oleh Julius Caesar untuk berkomunikasi dengan tentaranya. Caesar ini dipertimbangkan menjadi salah satu orang yang pertama kali menggunakan enkripsi untuk mengamankan pesannya. Caesar memutuskan menggeser setiap huruf dalam pesan yang akan menjadi algoritma standar, sehingga dia dapat menginformasikan semua keputusannya dan kemudian mengirim pesan ini dalam bentuk yang aman (Mukhtar, 2018). Jika melakukan pergeseran sebanyak 3 kali maka kunci yang digunakan untuk dekripsi adalah 3. Pergeseram kunci yang dipakai dapat diubah sesuai keinginan pengirim pesan. Pengirim pesan disa memakai kunci $a = 6$, $b = 7$, dan seterusnya.

Pada algoritma *Caesar Cipher* untuk plainteks memiliki simbol “P” dan cipherteks memiliki simbol “C” dan untuk kunci memiliki simbol “K”. sehingga rumusnya bisa dibuat seperti berikut:

$$C = E(P) \equiv (P + K)\ mod\ 26$$

Berdasarkan rumus enkripsi, untuk contoh kita dapat memasukkan kunci dengan nilai 3 supaya menjadi:

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

Sedangkan pada rumus dekripsinya adalah menjadi seperti dibawah ini:

$$P = D(C) \equiv (C - K)\ mod\ 26$$

Pada contoh sebelumnya, dengan memakai K = 3, maka:

$$P = D(C) \equiv (C - 3)\ mod\ 26$$

Diberikan sebuah plainteks SKRIPSI. Selanjutnya contoh akan dilakukan enkripsi dengan menggunakan K=3 dan akan didapatkan cipherteks VNUMSVM. Berikut proses perhitungannya:

$E(P) \equiv (18 + 3)\ mod\ 26 \equiv 21$ (huruf V)

$E(P) \equiv (10 + 3)\ mod\ 26 \equiv 13$ (huruf N)

$E(P) \equiv (17 + 3)\ mod\ 26 \equiv 20$ (huruf U)

$E(P) \equiv (9 + 3)\ mod\ 26 \equiv 12$ (huruf M)

$E(P) \equiv (15 + 3)\ mod\ 26 \equiv 18$ (huruf S)

$E(P) \equiv (18 + 3)\ mod\ 26 \equiv 21$ (huruf V)

$E(P) \equiv (9 + 3)\ mod\ 26 \equiv 12$ (huruf M)

Sedangkan untuk proses dekripsi, pertama diketahui sebuah cipherteks VNUMSVM kemudian akan didekripsi dengan menggunakan K=3. Berikut proses perhitungannya:

$D(C) \equiv (21 - 3)\ mod\ 26 \equiv 18$ (huruf S)

$D(C) \equiv (13 - 3)\ mod\ 26 \equiv 10$ (huruf K)

$D(C) \equiv (20 - 3)\ mod\ 26 \equiv 17$ (huruf R)

$D(C) \equiv (12 - 3)\ mod\ 26 \equiv 9$ (huruf I)

$D(C) \equiv (18 - 3)\ mod\ 26 \equiv 15$ (huruf P)

$D(C) \equiv (21 - 3)\ mod\ 26 \equiv 18$ (huruf S)

$D(C) \equiv (12 - 3)\ mod\ 26 \equiv 9$ (huruf I)

Plainteks yang didapatkan adalah SKRIPSI

2.1.1.4 Algoritma Route Cipher

Route Cipher sendiri merupakan salah satu jenis *cipher* transposisi. *Route Cipher* memiliki kunci berupa rute yang mana akan diikuti saat membaca cipherteks dari blok yang dibuat dengan plainteks. Plainteks ditulis dalam kotak lalu dibaca mengikuti rute yang dipilih (Wahyuni, 2019). Route Cipher adalah plainteks yang pertama ditulis kemudian dibaca menurut kunci yang sudah ditentukan. Pembacaan cipherteks dilakukan dalam pola yang diberikan pada kunci (Girsang dkk, 2019).

Tahapan-tahapan dalam algoritma *Route Cipher* yaitu :

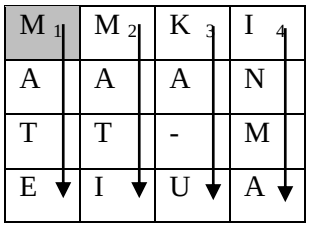
1. Membuat matriks menggunakan jumlah baris yang akan diisi plainteks dengan membagi jumlah plainteks dengan kunci.
2. Menentukan arah tranpsposisi plainteks, misalnya apabila arah yang dtentukan itu spiral, maka cipherteks diperoleh dengan membaca plainteks pada matriks menggunakan arah spiral.
3. Untuk proses dekripsi, algoritma *Route Cipher* hanya membaca posisi menurut urutan kata yang disusun dalam matriks menurut susunan berdasarkan arah yang dipakai untuk membangun cipherteks.

Algoritma *Route Cipher* adalah salah satu teknik kriptografi klasik yang menggunakan transposisi dalam melakukan enkripsi pada plainteks. *Route Cipher* melakukan transposisi/permutasi dengan cara menuliskan plainteks

dari atas ke bawah pada suatu matriks berdasarkan ukuran yang sudah ditentukan. Cipherteksnya dibaca dengan rute (arah) yang telah ditentukan, misalnya dibaca seperti bentuk spiral dengan arah yang berlawanan jarum jam, mulai dari kanan bawah atau seperti ular tangga, yang dimulai dari kanan bawah dan lain sebagainya (Bangun, 2019).

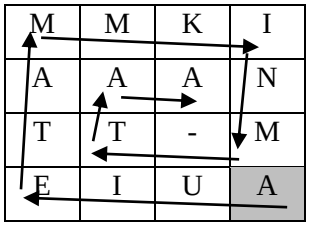
Contoh:

1. Diberikan plainteks "MATEMATIKA UINMA". Plainteks akan ditulis vertikal dari kiri atas ke bawah dan untuk spasi akan diganti dengan simbol "-". Selanjutnya kunci yang digunakan untuk membentuk matrik adalah 4.



Gambar 2.1 *Contoh Plainteks Enkripsi Route Cipher*

Berikutnya cipherteks yang didapat dengan menyusun teks selaras dengan arah yang telah ditentukan yaitu spiral searah jarum jam dari kanan bawah dan memperoleh hasil sebagai berikut:

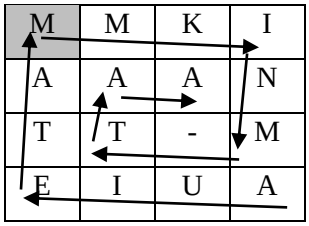


Gambar 2.2 *Contoh Cipherteks Enkripsi Route Cipher*

Dan cipherteks yang dihasilkan adalah AUIETAMMKINM-TAA.

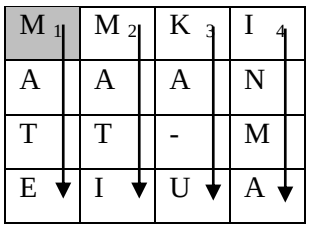
2. Sedangkan contoh untuk proses dekripsi dari cipherteks AUIETAMMKINM-TAA akan ditulis spiral searah jarum jam dari kanan

bawah dan kunci yang digunakan untuk membentuk matriks adalah 4, vertikal dari kiri atas ke bawah.



Gambar 2.3 *Contoh Cipherteks Dekripsi Route Cipher*

Kemudian akan dibaca vertikal dari kiri atas ke bawah dan simbol "-" diganti menjadi spasi. Kemudian pembacaan plainteks akan diperlihatkan pada gambar di bawah ini.



Gambar 2.4 *Contoh Plainteks Dekripsi Route Cipher*

Dan plainteks yang didapatkan adalah MATEMATIKA UINMA.

2.1.1.5 Super Enkripsi

Super enkripsi atau enkripsi super adalah sebuah gagasan yang mengkombinasikan dua atau lebih teknik substitusi dan teknik transposisi/permutasi agar memperoleh sebuah algoritma yang lebih aman atau tidak mudah dipecahkan. Teknik dari super enkripsi sendiri dapat dilakukan asalkan sudah memahami teknik subtitusi dan teknik transposisi di atas. Dimulai dengan melakukan penyandian pesan dengan memakai teknik substitusi dan cipherteks disandikan lagi dengan memakai teknik transposisi/permutasi atau sebaliknya (Ariyus, 2008).

Berikut adalah tahapan dalam proses super enkripsi yaitu:

1. Melakukan enkripsi plainteks menggunakan *Caesar Cipher* dan menjadi cipherteks.
2. Melakukan enkripsi kembali cipherteks memakai transposisi *Route Cipher*.
3. Melakukan dekripsi cipherteks dari hasil *Route Cipher* dengan transposisi/permutasi *Route Cipher.*
4. Melakukan dekripsi kembali pada hasil proses dekripsi *Route Cipher* dengan *Caesar Cipher.*
5. Mendapatkan plainteks seperti pesan awal yang dikirim.

2.1.1.6 Kode ASCII

ASCII singkatan dari *American Standart Code for Information Interchange* yang merupakan salah satu *standart* yang dipakai dalam mempresentasikan sebuah karakter. Kode ASCII terdiri dari bilangan biner sebanyak 8 bit. Mulai dari 00000000 sampai 1111111. Kombinasi yang didapatkan memliki total sebanyak 255, terdiri dari beberapa karakter kontrol, beberapa tanda baca yang umum dipakai, angka 0-9, dan huruf alfabet a-z dan A-Z. Oleh sebab itu ASCII merupakan salah satu standart yang banyak dipakai pada *computer* dan perangkat komunikasi (Kurnia, 2013).

2.1.1.7 Algoritma *Brute Force*

Algoritma *Brute Force* adalah sebuah metode pemecahan masalah dengan cara mencoba semua kemungkinan solusi dan melakukan pengecekan apakah semua kemungkinan solusi yang diberikan dapat memenuhi syarat-syarat sebagai solusi atau tidak. Cara pemecahan masalah yang digunakan pada

algoritma *Brute Force* pada umumnya merupakan cara yang mudah dimengerti (Kurnia, 2013). Penggunaan algoritma Brute Force pada Caesar Cipher dilakukan dengan mencoba semua kunci yang ada yaitu dengan melakukan pergeseran sebanyak semua kunci.

2.1.2 Modulo

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat lebih dari nol. Operasi $a \bmod m$ memberikan sisa apabila a dibagi oleh bilangan m yang dinamai dengan modulo atau modulus. Hasil operasi modulo m terdapat pada himpunan $\{0,1,2, \ldots, m-1\}$ (Munir, 2019).

Contoh: 1. 25 mod 7 = 4 (25 = 7.3+4)

2. 5 mod 9 = 5 (5 = 9.0+5)

3. 20 mod 4 = 0 (20 = 4.5+0)

Definisi : Apabila suatu bilangan bulat M yang bukan nol, membagi selisih $a-b$, maka dikatakan a kongruen b modulo M dan ditulis $a \equiv b(mod\ M)$. Jika $a-b$ tidak dibagi M, maka dikatakan a tidak kongruen $b\ (mod\ M)$, dan ditulis $a \not\equiv b(mod\ M)$ (Irawan, Hijriyah, & Habibi, 2014).

Contoh: 1. $27 \equiv 2(mod\ 5)$ karena (27-2) terbagi oleh 5

2. $35 \not\equiv 6(mod\ 7)$ karena (35-6) tidak terbagi oleh 7

Dari definisi dan contoh di atas, dapat ditelaah sebagai berikut:

Jika M lebih dari 0 dan $M|(a-b)$ maka terdapat suatu bilangan bulat t sehingga $a-b = Mt$. sehingga $a \equiv b(mod\ M)$ bisa juga dinyatakan sebagai $a-b = Mt$, ini mempunyai arti yang sama dengan $a \equiv b(mod\ M)$ atau beda antara a dan b adalah kelipatan M. Jadi $a \equiv b(mod\ M)$ bisa juga dinyatakan $a = Mt +$

b, yaitu $a = b$ ditambah kelipatan M. menurut contoh di atas $27 \equiv 2(mod\ 5)$ mempunyai arti yang sama dengan 27 = 5.5 +2.

2.1.3 Matriks

Matriks merupakan sekumpulan bilangan yang tersusun menggunakan cara tertentu ke bentuk baris & kolom sehingga membangun sebuah persegi panjang ataupun bujur sangkar yang ditulis diantara dua tanda kurung, yaitu ( ) atau [ ] (Ruminta, 2014). Seperti yang telah dijelaskan di atas bahwa matriks terdiri atas unsur- unsur yang disusun secara baris dan kolom. Jika banyak baris pada sebuah matriks adalah m, dan banyak kolom pada suatu matriks adalah n, maka matriks itu mempunyai ordo matriks mxn.

Notasi pada matriks memakai huruf besar, dan notasi untuk elemen- elemen didalamnya adalah huruf kecil sesuai berdasarkan penamaan matriks tersebut dan diberi indeks ij. Indeks tersebut menyatakan posisi elemen pada matriks, yaitu baris ke-i & kolom ke-j. Ada beberapa jenis matriks yang perlu diketahui yaitu:

1. Matriks Nol, yaitu matriks yang setiap elemenya adalah 0.
2. Matriks Baris, yaitu matriks yang hanya punya satu baris.
3. Matriks Kolom, yaitu matriks yang hanya punya satu kolom.
4. Matriks Persegi, yaitu matriks yang punya jumlah baris & kolom yang sama.
5. Matriks Identitas, yaitu matriks konstanta dengan elemen diagonal utama 1.

2.2 Amanah dalam Al-Quran dan Hadits

Dalam ajaran agama Islam juga terdapat amanah. Kata “amanah” berasal dari ”*al-hamzah*”, “*mim*”, “*nun*”, kata ini mengarah pada dua pokok makna kata yang berdekatan yaitu Al-amanah lawan dari kata al-khiyanah yaitu suk-n al-qabl (ketenangan hati) dan Al-tasdiq yang artinya mempercayakan (Dalimunthe, 2016).

Menurut Kementerian Pendidikan dan Kebudayaan dalam Kamus Besar Bahasa Indonesia (2015), amanah adalah sesuatu yang dipercayakan (dititipkan) kepada orang lain, keamanan, ketentraman, dan dapat dipercaya. Pengertian amanah secara bahasa adalah jujur dan dapat dipercaya sedangkan secara istilah amanah adalah segala sesuatu perbuatan yang harus dipertanggungjawabkan kepada orang lain, menyangkut hak-hak Allah dan hak hambanya baik itu berupa benda, perkataan, perbuatan bahkan kepercayaan yang harus disampaikan kepada yang berhak tanpa ada pengurangan ataupun penambahan apapun (Andika, Taquyyudin, & Admizal, 2020). Amanah dijelaskan dalam Al-Qur'an surah An-Nisa' ayat 58 ((LPMQ), 2022).

اِنَّ اللّٰهَ يَأْمُرُكُمْ اَنْ تُؤَدُّوا الْاَمٰنٰتِ اِلٰٓى اَهْلِهَاۙ وَاِذَا حَكَمْتُمْ بَيْنَ النَّاسِ اَنْ تَحْكُمُوْا بِالْعَدْلِۗ اِنَّ اللّٰهَ نِعِمَّا يَعِظُكُمْ بِهٖۗ اِنَّ اللّٰهَ كَانَ سَمِيْعًاۢ بَصِيْرًا

"Sungguh, Allah menyuruhmu menyampaikan amanat kepada yang berhak menerimanya, dan apabila kamu menetapkan hukum di antara manusia hendaknya kamu menetapkannya dengan adil. Sungguh, Allah sebaik-baik yang memberi pengajaran kepadamu. Sungguh, Allah Maha Mendengar, Maha Melihat."(Q.S. An-Nisa'/4:58)

Dalam kitab Tafsir Ibnu Katsir jilid 2(2001) Allah mengabarkan bahwa dia memerintahkan untuk menunaikan amanah kepada ahlinya. Sesuai dengan hadits Al-Hasan dari Samurah yang berarti "Tunaikanlah Amanah kepada yang memberikan amanah dan jangan khianati orang yang berkhianat kepadamu" (HR. Ahmad dan Ahlus Sunah).

Hal ini mencakup semua amanah yang wajib bagi manusia berupa hak-hak Allah terhadap para hamba-nya seperti salat, zakat, puasa, kafarat, nazar, dan selain dari itu, yang kesemuanya adalah amanah yang diberikan tanpa pengawas hambanya yang lain. Serta amanah yang berupa hak-hak sebagian hamba dengan

hamba lainnya, seperti titipan dan selanjutnya, yang kesemuanya adalah amanah yang dilakukan tanpa pengawasan saksi. Itulah yang diperintahkan oleh Allah untuk ditunaikan. Barang siapa yang tidak melakukanya di dunia ini, maka akan dimintai pertanggungjawabanya di hari Kiamat. (Al-Sheikh, 2001).

Dalam kitab Tafsir Ath-Thabari jilid 7 (2007) Abu Ja'far berkata : Wahai para pemimpin kaum muslim, sesungguhnya Allah telah memerintahkan kalian untuk melaksanakan apa yang telah dipercayakan kepada kalian berupa tanggung jawab terhadap harta rampasan perang, hak-hak, harta, dan sedekah mereka, untuk dijalankan dengan baik sesuai perintah Allah kepadamu, tentunya setelah berada ditanganmu. Laksanakanlah semua itu dengan baik, karena memang telah diserahkan kepada orang yang memang menjadi ahlinya. Jangnlah kalian menzalimi ahlinya, jangan memonopoli sesuatu tersebut, jangan menempatkan sesuatu yang bukan pada tempatnya, dan jangan mengambilnya kecuali dari apa yang telah diizinkan untuk kalian ambil dari sebagiannya sebelum berada dalam kekuasaanmu (Bakri, Muhammad, Khalaf, & Hamid, 2007)

2.3 Kajian Topik dengan Teori Pendukung

Penelitian ini disusun menggunakan beberapa teori pendukung. Seperti dalam Algoritma *Caesar Cipher* juga perlu untuk mempelajari modulo. Dalam hal ini modulo dipakai saat melakukan enkripsi dan dekripsi. Modulo sendiri digunakan agar diperoleh sisa pembagian yang terdapat dalam kode karakter plainteks yang digunakan.

Selanjutnya dalam Algoritma *Route Cipher* perlu menggunakan matriks. Matriks merupakan sekumpulan bilangan yang tersusun menggunakan cara tertentu ke bentuk baris & kolom sehingga membangun sebuah persegi panjang ataupun

bujur sangkar. Matriks dalam Algoritma *Route Cipher* digunakan dalam proses enkripsi dan dekripsi. Plainteks akan disusun dalam bentuk matriks dan selanjutnya akan dibaca sesuai dengan keinginan si pengirim pesan.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Skripsi ini termasuk dalam jenis penelitian kualitatif. Metode penelitian yang digunakan dalam penelitian ini adalah studi literatur. Penulisan dimulai dengan mempelajari beberapa buku, jurnal, dan referensi lain yang mendukung penelitian ini.

3.2 Pra Penelitian

Hal-hal yang dilakukan oleh penulis sebelum menulis penelitian ini adalah membaca jurnal-jurnal, buku-buku, dan penelitian-penelitian sebelumnya yang terkait dengan judul skripsi yang diambil penulis. Salah satu jurnal yang dikaji adalah jurnal oleh Latifah dkk (2017) yang menggunakan algoritma *Caesar Cipher* dan *Rail Fence* untuk mengamankan pesan teks alfanumerik dan karakter khusus.

3.3 Tahapan Penelitian

Adapun tahapan-tahapan dalam penyelesaian penelitian ini adalah sebagai berikut.

1. Menyiapkan algoritma enkripsi dan dekripsi

   Pada penelitian ini penulis akan menyusun algoritma yang akan digunakan untuk proses enkripsi dan dekripsi. Algoritma yang akan dipakai adalah *Caesar Cipher* dan *Route Cipher.*

2. Melakukan simulasi.

   Simulasi yang dilakukan dalam proses enkripsi sebagai berikut:

   a. Menentukan plainteks yang akan di enkripsi.

   b. Menentukan kunci yang akan digunakan untuk enkripsi.

c. Mengkonversi plainteks ke numerik berdasarkan tabel ASCII.
d. Melakukan penghitungan dengan *Caesar Cipher* menggunakan kunci yang sudah ditentukan.
e. Mengkonversi numerik ke alfabet dan simbol dalam tabel ASCII.
f. Melakukan penghitungan dengan *Route Cipher* dari hasil penghitungan *Caesar Cipher*.
g. Mendapatkan cipherteks.

Simulasi yang dilakukan dalam proses dekripsi adalah sebagai berikut:

a. Memasukkan cipherteks.
b. Menentukan kunci yang akan dipakai untuk dekripsi.
c. Melakukan penghitungan dengan *Route Cipher*.
d. Mengkonversi cipherteks ke numerik berdasarkan tabel ASCII.
e. Melakukan penghitungan dengan *Caesar Cipher* menggunakan kunci yang sudah ditentukan.
f. Mengkonversi numerik ke alfabet dan simbol dalam tabel ASCII.
g. Mendapatkan plainteks.

3. Menganalisis keamanan algoritma.

Analisis keamanan dilakukan dengan langkah-langkah sebagai berikut:

a. Menyiapkan cipherteks algoritma *Caesar Cipher*.
b. Menyerang cipherteks dengan algoritma *Brute Force*.
c. Menyiapkan cipherteks dari algoritma super enkripsi *Caesar Cipher* dan *Route Cipher*.
d. Menyerang cipherteks dengan algoritma *Brute Force*.

BAB IV

PEMBAHASAN

Bab ini berisi proses enkripsi dan dekripsi pesan menggunakan kombinasi dari dua algoritma substitusi dan transposisi atau disebut dengan algoritma super enkripsi. Algoritma yang dipakai pada penelitian ini yaitu *Caesar Cipher* yang merupakan algoritma substitusi dan *Route Cipher* yang merupakan algoritma transposisi. Adapun tahapan-tahapan pada proses enkripsi adalah melakukan enkripsi menggunakan algoritma *Caesar Cipher* dan setelah mendapatkan hasil enkripsinya dilanjutkan dengan melakukan enkripsi menggunakan algoritma *Route Cipher*. Sedangkan tahapan-tahapan pada proses dekripsi dimulai dengan melakukan dekripsi menggunakan algoritma *Route Cipher* dan setelah mendapatkan hasil dekripsinya dilanjutkan dengan melakukan dekripsi menggunakan algoritma *Caesar Cipher*. Selanjunya untuk mengetahui apakah algoritma super enkripsi memiliki keamanan yang lebih ditingkatkan, akan dilakukan analisis keamanan terhadap pesan yang telah dienkripsi.

4.1 Enkripsi Pesan Meggunakan Algoritma Super Enkripsi Caesar Cipher dan Route Cipher

Pada saat melakukan proses enkripsi, penulis menentukan plainteks yang akan disandikan menggunakan algoritma *Caesar Cipher* dan *Route Cipher*. Pada kali ini plainteks yang dipakai adalah “Ali dari Prodi MATEMATIKA UIN MALANG”.

Langkah selanjutnya adalah menentukan kunci. Kunci yang akan digunakan dalam proses enkripsi adalah 5 untuk *Caesar Cipher* dan 6 untuk *Route Cipher*. Setelah menentukan kunci, dilanjutkan dengan mengubah plainteks ke bentuk kode numerik dalam ASCII yang ditampilkan dalam tabel 4.1.

Tabel 4.1 *Kode Karakter Plainteks untuk Enkripsi*

Karakter	Kode	Karakter	Kode	Karakter	Kode
A	65	d	100	A	65
L	108	i	105	(spasi)	32
I	105	(spasi)	32	U	85
(spasi)	32	M	77	I	73
d	100	A	65	N	78
a	97	T	84	(spasi)	32
r	114	E	69	M	77
i	105	M	77	A	65
(spasi)	32	A	65	L	76
P	80	T	84	A	65
r	114	I	73	N	78
o	111	K	75	G	71

Selanjutnya melakukan penghitungan dengan algoritma *Caesar Cipher* menggunakan kunci yang sudah ditentukan. Penghitungan enkripsi adalah sebagai berikut:

$E(x) \equiv ((x - 32 + 5)\ mod\ 95 + 32\ )$

Selanjutnya masukkan plainteks pada rumus enkripsi di atas.

$E(A) \equiv \big((65 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 38\ mod\ 95 + 32 \equiv 70$

$E(l) \equiv \big((108 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 81\ mod\ 95 + 32 \equiv 113$

$E(i) \equiv \big((105 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 78\ mod\ 95 + 32 \equiv 110$

$E(spasi) \equiv \big((32 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 5\ mod\ 95 + 32 \equiv 37$

$E(d) \equiv \big((100 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 73\ mod\ 95 + 32 \equiv 105$

$E(a) \equiv \big((97 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 70\ mod\ 95 + 32 \equiv 102$

$E(r) \equiv \big((114 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 87\ mod\ 95 + 32 \equiv 119$

$E(i) \equiv \big((105 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 78\ mod\ 95 + 32 \equiv 110$

$E(spasi) \equiv \big((32 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 5\ mod\ 95 + 32 \equiv 37$

$E(P) \equiv \big((80 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 53\ mod\ 95 + 32 \equiv 85$

$E(r) \equiv \big((114 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 82\ mod\ 95 + 32 \equiv 119$

$E(o) \equiv \big((111 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 79\ mod\ 95 + 32 \equiv 116$

$E(d) \equiv \big((100 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 68\ mod\ 95 + 32 \equiv 105$

$E(i) \equiv \big((105 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 78\ mod\ 95 + 32 \equiv 110$

$E(spasi) \equiv \big((32 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 5\ mod\ 95 + 32 \equiv 37$

$E(M) \equiv \big((77 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 50\ mod\ 95 + 32 \equiv 82$

$E(A) \equiv \big((65 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 38\ mod\ 95 + 32 \equiv 70$

$E(T) \equiv \big((84 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 57\ mod\ 95 + 32 \equiv 89$

$E(E) \equiv \big((69 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 42\ mod\ 95 + 32 \equiv 74$

$E(M) \equiv \big((77 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 50\ mod\ 95 + 32 \equiv 82$

$E(A) \equiv \big((65 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 38\ mod\ 95 + 32 \equiv 70$

$E(T) \equiv \big((84 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 57\ mod\ 95 + 32 \equiv 89$

$E(I) \equiv \big((73 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 46\ mod\ 95 + 32 \equiv 78$

$E(K) \equiv \big((75 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 48\ mod\ 95 + 32 \equiv 80$

$E(A) \equiv \big((65 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 38\ mod\ 95 + 32 \equiv 70$

$E(spasi) \equiv \big((32 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 5\ mod\ 95 + 32 \equiv 37$

$E(U) \equiv \big((85 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 58\ mod\ 95 + 32 \equiv 90$

$E(I) \equiv \big((73 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 46\ mod\ 95 + 32 \equiv 78$

$E(N) \equiv \big((78 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 51\ mod\ 95 + 32 \equiv 83$

$E(spasi) \equiv \big((32 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 5\ mod\ 95 + 32 \equiv 37$

$E(M) \equiv \big((77 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 50\ mod\ 95 + 32 \equiv 82$

$E(A) \equiv \big((65 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 38\ mod\ 95 + 32 \equiv 70$

$E(L) \equiv \big((76 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 49\ mod\ 95 + 32 \equiv 81$

$E(A) \equiv \big((65 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 38\ mod\ 95 + 32 \equiv 70$

$E(N) \equiv \big((78 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 51\ mod\ 95 + 32 \equiv 83$

$E(G) \equiv \big((71 - 32 + 5)\ mod\ 95 + 32\ \big) \equiv 44\ mod\ 95 + 32 \equiv 76$

Setelah melakukan penghitungan, kemudian kode-kode tersebut diubah kembali ke bentuk karakter dalam ASCII yang ditampilkan dalam tabel 4.2.

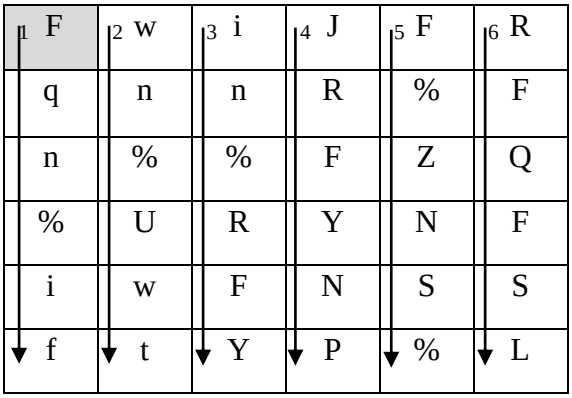
Tabel 4.2 *Kode Karakter Cipherteks untuk Enkripsi*

Kode	Karakter	Kode	Karakter	Kode	Karakter
70	F	105	i	70	F
113	q	110	n	37	%
110	n	37	%	90	Z
37	%	82	R	78	N
105	i	70	F	83	S
102	f	89	Y	37	%
119	w	74	J	82	R
110	n	82	R	70	F
37	%	70	F	81	Q
85	U	89	Y	70	F
119	w	78	N	83	S
116	t	80	P	76	L

Sehingga diperoleh cipherteks dari tabel di atas yaitu

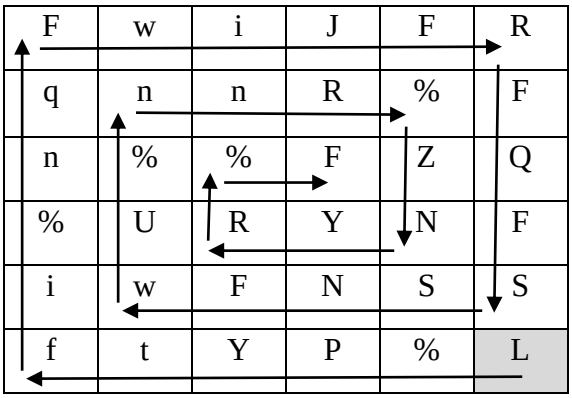
Fqn%ifwn%Uwtin%RFYJRFYNPF%ZNS%RFQFSL

Selanjutnya cipherteks tersebut dienkripsi kembali dengan menggunakan *Route Cipher*. Plainteks akan ditulis secara verikal dari kiri atas ke bawah. Kunci yang digunakan untuk membentuk matriks adalah 6.



Gambar 4.1 *Plainteks Enkripsi Route Cipher*

Plainteks yang telah disusun secara vertikal dari atas ke bawah kemudian dibaca secara spiral searah jarum jam dari kanan bawah dan didapatkan hasil cipherteks sebagai berikut:



Gambar 4.2 *Cipherteks Enkripsi Route Cipher*

Dan cipherteks yang dihasilkan adalah

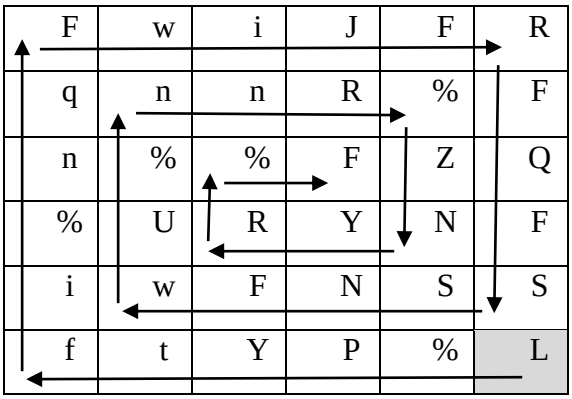
L%PYtfi%nqFwiJFRFQFSSNFwU%nnR%ZNYR%F

Berdasarkan proses enkripsi pesan dengan menggunakan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher* dengan plainteks “Ali dari Prodi MATEMATIKA UIN MALANG”. Plainteks dienkripsi dengan menggunakan algoritma *Caesar Cipher* dan diperoleh cipherteks ”Fqn%ifwn%Uwtin%RFYJRFYNPF%ZNS%RFQFSL”. Selanjutnya cipherteks

dienkripsi lagi menggunakan algoritma *Route Cipher* dan diperoleh cipherteks "L%PYtfi%nqFwiJFRFQFSSNFwU%nnR%ZNYR%F".

4.2 Dekripsi Pesan Menggunakan Algoritma Super Enkripsi *Caesar Cipher* dan *Route Cipher*

Dalam proses dekripsi, cipherteks yang digunakan adalah "L%PYtfi%nqFwiJFRFQFSSNFwU%nnR%ZNYR%F". Selanjutnya kunci yang digunakan dalam proses dekripsi adalah 5 untuk *Caesar Cipher* dan 6 untuk *Route Cipher*. Cipherteks ditulis secara spiral searah jarum jam dari kanan bawah. Selanjutnya kunci yang digunakan untuk membentuk matriks adalah 6.



Gambar 4.3 *Cipherteks Dekripsi Route Cipher*

Cipherteks yang telah disusun secara spiral dari kanan bawah dan searah jarum jam kemudian dibaca secara vertikal ke bawah dari kiri atas dan didapatkan hasil cipherteks.

1 F	2 w	3 i	4 J	5 F	6 R
q	n	n	R	%	F
n	%	%	F	Z	Q
%	U	R	Y	N	F
i	w	F	N	S	S
f	t	Y	P	%	L

Gambar 4.4 *Plainteks Dekripsi Route Cipher*

Sehingga plainteks yang dihasilkan adalah

Fqn%ifwn%Uwtin%RFYJRFYNPF%ZNS%RFQFSL

Selanjutnya setelah melakukan dekripsi dengan algoritma *Route Cipher* dan diperoleh painteks, akan dilanjutkan dengan melakukan dekripsi menggunakan algoritma *Caesar Cipher.* Untuk proses dekripsi plainteks diubah dulu ke benuk kode numerik didalam ASCII yang ditampilkan dalam tabel 4.3.

Tabel 4.3 *Kode Karakter Cipherteks untuk Dekripsi*

Karakter	Kode	Karakter	Kode	Karakter	Kode
F	70	i	105	F	70
q	113	n	110	%	37
n	110	%	37	Z	90
%	37	R	82	N	78
i	105	F	70	S	83
f	102	Y	89	%	37
w	119	J	74	R	82
n	110	R	82	F	70
%	37	F	70	Q	81
U	85	Y	89	F	70
w	119	N	78	S	83
t	116	P	80	L	76

Seanjunya akan didekripsi dengan algoritma *Caesar Cipher* menggunakan kunci yang sudah ditentukan. Penghitungan dekripsi adalah sebagai berikut:

$D(x) \equiv ((x - 32 - 5)\ mod\ 95 + 32\ )$

Selanjutnya masukkan plainteks pada rumus enkripsi di atas.

$D(F) \equiv \big((70 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 33\ mod\ 95 + 32 \equiv 65$

$D(q) \equiv \big((113 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 76\ mod\ 95 + 32 \equiv 108$

$$D(n) \equiv \big((110 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 73\ mod\ 95 + 32 \equiv 105$$

$$D(\%) \equiv \big((37 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 0\ mod\ 95 + 32 \equiv 32$$

$$D(i) \equiv \big((105 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 68\ mod\ 95 + 32 \equiv 100$$

$$D(f) \equiv \big((102 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 65\ mod\ 95 + 32 \equiv 97$$

$$D(w) \equiv \big((119 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 82\ mod\ 95 + 32 \equiv 114$$

$$D(n) \equiv \big((110 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 73\ mod\ 95 + 32 \equiv 105$$

$$D(\%) \equiv \big((37 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 0\ mod\ 95 + 32 \equiv 32$$

$$D(U) \equiv \big((85 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 48\ mod\ 95 + 32 \equiv 80$$

$$D(w) \equiv \big((119 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 77\ mod\ 95 + 32 \equiv 114$$

$$D(t) \equiv \big((116 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 74\ mod\ 95 + 32 \equiv 111$$

$$D(i) \equiv \big((105 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 63\ mod\ 95 + 32 \equiv 100$$

$$D(n) \equiv \big((110 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 73\ mod\ 95 + 32 \equiv 105$$

$$D(\%) \equiv \big((37 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 0\ mod\ 95 + 32 \equiv 32$$

$$D(R) \equiv \big((82 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 45\ mod\ 95 + 32 \equiv 77$$

$$D(F) \equiv \big((70 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 33\ mod\ 95 + 32 \equiv 65$$

$$D(Y) \equiv \big((89 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 52\ mod\ 95 + 32 \equiv 84$$

$$D(J) \equiv \big((74 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 37\ mod\ 95 + 32 \equiv 69$$

$$D(R) \equiv \big((82 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 45\ mod\ 95 + 32 \equiv 77$$

$$D(F) \equiv \big((70 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 33\ mod\ 95 + 32 \equiv 65$$

$$D(Y) \equiv \big((89 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 52\ mod\ 95 + 32 \equiv 84$$

$$D(N) \equiv \big((78 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 41\ mod\ 95 + 32 \equiv 73$$

$$D(P) \equiv \big((80 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 43\ mod\ 95 + 32 \equiv 75$$

$$D(F) \equiv \big((70 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 33\ mod\ 95 + 32 \equiv 65$$

$$D(\%) \equiv \big((37 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 0\ mod\ 95 + 32 \equiv 32$$

$D(Z) \equiv \big((90 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 53\ mod\ 95 + 32 \equiv 85$

$D(N) \equiv \big((78 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 41\ mod\ 95 + 32 \equiv 73$

$D(S)\ \equiv \big((83 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 46\ mod\ 95 + 32 \equiv 78$

$D(\%) \equiv \big((37 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 0\ mod\ 95 + 32 \equiv 32$

$D(R) \equiv \big((82 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 45\ mod\ 95 + 32 \equiv 77$

$D(F) \equiv \big((70 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 33\ mod\ 95 + 32 \equiv 65$

$D(Q) \equiv \big((81 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 44\ mod\ 95 + 32 \equiv 76$

$D(F) \equiv \big((70 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 33\ mod\ 95 + 32 \equiv 65$

$D(S) \equiv \big((83 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 46\ mod\ 95 + 32 \equiv 78$

$D(L) \equiv \big((76 - 32 - 5)\ mod\ 95 + 32\ \big) \equiv 39\ mod\ 95 + 32 \equiv 71$

Setelah melakukan penghitungan, kemudian kode-kode tersebut diubah kembali kebentuk karakter dalam ASCII yang ditampilkan dalam tabel 4.4.

Tabel 4.4 *Kode Karakter Plainteks untuk Dekripsi*

Kode	Karakter	Kode	Karakter	Kode	Karakter
65	A	100	d	65	A
108	l	105	i	32	(spasi)
105	i	32	(spasi)	85	U
32	(spasi)	77	M	73	I
100	d	65	A	78	N
97	a	84	T	32	(spasi)
114	r	69	E	77	M
105	i	77	M	65	A
32	(spasi)	65	A	76	L
80	P	84	T	65	A
114	r	73	I	78	N
111	o	75	K	71	G

Sehingga diperoleh plainteks dari tabel di atas yaitu

Ali dari Prodi MATEMATIKA UIN MALANG

Berdasarkan proses dekripsi pesan menggunakan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher* dengan Cipherteks L%PYtfi%nqFwiJFRFQFSSNFwU%nnR%ZNYR%F. Cipherteks didekripsi dengan menggunakan algoritma *Route Cipher* dan diperoleh plainteks Fqn%ifwn%Uwtin%RFYJRFYNPF%ZNS%RFQFSL. Selanjutnya plainteks didekripsi lagi menggunakan algoritma *Caesar Cipher* dan diperoleh plainteks "Ali dari Prodi MATEMATIKA UIN MALANG".

4.3 Analisis Keamanan Algoritma Super Enkripsi *Caesar Cipher* dan *Route Cipher*

Untuk mengetahui apakah algoritma super enkripsi memiliki keamanan yang lebih ditingkatkan, akan dilakukan analisis keamanan terhadap pesan yang telah dienkripsi. Berikut ini merupakan analisis keamanan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher*. Analisis keamanan dilakukan dengan membandingkan pesan yang dienkripsi hanya menggunakan algoritma *Caesar Cipher* dengan pesan yang dienkripsi menggunakan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher*. Analisis keamanan pesan dilakukan dengan menggunakan algoritma *Brute Force*. Pesan yang dienkripsi dengan algoritma *Caesar Cipher* diserang dengan algoritma *Brute Force* kemudian dibandingkan dengan pesan yang dienkripsi dengan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher* yang diserang dengan algoritma *Brute Force*.

1. Hasil Algoritma *Caesar Cipher*

   Cipherteks yang diperoleh darihasil enkripsi dengan algoritma *Caesar Cipher* selanjutnya akan dipecahkan dengan menggunakan algoritma *Brute Force*. Cipherteks yang akan dipecahkan adalah "Fqn%ifwn%Uwtin%RFYJRFYNPF%ZNS%RFQFSL". Algoritma *Brute Force* dilakukan secara manual dengan menggunakan semua kunci sebagai berikut.

   Kode numerik cipherteks: 70,113,110,37,105,102,119,110,37,85,119,116, 105,110,37,82,70,89,74,82,70,89,78,80,70,37,90,78,83,37,82,70,81,70,83,76

   Jika kunci yang dipakai adalah 1, maka:

   Kode numerik : 69,112,109,36,104,101,118,109,36,84,118,115,104,109,36, 81,69,88,73,81,69,88,77,79,69,36,89,77,82,36,81,69,80,69,82,75

   Kode karakter : Epm$hevm$Tvshm$QEXIQEXMOE$YMR$QEPERK

   Jika kunci yang dipakai adalah 2, maka:

   Kode numerik : 68,111,108,35,103,100,117,108,35,83,117,114,103,108,35, 80,68,87,72,80,68,87,76,78,68,35,88,76,81,35,80,68,79,68,81,74

   Kode karakter : Dol#gdul#Surgl#PDWHPDWLND#XLQ#PDODQJ

   Jika kunci yang dipakai adalah 3, maka:

   Kode numerik : 67,110,107,34,102,99,116,107,34,82,116,113,102,107,34, 79, 67,86,71,79,67,86,75,77,67,34,87,75,80,34,79,67,78,67,80,73

   Kode karakter : Cnk"fctk"Rtqfk"OCVGOCVC"WKP"OCNCPI

   Jika kunci yang dipakai adalah 4, maka:

   Kode numerik : 66,109,106,33,101,98,115,106,33,81,115,112,101,106,33, 78, 66,85,70,78,66,85,74,76,66,33,86,74,79,33,78,66,77,66,79,72

Kode karakter : Bmj!ebsj!Qspej!NBUFNBUJLB!VJO!NBMBOH

Jika kunci yang dipakai adalah 5, maka:

Kode numerik : 65,108,105,32,100,97,114,105,32,80,114,111,100,105,32,77, 65,84,69,77,65,84,73,75,65,32,85,73,78,32,77,65,76,65,78,71

Kode karakter: Ali dari Prodi MATEMATIKA UIN MALANG

Setelah cipherteks diserang menggunakan algoritma *Brute Force*, plainteks berhasil didapatkan pada percobaan ke-5. Hal ini menandakan bahwa meskipun pesan telah disandikan menggunakan algoritma *Caesar Cipher*, pesan masih bisa dipecahkan jika menggunakan algoritma *Brute Force.*

2. Hasil Algoritma Super Enkripsi

Cipherteks yang diperoleh dari algoritma *Caesar Cipher* selanjutnya akan dipecahkan dengan menggunakan algoritma *Brute Force*. Cipherteks yang dipakai adalah "L%PYtfi%nqFwiJFRFQFSSNFwU%nnR%ZNYR%F". Algoritma *Brute Force* akan dilakukan secara manual dengan menggunakan semua kunci.

Kode numerik cipherteks : 76,37,80,89,116,102,105,37,110,113,70,119,105, 74,70,82,70,81,70,83,83,78,70,119,85,37,110,110,82,37,90,78,89,82,37,70

Jika kunci yang dipakai adalah 1, maka:

Kode numerik plainteks : 75,36,79,88,115,101,104,36,109,112,69,118,104, 73,69,81,69,80,69,82,82,77,69,118,84,36,109,109,81,36,89,77,88,81,36,69

Kode karakter : K$OXseh$mpEvhIEQEPERRMEvTmmQYMXQ$E

Jika kunci yang dipakai adalah 2, maka:

Kode numerik plainteks : 74,35,78,87,114,100,103,35,108,111,68,117,103, 72,68,80,68,79,68,81,81,76,68,117,83,35,108,108,80,35,88,76,87,80,35,68

Kode karakter : J#NWrdg#loDugHDPDODQQLDuS#llP#XLWP#D

Jika kunci yang dipakai adalah 3, maka:

Kode numerik plainteks : 73,34,77,86,113,99,102,34,107,110,67,116,102,71,
67,79,67,78,67,80,80,75,67,116,82,34,107,107,79,34,87,75,86,79,34,67

Kode karakter : I”MVqcf”knCtfGCOCNCPPKCtR”kkO”WKVO”C

Jika kunci yang dipakai adalah 4, maka:

Kode numerik plainteks : 72,33,76,85,112,98,101,33,106,109,66,115,101,70,
66,78,66,77,66,79,79,74,66,115,81,33,106,106,78,33,86,74,85,78,33,66

Kode karakter : H!LUpbe!jmBseFBNBMBOOJBsQ!jjN!VJUN!B

Jika kunci yang dipakai adalah 5, maka:

Kode numerik plainteks : 71,32,75,84,111,97,100,32,105,108,65,114,100,69,
65,77,65,76,65,78,78,73,65,114,80,32,105,105,77,32,85,73,84,77,32,65

Kode karakter : G KToad ilArdEAMALANNIArP iiM UITM A

Jika kunci yang dipakai adalah 6, maka:

Kode numerik plainteks : 70,126,74,83,110,96,99,126,104,107,64,113,99,
68,64,76,64,75,64,77,77,72,64,113,79,126,104,104,76,126,84,72,83,76,126,
64

Kode karakter : F~JSn`c~hk@qcD@L@K@MMH@qO~THSL~@

Jika kunci yang dipakai adalah 7, maka:

Kode numerik painteks : 69,125,73,82,109,95,98,125,103,106,63,112,98,67,
63,75,63,74,63,76,76,71,63,112,78,125,103,103,75,125,83,71,82,75,125,63

Kode karakter : E}IRm_b}gj?pbC?K?J?LLG?pN}SGRK}?

Jika kunci yang dipakai adalah 8, maka:

Kode numerik plainteks : 68,124,72,81,108,94,97,124,102,105,62,111,97,66,
62,74,62,73,62,75,75,70,62,111,77,124,102,102,74,124,82,70,81,74,124,62

Kode karakter : D|HQl^a|fi>aoB>J>I>KKF>oM|ffJ|RFQJ|>

Jika kunci yang dipakai adalah 9, maka:

Kode numerik plainteks : 67,123,71,80,107,93,96,123,101,104,61,110,96,65,
61,73,61,72,61,74,74,69,61,110,76,123,101,101,73,123,81,69,80,73,123,61

Kode karakter : C{GPk]`{eh=`nA=I=H=JJE=nL{eeI{QEPI{=

Jika kunci yang dipakai adalah 10, maka:

Kode numerik plainteks : 66,122,70,79,106,92,95,122,100,103,60,109,95,64,
60,72,60,71,60,73,73,68,60,109,75,122,100,100,72,122,80,68,79,72,122,60

Kode karakter : BzFOj_zdg<_m@<H<G<IID<mKzddHzPDOHz<

Jika kunci yang dipakai adalah 11, maka:

Kode numerik plainteks : 65,121,69,78,105,91,94,121,99,102,59,108,94,63,
59,71,59,70,59,72,72,67,59,108,74,121,99,99,71,121,79,67,78,71,121,59

Kode karakter : AyENi[^ycf;^l?;G;F;HHC;lJyccGyOCNGy;

Jika kunci yang dipakai adalah 12, maka:

Kode numerik plainteks : 64,120,68,77,104,90,93,120,98,101,58,107,93,62,
58,70,58,69,58,71,71,66,58,107,73,120,98,98,70,120,78,66,77,70,120,58

Kode karakter : @xDMhZ]xbe:]k>:F:E:GGB:kIxbbFxNBMFx:

Jika kunci yang dipakai adalah 13, maka:

Kode numerik plainteks : 63,119,67,76,103,89,92,119,97,100,57,106,92,61,
57,69,57,68,57,70,70,65,57,106,72,119,97,97,69,119,77,65,76,69,119,57

Kode karakter : ?wCLgY\wad9\j=9E9D9FFA9jHwaaEwMALEw9

Jika kunci yang dipakai adalah 14, maka:

Kode numerik plainteks : 62,118,66,75,102,88,91,118,96,99,56,105,91,60,
56,68,56,67,56,69,69,64,56,105,71,118,96,96,68,118,76,64,75,68,118,56

Kode karakter : >vBKfX[v`c8[i<8D8C8EE@8iGv``DvL@KDv8

Jika kunci yang dipakai adalah 15, maka:

Kode numerik plainteks : 61,117,65,74,101,87,90,117,95,98,55,104,90,59,
55,67,55,66,55,68,68,63,55,104,70,117,95,95,67,117,75,63,74,67,117,55

Kode karakter : =uAJeWZu_b7Zh;7C7B7DD?7hFu__CuK?CJu7

Jika kunci yang dipakai adalah 16, maka:

Kode numerik plainteks : 60,116,64,73,100,86,89,116,94,97,54,103,89,58,
54,66,54,65,54,67,67,62,54,103,69,116,94,94,66,116,74,62,73,66,116,54

Kode karakter : <t@IdVYt^a6Yg:6B6A6CC>6gEt^^BtJ>IBt6

Jika kunci yang dipakai adalah 17, maka:

Kode numerik plainteks : 59,115,63,72,99,85,88,115,93,96,53,102,88,57,53,
65,53,64,53,66,66,61,53,102,68,115,93,93,65,115,73,61,72,65,115,53

Kode karakter : ;s?HcUXs]`5Xf95A5@5BB=5fDs]]AsI=Has5

Jika kunci yang dipakai adalah 18, maka:

Kode numerik plainteks : 58,114,62,71,98,84,87,114,92,95,52,101,87,56,52,
64,52,63,52,65,65,60,52,101,67,114,92,92,64,114,72,60,71,64,114,52

Kode karakter : :r>GbTWr_4We84@4?4AA<4eCr\\@rH<G@r4

Jika kunci yang dipakai adalah 19, maka:

Kode numerik plainteks : 57,113,61,70,97,83,86,113,91,94,51,100,86,55,51,
63,51,62,51,64,64,59,51,100,66,113,91,91,63,113,71,59,70,63,113,51

Kode karakter : 9q=FaSVq[^3Vd73?3>3@@;3dBq[[?qG;F?q3

Jika kunci yang dipakai adalah 20, maka:

Kode numerik plainteks : 56,112,60,69,96,82,85,112,90,93,50,99,85,54,50, 62,50,61,50,63,63,58,50,99,65,112,90,90,62,112,70,58,69,62,112,50

Kode karakter : 8p<E`RUpZ]2Uc62>2=2??:2cApZZ>pF:E>p2

Jika kunci yang dipakai adalah 21, maka:

Kode numerik plainteks : 55,111,59,68,95,81,84,111,89,92,49,98,84,53,49, 61,49,60,49,62,62,57,49,98,64,111,89,89,61,111,69,57,68,61,111,49

Kode karakter : 7o;D_QToY\1Tb51=1<1>>91b@oYY=oE9D=o1

Jika kunci yang dipakai adalah 22, maka:

Kode numerik plainteks : 54,110,58,67,94,80,83,110,88,91,48,97,83,52,48, 60,48,59,48,61,61,56,48,97,63,110,88,88,60,110,68,56,67,60,110,48

Kode karakter : 6n:C^PSnX[0Sa40<0;0==80a?nXX<nD8C<n0

Jika kunci yang dipakai adalah 23, maka:

Kode numerik plainteks : 53,109,57,66,93,79,82,109,87,90,47,96,82,51,47, 59,47,58,47,60,60,55,47,96,62,109,87,87,59,109,67,55,66,59,109,47

Kode karakter : 5m9B]ORmWZ/R`3/;/:/<<7/`>mWW;mC7B;m/

Jika kunci yang dipakai adalah 24, maka:

Kode numerik plainteks : 52,108,56,65,92,78,81,108,86,89,46,95,81,50,46, 58,46,57,46,59,59,54,46,95,61,108,86,86,58,108,66,54,65,58,108,46

Kode karakter : 4l8A\NQlVY.Q_2.:.9.;;6._+lVV:lB6A:l.

Jika kunci yang dipakai adalah 25, maka:

Kode numerik plainteks : 51,107,55,64,91,77,80,107,85,88,45,94,80,49,45, 57,45,56,45,58,58,53,45,94,60,107,85,85,57,107,65,53,64,57,107,45

Kode karakter : 3k7@[MPkUX-P^1-9-8-::5-^<kUU9kA5@9k-

Jika kunci yang dipakai adalah 26, maka:

Kode numerik plainteks : 50,106,54,63,90,76,79,106,84,87,44,93,79,48,44,
56,44,55,44,57,57,52,44,93,59,106,84,84,56,106,64,52,63,56,106,44

Kode karakter : 2j6?ZLOjTW,O]0,8,7,994,];jTT8j@4?8j,

Jika kunci yang dipakai adalah 27, maka:

Kode numerik plainteks : 49,105,53,62,89,75,78,105,83,86,43,92,78,47,43,
55,43,54,43,56,56,51,43,92,58,105,83,83,55,105,63,51,62,55,105,43

Kode karakter : 1i5>YKNiSV+N\/+7+6+883+\:iSS7i?3>7i+

Jika kunci yang dipakai adalah 28, maka:

Kode numerik plainteks : 48,104,52,61,88,74,77,104,82,85,42,91,77,46,42,
54,42,53,42,55,55,50,42,91,57,104,82,82,54,104,62,50,61,54,104,42

Kode karakter : 0h4=XJMhRU*M[.*6*5*772*[9hRR6h>2=6h*

Jika kunci yang dipakai adalah 29, maka:

Kode numerik plainteks : 47,103,51,60,87,73,76,103,81,84,41,90,76,45,41,
53,41,52,41,54,54,49,41,90,56,103,81,81,53,103,61,49,60,53,103,41

Kode karakter : /g3<WILgQT)LZ-)5)4)661)Z8gQQ5g=1<5g)

Jika kunci yang dipakai adalah 30, maka:

Kode numerik plainteks : 46,102,50,59,86,72,75,102,80,83,40,89,75,44,40,
52,40,51,40,53,53,48,40,89,55,102,80,80,52,102,60,48,59,52,102,40

Kode karakter : .f2;VHKfPS(KY,(4(3(550(Y7fPP4f<0;4f(

Jika kunci yang dipakai adalah 31, maka:

Kode numerik plainteks : 45,101,49,58,85,71,74,101,79,82,39,88,74,43,39,
51,39,50,39,52,52,47,39,88,54,101,79,79,51,101,59,47,58,51,101,39

Kode karakter : -e1:UGJeOR’JX+’3’2’44/’X6eOO3e;/:3fe’

Jika kunci yang dipakai adalah 32, maka:

Kode numerik plainteks : 44,100,48,57,84,70,73,100,78,81,38,87,73,42,38,
50,38,49,38,51,51,46,38,87,53,100,78,78,50,100,58,46,57,50,100,38

Kode karakter : ,d09TFIdNQ&IW*&2&1&33.&W5dNN2d:.92d&

Jika kunci yang dipakai adalah 33, maka:

Kode numerik plainteks : 43,99,47,56,83,69,72,99,77,80,37,86,72,41,37,49,
37,48,37,50,50,45,37,86,52,99,77,77,49,99,57,45,56,49,99,37

Kode karakter : +c/8SEHcMP%HV)%1%0%22-%V4cMM1c9-81c%

Jika kunci yang dipakai adalah 34, maka:

Kode numerik plainteks : 42,98,46,55,82,68,71,98,76,79,36,85,71,40,36,48,
36,47,36,49,49,44,36,85,51,98,76,76,48,98,56,44,55,48,98,36

Kode karakter : *b.7RDGbLO$GU($0$/$11,$U3bLL0b8,70b$

Jika kunci yang dipakai adalah 35, maka:

Kode numerik plainteks : 41,97,45,54,81,67,70,97,75,78,35,84,70,39,35,47,
35,46,35,48,48,43,35,84,50,97,75,75,47,97,55,43,54,47,97,35

Kode karakter :)a-6QCFaKN#FT’#/#.#00+#T2aKK/a7+6/a#

Jika kunci yang dipakai adalah 36, maka:

Kode numerik plainteks : 40,96,44,53,80,66,69,96,74,77,34,83,69,38,34,46,
34,45,34,47,47,42,34,83,49,96,74,74,46,96,54,42,53,46,96,34

Kode karakter : (`,5PBE`JM”ES&”.”-“//*”S1`JJ.`6*5.`”

Jika kunci yang dipakai adalah 37, maka:

Kode numerik plainteks : 39,95,43,52,79,65,68,95,73,76,33,82,68,37,33,45,
33,44,33,46,46,41,33,82,48,95,73,73,45,95,53,41,52,45,95,33

Kode karakter : ‘_+4OAD_IL!DR%!-!,!..)!R0_II-_5)4-_!

Jika kunci yang dipakai adalah 38, maka:

Kode numerik plainteks :38,94,42,51,78,64,67,94,72,75,32,81,67,36,32,44,

32,43,32,45,45,40,32,81,47,94,72,72,44,94,52,40,51,44,94,32

Kode karakter : &^*3N@C^HK CQ$, + --(Q/^HH,^4(3,^

Jika kunci yang dipakai adalah 39, maka:

Kode numerik plainteks : 37,93,41,50,77,63,66,93,71,74,126,80,66,35,126,

43,126,42,126,44,44,39,126,80,46,93,71,71,43,93,51,39,50,43,93,126

Kode karakter : %])2M?B]GJ~BP#~+~*~,,'~P.]GG+]3'2+]~

Jika kunci yang dipakai adalah 40, maka:

Kode numerik plainteks : 36,92,40,49,76,62,65,92,70,73,125,79,65,34,125,

42,125,41,125,43,43,38,125,79,45,92,70,70,42,92,50,38,49,42,92,125

Kode karakter : $\(1L>A\FI}AO"}*})}++&}O-\FF*\2&1*\}

Jika kunci yang dipakai adalah 41, maka:

Kode numerik plainteks : 35,91,39,48,75,61,64,91,69,72,124,78,64,33,124,

41,124,40,124,42,42,37,124,78,44,91,69,69,41,91,49,37,48,41,91,124

Kode karakter : #['0K=@[EH|@N!|)|(|**%|N,[EE)[1%0)[|

Jika kunci yang dipakai adalah 42, maka:

Kode numerik plainteks : 34,90,38,47,74,60,63,90,68,71,123,77,63,32,123,

40,123,39,123,41,41,36,123,77,43,90,68,68,40,90,48,36,47,40,90,123

Kode karakter : "Z&/J<?ZDG{?M {({'})${M+ZDD(Z0$/(Z{

Jika kunci yang dipakai adalah 43, maka:

Kode numerik plainteks : 33,89,37,46,73,59,62,89,67,70,122,76,62,126,122,

39,122,38,122,40,40,35,122,76,42,89,67,67,39,89,47,35,46,39,89,122

Kode karakter : !Y%.I;>YCFz>L~z'z&z((#zL*YCC'Y/#.'Yz

Jika kunci yang dipakai adalah 44, maka:

Kode numerik plainteks : 32,88,36,45,72,58,61,88,66,69,121,75,61,125,121,
38,121,37,121,39,39,34,121,75,41,88,66,66,38,88,46,34,45,38,88,121

Kode karakter : X$-H:=XBEy=K}y&y%y’”yK)XBB&X.”-&Xy

Jika kunci yang dipakai adalah 45, maka:

Kode numerik plainteks : 126,87,35,44,71,57,60,87,65,68,120,74,60,124,
120,37,120,36,120,38,38,33,120,74,40,87,65,65,37,87,45,33,44,37,87,120

Kode karakter : ~W#,G9<WADx<J|x%x$x&&!xJ(WAA%W-!,%Wx

Jika kunci yang dipakai adalah 46, maka:

Kode numerik plainteks : 125,86,34,43,70,56,59,86,64,67,119,73,59,123,
119,36,119,35,119,37,37,32,119,73,39,86,64,64,36,86,44,32,43,36,86,119

Kode karakter : }V”+F8;V@Cw;I{w$w#w%% wI’V@@$V,+$Vw

Jika kunci yang dipakai adalah 47, maka:

Kode numerik plainteks : 124,85,33,42,69,55,58,85,63,66,118,72,58,122,
118,35,118,34,118,36,36,126,118,72,38,85,63,63,35,85,43,126,42,35,85,11
8

Kode karakter : |U!*E7:U?Bv:Hzzv#v”v$$~vH&U??#U+~*#Uv

Jika kunci yang dipakai adalah 48, maka:

Kode numerik plainteks : 123,84,32,41,68,54,57,84,62,65,117,71,57,121,
117,34,117,33,117,35,35,125,117,71,37,84,62,62,34,84,42,125,41,34,84,11
7

Kode karakter : {T)D69T>Au9Gyu”u!u##}uG%T>>”T*})”Tu

Jika kunci yang dipakai adalah 49, maka:

Kode numerik plainteks : 122,83,126,40,67,53,56,83,61,64,116,70,56,120,116,33,116,32,116,34,34,124,116,70,36,83,61,61,33,83,41,124,40,33,83,116

Kode karakter : zS~(C58S=@t8Fxt!t t””|tF$S==!S)|(!St

Jika kunci yang dipakai adalah 50, maka:

Kode numerik plainteks : 121,82,125,39,66,52,55,82,60,63,115,69,55,119,115,32,115,126,115,33,33,123,115,69,35,82,60,60,32,82,40,123,39,32,82,115

Kode karakter : yR}’B47R<?s7Ews s~s!!{sE#R<< R({‘ Rs

Jika kunci yang dipakai adalah 51, maka:

Kode numerik plainteks : 120,81,124,38,65,51,54,81,59,62,114,68,54,118,114,126,114,125,114,32,32,122,114,68,34,81,59,59,126,81,39,122,38,126,81,114

Kode karakter : xQ|&A36Q;>r6Dvr~r}r zrD”Q;;~Q’z&~Qr

Jika kunci yang dipakai adalah 52, maka:

Kode numerik plainteks : 119,80,123,37,64,50,53,80,58,61,113,67,53,117,113,125,113,124,113,126,126,121,113,67,33,80,58,58,125,80,38,121,37,125,80,113

Kode karakter : wP{%@25P:=q5Cuq}q|q~~yqC!P::}P&y%}Pq

Jika kunci yang dipakai adalah 53, maka:

Kode numerik plainteks : 118,79,122,36,63,49,52,79,57,60,112,66,52,116,112,124,112,123,112,125,125,120,112,66,32,79,57,57,124,79,37,120,36,124,79,112

Kode karakter : vOz$?14O9<p4Btp|p{p}}xpB O99|O%x$|Op

Jika kunci yang dipakai adalah 54, maka:

Kode numerik plainteks : 117,78,121,35,62,48,51,78,56,59,111,65,51,115,111,123,111,122,111,124,124,119,111,65,126,78,56,56,123,78,36,119,35,123,78,111

Kode karakter : uny#>03N8;o3Aso{ozo||woA~N88{N$w#{No

Jika kunci yang dipakai adalah 55, maka:

Kode numerik plainteks : 116,77,120,34,61,47,50,77,55,58,110,64,50,114,110,122,110,121,110,123,123,118,110,64,125,77,55,55,122,77,35,118,34,122,77,110

Kode karakter : tMx”=/2M7:n2@rnznyn{{vn@}M77zM#v”zMn

Jika kunci yang dipakai adalah 56, maka:

Kode numerik plainteks : 115,76,119,33,60,46,49,76,54,57,109,63,49,113,109,121,109,120,109,122,122,117,109,63,124,76,54,54,121,76,34,117,33,121,76,109

Kode karakter : sLw!<.1L69m1?qmymxmzzum?|L66yL”u!yLm

Jika kunci yang dipakai adalah 57, maka:

Kode numerik plainteks : 114,75,118,32,59,45,48,75,53,56,108,62,48,112,108,120,108,119,108,121,121,116,108,62,123,75,53,53,120,75,33,116,32,120,75,108

Kode karakter : rKv ;-0K58l0>plxlwlyytl>{K55xK!t xKl

Jika kunci yang dipakai adalah 58, maka:

Kode numerik plainteks : 113,74,117,126,58,44,47,74,52,55,107,61,47,111,107,119,107,118,107,120,120,115,107,61,122,74,52,52,119,74,32,115,126,119,74,107

Kode karakter : qJu~:,/J47k/=okwkvkxxsk=zJ44wJ s~wJk

Jika kunci yang dipakai adalah 59, maka:

Kode numerik plainteks : 112,73,116,125,57,43,46,73,51,54,106,60,46,110,106,118,106,117,106,119,119,114,106,60,121,73,51,51,118,73,126,114,125,118,73,106

Kode karakter : pit}9+.I36j.<njvjujwwrj<yI33vI~r}vIj

Jika kunci yang dipakai adalah 60, maka:

Kode numerik plainteks : 111,72,115,124,56,42,45,72,50,53,105,59,45,109,105,117,105,116,105,118,118,113,105,59,120,72,50,50,117,72,125,113,124,117,72,105

Kode karakter : oHs|8*-H25i-;miuitivvqi:xH22uH}q|uHi

Jika kunci yang dipakai adalah 61, maka:

Kode numerik plainteks : 110,71,114,123,55,41,44,71,49,52,104,58,44,108,104,116,104,115,104,117,117,112,104,58,119,71,49,49,116,71,124,112,123,116,71,104

Kode karakter : nGr{7),G14h:,lhthshuuph:wG11tG|p{tGh

Jika kunci yang dipakai adalah 62, maka:

Kode numerik plainteks : 109,70,113,122,54,40,43,70,48,51,103,57,43,107,103,115,103,114,103,116,116,111,103,57,118,70,48,48,115,70,123,111,122,115,70,103

Kode karakter : mFqz6(+F03g+9kgsgrgttog9vF00sF{ozsFg

Jika kunci yang dipakai adalah 63, maka:

Kode numerik plainteks : 108,69,112,121,53,39,42,69,47,50,102,56,42,106,102,114,102,113,102,115,115,110,102,56,117,69,47,47,114,69,122,110,121,114,69,102

Kode karakter : lEpy5'*E/2f*8jfrfqfssnf8uE//rEznyrEf

Jika kunci yang dipakai adalah 64, maka:

Kode numerik plainteks : 107,68,111,120,52,38,41,68,46,49,101,55,41,105,101,113,101,112,101,114,114,109,101,55,116,68,46,46,113,68,121,109,120,113,68,101

Kode karakter : kDox4&)D.1e)7ieqeperrme7tD..qDymxqDe

Jika kunci yang dipakai adalah 65, maka:

Kode numerik plainteks : 106,67,110,119,51,37,40,67,45,48,100,54,40,104,100,112,100,111,100,113,113,108,100,54,115,67,45,45,112,67,120,108,119,112,67,100

Kode karakter : jCnw3%(C-0d(6hdpdodqqld6sC--pCxlwpCd

Jika kunci yang dipakai adalah 66, maka:

Kode numerik plainteks : 105,66,109,118,50,36,39,66,44,47,99,53,39,103,99,111,99,110,99,112,112,107,99,53,114,66,44,44,111,66,119,107,118,111,66,99

Kode karakter : iBmv2$'B,/c'5gcocncppkc5rB,,oBwkvBc

Jika kunci yang dipakai adalah 67, maka:

Kode numerik plainteks : 104,65,108,117,49,35,38,65,43,46,98,52,38,102,98,110,98,109,98,111,111,106,98,52,113,65,43,43,110,65,118,106,117,110,65,98

Kode karakter : hAlu1#&A+.b&4fbnbmboojb4qA++nAvjunAb

Jika kunci yang dipakai adalah 68, maka:

Kode numerik plainteks : 103,64,107,116,48,34,37,64,42,45,97,51,37,101, 97,109,97,108,97,110,110,105,97,51,112,64,42,42,109,64,117,105,116,109, 64,97

Kode karakter : g@kt0”%@*-a%3eamalannia3p@**m@uitm@a

Jika kunci yang dipakai adalah 69, maka:

Kode numerik plainteks : 102,63,106,115,47,33,36,63,41,44,96,50,36,100, 96,108,96,107,96,109,109,104,96,50,111,63,41,41,108,63,116,104,115,108, 63,96

Kode karakter : f?js/!$?),`$2d`l`k`mmh`2o?))l?thsl?`

Jika kunci yang digunakan adalah 70, maka:

Kode numerik plainteks : 101,62,105,114,46,32,35,62,40,43,95,49,35,99,95, 107,95,106,95,108,108,103,95,49,110,62,40,40,107,62,115,103,114,107,62, 95

Kode karakter : e>ir. #>(+_#1c_k_j_llg_1n>((k>sgrk>_

Jika kunci yang dipakai adalah 71, maka:

Kode numerik plainteks : 100,61,104,113,45,126,34,61,39,42,94,48,34,98, 94,106,94,105,94,107,107,102,94,48,109,61,39,39,106,61,114,102,113,106, 61,94

Kode karakter : d=hq-~”=’*^”0b^j^i^kkf^0m=’’j=rfqj=^

Jika kunci yang dipakai adalah 72, maka:

Kode numerik plainteks : 99,60,103,112,44,125,33,60,38,41,93,47,33,97,93, 105,93,104,93,106,106,101,93,47,108,60,38,38,105,60,113,101,112,105,60, 93

Kode karakter : c<gp,}!<&)]!/a]i]h]jje]/l<&&i<qepi<]

Jika kunci yang dipakai adalah 73, maka:

Kode numerik plainteks : 98,59,102,111,43,124,32,59,37,40,92,46,32,96,92,104,92,103,92,105,105,100,92,46,107,59,37,37,104,59,112,100,111,104,59,92

Kode karakter : b;fo+| ;%(\ .`\h\g\iid\.k;%%h;pdoh;\

Jika kunci yang dipakai adalah 74, maka:

Kode numerik plainteks : 97,58,101,110,42,123,126,58,36,39,91,45,126,95,91,103,91,102,91,104,104,99,91,45,106,58,36,36,103,58,111,99,110,103,58,91

Kode karakter : a:en*{~:$'[~-_[g[f[hhc[-j:$$g:ocng:[

Jika kunci yang dipakai adalah 75, maka:

Kode numerik plainteks : 96,57,100,109,41,122,125,57,35,38,90,44,125,94,90,102,90,101,90,103,103,98,90,44,105,57,35,35,102,57,110,98,109,102,57,90

Kode karakter : `9dm)z}9#&Z,}^ZfZeZggbZ,i9##f9nbmf9Z

Jika kunci yang dipakai adalah 76, maka:

Kode numerik plainteks : 95,56,99,108,40,121,124,56,34,37,89,43,124,93,89,101,89,100,89,102,102,97,89,43,104,56,34,34,101,56,109,97,108,101,56,89

Kode karakter : _8cl(y|8"%Y+|]YeYdYffaY+h8""e8male8Y

Jika kunci yang dipakai adalah 77, maka:

Kode numerik plainteks : 94,55,98,107,39,120,123,55,33,36,88,42,123,92,
88,100,88,99,88,101,101,96,88,42,103,55,33,33,100,55,108,96,107,100,55,
88

Kode karakter : ^7bk’x{7!$X*{\XdXcXee`X*g7!!d7l`kd7X

Jika kunci yang dipakai adalah 78, maka:

Kode numerik plainteks : 93,54,97,106,38,119,122,54,32,35,87,41,122,91,
87,99,87,98,87,100,100,95,87,41,102,54,32,32,99,54,107,95,106,99,54,87

Kode karakter :]6aj&wz6 #W)z[WcWbWdd_W)f6 c6k_jc6W

Jika kunci yang dipakai adalah 79, maka:

Kode numerik plainteks : 92,53,96,105,37,118,121,53,126,34,86,40,121,90,
86,98,86,97,86,99,99,94,86,40,101,53,126,126,98,53,106,94,105,98,53,86

Kode karakter : \5`i%vy5~”V(yZVbVaVcc^V(e5~~b5j^ib5V

Jika kunci yang dipakai adalah 80, maka:

Kode numerik plainteks : 91,52,95,104,36,117,120,52,125,33,85,39,120,89,
85,97,85,96,85,98,98,93,85,39,100,52,125,125,97,52,105,93,104,97,52,85

Kode karakter : [4_h$ux4}!U’xYUaU`Ubb]U’d4}}a4i]ha4U

Jika kunci yang dipakai adalah 81, maka:

Kode numerik plainteks : 90,51,94,103,35,116,119,51,124,32,84,38,119,88,
84,96,84,95,84,97,97,92,84,38,99,51,124,124,96,51,104,92,103,96,51,84

Kode karakter : Z3^g#tw3| T&wXT`T_Taa\T&c3||`3h\g`3T

Jika kunci yang dipakai adalah 82, maka:

Kode numerik plainteks : 89,50,93,102,34,115,118,50,123,126,83,37,118,87,
83,95,83,94,83,96,96,91,83,37,98,50,123,123,95,50,103,91,102,95,50,83

Kode karakter : Y2]f’sv2{~S%WS_S^R^``[S%b2{{_2g[f_2S

Jika kunci yang dipakai adalah 83, maka:

Kode numerik plainteks : 88,49,92,101,33,114,117,49,122,125,82,36,117,86,
82,94,82,93,82,95,95,90,82,36,97,49,122,122,94,49,102,90,101,94,49,82

Kode karakter : X1\e!ru1z}R$VR^R]R]__ZR$a1zz^1fZe^1R

Jika kunci yang dipakai adalah 84, maka:

Kode numerik plainteks : 87,48,91,100,32,113,116,48,121,124,81,35,116,85,
81,93,81,92,81,94,94,89,81,35,96,48,121,121,93,48,101,89,100,93,48,81

Kode karakter : W0[d qt0y|Q#UQ]Q\Q^^YQ#`0yy]0eYd]0Q

Jika kunci yang dipakai adalah 85, maka:

Kode numerik plainteks : 86,47,90,99,126,112,115,47,120,123,80,34,115,84,
80,92,80,91,80,93,93,88,80,34,95,47,120,120,92,47,100,88,99,92,47,80

Kode karakter : V/Zc~ps/x{P”TP|P[P]]XP”_/xx\/dXc\/P

Jika kunci yang dipakai adalah 86, maka:

Kode numerik plainteks : 85,46,89,98,125,111,114,46,119,122,79,33,114,83,
79,91,79,90,79,92,92,87,79,33,94,46,119,119,91,46,99,87,98,91,46,79

Kode karakter : U.Yb}or.wzO!SO[OZO\\WO!^.ww[.cWb[.O

Jika kunci yang dipakai adalah 87, maka:

Kode numerik plainteks : 84,45,88,97,124,110,113,45,118,121,78,32,113,82,
78,90,78,89,78,91,91,86,78,32,93,45,118,118,90,45,98,86,97,90,45,78

Kode karakter : T-Xa|nq-vyN qRNZNYN[[VN]-vvZ-bVaZ-N

Jika kunci yang dipakai adalah 88, maka:

Kode numerik plainteks : 83,44,87,96,123,109,112,44,117,120,77,126,112,
81,77, 89,77,88,77,90,90,85,77,126,92,44,117,117,89,44,97,85,96,89,44,77

Kode karakter : S,W`{mp,uxM~pQMYMXMZZUM~\,uuY,aU`Y,M

Jika kunci yang dipakai adalah 89, maka:

Kode numerik plainteks : 82,43,86,95,122,108,111,43,116,119,76,125,111,
80,76,88,76,87,76,89,89,84,76,125,91,43,116,116,88,43,96,84,95,88,43,76

Kode karakter : R+V_zlo+twL}oPLXLWLYYTL}[+ttX+`T_X+L

Jika kunci yang dipakai adalah 90, maka:

Kode numerik plainteks : 81,42,85,94,121,107,110,42,115,118,75,124,110,
79,75,87,75,86,75,88,88,83,75,124,90,42,115,115,87,42,95,83,94,87,42,75

Kode karakter : Q*U^ykn*svK|nOKWKVKXXSK|Z*ssW*_S^W*K

Jika kunci yang dipakai adalah 91, maka:

Kode numerik plainteks : 80,41,84,93,120,106,109,41,114,117,74,123,109,
78,74,86,74,85,74,87,87,82,74,123,89,41,114,114,86,41,94,82,93,86,41,74

Kode karakter : P)T]xjm)ruJ{mNJVJUJWWRJ{Y)rrV)^R]V)J

Jika kunci yang dipakai adalah 92, maka:

Kode numerik plainteks : 79,40,83,92,119,105,108,40,113,116,73,122,108,
77,73,85,73,84,73,86,86,81,73,122,88,40,113,113,85,40,93,81,92,85,40,73

Kode karakter : O(S\wil(qtIzlMIUITIVVQIzX(qqU(]Q\U(I

Jika kunci yang dipakai adalah 93, maka:

Kode numerik plainteks : 78,39,82,91,118,104,107,39,112,115,72,121,107,
76,72,84,72,83,72,85,85,80,72,121,87,39,112,112,84,39,92,80,91,84,39,72

Kode karakter : N’R[vhk’psHykLHTHSHUUPHyW’ppT’\P[T’H

Jika kunci yang dipakai adalah 94, maka:

Kode numerik plainteks : 77,38,81,90,117,103,106,38,111,114,71,120,106,
75,71,83,71,82,71,84,84,79,71,120,86,38,111,111,83,38,91,79,90,83,38,71

Kode karakter : M&QZugj&orGxjKGSGRGTTOGxV&ooS&[OZS&G

Jika kunci yang dipakai adalah 95, maka:

Kode numerik plainteks : 76,37,80,89,116,102,105,37,110,113,70,119,105,74,70,82,70,81,70,83,83,78,70,119,85,37,110,110,82,37,90,78,89,82,37,70

Kode karakter : L%PYtfi%nqFwiJFRFQFSSNFwU%nnR%ZNYR%F

Setelah mencoba memecahkan cipherteks dengan menggunakan semua kunci, plainteks masih belum bisa dibaca. Hal ini menunjukkan bahwa pesan yang di enkripsi menggunakan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher* lebih aman dari pada pesan yang hanya di enkripsi menggunakan algoritma *Caesar Cipher* saja.

4.4. Kriptografi dalam Pandangan Islam

Dalam pandangan Islam, kriptografi bisa juga di anggap sebagai perwujudan dari sifat amanah. Amanah sendiri merupakan salah satu sifat mulia yang dimiliki oleh Rasulullah SAW. Sifat amanah juga sejalan dengan perintah Allah dalam surat An Nisa ayat 58. Kriptografi bisa disebut sebagai perwujudan dari sifat amanah karena penggunaan kriptografi ditujukan agar pesan yang ingin disampaikan kepada seseorang tidak diketahui oleh orang lain atau agar hanya diketahui oleh penerima pesan yang mana sejalan dengan sifat amanah.

Sebagai manusia kita mengemban amanah sebagai pemimpin di muka bumi, minimal memimpin diri kita sendiri. Kita juga berinteraksi dengan manusia yang lainnya yang juga akan membuat kita memikul amanah lainnya, seperti kepercayaan, kejujuran, janji, ataupun tanggung jawab lainnya. Berdasarkan penjelasan pada sub bab sebelumnya, maka setiap pengirim dan penerima pesan mempunyai tanggung jawab untuk menjaga keamanan pesan tersebut agar tidak diketahui oleh orang lain.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pembahasan dapat diperoleh kesimpulan sebagai berikut:

1. Pada proses enkripsi pesan menggunakan algoritma super enkripsi yang dikakukan dengan menggunakan dua algoritma yaitu *Caesar Cipher* dan *Route Cipher.* Rumus yang dipakai dalam proses enkripsi dengan algoritma *Caesar Cipher* adalah $E(x) = ((x - 32 + 5)\ mod\ 95 + 32\ )$. setelah mendapatkan hasil enkripsi dilanjutkan dengan melakukan enkripsi menggunakan algoritma *Route Cipher*. Dalam proses enkripsi algoritma *Route Cipher* pesan disusun secara vertikal dari atas ke bawah kemudian akan dibaca secara spiral dari kanan bawah dan searah jarum jam.
2. Pada proses dekripsi untuk mengembalikan cipherteks kebentuk pesan asli (plainteks) dilakukan penghitungan dengan algoritma *Route Cipher* kemudian dilanjutkan dengan algoritma *Caesar Cipher.* Kebalikan dari proses enkripsi, pada proses dekripsi menggunakan algoritma *Route Cipher* cipherteks disusun secara spiral dari kanan bawah dan searah jarum jam kemudian akan dibaca secara vertikal ke bawah dari kiri atas. Setelah mendapatkan hasil dekripsi di lanjutkan dengan melakukan dekripsi menggunakan algoritma *Caesar Cipher*. Rumus yang dipakai dalam proses dekripsi dengan algoritma *Caesar Cipher* adalah $D(x) = ((x - 32 - 5)\ mod\ 95 + 32\ )$.
3. Dalam analisis keamanan pada cipherteks yang hanya memakai algoritma *Caesar Cipher*, isi pesan dapat diketahui jika cipherteks dipecahkan

menggunakan algoritma *Brute Force*. Sedangkan untuk cipherteks yang diamankan dengan algoritma super enkripsi *Caesar Cipher* dan *Route Cipher*, isi pesan tidak dapat diketahui setelah ciherteks diserang menggunakan algoritma *Brute Force*.

5.2 Saran

Untuk penelitian selanjutnya disarankan untuk melakukan modifikasi pada algoritma *Caesar Cipher*. Sedangkan untuk algoritma *Route Cipher* disarankan untuk menggunakan rute yang lain.

DAFTAR PUSTAKA

(LPMQ). (2022). *L.P.M.A.-Q.* Qur,an Kemenag.

Al-Sheikh, D. A. (2001). *Tafsir Ibnu Katsir Jilid 2.* Bogor: Pustaka Imam asy-Syafi'i.

Andika, T., Taquyyudin, M., & Admizal, I. (2020). Amanah dan Khianat dalam Al-Qur'an Menurut Quraish Shihab. *Jurnal Ilmu Al-Qur'an dan Tafsir*, 5(02).

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi.* Yogyakarta: C.V Andi Offset.

Bakri, A. A., Muhammad, M. A., Khalaf, M. A., & Hamid, M. M. (2007). *Tafsir Ath-Thabari jilid 7.* Jakarta: Pustaka Azzam.

Bangun, M. S. (2019). Implementasi Algoritma Route Cipher Dalam Pengamanan File Pdf. *Building of Informatics, Technology and Science (BITS)*, 1-6.

Dalimunthe, R. P. (2016). Amanah Dalam Perspektif Hadis. *Jurnal Ilmu Hadis 1*, 7-16.

Girsang, N. D., Siagian, H., Santso, M. H., Wahyudi, A., & Sitorus, B. A. (2019). Kombinasi Algoritma Kriptografi Transposisi Rail Fence Cipher dan Route Cipher. *Seminar Nasinal Teknologi Informatika*, 2(1).

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

Kurnia, A. D. (2013). Optimasi Konversi String Biner Hasil Least Significant Bit Steganography.

Latifah, Ambo, & Kurnia. (2017). Modifikasi Algoritma Caesar Cipher dan Rail Fence Untuk Peningkatan Keamanan Teks Alfanumerik dan Karakter Khusus. *Prosiding Semnastek*, ISSN:2407-1846.

Mukhtar, H. (2018). *Kriptografi untuk mengamankan data.* Yogyakarta: Deepublish.

Munir, R. (2019). *Kriptografi Edisi ke Dua.* Bandung: Informatika.

Nuraini, R. (2015). Desain Algorithma Operasi Perkalian Matriks Menggunakan Metode Flowchart. *Jurnal Teknik Komputer Amik BSI*, 1(1).

Ruminta. (2014). *Matriks Persamaan Linier dan Pemrograman Linier.* Bandung: Rekayasa Sains.

Santoso, B. W., Sundawa, F., & Azhari, M. (2016). Implementasi Algoritma Brute Force Sebagai Mesin Pencari (Search Engine) Berbasis Web Pada Database. *Jurnal Sisfitek Global*, 6(1).

Sasongko, J. (2005). Pengamanan Data Informasi Menggunakan Kriptografi Klasik. *Jurnal Teknologi Informasi Dinamik*, X(3).

Setyaningsih, E., Iswahyudi, C., & Widyastuti, N. (2011). Konsep Super Enkripsi Untuk Meningkatkan Keamanan Data Citra. *Seminar Nasional Sistem & Teknologi Informasi* .

Singh, A., Nandal, A., & Malik, S. (2012). Implementasi of Caesar Cipher with Rail Fence for Enchanging Data Security. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, Vol 2, Issue 12.

Wahyuni, N. F. (2019). Perancangan Aplikasi Penyandian File Teks Menggunakan Algoritma Route Cipher Berbasis Dekstop. *Jurnal Pelita Informasi*, Volume 8, Nomer 1.

LAMPIRAN

Lampiran 1 Tabel Kode ASCII (Kode Karakter 32-126)

Karakter	Hexadesimal	Desimal	Keterangan
(space)	0020	32	Spasi
!	0021	33	Tanda seru (exclamation)
"	0022	34	Tanda kutip dua
#	0023	35	Tanda pagar (kres)
$	0024	36	Tanda mata uang dolar
%	0025	37	Tanda persen
&	0026	38	Karakter ampersan (&)
‘	0027	39	Karakter Apostrof
(	0028	40	Tanda kurung buka
)	0029	41	Tanda kurung tutup
*	002A	42	Karakter asteris (bintang)
+	002B	43	Tanda tambah (plus)
,	002C	44	Karakter koma
-	002D	45	Karakter hyphen (strip)
.	002E	46	Tanda titik

/	002F	47	Garis miring (*slash*)
0	0030	48	Angka nol
1	0031	49	Angka satu
2	0032	50	Angka dua
3	0033	51	Angka tiga
4	0034	52	Angka empat
5	0035	53	Angka lima
6	0036	54	Angka enam
7	0037	55	Angka tujuh
8	0038	56	Angka delapan
9	0039	57	Angka sembilan
:	003A	58	Tanda titik dua
;	003B	59	Tanda titik koma
<	003C	60	Tanda lebih kecil
=	003D	61	Tanda sama dengan
>	003E	62	Tanda lebih besar
?	003F	63	Tanda tanya

@	0040	64	A keong (@)
A	0041	65	Huruf latin A kapital
B	0042	66	Huruf latin B kapital
C	0043	67	Huruf latin C kapital
D	0044	68	Huruf latin D kapital
E	0045	69	Huruf latin E kapital
F	0046	70	Huruf latin F kapital
G	0047	71	Huruf latin G kapital
H	0048	72	Huruf latin H kapital
I	0049	73	Huruf latin I kapital
J	004A	74	Huruf latin J kapital
K	004B	75	Huruf latin K kapital
L	004C	76	Huruf latin L kapital
M	004D	77	Huruf latin M kapital
N	004E	78	Huruf latin N kapital
O	004F	79	Huruf latin O kapital
P	0050	80	Huruf latin P kapital

Q	0051	81	Huruf latin Q kapital
R	0052	82	Huruf latin R kapital
S	0053	83	Huruf latin S kapital
T	0054	84	Huruf latin T kapital
U	0055	85	Huruf latin U kapital
V	0056	86	Huruf latin V kapital
W	0057	87	Huruf latin W kapital
X	0058	88	Huruf latin X kapital
Y	0059	89	Huruf latin Y kapital
Z	005A	90	Huruf latin Z kapital
[	005B	91	Kurung siku kiri
\	005C	92	Garis miring terbalik (*backslash*)
]	005D	93	Kurung sikur kanan
^	005E	94	Tanda pangkat
_	005F	95	Garis bawah (underscore)
`	0060	96	Tanda petik satu
a	0061	97	Huruf latin a kecil

b	0062	98	Huruf latin b kecil
c	0063	99	Huruf latin c kecil
d	0064	100	Huruf latin d kecil
e	0065	101	Huruf latin e kecil
f	0066	102	Huruf latin f kecil
g	0067	103	Huruf latin g kecil
h	0068	104	Huruf latin h kecil
i	0069	105	Huruf latin i kecil
j	006A	106	Huruf latin j kecil
k	006B	107	Huruf latin k kecil
l	006C	108	Huruf latin l kecil
m	006D	109	Huruf latin m kecil
n	006E	110	Huruf latin n kecil
o	006F	111	Huruf latin o kecil
p	0070	112	Huruf latin p kecil
q	0071	113	Huruf latin q kecil
r	0072	114	Huruf latin r kecil

s	0073	115	Huruf latin s kecil
t	0074	116	Huruf latin t kecil
u	0075	117	Huruf latin u kecil
v	0076	118	Huruf latin v kecil
w	0077	119	Huruf latin w kecil
x	0078	120	Huruf latin x kecil
y	0079	121	Huruf latin y kecil
z	007A	122	Huruf latin z kecil
{	007B	123	Kurung kurawal buka
|	007C	124	Garis vertikal (pipa)
}	007D	125	Kurung kurawal tutup
~	007E	126	Karakter gelombang (tilde)

RIWAYAT HIDUP

Ali Mahfudz, lahir di Kabupaten Bojonegoro pada tanggal 26 September 2000. Teman-temannya biasa memanggilnya Ali. Bertempat tinggal di jl. H. Mahmud Rt 01 Rw 01 Desa Lengkong, Kecamatan Balen, Kabupaten Bojonegoro. Merupakan putra dari Bapak Supriyanto dan Ibu Nurul Hidayah serta mempunyai seorang adik yang bernama Nur Rohman.

Jenjang pendidikannya dimulai sejak bersekolah di RA Mihtahul Huda di desa Lengkong yang lulus pada tahun 2006. Setelah itu melanjutkan pendidikan di MI Miftahul Huda Lengkong dan lulus pada tahun 2012. Pendidikan selanjutnya ditempuh diSMPN 1 Balen yang lulus pada tahun 2015. Kemudian melanjutkan pendidikan di SMAN 1 Sumberrejo yang lulus pada tahun 2018. Pada jenjang perguruan tinggi ia melanjutkan pendidikannya dengan berkuliah di UIN Maulana Malik Ibrahim Malang dengan menekuni bidang Matematika murni di Fakultas Sains dan Teknologi.

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

BUKTI KONSULTASI SKRIPSI

Nama : Ali Mahfudz
NIM : 18610107
Fakultas / Program Studi : Sains dan Teknologi / Matematika
Judul Skripsi : Modifikasi Algoritma Super Enkripsi Caesar Cipher dan Route Cipher untuk Mengamankan Pesan
Pembimbing I : Prof. Dr. H. Turmudi, M.Si., Ph.D
Pembimbing II : Ach. Nashichuddin, M.A

No	Tanggal	Hal	Tanda Tangan
1.	3 Februari 2022	Konsultasi Bab I	1.
2.	8 Februari 2022	Konsultasi Revisi Bab I	2.
3.	16 Februari 2022	Konsultasi Bab II dan III	3.
4.	25 Februari 2022	Konsultasi Revisi Bab II dan III	4.
5.	5 Maret 2022	Konsultasi Kajian Agama	5.
6.	14 Maret 2022	Konsultasi Revisi Kajian Agama	6.
7.	31 Maret 2022	ACC Seminar Proposal	7.
8.	31 Mei 2022	Konsultasi Bab IV dan V	8.
9.	13 Oktober 2022	Konsultasi Revisi Bab IV dan V	9.
10.	23 November 2022	Konsultasi Kajian Agama	10.
11.	29 November 2022	Konsultasi Revisi Kajian Agama	11.
12.	20 Desember 2022	ACC Matriks Revisi Seminar Hasil	12.
13.	26 Desember 2022	ACC Sidang Skripsi	13.
14.	28 Desember 2022	ACC Keseluruhan	14.

Malang, 28 Desember 2022
Mengetahui,
Ketua Program Studi Matematika

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