MODIFIKASI ALGORITMA *BEAUFORT CIPHER* DENGAN TRANSPOSISI GRUP SIMETRI UNTUK MENGAMANKAN PESAN

SKRIPSI

OLEH
MUHAMMAD ZULFIKRI RANGGA
NIM.18610096

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

MODIFIKASI ALGORITMA *BEAUFORT CIPHER* DENGAN TRANSPOSISI GRUP SIMETRI UNTUK MENGAMANKAN PESAN

SKRIPSI

OLEH
MUHAMMAD ZULFIKRI RANGGA
NIM.18610096

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

MODIFIKASI ALGORITMA *BEAUFORT CIPHER* DENGAN TRANSPOSISI GRUP SIMETRI 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
MUHAMMAD ZULFIKRI RANGGA
NIM. 18610096

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

MODIFIKASI ALGORITMA *BEAUFORT CIPHER* DENGAN TRANSPOSISI GRUP SIMETRI UNTUK MENGAMANKAN PESAN

SKRIPSI

Oleh
Muhammad Zulfikri Rangga
NIM. 18610096

Telah Diperiksa dan Disetujui untuk Diuji

Malang, 02 Desember 2022

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah, M.Si	Mohammad Nafie Jauhari, M.Si
NIDT. 199005112016080 1 057	NIDT. 19870218 20160801 1 056

Mengetahui,
Ketua Program Studi Matematika

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

MODIFIKASI ALGORITMA *BEAUFORT CHIPER* DENGAN TRANSPOSISI GRUP SIMETRI UNTUK MENGAMANKAN PESAN

SKRIPSI

Oleh
Muhammad Zulfikri Rangga
NIM. 18610096

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal, 14 Desember 2022

Ketua Penguji	: Prof. Dr. H. Turmudi, M.Si., Ph.D.	.....
Anggota Penguji 1	: Dr. H. Imam Sujarwo, M,Pd.	.....
Anggota Penguji 2	: Muhammad Khudzaifah, M.Si.	.....
Anggota Penguji 3	: Mohammad Nafie Jauhari, M.Si.	.....

Mengetahui,
Ketua Program Studi Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan dibawah ini :

Nama	:	Muhammad Zulfikri Rangga
NIM	:	18610096
Program Studi	:	Matematika
Fakultas	:	Sains dan Teknologi
Judul Skripsi	:	Modifikasi Algoritma *Beaufort Cipher* Dengan Transposisi Grup Simetri untuk Mengamankan Pesan.

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 tulisan dan pikiran saya sendiri, kecuali dengan mencantumkan sumber-sumber terkait pada daftar pustaka. Apabila dikemudian hari terbukti atau dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perilaku tersebut.

Malang, 14 Desember 2022
Yang membuat pernyataan

Muhammad Zulfikri Rangga
NIM. 18610096

MOTO

“Jangan mengeluh dengan apa yang anda lakukan, tetap semangat dan tidak berputus asa yakini semua pasti indah pada waktunya”.

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:

Kedua orang tua tercinta yaitu Bapak Ismail dan Ibu Aprilina Adi Warsa serta saudara saya Muhammad Zulfikar Rangga, yang senantiasa menyemangati dan mendo'akan penulis agar dapat menyelesaikan skripsi ini.

Seluruh teman-teman AKSIOMA dan sahabat-sahabat penulis yang selalu menyemangati, memberi motivasi serta dukungan moral untuk penulis menyelesaikan skripsi ini.

KATA PENGANTAR

Assalamu'alaikum Wr.Wb.

Segala puja dan puji syukur ke hadirat Allah SWT yang telah memberikan rahmat dan hidayah nya kepada penulis sehingga dapat menyelesaikan proposal skripsi saya yang berjudul "Modifikasi Algoritma Beaufort Cipher dengan Transposisi Grup Simetri untuk mengamankan pesan" dan menjadi syarat untuk mendapatkan gelar sarjana matematika pada Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Shalawat serta salam tercurahkan pada Nabi Muhammad Saw yang telah menunjukkan jalan yang terang benderang pada umatnya.

Ucapan terima kasih yang banyak penulis haturkan kepada berbagai pihak yang telah membantu, memotivasi dan mendukung penulis dalam menyelesaikan proposal skripsi yaitu kepada:

1. Prof. Dr. H. M. Zainuddin, M.A., 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, S.Pd., M.Sc., selaku Ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Muhammad Khudzaifah, M. Si, selaku pembimbing I.
5. Mohammad Nafie Jauhari, M. Si, selaku pembimbing II.
6. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Negeri Maulana Malik Ibrahim Malang.
7. Kedua orang tua dan keluarga yang selalu memberikan doa agar penulis dapat menyelesaikan skripsi nya dengan lancar dan baik.
8. Seluruh mahasiswa matematika angkatan 2018.

Penulis menyadari bahwa pembuatan draf skripsi ini masih banyak memiliki kekurangan oleh karena itu maka kritik serta saran yang membangun dan mendukung akan berdampak baik pada penulisan draf skripsi penulis. Harapan penulis setelah menyelesaikan draf skripsi ini adalah dapat menambah wawasan keilmuan dan daya tarik bagi penulis serta bagi pembaca terkait dalam keilmuan

matematika lebih khususnya pada bidang kriptografi terutama pada kriptografi klasik yang merupakan awal dari kriptografi dan berkembang hingga sekarang menjadi kriptografi modern.

Wassalamu'alaikum Wr.Wb.

Malang, 14 Desember 2022

Penulis

DAFTAR ISI

HALAMAN JUDUL ..... **i**
HALAMAN PENGAJUAN ..... **ii**
HALAMAN PERSETUJUAN ..... **iii**
HALAMAN PENGSAHAN ..... **iv**
PERNYATAAN KEASLIAN TULISAN ..... **v**
MOTO ..... **vi**
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 4
BAB II KAJIAN PUSTAKA **6**
2.1 Teori Pendukung 6
2.1.1 Keterbagian 6
2.1.2 Kongruensi 8
2.1.3 Grup 10
2.1.4 Grup Simetri 11
2.1.5 Kriptografi 14
2.1.6 Enkripsi dan Dekripsi 15
2.1.7 Metode Substitusi 16
2.1.8 Beaufort Cipher 17
2.1.8.1 Proses Enkripsi 19
2.1.8.2 Proses Dekripsi 20
2.1.9 Metode Transposisi 22
2.1.10 Super Enkripsi 28
2.1.11 Modifikasi *Beaufort Cipher* dengan Transposisi Grup Simetri 32
2.2 Kajian Integrasi Topik dengan Al-Quran/Hadist 35
2.3 Kajian Topik dengan Teori Pendukung 37
BAB III METODE PENELITIAN **38**
3.1 Jenis Penelitian 38
3.2 Pra Penelitian 38
3.3 Tahapan Penelitian 38
BAB IV PEMBAHASAN **42**
4.1 Proses Enkripsi Modifikasi Algoritma *Beaufort Cipher* dengan Transposisi Grup Simetri 42

4.1.1 Simulasi Proses Enkripsi *Beaufort Cipher* 42
4.1.2 Simulasi Proses Enkripsi $\boldsymbol{S_4}$ 44
4.1.3 Simulasi Proses Enkripsi $\boldsymbol{S_5}$ 49
4.1.4 Simulasi Proses Enkripsi $\boldsymbol{S_6}$ 52
4.2 Proses Dekripsi Modifikasi Algoritma *Beaufort Cipher* dengan Transposisi Grup Simetri 55
4.2.1 Simulasi Proses Dekripsi *Beaufort Cipher* 56
4.2.2 Simulasi Proses Dekripsi $\boldsymbol{S_4}$ 58
4.2.3 Simulasi Proses Dekripsi $\boldsymbol{S_5}$ 61
4.2.4 Simulasi Proses Dekripsi $\boldsymbol{S_6}$ 64
4.3 Amanah Dalam Kriptografi 70
BAB V PENUTUP 72
5.1 Kesimpulan 72
5.2 Saran untuk Penelitian Lanjutan 73
DAFTAR PUSTAKA 74
LAMPIRAN 75
RIWAYAT HIDUP 85

DAFTAR TABEL

Tabel 2.1 Tabel Cayley 12
Tabel 2.2 Tabel Konversi Enkripsi 19
Tabel 2.3 Tabel Konversi Dekripsi 20
Tabel 2.4 Tabel Kunci Algoritma Transposisi Grup Simetri 22
Tabel 2.5 Tabel Kunci Invers Algoritma Transposisi Grup Simetri 23
Tabel 2.6 Tabel Algoritma Zig-zag 26
Tabel 2.7 Tabel Algoritma Segitiga 27
Tabel 2.8 Tabel Algoritma Spiral 27
Tabel 2.9 Tabel Algoritma Diagonal 28
Tabel 2.10 Tabel Kunci Enkripsi Transposisi Grup Simetri 30
Tabel 2.11 Tabel Kunci Invers Dekripsi Transposisi Grup Simetri 30
Tabel 4.1 Tabel Konversi Enkripsi 42
Tabel 4.2 Tabel Konversi Dekripsi 56
Tabel 4.3 Pengelompokan Ciphertext 68
Tabel 4.4 Tabel Perbandingan Hasil Enkripsi 69

DAFTAR GAMBAR

Gambar 2.2 Mekanisme Kriptografi 16
Gambar 3.1 Flowchart Enkripsi 40
Gambar 3.2 Flowchart Dekripsi 41

ABSTRAK

Rangga, Muhammad Zulfikri.2022. **Modifikasi Algoritma *Beaufort Cipher* Dengan Transposisi Grup Simetri.** Skripsi. Program Studi Matematika. Fakultas Sains Dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si (II) Mohammad Nafie Jauhari, M.Si

Kata Kunci: Kriptografi, *Beaufort Cipher*, Transposisi Grup Simetri, Enkripsi, Dekripsi, Super Enkripsi

Kriptografi adalah sebuah cara untuk mengamankan pesan salah satunya adalah algoritma *Beaufort Cipher* yang telah ada. Namun algoritma tersebut dapat pecahkan dengan metode Kasiski dan *exhaustive key search*, oleh karena itu penulis ingin melakukan modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri, penelitian ini menggunakan metode subtitusi yakni *Beaufort Cipher* dengan persamaan enkripsinya adalah $C_i \equiv (K_i - P_i)\ mod\ n$ serta persamaan dekripsinya adalah $P_i \equiv (K_i - C_i)\ mod\ n$ dan metode transposisi grup simetri, dengan dua metode tersebut dapat dibuat sebuah algoritma baru yang tingkat keamanannya lebih tinggi daripada hanya menggunakan satu metode saja, penggabungan dua metode tersebut dikenal sebagai super enkripsi dengan begitu dapat disimpulkan bahwa modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri memiliki proses dua kali enkripsi dan dua kali proses dekripsi yang dapat dilakukan dengan urutan pertama menentukan *Plaintext*, kemudian akan dilakukan proses enkripsi dengan transposisi grup simetri terlebih dahulu lalu akan dienkripsi kembali dengan *Beaufort Cipher*. setelah proses tersebut untuk dekripsinya mengginakan *Beaufort Cipher* kemudian transposisi grup simetri. Dengan algoritma yang telah dimodifikasi tersebut pesan yang di enkripsi lebih aman, karena dengan metode Kasiski dan *exhaustive key search* sulit untuk dipecahkan.

ABSTRACT

Rangga, Muhammad Zulfikri. 2022. **Modification of the Beaufort Cipher Algorithm with Symmetry Group Transposition.** Thesis. Mathematics Study Program. Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisor: (I) Muhammad Khudzaifah, M.Si (II) Mohammad Nafie Jauhari, M.Si

Keywords: Cryptography, Beaufort Cipher, Symmetry Group Transposition, Encryption, Decryption, Super Encryption

Complicated cryptography with twice the security such as modification of the Beaufort Cipher algorithm with symmetric group transposition will make it difficult for message thieves. This study uses the substitution method namely Beaufort Cipher with the encryption equation is $C_i\ (K_i - P_i\ )\ mod$ n and its decryption equation is $P_i \equiv (K_i - C_i\ )\ mod\ n$ and the symmetric group transposition method. With these two methods, a new algorithm can be created which has a higher level of security than using only one method. The combination of the two methods is known as super encryption, so it can be concluded that the modification of the Beaufort Cipher algorithm with symmetric group transposition has two encryption processes this is done by first determining the Plaintext, then the encryption process will be carried out with group transposition symmetry first and then it will be re-encrypted with Beaufort Cipher. The decryption process used the Beaufort Cipher algoritm then the symetric group transposition. With the modified algorithm, the encrypted message is more secure, because with the Kasiski method and exhaustive key search it is difficult to solve.

مستخلص البحث

رانجا ، محمد ذو الفكري. ٢٠٢٢. تعديل خوارزمية *تشفير بوفورت* مع تبديل مجموعة التماثل. البحث العلمي. قسم الرياضيات. كلية العلوم والتكنولوجيا ، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف الأول: محمد خديفة، الماجستير، محمد خضيفة ،المشرفة الثانية: محمد نافع جوهري ، الماجستير.

الكلمات الرئيسية: التشفير ، نقل مجموعة التناظر ، التشفير ، فك التشفير ، التشفير *Beaufort Cipher* ، الفائق

التشفير هو وسيلة لتأمين الرسائل ، أحدها هي خوارزمية *Beaufort Cipher* . ومع ذلك ، يمكن حل *الموجودة* الخوارزمية بطريقة *Kasisiki* تعديل خوارزمية لذلك يريد المؤلف ، *الشامل عن المفاتيح* والبحث *Beaufort* مع تبديل مجموعة التماثل ، تستخدم هذه الدراسة طريقة الاستبدال ، وهي *Beaufort Cipher* مع معادلة التشفير هي $C_i \equiv (K_i - P_i)\ mod\ nP_i \equiv$ ومعادلة فك التشفير هي *Cipher* $(K_i - C_i)\ mod\ n$ وطريقة تبديل المجموعات المتماثلة، مع هاتين الطريقتين يمكن إنشاء خوارزمية جديدةهذه خوارزمية يكون مستوى أمانها أعلى من استخدام طريقة واحدة فقط، يعرف ويجمع الطريقتين بالتشفير مع تبديل مجموعة التماثل لديه عملية *Beaufort Cipher* الفائق بحيث يمكن استنتاج أن تعديل خوارزمية تشفير مرتين وضعف عملية فك التشفير التي يمكن القيام بها مع تحديد الترتيب الأول *نص عادي* ، ثم سيتم تنفيذ . بعد *Beaufort Cipher* عملية التشفير عن طريق تبديل مجموعة التماثل أولا ثم سيتم إعادة تشفيرها باستخدام عملية فك تشفيرها باستخدام *تشفي* بوفورت *ثم* تبديل مجموعة التماثل. باستخدام الخوارزمية المعدلة ، تكون والبحث *الشامل عن المفاتيح* ، يصعب حلها *Kasisiki* الرسالة المشفرة أكثر أمانا ، لأنه مع طريقة

BAB I
PENDAHULUAN

1.1 Latar Belakang

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 dengan langsung atau melalui perantara berupa media cetak, media elektronik, dan media sosial, namun tidak semua pesan yang disampaikan tersebut boleh dilihat dan dibaca oleh khalayak umum, karena beberapa informasi memiliki data yang penting. Untuk 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 informasi.(Setyaningsih Emy, 2015)

Kriptografi memiliki mekanisme dalam menyandikan informasi 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, 2015). Dalam hal ini dapat disimpulkan bahwa manusia akan terus mempelajari suatu ilmu dan akan mendapatkan ilmu tambahan dan telah dijelaskan dalam salah satu firman Allah SWT pada al-Quran surat at- Taha/20:114, yaitu:

﴿ فَتَعٰلَى اللّٰهُ الْمَلِكُ الْحَقُّۚ وَلَا تَعْجَلْ بِالْقُرْاٰنِ مِنْ قَبْلِ اَنْ يُّقْضٰٓى اِلَيْكَ وَحْيُهٗۖ وَقُلْ رَّبِّ زِدْنِيْ عِلْمًا ١١٤ ﴾(طٰه/20:114)

"Maha tinggi Allah, Raja yang sebenar-benarnya. Janganlah engkau (Nabi Muhammad) tergesa-gesa (membaca) Al-Qur'an sebelum selesai pewahyuan nya kepadaMu dan katakanlah, "Ya Tuhanku, tambahkanlah ilmu kepadaku". (Q.S Taha/10:114).

Berdasarkan penggalan surat At-Taha di atas menjelaskan bahwa ketika membaca sebuah ilmu maka bacalah secara berulang-ulang sehingga dapat segera hafal dan memahami secara menyeluruh terkait ilmu tersebut. Dalam hal ini penulis ingin mempelajari lebih dalam terkait dengan kriptografi klasik yang telah lama ditemukan, namun masih dapat dikembangkan kembali dengan menggunakan metode-metode kriptografi klasik lainnya sehingga akan menghasilkan algoritma yang tingkat keamanan nya lebih baik dari yang sebelumnya.

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 ingin menambah keamanan algoritma *Beaufort cipher* dengan menggabungkan algoritma tersebut dengan algoritma lain berupa algoritma transposisi grup simetri. 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 kriptografi grup simetri yang merupakan algoritma kriptografi *cipher* transposisi (Riskiyah, 2016). Dengan begitu peneliti ingin melakukan kajian penelitian yang berjudul "Modifikasi Algoritma *Beaufort Cipher* dengan Transposisi Grup Simetri untuk mengamankan pesan"

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* dengan transposisi grup simetri?
2. Bagaimana proses dekripsi menggunakan modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri?

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* dengan transposisi grup simetri untuk pengamanan pesan.

2. Mengetahui bagaimana proses dekripsi menggunakan modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri untuk pengamanan pesan.

1.4 Manfaat Penelitian

1. Bagi penulis

   Penelitian ini dapat menambah wawasan tentang kriptografi klasik dan modifikasi nya terutama pada algoritma Beaufort cipher dan transposisi grup simetri.

   Bagi pembaca

2. Penelitian ini dapat memperkaya ilmu pengetahuan dan tata cara proses enkripsi dan dekripsi tentang kriptografi klasik pada algoritma *Beaufort Cipher* dan transposisi grup simetri dalam pengamanan informasi.
3. Bagi lembaga

   Penelitian yang telah dibuat dapat menambah bahan literasi dan informasi 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 alfabet dan karakter persen “%” serta pagar “#” untuk proses enkripsi dan proses dekripsi.
2. Permutasi grup simetri yang digunakan adalah grup $S_4, S_5, dan\ S_6$.

1.6 Definisi Istilah

Penulisan pada penelitian ini menggunakan banyak istilah sehingga penulis memberikan definisi dari istilah pada bagian awal agar pembaca lebih mudah untuk memahami, berikut adalah istilah-istilah yang penulis gunakan:

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/Sistem kriptografi adalah keseluruhan proses dari kriptografi itu sendiri yang meliputi proses enkripsi, dekripsi, *Plaintext*, *Ciphertext* dan kunci.
7. Kunci permutasi dalam algoritma transposisi menggunakan simbol π.
8. Kunci invers dalam algoritma transposi menggunakan simbol π^{-1}.
9. Algoritma modifikasi dalam penelitian ini adalah merubah susunan dalam proses super enkripsi yang menggunakan algoritma transposisi terlebih dahulu kemudian menggunakan algoritma substitusi.

BAB II
KAJIAN PUSTAKA

2.1 Teori Pendukung

2.1.1 Keterbagian

Keterbagian adalah dasar dalam ilmu 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 embagi 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 $a|c$ maka $a|b \pm$ c

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)

2. $b + c = a(k_1 + k_2)$, $(k_1 + k_2) \in \mathbb{Z}$ (Menjumlahkan $b\ dan\ c$)

   $b - c = a(k_1 - k_2)$ $(k_1 + k_2) \in \mathbb{Z}$ (Mengurangkan $b\ dan\ c$)

   Terbukti $a|b \pm c$

Teorema 4

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 5

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 $x \equiv y(mod\ m)$.

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

$$x \equiv x\ (mod\ m)$$

Bukti:

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

2. Simetris

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

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

Dan untuk $y \equiv x(mod\ m)$ 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 $x \equiv y(mod\ m)$, maka $y \equiv x(mod\ m)$ akan ekuivalen dengan $x - y \equiv 0(mod\ m)$.

3. Transitif

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

   Bukti:

   $x \equiv y(mod\ m)$ berarti $m|(x - y)$ (Definisi kongruensi)

   $y \equiv z(mod\ m)$ 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 Grup

Struktur aljabar jika ada $(G,\circ)$ yang berisikan himpunan yang tak kosong G dengan operasi $\circ$ disebut sebuah grup jika memenuhi syarat-syarat berikut:

1. Tertutup: apabila operasi biner $\circ$ menghasilkan nilai yang juga ada pada G.

$$\forall\, a, b \in G, maka\ a * b\ \in G$$

2. Asosiatif: apabila operasi $\circ$ bersifat asosiatif pada G

$$\forall\, a, b, dan\ c\ \in G\ maka\ (a \circ b) \circ c = a \circ (b \circ c)$$

3. Memiliki elemen identitas yang dinotasikan dengan e sedemikian sehingga $e \circ a = a \circ e = a,\ \forall a \in G$.
4. Memiliki invers: setiap elemen di G memiliki invers $\forall\, a \in G, \exists a^{-1} \in G$ sedemikian sehingga $a \circ a^{-1} = a^{-1} \circ a = e$.

Apabila ada $(G,\circ)$ suatu grup yang memiliki sifat komutatif, maka $(G,\circ)$ grup tersebut dapat disebut dengan grup abelian.(Suryanti, 2017)

Contoh 2.1.2:

Misalkan diberikan Z adalah himpunan semua bilangan bulat dan didefinisikan dengan operasi $+$ atau dapat ditulis $(Z, +)$ adalah sebuah grup karena memenuhi syara-syarat berikut:

1. $\forall\, m, n \in Z\ maka\ m + n \in Z$

   Jadi Z tertutup terhadap operasi $+$.

2. $\forall\, m, n, dan\ o \in Z\ maka\ (m + n) + o = m + (n + o)$

   Jadi Z bersifat asosiatif.

3. Ambil $e \in Z$ sehingga $m + e = e + m = m\ , \forall\, m \in Z$

   Jadi $e = 0$ adalah elemen identitas pada $(Z, +)$.

4. $\forall\, m \in Z$, maka ada $m^{-1} \in Z$ sedemikian sehingga $m + m^{-1} = m^{-1} + m = e$, jadi $m^{-1} = -m$ merupakan invers dari m.

2.1.4 Grup Simetri

Didefinisikan N adalah sebarang himpunan tak kosong dan S_N adalah himpunan dari semua fungsi bijektif $f: N \to N$, maka S_N dengan operasi komposisi atau dapat dinotasikan dengan "$\circ$" merupakan suatu grup, jika $f: N \to N$ dan

$G: N \to N$ adalah fungsi-fungsi bijektif, maka $F \circ G$ juga suatu fungsi bijektif dari $N \to N$, kemudian operasi komposisi " $\circ$ " adalah komposisi fungsi yang bersifat asosiatif, memiliki elemen identitas dari S_n adalah $1(a) = a, \forall a \in n$, dan setiap permutasi memiliki invers yang memenuhi $f \circ f^{-1} = f^{-1} \circ f = 1$. Dengan demikian $(S_n, \circ)$ telah memenuhi semua syarat-syarat untuk dikatakan sebagai grup. $(S_n, \circ)$ biasanya disebut dengan grup permutasi atau grup simetri.(Suryanti, 2017)

Contoh 2.1.3:

Misalkan ambil $a = \{a, b, c\}$ akan membentuk suatu permutasi sebagai berikut:

$$a_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, a_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, a_3 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$

$$a_4 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, a_5 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, a_6 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$

Dari permutasi di atas dapat dilakukan sebuah operasi komposisi yang dapat dilihat pada tabel *Cayley* berikut:

Tabel 2. 1 Tabel Cayley

	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6
a_2	a_2	a_1	a_4	a_3	a_6	a_5
a_3	a_3	a_5	a_1	a_6	a_2	a_4
a_4	a_4	a_6	a_2	a_5	a_1	a_3
a_5	a_5	a_3	a_6	a_1	a_4	a_2
a_6	a_6	a_4	a_5	a_2	a_3	a_1

Dari tabel *Cayley* di atas maka dapat disimpulkan bahwa a memiliki sifat-sifat berikut:

1. Misalkan dari permutasi a diambil dan dilakukan operasi komposisi sebagai berikut:

$$a_2 \circ a_3 = a_5$$

dengan demikian jelas bahwa permutasi a tertutup.

2. Misalkan dari permutasi a diambil dan dilakukan operasi komposisi sebagai berikut:

$$(a_1 \circ a_2) \circ a_3 = a_2 \circ a_3 = a_5$$

$$a_1 \circ (a_2 \circ a_3) = a_1 \circ a_5 = a_4$$

Karena pernyataan di atas maka terbukti bahwa fungsi a dengan operasi komposisi bersifat asosiatif.

3. Tabel *Cayley* di atas menunjukkan bahwa identitas dari permutasi a adalah a_1 karena permutasi apapun yang ada di a apabila dioperasikan dengan a_1 akan menghasilkan dirinya sendiri, maka a_1 merupakan identitas.

$$a_1 \circ a_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

$$a_5 \circ a_4 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = a_1$$

4. Memiliki invers berarti suatu permutasi yang dioperasikan dengan permutasi lain menggunakan operasi komposisi menghasilkan identitas maka permutasi tersebut saling invers

   Dari contoh di atas maka dapat disimpulkan bahwa a_5 memiliki invers yaitu a_4.

2.1.5 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*

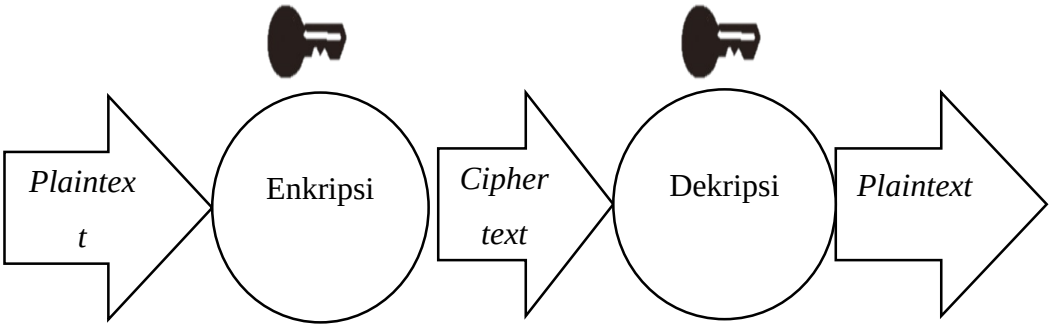
Bangsa Arab juga mengembangkan kriptografi sendiri karena kepandaian bangsa arab terhadap bidang statistik, matematika dan linguistik. Kriptografi dikemukakan oleh seorang filsuf terkenal yaitu Yusuf Ya'Qub Ishaq Ibnu As-Sabbah Ibnu 'Omran Ibnu Ismail Al-Kindi yang lebih sering dikenal sebagai Al-Kindi,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

2.1.6 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)



Gambar 2.1 Mekanisme Kriptografi

2.1.7 Metode Substitusi

Algoritma substitusi adalah sebuah algoritma kriptografi yang mengubah setiap karakter dari pesan asli (*Plaintext*) menjadi pesan yang dikode kan (*Ciphertext*), setiap karakter yang dimaksud dapat berupa karakter huruf, pasangan karakter, atau banyak kelompok pasangan karakter. (Rachman & Ariyus, 2020) Algoritma substitusi memiliki empat (4) jenis algoritma, yaitu:

1. *Cipher* abjad tunggal *(monoalphabethic cipher)*;
2. *Cipher homofonik (homophonic substitution cipher);*
3. *Cipher abjad majemuk (polyalphabethic substitution cipher);*

4. *Cipher poligram (polygram substitution cipher).*

Contoh algoritma kriptografi algoritma substitusi adalah *Caesar cipher*, *Vigenere cipher*, *Beaufort cipher*, *Playfair cipher*, *Hill cipher*, dan masih banyak yang lainnya.(Setyaningsih Emy, 2015)

2.1.8 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:

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

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:

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

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

$C_i \equiv (K_i - P_i) mod\ 26$ (Rumus enkripsi)

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

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

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

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

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

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

$P_i \equiv (K_i - C_i) mod\ 26$ (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 $C_i \equiv (K_i - P_i)\ mod\ n$.
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 $P_i \equiv (K_i - C_i)\ mod\ n$.
8. Diperoleh *Plaintext*.

2.1.8.1 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 2.1.4:

Plaintext: MATEMATIKA

Kunci: SAINS

Hasil yang telah didapatkan akan kita rubah dari bentuk alfabet ke dalam bentuk numerik (lampiran1) seperti di bawah ini:

Tabel 2.2 Tabel Konversi Enkripsi

PLAINTEXT	M 12	A 0	T 19	E 4	M 12	A 0	T 19	I 8	K 10	A 0
KUNCI	S 18	A 0	I 8	N 13	S 18	S 18	A 0	I 8	N 13	S 18

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

$$(S - M)\ mod\ 26\ \rightarrow (18 - 12)\ mod\ 26 \equiv 6\ mod\ 26 \equiv 6\ (G)$$

$$(A - A)\ mod\ 26\ \rightarrow (0 - 0)\ mod\ 26 \equiv 0\ mod\ 26 \equiv 0\ (A)$$

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

$$(N - E)\ mod\ 26\ \rightarrow (13 - 4)\ mod\ 26 \equiv 9\ mod\ 26 \equiv 9\ (J)$$

$$(S - M)\ mod\ 26\ \rightarrow (18 - 12)\ mod\ 26 \equiv 6\ mod\ 26 \equiv 6\ (G)$$

$$(S - A)\ mod\ 26\ \rightarrow (18 - 0)\ mod\ 26 \equiv 18\ mod\ 26 \equiv 18\ (S)$$

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

$$(I - I)\ mod\ 26\ \rightarrow (8 - 8)\ mod\ 26 \equiv 0\ mod\ 26 \equiv 0\ (A)$$

$$(N - K)\ mod\ 26\ \rightarrow (13 - 10)\ mod\ 26 \equiv 3\ mod\ 26 \equiv 3\ (D)$$

$$(S - A)\ mod\ 26\ \rightarrow (18 - 0)\ mod\ 26 \equiv 18\ mod\ 26 \equiv 18\ (S)$$

Telah didapatkan *Ciphertext* berupa **"GAPJGSHADS".**

2.1.8.2 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:

$$P_i = (K_i - C_i)\ mod\ n \tag{2.2}$$

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	G 6	A 0	P 15	J 9	G 6	S 18	H 7	A 0	D 3	S 18
KUNCI	S 18	A 0	I 8	N 13	S 18	S 18	A 0	I 8	N 13	S 18

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

$$(S - G)\ mod\ 26\ \rightarrow (18 - 6)\ mod\ 26 \equiv 12\ mod\ 26 \equiv 12\ (M)$$

$$(A - A)\ mod\ 26\ \rightarrow (0 - 0)\ mod\ 26 \equiv 0\ mod\ 26 \equiv 0\ (A)$$

$$(I - P)\ mod\ 26\ \rightarrow (9 - 15)\ mod\ 26 \equiv -7\ mod\ 26 \equiv 19\ (T)$$

$$(N - J)\ mod\ 26\ \rightarrow (13 - 9)\ mod\ 26 \equiv 4\ mod\ 26 \equiv 4\ (E)$$

$$(S - G)\ mod\ 26\ \rightarrow (18 - 6)\ mod\ 26 \equiv 12\ mod\ 26 \equiv 12\ (M)$$

$$(S - S)\ mod\ 26\ \rightarrow (0 - 0)\ mod\ 26 \equiv 0\ mod\ 26 \equiv 0\ (A)$$

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

$$(I - A)\ mod\ 26\ \rightarrow (8 - 0)\ mod\ 26 \equiv 8\ mod\ 26 \equiv 8\ (I)$$

$$(N - D)\ mod\ 26\ \rightarrow (13 - 3)\ mod\ 26 \equiv 10\ mod\ 26 \equiv 10\ (K)$$

$$(S - S)\ mod\ 26\ \rightarrow (0 - 0)\ mod\ 26 \equiv 0\ mod\ 26 \equiv 0\ (A)$$

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 irisan dari semua himpunan faktor pembagi nya jika ada lebih dua karakter yang berulang.
5. Melakukan proses *exhaustive key search* dengan irisan 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.)

2.1.9 Metode Transposisi

Algoritma transposisi atau *cipher* transposisi adalah salah satu algoritma kriptografi yang dilakukan dengan cara menyusun kembali karakter atau merubah posisi dari karakter tersebut, algoritma transposisi sering kali juga disebut dengan permutasi, karena transposisi karakter tersebut sama dengan mem-permutasikan karakter-karakter dengan kunci tertentu dan meletakkan karakter sesuai urutan tertentu. (Setyaningsih Emy, 2015)

Proses kriptografi pada algoritma transposisi diawali dengan mengubah pesan asli atau *Plaintext* menjadi beberapa blok atau grup yang ukurannya harus ditentukan oleh sang pengirim pesan dan harus disampaikan pada penerima pesan, kemudian untuk proses enkripsi pada algoritma ini adalah dengan cara merubah susunan huruf sesuai dengan kunci (π) untuk pesan asli atau *Plaintext* sedangkan dalam proses dekripsi dilakukan dengan cara penerima pesan harus menemukan kunci *invers* (π^{-1}) kemudian sang penerima pesan akan merubah susunan huruf sesuai kunci *invers* (π^{-1}) pada pesan yang telah disandikan (*Ciphertext*). (Sadikin, 2012)

Contoh 2.1.5:

Menentukan kunci untuk algoritma transposisi sebagai berikut:

Tabel 2.4 Tabel Kunci Algoritma Transposisi Grup Simetri

$\boldsymbol{x}$	$\boldsymbol{a_1}$	$\boldsymbol{a_2}$	$\boldsymbol{a_3}$	$\boldsymbol{a_4}$	$\boldsymbol{a_5}$
$\boldsymbol{\pi(x)}$	$\boldsymbol{a_3}$	$\boldsymbol{a_4}$	$\boldsymbol{a_5}$	$\boldsymbol{a_1}$	$\boldsymbol{a_2}$

Kemudian menentukan invers dari kunci yang telah dibuat:

Tabel 2.5 Tabel Kunci Invers Algoritma Transposisi Grup Simetri

$\boldsymbol{x}$	$\boldsymbol{a_1}$	$\boldsymbol{a_2}$	$\boldsymbol{a_3}$	$\boldsymbol{a_4}$	$\boldsymbol{a_5}$
$\boldsymbol{\pi^{-1}(x)}$	$\boldsymbol{a_4}$	$\boldsymbol{a_5}$	$\boldsymbol{a_1}$	$\boldsymbol{a_2}$	$\boldsymbol{a_3}$

Misalkan kita akan mencoba melakukan kriptografi algoritma transposisi pada kalimat berikut ini:

MATEMATIKA UIN MALANG

Sesuai dengan definisi algoritma transposisi kita harus membagi pesan asli (*Plaintext*) menjadi blok-blok yang ukurannya sama dengan kunci yang telah disepakati yaitu lima (5) blok, kemudian untuk kekurangan pada blok diganti dengan % dan untuk spasi diganti dengan #. Berikut ini contoh kriptografi algoritma transposisi:

MATEM	ATIKA	UIN%#	MALAN	G%%%%

Kemudian kita ubah sesuai dengan kunci yang telah disepakati bersama dan kita letakkan kunci di atas setiap blok seperti di bawah ini:

$$\text{Blok 1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ M & A & T & E & M \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \\ T & E & M & M & A \end{pmatrix}$$

= TEMMA

$$\text{Blok 2} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ A & T & I & K & A \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \\ I & K & A & A & T \end{pmatrix}$$

= IKAAT

$$\text{Blok 3} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ U & I & N & \% & \# \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \\ N & \% & \# & U & I \end{pmatrix}$$

= N%#UI

$$\text{Blok 4} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ M & A & L & A & N \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \\ L & A & N & M & A \end{pmatrix}$$

=LANMA

$$\text{Blok 5} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ G & \% & \% & \% & \% \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \\ \% & \% & \% & G & \% \end{pmatrix}$$

=%%%G%

Didapatkan *Ciphertext* kembali yaitu:

TEMMAIKAATN%#UILANMA%%%G%

Proses dekripsi dilakukan dengan cara yang sama dengan proses enkripsi dengan membagi *Ciphertext* menjadi blok-blok yang telah disepakati sesuai dengan kunci yaitu lima (5) blok seperti di bawah ini:

TEMMA	IKAAT	N%#UI	LANMA	%%%G%

Kemudian sesuai dengan definisi dalam algoritma algoritma transposisi maka kita ubah bentuk dengan kunci yang telah dicari invers nya seperti di bawah ini:

$$\text{Blok 1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ T & E & M & M & A \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \\ M & A & T & E & M \end{pmatrix}$$

=MATEM

$$\text{Blok 2} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ I & K & A & A & T \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \\ A & T & I & K & A \end{pmatrix}$$

=ATIKA

$$\text{Blok 3} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ N & \% & \# & U & I \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \\ U & I & N & \% & \# \end{pmatrix}$$

=UIN%#

$$\text{Blok 4} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ L & A & N & M & A \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \\ M & A & L & A & N \end{pmatrix}$$

=MALAN

$$\text{Blok 5} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \% & \% & \% & G & \% \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \\ G & \% & \% & \% & \% \end{pmatrix}$$

=G%%%%

Didapatkan kembali *Plaintext*:

MATEMATIKA UIN MALANG

Algoritma transposisi memiliki banyak jenis seperti transposisi zig-zag, segitiga, spiral dan diagonal.

1. Algoritma transposisi zig-zag yang memasukkan pesan asli (*Plaintext*) ke dalam sebuah tabel dan meletakkan secara zig-zag.

Tabel 2.6 Tabel Algoritma Zig-zag

			E						A						L			
		T		M				K		U				A		A		
	A				A		I				I		M				N	
M						T						N						G

Dari algoritma transposisi zig-zag didapatkan *Ciphertext* berupa “EALTMKUAAAAIIMNMTNG”

2. Algoritma transposisi segitiga yang membentuk pesan asli (*Plaintext*) yang diletakkan dalam sebuah tabel dan membentuk pola segitiga dari atas table .

Tabel 2. 7 Tabel Algoritma Segitiga

				M				
			A	T	E			
		M	A	T	I	K		
	A	U	I	N	M	A	L	
A	N	G	X	X	X	X	X	X

Dari algoritma transposisi segitiga *Ciphertextnya* yaitu "AANMUGAAIXMTTNXEIMXKAXLXX"

3. Algoritma transposisi spiral yang membentuk pesan asli (*Plaintext*) dibaca memutar pada tabel yang telah dibuat.

Tabel 2.8 Tabel Algoritma Spiral

M	A	T	E	M
L	A	N	G	A
A	X	X	X	T
M	X	X	X	I
N	I	U	A	K

Dari algoritma transposisi spiral *Ciphertextnya* yaitu "MLAMNAAXXITNXXUEGXXAMATIK"

4. Algoritma transposisi diagonal yang menyusun pesan asli (*Plaintext*) pada tabel secara diagonal.

Tabel 2.9 Tabel Algoritma Diagonal

M	A	U	L	X
A	T	I	A	X
T	I	N	N	X
E	K	M	G	X
M	A	A	X	X

Dari algoritma transposisi diagonal *Ciphertextnya* yaitu "MAULXATIAXTINNXEKMGXMAAXX"

Algoritma transposisi yang bermacam-macam sangat berguna dalam melakukan variasi algoritma kriptografi dan dapat membingungkan orang yang seharusnya tidak melihat apa isi dari pesan yang dikirimkan.(Ariyus, 2008)

2.1.10 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)

Contoh 2.1.6:

Misalkan kita menggunakan algoritma substitusi *beuafort cipher* dan algoritma transposisi dengan mekanisme kriptografi sebagai berikut:

1. Menentukan *Plaintext*.
2. Menentukan kunci untuk algoritma beaufort cipher.
3. Melakukan proses enkripsi dengan menggunakan algoritma *beuafort cipher* untuk mendapatkan *Ciphertext* pertama.
4. Kemudian melakukan kembali proses enkripsi dengan menggunakan algoritma transposisi untuk mendapatkan *Ciphertext* yang kedua.
5. Dari *Ciphertext* yang kedua akan dilakukan proses dekripsi menggunakan algoritma transposisi dan akan mendapatkan hasil *Ciphertext* yang pertama.
6. *Ciphertext* yang pertama akan dilakukan proses dekripsi menggunakan algoritma *beaufort cipher*.
7. Diperoleh *Plaintext*

Diketahui *Plaintext* yang diberikan berupa “MATEMATIKA” kemudian dienkripsi dengan algoritma *beuafort cipher* dengan persamaan (2.1) serta menggunakan kunci “SAINS” akan didapatkan hasil sebagai berikut:

$$(S - M)Mod\ 26\ \rightarrow (18 - 12)\ Mod\ 26 \equiv 6\ Mod\ 26 \equiv 6\ (G)$$

$$(A - A)Mod\ 26\ \rightarrow (0 - 0)\ Mod\ 26 \equiv 0\ Mod\ 26 \equiv 0\ (A)$$

$$(I - T)Mod\ 26\ \rightarrow (8 - 19)\ Mod\ 26 \equiv -11\ Mod\ 26 \equiv 15\ (P)$$

$$(N - E)Mod\ 26\ \rightarrow (13 - 4)\ Mod\ 26 \equiv 9\ Mod\ 26 \equiv 9\ (J)$$

$$(S - M)Mod\ 26\ \rightarrow (18 - 12)\ Mod\ 26 \equiv 6\ Mod\ 26 \equiv 6\ (G)$$

$$(S - A)Mod\ 26\ \rightarrow (18 - 0)\ Mod\ 26 \equiv 18\ Mod\ 26 \equiv 18\ (S)$$

$$(A - T)Mod\ 26\ \rightarrow (0 - 19)\ Mod\ 26 \equiv -19\ Mod\ 26 \equiv 7\ (H)$$

$$(I - I)Mod\ 26\ \rightarrow (8 - 8)\ Mod\ 26 \equiv 0\ Mod\ 26 \equiv 0\ (A)$$

$$(N - K)Mod\ 26\ \rightarrow (13 - 10)\ Mod\ 26 \equiv 3\ Mod\ 26 \equiv 3\ (D)$$

$$(S - A)Mod\ 26\ \rightarrow (18 - 0)\ Mod\ 26 \equiv 18\ Mod\ 26 \equiv 18\ (S)$$

Diperoleh hasil *Ciphertext;* **"GAPJGSHADS".** Kemudian dilakukan proses enkripsi kembali menggunakan algoritma transposisi grup simetri sebagai berikut:

Tabel 2. 10 Tabel Kunci Enkripsi Transposisi Grup Simetri

$\boldsymbol{x}$	$\boldsymbol{a_1}$	$\boldsymbol{a_2}$	$\boldsymbol{a_3}$	$\boldsymbol{a_4}$	$\boldsymbol{a_5}$
$\boldsymbol{\pi(x)}$	$\boldsymbol{a_4}$	$\boldsymbol{a_5}$	$\boldsymbol{a_1}$	$\boldsymbol{a_2}$	$\boldsymbol{a_3}$

Tabel 2.11 Tabel Kunci Invers Dekripsi Transposisi Grup Simetri

$\boldsymbol{x}$	$\boldsymbol{a_1}$	$\boldsymbol{a_2}$	$\boldsymbol{a_3}$	$\boldsymbol{a_4}$	$\boldsymbol{a_5}$
$\boldsymbol{\pi^{-1}(x)}$	$\boldsymbol{a_3}$	$\boldsymbol{a_4}$	$\boldsymbol{a_5}$	$\boldsymbol{a_1}$	$\boldsymbol{a_2}$

Ciphertext yang telah didapatkan akan dienkripsi kembali dengan menggunakan algoritma transposisi grup simetri dan prosesnya adalah sebagai berikut:

$$\text{Blok } \pi_1 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ G & A & P & J & G \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \\ J & G & G & A & P \end{pmatrix}$$

$$\text{Blok } \pi_2 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ S & H & A & D & S \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \\ D & S & S & H & A \end{pmatrix}$$

Setelah melakukan proses enkripsi dengan menggunakan algoritma transposisi grup simteri didapatkan hasil *Ciphertext* berupa **"JGGAPDSSHA".** Kemudian akan dilakukan proses dekripsi menggunakan algoritma transposisi grup simetri dengan kunci invers yang telah ditentukan.

Blok $\pi_1^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ J & G & G & A & P \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \\ G & A & P & J & G \end{pmatrix}$

Blok $\pi_2^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ D & S & S & H & A \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \\ S & H & A & D & S \end{pmatrix}$

Didapatkan kembali *Ciphertext* yang pertama berupa **"GAPJGSHADS".** Kemudian proses yang terakhir adalah mendekripsi dengan algoritma *Beaufort Cipher* menggunakan persamaan (2.2).

$$(S - G) Mod\ 26 \ \rightarrow (18 - 6)\ Mod\ 26 \equiv 12\ Mod\ 26 \equiv 12\ (M)$$

$$(A - A) Mod\ 26 \ \rightarrow (0 - 0)\ Mod\ 26 \equiv 0\ Mod\ 26 \equiv 0\ (A)$$

$$(I - P) Mod\ 26 \ \rightarrow (9 - 15)\ Mod\ 26 \equiv -7\ Mod\ 26 \equiv 19\ (T)$$

$$(N - J) Mod\ 26 \ \rightarrow (13 - 9)\ Mod\ 26 \equiv 4\ Mod\ 26 \equiv 4\ (E)$$

$$(S - G) Mod\ 26 \ \rightarrow (18 - 6)\ Mod\ 26 \equiv 12\ Mod\ 26 \equiv 12\ (M)$$

$$(S - S) Mod\ 26 \ \rightarrow (0 - 0)\ Mod\ 26 \equiv 0\ Mod\ 26 \equiv 0\ (A)$$

$$(A - H) Mod\ 26 \ \rightarrow (0 - 7)\ Mod\ 26 \equiv -7\ Mod\ 26 \equiv 19\ (T)$$

$$(I - A) Mod\ 26 \ \rightarrow (8 - 0)\ Mod\ 26 \equiv 8\ Mod\ 26 \equiv 8\ (I)$$

$$(N - D) Mod\ 26 \ \rightarrow (13 - 3)\ Mod\ 26 \equiv 10\ Mod\ 26 \equiv 10\ (K)$$

$$(S - S) Mod\ 26\ \rightarrow (0 - 0)\ Mod\ 26 \equiv 0\ Mod\ 26 \equiv 0\ (A)$$

Didapatkan kembali *Plaintext* awal berupa **"MATEMATIKA"**

2.1.11 Modifikasi *Beaufort Cipher* dengan Transposisi Grup Simetri

Penulis dalam skripsi ini menggabungkan dua algoritma (super enkripsi) yaitu algoritma substitusi yaitu *Beaufort Cipher* dan algoritma transposisi yaitu transposisi grup simetri. Pada umumnya super enkripsi melalui proses yang menggunakan algoritma substitusi kemudian menggunakan algoritma transposisi, modifikasi yang digunakan pada skripsi ini adalah dengan super enkripsi namun pada prosesnya akan digunakan algoritma transposisi kemudian menggunakan algoritma substitusi modifikasi *Beaufort Cipher* dengan transposisi grup simetri memiliki proses-proses sebagai berikut:

1. Menentukan *Plaintext*.
2. Menentukan kunci dan kunci invers transposisi grup simetri.
3. Melakukan proses enkripsi dengan transposisi grup simetri dan didapatkan *Ciphertext* pertama.
4. Melakukan proses enkripsi dengan *Beaufort Cipher* menggunakan rumus $C_i \equiv (K_i - P_i)\ mod\ n$ serta kunci yang telah ditentukan dan didapatkan *Ciphertext* kedua.
5. Melakukan proses dekripsi dengan *Beaufort Cipher* menggunakan rumus $P_i \equiv (K_i - C_i)\ mod\ n$ serta kunci yang telah ditentukan dan didapatkan *Ciphertext* pertama.
6. Melakukan proses dekripsi dengan transposisi grup simetri dengan menggunakan kunci invers.
7. Didapatkan *Plaintext*.

Contoh 2.1.7

Diketahui *Plaintext* yang diberikan berupa “MATEMATIKA” kemudian dienkripsi dengan algoritma *transposisi grup simetri* menggunakan kunci π sebagai berikut:

$$\text{Blok } \pi_1 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ M & A & T & E & M \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \\ E & M & M & A & T \end{pmatrix}$$

$$\text{Blok } \pi_2 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ A & T & I & K & A \\ \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 & \alpha_3 \\ K & A & A & T & I \end{pmatrix}$$

Diperoleh *Ciphertext* berupa **“EMMATKAATI”**, Kemudian akan dilakukan proses enkripsi dengan algoritma *Beaufort Cipher* menggunakan persamaan (2.1) dan kunci “SAINS” yang akan dijelaskan sebagai berikut:

$$(S - E) Mod\ 26 \ \rightarrow (18 - 4)\ Mod\ 26 = 14\ Mod\ 26 = 14\ (O)$$

$$(A - M) Mod\ 26 \ \rightarrow (0 - 13)\ Mod\ 26 \equiv -13\ Mod\ 26 \equiv 13\ (M)$$

$$(I - M) Mod\ 26 \ \rightarrow (8 - 13)\ Mod\ 26 \equiv -5\ Mod\ 26 \equiv 21\ (V)$$

$$(N - A) Mod\ 26 \ \rightarrow (13 - 0)\ Mod\ 26 \equiv 13\ Mod\ 26 \equiv 13\ (M)$$

$$(S - T) Mod\ 26 \ \rightarrow (18 - 19)\ Mod\ 26 \equiv -1\ Mod\ 26 \equiv 25\ (Z)$$

$$(S - K) Mod\ 26 \ \rightarrow (18 - 10)\ Mod\ 26 \equiv 8\ Mod\ 26 \equiv 8\ (I)$$

$$(A - A) Mod\ 26 \ \rightarrow (0 - 0)\ Mod\ 26 \equiv 0\ Mod\ 26 \equiv 0\ (A)$$

$$(I - A) Mod\ 26 \ \rightarrow (8 - 0)\ Mod\ 26 \equiv 8\ Mod\ 26 \equiv 8\ (I)$$

$$(N - T) Mod\ 26 \ \rightarrow (13 - 19)\ Mod\ 26 \equiv -6\ Mod\ 26 \equiv 20\ (U)$$

$$(S - I) Mod\ 26 \ \rightarrow (18 - 8)\ Mod\ 26 \equiv 10\ Mod\ 26 \equiv 10\ (K)$$

Diperoleh *Ciphertext* kedua berupa **"OMVMZIAIU"**, kemudian akan dilakukan proses dekripsi dengan algoritma *Beaufort Cipher* menggunakan persamaan (2.2) sebagai berikut:

$$(S-O)Mod\ 26\ \rightarrow (18-14)\ Mod\ 26 \equiv 4\ Mod\ 26 \equiv 4\ (E)$$

$$(A-M)Mod\ 26\ \rightarrow (0-13)\ Mod\ 26 \equiv -13\ Mod\ 26 \equiv 13\ (M)$$

$$(I-V)Mod\ 26\ \rightarrow (8-21)\ Mod\ 26 \equiv -13\ Mod\ 26 \equiv 13\ (M)$$

$$(N-M)Mod\ 26\ \rightarrow (13-13)\ Mod\ 26 \equiv 0\ Mod\ 26 \equiv 0\ (A)$$

$$(S-Z)Mod\ 26\ \rightarrow (18-25)\ Mod\ 26 \equiv -7\ Mod\ 26 \equiv 19\ (T)$$

$$(S-I)Mod\ 26\ \rightarrow (18-8)\ Mod\ 26 \equiv 10\ Mod\ 26 \equiv 10\ (K)$$

$$(A-A)Mod\ 26\ \rightarrow (0-0)\ Mod\ 26 \equiv 0\ Mod\ 26 \equiv 0\ (A)$$

$$(I-I)Mod\ 26\ \rightarrow (8-8)\ Mod\ 26 \equiv 0\ Mod\ 26 \equiv 0\ (A)$$

$$(N-U)Mod\ 26\ \rightarrow (13-20)\ Mod\ 26 \equiv -7\ Mod\ 26 \equiv 19\ (T)$$

$$(S-K)Mod\ 26\ \rightarrow (18-10)\ Mod\ 26 \equiv 8\ Mod\ 26 \equiv 8\ (I)$$

Diperoleh *Ciphertext* pertama berupa **"EMMATKAATI"**, kemudian untuk proses selanjutnya adalah proses dekripsi menggunakan algoritma transposisi grup simetri dengan kunci inver π^{-1} yang akan dijelaskan sebagai berikut:

$$\text{Blok } \pi_1^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ E & M & M & A & T \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \\ M & A & T & E & M \end{pmatrix}$$

$$\text{Blok } \pi_2^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ K & A & A & T & I \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_1 & \alpha_2 \\ A & T & I & K & A \end{pmatrix}$$

didapatkan kembali *Plaintext* pertama berupa **"MATEMATIKA"**.

Modifikasi dengan menggunakan algoritma transposisi terlebih dahulu kemudian menggunakan algoritma substitusi dapat dilakukan karena hanya merubah posisi algoritma mana yang digunakan terlebih dahulu tanpa merubah proses enkripsi dan proses dekripsi yang digunakan sesuai metode super enkripsi.(Sinaga et al., 2018)

2.2 Kajian Integrasi Topik dengan Al-Quran/Hadist

Kriptografi pada dasarnya adalah sebuah cara atau metode yang digunakan untuk mengamankan suatu pesan agar pesan tersebut dapat diterima oleh sang penerima dengan aman, pada agama islam telah diajarkan bahwa seseorang harus amanah dalam menjalani kehidupan terutama dalam berkomunikasi dan bersosialisasi. Berikut adalah beberapa firman Allah SWT yang membahas tentang amanah:

1. Al-Quran surat Al-Ahzab ayat 72:

   ﴿ اِنَّا عَرَضْنَا الْاَمَانَةَ عَلَى السَّمٰوٰتِ وَالْاَرْضِ وَالْجِبَالِ فَاَبَيْنَ اَنْ يَّحْمِلْنَهَا وَاَشْفَقْنَ مِنْهَا وَحَمَلَهَا الْاِنْسَانُۗ اِنَّه كَانَ ظَلُوْمًا جَهُوْلًاۙ ٧٢ ﴾ (الاحزاب/33:72)

   "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 ia (manusia) sangat zalim lagi sangat bodoh." (Agama, 2009)

2. Al-Quran surat Al-Mu'minun ayat 8:

   ﴿ وَالَّذِيْنَ هُمْ لِاَمٰنٰتِهِمْ وَعَهْدِهِمْ رَاعُوْنَ ۙ٨ ﴾ (المؤمنون/23:8)

   "(Sungguh beruntung pula) orang-orang yang memelihara amanat dan janji mereka." (Agama, 2009)

3. Al-Quran surat An-Nisa ayat 58:

﴿ ۞ اِنَّ اللّٰهَ يَأْمُرُكُمْ اَنْ تُؤَدُّوا الْاَمٰنٰتِ اِلٰٓى اَهْلِهَاۙ وَاِذَا حَكَمْتُمْ بَيْنَ النَّاسِ اَنْ تَحْكُمُوْا بِالْعَدْلِ ۗ اِنَّ اللّٰهَ نِعِمَّا يَعِظُكُمْ بِهٖ ۗ اِنَّ اللّٰهَ كَانَ سَمِيْعًاۢ بَصِيْرًا ٥٨ ﴾ (النسآء/4:58)

"Sesungguhnya Allah menyuruh kamu menyampaikan amanah kepada pemiliknya. Apabila kamu menetapkan hukum di antara manusia, hendaklah kamu tetapkan secara adil. Sesungguhnya Allah memberi pengajaran yang paling baik kepadaMu. Sesungguhnya Allah Maha Mendengar lagi Maha Melihat." (Agama, 2009)

4. Al-Quran surat Al-Anfal ayat 27:

﴿ يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَخُوْنُوا اللّٰهَ وَالرَّسُوْلَ وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ ٢٧ ﴾
(الانفال/8:27)

"Wahai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul serta janganlah kamu mengkhianati amanat yang dipercayakan kepadaMu, sedangkan kamu mengetahui". (Agama, 2009)

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. Selain itu menurut Ahmad Musthafa Al-Maraghi amanah adalah segala sesuatu yang harus dijaga dan dan dipelihara agar dapat tersampaikan kepada orang yang berhak menerimanya. (Andika et al., 2020)

Sifat amanah juga dijelaskan dalam kitab Syar¥ Hud-d yang berarti suatu perbuatan manusia yang membantu untuk menjaga sesuatu urusan baik itu yang berkaitan dengan hak Allah ataupun hak manusia, selain dalam kitab tersebut sifat amanah juga dijelaskan dalam kitab Ihya Ulumuddin yang diartikan sebagai

bersihnya diri secara batin dari kefasikan,dosa-dosa besar dan suatu tindakan untuk menghindari dosa kecil.(Dalimunthe, 2018)

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, sedangkan untuk algoritma transposisi nya menggunakan algoritma transposisi grup simetri yang menerapkan materi pada struktur aljabar yaitu grup dan grup simetri.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Penulis pada penelitian ini menggunakan algoritma kualitatif karena pada penelitian ini menerapkan dan melakukan kajian pustaka (*library research*) yang meliputi mengumpulkan data dan berbagai informasi dari berbagai referensi berupa buku, tesis, jurnal, dan karya ilmiah terkait dengan algoritma *Beaufort Cipher* dan algoritma *cipher* transposisi.

3.2 Pra Penelitian

Penelitian ini pada awalnya merujuk pada skripsi milik Riskiyah yang berjudul "Enkripsi dan Dekripsi Pesan menggunakan Grup Simetri untuk Mengamankan Pesan". Pada skripsi tersebut hanya menggunakan grup simetri yang digunakan dalam algoritma pertukaran kunci, dan pada skripsi tersebut memiliki saran untuk menggunakan algoritma-algoritma lain yang dapat digunakan dengan grup simetri, penulis berfikir menggunakan algoritma super enkripsi yang menggabungkan algoritma substitusi dan algoritma transposisi untuk mengamankan suatu pesan, penulis memilih algoritma *Beaufort cipher* dan transposisi grup simetri untuk diangkat sebagai penelitian selanjutnya.

3.3 Tahapan Penelitian

1. Menentukan metode

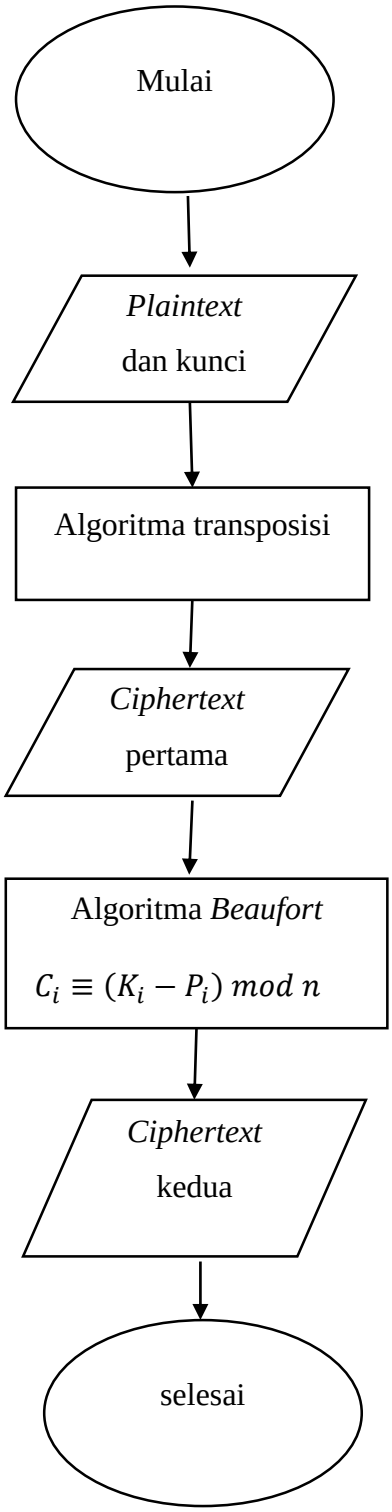
   Penelitian ini penulis angkat karena algoritma *Beaufort* cipher adalah pengembangan dari algoritma lain yaitu *Vigenere Cipher*, dan banyak orang yang tidak mengetahui apa perbedaan dari kedua algoritma tersebut. Kemudian untuk algoritma transposisi grup simetri adalah algoritma transposisi yang menerapkan

materi grup dan grup simetri yang lebih matematis dibandingkan dengan algoritma transposisi yang lain.

2. Algoritma proses enkripsi dan dekripsi:
    a. Menentukan *Plaintext*
    b. Menentukan grup simetri yang digunakan dalam algoritma transposisi grup simetri.
    c. Melakukan proses enkripsi menggunakan algoritma transposisi grup simetri.
    d. Mendapatkan *Ciphertext* pertama.
    e. Melakukan proses enkripsi menggunakan algoritma *Beaufort cipher* dengan persamaan (2.1).
    f. Mendapatkan *Ciphertext* kedua.
    g. Melakukan proses dekripsi menggunakan algoritma *Beaufort cipher* dengan persamaan (2.2).
    h. Mendapatkan *Ciphertext* pertama.
    i. Melakukan proses dekripsi menggunakan algoritma grup simetri.
    j. Mendapatkan *Plaintext*.

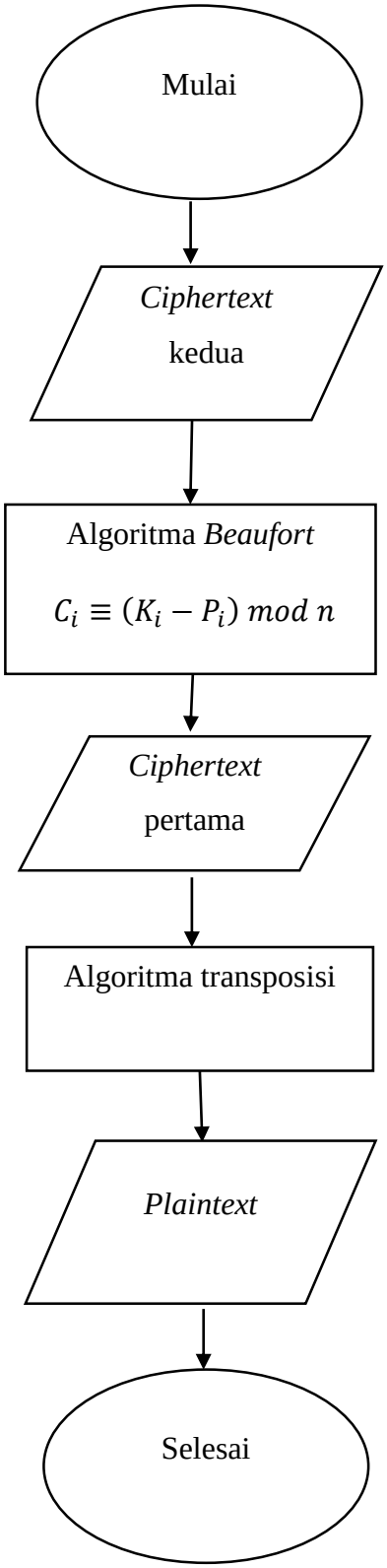
Langkah-langkah di atas adalah prosedur dalam algoritma super enkripsi antra *Beaufort cipher* dengan dan algoritma transposisi grup simetri.

Berikut ini adalah *flowchart* proses enkripsi modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri sebagai berikut:



Gambar 3.1 Flowchart Enkripsi

Berikut ini adalah *flowchart* proses dekripsi modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri sebagai berikut:



Gambar 3.2 Flowchart Dekripsi

BAB IV
PEMBAHASAN

4.1 Proses Enkripsi Modifikasi Algoritma *Beaufort Cipher* dengan Transposisi Grup Simetri

4.1.1 Simulasi Proses Enkripsi *Beaufort Cipher*

Proses enkripsi pada algoritma *Beaufort Cipher* sebelum dimodifikasi akan dijelaskan terlebih dahulu, agar dapat menjadi perbandingan dengan proses enkripsi modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri akan dijelaskan sebagai berikut:

Misalkan penulis akan mengirimkan suatu pesan berupa plaintext **FUN MATH FOR MATHEMATICIANS** dengan kuncinya **ABC**. Langkah pertama adalah mengkonversi huruf alfabet dan kunci ke dalam angka (Lampiran.1). Sehingga,

Tabel 4.1 Tabel Konversi Enkripsi

Plaintext											
F 5	U 20	N 13	M 12	A 0	T 19	H 7	F 5	O 14	R 17	M 12	A 0
Kunci											
A 0	B 1	C 2	A 0	B 1	C 2	A 0	B 1	C 2	A 0	B 1	C 2

Lanjutan *Tabel 4.1 Tabel Konversi*

Plaintext

T 19	H 7	E 4	M 12	A 0	T 19	I 8	C 2	I 8	A 0	N 13	S 18
Kunci											
A 0	B 1	C 2	A 0	B 1	C 2	A 0	B 1	C 2	A 0	B 1	C 2

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

$$(A - F)\ mod\ 26\ \rightarrow (0 - 5)\ mod\ 26 \equiv -5\ mod\ 26 \equiv 21\ (V)$$

$$(B - U)\ mod\ 26\ \rightarrow (1 - 20)\ mod\ 26 \equiv -19\ mod\ 26 \equiv 7\ (H)$$

$$(C - N)\ mod\ 26\ \rightarrow (2 - 13)\ mod\ 26 \equiv -11\ mod\ 26 \equiv 15\ (P)$$

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

$$(B - A)\ mod\ 26\ \rightarrow (1 - 0)\ mod\ 26 \equiv 1\ mod\ 26 \equiv 1\ (B)$$

$$(C - T)\ mod\ 26\ \rightarrow (2 - 19)\ mod\ 26 \equiv -17\ mod\ 26 \equiv 9\ (J)$$

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

$$(B - F)\ mod\ 26\ \rightarrow (1 - 5)\ mod\ 26 \equiv -4\ mod\ 26 \equiv 22\ (W)$$

$$(C - O)\ mod\ 26\ \rightarrow (2 - 14)\ mod\ 26 \equiv -12\ mod\ 26 \equiv 14\ (O)$$

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

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

$$(C - A)\ mod\ 26\ \rightarrow (2 - 0)\ mod\ 26 \equiv 2\ mod\ 26 \equiv 2\ (C)$$

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

$$(B - H)\ mod\ 26\ \rightarrow (1 - 7)\ mod\ 26 \equiv -6\ mod\ 26 \equiv 20\ (U)$$

$$(C - E)\ mod\ 26\ \rightarrow (2 - 4)\ mod\ 26 \equiv -2\ mod\ 26 \equiv 24\ (Y)$$

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

$$(B - A)\ mod\ 26\ \rightarrow (1 - 0)\ mod\ 26 \equiv 1\ mod\ 26 \equiv 1\ (B)$$

$$(C - T)\ mod\ 26\ \rightarrow (2 - 19)\ mod\ 26 \equiv -17\ mod\ 26 \equiv 9\ (J)$$

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

$$(B - C)\ mod\ 26\ \rightarrow (1 - 2)\ mod\ 26 \equiv -1\ mod\ 26 \equiv 25\ (Z)$$

$$(C - I)\ mod\ 26\ \rightarrow (2 - 8)\ mod\ 26 \equiv -6\ mod\ 26 \equiv 20\ (U)$$

$$(A - A)\ mod\ 26\ \rightarrow (0 - 0)\ mod\ 26 \equiv 0\ mod\ 26 \equiv 0\ (A)$$

$$(C - N)\ mod\ 26\ \rightarrow (1 - 13)\ mod\ 26 \equiv -12\ mod\ 26 \equiv 14\ (O)$$

$$(C - S)\ mod\ 26\ \rightarrow (2 - 18)\ mod\ 26 \equiv -16\ mod\ 26 \equiv\ 10\ (K)$$

Dari proses enkripsi di atas didapatkan *Ciphertext* berupa **VHP OBJT WOJ PCHUYOBJSZUAOK**.

4.1.2 Simulasi Proses Enkripsi S_4

Proses enkripsi pada modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri yang dilakukan memiliki algoritma yang berbeda dengan metode super enkripsi pada biasanya, algoritma enkripsi metode algoritma *Beaufort Cipher* dengan transposisi grup simetri akan dijelaskan sebagai berikut:

1. Menentukan *Plaintext* dan kunci π serta kunci invers π^{-1} untuk metode transposisi.
2. Merubah susunan berdasarkan kunci π yang telah ditentukan.
3. Melakukan proses enkripsi dengan algoritma *Beaufort Cipher* menggunakan persamaan $c_i \equiv (K_i - P_i)\ mod\ 28$. Mod 28 dikarenakan

menggunakan 26 karakter alfabet dan tambahan simbol persen “%” dan pagar “#”.

4. Didapatkan *Ciphertext*.

Proses enkripsi dengan modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri menggunakan *Plaintext* yang sama dengan algoritma *Beaufort Cipher* dan simulasinya akan dijelaskan sebagai berikut:

FUN MATH FOR MATHEMATICIANS

Kunci permutasi yang digunakan adalah:

$$\pi = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \end{pmatrix}$$

Plaintext yang telah ditentukan akan dibagi sesuai dengan transposisi grup simetri S_4 sehingga *Plaintext* akan menjadi diuraikan menjadi blok-blok yang isinya ada 4 karakter dan untuk karakter spasi akan digantikan dengan karakter # dan untuk kekurangan karakter dalam blok akan digunakan tambahan karakter % sebagai berikut:

FUN#	MATH	#FOR	#MAT	HEMA
TICI	ANS%			

Kemudian akan dilakukan proses enkripsi dengan satu-persatu blok sebagai berikut:

$$\pi_1 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ F & U & N & \# \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \\ \# & N & F & U \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok pertama yaitu **#NFU**.

$$\pi_2 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ M & A & T & H \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \\ H & T & M & A \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok kedua yaitu **HTMA**.

$$\pi_3 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \# & F & O & R \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \\ R & O & \# & F \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok ketiga yaitu **RO#F**.

$$\pi_4 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \# & M & A & T \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \\ T & A & M & \# \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok keempat yaitu **TAM#**.

$$\pi_5 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ H & E & M & A \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \\ A & M & H & E \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok terakhir yaitu **AMHE**,

$$\pi_6 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ T & I & C & I \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \\ I & C & T & I \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok terakhir yaitu **ICTI**,

$$\pi_7 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ A & N & S & \% \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \\ \% & S & A & N \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok terakhir yaitu **%SAN**, dan jika digabungkan dari blok pertama sampai blok terakhir didapatkan *Ciphertext* pertama berupa #NFUHTMARO#FTA#MAMHEICTI%SAN.

Kemudian akan dilakukan proses enkripsi dengan algoritma *Beaufort Cipher* dan menggunakan kunci yang ditentukan yaitu “ABC”, untuk prosesnya akan dijelaskan sebagai berikut:

PLAINTEXT: #, N, F, U, H, T, M, A, R, O, #, F, T, A, #, M, A, M, H, E, I, C, T, I, %, S, A, N

KUNCI: A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B , C, A, B, C, A

Proses enkripsi pesan dengan menggunakan persamaan (2.1) namun karena dalam perhitungan ini menambah dua karakter berupa “%” dan “#” sehingga merubah persamaan (2.1) menjadi seperti dibawah ini:

$$C_i \equiv (K_i - P_i) mod\ 28 \tag{2.3}$$

Keterangan

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

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

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

Persamaan (2.3) akan digunakan untuk melakukan proses enkripsi yang akan dijelaskan sebagai berikut:

$$(A - \#)\ mod\ 28\ \rightarrow (0 - 26)\ mod\ 28 \equiv -26\ mod\ 28 \equiv 2\ (C)$$

$$(B - N)\ mod\ 28\ \rightarrow (1 - 13)\ mod\ 28 \equiv -12\ mod\ 28 \equiv 16\ (Q)$$

$$(C - F)\ mod\ 28\ \rightarrow (2 - 5)\ mod\ 28 \equiv -3\ mod\ 28 \equiv 25\ (Z)$$

$$(A - U)\ mod\ 28\ \rightarrow (0 - 20)\ mod\ 28 \equiv -20\ mod\ 28 \equiv 8\ (I)$$

$$(B - H)\ mod\ 28\ \rightarrow (1 - 7)\ mod\ 28 \equiv -6\ mod\ 28 \equiv 22\ (W)$$

$$(C - T)\ mod\ 28 \rightarrow (2 - 19)\ mod\ 28 \equiv -17\ mod\ 28\ \equiv 11\ (L)$$

$$(A - M)\ mod\ 28 \rightarrow (0 - 12)\ mod\ 28 \equiv -12\ mod\ 28 \equiv 16\ (Q)$$

$$(B - A)\ mod\ 28 \rightarrow (1 - 0)\ mod\ 28 \equiv 1\ mod\ 28 \equiv 1\ (B)$$

$$(C - R)\ mod\ 28 \rightarrow (2 - 17)\ mod\ 28 \equiv -15\ mod\ 28 \equiv 13\ (N)$$

$$(A - O)\ mod\ 28 \rightarrow (0 - 14)\ mod\ 28 \equiv -14\ mod\ 28 \equiv 14\ (O)$$

$$(B - \#)\ mod\ 28 \rightarrow (1 - 26)\ mod\ 28 \equiv -25\ mod\ 28 \equiv 3\ (D)$$

$$(C - F)\ mod\ 28 \rightarrow (2 - 5)\ mod\ 28 \equiv -3\ mod\ 28 \equiv 25\ (Z)$$

$$(A - T)\ mod\ 28 \rightarrow (0 - 19)\ mod\ 28 \equiv -19\ mod\ 28 \equiv 9\ (J)$$

$$(B - A)\ mod\ 28 \rightarrow (1 - 0)\ mod\ 28 \equiv 1\ mod\ 28 \equiv 1\ (B)$$

$$(C - \#)\ mod\ 28 \rightarrow (2 - 26)\ mod\ 28 \equiv -24\ mod\ 28 \equiv 4\ (E)$$

$$(A - M)\ mod\ 28 \rightarrow (0 - 12)\ mod\ 28 \equiv -12\ mod\ 28 \equiv 16\ (Q)$$

$$(B - A)\ mod\ 28 \rightarrow (1 - 0)\ mod\ 28 \equiv 1\ mod\ 28 \equiv 1\ (B)$$

$$(C - M)\ mod\ 28 \rightarrow (2 - 12)\ mod\ 28 \equiv -10\ mod\ 28 \equiv 18\ (S)$$

$$(A - H)\ mod\ 28 \rightarrow (0 - 7)\ mod\ 28 \equiv -7\ mod\ 28 \equiv 21\ (V)$$

$$(B - E)\ mod\ 28 \rightarrow (1 - 4)\ mod\ 28 \equiv -3\ mod\ 28 \equiv 25\ (Z)$$

$$(C - I)\ mod\ 28 \rightarrow (2 - 8)\ mod\ 28 \equiv -6\ mod\ 28 \equiv 22\ (W)$$

$$(A - C)\ mod\ 28 \rightarrow (0 - 2)\ mod\ 28 \equiv -2\ mod\ 28 \equiv 26\ (\#)$$

$$(B - T)\ mod\ 28 \rightarrow (1 - 19)\ mod\ 28 \equiv -18\ mod\ 28 \equiv 10\ (K)$$

$$(C - I)\ mod\ 28 \rightarrow (2 - 8)\ mod\ 28 \equiv -6\ mod\ 28 \equiv\ 22\ (W)$$

$$(A - \%)\ mod\ 28 \rightarrow (0 - 27)\ mod\ 28 \equiv -27\ mod\ 28 \equiv 1(B)$$

$$(B - S)\ mod\ 28 \rightarrow (1 - 18)\ mod\ 28 \equiv -17\ mod\ 28 \equiv 11\ (L)$$

$$(C - A)\ mod\ 28 \rightarrow (2 - 0)\ mod\ 28 \equiv 2\ mod\ 28 \equiv\ 2\ (C)$$

$$(A - N)\ mod\ 28 \rightarrow (0 - 13)\ mod\ 28 \equiv -13\ mod\ 28 \equiv 15\ (P)$$

Proses enkripsi yang telah dilakukan menghasilkan *Ciphertext* berupa CQZIWLQBNODZJBEQBSVZW#KWBLCP.

4.1.3 Simulasi Proses Enkripsi S_5

Plaintext yang penulis gunakan adalah:

FUN MATH FO MATHEMATICIANS

Kunci permutasi yang digunakan adalah:

$$\pi = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & \alpha_5 \\ \alpha_2 & \alpha_4 & \alpha_1 & a_5 & a_3 \end{pmatrix}$$

Plaintext yang telah ditentukan akan dibagi sesuai dengan transposisi grup simetri S_5 sehingga *Plaintext* akan menjadi diuraikan menjadi blok-blok yang isinya ada 5 karakter dan untuk karakter spasi akan digantikan dengan karakter # dan untuk kekurangan karakter dalam blok akan digunakan tambahan karakter % sebagai berikut:

FUN#M	ATH#F	OR#MA	THEMA
TICIA	NS%%%		

Kemudian akan dilakukan proses enkripsi dengan satu-persatu blok sebagai berikut:

$$\pi_1 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & \alpha_5 \\ \alpha_2 & \alpha_4 & \alpha_1 & a_5 & a_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & \alpha_5 \\ F & U & N & \# & M \\ \alpha_2 & \alpha_4 & \alpha_1 & a_5 & \alpha_3 \\ U & \# & F & M & N \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok pertama yaitu **U#FMN.**

$$\pi_2 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & \alpha_5 \\ \alpha_2 & \alpha_4 & \alpha_1 & a_5 & a_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 \\ A & T & H & \# & F \\ \alpha_2 & \alpha_4 & \alpha_1 & a_5 & \alpha_3 \\ T & \# & A & F & H \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok kedua yaitu **T#AFH**.

$$\pi_3 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & \alpha_5 \\ \alpha_2 & \alpha_4 & \alpha_1 & a_5 & a_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 \\ O & R & \# & M & A \\ \alpha_2 & \alpha_4 & \alpha_1 & a_5 & \alpha_3 \\ R & M & O & A & \# \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok ketiga yaitu **RMOA#.**

$$\pi_4 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & \alpha_5 \\ \alpha_2 & \alpha_4 & \alpha_1 & a_5 & a_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 \\ T & H & E & M & A \\ \alpha_2 & \alpha_4 & \alpha_1 & a_5 & \alpha_3 \\ H & M & T & A & E \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok terakhir yaitu **HMTAE.**

$$\pi_4 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & \alpha_5 \\ \alpha_2 & \alpha_4 & \alpha_1 & a_5 & a_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 \\ T & I & C & I & A \\ \alpha_2 & \alpha_4 & \alpha_1 & a_5 & \alpha_3 \\ I & I & T & A & C \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok terakhir yaitu **IITAC.**

$$\pi_4 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & \alpha_5 \\ \alpha_2 & \alpha_4 & \alpha_1 & a_5 & a_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 \\ N & S & \% & \% & \% \\ \alpha_2 & \alpha_4 & \alpha_1 & a_5 & \alpha_3 \\ S & \% & N & \% & \% \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok terakhir yaitu **S%N%%.** dan jika digabungkan dari blok pertama sampai blok terakhir didapatkan *Ciphertext* pertama berupa U#FMNT#AFHRMOA#HMTAEIITACS%N%%

Kemudian akan dilakukan proses enkripsi dengan algoritma *Beaufort Cipher* dan menggunakan kunci yang telah disepakati bersama, dan untuk prosesnya akan dijelaskan sebagai berikut:

PLAINTEXT: U, #, F, M, N, T, #, A, F, H, R, M, O, A, #, H, M, T, A, E, I, I T, A, C, S, %, N, %, %

KUNCI: A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C

Dilakukan proses enkripsi pesan dengan menggunakan persamaan (2.3) seperti yang dibawah ini:

$$(A - U)\ mod\ 28\ \rightarrow (0 - 20)\ mod\ 28 \equiv -20\ mod\ 28 \equiv 8\ (I)$$

$$(B - \#)\ mod\ 28\ \rightarrow (1 - 26)\ mod\ 28 \equiv -25\ mod\ 28 \equiv 3\ (D)$$

$$(C - F)\ mod\ 28\ \rightarrow (2 - 5)\ mod\ 28 \equiv -3\ mod\ 28 \equiv 25\ (Z)$$

$$(A - M)\ mod\ 28\ \rightarrow (0 - 12)\ mod\ 28 \equiv -12\ mod\ 28 \equiv 16\ (Q)$$

$$(B - N)\ mod\ 28\ \rightarrow (1 - 13)\ mod\ 28 \equiv -12\ mod\ 28 \equiv 16\ (Q)$$

$$(C - T)\ mod\ 28 \rightarrow (2 - 19)\ mod\ 28 \equiv -17\ mod\ 28\ \equiv 11\ (L)$$

$$(A - \#)\ mod\ 28 \rightarrow (0 - 26)\ mod\ 28 \equiv -26\ mod\ 28 \equiv 2\ (C)$$

$$(B - A)\ mod\ 28\ \rightarrow (1 - 0)\ mod\ 28 \equiv 1\ mod\ 28 \equiv 1\ (B)$$

$$(C - F)\ mod\ 28\ \rightarrow (2 - 5)\ mod\ 28 \equiv -3\ mod\ 28 \equiv 25\ (Z)$$

$$(A - H)\ mod\ 28\ \rightarrow (0 - 7)\ mod\ 28 \equiv -7\ mod\ 28 \equiv 21\ (V)$$

$$(B - R)\ mod\ 28\ \rightarrow (1 - 17)\ mod\ 28 \equiv -16\ mod\ 28 \equiv 12\ (M)$$

$$(C - M)\ mod\ 28\ \rightarrow (2 - 12)\ mod\ 28 \equiv -10\ mod\ 28 \equiv 18\ (S)$$

$$(A - O)\ mod\ 28\ \rightarrow (0 - 14)\ mod\ 28 \equiv -14\ mod\ 28 \equiv 14\ (O)$$

$$(B - A)\ mod\ 28\ \rightarrow (1 - 0)\ mod\ 28 \equiv 1\ mod\ 28 \equiv 1\ (B)$$

$$(C - \#)\ mod\ 28\ \rightarrow (2 - 26)\ mod\ 28 \equiv -24\ mod\ 28 \equiv 4\ (E)$$

$$(A - H)\ mod\ 28\ \rightarrow (0 - 7)\ mod\ 28 \equiv -7\ mod\ 28 \equiv 21\ (V)$$

$$(B - M)\ mod\ 28\ \rightarrow (1 - 12)\ mod\ 28 \equiv -11\ mod\ 28 \equiv 17\ (R)$$

$$(C - T)\ mod\ 28\ \rightarrow (2 - 19)\ mod\ 28 \equiv -17\ mod\ 28 \equiv 11\ (L)$$

$$(A - A)\ mod\ 28\ \rightarrow (0 - 0)\ mod\ 28 \equiv 0\ mod\ 28 \equiv 0\ (A)$$

$$(B - E)\ mod\ 28\ \rightarrow (1 - 4)\ mod\ 28 \equiv -3\ mod\ 28 \equiv 25\ (Z)$$

$$(C - I)\ mod\ 28\ \rightarrow (2 - 8)\ mod\ 28 \equiv -6\ mod\ 28 \equiv 22\ (W)$$

$$(A - I)\ mod\ 28\ \rightarrow (0 - 8)\ mod\ 28 \equiv -8\ mod\ 28 \equiv 20\ (U)$$

$$(B - T)\ mod\ 28\ \rightarrow (1 - 19)\ mod\ 28 \equiv -18\ mod\ 28 \equiv 10\ (K)$$

$$(C - A)\ mod\ 28\ \rightarrow (2 - 0)\ mod\ 28 \equiv 2\ mod\ 28 \equiv\ 2\ (C)$$

$$(A - C)\ mod\ 28\ \rightarrow (0 - 2)\ mod\ 28 \equiv -2\ mod\ 28 \equiv 26\ (\#)$$

$$(B - S)\ mod\ 28\ \rightarrow (1 - 18)\ mod\ 28 \equiv -17\ mod\ 28 \equiv 11\ (L)$$

$$(C - \%)\ mod\ 28\ \rightarrow (2 - 27)\ mod\ 28 \equiv -25\ mod\ 28 \equiv\ 3\ (D)$$

$$(A - N)\ mod\ 28\ \rightarrow (0 - 13)\ mod\ 28 \equiv -13\ mod\ 28 \equiv 15\ (P)$$

$$(B - \%)\ mod\ 28\ \rightarrow (1 - 27)\ mod\ 28 \equiv -26\ mod\ 28 \equiv 2\ (C)$$

$$(C - \%)\ mod\ 28\ \rightarrow (2 - 27)\ mod\ 28 \equiv -25\ mod\ 28 \equiv\ 3\ (D)$$

Proses enkripsi yang telah dilakukan menghasilkan *Ciphertext* berupa IDZQQLCBZVMSOBEVRLAZWUKC#LDPCD.

4.1.4 Simulasi Proses Enkripsi S_6

Plaintext yang penulis gunakan adalah:

FUN MATH FOR MATHEMATICIANS

Kunci permutasi yang digunakan adalah:

$$\pi = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ \alpha_3 & \alpha_5 & \alpha_4 & a_6 & a_1 & a_2 \end{pmatrix}$$

Plaintext yang telah ditentukan akan dibagi sesuai dengan transposisi grup simetri S_6 sehingga *Plaintext* akan menjadi diuraikan menjadi blok-blok yang isinya ada 6 karakter dan untuk karakter spasi akan digantikan dengan karakter # dan untuk kekurangan karakter dalam blok akan digunakan tambahan karakter % sebagai berikut:

FUN#MA	TH#FOR	#MATHE	MATICI
ANS%%%			

Kemudian akan dilakukan proses enkripsi dengan satu-persatu blok sebagai berikut:

$$\pi_1 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ \alpha_3 & \alpha_5 & \alpha_4 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ F & U & N & \# & M & A \\ \alpha_3 & \alpha_5 & \alpha_4 & a_6 & a_1 & \alpha_2 \\ N & M & \# & A & F & U \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok pertama yaitu **NM#AFU.**

$$\pi_2 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ \alpha_3 & \alpha_5 & \alpha_4 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ T & H & \# & F & O & R \\ \alpha_3 & \alpha_5 & \alpha_4 & a_6 & a_1 & \alpha_2 \\ \# & O & F & R & T & H \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok kedua yaitu **#OFRTH**.

$$\pi_3 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ \alpha_3 & \alpha_5 & \alpha_4 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ \# & M & A & T & H & E \\ \alpha_3 & \alpha_5 & \alpha_4 & a_6 & a_1 & \alpha_2 \\ A & H & T & E & \# & M \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok terakhir yaitu **AHTE#M.**

$$\pi_4 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ \alpha_3 & \alpha_5 & \alpha_4 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ M & A & T & I & C & I \\ \alpha_3 & \alpha_5 & \alpha_4 & a_6 & a_1 & \alpha_2 \\ T & C & I & I & M & A \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok terakhir yaitu **TCIIMA.**

$$\pi_5 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ \alpha_3 & \alpha_5 & \alpha_4 & a_6 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ A & N & S & \% & \% & \% \\ \alpha_3 & \alpha_5 & \alpha_4 & a_6 & a_1 & \alpha_2 \\ S & \% & \% & \% & A & N \end{pmatrix}$$

Didapatkan hasil *Ciphertext* dari blok terakhir yaitu **S%%%AN.** Dan jika digabungkan dari blok pertama sampai blok terakhir didapatkan *Ciphertext* pertama berupa NM#AFU#OFRTHAHTE#MTCIIMAS%%%AN

Kemudian akan dilakukan proses enkripsi dengan algoritma *Beaufort Cipher* dan menggunakan kunci yang ditentukan, dan prosesnya akan dijelaskan sebagai berikut:

PLAINTEXT: N, M, #, A, F, U, #, O, F, R, T, H, A, H, T, E, #, M, T, C, I, I, M, A, S, %, %, %, A, N

KUNCI: A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C

Dilakukan proses enkripsi pesan dengan menggunakan rumus persamaan (2.3) seperti yang dibawah ini:

$$(A - N)\ mod\ 28\ \rightarrow (0 - 13)\ mod\ 28 \equiv -13\ mod\ 28 \equiv 15\ (P)$$

$$(B - M)\ mod\ 28\ \rightarrow (1 - 12)\ mod\ 28 \equiv -11\ mod\ 28 \equiv 17\ (R)$$

$$(C - \#)\ mod\ 28\ \rightarrow (2 - 26)\ mod\ 28 \equiv -24\ mod\ 28 \equiv 4\ (E)$$

$$(A - A)\ mod\ 28\ \rightarrow (0 - 0)\ mod\ 28 \equiv 0\ mod\ 28 \equiv 0\ (A)$$

$$(B - F)\ mod\ 28\ \rightarrow (1 - 5)\ mod\ 28 \equiv -4\ mod\ 28 \equiv 24\ (Y)$$

$$(C - U)\ mod\ 28 \rightarrow (2 - 20)\ mod\ 28 \equiv -18\ mod\ 28\ \equiv 10\ (K)$$

$$(A - \#)\ mod\ 28 \rightarrow (0 - 26)\ mod\ 28 \equiv -26\ mod\ 28 \equiv 2\ (C)$$

$$(B - O)\ mod\ 28\ \rightarrow (1 - 14)\ mod\ 28 \equiv -13\ mod\ 28 \equiv 15\ (P)$$

$$(C - F)\ mod\ 28\ \rightarrow (2 - 5)\ mod\ 28 \equiv -3\ mod\ 28 \equiv 25\ (Z)$$

$$(A - R)\ mod\ 28\ \rightarrow (0 - 17)\ mod\ 28 \equiv -17\ mod\ 28 \equiv 11\ (L)$$

$$(B - T)\ mod\ 28\ \rightarrow (1 - 19)\ mod\ 28 \equiv -18\ mod\ 28 \equiv 10\ (K)$$

$$(C - H)\ mod\ 28\ \rightarrow (2 - 7)\ mod\ 28 \equiv -5\ mod\ 28 \equiv 23\ (X)$$

$$(A - A)\ mod\ 28\ \rightarrow (0 - 0)\ mod\ 28 \equiv 0\ mod\ 28 \equiv 0\ (A)$$

$$(B - H)\ mod\ 28\ \rightarrow (1 - 7)\ mod\ 28 \equiv -6\ mod\ 28 \equiv 22\ (W)$$

$$(C - T)\ mod\ 28\ \rightarrow (2 - 19)\ mod\ 28 \equiv -17\ mod\ 28 \equiv 11\ (L)$$

$$(A - E)\ mod\ 28\ \rightarrow (0 - 4)\ mod\ 28 \equiv -4\ mod\ 28 \equiv 24\ (Y)$$

$$(B - \#)\ mod\ 28\ \rightarrow (1 - 26)\ mod\ 28 \equiv -25\ mod\ 28 \equiv 3\ (D)$$

$$(C - M)\ mod\ 28\ \rightarrow (2 - 12)\ mod\ 28 \equiv -10\ mod\ 28 \equiv 18\ (S)$$

$$(A - T)\ mod\ 28\ \rightarrow (0 - 19)\ mod\ 28 \equiv -19\ mod\ 28 \equiv 9\ (J)$$

$$(B - C)\ mod\ 28\ \rightarrow (1 - 2)\ mod\ 28 \equiv -1\ mod\ 28 \equiv 27\ (\%)$$

$$(C - I)\ mod\ 28\ \rightarrow (2 - 8)\ mod\ 28 \equiv -6\ mod\ 28 \equiv 22\ (W)$$

$$(A - I)\ mod\ 28\ \rightarrow (0 - 8)\ mod\ 28 \equiv -8\ mod\ 28 \equiv 20\ (U)$$

$$(B - M)\ mod\ 28\ \rightarrow (1 - 12)\ mod\ 28 \equiv -11\ mod\ 28 \equiv 17\ (R)$$

$$(C - A)\ mod\ 28\ \rightarrow (2 - 0)\ mod\ 28 \equiv 2\ mod\ 28 \equiv\ 2\ (C)$$

$$(A - S)\ mod\ 28\ \rightarrow (0 - 18)\ mod\ 28 \equiv -18\ mod\ 28 \equiv 10\ (K)$$

$$(B - \%)\ mod\ 28\ \rightarrow (1 - 27)\ mod\ 28 \equiv -26\ mod\ 28 \equiv 2\ (C)$$

$$(C - \%)\ mod\ 28\ \rightarrow (2 - 27)\ mod\ 28 \equiv -25\ mod\ 28 \equiv\ 3\ (D)$$

$$(A - \%)\ mod\ 28\ \rightarrow (0 - 27)\ mod\ 28 \equiv -27\ mod\ 28 \equiv 1\ (B)$$

$$(B - A)\ mod\ 28\ \rightarrow (1 - 0)\ mod\ 28 \equiv 1\ mod\ 28 \equiv 1\ (B)$$

$$(C - N)\ mod\ 28\ \rightarrow (2 - 13)\ mod\ 28 \equiv -11\ mod\ 28 \equiv\ 17\ (R)$$

Proses enkripsi yang telah dilakukan menghasilkan *Ciphertext* berupa PREAYKCPZLKXAWLYDSJ%WURCKCDBBR.

4.2 Proses Dekripsi Modifikasi Algoritma *Beaufort Cipher* dengan Transposisi Grup Simetri

Proses dekripsi pada modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri yang dilakukan memiliki algoritma yang berbeda dengan metode super enkripsi pada biasanya, algoritma dekripsi metode algoritma *Beaufort Cipher* dengan transposisi grup simetri akan dijelaskan sebagai berikut:

1. Menggunakan *Ciphertext* dari proses enkripsi dan melakukan proses dekripsi dengan algoritma *Beaufort Cipher* menggunakan persamaan $P_i \equiv (K_i - C_i)\ mod\ 28$, Mod 28 dikarenakan menggunakan 26 karakter alfabet dan tambahan simbol persen "%" dan pagar "#".
2. Merubah susunan *Ciphertext* berdasarkan kunci π^{-1} yang telah ditentukan.
3. Didapatkan *Plaintext*.

4.2.1 Simulasi Proses Dekripsi *Beaufort Cipher*

Proses dekripsi pada algoritma *Beaufort Cipher* sebelum dimodifikasi akan dijelaskan terlebih dahulu, agar dapat menjadi perbandingan dengan proses enkripsi modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri akan dijelaskan sebagai berikut:

Tabel 4.2 Tabel Konversi Dekripsi

Ciphertext											
V	H	P	O	B	J	T	W	O	J	P	C
21	7	15	14	1	9	19	22	14	9	15	2
Kunci											
A	B	C	A	B	C	A	B	C	A	B	C
0	1	2	0	1	2	0	1	2	0	1	2

Lanjutan Tabel 4.5 Tabel Konversi Dekripsi

Ciphertext											
H 7	U 20	Y 24	O 14	B 1	J 9	S 18	Z 25	U 20	A 0	O 14	K 10
Kunci											
A 0	B 1	C 2	A 0	B 1	C 2	A 0	B 1	C 2	A 0	B 1	C 2

$$(A - V)\ mod\ 26\ \rightarrow (0 - 21)\ mod\ 26 \equiv -21\ mod\ 26 \equiv 5\ (F)$$

$$(B - H)\ mod\ 26\ \rightarrow (1 - 7)\ mod\ 26 \equiv -6\ mod\ 26 \equiv 20\ (U)$$

$$(C - P)\ mod\ 26\ \rightarrow (2 - 15)\ mod\ 26 \equiv -13\ mod\ 26 \equiv 13\ (N)$$

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

$$(B - B)\ mod\ 26\ \rightarrow (1 - 1)\ mod\ 26 \equiv 0\ mod\ 26 \equiv 0\ (A)$$

$$(C - J)\ mod\ 26\ \rightarrow (2 - 9)\ mod\ 26 \equiv -7\ mod\ 26 \equiv 19\ (T)$$

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

$$(B - W)\ mod\ 26\ \rightarrow (1 - 22)\ mod\ 26 \equiv -21\ mod\ 26 \equiv 5\ (F)$$

$$(C - O)\ mod\ 26\ \rightarrow (2 - 14)\ mod\ 26 \equiv -12\ mod\ 26 \equiv 14\ (O)$$

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

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

$$(C - C)\ mod\ 26\ \rightarrow (2 - 2)\ mod\ 26 \equiv 0\ mod\ 26 \equiv 0\ (A)$$

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

$$(B - U)\ mod\ 26\ \rightarrow (1 - 20)\ mod\ 26 \equiv -19\ mod\ 26 \equiv 7\ (H)$$

$$(C - Y)\ mod\ 26\ \rightarrow (2 - 24)\ mod\ 26 \equiv -22\ mod\ 26 \equiv 4\ (E)$$

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

$$(B - B)\ mod\ 26\ \rightarrow (1 - 1)\ mod\ 26 \equiv 0\ mod\ 26 \equiv 0\ (A)$$

$$(C - J)\ mod\ 26\ \rightarrow (2 - 9)\ mod\ 26 \equiv -7\ mod\ 26 \equiv 19\ (T)$$

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

$$(B - Z)\ mod\ 26\ \rightarrow (1 - 25)\ mod\ 26 \equiv -24\ mod\ 26 \equiv 2\ (C)$$

$$(C - U)\ mod\ 26\ \rightarrow (2 - 20)\ mod\ 26 \equiv -18\ mod\ 26 \equiv 8\ (I)$$

$$(A - A)\ mod\ 26\ \rightarrow (0 - 0)\ mod\ 26 \equiv 0\ mod\ 26 \equiv 0\ (A)$$

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

$$(C - K)\ mod\ 26\ \rightarrow (2 - 10)\ mod\ 26 \equiv -8\ mod\ 26 \equiv\ 18\ (S)$$

Didapatkan plaintext kembali berupa **FUN MATH FOR MATHEMATICIAN.**

4.2.2 Simulasi Proses Dekripsi S_4

CIPHERTEXT: C, Q, Z, I, W, L, Q, B, N, O, D, Z, J, B, E, Q, B, S, V, Z, W, #, K, W, B, L, C, P

KUNCI: A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A

Dilakukan proses dekripsi pesan dengan menggunakan persamaan (2.2) namun karena proses dekripsi juga juga menggunakan karakater “%” dan “#” maka persamaannya akan menjadi seperti berikut:

$$P_i \equiv (K_i - C_i)\ mod\ 28 \qquad (2.4)$$

Keterangan

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

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

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

Proses dekripsi akan menggunakan persamaan (2.4), dan prosesnya akan dijelaskan seperti dibawah ini:

$$(A - C)\ mod\ 28\ \rightarrow (0 - 2)\ mod\ 28 \equiv -2\ mod\ 28 \equiv 26\ (\#)$$

$$(B - Q)\ mod\ 28\ \rightarrow (1 - 16)\ mod\ 28 \equiv -15\ mod\ 28 \equiv 13\ (N)$$

$$(C - Z)\ mod\ 28\ \rightarrow (2 - 25)\ mod\ 28 \equiv -23\ mod\ 28 \equiv 5\ (F)$$

$$(A - I)\ mod\ 28\ \rightarrow (0 - 8)\ mod\ 28 \equiv -8\ mod\ 28 \equiv 20\ (U)$$

$$(B - W)\ mod\ 28\ \rightarrow (1 - 22)\ mod\ 28 \equiv -21\ mod\ 28 \equiv 7\ (H)$$

$$(C - L)\ mod\ 28 \rightarrow (2 - 11)\ mod\ 28 \equiv -9\ mod\ 28\ \equiv 19\ (T)$$

$$(A - Q)\ mod\ 28 \rightarrow (0 - 16)\ mod\ 28 \equiv -16\ mod\ 28 \equiv 12\ (M)$$

$$(B - B)\ mod\ 28\ \rightarrow (1 - 1)\ mod\ 28 \equiv 0\ mod\ 28 \equiv\ (A)$$

$$(C - N)\ mod\ 28\ \rightarrow (2 - 13)\ mod\ 28 \equiv -11\ mod\ 28 \equiv 17\ (R)$$

$$(A - O)\ mod\ 28\ \rightarrow (0 - 14)\ mod\ 28 \equiv -14\ mod\ 28 \equiv 14\ (O)$$

$$(B - D)\ mod\ 28\ \rightarrow (1 - 3)\ mod\ 28 \equiv -2\ mod\ 28 \equiv 26\ (\#)$$

$$(C - Z)\ mod\ 28\ \rightarrow (2 - 25)\ mod\ 28 \equiv -23\ mod\ 28 \equiv 5\ (F)$$

$$(A - J)\ mod\ 28\ \rightarrow (0 - 9)\ mod\ 28 \equiv -9\ mod\ 28 \equiv 19\ (T)$$

$$(B - B)\ mod\ 28\ \rightarrow (1 - 1)\ mod\ 28 \equiv 0\ mod\ 28 \equiv 0\ (A)$$

$$(C - E)\ mod\ 28\ \rightarrow (2 - 4)\ mod\ 28 \equiv -2\ mod\ 28 \equiv 26\ (\#)$$

$$(A - Q)\ mod\ 28\ \rightarrow (0 - 16)\ mod\ 28 \equiv -16\ mod\ 28 \equiv 12\ (M)$$

$$(B - B)\ mod\ 28\ \rightarrow (1 - 1)\ mod\ 28 \equiv 0\ mod\ 28 \equiv 0\ (A)$$

$$(C - S)\ mod\ 28\ \rightarrow (2 - 18)\ mod\ 28 \equiv -16\ mod\ 28 \equiv 12\ (M)$$

$$(A - V)\ mod\ 28\ \rightarrow (0 - 21)\ mod\ 28 \equiv -21\ mod\ 28 \equiv 7\ (H)$$

$$(B - Z)\ mod\ 28\ \rightarrow (1 - 25)\ mod\ 28 \equiv -24\ mod\ 28 \equiv 4\ (E)$$

$$(C - W)\ mod\ 28\ \rightarrow (2 - 22)\ mod\ 28 \equiv -20\ mod\ 28 \equiv 8\ (I)$$

$$(A - \#)\ mod\ 28\ \rightarrow (0 - 26)\ mod\ 28 \equiv -26\ mod\ 28 \equiv 2\ (C)$$

$$(B-K)\ mod\ 28\ \rightarrow (1-10)\ mod\ 28 \equiv -9\ mod\ 28 \equiv 19\ (T)$$

$$(C-W)\ mod\ 28\ \rightarrow (2-22)\ mod\ 28 \equiv -20\ mod\ 28 \equiv\ 8\ (I)$$

$$(A-B)\ mod\ 28\ \rightarrow (0-1)\ mod\ 28 \equiv -1\ mod\ 28 \equiv 27(\%)$$

$$(B-L)\ mod\ 28\ \rightarrow (1-11)\ mod\ 28 \equiv -10\ mod\ 28 \equiv 18\ (S)$$

$$(C-C)\ mod\ 28\ \rightarrow (2-2)\ mod\ 28 \equiv 0\ mod\ 28 \equiv\ 0\ (A)$$

$$(A-P)\ mod\ 28\ \rightarrow (0-15)\ mod\ 28 \equiv -15\ mod\ 28 \equiv 13\ (N)$$

Proses dekripsi yang telah dilakukan menghasilkan *Ciphertext* berupa #NFUHTMARO#FTA#MAMHEICTI%SAN. Kemudian akan dilakukan proses dekripsi dengan algoritma transposisi grup simetri dengan merubah *Ciphertext* yang telah didapatkan menjadi blok-blok sesuai dengan apa yang disepakati oleh pengirim pesan dan penerima pesan yaitu transposisi grup simetri S_4 yang akan dijelaskan sebagai berikut:

#NFU	HTMA	RO#F	TA#M	AMHE
ICTI	%SAN			

Kunci *invers* permutasi yang digunakan adalah:

$$\pi_1^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \# & N & F & U \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \\ F & U & N & \# \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok pertama yaitu **FUN#**.

$$\pi_2^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ H & T & M & A \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \\ M & A & T & H \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok kedua yaitu **MATH**.

$$\pi_3^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ R & O & \# & F \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \\ \# & F & O & R \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok ketiga yaitu **#FOR**.

$$\pi_4^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ T & A & \# & M \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \\ \# & M & A & T \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok keempat yaitu **#MAT**.

$$\pi_5^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ A & M & H & E \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \\ H & E & M & A \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok terakhir yaitu **HEMA**.

$$\pi_5^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ I & C & T & I \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \\ T & I & C & I \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok terakhir yaitu **TICI**.

$$\pi_5^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \% & S & A & N \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \\ A & N & S & \% \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok terakhir yaitu **ANS%**. Dan jika digabungkan dari blok pertama sampai blok terakhir didapatkan *Plaintext* awal berupa FUN MATH FOR MATEMATCIANS".

4.2.3 Simulasi Proses Dekripsi S_5

CIPHERTEXT: I, D, Z, Q, Q, L, C, B, Z, V, M, S, O, B, E, V, R, L, A, Z, W, U, K, C, #, L, D, P, C, D

KUNCI: A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, B, C, A, B, C, A, B, C, A, B, C

Dilakukan proses dekripsi pesan dengan menggunakan persamaan (2.4) yang dibawah ini:

$$(A - I)\ mod\ 28\ \rightarrow (0 - 8)\ mod\ 28 \equiv -8\ mod\ 28 \equiv 20\ (U)$$

$$(B - D)\ mod\ 28\ \rightarrow (1 - 3)\ mod\ 28 \equiv -2\ mod\ 28 \equiv 26\ (\#)$$

$$(C - Z)\ mod\ 28\ \rightarrow (2 - 25)\ mod\ 28 \equiv -23\ mod\ 28 \equiv 5\ (F)$$

$$(A - Q)\ mod\ 28\ \rightarrow (0 - 16)\ mod\ 28 \equiv -16\ mod\ 28 \equiv 12\ (M)$$

$$(B - Q)\ mod\ 28\ \rightarrow (1 - 16)\ mod\ 28 \equiv -15\ mod\ 28 \equiv 13\ (N)$$

$$(C - L)\ mod\ 28 \rightarrow (2 - 11)\ mod\ 28 \equiv -9\ mod\ 28\ \equiv 19\ (T)$$

$$(A - C)\ mod\ 28 \rightarrow (0 - 2)\ mod\ 28 \equiv -2\ mod\ 28 \equiv 26\ (\#)$$

$$(B - B)\ mod\ 28\ \rightarrow (1 - 1)\ mod\ 28 \equiv 0\ mod\ 28 \equiv 0\ (A)$$

$$(C - Z)\ mod\ 28\ \rightarrow (2 - 25)\ mod\ 28 \equiv -23\ mod\ 28 \equiv 5\ (F)$$

$$(A - V)\ mod\ 28\ \rightarrow (0 - 21)\ mod\ 28 \equiv -21\ mod\ 28 \equiv 7\ (H)$$

$$(B - M)\ mod\ 28\ \rightarrow (1 - 12)\ mod\ 28 \equiv -11\ mod\ 28 \equiv 17\ (R)$$

$$(C - S)\ mod\ 28\ \rightarrow (2 - 18)\ mod\ 28 \equiv -16\ mod\ 28 \equiv 12\ (M)$$

$$(A - O)\ mod\ 28\ \rightarrow (0 - 14)\ mod\ 28 \equiv -14\ mod\ 28 \equiv 14\ (O)$$

$$(B - B)\ mod\ 28\ \rightarrow (1 - 1)\ mod\ 28 \equiv 0\ mod\ 28 \equiv 0\ (A)$$

$$(C - E)\ mod\ 28\ \rightarrow (2 - 4)\ mod\ 28 \equiv -2\ mod\ 28 \equiv 26\ (\#)$$

$$(A - V)\ mod\ 28\ \rightarrow (0 - 21)\ mod\ 28 \equiv -21\ mod\ 28 \equiv 7\ (H)$$

$$(B - R)\ mod\ 28\ \rightarrow (1 - 17)\ mod\ 28 \equiv -16\ mod\ 28 \equiv 12\ (M)$$

$$(C - L)\ mod\ 28\ \rightarrow (2 - 11)\ mod\ 28 \equiv -9\ mod\ 28 \equiv 19\ (T)$$

$$(A - A)\ mod\ 28\ \rightarrow (0 - 0)\ mod\ 28 \equiv 0\ mod\ 28 \equiv 0\ (A)$$

$$(B - Z)\ mod\ 28\ \rightarrow (1 - 25)\ mod\ 28 \equiv -24\ mod\ 28 \equiv 4\ (E)$$

$$(C - W)\ mod\ 28\ \rightarrow (2 - 22)\ mod\ 28 \equiv -20\ mod\ 28 \equiv 8\ (I)$$

$$(A - U)\ mod\ 28\ \rightarrow (0 - 20)\ mod\ 28 \equiv -20\ mod\ 28 \equiv 8\ (I)$$

$$(B-K)\ mod\ 28\ \rightarrow (1-10)\ mod\ 28 \equiv -9\ mod\ 28 \equiv 19\ (T)$$

$$(C-C)\ mod\ 28\ \rightarrow (2-2)\ mod\ 28 \equiv 0\ mod\ 28 \equiv\ 0\ (A)$$

$$(A-\#)\ mod\ 28\ \rightarrow (0-26)\ mod\ 28 \equiv -26\ mod\ 28 \equiv 2\ (C)$$

$$(B-L)\ mod\ 28\ \rightarrow (1-11)\ mod\ 28 \equiv -10\ mod\ 28 \equiv 18\ (S)$$

$$(C-D)\ mod\ 28\ \rightarrow (2-3)\ mod\ 28 \equiv -1\ mod\ 28 \equiv\ 27\ (\%)$$

$$(A-P)\ mod\ 28\ \rightarrow (0-15)\ mod\ 28 \equiv -15\ mod\ 28 \equiv 13\ (N)$$

$$(B-C)\ mod\ 28\ \rightarrow (1-2)\ mod\ 28 \equiv -1\ mod\ 28 \equiv 27\ (\%)$$

$$(C-D)\ mod\ 28\ \rightarrow (2-3)\ mod\ 28 \equiv -1\ mod\ 28 \equiv\ 27\ (\%)$$

Proses dekripsi yang telah dilakukan menghasilkan *Ciphertext* berupa U#FMNT#AFHRMOA#HMTAEIITACS%N%%. Kemudian akan dilakukan proses dekripsi dengan algoritma transposisi grup simetri dengan merubah *Ciphertext* yang telah didapatkan menjadi blok-blok sesuai dengan apa yang disepakati oleh pengirim pesan dan penerima pesan yaitu transposisi grup simetri S_5 yang akan dijelaskan sebagai berikut:

U#FMN	T#AFH	RMOA#	HMTAE
IITAC	S%N%%		

Kunci *invers* permutasi yang digunakan adalah:

$$\pi_1^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_3 & \alpha_1 & \alpha_5 & \alpha_2 & \alpha_4 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ U & \# & F & M & N \\ \alpha_3 & \alpha_1 & \alpha_5 & \alpha_2 & \alpha_4 \\ F & U & N & \# & M \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok pertama yaitu **FUN#M.**

$$\pi_2^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & \alpha_5 \\ \alpha_3 & \alpha_1 & \alpha_5 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 \\ T & \# & A & F & H \\ \alpha_3 & \alpha_1 & \alpha_5 & a_2 & \alpha_4 \\ A & T & H & \# & F \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok kedua yaitu **ATH#F.**

$$\pi_3^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & \alpha_5 \\ \alpha_3 & \alpha_1 & \alpha_5 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 \\ R & M & O & A & \# \\ \alpha_3 & \alpha_1 & \alpha_5 & a_2 & \alpha_4 \\ O & R & \# & M & A \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok ketiga yaitu **OR#MA.**

$$\pi_4^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & \alpha_5 \\ \alpha_3 & \alpha_1 & \alpha_5 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 \\ H & M & T & A & E \\ \alpha_3 & \alpha_1 & \alpha_5 & a_2 & \alpha_4 \\ T & H & E & M & A \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok keempat yaitu **THEMA**.

$$\pi_5^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & \alpha_5 \\ \alpha_3 & \alpha_1 & \alpha_5 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 \\ I & I & T & A & C \\ \alpha_3 & \alpha_1 & \alpha_5 & a_2 & \alpha_4 \\ T & I & C & I & A \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok kelima yaitu **TICIA.**

$$\pi_6^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & \alpha_5 \\ \alpha_3 & \alpha_1 & \alpha_5 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 \\ S & \% & N & \% & \% \\ \alpha_3 & \alpha_1 & \alpha_5 & a_2 & \alpha_4 \\ N & S & \% & \% & \% \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok terakhir yaitu NS%%%. Dan jika digabungkan dari blok pertama sampai blok terakhir didapatkan *Plaintext* awal berupa FUN MATH FOR MATHEMATICIANS.

4.2.4 Simulasi Proses Dekripsi S_6

CIPHERTEXT: P, R, E, A, Y, K, C, P, Z, L, K, X, A, W, L, Y, D, S, J, %, W, U, R, C, K, C, D, B, B, R.

KUNCI: A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C, A, B, C

Dilakukan proses dekripsi pesan dengan menggunakan persamaan (2.4) seperti yang dibawah ini:

$$(A - P)\ mod\ 28\ \rightarrow (0 - 15)\ mod\ 28 \equiv -15\ mod\ 28 \equiv 13\ (N)$$

$$(B - R)\ mod\ 28\ \rightarrow (1 - 17)\ mod\ 28 \equiv -16\ mod\ 28 \equiv 12\ (M)$$

$$(C - E)\ mod\ 28\ \rightarrow (2 - 4)\ mod\ 28 \equiv -2\ mod\ 28 \equiv 26\ (\#)$$

$$(A - A)\ mod\ 28\ \rightarrow (0 - 0)\ mod\ 28 \equiv 0\ mod\ 28 \equiv 0\ (A)$$

$$(B - Y)\ mod\ 28\ \rightarrow (1 - 24)\ mod\ 28 \equiv -23\ mod\ 28 \equiv 5\ (F)$$

$$(C - K)\ mod\ 28 \rightarrow (2 - 10)\ mod\ 28 \equiv -8\ mod\ 28\ \equiv 20\ (U)$$

$$(A - C)\ mod\ 28 \rightarrow (0 - 2)\ mod\ 28 \equiv -2\ mod\ 28 \equiv 26\ (\#)$$

$$(B - P)\ mod\ 28\ \rightarrow (1 - 15)\ mod\ 28 \equiv -14\ mod\ 28 \equiv 14\ (O)$$

$$(C - Z)\ mod\ 28\ \rightarrow (2 - 25)\ mod\ 28 \equiv -23\ mod\ 28 \equiv 5\ (F)$$

$$(A - L)\ mod\ 28\ \rightarrow (0 - 11)\ mod\ 28 \equiv -11\ mod\ 28 \equiv 17\ (R)$$

$$(B - K)\ mod\ 28\ \rightarrow (1 - 10)\ mod\ 28 \equiv -9\ mod\ 28 \equiv 19\ (T)$$

$$(C - X)\ mod\ 28\ \rightarrow (2 - 23)\ mod\ 28 \equiv -21\ mod\ 28 \equiv 7(H)$$

$$(A - A)\ mod\ 28\ \rightarrow (0 - 0)\ mod\ 28 \equiv 0\ mod\ 28 \equiv 0\ (A)$$

$$(B - W)\ mod\ 28\ \rightarrow (1 - 22)\ mod\ 28 \equiv -21\ mod\ 28 \equiv 7\ (H)$$

$$(C - L)\ mod\ 28\ \rightarrow (2 - 11)\ mod\ 28 \equiv -9\ mod\ 28 \equiv 19\ (T)$$

$$(A - Y)\ mod\ 28\ \rightarrow (0 - 24)\ mod\ 28 \equiv -24\ mod\ 28 \equiv 4\ (E)$$

$$(B - D)\ mod\ 28\ \rightarrow (1 - 3)\ mod\ 28 \equiv -2\ mod\ 28 \equiv 26\ (\#)$$

$$(C - S)\ mod\ 28\ \rightarrow (2 - 18)\ mod\ 28 \equiv -16\ mod\ 28 \equiv 12\ (M)$$

$$(A - J)\ mod\ 28\ \rightarrow (0 - 9)\ mod\ 28 \equiv -9\ mod\ 28 \equiv 19\ (T)$$

$$(B - \%)\ mod\ 28\ \rightarrow (1 - 27)\ mod\ 28 \equiv -26\ mod\ 28 \equiv 2\ (C)$$

$$(C - W)\ mod\ 28\ \rightarrow (2 - 22)\ mod\ 28 \equiv -20\ mod\ 28 \equiv 8\ (I)$$

$$(A - U)\ mod\ 28\ \rightarrow (0 - 20)\ mod\ 28 \equiv -20\ mod\ 28 \equiv 8\ (I)$$

$$(B - R)\ mod\ 28\ \rightarrow (1 - 17)\ mod\ 28 \equiv -16\ mod\ 28 \equiv 12\ (M)$$

$$(C - C)\ mod\ 28\ \rightarrow (2 - 2)\ mod\ 28 \equiv 0\ mod\ 28 \equiv\ 0\ (A)$$

$$(A - K)\ mod\ 28\ \rightarrow (0 - 10)\ mod\ 28 \equiv -10\ mod\ 28 \equiv 18\ (S)$$

$$(B - C)\ mod\ 28\ \rightarrow (1 - 2)\ mod\ 28 \equiv -1\ mod\ 28 \equiv 27\ (\%)$$

$$(C - D)\ mod\ 28\ \rightarrow (2 - 3)\ mod\ 28 \equiv -1\ mod\ 28 \equiv\ 27\ (\%)$$

$$(A - B)\ mod\ 28\ \rightarrow (0 - 1)\ mod\ 28 \equiv -1\ mod\ 28 \equiv 27\ (\%)$$

$$(B - B)\ mod\ 28\ \rightarrow (1 - 1)\ mod\ 28 \equiv 0\ mod\ 28 \equiv 0\ (A)$$

$$(C - R)\ mod\ 28\ \rightarrow (2 - 17)\ mod\ 28 \equiv -15\ mod\ 28 \equiv\ 13\ (N)$$

Proses dekripsi yang telah dilakukan menghasilkan *Ciphertext* berupa NM#AFU#OFRTHAHTE#MTCIIMAS%%%AN. Kemudian akan dilakukan proses dekripsi dengan algoritma transposisi grup simetri dengan merubah *Ciphertext* yang telah didapatkan menjadi blok-blok sesuai dengan apa yang disepakati oleh pengirim pesan dan penerima pesan yaitu transposisi grup simetri S_6 yang akan dijelaskan sebagai berikut:

NM#AFU	#OFRTH	AHTE#M	TCIIMA
S%%%AN			

Kunci invers permutasi yang digunakan adalah:

$$\pi_1^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ \alpha_5 & \alpha_6 & \alpha_1 & a_3 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ N & M & \# & A & F & U \\ \alpha_5 & \alpha_6 & \alpha_1 & a_3 & a_2 & \alpha_4 \\ F & U & N & \# & M & A \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok pertama yaitu **FUN#MA.**

$$\pi_2^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ \alpha_5 & \alpha_6 & \alpha_1 & a_3 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ \# & O & F & R & T & H \\ \alpha_5 & \alpha_6 & \alpha_1 & a_3 & a_2 & \alpha_4 \\ T & H & \# & F & O & R \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok kedua yaitu **TH#FOR.**

$$\pi_3^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ \alpha_5 & \alpha_6 & \alpha_1 & a_3 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ A & H & T & E & \# & M \\ \alpha_5 & \alpha_6 & \alpha_1 & a_3 & a_2 & \alpha_4 \\ \# & M & A & T & H & E \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok kedua yaitu **#MATHE.**

$$\pi_3^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ \alpha_5 & \alpha_6 & \alpha_1 & a_3 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ T & C & I & I & M & A \\ \alpha_5 & \alpha_6 & \alpha_1 & a_3 & a_2 & \alpha_4 \\ M & A & T & I & C & I \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok kedua yaitu **MATICI.**

$$\pi_3^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ \alpha_5 & \alpha_6 & \alpha_1 & a_3 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & a_4 & a_5 & \alpha_6 \\ S & \% & \% & \% & A & N \\ \alpha_5 & \alpha_6 & \alpha_1 & a_3 & a_2 & \alpha_4 \\ A & N & S & \% & \% & \% \end{pmatrix}$$

Didapatkan hasil *Plaintext* dari blok terakhir yaitu **ANS%%%.** Dan jika digabungkan dari blok pertama sampai blok terakhir didapatkan *Plaintext* awal berupa FUN MATH FOR MATHEMATICIANS.

Algoritma *Beaufort Cipher* memiliki kelemahan yaitu penggunaan kunci berulang yang dapat dipecahkan menggunakan metode kasiski dan *exhaustive key search* dengan cara menemukan dua karakter berpasangan atau lebih *Ciphertext* yang berulang dan kemudian hitung jarak antara karakter tersebut, lalu hitung faktor pembagi nya (panjang kunci yang mungkin digunakan), dan yang terakhir mencoba semua kemungkinan kunci yang ada. Semua kemungkinan yang harus dicoba adalah 26^p dengan p adalah panjang kunci yang digunakan, jadi semakin panjang

kunci yang digunakan semakin banyak pula kemungkinan kunci yang harus digunakan.

Perhatikan contoh yang telah digunakan pada simulasi algoritma *Beaufort Cipher*, untuk plaintext berupa FUN MATH FOR MATHEMATICIANS jika dienkripsi akan menghasilkan *Ciphertext* berupa VHP ***OBJ***T WOJ PCHUY***OBJ***SZUAOK. Perhitungan metode kasiski untuk menemukan panjang kunci yang digunakan akan dijelaskan sebagai berikut:

1. Jarak antara OBJ ke OBJ= 12
2. Faktor pembagi dari 12 adalah $\{2,3,4,6\}$ yang berjumlah 4
3. Dengan demikian panjang kunci nya adalah 3, karena pembagian dari jarak antar karakter dengan faktor pembagi.

Kemudian dengan menggunakan *exhaustive key search* dengan mengelompokkan karakter *Ciphertext* sesuai dengan kuncinya, kelompok 1 terdiri dari *Ciphertext* dengan karakter kunci ke-1, kelompok 2 terdiri dari *Ciphertext* dengan karakter kunci ke-2, kelompok 3 terdiri dari *Ciphertext* dengan karakter kunci ke-3.

VHP	***OBJ***	TWO	JPC	***OBJ***	HUY	SZU	AOK
123	123	123	123	123	123	123	123

Tabel 4. 3 Pengelompokan Ciphertext

Kelompok	Ciphertext	Huruf yang sering muncul
1	VOTJHSA	V=1, S=1, T=1, S=1 O=1, H=1, J=1, A=1
2	HBWPBUZO	H=1, B=2, W=1, P=1 U=1, Z=1, O=1
3	PJOCJYUK	P=1, J=2, O=1, C=1

		Y=1, U=1, K=1

Dari kemungkinan diatas dapat dicoba-coba untuk menemukan kunci dengan panjang tiga karakter dan akan ditemukan kunci sebenarnya yaitu ABC. Kemudian lakukan dekripsi pesan dengan kunci ABC sehingga diperoleh *plaintext* FUN MATH FOR MATHEMATICIANS.

Setelah mendapatkan hasil enkripsi dari algoritma *Beaufort Cipher* dan modifikasi algoritma *Beaufort Cipher* dengan grup simetri, akan dilakukan uji hasil enkripsi dengan menggunakan metode Kasiski dan *exhaustive key search* untuk mengetahui kemungkinan kunci yang digunakan dan perbandingannya akan dijelaskan sebagai berikut:

Tabel 4. 4 Tabel Perbandingan Hasil Enkripsi

Ciphertext Modifikasi *Beaufort Cipher*			Kunci	*Ciphertext Beaufort Cipher*
Grup	S_4	CQZIWLQBNODZJ BEQBSVZW#KWB LCP.	ABC	VHP **OBJ**T WOJ PCHUY**OBJ**SZUAOK.
	S_5	IDZQQLCBZVM SOBEVRLAZWU KC#LDPCD		
	S_6	PREAYKCPZLKX AWLYDSJ%WUR CKCDBBR.		

Perhatikan tabel 4.4 dapat dilihat hasil enkripsi dari algoritma *Beaufort Cipher* memiliki perulangan karakter yang lebih dari satu kali dan dengan menggunakan metode kasiski serta exhaustive key search dapat diketahui panjang kunci yang digunakan adalah tiga, sedangkan untuk modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri memiliki penambahan jumlah karakter serta memuat simbol persen dan pagar. Pada modifikasi algoritma *Beaufort Cipher* dengan grup simetri tidak memiliki perulangan karakter lebih dari satu kali, hal ini akan menyulitkan peretas yang akan mencari kemungkinan kunci dengan menggunakan metode Kasiski dan *exhaustive key search* sehingga peretas akan mencoba dengan kemungkinan sebanyak 28^p dengan p adalah panjang kunci sehingga akan terdapat $28^3 = 21{,}952$ kemungkinan kunci, sedangkan untuk algoritma *Beaufort Cipher* memiliki $26^3 = 17{,}576$ kemungkinan kunci yang ada. Dapat disimpulkan bahwa modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri lebih aman daripada algoritma *Beaufort Cipher*.

4.3 Amanah Dalam Kriptografi

Amanah adalah salah satu sifat mulia yang harus dimiliki oleh setiap manusia sebagai perwujudan rasa tanggung jawabnya terhadap sesama makhluk ataupun terhadap sang pencipta. Sifat amanah ini dituliskan dalam al qur'an surat An-Nisa ayat 58, selain itu sifat amanah juga diriwayatkan oleh Ahmad Musthafa Al-Maraghi "amanah adalah segala sesuatu yang harus dijaga dan dan dipelihara agar dapat tersampaikan kepada orang yang berhak menerimanya".

Amanah yang diberikan kepada seseorang kepada kita haruslah kita jaga dengan baik tanpa melakukan suatu pengurangan ataupun penambahan yang dapat merusak amanah yang telah diberikan. Berdasarkan penjelasan sub bab sebelumnya

maka untuk setiap amanah (pesan) yang akan dikirimkan haruslah kita jaga kerahasiaannya agar tidak dapat disalahgunakan oleh orang yang bertanggung jawab.

BAB V
PENUTUP

5.1 Kesimpulan

Kriptografi yang dengan menggunakan modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri untuk mengamankan pesan telah dilakukan dan penulis mendapatkan kesimpulan sebagai berikut:

1. Proses enkripsi yang dilakukan dengan modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri dilakukan dengan mengenkripsi *Plaintext* yang telah ditentukan menggunakan algoritma transposisi grup simetri terlebih dahulu, kemudian hasil dari enkripsi tersebut berupa *Ciphertext* akan diproses kembali dengan *Beaufort Cipher* sehingga diperoleh *Ciphertext* yang kedua, dengan demikian proses enkripsi pada modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri melalui dua kali proses enkripsi, dengan metode *Kasiski* serta *exhaustive key search* dapat disimpulkan bahwa modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri lebih aman daripada algoritma *Beaufort Cipher* biasa.
2. Proses dekripsi yang dilakukan dengan modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri dilakukan dengan mengdekripsi ciphertkes kedua menggunakan algoritma *Beaufort Cipher* terlebih dahulu, kemudian hasil dari dekripsi berupa *Ciphertext* yang pertama tersebut akan diproses kembali dengan algortima transposisi grup simetri sehingga diperoleh *Plaintext* awal, dengan demikian proses dekripsi pada modifikasi

algoritma *Beaufort Cipher* dengan transposisi grup simetri melalui dua kali proses dekripsi.

5.2 Saran untuk Penelitian Lanjutan

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

DAFTAR PUSTAKA

Agama, R. D. (2009). *Yasmina Al'quran & Terjemah* (RI Departemen Agama (ed.); Syaamil Al). PT Sygma Examedia Arkanleema.

Andika, T., Taqiyuddin, M., & Yunita, N. (2020). Amanah dan Khianat dalam Al-Qur'an Menurut Quraish Shihab. *Jurnal Ilmu Al-Qur'an Dan Tafsir*, *5*(02), 177–206. https://jurnal.staialhidayahbogor.ac.id/index.php/alt/article/view/926

Ariyus, D. (2008). *Pengantar Ilmu Kriptogradi Teori, Analisis dan Implementasi* (F. S. Suyantoro (ed.); 1st ed.). CV Andi Offset.

Dalimunthe, R. P. (2018). Amanah Dalam Perspektif Hadis. *Diroyah : Jurnal Studi Ilmu 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 Implementasi Aplikasi Keamanan File Audio Wav Dengan Menerapkan Algoritma Beaufort Cipherdan Root 13. *Jurnal Pelita Informatika*, *8*(1), 33–40.

Munir, R. (2019). *Kriptografi* (2nd ed.). Penerbit Informatika Bandung.

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.

Rachman, Y. F., & Ariyus, D. (2020). *Kriptografi Teks Menggunakan Modifikasi Substitusi Cipher Dan Elemen Musik*. 581–588.

Riskiyah, W. (2016). Enkripsi dan Dekripsi Pesan menggunakan Grup Simetri untuk Mengamankan Informasi. In *Science of Surverying and Mapping* (Vol. 41).

Sadikin, R. (2012). *Kriptografi untuk Keamanan Jaringan* (edition 1). Andi Offset.

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

Sinaga, D., Umam, C., Setiadi, D. R. I. M., & Rachmawanto, E. H. (2018). Teknik Super Enkripsi Menggunakan Transposisi Kolom Berbasis Vigenere Cipher Pada Citra Digital. *Dinamika Rekayasa*, *14*(1), 57. https://doi.org/10.20884/1.dr.2018.14.1.198

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

Suryanti, S. (2017). *Teori Grup (Struktur Aljabar 1)*.

LAMPIRAN

Lampiran 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	26	27

Lampiran 2 Program Python untuk Grup Simetri S_4

```
# ENKRIPSI TRANSPOSISI
def enkripsi(p):
    c=''
    while len(p)%4!=0:
        p=p+'%'
    for i in range(len(p)//4):
       c=c+p[3+(4∘i)]
       c=c+p[2+(4∘i)]
       c=c+p[0+(4∘i)]
       c=c+p[1+(4∘i)]
    return c
# HASIL ENKRIPSI DENGAN MENGGUNAKAN TRANPOSISI GRUP
    SIMETRI
pesanEnkripsi = str(input("masukkan pesan: ").upper())
pesanEnkripsi2 = enkripsi(pesanEnkripsi)
print(pesanEnkripsi2)
# KAMUS MERUBAH ALFABET KE DALAM ANGKA DAN SEBALIKNYA
kamus1 = {'A': 0, 'B': 1, 'C': 2, 'D': 3, 'E': 4,
```

```
        'F': 5, 'G': 6, 'H': 7, 'I': 8, 'J': 9,
        'K': 10, 'L': 11, 'M': 12, 'N': 13, 'O': 14,
        'P': 15, 'Q': 16, 'R': 17, 'S': 18, 'T': 19,
        'U': 20, 'V': 21, 'W': 22, 'X': 23, 'Y': 24, 'Z':25, '#':26, '%':27}
kamus2 = {0: 'A', 1: 'B', 2: 'C', 3: 'D', 4: 'E',
        5: 'F', 6: 'G', 7: 'H', 8: 'I', 9: 'J',
        10: 'K', 11: 'L', 12: 'M', 13: 'N', 14: 'O',
        15: 'P', 16: 'Q', 17: 'R', 18: 'S', 19: 'T',
        20: 'U', 21: 'V', 22: 'W', 23: 'X', 24: 'Y', 25: 'Z', 26:'#', 27:'%'}
#MEMBENTUK KUNCI SEPANJANG TEKS
def kunci_umum(pesan, kunci):
    x = len(pesan)
    i = 0
    while True:
        if x == 0:
            i = 0
        if len(kunci) == len(pesan):
            break
        kunci += kunci[i]
        i += 1
    return kunci
# HASIL KUNCI
pesan=pesanEnkripsi2.upper()
kunci=str(input("masukkan kunci: ").upper())
hasil= kunci_umum(pesan, kunci)
print(hasil)
# FUNGSI ENKRIPSI
def ciphertext(pesan, kunci_baru):
    cipher_text = ''
    i = 0
    for huruf in pesan:
        if huruf == ' ':
```

```
            cipher_text += ' '
        else:
            x = (kamus1[kunci_baru[i]]-kamus1[huruf]) % 28
            i += 1
            cipher_text += kamus2[x]
    return cipher_text
# HASIL ENKRIPSI DENGAN MENGGUNAKAN BEAUFORT CIPHER
hasil2 = ciphertext(pesan, hasil)
print(hasil2)
# FUNGSI DEKRIPSI
def plaintext(cipher_text, kunci_baru):
    plain_text = ''
    i = 0
    for huruf in cipher_text:
        if huruf == ' ':
            plain_text == ' '
        else:
            x = (kamus1[kunci_baru[i]]-kamus1[huruf]) % 28
            i += 1
            plain_text += kamus2[x]
    return plain_text
# HASIL DEKRIPSI DENGAN MENGGUNAKAN BEAUFORT CIPHER
hasil3 = plaintext(hasil2, hasil)
print(hasil3)
# DEKRIPSI TRANSPOSISI
def dekripsi(c):
    p=''
    while len(c)%4!=0:
        c=c+'%'
    for i in range(len(c)//4):
       p=p+c[2+(4∘i)]
       p=p+c[3+(4∘i)]
```

```
        p=p+c[1+(4∘i)]
        p=p+c[0+(4∘i)]
    return p
# HASIL DEKRIPSI DENGAN MENGGUNAKAN TRANSPOSISI GRUP
    SIMETRI
dekripsi(hasil3)
```

Lampiran 3 Program Python untuk Grup Simetri S_5

```
# ENKRIPSI TRANSPOSISI
def enkripsi(p):
    c=''
    while len(p)%5!=0:
        p=p+'%'
    for i in range(len(p)//5):
        c=c+p[1+(5∘i)]
        c=c+p[3+(5∘i)]
        c=c+p[0+(5∘i)]
        c=c+p[4+(5∘i)]
        c=c+p[2+(5∘i)]
    return c
# HASIL ENKRIPSI DENGAN MENGGUNAKAN TRANPOSISI GRUP
    SIMETRI
pesanEnkripsi = str(input("masukkan pesan: ").upper())
pesanEnkripsi2 = enkripsi(pesanEnkripsi)
print(pesanEnkripsi2)
# KAMUS MERUBAH ALFABET KE DALAM ANGKA DAN SEBALIKNYA
kamus1 = {'A': 0, 'B': 1, 'C': 2, 'D': 3, 'E': 4,
          'F': 5, 'G': 6, 'H': 7, 'I': 8, 'J': 9,
          'K': 10, 'L': 11, 'M': 12, 'N': 13, 'O': 14,
          'P': 15, 'Q': 16, 'R': 17, 'S': 18, 'T': 19,
          'U': 20, 'V': 21, 'W': 22, 'X': 23, 'Y': 24, 'Z':25, '#':26, '%':27}
```

```
kamus2 = {0: 'A', 1: 'B', 2: 'C', 3: 'D', 4: 'E',
        5: 'F', 6: 'G', 7: 'H', 8: 'I', 9: 'J',
        10: 'K', 11: 'L', 12: 'M', 13: 'N', 14: 'O',
        15: 'P', 16: 'Q', 17: 'R', 18: 'S', 19: 'T',
        20: 'U', 21: 'V', 22: 'W', 23: 'X', 24: 'Y', 25: 'Z', 26:'#', 27:'%'} # KAMUS
       MERUBAH ALFABET KE DALAM ANGKA DAN SEBALIKNYA
kamus1 = {'A': 0, 'B': 1, 'C': 2, 'D': 3, 'E': 4,
        'F': 5, 'G': 6, 'H': 7, 'I': 8, 'J': 9,
        'K': 10, 'L': 11, 'M': 12, 'N': 13, 'O': 14,
        'P': 15, 'Q': 16, 'R': 17, 'S': 18, 'T': 19,
        'U': 20, 'V': 21, 'W': 22, 'X': 23, 'Y': 24, 'Z':25, '#':26, '%':27}
kamus2 = {0: 'A', 1: 'B', 2: 'C', 3: 'D', 4: 'E',
        5: 'F', 6: 'G', 7: 'H', 8: 'I', 9: 'J',
        10: 'K', 11: 'L', 12: 'M', 13: 'N', 14: 'O',
        15: 'P', 16: 'Q', 17: 'R', 18: 'S', 19: 'T',
        20: 'U', 21: 'V', 22: 'W', 23: 'X', 24: 'Y', 25: 'Z', 26:'#', 27:'%'} # KAMUS
       MERUBAH ALFABET KE DALAM ANGKA DAN SEBALIKNYA
kamus1 = {'A': 0, 'B': 1, 'C': 2, 'D': 3, 'E': 4,
        'F': 5, 'G': 6, 'H': 7, 'I': 8, 'J': 9,
        'K': 10, 'L': 11, 'M': 12, 'N': 13, 'O': 14,
        'P': 15, 'Q': 16, 'R': 17, 'S': 18, 'T': 19,
        'U': 20, 'V': 21, 'W': 22, 'X': 23, 'Y': 24, 'Z':25, '#':26, '%':27}
kamus2 = {0: 'A', 1: 'B', 2: 'C', 3: 'D', 4: 'E',
        5: 'F', 6: 'G', 7: 'H', 8: 'I', 9: 'J',
        10: 'K', 11: 'L', 12: 'M', 13: 'N', 14: 'O',
        15: 'P', 16: 'Q', 17: 'R', 18: 'S', 19: 'T',
        20: 'U', 21: 'V', 22: 'W', 23: 'X', 24: 'Y', 25: 'Z', 26:'#', 27:'%'}
#MEMBENTUK KUNCI SEPANJANG TEKS
def kunci_umum(pesan, kunci):
    x = len(pesan)
    i = 0
    while True:
```

```
        if x == 0:
            i = 0
        if len(kunci) == len(pesan):
            break
        kunci += kunci[i]
        i += 1
    return kunci
# HASIL KUNCI
pesan=pesanEnkripsi2.upper()
kunci=str(input("masukkan kunci: ").upper())
hasil= kunci_umum(pesan, kunci)
print(hasil)
# FUNGSI ENKRIPSI
def ciphertext(pesan, kunci_baru):
    cipher_text = ''
    i = 0
    for huruf in pesan:
        if huruf == ' ':
            cipher_text += ' '
        else:
            x = (kamus1[kunci_baru[i]]-kamus1[huruf]) % 28
            i += 1
            cipher_text += kamus2[x]
    return cipher_text
# HASIL ENKRIPSI DENGAN MENGGUNAKAN BEAUFORT CIPHER
hasil2 = ciphertext(pesan, hasil)
print(hasil2)
# FUNGSI DEKRIPSI
def plaintext(cipher_text, kunci_baru):
    plain_text = ''
    i = 0
    for huruf in cipher_text:
```

```
        if huruf == ' ':
            plain_text == ' '
        else:
            x = (kamus1[kunci_baru[i]]-kamus1[huruf]) % 28
            i += 1
            plain_text += kamus2[x]
    return plain_text
# HASIL DEKRIPSI DENGAN MENGGUNAKAN BEAUFORT CIPHER
hasil3 = plaintext(hasil2, hasil)
print(hasil3)
# DEKRIPSI TRANSPOSISI
def dekripsi(c):
    p=''
    while len(c)%5!=0:
        c=c+'%'
    for i in range(len(c)//5):
        p=p+c[2+(5∘i)]
        p=p+c[0+(5∘i)]
        p=p+c[4+(5∘i)]
        p=p+c[1+(5∘i)]
        p=p+c[3+(5∘i)]
    return p
# HASIL DEKRIPSI DENGAN MENGGUNAKAN TRANSPOSISI GRUP
    SIMETRI
dekripsi(hasil3)
```

Lampiran 4 Program Python untuk Grup Simetri S_6

```
# ENKRIPSI TRANSPOSISI
def enkripsi(p):
    c=''
    while len(p)%6!=0:
        p=p+'%'
```

```
    for i in range(len(p)//6):
        c=c+p[2+(6∘i)]
        c=c+p[4+(6∘i)]
        c=c+p[3+(6∘i)]
        c=c+p[5+(6∘i)]
        c=c+p[0+(6∘i)]
        c=c+p[1+(6∘i)]
    return c
# HASIL ENKRIPSI DENGAN MENGGUNAKAN TRANPOSISI GRUP
    SIMETRI
pesanEnkripsi = str(input("masukkan pesan: ").upper())
pesanEnkripsi2 = enkripsi(pesanEnkripsi)
print(pesanEnkripsi2)
# KAMUS MERUBAH ALFABET KE DALAM ANGKA DAN SEBALIKNYA
kamus1 = {'A': 0, 'B': 1, 'C': 2, 'D': 3, 'E': 4,
        'F': 5, 'G': 6, 'H': 7, 'I': 8, 'J': 9,
        'K': 10, 'L': 11, 'M': 12, 'N': 13, 'O': 14,
        'P': 15, 'Q': 16, 'R': 17, 'S': 18, 'T': 19,
        'U': 20, 'V': 21, 'W': 22, 'X': 23, 'Y': 24, 'Z':25, '#':26, '%':27}
kamus2 = {0: 'A', 1: 'B', 2: 'C', 3: 'D', 4: 'E',
        5: 'F', 6: 'G', 7: 'H', 8: 'I', 9: 'J',
        10: 'K', 11: 'L', 12: 'M', 13: 'N', 14: 'O',
        15: 'P', 16: 'Q', 17: 'R', 18: 'S', 19: 'T',
        20: 'U', 21: 'V', 22: 'W', 23: 'X', 24: 'Y', 25: 'Z', 26:'#', 27:'%'}
#MEMBENTUK KUNCI SEPANJANG TEKS
def kunci_umum(pesan, kunci):
    x = len(pesan)
    i = 0
    while True:
        if x == 0:
            i = 0
        if len(kunci) == len(pesan):
```

```
            break
        kunci += kunci[i]
        i += 1
    return kunci
# HASIL KUNCI
pesan=pesanEnkripsi2.upper()
kunci=str(input("masukkan kunci: ").upper())
hasil= kunci_umum(pesan, kunci)
print(hasil)
# FUNGSI ENKRIPSI
def ciphertext(pesan, kunci_baru):
    cipher_text = ''
    i = 0
    for huruf in pesan:
        if huruf == ' ':
            cipher_text += ' '
        else:
            x = (kamus1[kunci_baru[i]]-kamus1[huruf]) % 28
            i += 1
            cipher_text += kamus2[x]
    return cipher_text
# HASIL ENKRIPSI DENGAN MENGGUNAKAN BEAUFORT CIPHER
hasil2 = ciphertext(pesan, hasil)
print(hasil2)
# FUNGSI DEKRIPSI
def plaintext(cipher_text, kunci_baru):
    plain_text = ''
    i = 0
    for huruf in cipher_text:
        if huruf == ' ':
            plain_text == ' '
        else:
```

```
            x = (kamus1[kunci_baru[i]]-kamus1[huruf]) % 28
            i += 1
            plain_text += kamus2[x]
    return plain_text
# HASIL DEKRIPSI DENGAN MENGGUNAKAN BEAUFORT CIPHER
hasil3 = plaintext(hasil2, hasil)
print(hasil3)
# DEKRIPSI TRANSPOSISI
def dekripsi(c):
    p=''
    while len(c)%6!=0:
        c=c+' '
    for i in range(len(c)//6):
        p=p+c[4+(6∘i)]
        p=p+c[5+(6∘i)]
        p=p+c[0+(6∘i)]
        p=p+c[2+(6∘i)]
        p=p+c[1+(6∘i)]
        p=p+c[3+(6∘i)]
    return p
# HASIL DEKRIPSI DENGAN MENGGUNAKAN TRANSPOSISI GRUP
    SIMETRI
dekripsi(hasil3)
```

RIWAYAT HIDUP

Muhammad Zulfikri Rangga dilahirkan di malang pada tanggal 5 juli 2000. Nama panggilan Fikri, tinggal di Jalan Teluk Grajakan Gg V No. 39 RT/RW 02/02 Kelurahan Pandanwangi, Kecamatan Blimbing, Kota Malang, dan memiliki saudara yang bernama Muhammad Zulfikar Rangga dari pasangan Bapak Ismail dan Ibu Aprilina Adi Warsa.

Penulis telah menempuh pendidikan formal mulai dari TK dian Pertiwi Malang dan lulus pada tahun 2006. Pada tahun yang sama penulis masuk jenjang pendidikan sekolah dasar Pandanwangi 3 Malang dan lulus pada tahun 2012. Kemudian penulis menempuh pendidikan sekolah menengah pertama di SMPN 14 Malang dan lulus pada tahun 2015, selanjutnya masuk pada jenjang pendidikan sekolah menengah atas di SMAN 6 Malang lalu pindah ke SMAN 10 Malang pada tahun pertama dan lulus pada tahun 2018. Pada tahun yang sama penulis masuk jenjang perkuliahan di Universitas Islam Negeri Maulana Malik Ibrahim Malang dengan mengambil prodi matematika.

Selama menempuh jenjang pendidikan di universitas penulis aktif dalam mengikuti acara-acara prodi seperti lomba-lomba antar mahasiswa prodi dan komet. Selain kegiatan tersebut penulis juga aktif dalam kegiatan non akademis yang membantu penulis dalam mencari pengalaman serta bersosialisasi dengan warga sekitar.

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 Zulfikri Rangga
NIM : 18610096
Fakultas / Program Studi : Sains dan Teknologi / Matematika
Judul Skripsi : Modifikasi Algoritma *Beaufort Cipher* dengan Transposisi Grup Simetri untuk Mengamankan Pesan
Pembimbing I : Muhammd Khudzaifah, M.Si
Pembimbing II : Mohammad Nafie Jauhari, M.Si

No	Tanggal	Hal	Tanda Tangan
1.	19 Januari 2022	Konsultasi Bab I	1.
2.	4 Februari 2022	Konsultasi Revisi Bab I	2.
3.	18 Februari 2022	Konsultasi Bab II dan III	3.
4.	7 Maret 2022	Konsultasi Revisi Bab II dan III	4.
5.	28 Maret 2022	Konsultasi Kajian Agama	5.
6.	31 Maret 2022	Konsultasi Revisi Kajian Agama	6.
7.	12 April 2022	ACC untuk Seminar Proposal	7.
8.	8 Juni 2022	Konsultasi Bab IV dan V	8.
9.	9 Agustus 2022	Konsultasi Revisi Bab IV dan V	9.
10.	10 September 2022	Konsultasi Revisi Bab IV dan V	10.
11.	28 September 2022	ACC untuk Seminar Hasil	11.
12.	8 November 2022	ACC Matriks Revisi Seminar Hasil	12.
13.	23 November 2022	ACC untuk Sidang Skripsi	13.
14.	14 Desember 2022	ACC Keseluruhan	14.

Malang, 14 Desember 2022
Mengetahui,
Ketua Program Studi Matematika

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