MODIFIKASI SUPER ENKRIPSI ALGORITMA BEAUFORT CIPHER DAN ROUTE CIPHER UNTUK MENGAMANKAN DATA PENDUDUK

SKRIPSI

OLEH:
MUHAMMAD FAHRUL ROIS
NIM. 18610110

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2025

MODIFIKASI SUPER ENKRIPSI ALGORITMA BEAUFORT CIPHER DAN ROUTE CIPHER UNTUK MENGAMANKAN DATA PENDUDUK

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
Muhammad Fahrul Rois
NIM. 18610110

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2025

MODIFIKASI SUPER ENKRIPSI ALGORITMA BEAUFORT CIPHER DAN ROUTE CIPHER UNTUK MENGAMANKAN DATA PENDUDUK

SKRIPSI

Oleh
Muhammad Fahrul Rois
NIM. 18610110

Telah Disetujui Untuk Diuji

Malang, 25 Juni 2025

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad khudzaifah, M.Si.	Erna Herawati, M.Pd.
NIPPPK. 19900511 202321 1 029	NIPPPK. 19760723 202321 2 006

Mengetahui,
Ketua Program Studi Matematika

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

MODIFIKASI SUPER ENKRIPSI ALGORITMA BEAUFORT CIPHER DAN ROUTE CIPHER UNTUK MENGAMANKAN DATA PENDUDUK

SKRIPSI

Oleh
Muhammad Fahrul Rois
NIM. 18610110

Telah Dipertahankan di Depan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Malang, 25 Juni 2025

Ketua Penguji	: Dr. Elly Susanti, M.Sc.	.....
Anggota Penguji 1	: Mohammad Nafie Jauhari, M.Si.	.....
Anggota Penguji 2	: Muhammad Khudzaifah, M.Si.	.....
Anggota Penguji 3	: Erna Herawati, 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 : Muhammad Fahrul Rois

NIM : 18610110

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Modifikasi Super Enkripsi Algoritma Beaufort Cipher dan Route Cipher Untuk Mengamankan Data Penduduk.

Menyatakan dengan sebenar-benarnya 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 dan pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka. Apabila di kemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 25 Juni 2025

Yang membuat pernyataan,

Muhammad Fahrul Rois

NIM. 18610110

HALAMAN MOTTO

"Akhiri Apa yang Pernah Kau Mulai"

HALAMAN PERSEMBAHAN

Bismillahirrahmanirrahim. Dengan mengucap segala puji dan syukur kepada Allah Swt. penulis persembahkan skripsi ini untuk ibu saya Mardliyah, ayah kandung saya Mad Thomaji yang telah tanpa pamrih melahirkan dan membesarkan saya, memberi dukungan dan dorongan baik moral maupun moril, serta menjadi teladan yang selalu memotivasi penulis untuk senantiasa kuat dan tabah melalui perjalanan panjang dalam menyelesaikan penelitian ini.

KATA PENGANTAR

Assalamualaikum warahmatullahi wabarakatuh.

Alhamdulillah, puji syukur peneliti panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat serta hidayah-Nya sehingga peneliti mampu menyelesaikan skripsi yang berjudul "Modifikasi Super Enkripsi Algoritma *Beaufort Cipher* dan *Route Cipher* Untuk Mengamankan Data Penduduk" dengan baik, dalam rangka mendapat gelar sarjana Matematika di Fakultas sains dan Teknologi, Universitas slam Negeri Maulana Malik ibrahim Malang. Shalawat serta salam semoga tetap tercurahkan kepada junjungan kita Nabi Muhammad SAW yang telah mengarahkan kita dari zaman kegelapan menuju zaman yang terang benerang yakni agama slam seperti yang kita rasakan sekarang ini.

Dalam proses mengerjakan skripsi ini, banyak bimbingan, masukan, serta arahan yang diterima oleh penulis. Oleh karena itu penulis ingin mengucapkan terimakasih melalui halaman ini kepada:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku Rektor Universitas slam Negeri Maulana Malik brahim Malang.
2. Prof. Dr. Hj. Sri Harini, M.Si., selaku Dekan Fakultas Sains dan Teknologi Universitas slam Negeri Maulana Malik brahim Malang.
3. Dr. Elly Susanti, M.Sc., selaku Ketua Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas slam Negeri Maulana Malik brahim Malang.
4. Muhammad Khuzaifah, M.Si, selaku Dosen Pembimbing yang telah memberikan banyak lmu, bimbingan, arahan, nasihat dan motivasi kepada penulis selama perkuliahan sampai penulisan skripsi ini.
5. Erna Herawati, M.Pd, selaku Dosen pembimbing I yang telah memberi bimbingan, arahan serta nasihat kepada penulis.
6. Seluruh Dosen Matematika, Fakultas Sains dan Teknologi, Universitas slam Negeri Maulana Malik brahim Malang.
7. Orang tua dan seluruh keluarga yang selalu memberi dukungan baik dalam bentuk moral maupun material, serta selalu mendoakan untuk kelancaran penulisan skripsi ini.

8. Seluruh teman teman yang selalu menemani dan memberi semangat dalam proses pengerjaan skripsi ini.

Akhir kata, penulis berharap semoga Allah SWT SWT berkenan membalas segala kebaikan semua pihak yang telah membantu dalam proses penulisan skripsi ini dan semoga skripsi ini membawa manfaat baik bagi penulis maupun pembaca.

Wassalamualaikum Warahmatullahi Wabarakatuh.

Malang, 25 Juni 2025

Penulis

DAFTAR ISI

HALAMAN JUDUL ..... **i**
HALAMAN PENGAJUAN ..... **ii**
HALAMAN PERSETUJUAN ..... **iii**
HALAMAN PENGESAHAN ..... **iv**
PERNYATAAN KEASLIAN TULISAN ..... **v**
HALAMAN MOTTO ..... **vi**
HALAMAN PERSEMBAHAN ..... **vii**
KATA PENGANTAR ..... **viii**
DAFTAR ISI ..... **x**
DAFTAR TABEL ..... **xii**
DAFTAR GAMBAR ..... **xiii**
ABSTRAK ..... **xiv**
ABSTRACT ..... **xv**
مستخلص البحث ..... **xvi**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Tujuan Penelitian 3
1.4 Manfaat Penelitian 4
1.5 Batasan Masalah 4
1.6 Definisi Istilah 5
BAB II KAJIAN TEORI **7**
2.1 Teori Pendukung 7
2.1.1 Keterbagian 7
2.1.2 Kongruensi 9
2.1.3 Modulo 11
2.1.4 Kriptografi 12
2.1.5 Enkripsi dan Dekripsi 14
2.1.6 Beaufort Cipher 14
2.1.7 Route Cipher 19
2.1.8 Super Enkripsi 22
2.2 Amanah Dalam Perspektif slam 26
2.3 Kajian Topik dengan Teori Pendukung 27
BAB III METODE PENELITIAN **30**
3.1 Jenis Penelitian 30
3.2 Pra Penelitian 30
3.3 Tahapan Penelitian 30
BAB IV PEMBAHASAN **35**
4.1 Algoritma Modifikasi Beaufort Cipher dengan Route Cipher 35
4.2 Simulasi proses Enkripsi dan Dekripsi Modifikasi Beaufort Cipher dengan Route Cipher 37
4.2.1 Simulasi Enkripsi Beaufort Cipher dengan Route Cipher 37
4.2.2 Simulasi Dekripsi Beaufort Cipher dengan Route Cipher 44
4.3 Kriptografi Dalam Perspektif Islam 52
BAB V PENUTUP **54**
5.1 Kesimpulan 54

5.2 Saran 54
DAFTAR PUSTAKA 55
RIWAYAT HIDUP 57

DAFTAR TABEL

Tabel 2.1 Tabel Konversi 16
Tabel 2.2 Tabel Konversi Enkripsi 17
Tabel 2.3 Tabel Konversi Dekripsi 18
Tabel 4.1 Tabel Data Kartu Keluarga 38
Tabel 4.2 Tabel Konversi 40
Tabel 4.3 Tabel Plaintext 52

DAFTAR GAMBAR

Gambar 2.1 Contoh Plainteks Enkripsi Route Cipher 21
Gambar 2.2 Contoh Ciphherteks Enkripsi Route Cipher..... 21
Gambar 2.3 Contoh Cipherteks Dekripsi Route Cipher..... 21
Gambar 2.4 Contoh Plainteks Dekripsi Route Cipher 22
Gambar 2.5 Contoh Plainteks Enkripsi Route Cipher 23
Gambar 2.6 Contoh Ciphherteks Enkripsi Route Cipher..... 23
Gambar 2.7 Contoh Cipherteks Dekripsi Route Cipher..... 25
Gambar 2.8 Contoh Plainteks Dekripsi Route Cipher 26
Gambar 3.1 Flowchart Enkripsi 33
Gambar 3.2 Flowchart Dekripsi..... 35
Gambar 4.1 Plainkey Enkripsi Route Cipher..... 39
Gambar 4.2 Cipherkey Enkripsi route Cipher 39
Gambar 4.3 Plainkey Dekripsi Route Cipher..... 46
Gambar 4.4 Cipherkey Dekripsi route Cipher 46

ABSTRAK

Rois, Muhammad F. 2025. **Modifikasi Super Enkripsi Algoritma Beaufort Cipher Dan Route Cipher Untuk Mengamankan Data Penduduk**. Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si. (II) Erna herawati, M.Pd.

Kata Kunci: Enkripsi, Dekripsi, Modifikasi Super Enkripsi, Beaufort Cipher, Route Cipher

Keamanan suatu data 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 modifikasi algoritma super enkripsi Beaufort Cipher dan Route Cipher. Tujuan penelitian ini yaitu untuk mengetahui proses enkripsi dan dekripsi dari algoritma super enkripsi Beaufort Cipher dan Route Cipher. Tahapan dalam penelitian ini menggunakan pendekatan kualitatif dengan metode *library research*. Dalam proses enkripsi dengan algoritma Route Cipher. *Cipherkey* disusun secara vertikal dari atas ke bawah kemudian akan dibaca secara spiral dari kanan bawah dan searah jarum jam untuk mengacak *cipherkey*. Selanjutnya *cipherkey* yang didapat dari enkripsi algoritma Route Cipher digunakan dalam proses enkripsi menggunakan algoritma Beaufort Cipher, rumus yang dipakai adalah $C_i = (K_i - P_i)\ mod\ 26$. Pada proses dekripsi menggunakan algoritma Route Cipher Cipherkey disusun secara vertikal dari atas ke bawah kemudian akan dibaca secara spiral dari kanan bawah dan searah jarum jam untuk mengacak Cipherkey. Selanjutnya dalam proses dekripsi menggunakan algoritma Beaufort Cipher melakukan penghitungan dengan rumus $P_i = (K_i - C_i)\ mod\ 26$.

ABSTRACT

Rois, Muhammad F. 2025. **Modification of Super Encryption Algorithm Using Beaufort Cipher and Route Cipher to Secure Population Data**. Thesis. Department of Mathematics, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Supervisors: (I) Muhammad Khudzaifah, M.Si. (II) Erna Herawati, M.Pd.

Keywords: Encryption, Decryption, Super Encryption Modification, Beaufort Cipher, Route Cipher

Data security is essential to ensure that information is not easily recognized or accessed by unauthorized parties. One effective method to achieve this goal is cryptography. This study applies a modification of the super encryption algorithm combining Beaufort Cipher and Route Cipher. The purpose of this research is to analyze the encryption and decryption processes of the modified algorithm. This research follows a qualitative approach through library research. In the encryption process, Route Cipher is used to arrange the cipher key vertically from top to bottom, then read in a clockwise spiral from the bottom-right corner to scramble the key. The resulting Cipherkey is then used in Beaufort Cipher encryption using the formula: $C_i = (K_i - P_i)\ mod\ 26$. In the decryption process, Route Cipher is used again with the same spiral reading pattern to retrieve the Cipherkey. Subsequently, decryption with Beaufort Cipher is performed using the formula: $P_i = (K_i - C_i)\ mod\ 26$.

مستخلص البحث

الرئيس، محمد فحر. ٢٠٢٥. **تعديل التشفير الفائق لخوارزميات** *Beaufort Cipher* و *Route Cipher* **لتأمين بيانات السكان**. اطروحه. برنامج دراسة الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم إبراهيم الإسلامية الحكومية مالانج. المشرف: الأول: محمد خذيفة، الماجستر. المشرفة الثاني: إيرنا هيراواتي، الماجستر.

الكلمات الأساسية: التشفير، فك التشفير، تعديل التشفير الفائق، *Beaufort Cipher*، *Route Cipher*

يعد أمان البيانات أمرا مهما لمنع التعرف على البيانات بسهولة من قبل الآخرين. الوسائل المستخدمة لتحقيق هذا الهدف هي التشفير. في هذا البحث، تم استخدام تعديل لخوارزميات التشفير الفائق *Beaufort Cipher* و *Route Cipher*. الغرض من هذا الباحث هو تحديد عملية التشفير وفك التشفير بالإضافة إلى أمان خوارزميات *Beaufort Cipher* و *Route Cipher*. تستخدم مراحل هذا البحث نهجا نوعيا مع طريقة البحث المكتبي. في عملية التشفير باستخدام خوارزمية *Route Cipher*، تم ترتيب مفتاح التشفير عموديا من أعلى إلى أسفل، ثم ستتم قراءته حلزونيا من أسفل اليمين وفي اتجاه عقارب الساعة لترتيب المفتاح التشفير عشوائيا. علاوة على ذلك ، تم استخدام مفتاح التشفير الذي تم الحصول عليه من تشفير خوارزمية *Route Cipher* في عملية التشفير باستخدام خوارزمية *Beaufort Cipher*، والصيغة المستخدمة هي. $C_i = (K_i - P_i) \bmod 26$ في عملية فك التشفير باستخدام خوارزمية *Route Cipher*، تم ترتيب مفتاح التشفير عموديا من أعلى إلى أسفل، ثم ستتم قراءته في شكل حلزوني من أسفل اليمين وفي اتجاه عقارب الساعة لترتيب مفتاح التشفير عشوائيا. علاوة على ذلك، في عملية فك التشفير باستخدام خوارزمية *Beaufort Cipher*، تم إجراء الحساب باستخدام الصيغة$P_i = (K_i - C_i) \bmod 26$.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada dasarnya manusia adalah makhluk sosial yang saling membutuhkan satu sama lain dan untuk mencapai suatu hubungan tersebut manusia melakukan komunikasi secara fisik ataupun lisan. Manusia menyampaikan sesuatu pesan baik secara langsung atau melalui perantara berupa media cetak, media elektronik, dan media sosial, namun tidak semua pesan yang disampaikan tersebut boleh dilihat maupun dibaca oleh khalayak umum, karena beberapa nformasi memiliki data yang terkesan penting.

Dalam menjaga keamanan informasi atau pesan yang akan diberikan pada seseorang maka telah ditemukan salah satu cara yaitu dengan menyandikan pesan tersebut menjadi kode atau simbol-simbol tertentu sehingga pesan yang asli tidak dapat diketahui oleh pihak lain yang tidak bertanggung jawab dan proses tersebut dikenal sebagai kriptografi. Kriptografi adalah sebuah kajian ilmiah matematis yang bertujuan untuk menjaga atau melindungi kerahasiaan nformasi.(Setyaningsih Emy, 2015a)

Dalam undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Undang-undang ini merupakan tonggak penting dalam upaya negara untuk melindungi data pribadi warganya di era digital yang semakin berkembang pesat. Dengan perkembangan teknologi informasi yang semakin canggih, perlindungan terhadap data pribadi menjadi isu yang sangat vital untuk menjaga hak privasi individu serta keamanan informasi di dunia maya.

Kriptografi memiliki mekanisme dalam menyandikan nformasi yaitu dengan dua proses yang dikenal sebagai proses enkripsi dan proses dekripsi. Proses enkripsi adalah sebuah algoritma matematis yang mengubah pesan asli (Plaintext) menjadi pesan yang tidak bisa dipahami (Ciphertext), sedangkan untuk proses dekripsi adalah sebaliknya yaitu algoritma matematis untuk mengubah pesan yang tidak bisa dipahami menjadi pesan yang asli.

Dalam perkembangannya kriptografi memiliki banyak sekali algoritma yang sangat rumit sehingga sulit untuk dipecahkan, kriptografi pada zaman dahulu merupakan kriptografi klasik yang menjadi dasar perkembangan dari kriptografi modern yang sekarang ini. Kriptografi klasik beberapa diantaranya adalah Caesar cipher, Vigenere cipher, Playfair cipher, Hill cipher, cipher transposisi dan masih banyak yang lainnya. Dalam kriptografi klasik tersebut dapat dikembangkan kembali menjadi algoritma kriptografi baru seperti algoritma Beaufort cipher yang merupakan variasi dari algoritma Vigenere cipher, beaufort cipher adalah sebuah algoritma yang melakukan pergeseran kunci dengan urutan kunci $K = k_i, \dots, k_n$ dan k_i adalah banyaknya pergeseran pada alfabet ke-i sama dengan algoritma Vigenere cipher (Setyaningsih Emy, 2015b).

Dalam ajaran agama slam juga terdapaat sebuah konsep kriptografi yang berupa Amanah. Hal tersebut dijelaskan dalam surat Al-Mu'minun ayat 8:

وَالَّذِيْنَ هُمْ لِاَمٰنٰتِهِمْ وَعَهْدِهِمْ رَاعُوْنَۙ ﴿٨﴾

"(Sungguh beruntung pula) orang-orang yang memelihara amanat dan janji mereka.".

Dalam surat Al-mu'minun ayat 8 menjelaskan bahwa orang beriman memiliki ciri-ciri utama, yaitu menjaga amanah dan menepati janji Amanah di sini tidak hanya terbatas pada amanah berupa barang atau harta, tetapi juga mencakup segala bentuk tanggung jawab yang dipercayakan kepada seseorang, baik dari Allah SWT

maupun dari sesama manusia. Ini bisa berupa tugas, pekerjaan, rahasia, atau hal lainnya yang dipercayakan.

Algoritma *Beaufort Cipher* termasuk dalam kriptografi klasik yang telah lama ditemukan sehingga akan sangat mudah untuk diserang oleh pihak-pihak yang tidak bertanggung jawab, oleh karena itu penulis ngin menambah keamanan algoritma *Beaufort cipher* dengan menggabungkan algoritma tersebut dengan algoritma lain berupa algoritma *Route Cipher*. Penggabungan dua *cipher* substitusi dan *cipher* transposisi yang dapat menghasilkan suatu kriptografi yang sulit untuk dipecahkan dan dikenal sebagai algoritma super enkripsi. Pada penelitian sebelumnya telah dibahas tentang penggunaan algoritma *Route Cipher* yang merupakan algoritma kriptografi *cipher* transposisi(Bangun, 2019). Dengan begitu peneliti ingin melakukan kajian penelitian yang berjudul "Modifikasi Algoritma super enkripsi *Beaufort Cipher* dan *Route Cipher* untuk mengamankan data penduduk".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dibuat, rumusan masalah dari penelitian ini adalah sebagai berikut:

1. Bagaimana proses enkripsi menggunakan modifikasi algoritma *Beaufort Cipher* dan algoritma *Route Cipher*?
2. Bagaimana proses dekripsi menggunakan modifikasi algoritma *Beaufort Cipher* dan algoritma *Route Cipher*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui bagaimana proses enkripsi menggunakan modifikasi algoritma *Beaufort Cipher* dan algoritma *Route Cipher* untuk pengamanan data penduduk.
2. Mengetahui bagaimana proses dekripsi menggunakan modifikasi algoritma Beaufort Cipher dan Route Cipher untuk pengamanan data penduduk.

1.4 Manfaat Penelitian

1. Bagi penulis

   Penelitian ini dapat menambah wawasan tentang kriptografi klasik dan modifikasi nya terutama pada algoritma *Beaufort cipher* dan algoritma *Route Cipher*.

2. Bagi pembaca

   Penelitian ini dapat memperkaya lmu pengetahuan dan tata cara proses enkripsi dan dekripsi tentang kriptografi klasik pada algoritma Beaufort Cipher dan algoritma Route Cipher dalam pengamanan nformasi.

3. Bagi lembaga

   Penelitian yang telah dibuat dapat menambah bahan literasi dan nformasi yang mencakup mata kuliah terutama pada kriptografi.

1.5 Batasan Masalah

Pembahasan dalam penelitian ini dibatasi dengan menggunakan beberapa batasan sebagai berikut:

1. Menggunakan 26 huruf alfabet untuk proses enkripsi dan proses dekripsi.

2. Dalam proses enkripsi dan dekripsi kunci yang dipakai untuk Beaufort cipher adalah pembukaan UUD 1945 Alinea pertama dan kunci yang dipakai untuk Route Cipher adalah 11 dengan rute spiral.
3. Algoritma yang dipakai dalam super enkripsi adalah Beaufort Cipher dan Route Cipher.

1.6 Definisi Istilah

Agar pembaca lebih mudah untuk memahami pada penelitian ini penulis menggunakan banyak istilah sehingga penulis memberikan definisi dari istilah pada bagian awal sebaigai berikut:

1. Enkripsi adalah sebuah proses dalam kriptografi untuk menyandikan pesan asli (*Plaintext*) menjadi sebuah pesan yang dikodekan (*Ciphertext*).
2. Dekripsi adalah sebuah proses dalam kriptografi untuk merubah kembali pesan yang telah dikodekan (Ciphertext) menjadi pesan yang asli (Plaintext).
3. Plaintext adalah pesan asli yang akan dikirim kepada penerima.
4. Ciphertext adalah pesan yang telah dikodekan dan siap untuk dikirimkan kepada penerima.
5. Kunci/key adalah sebuah komponen penting untuk melakukan proses enkripsi maupun dekripsi pada pesan.
6. Plainkey adalah kunci asli yang akan dikirim kepada penerima.
7. Cipherkey adalah Plainkey yang telah dikodekan dan siap untuk dikirimnkan kepada penerima.
8. Cryptosystem/Sistem kriptografi adalah keseluruhan proses dari kriptografi itu sendiri yang meliputi proses enkripsi, dekripsi, Plaintext, Ciphertext dan kunci.

9. Algoritma modifikasi dalam penelitian ini adalah merubah susunan Plainkey menggunakan algoritma transposisi terlebih dahulu kemudian menggunakan algoritma substitusi.

BAB II
KAJIAN TEORI

2.1 Teori Pendukung

2.1.1 Keterbagian

Keterbagian adalah dasar dalam lmu matematika khususnya dalam teori bilangan dan berpengaruh besar dalam materi kriptografi, berikut ini adalah penjelasan untuk materi keterbagian.

Definisi :

Misalkan ada $a, b \in \mathbb{Z}$ dengan $a \neq 0$ maka dapat disimpulkan bahwa a membagi b dan dapat dituliskan sebagai $a|b$ apabila $b = a \cdot k$ untuk suatu $k \in \mathbb{Z}$.

Definisi menjelaskan bahwa apabila ada suatu bilangan bulat a dan $a \neq 0$ maka bilangan bulat a dapat membagi bilangan bulat b jika ada bilangan bulat k sedemikian sehingga $b = a \cdot k$ dan dapat dinotasikan sebagai $a|b$ yang dibaca seperti "a membagi b" atau "b habis dibagi oleh a". Apabila bilangan bulat a tersebut tidak dapat membagi bilangan bulat b maka dinotasikan sebagai $a \nmid b$.(Irawan, Wahyu Henky, 2014)

Contoh 2.1.1:

1. $9|27$ karena ada $3 \in \mathbb{Z}$ sehingga $27 = 9 \cdot 3$
2. $2 \nmid 5$ karena tidak ada $k \in \mathbb{Z}$ sedemikian sehingga $5 = 2 \cdot k$

Teorema 1

Jika $a|b$ maka $a|bc$ untuk setiap bilangan bulat c.

Bukti:

1. $a|b$ maka $b = ak$ untuk suatu $k \in \mathbb{Z}$ (definisi)

2. $bc = (ak)c$ untuk setiap $c \in \mathbb{Z}$ (dikalikan dengan c)
3. $bc = a(kc)$ untuk setiap $kc \in z$ (asosiatif perkalian)

Terbukti bahwa $a|bc$.

Teorema 2

Jika $a|b$ dan $b|c$, maka $a|c$.

Bukti:

1. $a|b$ maka $b = ak$ untuk suatu $k \in \mathbb{Z}$ (definisi)

   $b|c$ maka $c = bl$ untuk suatu $l \in \mathbb{Z}$ (definisi)
2. $c = (ak)l$ (substitusi b pada $b|c$)
3. $c = a(kl)$, $kl \in \mathbb{Z}$ (asosiatif perkalian)

Terbukti $a|c$.

Teorema 3

Jika $a|b$ dan $b|c$ maka $a|(bx \pm cy)$, $c\ dan\ y \in \mathbb{Z}$

Bukti:

1. $a|b$ maka $b = ak_1$ untuk suatu $k_1 \in \mathbb{Z}$ (definisi)

   $b|c$ maka $c = bk_2$ untuk suatu $k_2 \in \mathbb{Z}$ (definisi)

   Maka $bx = (ak_1)x$ dan $cy = (ak_2)y$, untuk $x, y \in \mathbb{Z}$
2. $bx + cy = (ak_1)x + (ak_2)y$ (menjumlahkan $bx + cy$)
3. $bx + cy = a(k_1x + k_2y)$ (teorema 4)
4. $bx - cy = (ak_1)x - (ak_2)y$ (menjumlahkan $bx - cy$)
5. $bx - cy = a(k_1x - k_2y)$ (teorema 4)

Terbukti $a|(bx \pm cy)$.

Teorema 4

Jika $a|b\ dan\ b|a$, maka $a = \pm b,\ \ a \neq 0\ dan\ b \neq 0$

Bukti:

1. $a|b$ maka $b = ak$ untuk suatu $k \in \mathbb{Z}$ (definisi)

   $b|a$ maka $a = bl$ untuk suatu $k \in \mathbb{Z}$ (definisi)

2. $b = (bl)k = b(lk) = b(kl)$ (asosiatif perkalian)

   $a = (ak)l = a(kl)$ (asosiatif perkalian)

   Karena $b = b(kl)$ dan $a = a(kl)$ maka $kl = 1$

Oleh karena itu maka $k = 1\ dan\ l = 1\ atau\ k = -1\ dan\ l = -1$.

Jika $x = 1\ dan\ y = 1$ maka $a = b$

Jika $x = -1\ dan\ y = -1$ maka $a = -b$

Terbukti $a = \pm$b. (Irawan, Wahyu Henky, 2014)

2.1.2 Kongruensi

Kongruensi adalah salah satu materi yang membahas konsep-konsep yang telah dipelajari pada materi keterbagian dan kongruensi juga merupakan alternatif lain dalam mengkaji materi keterbagian pada bilangan bulat.

Definisi:

Misalkan ada x, y dan $m \in \mathbb{Z}$ dengan $m \neq 0$, bilangan x dapat dikatakan kongruen y modulo m jika $m|(x - y)$ dan dapat ditulis sebagai $x = y(mod\ m)$.

Jika $m > 0$ dan $m|(x - y)$ maka ada suatu bilangan bulat z sehingga $x - y = mz$. Dan sesuai dengan definisi maka dapat dinyatakan sebagai berikut:

$$x = y + mz$$

Teorema 1

Jika $a, b\ dan\ c \in \mathbb{Z}$ maka akan memenuhi sifat-sifat berikut:

1. Refleksi

$$x = x\ (mod\ m)$$

Bukti:

Jika $m \neq 0$ maka $m|0$, dan dapat dituliskan sebagai $m|x - x$. Sesuai dengan definisi di atas maka berlaku $x = x(mod\ m)$ untuk x adalah anggota bilangan bulat dan $m \neq 0$.

2. Simetris

Jika $x = y(mod\ m)$, maka $y = x(mod\ m)$ akan ekuivalen dengan $x - y = 0(mod\ m)$.

Bukti:

Sesuai definisi didapatkan $m|x - y$, maka

$x - y = mz$, z anggota bilangan bulat	(definisi kongruensi)
$-(x - y) = -(mz)$	(kalikan dengan negatif)
$-x + y = -mz$	(komutatif)
$y - x = (-z)m$	(definisi kongruensi)

Dari definisi di atas diketahui bahwa $x = y(mod\ m)$dapat ditulis $m|x - y$ yang berarti bahwa $x - y = mz$, untuk z anggota bilangan bulat.

Dan untuk $y = x(mod\ m)$ dapat ditulis $m|y - x$ yang berarti $y - x = (-z)m$, untuk $(-z)$ anggota bilangan bulat. Untuk setiap $(x - y) - 0 = zm$ juga dapat dituliskan sebagai:

$$x - y = 0(mod\ m)$$

Pernyataan di atas menunjukkan bahwa $x = y(mod\ m)$, maka $y = x(mod\ m)$ akan ekuivalen dengan $x - y = 0(mod\ m)$.

3. Transitif

Jika $x = y(mod\ m)$dan $y\ = z(mod\ m)$, maka $x = z(mod\ m)$.

Bukti:

$x = y(mod\ m)$ berarti $m|(x - y)$ (definisi kongruensi)

$y = z(mod\ m)$ berarti $m|(y - z)$ (definisi kongruensi)

Menurut definisi kongruensi maka terdapat $t_1 dan\ t_2$ sehingga didapatkan:

$m|(x - y)$ dapat dinyatakan sebagai $x - y = t_1 m$,

$m|(y - z)$ dapat dinyatakan sebagai $y - z = t_2 m$.

Kemudian kedua persamaan di atas dijumlahkan sehingga diperoleh:

$(x - y) + (y - z) = (t_1 m) + (t_2 m)$

$x - y + y - z = t_1 m + t_2 m$

$x - z = (t_1 + t_2)m$

Maka sesuai definisi didapatkan $x - z\ (mod\ m)$.(Irawan, Wahyu Henky, 2014)

2.1.3 Modulo

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat lebih dari nol. Operasi $a\ mod\ m$ memberikan sisa apabila a dibagi oleh bilangan m yang dinamai dengan modulo atau modulus. Hasil operasi modulo m terdapat pada himpunan $\{0,1,2, \dots , m - 1\}$ (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 $a = b(mod\ M)$. 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 = 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 $a = b(mod\ M)$ bisa juga dinyatakan sebagai $a - b = Mt$, ini mempunyai arti yang sama dengan $a = b(mod\ M)$ atau beda antara a dan b adalah kelipatan M. Jadi $a = b(mod\ M)$ bisa juga dinyatakan $a = Mt + b$, yaitu $a = b$ ditambah kelipatan M. menurut contoh di atas 27 = 2$(mod\ 5)$ mempunyai arti yang sama dengan 27 = 5.5 +2.

2.1.4 Kriptografi

Kriptografi pada awalnya digunakan oleh beberapa kelompok yang berhubungan dengan kegiatan seperti militer, diplomatik, penulis buku harian, pecinta, dan keagamaan. Penulisan kriptografi oleh bangsa Mesir menggunakan Hieroglyphics dan memiliki arti ‘ukiran rahasia’, Hieroglyphics telah digunakan 3000 tahun sebelum masehi dan terus berkembang menjadi Hieratic yang menggunakan aksara bergaya dan lebih mudah untuk digunakan. Kriptografi militer digunakan oleh bangsa Sparta pada tahun 400 sebelum masehi yang menggunakan sebuah alat scytale berupa media tulis dari kulit dan dibungkus menggunakan batang kayu silinder. Pada media tersebut ditulis pesan secara horizontal dan untuk mengetahui isi dari pesan tersebut adalah dengan melepaskan pita pada media tulis kemudian penerima harus melilitkan kembali

pada batang kayu silinder yang diameternya sama dengan diameter milik pengirim pesan.(Setyaningsih Emy, 2015)

Julius Caesar sebagai kaisar Roma menggunakan kriptografi untuk mengirim pesan rahasia pada Marcus Tullius Cicero, kriptografi yang digunakan oleh Julius Caesar mensubstitusikan (pergeseran) huruf alfabet ke dalam huruf lain pada alfabet yang sama dan sekarang dikenal sebagai Caesar cipher. Pada Caesar cipher pesan asli disebut dengan Plaintext dan pesan yang telah dikodekan disebut sebagai Ciphertext, secara umum Caesar cipher memiliki persamaan sebagai berikut:

$$Z_i = C_n(P_i)$$

Keterangan:

Z_i = Karakter-karakter *Ciphertext*

C_n = Transformasi substitusi alfabetis

n = Jumlah huruf yang digeser

P_i = Karakter-karakter *Plaintext*

Bangsa Arab juga mengembangkan kriptografi sendiri karena kepandaian bangsa arab terhadap bidang statistik, matematika dan linguistik. Kriptografi dikemukakan oleh seorang filsuf terkenal yaitu Yusuf Ya'Qub shaq bnu As-Sabbah bnu 'Omran bnu smail Al-Kindi yang lebih sering dikenal sebagai Al-Kindi, beliau menulis buku yang berjudul "Risalah fi stikhraj al-Mu'amma" atau "A Manuscript on Deciphering Cryptographic Messages". (Setyaningsih Emy, 2015)

2.1.5 Enkripsi dan Dekripsi

Kriptografi memiliki mekanisme yang telah ditemukan oleh bangsa Mesir kuno pada tahun 4000 tahun yang lalu dan dalam penyesuaian pada zaman sekarang maka terdapat istilah-istilah yang digunakan dalam mekanisme kriptografi tersebut, dan berikut ini adalah beberapa istilah yang sering digunakan dalam kriptografi.

1. Enkripsi adalah sebuah proses dalam kriptografi untuk menyandikan pesan asli (*Plaintext*) menjadi sebuah pesan yang dikodekan (*Ciphertext*).
2. Dekripsi adalah sebuah proses dalam kriptografi untuk merubah kembali pesan yang telah dikodekan (*Ciphertext*) menjadi pesan yang asli (*Plaintext*).
3. *Plaintext* adalah pesan asli yang akan dikirim kepada seseorang.
4. *Ciphertext* adalah pesan yang telah dikodekan dan siap untuk dikirimkan kepada seseorang.
5. Kunci/*key* adalah sebuah komponen penting untuk melakukan proses enkripsi maupun dekripsi pada pesan.
6. *Cryptosystem/*System kriptografi adalah keseluruhan proses dari kriptografi itu sendiri yang meliputi proses enkripsi, dekripsi, *Plaintext, Ciphertext* dan kunci.(Setyaningsih Emy, 2015)

2.1.6 Beaufort Cipher

Beaufort cipher merupakan salah algoritma kriptografi klasik dan juga termasuk dalam metode subtitusi yang sejenis dengan Vigenere Cipher dan memiliki mekanisme yang sama yaitu merubah karakter-karakter pada pesan asli (Plaintext) dengan cara melakukan pergeseran alfabet ke-i dengan kunci yang

telah ada dalam proses enkripsi dan dekripsinya. (Lingga, 2019) untuk Vigenere Cipher memiliki persamaan sebagai berikut:

$$C_i = (P_i - K_i)\ mod\ n$$

Keterangan:

$C_i = Ciphertext = (c_1, c_2, c_3, \dots, c_m)$

$K_i = Kunci = (k_1, k_2, k_3, \dots, k_m)$

$P_i = Plaintext = (p_1, p_2, p_3, \dots, p_m)$

Beaufort Cipher yang ditemukan oleh Laksamana Sir Francis Beaufort yang mempunyai sedikit perbedaan dengan Vigenere Cipher yaitu kunci yang digunakan akan dikurangi oleh Ciphertext dan juga Plaintext.(Rachmadsyah et al., 2020) Untuk persamaan Beaufort cipher adalah sebagai berikut:

$$C_i = (K_i - P_i)\ mod\ n \qquad (2.1)$$

Keterangan:

$C_i = Ciphertext = (c_1, c_2, c_3, \dots, c_m)$

$K_i = Kunci = (k_1, k_2, k_3, \dots, k_m)$

$P_i = Plaintext = (p_1, p_2, p_3, \dots, p_m)$

Pembuktian algoritma *Beaufort* cipher

$C_i = (K_i - P_i) mod\ 26$ (rumus enkripsi)

$26 \mid \mathrm{C_i} - (K_i - P_i)$ (definisi kongruensi)

$C_i - (K_i - P_i) = a \cdot 26,\ \ a \in \mathbb{Z}$ (definisi kongruensi)

$C_i - K_i + P_i = \ a \cdot 26,\ a \in \mathbb{Z}$ (sifat distributif)

$P_i + C_i - K_i = a \cdot 26\ , a \in \mathbb{Z}$ (sifat komutatif)

$P_i - (K_i - C_i) = a \cdot 26, a \in \mathbb{Z}$ (sifat distributif)

$26 \mid \mathrm{P_i} - (K_i - C_i)$ (definisi kongruensi)

$P_i = (K_i - C_i) mod\ 26$ (rumus dekripsi)

Algoritma *Beaufort Cipher* memiliki proses-proses sebagai berikut:

1. Menentukan *Plaintext*.
2. Menentukan kunci.
3. Menggunakan algoritma Beaufort Cipher untuk melakukan proses enkripsi
4. Dengan persamaan $C_i = (K_i - P_i)\ mod\ n$.
5. Diperoleh *Ciphertext*.
6. Menggunakan *Ciphertext* dan yang telah didapatkan dan menggunakan kunci yang sama, kemudian menggunakan algoritma Beaufort Cipher untuk melakukan proses dekripsi
7. Dengan persamaan $P_i = (K_i - C_i)\ mod\ n$.
8. Diperoleh *Plaintext*.

Proses Enkripsi

Proses enkripsi dengan algoritma Beaufort cipher menggunakan $mod\ 26$ karena sama dengan jumlah karakter alfabet, untuk $mod\ n$ dapat berubah-ubah sesuai dengan jumlah karakter yang akan digunakan. Proses enkripsi dilakukan dengan cara menentukan Plaintext dan kunci yang akan digunakan, untuk kunci akan digunakan dalam dua proses yaitu proses enkripsi dan proses dekripsi.

Contoh 2.1.2:

Tabel 2.1 Tabel Konversi

Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Numerik	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

Plaintext: MATEMATIKA

Kunci: BULAN

Hasil yang telah didapatkan akan kita rubah dari bentuk alfabet ke dalam bentuk numerik seperti di bawah ini:

Tabel 2.2 Tabel Konversi Enkripsi

PLAINTEXT	M	A	T	E	M	A	T	I	K	A
	12	0	19	4	12	0	19	8	10	0
KUNCI	B	U	L	A	N	B	U	L	A	N
	1	20	11	0	13	1	20	11	0	13

Kita menggunakan persamaan (2.1) untuk melakukan proses enkripsi pada pesan seperti di bawah ini:

$$(B - M)\ mod\ 26 = (1 - 12)\ mod\ 26 = -11\ mod\ 26 = 15\ (P)$$

$$(U - A)\ mod\ 26 = (20 - 0)\ mod\ 26 = 20\ mod\ 26 = 20\ (U)$$

$$(L - T)\ mod\ 26 = (11 - 19)\ mod\ 26 = -8\ mod\ 26 = 18\ (S)$$

$$(A - E)\ mod\ 26 = (0 - 4)\ mod\ 26 = -4\ mod\ 26 = 22\ (W)$$

$$(N - M)\ mod\ 26 = (13 - 12)\ mod\ 26 = 1\ mod\ 26 = 1\ (B)$$

$$(B - A)\ mod\ 26 = (1 - 0)\ mod\ 26 = 1\ mod\ 26 = 1\ (B)$$

$$(U - T)\ mod\ 26 = (20 - 19)\ mod\ 26 = 1\ mod\ 26 = 1\ (B)$$

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

$$(A - K)\ mod\ 26 = (0 - 10)\ mod\ 26 = -10\ mod\ 26 = 16\ (Q)$$

$$(N - A)\ mod\ 26 = (13 - 0)\ mod\ 26 = 13\ mod\ 26 = 13\ (N)$$

Telah didapatkan Ciphertext berupa “PUSWBBBDQN”.

Proses Dekripsi

Proses dekripsi pada algoritma Beaufort cipher sama dengan proses enkripsi, tetapi berbeda persamaan yang digunakan. Persamaan proses dekripsi pada algoritma Beaufort cipher sebagai berikut:

$$P_i = (K_i - C_i)\ mod\ n \qquad (2.2)$$

Keterangan

$C_i = Ciphertext = (c_1, c_2, c_3, \dots, c_m)$

$K_i = Kunci = (k_1, k_2, k_3, \dots, k_m)$

$P_i = Plaintext = (p_1, p_2, p_3, \dots, p_m)$

Tabel 2.3 Tabel Konversi Dekripsi

CIPHERTEXT	P	U	S	W	B	B	B	D	Q	N
	15	20	18	22	1	1	1	3	16	13
KUNCI	B	U	L	A	N	B	U	L	A	N
	1	20	11	0	13	1	20	11	0	13

Kemudian untuk mengembalikan pesan akan dilakukan proses dekripsi dengan persamaan (2.2), proses perhitungan nya akan dijelaskan seperti dibawah ini:

$$(B - P)\ mod\ 26 = (1 - 15)\ mod\ 26 = -14\ mod\ 26 = 12\ (M)$$

$$(U - U)\ mod\ 26 = (20 - 20)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(L - S)\ mod\ 26 = (11 - 18)\ mod\ 26 = -7\ mod\ 26 = 19\ (T)$$

$$(A - W)\ mod\ 26 = (0 - 22)\ mod\ 26 = -22\ mod\ 26 = 4\ (E)$$

$$(N - B)\ mod\ 26 = (13 - 1)\ mod\ 26 = 12\ mod\ 26 = 12\ (M)$$

$$(B - B)\ mod\ 26 = (1 - 1)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(U - B)\ mod\ 26 = (20 - 1)\ mod\ 26 = 19\ mod\ 26 = 19\ (T)$$

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

$$(A - Q)\ mod\ 26 = (0 - 16)\ mod\ 26 = -16\ mod\ 26 = 10\ (K)$$

$$(N - N)\ mod\ 26 = (13 - 13)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

Didapatkan *Plaintext* awal yang telah diberikan berupa **"MATEMATIKA".**

Namun dalam algoritma Beaufort Cipher memiliki suatu kelemahan yaitu kunci yang berulang sehingga san peretas dapat mencoba dengan metode Kasiski dan exhaustive key search. Metode ini akan dijelaskan sebagi berikut:

1. Mencari pasangan karakter yang berulang lebih dari satu kali.
2. Menghitung jarak antara karakter berulang yang pertama dan seterusnya/
3. Menghitung faktor pembaginya.
4. Menentukan risan dari semua himpunan faktor pembagi nya jika ada lebih dua karakter yang berulang.
5. Melakukan proses exhaustive key search dengan risan yang telah didapatkan sebagai panjang kunci.
6. Melakukan pengelompokan karakter sesuai urutan kunci.
7. Melakukan percobaan analisis frekuensi untuk menentukan kunci yang digunakan. (Surya, n.d.)

2.1.7 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.

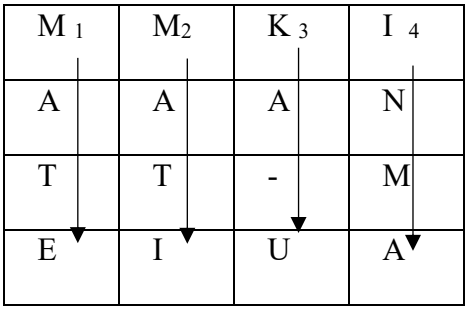
Tahapan-tahapan dalam algoritma Route Cipher yaitu:

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 ditentukan 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).

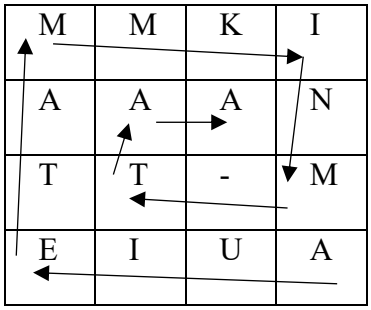
Contoh:

Diberikan plainteks “MATEMATIKA UINMA”. Plainteks akan ditulis vertikal dari kiri atas ke bawah dan untuk spasi akan diganti dengan simbol “-“..



Gambar 2.1 Contoh Plainteks Enkripsi Route Cipher.

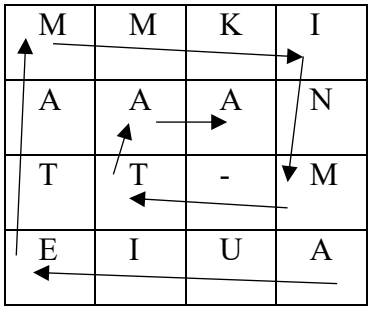
Berikutnya cipherteks yang didapat dengan menyusun teks selaras dengan arah yang telah ditentukan yaitu spiral searah jarum jam dari kanan bawah dan memperoleh hasil sebagai berikut:



Gambar 2.2 Contoh Cipherteks Enkripsi Route Cipher.

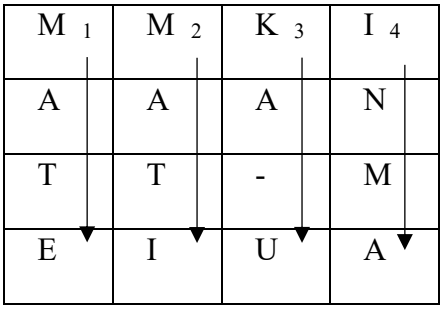
Dan cipherteks yang dihasilkan adalah AUIETAMMKINM-TAA.

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 dibawah ini



Gambar 2.4 Contoh Plainteks Dekripsi Route Cipher.

Maka plainteks yang didapatt adalah MATEMATIKA UINMA.

2.1.8 Super Enkripsi

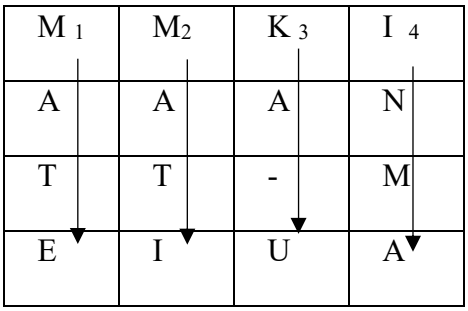
Enkripsi menggunakan satu algoritma kriptografi akan dengan mudah dipecahkan oleh orang yang tidak bertanggung jawab, oleh karena itu terdapat algoritma dalam kriptografi yang menggabungkan dua atau lebih algoritma substitusi dengan algoritma transposisi atau juga sebaliknya, hal ini bertujuan untuk menyulitkan penyerang atau orang yang tidak bertanggung jawab dalam memecahkan kode Ciphertext yang telah di enkripsi dan dikenal dengan algoritma super enkripsi. (Munir, 2019)

Misalkan kita menggunakan algoritma substitusi beuafort cipher dan algoritma Route Cipher dengan mekanisme enkripsi sebagai berikut:

1. Menentukan *plaintext*.
2. Melakukan enkripsi menggunakan algoritma *Route Cipher* menggunakan arah spiral.
3. Melakukan enkripsi kembali menggunakan algoritma *Beaufort Cipher*.

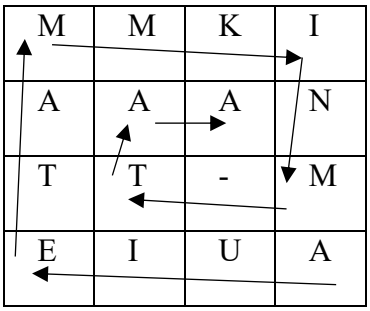
Contoh:

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 2.5 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 2.6 Contoh Cipherteks Enkripsi Route Cipher.

Dan cipherteks yang dihasilkan adalah AUIETAMMKINMTAA. kemudian dienkripsi dengan algoritma beuafort cipher dengan persamaan (2.1) serta menggunakan kunci “BULAN” akan didapatkan hasil sebagai berikut:

$$(B - A)\ mod\ 26 = (1 - 0)\ mod\ 26 = 1\ mod\ 26 = 1\ (B)$$

$$(U - U)\ mod\ 26 = (20 - 20)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(L - I)\ mod\ 26 = (11 - 9)\ mod\ 26 = 2\ mod\ 26 = 2\ (C)$$

$$(A - E)\ mod\ 26 = (0 - 4)\ mod\ 26 = -4\ mod\ 26 = 22\ (W)$$

$$(N - T)\ mod\ 26 = (13 - 19)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(B - A)\ mod\ 26 = (1 - 0)\ mod\ 26 = 1\ mod\ 26 = 1\ (B)$$

$$(U - M)\ mod\ 26 = (20 - 12)\ mod\ 26 = 8\ mod\ 26 = 8\ (I)$$

$$(L - M)\ mod\ 26 = (11 - 12)\ mod\ 26 = -1\ mod\ 26 = 25\ (Z)$$

$$(A - K)\ mod\ 26 = (0 - 10)\ mod\ 26 = -10\ mod\ 26 = 16\ (Q)$$

$$(N - I)\ mod\ 26 = (13 - 8)\ mod\ 26 = 5\ mod\ 26 = 5\ (F)$$

$$(B - N)\ mod\ 26 = (1 - 13)\ mod\ 26 = -12\ mod\ 26 = 14\ (O)$$

$$(U - M)\ mod\ 26 = (20 - 12)\ mod\ 26 = 8\ mod\ 26 = 8\ (I)$$

$$(L - T)\ mod\ 26 = (11 - 19)\ mod\ 26 = -8\ mod\ 26 = 18\ (S)$$

$$(A - A)\ mod\ 26 = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(N - A)\ mod\ 26 = (13 - 0)\ mod\ 26 = 13\ mod\ 26 = 13\ (N)$$

Diperoleh hasil Ciphertext; “BACWUBIZOFQISA”.

Tahapan-tahapan dekripsi dalam algoritma super enkripsi beaufort cipher dan route cipher yaitu:

1. Melakukan dekripsi menggunakan algoritma *Beaufort Cipher*.
2. Melakukan dekripsi kembali menggunakan algoritma *Route Cipher*.
3. Mendapatkan *Plaintext*.

Contoh:

Ciphertext yang telah didapatkan akan didekripsi dengan menggunakan algoritma Beaufort Cipher dengan persamaan (2.2) dengan Ciphertext; “BACWUBIZQFOISA”. dan prosesnya adalah sebagai berikut:

$$(B - B)\ mod\ 26 = (1 - 1)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(U - A)\ mod\ 26 = (20 - 0)\ mod\ 26 = 20\ mod\ 26 = 20\ (U)$$

$$(L - C)\ mod\ 26 = (11 - 2)\ mod\ 26 = 9\ mod\ 26 = 9\ (I)$$

$$(A - W)\ mod\ 26 = (0 - 22)\ mod\ 26 = -22\ mod\ 26 = 4\ (E)$$

$$(N - U)\ mod\ 26 = (13 - 20)\ mod\ 26 = -7\ mod\ 26 = 19\ (T)$$

$$(B - B)\ mod\ 26 = (1 - 1)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(U - I)\ mod\ 26 = (20 - 8)\ mod\ 26 = 12\ mod\ 26 = 12\ (M)$$

$$(L - Z)\ mod\ 26 = (11 - 25)\ mod\ 26 = -14\ mod\ 26 = 12\ (M)$$

$$(A - Q)\ mod\ 26 = (0 - 16)\ mod\ 26 = -16\ mod\ 26 = 10\ (K)$$

$$(N - F)\ mod\ 26 = (13 - 5)\ mod\ 26 = 8\ mod\ 26 = 8\ (I)$$

$$(B - O)\ mod\ 26 = (1 - 14)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(U - I)\ mod\ 26 = (20 - 8)\ mod\ 26 = 12\ mod\ 26 = 12\ (M)$$

$$(L - S)\ mod\ 26 = (11 - 18)\ mod\ 26 = -7\ mod\ 26 = 19\ (T)$$

$$(A - A)\ mod\ 26 = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

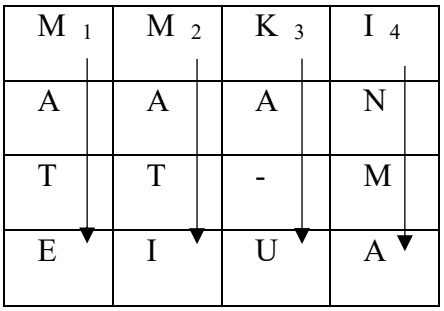
$$(N - N)\ mod\ 26 = (13 - 13)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

Diperoleh hasil Ciphertext; “AUIETAMMKINMTAA”. akan ditulis spiral searah jarum jam dari kanan bawah dan kunci yang digunakan untuk membentuk matriks adalah 4, vertikal dari kiri atas ke bawah.

M	M	K	I
A	A	A	N
T	T	-	M
E	I	U	A

Gambar 2.7 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 dibawah ini



Gambar 2.8 Contoh Plainteks Dekripsi Route Cipher.

Maka plainteks yang didapat adalah MATEMATIKA UINMA.

2.2 Amanah Dalam Perspektif slam

Dalam ajaran agama slam juga terdapat amanah. Kata “amanah” berasal dari ”hamzah”, “mim”, “nun”,Secara etimologis kata amanah berasal dari bahasa arab dalam bentuk masdar dari amanatan yang berarti jujur atau dapat dipercaya, sedangkan dalam bahasa indonesia Amanah berarti pesan, atau perintah. Menurut kamus Al-Munawwir pengertian Al-Amanah itu adalah segala yang diperintahkan Allah SWT kepada hamba-Nya (Munawir, 1997:41). mengarah pada dua pokok makna kata yang berdekatan yaitu Al-amanah lawan dari kata al-khiyanah yaitu 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, terkait hak-hak Allah SWT 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 surat Al-Ahzab ayat 72:

اِنَّا عَرَضْنَا الْاَمَانَةَ عَلَى السَّمٰوٰتِ وَالْاَرْضِ وَالْجِبَالِ فَاَبَيْنَ اَنْ يَّحْمِلْنَهَا وَاَشْفَقْنَ مِنْهَا وَحَمَلَهَا الْاِنْسَانُۗ اِنَّه كَانَ ظَلُوْمًا جَهُوْلًاۙ ﴿٧٢﴾

"Sesungguhnya Kami telah menawarkan amanat kepada langit, bumi, dan gunung-gunung; tetapi semuanya enggan untuk memikul amanat itu dan mereka khawatir tidak akan melaksanakannya. Lalu, di pikullah amanat itu oleh manusia. Sesungguhnya a (manusia) sangat zalim lagi sangat bodoh."

Dalam kitab Tafsir bnu Katsir jilid 2 (2001) Allah SWT mengabarkan bahwa Allah SWT 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 SWT 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 SWT untuk ditunaikan. Barang siapa yang tidak melakukanya di dunia ini, maka akan dimintai pertanggungjawabanya di hari Kiamat. (Al-Sheikh, 2001).

2.3 Kajian Topik dengan Teori Pendukung

Penelitian ini membahas kriptografi yang menggunakan algoritma super enkripsi, super enkripsi adalah algoritma yang menggabungkan antara algoritma substitusi dan algoritma transposisi agar tingkat keamanan pesan asli yang telah di

enkripsi tidak mudah untuk diketahui oleh pihak yang seharusnya tidak berhak menerima pesan tersebut. Algoritma substitusi yang digunakan pada penelitian ini adalah algoritma *Beaufort cipher* dengan persamaan (2.1) dan pada algoritma ini menerapkan materi pada teori bilangan yaitu keterbagian dan kekongruenan.

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. Adapun hasil *output* dari program ini yaitu berupa plainteks.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian ini adalah penelitian kualitatif dengan menggunakan metode studi pustaka. dengan cara mengumpulkan informasi dari berbagai sumber literatur yang telah ada, seperti buku, jurnal, paper, tugas akhir, dan dan karya lmiah terkait dengan algoritma *Beaufort Cipher* dan algoritma *Route Cipher*.

3.2 Pra Penelitian

Pra penelitian merupakan tahapan yang dilakukan sebelum melakukan penelitian. Penelitian ini pada awalnya merujuk pada skripsi milik Muhammad Zulfikri Rangga yang berjudul "Modifikasi Algoritma Beaufort Cipher dengan Transposisi Grup Simetri untuk Mengamankan Data Penduduk". Pada skripsi tersebut hanya menggunakan Beaufort Cipher yang digunakan dalam algoritma subtitusi, dan pada skripsi tersebut memiliki saran untuk menggunakan algoritma-algoritma lain yang dapat digunakan dengan Beaufort Cipher, penulis berfikir menggunakan algoritma super enkripsi yang menggabungkan algoritma substitusi dan algoritma transposisi untuk mengamankan suatu pesan, penulis memilih algoritma Beaufort cipher dan Route Cipher untuk diangkat sebagai penelitian selanjutnya.

3.3 Tahapan Penelitian

Penelitian ini terdiri dari dua tahapan yaitu tahap enkripsi, dan tahap dekripsi. Pada tahap enkripsi akan dilakukan dengan modifikasi algoritma *Beaufort*

Cipher dengan *Route Cipher* dilakukan dengan mengenkripsi Plainkey yang telah ditentukan menggunakan algoritma *Route Cipher* terlebih dahulu, hasil dari enkripsi tersebut berupa *Cipherkey*, kemudian *Cipherkey* tersebut akan digunakan sebagai kunci kriptografi *Beaufort Cipher*, sedangkan pada tahap dekripsi akan dilakukan dengan modifikasi algoritma *Beaufort Cipher* dengan algoritma Route Cipher dilakukan dengan mendekripsi *cipherkey* menggunakan *Route Cipher* terlebih dahulu, kemudian hasil dari dekripsi berupa *Cipherkey* tersebut akan digunakan sebagai kunci kriptografi *Beaufort Cipher* sehingga diperoleh *Plaintext*.

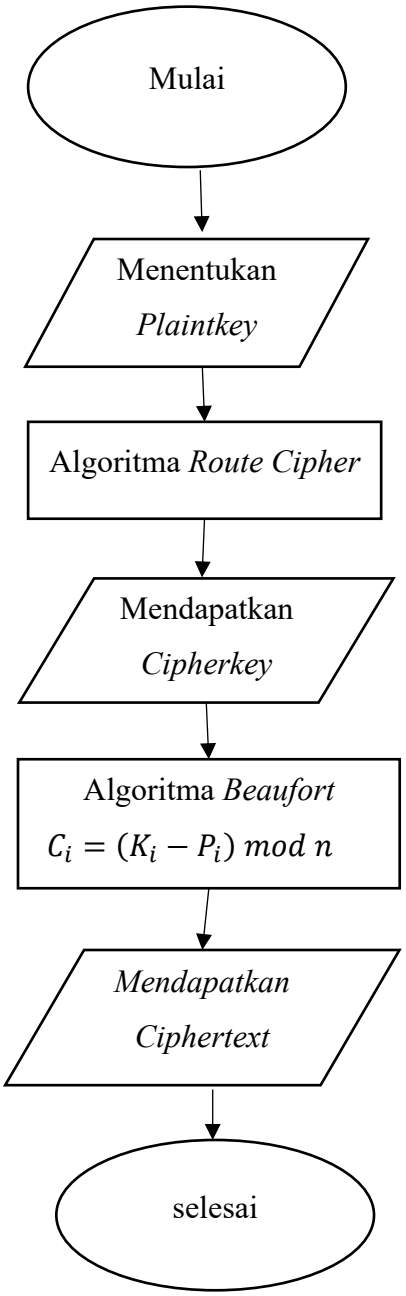
1. Algoritma proses enkripsi
   a. Menentukan *Plainkey* yang akan digunakan sebagai kunci dengan panjang n.
   b. Membuat Tabel $n \times n$ dan menuliskan Plainkey vertikal dari kiri atas ke bawah. Tabel dibuat sebanyak $n \times n$ tergantung oleh panjang kunci, panjang kunci yang akan digunakan adalah 118 maka tabel bisa dibuat 11×11.
   c. Mengenkripsi *Plainkey* dengan membaca teks selaras dengan arah yang telah ditentukan yaitu spiral searah jarum jam dari kanan bawah sehingga didapatkan *Cipherkey*.
   d. Mengenkripsi Plaintext dengan Cipherkey menggunakan formula $C_i = (P_i - K_i)\ mod\ 26$ sehingga didapatkan *Ciphertext* dengan keterangan

      $C_i =$ Karakter $Ciphertext\ ke - i$

      $K_i =$ Karakter $Cipherkey\ ke - i$

      $P_i =$ Karakter $Plaintext\ ke - i$

Berikut ini adalah *flowchart* proses enkripsi modifikasi algoritma *Beaufort Cipher* dengan *Route Cipher* sebagai berikut:



Gambar 3.1 Flowchart Enkripsi

2. Algoritma proses dekripsi

   a. Membuat Tabel $n \times n$ dan menuliskan Plainkey vertikal dari kiri atas ke bawah. Tabel dibuat sebanyak $n \times n$ tergantung oleh panjang kunci, panjang kunci yang akan digunakan adalah 118 maka tabel bisa dibuat 11×11.

   b. Dekripsi *Plainkey* dengan membaca teks selaras dengan arah yang telah ditentukan yaitu spiral searah jarum jam dari kanan bawah sehingga didapatkan *Cipherkey*.

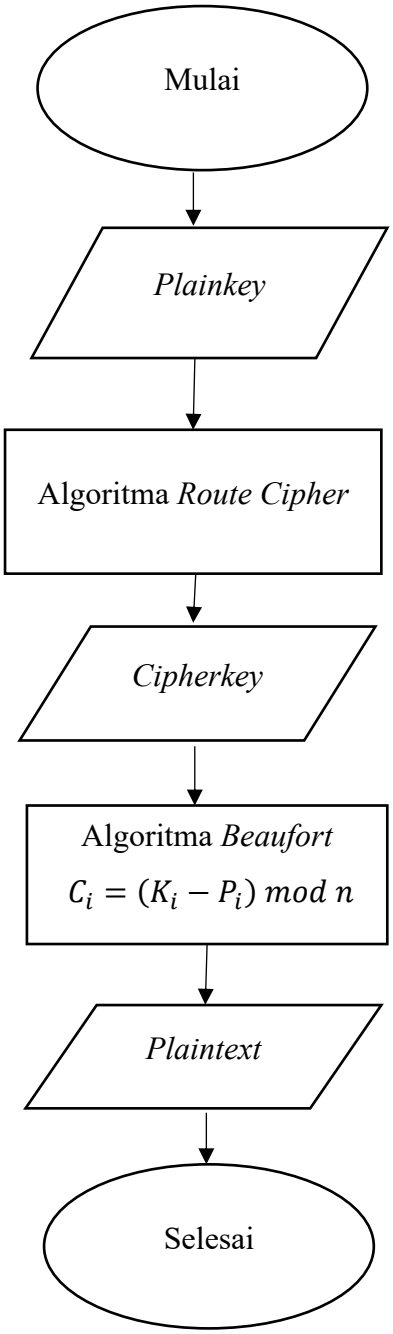
   c. Dekripsi *Ciphertext* dengan formula $P_i = (K_i - C_i)\ mod\ 26$ sehingga didapatkan *Plainktext* dengan keterangan

      $C_i =$ Karakter $Ciphertext\ ke - i$

      $K_i =$ Karakter $Kunci\ ke - i$

      $P_i =$ Karakter $Plaintext\ ke - i$.

Berikut ini adalah *flowchart* proses dekripsi modifikasi algoritma *Beaufort Cipher* dengan *Route Cipher* sebagai berikut:



Gambar 3.2 Flowchart Dekripsi.

Langkah-langkah di atas adalah prosedur dalam modifikasi algoritma super enkripsi *Beaufort cipher* dan algoritma *Route Cipher*.

BAB IV

PEMBAHASAN

Bab ini menyajikan pembahasan dari Modifikasi super enkripsi Algoritma *Beaufort Cipher* dan *Route Cipher* untuk mengamankan data penduduk. Tujuan dari penelitian ini adalah untuk memodifikasi penggunaan algoritma transposisi berupa algoritma *Route Cipher* yang akan digunakan dalam mengacak kunci pada algoritma *Beaufort Cipher*.

Proses modifikasi dimulai dengan mengubah Plainkey menggunakan algoritma Route Cipher sehinngga didapatkan Cipherkey, selanjutnya Cipherteks dienkripsi menggunakan algoritma Beaufort Cipher dan akan mendapatkan Ciphertext. Selanjutnya dilakukan proses dekripsi dengan mengubah Plainkey menggunakan algoritma Route Cipher sehinngga didapatkan Cipherkey, selanjutnya Cipherteks didekripsi menggunakan algoritma Beaufort Cipher dan akan mendapatkan Plaintext.

4.1 Algoritma Modifikasi Beaufort Cipher dengan Route Cipher

Untuk meningkatkan keamanan data, dilakukan penerapan Algoritma *route Cipher* bertujuan untuk mengacak kunci pada Algoritma *beaufort Cipher*. Sehingga menghasilkan susunan kunci acak dan tidak mudah dianalisis secara langsung.

1. Algoritma proses enkripsi
   a. Menentukan *Plainkey* yang akan digunakan sebagai kunci dengan panjang n.
   b. Membuat Tabel n x n dan menuliskan Plainkey vertikal dari kiri atas ke bawah. Tabel dibuat sebanyak n × n tergantung oleh panjang kunci,

panjang kunci yang akan digunakan adalah 118 maka tabel bisa dibuat 11 x 11.

c. Mengenkripsi *Plainkey* dengan membaca teks selaras dengan arah yang telah ditentukan yaitu spiral searah jarum jam dari kanan bawah sehingga didapatkan *Cipherkey*.

d. Mengenkripsi Plaintext dengan Cipherkey menggunakan formula $C_i = (P_i - K_i)\ mod\ 26$ sehingga didapatkan *Ciphertext* dengan keterangan

$C_i =$ Karakter $Ciphertext\ ke - i$

$K_i =$ Karakter $Cipherkey\ ke - i$

$P_i =$ Karakter $Plaintext\ ke - i$.

2. Algoritma proses dekripsi

a. Membuat Tabel $n \times n$ dan menuliskan Plainkey vertikal dari kiri atas ke bawah. Tabel dibuat sebanyak $n \times n$ tergantung oleh panjang kunci, panjang kunci yang akan digunakan adalah 118 maka tabel bisa dibuat 11×11.

b. Dekripsi Plainkey dengan membaca teks selaras dengan arah yang telah ditentukan yaitu spiral searah jarum jam dari kanan bawah sehingga didapatkan Cipherkey.

c. Dekripsi Ciphertext dengan formula $P_i = (K_i - C_i)\ mod\ 26$ sehingga didapatkan Plainktext dengan keterangan

$C_i =$ Karakter $Ciphertext\ ke - i$

$K_i =$ Karakter $Kunci\ ke - i$

$P_i =$ Karakter $Plaintext\ ke - i$.

4.2 Simulasi proses Enkripsi dan Dekripsi Modifikasi Beaufort Cipher dengan Route Cipher

4.2.1 Simulasi Enkripsi Beaufort Cipher dengan Route Cipher

Pada saat melakukan proses enkripsi, penulis menentukan plainteks yang akan disandikan menggunakan algoritma Beaufort Cipher dan Route Cipher. Pada kali ini plainteks yang dipakai adalah

Tabel 4.1 Tabel Data Kartu Keluarga

NAMA	TEMPAT LAHIR	NAMA ORANG TUA
KHOIRUL HADI	TUBAN	SUYONO
ADELIA PUTRI	GRESIK	SUTRISNO
ALAMUL HUDA	MALANG	AHMAD KHOIRUL
AHMAD PUJI	NGANJUK	KASNOTO
WAHYU	MALANG	KHOIRUDIN

Kunci yang akan digunakan adalah: “BAHWA KEMERDEKAAN ADALAH HAK SEGALA BANGSA DAN PENJAJAHAN HARUS DIHAPUSKAN KARENA TIDAK SESUAI DENGAN PERIKEMANUSIAAN DAN PERIKEADILAN”. Kunci tersebut akan digunakan untuk satu kartu keluarga.

Plainkey dienkripsi dengan menggunakan algoritma Route Cipher. Plainkey akan ditulis secara verikal dari kiri atas ke bawah. Kunci yang digunakan untuk membentuk matriks adalah 11.

B	E	H	N	A	D	A	E	P	I	K
A	K	A	G	J	I	R	S	E	A	E
H	A	K	S	A	H	E	U	R	A	A

W	A	S	A	H	A	N	A	I	N	D
A	N	E	D	A	P	A	I	K	D	I
K	A	G	A	N	U	T	D	E	A	L
E	D	A	N	H	S	I	E	M	N	A
M	A	L	P	A	K	D	N	A	P	N
E	L	A	E	R	A	A	G	N	E	#
R	A	B	N	U	N	K	A	U	R	#
D	H	A	J	S	K	S	N	S	I	#

Gambar 4. 1 Plainkey Enkripsi Route Cipher

Plaintext yang telah disusun secara vertikal dari atas ke bawah kemudian dibaca secara spiral searah jarum jam dari kiri bawah dan untuk kekurangan karakter dalam blok akan digunakan tambahan karakter # sebagai berikut:

B	E	H	N	A	D	A	E	P	I	K
A	K	A	G	J	I	R	S	E	A	E
H	A	K	S	A	H	E	U	R	A	A
W	A	S	A	J	A	N	A	I	N	D
A	N	E	D	A	P	A	I	K	D	I
K	A	G	A	N	U	T	D	E	A	L
E	D	A	N	H	S	I	E	M	N	A
M	A	L	P	A	K	D	N	A	P	N
E	L	A	E	R	A	A	G	N	E	#
R	A	B	N	U	N	K	A	U	R	#
D	H	A	J	S	K	S	N	S	I	#

Gambar 4. 2 Cipherkey Enkripsi Route Cipher

Berdasarkan proses enkripsi *Plainkey* dengan menggunakan algoritma Route Cipher dengan plainteks “bahwa Kemerdekaan adalah hak segala bangsa dan penjajahan harus dihapuskan karena tidak sesuai dengan perikemanusiaan dan perikeadilan”. Plainteks dienkripsi dengan menggunakan algoritma Route Cipher dan dengan menghapus karakter # yang yang hanya digunnakan sebagai tambahan untuk kekurangan karakter dalam blok.maka plainkey yang didapatkan adalah

“ISNSKSJAHDREMEKAWHABEHNADAEPIKEADILANRUAKNUNBALADANAAKAGJIRSEAANDANPENGAAREALAGESKSAHEURIKEMANDKAPNADAJANAIDEISHNAPATU”.

Selanjutnya Kita menggunakan persamaan (2.1) untuk melakukan proses enkripsi pada pesan seperti di bawah ini:

Tabel 4.2 Tabel Konversi

Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Numerik	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

$$(I - K)\ mod\ 26 = (8 - 10)\ mod\ 26 = -2\ mod\ 26 = 24\ (Y)$$

$$(S - H)\ mod\ 26 = (18 - 7)\ mod\ 26 = 11\ mod\ 26 = 11\ (L)$$

$$(N - O)\ mod\ 26 =\ mod\ 26 = -1\ \ mod\ 26 = 25\ (Z)$$

$$(S - I)\ mod\ 26 = (18 - 8)\ mod\ 26 = 10\ mod\ 26 = 10\ (K)$$

$$(K - R)\ mod\ 26 = (10 - 17)\ mod\ 26 = -7\ mod\ 26 = 19\ (T)$$

$$(S - U)\ mod\ 26 = (18 - 20)\ mod\ 26 = -2\ mod\ 26 = 24\ (Y)$$

$$(J - L)\ mod\ 26 = (9 - 11)\ mod\ 26 = -2\ mod\ 26 = 24\ (Y)$$

$$(A - H)\ mod\ 26 = (0 - 7)\ mod\ 26 = -7\ mod\ 26 = 19\ (T)$$

$$(H - A)\ mod\ 26 = (7 - 0)\ mod\ 26 = 7\ mod\ 26 = 7\ (H)$$

$$(D - D)\ mod\ 26 = (3 - 3)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(R - I)\ mod\ 26 = (17 - 9)\ mod\ 26 = 8\ mod\ 26 = 8\ (I)$$

$$(E - T)\ mod\ 26 = (4 - 19)\ mod\ 26 = -15\ mod\ 26 = 11\ (L)$$

$$(M - U)\ mod\ 26 = (12 - 20)\ mod\ 26 = -8\ mod\ 26 = 18\ (S)$$

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

$$(K - A)\ mod\ 26 = (10 - 0)\ mod\ 26 = 10\ mod\ 26 = 10\ (K)$$

$$(A - N)\ mod\ 26 = (0 - 13)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(W - S)\ mod\ 26 = (22 - 18)\ mod\ 26 = 4\ mod\ 26 = 4\ (E)$$

$$(H - U)\ mod\ 26 = (7 - 20)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(A - Y)\ mod\ 26 = (0 - 24)\ mod\ 26 = -24\ mod\ 26 = 2\ (C)$$

$$(B - O)\ mod\ 26 = (1 - 14)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(E - N)\ mod\ 26 = (4 - 13)\ mod\ 26 = -9\ mod\ 26 = 17\ (R)$$

$$(H - O)\ mod\ 26 = (7 - 14)\ mod\ 26 = -7\ mod\ 26 = 19\ (T)$$

$$(N - A)\ mod\ 26 = (13 - 0)\ mod\ 26 = 13\ mod\ 26 = 13\ (N)$$

$$(A - D)\ mod\ 26 = (0 - 3)\ mod\ 26 = -3\ mod\ 26 = 23\ (X)$$

$$(D - E)\ mod\ 26 = (3 - 4)\ mod\ 26 = -1\ mod\ 26 = 25\ (Z)$$

$$(A - L)\ mod\ 26 = (0 - 11)\ mod\ 26 = -11\ mod\ 26 = 15\ (P)$$

$$(E - I)\ mod\ 26 = (4 - 8)\ mod\ 26 = -4\ mod\ 26 = 22\ (W)$$

$$(P - A)\ mod\ 26 = (15 - 0)\ mod\ 26 = 15\ mod\ 26 = 15\ (P)$$

$$(I - P)\ mod\ 26 = (8 - 15)\ mod\ 26 = -7\ mod\ 26 = 19\ (T)$$

$$(K - U)\ mod\ 26 = (10 - 20)\ mod\ 26 = -10\ mod\ 26 = 16\ (Q)$$

$$(E - T)\ mod\ 26 = (4 - 19)\ mod\ 26 = -15\ mod\ 26 = 11\ (L)$$

$$(A - R)\ mod\ 26 = (0 - 17)\ mod\ 26 = -17\ mod\ 26 = 9\ (J)$$

$$(D - I)\ mod\ 26 = (3 - 8)\ mod\ 26 = -5\ mod\ 26 = 21\ (V)$$

$$(I - G)\ mod\ 26 = (8 - 6)\ mod\ 26 = 2\ mod\ 26 = 2\ (C)$$

$$(L - R)\ mod\ 26 = (11 - 17)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(A - E)\ mod\ 26 = (0 - 4)\ mod\ 26 = -4\ mod\ 26 = 22\ (W)$$

$$(N - S)\ mod\ 26 = (13 - 18)\ mod\ 26 = -5\ mod\ 26 = 21\ (V)$$

$$(R - I)\ mod\ 26 = (17 - 8)\ mod\ 26 = 9\ mod\ 26 = 9\ (J)$$

$$(U - K)\ mod\ 26 = (20 - 10)\ mod\ 26 = 10\ mod\ 26 = 10\ (K)$$

$$(A - S)\ mod\ 26 = (0 - 18)\ mod\ 26 = -18\ mod\ 26 = 8\ (I)$$

$$(K - U)\ mod\ 26 = (10 - 20)\ mod\ 26 = -10\ mod\ 26 = 16\ (Q)$$

$$(N - T)\ mod\ 26 = (13 - 19)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

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

$$(N - I)\ mod\ 26 = (13 - 8)\ mod\ 26 = 5\ mod\ 26 = 5\ (F)$$

$$(B - S)\ mod\ 26 = (1 - 18)\ mod\ 26 = -17\ mod\ 26 = 9\ (J)$$

$$(A - N)\ mod\ 26 = (0 - 13)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(L - O)\ mod\ 26 = (11 - 14)\ mod\ 26 = -3\ mod\ 26 = 23\ (X)$$

$$(A - A)\ mod\ 26 = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(D - L)\ mod\ 26 = (3 - 11)\ mod\ 26 = -8\ mod\ 26 = 18\ (S)$$

$$(A - A)\ mod\ 26 = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(N - M)\ mod\ 26 = (13 - 12)\ mod\ 26 = 1\ mod\ 26 = 1\ (B)$$

$$(A - U)\ mod\ 26 = (0 - 20)\ mod\ 26 = -20\ mod\ 26 = 6\ (G)$$

$$(A - L)\ mod\ 26 = (0 - 11)\ mod\ 26 = -11\ mod\ 26 = 15\ (P)$$

$$(K - H)\ mod\ 26 = (10 - 7)\ mod\ 26 = 3\ mod\ 26 = 3\ (D)$$

$$(A - U)\ mod\ 26 = (0 - 20)\ mod\ 26 = -20\ mod\ 26 = 6\ (G)$$

$$(G - D)\ mod\ 26 = (6 - 3)\ mod\ 26 = 3\ mod\ 26 = 3\ (D)$$

$$(J - A)\ mod\ 26 = (9 - 0)\ mod\ 26 = 9\ mod\ 26 = 9\ (J)$$

$$(I - M)\ mod\ 26 = (8 - 12)\ mod\ 26 = -4\ mod\ 26 = 22\ (W)$$

$$(R - A)\ mod\ 26 = (17 - 0)\ mod\ 26 = 17\ mod\ 26 = 17\ (R)$$

$$(S - L)\ mod\ 26 = (18 - 11)\ mod\ 26 = 7\ mod\ 26 = 7\ (H)$$

$$(E - A)\ mod\ 26 = (4 - 0)\ mod\ 26 = 4\ mod\ 26 = 4\ (E)$$

$$(A - N)\ mod\ 26 = (0 - 13)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(A - G)\ mod\ 26 = (0 - 6)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(N - A)\ mod\ 26 = (13 - 0)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(D - H)\ mod\ 26 = (3 - 7)\ mod\ 26 = -4\ mod\ 26 = 22\ (W)$$

$$(A - M)\ mod\ 26 = (0 - 12)\ mod\ 26 = -12\ mod\ 26 = 14\ (O)$$

$$(N - A)\ mod\ 26 = (13 - 0)\ mod\ 26 = 13\ mod\ 26 = 13\ (N)$$

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

$$(E - K)\ mod\ 26 = (4 - 10)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(N - H)\ mod\ 26 = (13 - 7)\ mod\ 26 = 6\ mod\ 26 = 6\ (G)$$

$$(G - O)\ mod\ 26 = (6 - 14)\ mod\ 26 = -8\ mod\ 26 = 18\ (S)$$

$$(A - I)\ mod\ 26 = (0 - 8)\ mod\ 26 = -8\ mod\ 26 = 18\ (S)$$

$$(A - R)\ mod\ 26 = (0 - 17)\ mod\ 26 = -17\ mod\ 26 = 9\ (J)$$

$$(R - U)\ mod\ 26 = (17 - 20)\ mod\ 26 = -3\ mod\ 26 = 23\ (X)$$

$$(E - L)\ mod\ 26 = (4 - 11)\ mod\ 26 = -7\ mod\ 26 = 19\ (T)$$

$$(A - A)\ mod\ 26 = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(L - H)\ mod\ 26 = (11 - 7)\ mod\ 26 = 4\ mod\ 26 = 4\ (E)$$

$$(A - M)\ mod\ 26 = (0 - 12)\ mod\ 26 = -12\ mod\ 26 = 14\ (O)$$

$$(G - A)\ mod\ 26 = (6 - 0)\ mod\ 26 = 6\ mod\ 26 = 6\ (G)$$

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

$$(S - P)\ mod\ 26 = (18 - 15)\ mod\ 26 = 3\ mod\ 26 = 3\ (D)$$

$$(K - U)\ mod\ 26 = (10 - 20)\ mod\ 26 = -10\ mod\ 26 = 16\ (Q)$$

$$(S - J)\ mod\ 26 = (18 - 9)\ mod\ 26 = 9\ mod\ 26 = 9\ (J)$$

$$(A - I)\ mod\ 26 = (0 - 8)\ mod\ 26 = -8\ mod\ 26 = 18\ (S)$$

$$(H - N)\ mod\ 26 = (7 - 13)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(E - G)\ mod\ 26 = (4 - 6)\ mod\ 26 = -2\ mod\ 26 = 24\ (Y)$$

$$(U - A)\ mod\ 26 = (20 - 0)\ mod\ 26 = 20\ mod\ 26 = 20\ (U)$$

$$(R - N)\ mod\ 26 = (17 - 13)\ mod\ 26 = 4\ mod\ 26 = 4\ (E)$$

$$(I - J)\ mod\ 26 = (8 - 9)\ mod\ 26 = -1\ mod\ 26 = 25\ (Z)$$

$$(K - U)\ mod\ 26 = (10 - 20)\ mod\ 26 = -10\ mod\ 26 = 16\ (Q)$$

$$(E - K)\ mod\ 26 = (4 - 10)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(M - K)\ mod\ 26 = (12 - 10)\ mod\ 26 = 2\ mod\ 26 = 2\ (B)$$

$$(A - A)\ mod\ 26 = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(N - S)\ mod\ 26 = (13 - 18)\ mod\ 26 = -5\ mod\ 26 = 21\ (V)$$

$$(D - N)\ mod\ 26 = (3 - 13)\ mod\ 26 = -10\ mod\ 26 = 16\ (Q)$$

$$(K - O)\ mod\ 26 = (10 - 14)\ mod\ 26 = -4\ mod\ 26 = 22\ (W)$$

$$(A - T)\ mod\ 26 = (0 - 19)\ mod\ 26 = -19\ mod\ 26 = 7\ (H)$$

$$(P - O)\ mod\ 26 = (15 - 14)\ mod\ 26 = 1\ mod\ 26 = 1\ (B)$$

$$(N - W)\ mod\ 26 = (13 - 22)\ mod\ 26 = -9\ mod\ 26 = 17\ (R)$$

$$(A - A)\ mod\ 26 = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(D - H)\ mod\ 26 = (3 - 7)\ mod\ 26 = -4\ mod\ 26 = 22\ (W)$$

$$(A - Y)\ mod\ 26 = (0 - 24)\ mod\ 26 = -24\ mod\ 26 = 2\ (B)$$

$$(J - U)\ mod\ 26 = (9 - 20)\ mod\ 26 = -11\ mod\ 26 = 15\ (P)$$

$$(A - M)\ mod\ 26 = (0 - 12)\ mod\ 26 = -12\ mod\ 26 = 14\ (O)$$

$$(N - A)\ mod\ 26 = (13 - 0)\ mod\ 26 = 13\ mod\ 26 = 13\ (N)$$

$$(A - L)\ mod\ 26 = (0 - 11)\ mod\ 26 = -11\ mod\ 26 = 15\ (P)$$

$$(I - A)\ mod\ 26 = (8 - 0)\ mod\ 26 = 8\ mod\ 26 = 8\ (I)$$

$$(D - N)\ mod\ 26 = (3 - 13)\ mod\ 26 = -10\ mod\ 26 = 16\ (Q)$$

$$(E - G)\ mod\ 26 = (4 - 6)\ mod\ 26 = -2\ mod\ 26 = 24\ (Y)$$

$$(I - K)\ mod\ 26 = (8 - 10)\ mod\ 26 = -2\ mod\ 26 = 24\ (Y)$$

$$(S - H)\ mod\ 26 = (18 - 7)\ mod\ 26 = 11\ mod\ 26 = 11\ (L)$$

$$(H - O)\ mod\ 26 = (7 - 14)\ mod\ 26 = -7\ mod\ 26 = 19\ (T)$$

$$(N - I)\ mod\ 26\ = (13 - 8)\ mod\ 26 = 5\ mod\ 26 = 5\ (F)$$

$$(A - R)\ mod\ 26\ = (0 - 17)\ mod\ 26 = -17\ mod\ 26 = 9\ (J)$$

$$(P - U)\ mod\ 26\ = (15 - 20)\ mod\ 26 = -5\ mod\ 26 = 21\ (V)$$

$$(A - D)\ mod\ 26\ = (0 - 3)\ mod\ 26 = -3\ mod\ 26 = 23\ (X)$$

$$(T - I)\ mod\ 26\ = (19 - 8)\ mod\ 26 = 11\ mod\ 26 = 11\ (L)$$

$$(U - N)\ mod\ 26\ = (20 - 13)\ mod\ 26 = 7\ mod\ 26 = 7\ (H)$$

Proses enkripsi yang telah dilakukan menghasilkan Ciphertext berupa "YLZKTYYTHAILSDKNENCRNTNXZPWPTQLJVCUWVJKIQUDFJNXA SABGPDGDJWRHENUNWONMUGSSJXTAEOGBDQJSUYUEZQUBAV QWHBRAWBPONPIQYYLTFJVXLH".

4.2.2 Simulasi Dekripsi Beaufort Cipher dengan Route Cipher

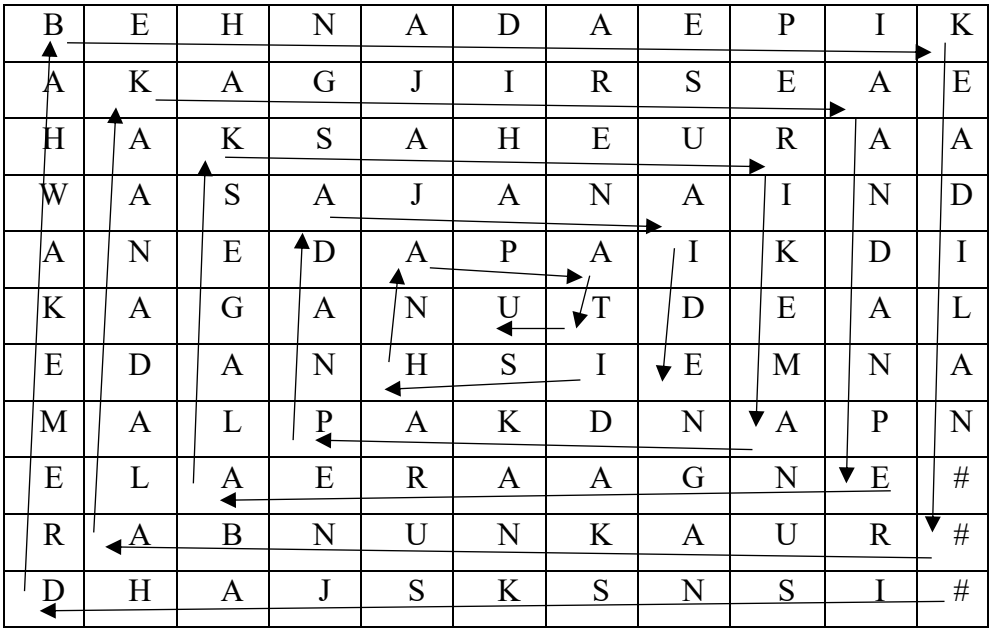
Penerima data akan melakukan transposisi terhadap kunci yang akan digunakan, kunci yang akan digunakan adalah: "BAHWA KEMERDEKAAN ADALAH HAK SEGALA BANGSA DAN PENJAJAHAN HARUS

DIHAPUSKAN KARENA TIDAK SESUAI DENGAN PERIKEMANUSIAAN DAN PERIKEADILAN". Cipherkey didekripsi dengan menggunakan Route Cipher. Plainteks akan ditulis secara verikal dari kiri atas ke bawah. Kunci yang digunakan untuk membentuk matriks adalah 11.

B	E	H	N	A	D	A	E	P	I	K
A	K	A	G	J	I	R	S	E	A	E
H	A	K	S	A	H	E	U	R	A	A
W	A	S	A	H	A	N	A	I	N	D
A	N	E	D	A	P	A	I	K	D	I
K	A	G	A	N	U	T	D	E	A	L
E	D	A	N	H	S	I	E	M	N	A
M	A	L	P	A	K	D	N	A	P	N
E	L	A	E	R	A	A	G	N	E	#
R	A	B	N	U	N	K	A	U	R	#
D	H	A	J	S	K	S	N	S	I	#

Gambar 4. 3 Plainkey Dekripsi Route Cipher

Plainkey dibaca secara spiral searah jarum jam dari kiri bawah:



Gambar 4. 4 Cipherkey Dekripsi Route Cipher

Berdasarkan proses dekripsi Cipherkey dengan menggunakan algoritma Route Cipher dengan plainkey “BAHWA KEMERDEKAAN ADALAH HAK SEGALA BANGSA DAN PENJAJAHAN HARUS DIHAPUSKAN KARENA TIDAK SESUAI DENGAN PERIKEMANUSIAAN DAN PERIKEADILAN”. Plainkey didekripsi dengan menggunakan algoritma Route Cipher dan diperoleh cipherkey

“ISNSKSJAHDREMEKAWHABEHNADAEPIKEADILANRUAKNUNBAL ADANAAKAGJIRSEAANDANPENGAAREALAGESKSAHEURIKEMAN DKAPNADAJANAIDEISHNAPATU”.

dengan menghapus karakter # yang yang hanya digunnakan sebagai tambahan untuk kekurangan karakter dalam blok.

Dalam proses dekripsi, Ciphertext yang digunakan adalah

“YLZKTYYTHAILSDKNENCRNTNXZPWPTQLJVCUWVJKIQUDFJ NXASABGPDGDJWRHENUNWONMUGSSJXTAEOGBDQJSUYUEZQU BAVQWHBRAWBPONPIQYYLTFJVXLH”.

Selanjutnya Kita menggunakan persamaan (2.2) untuk melakukan proses dekripsi pada pesan seperti di bawah ini:

$$(I - Y)\ mod\ 26\ = (8 - 24)\ mod\ 26 = -16\ mod\ 26 = 10\ (K)$$

$$(S - L)\ mod\ 26\ = (18 - 11)\ mod\ 26 = 7\ mod\ 26 = 7\ (H)$$

$$(N - Z)\ mod\ 26\ = (13 - 25)\ mod\ 26 = -12\ \ mod\ 26 = 14\ (O)$$

$$(S - K)\ mod\ 26\ = (18 - 10)\ mod\ 26 = 8\ mod\ 26 = 8\ (I)$$

$$(K - T)\ mod\ 26\ = (10 - 19)\ mod\ 26 = -9\ mod\ 26 = 17\ (R)$$

$$(S - Y)\ mod\ 26\ = (18 - 24)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(J - Y)\ mod\ 26\ = (9 - 24)\ mod\ 26 = -15\ mod\ 26 = 11\ (L)$$

$$(A-T)\ mod\ 26\ = (0-19)\ mod\ 26 = -19\ mod\ 26 = 7\ (H)$$

$$(H-H)\ mod\ 26\ = (7-7)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(D-A)\ mod\ 26\ = (3-0)\ mod\ 26 = 3\ mod\ 26 = 3\ (D)$$

$$(R-I)\ mod\ 26\ = (17-9)\ mod\ 26 = 8\ mod\ 26 = 8\ (I)$$

$$(E-L)\ mod\ 26\ = (4-11)\ mod\ 26 = -7\ mod\ 26 = 19\ (T)$$

$$(M-S)\ mod\ 26\ = (12-18)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

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

$$(K-K)\ mod\ 26\ = (10-10)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(A-N)\ mod\ 26\ = (0-13)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(W-E)\ mod\ 26\ = (22-4)\ mod\ 26 = 18\ mod\ 26 = 18\ (S)$$

$$(H-N)\ mod\ 26\ = (7-13)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(A-C)\ mod\ 26\ = (0-2)\ mod\ 26 = -2\ mod\ 26 = 24\ (Y)$$

$$(B-N)\ mod\ 26\ = (1-13)\ mod\ 26 = -12\ mod\ 26 = 14\ (O)$$

$$(E-R)\ mod\ 26\ = (4-17)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(H-T)\ mod\ 26\ = (7-19)\ mod\ 26 = -12\ mod\ 26 = 14\ (O)$$

$$(N-N)\ mod\ 26\ = (13-13)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(A-X)\ mod\ 26\ = (0-23)\ mod\ 26 = -23\ mod\ 26 = 3\ (D)$$

$$(D-Z)\ mod\ 26\ = (3-25)\ mod\ 26 = -22\ mod\ 26 = 4\ (E)$$

$$(A-P)\ mod\ 26\ = (0-15)\ mod\ 26 = -15\ mod\ 26 = 11\ (L)$$

$$(E-W)\ mod\ 26\ = (4-22)\ mod\ 26 = -18\ mod\ 26 = 8\ (I)$$

$$(P-P)\ mod\ 26\ = (15-15)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(I-T)\ mod\ 26\ = (8-19)\ mod\ 26 = -11\ mod\ 26 = 15\ (P)$$

$$(K-Q)\ mod\ 26\ = (10-16)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(E-L)\ mod\ 26\ = (4-11)\ mod\ 26 = -7\ mod\ 26 = 19\ (T)$$

$$(A-J)\ mod\ 26\ = (0-9)\ mod\ 26 = -9\ mod\ 26 = 17\ (R)$$

$$(D-V)\ mod\ 26\ = (3-21)\ mod\ 26 = -18\ mod\ 26 = 8\ (I)$$

$$(I-C)\ mod\ 26\ = (8-2)\ mod\ 26 = 6\ mod\ 26 = 6\ (G)$$

$$(L-U)\ mod\ 26\ = (11-20)\ mod\ 26 = -9\ mod\ 26 = 17\ (R)$$

$$(A-W)\ mod\ 26\ = (0-22)\ mod\ 26 = -22\ mod\ 26 = 4\ (E)$$

$$(N-V)\ mod\ 26\ = (13-21)\ mod\ 26 = -8\ mod\ 26 = 18\ (S)$$

$$(R-J)\ mod\ 26\ = (17-9)\ mod\ 26 = 8\ mod\ 26 = 8\ (I)$$

$$(U-K)\ mod\ 26\ = (20-10)\ mod\ 26 = 10\ mod\ 26 = 10\ (K)$$

$$(A-I)\ mod\ 26\ = (0-8)\ mod\ 26 = -8\ mod\ 26 = 18\ (S)$$

$$(K-Q)\ mod\ 26\ = (10-16)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(N-U)\ mod\ 26\ = (13-20)\ mod\ 26 = -7\ mod\ 26 = 19\ (T)$$

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

$$(N-F)\ mod\ 26\ = (13-5)\ mod\ 26 = 8\ mod\ 26 = 8\ (I)$$

$$(B-J)\ mod\ 26\ = (1-9)\ mod\ 26 = -8\ mod\ 26 = 18\ (S)$$

$$(A-N)\ mod\ 26\ = (0-13)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(L-X)\ mod\ 26\ = (11-23)\ mod\ 26 = -12\ mod\ 26 = 14\ (O)$$

$$(A-A)\ mod\ 26\ = (0-0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(D-S)\ mod\ 26\ = (3-18)\ mod\ 26 = -15\ mod\ 26 = 11\ (L)$$

$$(A-A)\ mod\ 26\ = (0-0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(N-B)\ mod\ 26\ = (13-1)\ mod\ 26 = 12\ mod\ 26 = 12\ (M)$$

$$(A-G)\ mod\ 26\ = (0-6)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(A-P)\ mod\ 26\ = (0-15)\ mod\ 26 = -15\ mod\ 26 = 11\ (L)$$

$$(K-D)\ mod\ 26\ = (10-3)\ mod\ 26 = 7\ mod\ 26 = 7\ (H)$$

$$(A-G)\ mod\ 26\ = (0-6)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(G - D)\ mod\ 26\ = (6 - 3)\ mod\ 26 = 3\ mod\ 26 = 3\ (D)$$

$$(J - J)\ mod\ 26\ = (9 - 9)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(I - W)\ mod\ 26\ = (8 - 22)\ mod\ 26 = -14\ mod\ 26 = 12\ (M)$$

$$(R - R)\ mod\ 26\ = (17 - 17)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(S - H)\ mod\ 26\ = (18 - 7)\ mod\ 26 = 11\ mod\ 26 = 11\ (L)$$

$$(E - E)\ mod\ 26\ = (4 - 4)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(A - N)\ mod\ 26\ = (0 - 13)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(A - U)\ mod\ 26\ = (0 - 20)\ mod\ 26 = -20\ mod\ 26 = 6\ (G)$$

$$(N - N)\ mod\ 26\ = (13 - 13)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(D - W)\ mod\ 26\ = (3 - 22)\ mod\ 26 = -19\ mod\ 26 = 7\ (H)$$

$$(A - O)\ mod\ 26\ = (0 - 14)\ mod\ 26 = -14\ mod\ 26 = 12\ (M)$$

$$(N - N)\ mod\ 26\ = (13 - 13)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

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

$$(E - U)\ mod\ 26\ = (4 - 20)\ mod\ 26 = -16\ mod\ 26 = 10\ (K)$$

$$(N - G)\ mod\ 26\ = (13 - 6)\ mod\ 26 = 7\ mod\ 26 = 7\ (H)$$

$$(G - S)\ mod\ 26\ = (6 - 18)\ mod\ 26 = -12\ mod\ 26 = 14\ (O)$$

$$(A - S)\ mod\ 26\ = (0 - 18)\ mod\ 26 = -18\ mod\ 26 = 8\ (I)$$

$$(A - J)\ mod\ 26\ = (0 - 9)\ mod\ 26 = -9\ mod\ 26 = 17\ (R)$$

$$(R - X)\ mod\ 26\ = (17 - 23)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(E - T)\ mod\ 26\ = (4 - 19)\ mod\ 26 = -15\ mod\ 26 = 11\ (L)$$

$$(A - A)\ mod\ 26\ = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(L - E)\ mod\ 26\ = (11 - 4)\ mod\ 26 = 7\ mod\ 26 = 7\ (H)$$

$$(A - O)\ mod\ 26\ = (0 - 14)\ mod\ 26 = -14\ mod\ 26 = 12\ (M)$$

$$(G - G)\ mod\ 26\ = (6 - 6)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

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

$$(S - D)\ mod\ 26\ = (18 - 3)\ mod\ 26 = 15\ mod\ 26 = 15\ (P)$$

$$(K - Q)\ mod\ 26\ = (10 - 16)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(S - J)\ mod\ 26\ = (18 - 9)\ mod\ 26 = 9\ mod\ 26 = 9\ (J)$$

$$(A - S)\ mod\ 26\ = (0 - 18)\ mod\ 26 = -18\ mod\ 26 = 8\ (I)$$

$$(H - U)\ mod\ 26\ = (7 - 20)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(E - Y)\ mod\ 26\ = (4 - 24)\ mod\ 26 = -20\ mod\ 26 = 6\ (G)$$

$$(U - U)\ mod\ 26\ = (20 - 20)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(R - E)\ mod\ 26\ = (17 - 4)\ mod\ 26 = 13\ mod\ 26 = 13\ (N)$$

$$(I - Z)\ mod\ 26\ = (8 - 25)\ mod\ 26 = -17\ mod\ 26 = 9\ (J)$$

$$(K - Q)\ mod\ 26\ = (10 - 16)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(E - U)\ mod\ 26\ = (4 - 20)\ mod\ 26 = -16\ mod\ 26 = 10\ (K)$$

$$(M - B)\ mod\ 26\ = (12 - 2)\ mod\ 26 = 10\ mod\ 26 = 10\ (K)$$

$$(A - A)\ mod\ 26\ = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(N - V)\ mod\ 26\ = (13 - 21)\ mod\ 26 = -8\ mod\ 26 = 18\ (S)$$

$$(D - Q)\ mod\ 26\ = (3 - 16)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(K - W)\ mod\ 26\ = (10 - 22)\ mod\ 26 = -12\ mod\ 26 = 14\ (O)$$

$$(A - H)\ mod\ 26\ = (0 - 7)\ mod\ 26 = -7\ mod\ 26 = 19\ (T)$$

$$(P - B)\ mod\ 26\ = (15 - 1)\ mod\ 26 = 14\ mod\ 26 = 14\ (O)$$

$$(N - R)\ mod\ 26\ = (13 - 17)\ mod\ 26 = -4\ mod\ 26 = 22\ (W)$$

$$(A - A)\ mod\ 26\ = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(D - W)\ mod\ 26\ = (3 - 22)\ mod\ 26 = -19\ mod\ 26 = 7\ (H)$$

$$(A - B)\ mod\ 26\ = (0 - 2)\ mod\ 26 = -2\ mod\ 26 = 24\ (Y)$$

$$(J - P)\ mod\ 26\ = (9 - 15)\ mod\ 26 = -6\ mod\ 20\ (U)$$

$$(A - O)\ mod\ 26\ = (0 - 14)\ mod\ 26 = -14\ mod\ 26 = 12\ (M)$$

$$(N - N)\ mod\ 26\ = (13 - 13)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(A - P)\ mod\ 26\ = (0 - 15)\ mod\ 26 = -15\ mod\ 26 = 11\ (L)$$

$$(I - I)\ mod\ 26\ = (8 - 8)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)$$

$$(D - Q)\ mod\ 26\ = (3 - 16)\ mod\ 26 = -13\ mod\ 26 = 13\ (N)$$

$$(E - Y)\ mod\ 26\ = (4 - 24)\ mod\ 26 = -20\ mod\ 26 = 6\ (G)$$

$$(I - Y)\ mod\ 26\ = (8 - 24)\ mod\ 26 = -16\ mod\ 26 = 10\ (K)$$

$$(S - L)\ mod\ 26\ = (18 - 11)\ mod\ 26 = 7\ mod\ 26 = 7\ (H)$$

$$(H - T)\ mod\ 26\ = (7 - 19)\ mod\ 26 = -12\ mod\ 26 = 14\ (O)$$

$$(N - F)\ mod\ 26\ = (13 - 5)\ mod\ 26 = 8\ mod\ 26 = 8\ (I)$$

$$(A - J)\ mod\ 26\ = (0 - 9)\ mod\ 26 = -9\ mod\ 26 = 17\ (R)$$

$$(P - V)\ mod\ 26\ = (15 - 21)\ mod\ 26 = -6\ mod\ 26 = 20\ (U)$$

$$(A - X)\ mod\ 26\ = (0 - 23)\ mod\ 26 = -23\ mod\ 26 = 3\ (D)$$

$$(T - L)\ mod\ 26\ = (19 - 11)\ mod\ 26 = 8\ mod\ 26 = 8\ (I)$$

$$(U - H)\ mod\ 26\ = (20 - 7)\ mod\ 26 = 13\ mod\ 26 = 13\ (N)$$

Sehingga Didapatkan hasil *Plaintext* yaitu:

Tabel 4.3 Tabel Plaintext

KHOIRUL HADI	TUBAN	SUYONO
ADELIA PUTRI	GRESIK	SUTRISNO
ALAMUL HUDA	MALANG	AHMAD KHOIRUL
AHMAD PUJI	NGANJUK	KASNOTO
WAHYU	MALANG	KHOIRUDIN

4.3 Kriptografi Dalam Perspektif Islam

Prinsip ketelitian dan konsistensi dalam penggunaan kunci menjadi hal utama Pada algoritma *Beaufort Cipher*, sifat ini mencerminkan bahwa seseorang yang diberi amanah harus menjaga informasi secara akurat dan utuh, tidak boleh ada penyimpangan dalam proses penyampaian (enkripsi) maupun penerimaan (dekripsi). Karena *Beaufort Cipher* bersifat *symmetric cipher* (pengirim dan penerima harus memiliki kunci yang sama), maka terdapat kepercayaan bersama dalam menjaga kerahasiaan kunci. Ini mencerminkan tanggung jawab bersama dalam menjaga amanah antara pemberi dan penerima informasi (Singh, 2000).

Algoritma Route Cipher adalah jenis algoritma transposisi, di mana pesan asli ditempatkan dalam matriks dan kemudian dibaca berdasarkan pola lintasan tertentu (route). Misalnya, bisa dibaca secara spiral, zig-zag, atau arah tertentu yang hanya diketahui oleh pengirim dan penerima. Kaitannya dengan Amanah Route Cipher mengajarkan pentingnya penataan dan pengorganisasian informasi. Pesan yang tidak disusun dan dibaca sesuai aturan yang tepat tidak akan menghasilkan informasi yang bermakna. Ini mengandung nilai ketelitian dalam menjaga struktur amanah, bahwa bukan hanya isi informasi yang penting, tetapi juga cara dan aturan dalam menyampaikannya.Route Cipher juga menyiratkan bahwa dalam menjaga amanah tidak cukup hanya menyembunyikan isi pesan, tetapi juga harus menyamarkan cara mengaksesnya ini menambah lapisan perlindungan terhadap informasi (Stallings, 2017).

Dalam Islam, menjaga amanah tidak terbatas pada aspek fisik, tetapi juga meliputi informasi, data, dan bahkan rahasia pribadi atau publik. Rasulullah SAW

bersabda: "Tidak beriman orang yang tidak bisa dipercaya dan tidak ada agama bagi orang yang tidak memegang janji." (HR. Ahmad dan Al-Baihaqi).

Kriptografi termasuk algoritma Beaufort Cipher dan Route Cipher, dapat dipahami sebagai bentuk ijtihad teknologi dalam menjaga amanah di era digital. Tujuan utama dari penggunaan algoritma ini adalah untuk Menjamin kerahasiaan pesan, Menjaga integritas data (tidak diubah pihak ketiga), Menentukan akses yang sah terhadap informasi (hanya oleh pemilik kunci), Mencegah penyalahgunaan informasi oleh pihak yang tidak bertanggung jawab (Stinson, 2006).

Dengan pendekatan gabungan antara algoritma kriptografi klasik dan nilai-nilai Islam, dapat disimpulkan bahwa Beaufort Cipher menunjukkan pentingnya kunci yang dijaga secara simetris dan penuh tanggung jawab, sejalan dengan kepercayaan antar sesama pemegang amanah. Route Cipher menekankan pentingnya struktur dan sistematika dalam menjaga Amanah mirip dengan cara Islam mengatur hukum dan amanah sesuai tempatnya.

Kriptografi bukan sekadar solusi teknis, tetapi juga merupakan bagian dari etika digital yang selaras dengan ajaran Islam, khususnya dalam menjaga dan menunaikan amanah secara profesional, teliti, dan bertanggung jawab.

BAB V

PENUTUP

5.1 Kesimpulan

Kriptografi yang dengan menggunakan modifikasi algoritma Beaufort Cipher dengan algoritma Route Chipeh untuk mengamankan data penduduk telah dilakukan dan penulis mendapatkan kesimpulan sebagai berikut:

1. Proses enkripsi yang dilakukan dengan modifikasi algoritma *Beaufort Cipher* dengan *Route Cipher* dilakukan dengan mengenkripsi Plainkey yang telah ditentukan menggunakan algoritma *Route Cipher* terlebih dahulu, hasil dari enkripsi tersebut berupa *Cipherkey*, kemudian *Cipherkey* tersebut akan digunakan sebagai kunci kriptografi *Beaufort Cipher*.
2. Proses dekripsi yang dilakukan dengan modifikasi algoritma *Beaufort Cipher* dengan algoritma Route Cipher dilakukan dengan mendekripsi *cipherkey* menggunakan *Route Cipher* terlebih dahulu, kemudian hasil dari dekripsi berupa *Cipherkey* tersebut akan digunakan sebagai kunci kriptografi *Beaufort Cipher* sehingga diperoleh *Plaintext*, dengan demikian proses dekripsi pada modifikasi algoritma *Beaufort Cipher* dengan algoritma *Route Cipher* melalui dua kali proses dekripsi.

5.2 Saran

Skripsi ini menggunakan algoritma *Beaufort Cipher* dengan algoritma *Route Cipher*. serta terbatas pada 26 huruf alfabet dan karakter tambahan berupa karakter pagar (#). Sehingga untuk skripsi selanjutnya diharapkan dapat menggunakan algoritma lain yang lebih aman dan dapat memuat berbagai karakter baik itu huruf alfabet, angka, dan simbol-simbol lainnya.

DAFTAR PUSTAKA

Ahmad Warson Munawir, 1997, “Al-Insaan fi Al-Qur’an” penerjemaah, Tim Penerjemah Pustaka Firdaus, Manusia Diungkap Al-Qur’an, Jakarta: Pustaka Fidaus.

Al-Baihaqi. (n.d.). *Syu’ab al-Iman*.

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

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

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). mplementasi Algoritma Route Cipher Dalam Pengamanan File Pdf. *Building of nformatics,Technology and Science (BITS)*, *1*(1), 1-6.

Dalimunthe, R. P. (2018). Amanah Dalam Perspektif Hadis. *Diroyah : Jurnal Studi lmu Hadis*, *1*(1), 7–16. https://doi.org/10.15575/diroyah.v1i1.2050

Irawan, Wahyu Henky, D. (2014). *Pengantar Teori Bilangan* (F. H. A, Ed.; 1st ed.). Uin-Maliki Press.

Lingga, A. (2019). Analisa mplementasi Aplikasi Keamanan File Audio Wav Dengan Menerapkan Algoritma Beaufort Cipherdan Root 13. *Jurnal Pelita nformatika*, *8*(1), 33–40.

Rachmadsyah, A., Perdana, A., & Budiman, A. (2020). Kombinasi Algoritma Beaufort Cipher dan Vigenere Cipher untuk Pengamanan Pesan Teks Berbasis Mobile Application. *Jurnal Minfo Polgan*, *9*(September), 12–17.

Setyaningsih Emy. (2015). *Kriptografi & mplementasi menggunakan Matlab* (Nikodemus WK, Ed.; 1st ed.).

Setyaningsih Emy. (2015a). *Kriptografi & mplementasi menggunakan Matlab* (Nikodemus WK, Ed.; 1st ed.).

Setyaningsih Emy. (2015b). *Kriptografi & mplementasi menggunakan Matlab* (Nikodemus WK, Ed.; 1st ed.).

Singh, S. (2000). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. London: Fourth Estate.

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.

Stinson, D. R. (2006). *Cryptography: Theory and Practice* (3rd ed.). CRC Press.

Surya, M. (n.d.). *Modifikasi Vigenere Cipher Dengan Menggunakan Teknik Pengenkripsian Pada Kuncinya*.

RIWAYAT HIDUP

Muhammad Fahrul Rois lahir pada tanggal 1 Desember 1999. Laki-laki yang biasa dipanggil Rois ini beralamat di Desa Sumurber RT/RW 001/001, Kecamatan Panceng, Kabupaten Gresik, anak kedua dari dua bersaudara yakni dari pasangan Bapak Mad Thomaji dan Ibu Mardliyah.

Penulis telah menempuh pendidikan formal mulai dari TK Muslimat NU dan lulus pada tahun 2006. Setelah itu, penulis menempuh pendidikan dasar di MI Tarbiyatul Athfal dan lulus pada tahun 2012. Selanjutnya penulis menempuh pendidikan menengah pertama di SMP Negeri 1 Sidayu dan lulus pada tahun 2015. Kemudian, penulis menempuh pendidikan menengah atas di MAN 4 Jombang dan lulus pada tahun 2018. Selanjutnya penulis menempuh pendidikan tinggi di Universitas Islam Negeri Maulana Malik Ibrahim Malang pada tahun 2018.

Selain menjadi mahasiswa, penulis juga berperan dalam mengembangkan kemampuannya di organisasi ekstra kampus. Antara lain pernah aktif menjadi pengurus IKAPPMAMM (Ikatan Alumni Pondok Pesantren Mamba'ul Ma'arif) pada tahun 2019-2020.

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 : Muhammad Fahrul Rois
NIM : 18610110
Fakultas / Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Modifikasi Super Enkripsi Algoritma Beaufort Cipher dan Route Cipher Untuk Mengamankan Data Penduduk
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Erna Herawati, M.Pd

No	Tanggal	Hal	Tanda Tangan
1.	25 Februari 2025	Konsultasi Topik dan Data	1.
2.	3 Maret 2025	Konsultasi Bab I, II, dan III	2.
3.	7 Maret 2025	Konsultasi Kajian Agama Bab I dan II	3.
4.	14 April 2025	Konsultasi Bab I, II, dan III	4.
5.	21 April 2025	Konsultasi Bab I, II, dan III	5.
6.	2 Mei 2025	ACC Bab I, II, dan III	6.
7.	14 Mei 2025	ACC Kajian Agama Bab I dan II	7.
8.	19 Mei 2025	ACC Seminar Proposal	8.
9.	23 Mei 2025	Konsultasi Revisi Seminar Proposal	9.
10.	23 Mei 2025	Konsultasi Bab IV dan V	10.
11.	26 Mei 2025	Konsultasi Bab IV dan V	11.
12.	26 Mei 2025	ACC Bab IV dan V	12.
13.	23 Mei 2025	Konsultasi Kajian Agama Bab IV	13.
14.	26 Mei 2025	ACC Kajian Agama Bab IV	14.
15.	27 Mei 2025	ACC Seminar Hasil	15.

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

16.	9 Juni 2024	Konsultasi Revisi Seminar Hasil	16.
17.	13 Juni 2024	ACC Sidang Skripsi	17.
18.	25 Juni 2024	ACC Keseluruhan	18.

Malang, 25 Juni 2025
Mengetahui,
Ketua Program Studi Matematika

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