MODIFIKASI ALGORITMA HILL CIPHER MENGGUNAKAN GRUP SIMETRI UNTUK MENGGAMANKAN PESAN TEKS

SKRIPSI

OLEH:
DONI YOGA PRATAMA
NIM. 16610009

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2023

MODIFIKASI ALGORITMA HILL CIPHER MENGGUNAKAN GRUP SIMETRI UNTUK MENGGAMANKAN PESAN TEKS

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
DONI YOGA PRATAMA
NIM. 16610009

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2023

MODIFIKASI ALGORITMA HILL CIPHER MENGGUNAKAN GRUP SIMETRI UNTUK MENGGAMANKAN PESAN TEKS

SKRIPSI

Oleh
Doni Yoga Pratama
NIM. 16610009

Telah Disetujui untuk Diuji
Malang, 21 Juni 2023

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah, M.Si.	Erna Herawati, M.Pd.
NIDT. 19900511201608011 057	NIDT. 19760723201802012 222

Mengetahui,
Ketua Program Studi Matematika

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

MODIFIKASI ALGORITMA HILL CIPHER MENGGUNAKAN GRUP SIMETRI UNTUK MENGGAMANKAN PESAN TEKS

SKRIPSI

Oleh
Doni Yoga Pratama
NIM. 16610009

Telah Dipertahankan di Depan Penguji Ujian Skripsi
Dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
Untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal, 22 Juni 2023

Ketua Penguji	: Dr. Elly Susanti, S.Pd, M.Sc.	.....
Anggota Penguji 1	: Hisyam Fahmi, M.Kom.	.....
Anggota Penguji 2	: Muhammad Khudzaifah, M.Si.	.....
Anggota Penguji 3	: Erna Herawati, M.Pd.	.....

Mengetahui,
Ketua Program Studi Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Wahyu Nurlaili

NIM : 17610079

Judul Skripsi : Analisis Sistem Dinamik Untuk Model Interaksi Antara Autofagi Dan Apoptosis Di Sel Mamalia.

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

Malang, 01 Juni 2023

Yang membuat pernyataan,

Wahyu Nurlaili

NIM. 17610079

MOTO

Berimajinasi bebas, Coret tinta dan kertas

Jangan lupa bernafas

PERSEMBAHAN

Dengan penuh rasa terima kasih, saya dengan gembira menghadirkan karya ini kepada: Orang-orang istimewa, terutama kepada kedua orang tua saya, yaitu bapak Sugianto dan ibu Murtini yang saya cintai, yang selalu memberikan dukungan dan doa yang tak pernah berhenti bagi saya. Saya juga ingin menyampaikan terima kasih kepada teman-teman saya yang selalu memberikan semangat dan dukungan moral selama proses penulisan skripsi ini.

KATA PENGANTAR

Dengan rasa syukur yang tak terhingga, peneliti ingin mengucapkan terima kasih kepada Allah SWT. atas berkah-Nya, petunjuk-Nya, dan anugerah-Nya yang telah memungkinkan penyelesaian skripsi ini dengan lancar. Doa dan salam juga tak terlupakan yang senantiasa ditujukan kepada Nabi Agung Muhammad SAW., yang telah membimbing umat manusia dari zaman kegelapan (jahiliyyah) menuju zaman yang penuh cahaya, yaitu zaman keagungan Islam.

Alhamdulillah berkat taufiq dan hidayahnya,terselesaikannya skripsi ini denggan judul "**Modifikasi Algoritma Hill Cipher menggunakan Grup Simetri Untuk Mengamankan Pesan Teks**". Dalam proses penyelesaian skripsi tidak lepas dari doa, bantuan, bimbingan, serta arahan dari berbagai pihak, karena itu peneliti mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. M. Zainuddin, M.A. selaku Rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Ibu Dr. Sri Harini M.Si. selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Ibu Dr. Elly Susanti, M.Sc. selaku ketua Program Studi Matematika Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Bapak Muhammad Khudzaifah, M.Si selaku dosen pembimbing I yang senantiasa memberikan bimbingan, arahan, dan ilmu kepada peneliti dalam menyelesaikan skripsi ini.
5. Ibu Erna Herawati, M.Pd. selaku dosen pembimbing II yang senantiasa memberikan bimbingan, arahan, dan ilmu kepada peneliti dalam menyelesaikan skripsi ini.
6. Seluruh sivitas akademika Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang khususnya seluruh dosen yang memberikan banyak ilmu dan pengalaman berharga bagi para peneliti.
7. Teristimewa dari peneliti untuk kedua orang tua dan adik peneliti yang senantiasa memberikan dukungan kepada peneliti baik moril maupun materiil sehingga peneliti dapat menyusun dan menyelesaikan laporan skripsi ini dengan baik.

8. Teman teman terbaik peneliti terutama teman kos yang bersedia menemani, membantu, dan mendukung peneliti baik secara langsung maupun tidak langsung.
9. Seluruh teman teman seperjuangan SOULMATH ’16.
10. Semua pihak yang tidak dapat disebutkan satu persatu, yang telah membantu menyelesaikan skripsi baik moril maupun materil.

Semoga segala bantuan yang tulus dari berbagai pihak mendapatkan balasan yang sepadan dari Allah SWT. Penulis juga berharap agar skripsi ini memberikan manfaat kepada para pembaca yang meluangkan waktu untuk membacanya.

Malang, 23 Juni 2023

Peneliti

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SIMBOL

Ω = Himpunan
S = Grup simetri
K = Matriks
C = *Ciphertext*
P = *Plaintext*
K^{-1} = Matriks invers
T = Tranposisi grup simetri
T^{-1} = Invers tranposisi grup simetri
P_T = *Plaintext* algoritma grup simetri
C_T = *Ciphertext* algoritma grup simetri

ABSTRAK

Pratama, Doni Yoga. 2023. **Modifikasi Algoritma Hill Cipher menggunakan Grup Simetri Untuk Mengamankan Pesan Teks.** Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing (I) Muhammad Khudzaifah, M.Si. (II) Erna Herawati, M.Pd.

Kata Kunci: Hill Cipher, Grup Simetri, Modifkasi, Judul Skripsi

Informasi dan data penting yang bernilai tinggi patut dijaga agar tidak dapat di akses oleh pihak yang tidak bertanggung jawab. Hill Cipher merupakan metode pengamanan pesan menggunakan matriks untuk melakukan enkripsi dan menghitung matriks balikan terlebih dahulu untuk melakukan deskripsi. Namun, tingkat keamanan metode Hil Cipher masih kurang aman. Oleh karena itu, perlu dilakukan modifikasi proses enkripsi algoritma Hill Cipher dengan menggunakan grup simetri. Hal tersebut bertujuan untuk mengamankan *plaintext* dengan mengacak terlebih dahulu menggunakan penyandian grup simetri. Kemudian dilanjutkan dengan menggunakan algoritma Hill Cipher untuk melakukan enkripsi. Sedangkan untuk dekripsinya menggunakan invers dari Hill Cipher kemudian mengembalikannya dengan invers grup simetri yang sudah disepakati sebelumnya.

ABSTRACT

Pratama, Doni Yoga. 2023. **The Modification of the Hill Cipher Algorithm Employing Symmetry Groups Aimed to Preserve Text Messages.** Thesis. Department of Mathematics, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisors: (I) Muhammad Khudzaifah, M.Si. (II) Erna Herawati, M.Pd.

Keywords: Hill Chiper, Symmetry Group, Modification, Thesis Title

As time goes by, a high value of information and data should be secret to avoid any hacking experiments done by unauthorized parties. Following Hill Cipher, one of the message security methods which applies matrix, it is done by formerly encrypting and calculating the feedback matrix to conduct the decryption. However, the security level of the Hill Cipher method is still less secure. Therefore, a symmetric group is necessary to modify the Hill Cipher algorithm encryption process. This present study aimed to secure the plaintext by formerly randomizing it utilizing symmetric group encoding. Further, it proceeded by applying the Hill Cipher algorithm to perform encryption. Nevertheless, to execute decryption, it employed the inverse of the Hill Cipher and returned it with the inverse of the symmetry group that had been agreed upon beforehand.

برتما،دولني يوغا. ٢٠٢٣. **تعديل (*Hill Cipher*) باستخدام مجموعات التماثل (*Symmetric Group*) الخوارزمية**. البحث العلمي. قسم الرياضييات، كتية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامي الحكومية بمالانج. المشرف : (١) محمد خذيف ، الماجستير (٢) إيرنا هيراواتي ،الماجستير.

الكلمات الرئيسية : *Hill Cipher*، *Symmetric Group*، تعديل

يجب حماية المعلومات والبيانات الهامة ذات القيمة العالية بحيث لا يمكن الوصول إليها من قبل أطراف غير مسؤولة. *Hill Cipher* هي طريقة أمان للرسائل تستخدم مصفوفة لتشفير وحساب مصفوفة الملاحظات أولاً للقيام بفك التشفير. ومع ذلك، لا يزال مستوى الأمان الخاص بطريقة *Hill Cipher* أقل أمانًا. لذلك، من الضروري تعديل عملية تشفير لخوارزمية *Hill Cipher* باستخدام *Symmetry Group*. يهدف إلى تأمين النص العادي عن طريق توزيعه عشوائيًا أولاً باستخدام تشفير *Symmetry Group*. ثم تابع استخدام خوارزمية *Hill Cipher* لإجراء التشفير. أما بالنسبة لفك التشفير، فيستخدم معكوس *Hill Cipher* ثم يعيده بعكس *Symmetry Group* التي تم الاتفاق عليها مسبقًا.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Semakin pesat kemajuan teknologi informasi, kejahatan informasi komunikasi semakin marak terjadi, seperti kasus penyadapan percakapan, perentasan data pribadi, dan bahkah pencurian dokumen milik negara. Dengan semakin berkembangnya teknologi informasi, diperlukan juga keamanan dalam penggunaannya, terutama dalam hal pengamanan pesan. Penting untuk menjaga keamanan informasi yang bersifat rahasia, sensitif, atau memiliki nilai tinggi agar tidak dapat diakses oleh pihak yang tidak berwenang. Oleh karena itu, ada kebutuhan untuk meningkatkan keamanan kerahasiaan informasi yang dipertukarkan melalui Internet. Informasi yang biasa dipertukarkan antara lain data atau pesan dalam bentuk teks. Keamanan data dapat dijamin melalui penggunaan teknik enkripsi. Penggunaan teknik enkripsi dalam pesan teks dimaksudkan untuk mencegah orang yang tidak berhak mengetahui isi pesan tersebut. Pesan rahasia terkait dengan amanah untuk dikirim ke penerima yang berwenang (Munir, 2019).

Amanah merupakan sebuah janji atau titipan dan sesuatu yang dipercayakan sesorang baik materi maupun non-materi untuk selalu dijaga dan ditunaikan dengan sebaik-baiknya. Dalam Al-Qur'an surah An-Nisaa' ayat 58 dijelaskan pentingnya menjaga amanah.

إِنَّ اللَّهَ يَأْمُرُكُمْ أَنْ تُؤَدُّوا الْأَمَانَاتِ إِلَىٰ أَهْلِهَا وَإِذَا حَكَمْتُمْ بَيْنَ النَّاسِ أَنْ تَحْكُمُوا بِالْعَدْلِ ۚ إِنَّ اللَّهَ نِعِمَّا يَعِظُكُمْ بِهِ ۗ إِنَّ اللَّهَ كَانَ سَمِيعًا بَصِيرًا.

"Sungguh, Allah menyuruhmu menyampaikan amanat kepada yang berhak menerimanya, dan apabila kamu menetapkan hukum di antara manusia hendaknya kamu menetapkannya dengan adil. Sungguh, Allah sebaik-baik yang memberi pengajaran kepadamu. Sungguh, Allah Maha Mendengar, Maha Melihat".

Berdasarkan ayat 58 dalam surah An-Nisaa’ dari Al-Qur'an, Allah SWT. memberikan petunjuk kepada manusia untuk mempercayakan amanat kepada pihak yang berhak menerimanya. Dalam agama Islam, amanah dianggap sebagai sesuatu yang sangat penting untuk dijaga. Oleh karena itu, dapat disimpulkan bahwa sebuah pesan harus dianggap sebagai amanah yang harus dijaga kerahasiannya sampai sampai penerima pesan tersebut menerimanya. Dalam hal ini, kriptografi digunakan sebagai salah satu metode untuk mengamankan data dan mengurangi risiko penyalahgunaan informasi yang bersifat penting dan rahasia (Hariati, Hardiyati, & Putri, 2018).

Kriptografi merupakan suatu disiplin ilmu dan seni yang bertujuan untuk memastikan kerahasiaan pesan yang dikirimkan dari satu lokasi ke lokasi lainnya (Ariyus, 2008). Ada dua jenis kriptografi yang dikenal dalam presentasinya, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik biasanya bekerja dengan memanipulasi karakter dalam pesan, sedangkan kriptografi modern berfokus pada operasi pada level bit. Kriptografi menggunakan berbagai metode dengan tujuan untuk mengubah pesan yang dikirim sehingga meningkatkan keamanan pesan tersebut (Munir, 2019). Kriptografi melibatkan dua tahap utama, yaitu enkripsi dan dekripsi. Saat pengiriman data, pengirim melakukan proses enkripsi untuk mengubah data menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang. Setelah data sampai ke penerima, penerima melakukan proses dekripsi untuk mengembalikan data ke bentuk aslinya. Baik proses enkripsi maupun dekripsi membutuhkan penggunaan kunci rahasia yang disepakati oleh kedua belah pihak sebagai bagian penting dari proses tersebut.

Protokol perjanjian kunci adalah sebuah metode kriptografi yang digunakan oleh dua pihak untuk mengatasi tantangan dalam proses enkripsi dan dekripsi dalam keamanan pesan. Dalam metode ini, kedua pihak saling bertukar parameter yang diketahui oleh pihak yang ingin menerima pesan. Sebelumnya, Wasiatun Rizkiah (2016) sebelumnya telah dibahas suatu protokol perjanjian kunci yang melibatkan teknik transposisi dengan menggunakan kunci yang dibentuk melalui proses pembentukan kunci dalam grup simetri-n. Penelitian tersebut merujuk pada penelitian yang dilakukan oleh Stickel pada tahun 2005, yang memperkenalkan sebuah algoritma protokol perjanjian kunci yang berdasarkan pada kelompok non-komutatif.

Hill Cipher merupakan salah satu algoritma kriptografi klasik yang sulit untuk dipecahkan oleh kriptanalis hanya dengan menggunakan *ciphertext*. Keunikan dari metode Hill Cipher terletak pada fakta bahwa setiap huruf yang sama dalam *ciphertext* tidak diubah, hal ini karena metode ini menggunakan operasi perkalian matriks sebagai dasar dalam proses enkripsi dan dekripsi. Hill Cipher adalah sebuah algoritma yang digunakan untuk melakukan enkripsi dan dekripsi, yang melibatkan penggunaan matriks transformasi, dan termasuk dalam kategori kriptografi kunci simetris.. Pada Hill Cipher, kunci yang digunakan adalah matriks berukuran $n \times n$ yang sama untuk proses enkripsi dan dekripsi. Hal ini menyebabkan *plaintext* yang dihasilkan tidak selalu menghasilkan *ciphertext* yang sama (Munir, 2019). Dalam Hill Cipher, kunci matriks yang digunakan haruslah matriks *invertible*, yang berarti kunci K memiliki sebuah matriks invers K^{-1} yang memenuhi persamaan $K.K^{-1} = I$. Matriks invers K^{-1} ini kemudian digunakan dalam proses dekripsi (Hasugian, 2013).

Sebuah penelitian modifikasi dari Hill Cipher telah dilakukan oleh Giki, Kiswara, dan Ahmad pada tahun 2021. Penelitian ini menggunakan data teks yang terdiri dari karakter ASCII printable. Penelitian serupa juga telah dilakukan oleh Celine dan Dony pada tahun 2020. Penelitian tersebut menggabungkan Hill Cipher dengan Vigenere Cipher menjadi satu. Kedua penelitian tersebut menghasilkan algoritma yang lebih aman dibandingkan Hill Cipher konvensional. Namun, penelitian tersebut hanya menggunakan matriks berukuran $2x2$ dan dibatasi pada karakter yang dapat ditampilkan.

Dalam penelitian ini, dilakukan modifikasi pada algoritma Hill Cipher dengan menggunakan grup simetri untuk mengacak *plaintext*. Grup simetri tranposisi digunakan dengan tujuan mengacak urutan karakter dalam *plaintext* sebelum diproses menggunakan metode Hill Cipher. Tujuan dari penelitian ini adalah untuk meningkatkan tingkat keamanan algoritma Hill Cipher dengan menghasilkan sebuah algoritma baru yang lebih aman daripada Hill Cipher konvensional.

1.2 Rumusan Masalah

Dengan mengacu pada konteks yang telah dijelaskan sebelumnya, masalah yang dapat difokuskan adalah bagaimana melakukan perubahan pada algoritma Hill Cipher dengan menggabungkan penggunaan grup simetri untuk meningkatkan keamanan pesan teks..

1.3 Tujuan Penelitian

Berdasarkan konteks rumusan masalah yang telah disebutkan, tujuan dari penelitian ini adalah untuk menginvestigasi penggunaan grup simetri dalam

melakukan modifikasi pada algoritma Hill Cipher dengan tujuan meningkatkan keamanan pesan teks.

1.4 Manfaat Penelitian

1. Bagi Penulis

   Melalui penelitian ini, penulis bertujuan untuk mendalami pemahaman tentang metode Hill Cipher serta grup simetri. Pengetahuan yang diperoleh akan membatu metode pengamanan pesan melalui modifikasi algoritma Hill Cipher menggunakan grup simetri.

2. Bagi Pembaca

   Pembaca dapat merujuk kepada sumber referensi atau informasi yang membahas tentang modifikasi Hill Cipher dengan penerapan grup simetri.

1.5 Batasan Masalah

Batasan masalah yang kemudian akan digunakan pada penelitian ini adalah sebagai berikut.

1. Data yang digunakan dalam penelitian ini berupa teks yang akan diberlakukan pengacakan untuk menguatkan keamanan pesan.
2. Dalam proses enkripsi grup simetri, kunci dibentuk menggunakan metode Stickel, yang melibatkan algoritma grup simetri S_n.
3. Pada implementasi algoritma baru yang dihasilkan, digunakan grup simetri S_6.

BAB II
KAJIAN TEORI

2.1 Aritmatika Modulo

Aritmatika modulo merupakan salah satu bidang dalam teori bilangan yang memiliki peran penting dalam operasi bilangan bulat. Aritmatika modulo digunakan sebagai dasar dalam komputasi bilangan bulat dan bertujuan untuk menghasilkan bilangan bulat dalam suatu interval tertentu. Dalam konteks kriptografi, contohnya adalah penerapan aritmatika modulo pada karakter alfabet. Alfabet terdiri dari 26 karakter, yaitu huruf A hingga Z. Dalam aritmatika modulo, dilakukan pemetaan karakter alfabet {A,...,Z} ke angka $\{0,\ldots,25\}$. Tujuan dari penggunaan aritmetika modulo dalam kriptografi klasik adalah untuk memastikan bahwa transformasi penyandian berada dalam interval yang seragam, yaitu $\{0,\ldots,25\}$ (Sadikin, 2012).

Aritmetika modulo menggunakan operator berupa *mod*. Operasi modulo pada dasarnya butuh dua input, berupa bilangan bulat *z* dan modulo *n*, dengan syarat $n > 0$. Operasi ini menghasilkan nilai r, yang merupakan sisa pembagian z oleh n (Sadikin, 2012). Operator modulo dapat dinotasikan sebagai berikut:

$$z \; mod \; n \equiv r$$

Contoh 2.1

1. Hasil dari operasi dari $27 \; mod \; 5$

   Jawab: 27 dibagi 5 adalah 5 sisa 2,

   $27 = (5 \times 5) + 2$, jadi $27 \; mod \; 5 \equiv 2$

2. Hasil dari operasi $21 \; mod \; 7$

   Jawab: 21 dibagi 7 adalah 3 sisa 0,

$21 = (7 \times 3) + 0$, jadi $21\ mod\ 7 \equiv 0$

2.2 Keterbagian

Konsep keterbagian merupakan salah satu fondasi dalam pengembangan teori bilangan. Oleh karena itu, konsep keterbagian banyak digunakan dalam berbagai aspek kriptografi. Berikut ini adalah penjelasan mengenai konsep keterbagian.

Definisi 2.2

Misal a dan b adalah merupakan bilangan bulat di mana $a \neq 0$. Dari sini, dapat diambil kesimpulkan bahwa a membagi b dan dapat dituliskan sebagai $a|b$ jika terdapat bilangan bulat k sedemikian sehingga $b = a.k$. Definisi ini menjelaskan bahwa jika ada bilangan bulat a yang bukan nol, maka a dapat membagi bilangan bulat b jika terdapat bilangan bulat k sehingga $b = a.k$. Notasi yang digunakan untuk menyatakan ini adalah $a|b$ yang dibaca sebagai "a membagi b" atau "b habis dibagi oleh a". Jika a tidak dapat membagi b, maka dituliskan sebagai $a \nmid b$ (Irawan, 2014).

Contoh 2.2

1. $5|25$ karena terdapat $5 \in \mathbb{Z}$ sehingga $25 = 5.5$
2. $3 \nmid 7$ karena tidak terdapat $k \in \mathbb{Z}$ sehingga $7 = 3.k$

Teorema 2.1

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

Bukti:

1. $a|b$ maka $b = ak$ untuk suatu $k \in \mathbb{Z}$
2. $bc = (ak)c$ untuk setiap $c \in \mathbb{Z}$
3. $bc = a(kc)$ untuk setiap $kc \in \mathbb{Z}$

Teorema 2.2

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

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

   Terbukti $a|c$.

Teorema 2.3

Jika $a|b$ dan $a|c$ maka $a|b \pm c$

Bukti:

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

   $b|c$ maka $c = bk_2$ untuk suatu $k_2 \in \mathbb{Z}$
2. $b + c = a(k_1 + k_2)$, $(k_1 + k_2) \in \mathbb{Z}$

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

   Terbukti $a|b \pm c$

Teorema 2.4

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 $k_1 \in \mathbb{Z}$

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

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

Terbukti $a|(bx \pm cy)$

Teorema 2.5

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

Bukti:

1. $a|b\ maka\ b|a = ak$ utuk suatu $k\ \in \mathbb{Z}$

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

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

3. $a = (ak)l = a(kl)$

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

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

2.3 Kongruensi

Salah satu konsep teori bilangan yang penting adalah kongruensi. Berikut definisi kongruensi:

Definisi 2.3

Diberikan bilangan bulat $a, b,$ dan m di mana $m > 0$. Bilangan bulat a dikatakan kongruen $b\ modulo\ M$ jika $(a - b)$ dapat dibagi dengan m, dan hal ini dinyatakan sebagai $a \equiv b\ (mod\ m)$. Jika nilai a tidak kongruen $b\ modulo\ m$, maka dapat disimpulkan sebagai $a \not\equiv b\ (mod\ m)$. (Munir, 2019).

Contoh 2.3

1. $11 \equiv 8(mod\ 3)$ karena $3|(11 - 8)$
2. $-5 \not\equiv 24\ (mod\ 4)$ karena $4 \nmid (-5 - 24)$

2.4 Definisi Grup

Misal grup $(G,*)$ terdiri dari himpunan tak kosong G bersamaan dengan operasi biner $*$ pada G (yaitu $G \times G \rightarrow G$) akan memenuhi aksioma sebagai berikut:

1. Tertutup

   Operasi biner $*$ menghasilkan nilai di dalam G, yaitu untuk semua $a\ dan\ b$ di dalam $G, a * b$ di mana juga berada didalam G.

2. Asosiatif

   Untuk semua $a, b, dan\ c$ didalam G $(a * b) * c = a * (b * c)$.

3. Element Identitas

   Terdapat elemen idetitas e sedemikian sehingga untuk semua a di dalam G, maka berlaku $\boldsymbol{I} * a = a * \boldsymbol{I} = a$.

4. Invers

   Untuk semua a di dalam G, terdapat element $a' \in G$ sedemikian sehingga $a * a' = a' * a = \boldsymbol{I}$, yang dalam hal ini $\boldsymbol{I}$ adalah element identitas.

Contoh 2.4

Misal grup $(\mathbb{Z}, +)$, dengan $\mathbb{Z}$ adalah himpunan bilangan bulat maka berlaku:

1. Untuk setiap $a, b \in \mathbb{Z}$ maka $(a + b) \in \mathbb{Z}$. Jadi untuk operasi $+$ adalah operasi biner pada $\mathbb{Z}$ atau dengan kata lain, operasi $+$ tertutup
2. Untuk setiap $a, b, c \in \mathbb{Z}$ maka $a + (b + c) = (a + b) + c$. Jadi untuk $\mathbb{Z}$ dengan operasi + memenuhi sifat asosiatif.
3. Terdapat elemen identitas yaitu $0 \in \mathbb{Z}$ sedemikian sehingga $a + 0 = 0 + a = a$, untuk setiap $a \in \mathbb{Z}$.

4. Untuk setiap $a \in \mathbb{Z}$ terdapat a^{-1} yaitu $(-a) \in \mathbb{Z}$ sedemikian sehingga $a + (-a) = -a) + a = 0$, elemen $(-a)$ adala invers a.

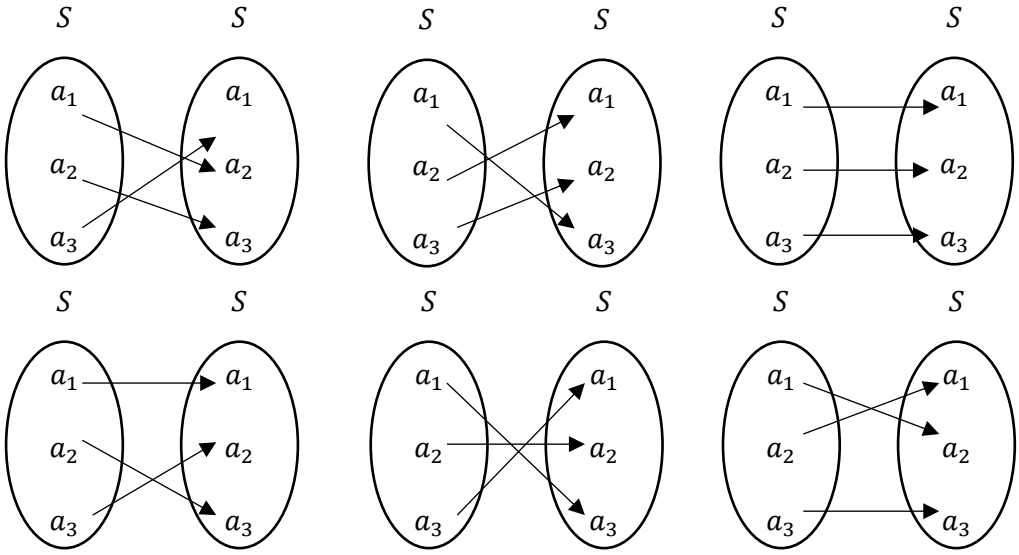
   Apabila ada suatu grup yang memiliki sifat komutatif, grup tersebut dapat disebut dengan grup abelian (Arifin, 2000).

2.5 Grup Simetri

Anggaplah Ω sebagai sebuah himpunan yang tidak kosong, dan S_Ω sebagai himpunan semua fungsi bijektif dari Ω ke Ω, yang juga dikenal sebagai himpunan permutasi Ω. Himpunan S_Ω, dengan operasi " ∘ " atau yang dapat ditulis sebagai $(S_\Omega,\circ)$, membentuk sebuah kelompok. Operasi komposisi merupakan operasi biner pada S_Ω jika dan hanya jika $\sigma: \Omega \to \Omega$ dan $\tau: \Omega \to \Omega$ merupakan fungsi bijektif, maka $\sigma \circ \tau$ merupakan fungsi bijektif dari Ω ke Ω. Oleh karena itu, operasi " ∘ " adalah operasi komposisi fungsi yang bersifat asosiatif. Himpunan S_Ω memiliki elemen $\boldsymbol{I}$ (identitas), yang didefinisikan sebagai $\boldsymbol{I}(a) = a,$. Untuk setiap elemen $a \in \Omega$, setiap permutasi $\sigma: \Omega \to \Omega$ memiliki fungsi invers $\sigma^{-1}: \Omega \to \Omega$ yang memenuhi$\sigma \circ \sigma^{-1} \circ \sigma = \boldsymbol{I}$ (identitas). Dengan demikian, semua aksioma grup terpenuhi oleh $(S_\Omega,\circ)$. Grup $(S_\Omega,\circ)$ dikenal sebagai grup simetri pada himpunan Ω. Elemen-elemen dari S_Ω adalah permutasi dari $\Omega = \{1,2,\ldots,n\}$, dan grup simetri pada Ω dinotasikan sebagai S_Ω dengan orde S_Ω adalah $n!$ (Dummit & Foote, 2004).

Definisi 2.6

Misalkan S adalah sebuah himpunan tak kosong dengan $M(S)$, dan S terdiri dari elemen-elemen $\{a_1, a_2, a_3\}$. Jika kita mengambil semua pemetaan dari S ke S yang merupakan fungsi bijektif, maka daftar fungsi-fungsi bijektif tersebut adalah sebagai berikut:



Gambar 2.1 Fungsi-fungsi Bijektif Dari Himpunan *S ke S*

Maka fungsi-fungsi bijektif dari himpuna S ke S dapat ditulis ke dalam bentuk sikel berikut:

$$\sigma_1 = (a_1\ a_2\ a_3) \qquad \sigma_4 = (a_1)\,(a_2\ a_3)$$

$$\sigma_2 = (a_1\ a_3\ a_2) \qquad \sigma_5 = (a_2)\ (a_1\ a_3)$$

$$\sigma_3 = (a_1)\ (a_2)\ (a_3) \qquad \sigma_6 = (a_3)\ (a_1\ a_2)$$

Misalkan S_3 adalah himpunan semua permutasi bijektif dari $S\ ke\ S$, dengan $S_3 = \{\sigma_1\ \sigma_2\ \sigma_3\ \sigma_4\ \sigma_5\ \sigma_6\}$ Jika kita menggunakan operasi komposisi "$\circ$" pada S_3, struktur (S_3,$\circ$) membentuk grup simetri-3. Hal ini dapat dilihat melalui tabel Cayley berikut:

Tabel 2.1 Tabel Cayley Hasil Operasi Komposisi Dari S_3

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	a_2	a_3	a_1	a_6	a_4	a_5
σ_2	a_3	a_1	a_2	a_5	a_6	a_4
σ_3	a_1	a_2	a_3	a_4	a_5	a_6
σ_4	a_5	a_6	a_4	a_3	a_4	a_2
σ_5	a_6	a_4	a_5	a_2	a_3	a_4
σ_6	a_4	a_5	a_6	a_1	a_2	a_3

Sehingga komposisi S_3 terbukti bahwa:

1. Operasi komposisi S_3 " $\circ$ " mempunyai sifat tertutup pada S_3.
2. Operasi komposisi S_3 " $\circ$ " mempunyai sifat asosiatif pada S_3.
3. S_3 mempunyai identitas terhadap operasi komposisi yaitu σ_3.
4. Untuk setiap unsur di S_3 mempunyai invers pada operasi komposisi " $\circ$ ".

2.6 Order dari suatu elemen

Jika G merupakan grup dan σ adalah suatu elemen dalam G, maka ada suatu bilangan positif terkecil k di mana $\sigma^k = \boldsymbol{I}$, yang dapat disimbolkan sebagai $|\sigma| = k$ (Raisinghania & Aggarwal, 1980).

Contoh 2.6

Grup simetri (S_3) diberikan dengan penggabungan atau kombinasi operasi "$\circ$" atau disimbolkan sebagai $(S_3,\circ)$. Elemen-elemen dari grup simetri S_3 adalah sebagai berikut:

$$\sigma_1 = (a_1\ a_2\ a_3) \qquad \sigma_4 = (a_1)\,(a_2\ a_3)$$

$$\sigma_2 = (a_1\ a_3\ a_2) \qquad \sigma_5 = (a_2)\ (a_1\ a_3)$$

$$\sigma_3 = (a_1)\ (a_2)\ (a_3) \qquad \sigma_6 = (a_3)\ (a_1\ a_2)$$

Unsur σ_3 merupakan identitas, maka

$\sigma_1 \circ \sigma_1 \circ \sigma_1 = \sigma_2 \circ \sigma_1 = \sigma_3$ maka $|\sigma_1| = 3$

$\sigma_2 \circ \sigma_2 \circ \sigma_2 = \sigma_1 \circ \sigma_2 = \sigma_3$ maka $|\sigma_3| = 3$

$|\sigma_3| = 1$

$\sigma_4 \circ \sigma_4 = \sigma_3$ maka $|\sigma_4| = 2$

$\sigma_5 \circ \sigma_5 = \sigma_3$ maka $|\sigma_5| = 2$

$\sigma_6 \circ \sigma_6 = \sigma_3$ maka $|\sigma_6| = 2$

Teorema 2.6

Orde suatu permutasi dalam grup simetri dapat dinyatakan sebagai hasil perkalian sikel-sikel yang tidak memiliki elemen yang sama. Ini merupakan kelipatan persekutuan terkecil (KPK) dari panjang sikel-sikel tersebut (Ruffini, 1799).

Bukti:

Misalkan terdapat sikel yang memiliki panjang n yang memiliki orde n. Dalam kasus ini, asumsikan α dan β adalah dua sikel yang saling lepas dengan panjang m dan n secara berturut-turut. Misal k adalah Kelipatan Persekutuan Terkecil (KPK) dari m dan n. Dalam hal ini, α^k dan β^k akan menjadi permutasi identitas ε karena α dan β bersifat komutatif. Oleh karena itu, $(\alpha\beta)^k = \alpha^k\beta^k = \varepsilon\varepsilon = \varepsilon$ (teorema dan bukti dapat ditemukan dalam buku Contemporary Abstract Algebra).

Maka, orde $|\alpha\beta|$ dapat dinyatakan sebagai t yang membagi k. Selanjutnya, $(\alpha\beta)^t = \alpha^t\beta^t = \varepsilon$, sehingga $\alpha^t = \beta^{-t}$. Namun, jika elemen-elemen dari sikel α tidak ada di dalam sikel β dan sebaliknya, maka disebut bahwa sikel-sikel tersebut saling lepas. Ketika suatu berpangkat tidak ada elemen baru yang ditambahkan. Akan tetapi, jika α^t dan β^t sama atau saling lepas, maka $\alpha^t = \beta^{-t} = \varepsilon$, karena setiap elemen dalam α^t dipetakan ke β^{-t}, dan sebaliknya.

Dari sini, dapat disimpulkan bahwa m dan n harus membagi t, karena orde $|\alpha|$ dan $|\beta|$ membagi t. Oleh karena itu, dapat ditunjukkan bahwa k harus membagi t, dan dengan demikian $k = t$.

Contoh 2.6

$\sigma_1 = (a_1\ a_2\ a_3)$ $\qquad$ $\sigma_4 = (a_1)\,(a_2\ a_3)$

$\sigma_2 = (a_1\ a_3\ a_2)$ $\qquad$ $\sigma_5 = (a_2)\ (a_1\ a_3)$

$\sigma_3 = (a_1)\ (a_2)\ (a_3)$ $\sigma_6 = (a_3)\ (a_1\ a_2)$

Unsur identitas adalah σ_3, maka

Orde dari unsur $\sigma_1 = (a_1\ a_2\ a_3)$ merupakan KPK dari $|\sigma_1|$adalah 3

Orde dari unsur $\sigma_2 = (a_1\ a_3\ a_2)$ merupakan KPK dari $|\sigma_2|$adalah 3

Orde dari unsur $\sigma_3 = (a_1)\ (a_2)\ (a_3)$merupakan KPK dari $|\sigma_3|$adalah 1

Orde dari unsur $\sigma_4 = (a_1)\ (a_2\ a_3)$merupakan KPK dari $|\sigma_4|$adalah 2

Orde dari unsur $\sigma_5 = (a_2)\ (a_1\ a_3)$merupakan KPK dari $|\sigma_5|$adalah 2

Orde dari unsur $\sigma_6 = (a_3)\ (a_1\ a_2)$merupakan KPK dari $|\sigma_6|$adalah 2

Jadi dapat disimpukan

$|\sigma_3| = 1, |\sigma_4| = |\sigma_5| = |\sigma_6| = 2,$ dan $|\sigma_1| = |\sigma_2| = 2$

2.7 Kriptografi

Kriptografi (*cryptography*) memiliki asal kata dari bahasa Yunani, terbentuk dari Cryptos yang berarti "*secret*" (rahasia) dan Graphein yang berarti "*writing*" (penulisan rahasia) (Munir, 2019). Definisi yang ditemukan dalam buku-buku lama sebelum tahun 1980-an menyatakan bahwa kriptografi adalah ilmu dan seni yang bertujuan menjaga kerahasiaan pesan dengan cara mengubahnya ke dalam bentuk yang dapat dipahami kembali maknanya (Meyer & Matyas, 1982). Beberapa sumber lain juga mengajukan definisi kriptografi sebagai bidang ilmu yang mempelajari metode-metode matematika yang terkait dengan keamanan informasi, termasuk meliputi kerahasiaan, integritas data, dan otentikasi. Ini merupakan perbandingan dengan definisi sebelumnya. (A. Menezes, Van Oorschot, & S. Vanstone, 1996).

Proses menjaga keamanan pesan menggunakan kriptografi melibatkan langkah-langkah berikut: pertama, teks pesan asli (*plaintext*) akan diubah menjadi

teks terenkripsi (*ciphertext*) menggunakan algoritma kriptografi dan kunci rahasia. Pengirim pesan bertanggung jawab untuk menentukan kunci rahasia yang akan digunakan. Selanjutnya, melalui operasi matematika yang disebut enkripsi, angka-angka dalam teks pesan diubah menjadi bentuk teks terenkripsi. Teks terenkripsi dan kunci akan dikirimkan kepada penerima pesan. Penerima dapat melakukan proses dekripsi untuk mengembalikan teks terenkripsi menjadi teks asli (*plaintext*) (Rachmawati, Budiman, & Aulia, 2018). Enkripsi (*encryption*) adalah proses penyandian pesan, sedangkan dekripsi (*decryption*) adalah proses pengembalian pesan. Pesan yang belum terenkripsi disebut sebagai pesan asli atau *plaintext*, sementara pesan yang telah melalui tahap enkripsi disebut *ciphertext* (Mukhtar, 2018).

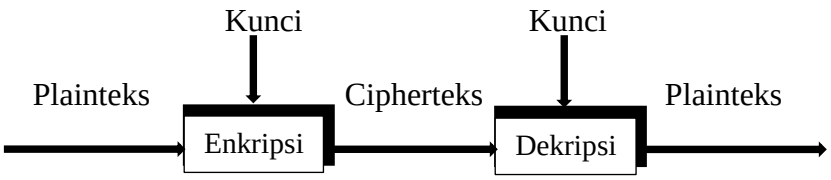
2.8 Algoritma Kriptografi

Algoritma kriptografi adalah serangkaian langkah atau urutan yang didesain secara matematis untuk mengamankan pesan dari pihak yang tidak berwenang. Tujuan dari algoritma kriptografi adalah menyembunyikan isi pesan agar hanya dapat diakses oleh pihak yang sah atau berwenang. Dengan demikian, algoritma kriptografi digunakan untuk melindungi keamanan pesan kepada pihak tertentu (Ariyus, 2008). Algoritma kriptografi dapat dibagi menjadi dua kelompok berdasarkan kunci yang digunakan untuk enkripsi. Kelompok pertama adalah algoritma kriptografi kunci simetri, di mana enkripsi dan dekripsi menggunakan kunci yang sama. Kelompok kedua adalah algoritma kriptografi kunci asimetris, di mana enkripsi dan dekripsi menggunakan pasangan kunci publik dan kunci privat yang berbeda.

Istilah lain untuk kriptografi kunci-simetris adalah kriptografi kunci-pribadi (*private-key cryptography*) atau kriptografi konvensional (*conventional cryptography*). Dalam konteks ini, diasumsikan bahwa pengirim dan penerima pesan telah memiliki kunci yang sama sebelum bertukar pesan. Bagaimana kunci tersebut diperoleh oleh pengirim dan penerima tidak dibahas dalam penjelasan ini.

1. Algoritma Simetri

Keamanan algoritma simetris terletak pada kerahasiaan kuncinya. Jika kunci tersebut diketahui oleh pihak lain, mereka dapat melakukan dekripsi terhadap pesan yang terenkripsi. Saat ini, standar yang paling umum digunakan adalah AES (*Advanced Encryption Standard*) (Munir, 2019).



Gambar 2.2 Algoritma Simetri (Munir, 2019)

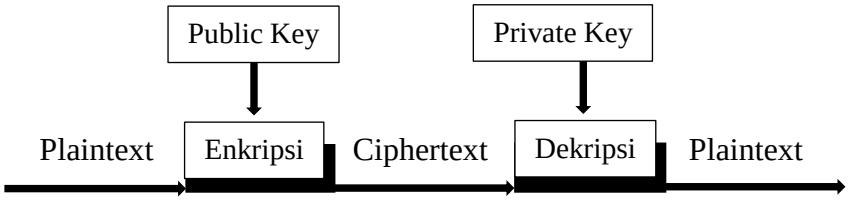
2. Algoritma Asimetri

Algoritma asimetri juga dikenal sebagai algoritma kunci publik, yang berarti bahwa kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Dalam algoritma asimetris kunci publik, terdapat dua bagian utama, yaitu:

a. Kunci umum (*public key*): kunci yang boleh semua orang tahu (dipublikasi).
b. Kunci rahasia (*private key*): kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang).

Kunci-kunci tersebut memiliki hubungan yang saling terkait. Dengan menggunakan kunci publik, seseorang dapat mengenkripsi pesan tetapi tidak dapat mendekripsinya. Hanya individu yang memiliki kunci pribadi yang sesuai yang

dapat melakukan dekripsi pesan tersebut. Beberapa contoh algoritma yang menggunakan kunci publik termasuk DSA (*Digital Signature Algorithm*), RSA, DH (*Diffie-Hellman*), ECC (*Elliptic Curve Cryptography*), Kriptografi Quantum, dan sebagainya.



Gambar 2.3 Algoritma Asimetri (Munir, 2019)

3. Fungsi Hash

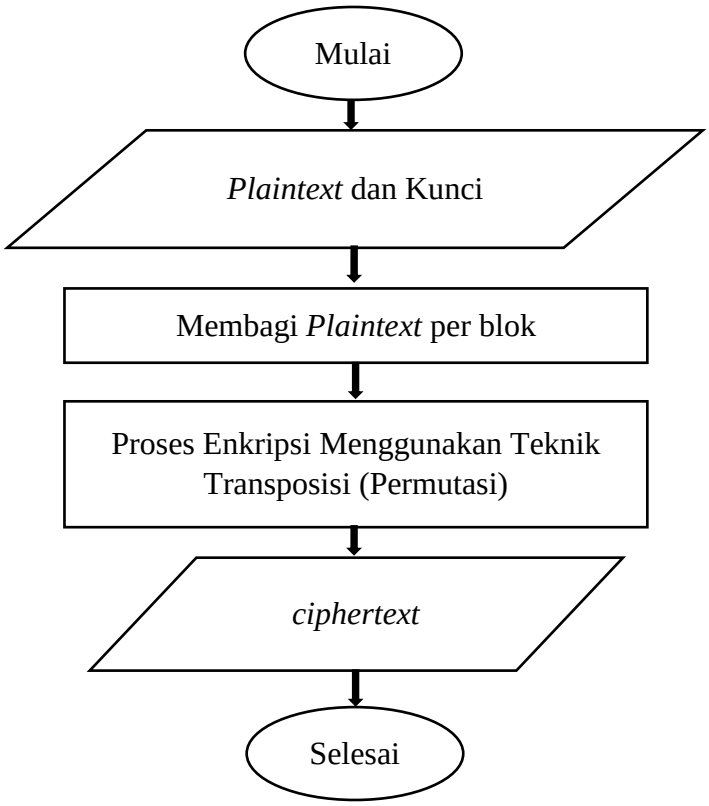
Fungsi hash adalah suatu fungsi matematika yang mengambil input berupa data dengan panjang yang bervariasi dan mengubahnya menjadi representasi biner dengan panjang yang tetap. Fungsi ini juga dikenal dengan beberapa istilah seperti fungsi satu arah (*one-way function*), *fingerprint*, *message digest*, fungsi kompresi, dan *message authentication code* (MAC) (Ariyus, 2008).

2.9 Teknik Transposisi (Permutasi)

Teknik permutasi transposisi melibatkan penggunaan permutasi karakter untuk mengubah pesan asli sehingga tidak dapat dibaca, kecuali oleh pihak yang memiliki kunci aksesnya (Ariyus, 2008). Algoritma enkripsi menggunakan teknik transposisi (permutasi) dengan melakukan permutasi t pada teks asli (*plaintext*). Sebaliknya, dalam proses dekripsi, algoritma menggunakan invers dari permutasi t^{-1} pada teks terenkripsi (*ciphertext*).. (Sadikin, 2012).

1. Proses Enkripsi Teknik Transpormasi (Permutasi).

Berikut ini adalah *flowchart* yang menjelaskan proses enkripsi menggunakan teknik transformasi (permutasi):



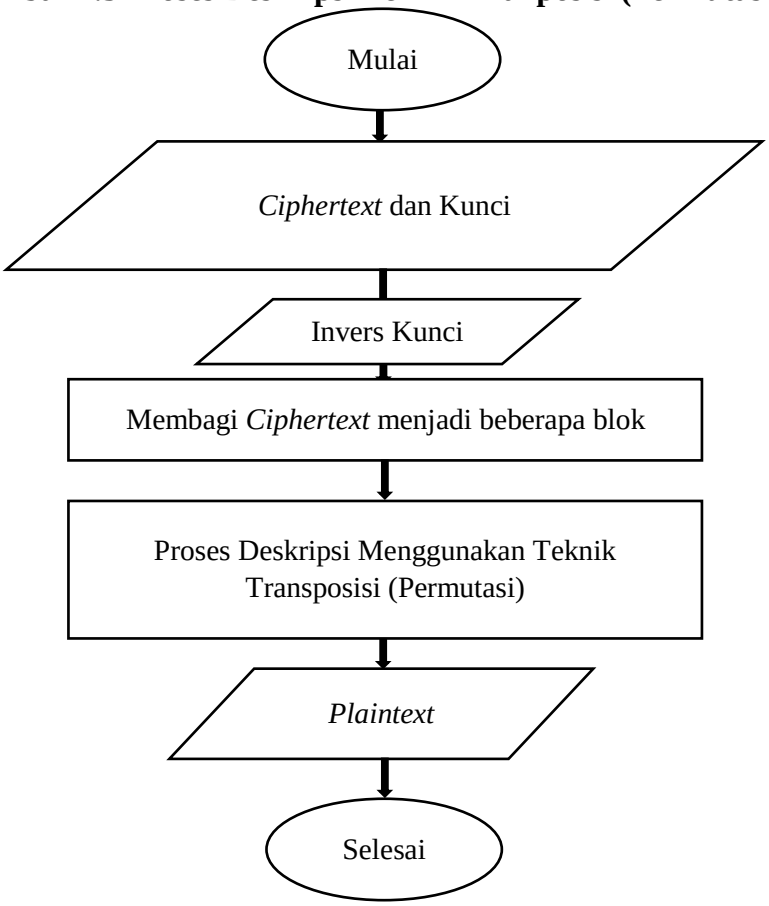
Gambar 2.4 Proses Enkripsi Teknik Tranposisi(Permutasi)

Proses enkripsi permutasi dimulai dengan membagi pesan plaintext menjadi blok-blok huruf. Pada teknik transposisi (permutasi), kunci yang digunakan memiliki format n-permutasi. Dengan menggunakan cara ini, pesan asli tidak dapat dibaca kecuali pihak yang memiliki invers kunci untuk mengembalikan pesan ke bentuk aslinya.

2. Proses Dekripsi Teknik Transposisi (Permutasi)

Pada prinsipnya, proses dekripsi dan enkripsi hampir sama, akan tetapi pada tahap dekripsi melalui pengoprasian invers permutasi . Proses dekripsi dengan menggunakan teknik transposisi (permutasi) dapat diilustrasikan melalui diagram alur (flowchart) berikut ini.

Gambar 2.5 Proses Deskripsi Teknik Tranposisi (Permutasi)



Adapun kunci untuk melakukan permutasi kode:

x	a_1	a_2	a_3	a_4	a_5
$t(x)$	a_3	a_5	a_1	a_2	a_4

(2.1)

Kemudian untuk kunci invers di atas adalah:

x	a_1	a_2	a_3	a_4	a_5
$t^{-1}(x)$	a_3	a_4	a_1	a_5	a_2

(2.2)

Seandaiya kita akan melakuka permutasi terhadap kalimat di bawah ini:

SAYA SEDANG BERUSAHA CEPAT SELESAI

Langkah awal, kalimat di atas akan dipecah menjadi beberapa kata yang akan membentuk 7 blok. Jika ada kekurangan huruf dalam setiap kata, karakter tambahan dapat ditambahkan sesuai keinginan. Sebagai contoh, karakter spasi akan diwakili dengan "sp". Hal ini bertujuan untuk membuat analisis kode tersebut menjadi lebih sulit.

SAYAsp	SEDAN	GspBER
USAHA	spCEPA	TspSEL
ESAIsp		

Setelah membaginya menjadi 7 blok, menggunakan kunci (2.1) di atas, setiap blok akan mengalami transformasi sebagai berikut:

Blok I : $T = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_5 & a_1 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ S & A & Y & A & \$ \\ a_3 & a_5 & a_1 & a_2 & a_4 \\ Y & \$ & S & A & A \end{pmatrix}$

= YspSAA

Blok II: $T = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_5 & a_1 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ S & E & D & A & N \\ a_3 & a_5 & a_1 & a_2 & a_4 \\ D & N & S & E & A \end{pmatrix}$

= DNSEA

Blok III: $T = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_5 & a_1 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ G & \$ & B & E & R \\ a_3 & a_5 & a_1 & a_2 & a_4 \\ B & R & G & \$ & E \end{pmatrix}$

= BRGspE

Blok IV: $T = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_5 & a_1 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ U & S & A & H & A \\ a_3 & a_5 & a_1 & a_2 & a_4 \\ A & A & U & S & H \end{pmatrix}$

= AAUSH

Blok V: $T = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_5 & a_1 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \$ & C & E & P & A \\ a_3 & a_5 & a_1 & a_2 & a_4 \\ E & A & \$ & C & P \end{pmatrix}$

= EAspCP

Blok VI: $T = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_5 & a_1 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ T & \$ & S & E & L \\ a_3 & a_5 & a_1 & a_2 & a_4 \\ S & L & T & \$ & E \end{pmatrix}$

= SLTspE

Blok VI: $T = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_5 & a_1 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ E & S & A & I & \$ \\ a_3 & a_5 & a_1 & a_2 & a_4 \\ A & \$ & E & S & I \end{pmatrix}$

= AspESI

Jadi cipherteks yang dihasilkan

YspSAADNSEABRGspEAAUSHEAspCPSLTspEAspESI

Untuk mengembalikan *ciphertext* ke bentuk teks asli, dilakukan invers terhadap *ciphertext* dengan mengikuti kunci (2.2) di atas. Dalam hal ini, t adalah anggota dari T, dan t^{-1} merupakan anggota dari invers T^{-1}.

Ada berbagai pola yang dapat digunakan dalam teknik transposisi (permutasi) untuk menyembunyikan pesan . Kombinasi pola tersebut menjadi dasar bagi pengembangan algoritma kriptografi yang kita kenal saat ini, yang sering disebut sebagai kriptografi modern.

2.10 Protokol Perjanjian Kunci

Protokol perjanjian kunci merupakan sebuah skema enkripsi yang mengatasi permasalahan negosiasi kunci rahasia antara pengirim dan penerima yang telah menyetujui kunci tersebut. Dalam teknik ini, pengirim dan penerima saling menukar parameter pesan sebagai bagian dari prosesnya. Meskipun parameter tersebut mungkin diketahui oleh publik tapi dengan adannya protokol perjanjian kunci maka pesan tidak bisa diketahui ole publik (Musthofa & Lestari, 2014). Protokol perjanjian kunci Stickel adalah salah satu algoritma yang terkenal dalam protokol perjanjian kunci. Algoritma ini mengadopsi grup non-komutatif sebagai landasan utamanya (Myasnikov, Shpilrain, & Ushakov, 2008). Protokol Diffie-Hellman adalah salah satu contoh perjanjian kunci yang relatif sederhana dan pertama kali diperkenalkan pada tahun 1976.

Protokol perjanjian kunci Diffie-Hellman melibatkan pengirim dan penerima dalam memilih bilangan asli secara acak. Pengirim memilih bilangan M yang memenuhi syarat $M < R$ dan $N < S$, dan mengirim pesan $r = {\sigma_1}^M \circ {\sigma_2}^N$. Penerima juga memilih bilangan P yang memenuhi syarat $P < R$ dan $Q < S$, dan

mengirim pesan $s = {\sigma_1}^P \circ {\sigma_2}^Q$. Kedua belah pihak kemudian menghitung $K_1 dan\ K_2$ menggunakan rumus yang diberikan.

$$T_1 = {\sigma_1}^M \circ s \circ {\sigma_2}^N$$

dan

$$T_2 = {\sigma_1}^P \circ r \circ {\sigma_2}^Q$$

Sehingga dapat diperoleh kunci yang disepakati oleh kedua belah pihak

$$T_1 = {\sigma_1}^M \circ s \circ {\sigma_2}^N = {\sigma_1}^M {\sigma_1}^P \circ {\sigma_2}^Q \circ s \circ {\sigma_2}^N$$

$$T_1 = {\sigma_1}^{M+P} \circ {\sigma_2}^{N+Q} = {\sigma_1}^P \circ r \circ {\sigma_2}^Q = K_2$$

Jadi, $T = T_1 = T_2$

2.11 Hill Cipher

Hill Cipher adalah suatu algoritma cipher poligrafik yang ditemukan oleh Lester S. Hill pada tahun 1929. Algoritma ini menggunakan transformasi linier dan merupakan algoritma cipher blok di mana *plaintext* dibagi menjadi blok-blok dengan ukuran yang sama. Hill Cipher menggunakan matriks transformasi sebagai kunci untuk melaksanakan proses enkripsi dan dekripsi. Untuk melakukan dekripsi pesan, penerima perlu menghitung invers matriks, karena invers tersebut dapat digunakan untuk mengubah *ciphertext* menjadi *plaintext*. Namun, perhitungan matriks balikan hanya dapat dilakukan jika matriks kunci diketahui. Secara matematik, proses enkripsi mengubah *plaintext* $P = (p_1, p_2, \dots, p_n)$ dengan menggunakan matriks kunci $K = k_{ij}$ menjadi *ciphertext* $C = (c_1, c_2, \dots, c_n)$.

$$\begin{pmatrix} c_1 \\ c_2 \\ c_n \end{pmatrix} = \begin{pmatrix} k_{11} & \dots\dots & k_{1n} \\ \vdots & k_{22} & \vdots \\ k_{n1} & \dots\dots & k_{nn} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_n \end{pmatrix} mod\ 26$$

Maka dapat ditulis dengan sistem persamaan lanjar dalam modulus 26

$$c_1 = (k_{11}p_1 + k_{12}p_2 + \cdots + k_{1n}p_n) mod\ 26$$

$$c_2 = (k_{21}p_1 + \ k_{22}p_2 + \cdots + k_{2n}p_n) mod\ 26$$

… … … … … … … … … … … ….

$$c_n = (k_{n1}p_1 + \ k_{n2}p_2 + \cdots + k_{nn}p_n) mod\ 26$$

Atau dalam jika dinotasikan mejadi

$$C = K.P\ mod\ 26$$

Keterangan:

K : Matriks Kunci k_n

P : *Plaintext* p_n

C : *Ciphertetx* c_n

Sedangkan deskripsi *ciphertext* $C = (c_1, c_2, \dots , c_n)$ dengan matiks kunci $K^{-1} = [k_{ij}]^{-1}$ menggasilkan *plaintext* $P = C = (p_1, p_2, \dots , p_n)$ dinyatakan sebagai

$$p_1 = (k'_{11}c_1 + \ k'_{12}c_2 + \cdots + k'_{1n}c_n) mod\ 26$$

$$p_2 = (k'_{21}c_1 + \ k'_{22}c_2 + \cdots + k'_{2n}c_n) mod\ 26$$

… … … … … … … … … … … ….

$$p_n = (k'_{n1}c_1 + \ k'_{n2}c_2 + \cdots + k'_{nn}c_n) mod\ 26$$

Atau jika dinotasikan menjadi

$$P = K^{-1}.C\ mod\ 26$$

Salah satu aspek yang sangat penting dalam Hill Cipher adalah perhitungan matriks balikan (K^{-1}) sedemikian sehingga $KK^{-1} = \boldsymbol{I}$, di mana *I* adalah matriks identitas. Dalam aritmetika modulo, perhitungan matriks balikan harus menghasilkan bilangan bulat positif, dan tidak boleh ada bilangan negatif atau pecahan. Jika terdapat terdapat hasil perhitungan hasil negatif maka bilangan hasil tersebut perlu diganti degan bilangan bulat positif. Demikian pula, jika ada pecahan $\frac{1}{a}$, maka a^{-1} diganti dengan invers a dalam modulo 26. Perhitungan matriks balikan

dalam Hill Cipher mirip dengan metode perhitungan matriks balikan yang diajarkan dalam materi aljabar lanjar.

Contoh:

Matriks enkripsi yang memiliki inverse pada Z_{26}:

$$\begin{bmatrix}11 & 8\\ 3 & 7\end{bmatrix}^{-1} = \begin{bmatrix}7 & 18\\ 23 & 11\end{bmatrix}$$

Karena,

$$\begin{bmatrix}11 & 8\\ 3 & 7\end{bmatrix}\begin{bmatrix}7 & 18\\ 23 & 11\end{bmatrix} = \begin{bmatrix}11\times 7+8\times 23 & 11\times 18+8\times 11\\ 3\times 7+7\times 23 & 3\times 18+7\times 11\end{bmatrix}$$

$$=\begin{bmatrix}261 & 286\\ 182 & 131\end{bmatrix}$$

$$=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}.$$

Enkripsi melibatkan transformasi karakter yang dapat dibaca (*plaintext*) akan berubah ke bentuk (*ciphertext*) yang tidak dapat diidentifikasi. Untuk mencapai hal ini, diperlukan perubahan abjad dengan penambahan tiga karakter tambahan, dan kemudian dikonversikan menjadi angka dengan langkah-langkah berikut ini. Dalam proses ini menggunakan modulo 26 memiliki dua tahapan, untuk tahapan pertama pada enkripsi dilakukan sesuai Hill Cipher biasa yaitu dengan persamaan sebagai berikut:

$$C = K.P \ mod\ 26$$

C = *Ciphertetx*

K = Kunci

P = *Plaintexts*

Sebagai contoh diberikan kata JULY kemudian dienkripsi pada metode Hill Cipher modulo 26 sebagai berikut:

Tabel 2.2 Tabel konversi Numerik Alfabet Modulo 26

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

P = JULY

Kemudian dikonversikan menjadi angka:

P = 9,20,11,24

Kemudian menentukan matriks kunci:

$$K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$$

Kemudian melakukan perhitungan berikut:

$$\begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} . [9 \quad 20] = (99 + 60, 72 + 140) mod\ 26 = (3,4) \rightarrow DE$$

$$\begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} . [11 \quad 24] = (121 + 72, 192 + 168) mod\ 26 = (11,22) \rightarrow LW$$

Maka enkripsi pesan JULY menjadi DELW

Untuk mendeskripsikan, dilakukan dengan cara sebagai berikut:

$$P = C . K^{-1}\ mod\ 26$$

$$\begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} . [3 \quad 4]\ mod\ 26 = (21 + 92, 72 + 44) = (133,116) mod\ 26 =$$

$$(9,12) \rightarrow JU$$

$$\begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} . [11 \quad 22]\ mod\ 26 = (77 + 506, 198 + 242) = (583,440) mod\ 26 =$$

$$(11,24) \rightarrow LY$$

Dengan demikian, *plaintext* dapat dikembalikan ke bentuk aslinya. Penjelasan ini menunjukkan bahwa dekripsi hanya dapat dilakukan jika matriks K

memiliki invers. Suatu matriks K memiliki invers jika dan hanya jika determinannya tidak sama dengan nol. Namun, karena bedasarkan modulus 26, matriks K akan memiliki invers modulo 26 jika dan hanya jika determinannya modulo 26 adalah 1, yaitu $(\det K, 26) = 1$.

2.12 Kajian Integrasi Topik dengan Al-Qur'an/Hadis

Keamanan dan kerahasiaan data menjadi faktor yang sangat penting ketika data tersebut memiliki nilai yang signifikan. Hal ini juga berlaku untuk pesan yang ditujukan kepada orang tertentu, yang biasa disebut sebagai pesan rahasia. Pesan rahasia adalah pesan yang hanya boleh dilihat oleh penerima yang dituju. Pesan rahasia juga dapat dianggap sebagai amanah yang harus menjaga kerahasiaannya hingga sampai ke tangan penerima. Seperti yang dinyatakan dalam Al-Qur'an Surah Al-Anfal ayat 27, Allah SWT berfirman:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَخُوْنُوا اللّٰهَ وَالرَّسُوْلَ وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ

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

Menurut ayat 27 dalam Surah Al-Anfal, Allah SWT memberikan larangan untuk mengkhianati amanah-amanah yang telah dipercayakan kepada kita. Larangan ini mencakup ketidakpatuhan terhadap kewajiban yang ditetapkan oleh Rasulullah, serta pengkhianatan terhadap amanat yang telah diberikan kepada kita. Dengan demikian, kita diingatkan untuk menjaga integritas dan kepercayaan yang diberikan kepada kita, baik dalam hal kewajiban agama maupun tanggung jawab dunia.

Terkait dengan ayat tersebut, Rasulullah SAW juga memberikan penjelasan dan keterangan dalam sebuah hadits yang diriwayatkan oleh Abu Daud. Hadits tersebut menjelaskan hal-hal sebagai berikut:

حَدَّثَنَا مُحَمَّدُ بْنُ الْعَلاَءِ، وَأَحْمَدُ بْنُ إِبْرَاهِيمَ، قَالاَ حَدَّثَنَا طَلْقُ بْنُ غَنَّامٍ، عَنْ شَرِيكٍ، - قَالَ ابْنُ الْعَلاَءِ وَقَيْسٍ عَنْ أَبِي حُسَيْنٍ، عَنْ أَبِي صَالِحٍ، عَنْ أَبِي هُرَيْرَةَ، قَالَ قَالَ رَسُولُ اللَّهِ صلى الله عليه وسلم " أَدِّ الأَمَانَةَ إِلَى مَنِ ائْتَمَنَكَ وَلاَ تَخُنْ مَنْ (رواه ابو داود,٣٥٣٥) خَانَكَ "

"Tunaikanlah amanah kepada orang yang mempercayaimu dan jangan engkau mengkhianati orang yang mengkhianatimu!" (HR. Abu Daud) (Katsir, 2004)

Hadits ini mencakup berbagai jenis amanah yang harus dipenuhi oleh seseorang yang diberikan tanggung jawab atasnya. Amat penting untuk melaksanakan amanah tersebut, baik berupa kewajiban kepada Allah SWT, seperti menjalankan sholat, membayar zakat, melaksanakan kaffarat, memenuhi nadzar, menjalankan puasa, dan lain sebagainya, maupun amanah-amanah lainnya yang dipercayakan kepada seseorang dan tidak dilihat oleh orang lain (Ad-Dimasyqi, 2001). Orang yang tidak memenuhi amanah-amanah tersebut di dunia ini akan dimintai pertanggungjawabannya di hari kiamat nanti. Manusia diperintahkan untuk menjalankan amanah, termasuk menegakkan hukum yang adil di antara sesama manusia, sesuai dengan perintah-perintah dan syariat yang sempurna (Al-Sheik, 1994).

Amanah dimulai dengan kaitannya dengan fitrah manusia, di mana bumi, langit, dan gunung-gunung tidak mau mengemban amanah tersebut, tetapi manusia mau menerima beban amanah tersebut. Amanah yang dimaksud adalah amanah hidayah, pengetahuan tentang Allah SWT, dan iman kepada-Nya, yang melibatkan niat, kehendak hati, kesungguhan, dan petunjuk. Selain manusia, makhluk lain juga

diberi ilham oleh Allah SWT untuk beriman, mengikuti petunjuk-Nya, beribadah kepada-Nya, dan taat kepada-Nya. Oleh karena itu, hanya manusia yang diberikan tanggung jawab untuk mengikuti fitrah, menggunakan akal, mencapai pengetahuan tentang-Nya, menetapkan tujuan hidup, dan berusaha mencapai kedekatan dengan Allah SWT. Inilah amanah-amanah yang Allah SWT perintahkan untuk dilaksanakan dan disebutkan secara umum dalam tafsir (Sayyid, 2001).

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian ini menggunakan metode studi kepustakaan, jenis penelitian yang melibatkan pengumpulan dan analisis berbagai buku, *leaflet*, majalah. Proses pengumpulan dan analisis melibatkan berbagai sumber literatur seperti jurnal ilmiah, skripsi atau tesis, dan buku yang berkaitan tentang enkripsi Hill Cipher dan konsep grup simetri.

3.2 Pra Penelitian

Pada tahap awal penelitian, dilakukan pemilihan masalah dan penentuan judul penelitian. Setelah masalah dan judul disetujui oleh pembimbing, langkah selanjutnya adalah menyusun pendahuluan guna mendapatkan pemahaman awal mengenai modifikasi Hill Cipher menggunakan grup simetri sebagai metode pengamanan pesan teks. Selanjutnya, dilakukan pengumpulan data dari berbagai sumber referensi teori yang relevan terkait penyandian modifikasi Hill Cipher dan konsep grup simetri.

3.3 Tahapan Penelitian

Tahapan penelitian yang dilakukan dalam penelitian ini adalah sebagai berikut:

Membuat algoritma modifikasi Hill Cipher dengan menggunakan grup simetri S_n dan mengimplementasikannya dengan menggunakan grup simetri S_6.

1. Proses enkripsi menggunakan Hill Cipher yang dimodifikasi dengan memanfaatkan grup simetri sebagai berikut:
   a. Melakukan penentuan *plaintext* serta membentuk kunci dengan algoritma perjanjian kunci *stickel* terhadap grup simetri.

b. Memisahkan *plaintext* menjadi blok-blok tertentu dan melakukan enkripsi menggunakan kunci dari grup simetri dengan menerapkan teknik transposisi (permutasi), yang menghasilkan *plaintext* yang sudah diacak oleh grup simetri.

c. Kemudian, langkah selanjutnya yaitu menentukan kunci dari matriks kunci untuk melakukan operasi Hill Cipher.

d. Mengoprasikan *plaintext* yang sudah diacak dengan grup simetri dengan mekalikan dengan matriks kunci Hill Cipher, sehingga akan didapatkan *ciphertext* dari hasil modifikasi Hill Cipher menggunaka grup simetri.

2. Proses dekripsi menggunakan Hill Cipher yang dimodifikasi dengan memanfaatkan grup simetri dilakukan dengan langkah-langkah berikut:

a. *Ciphertext* akhir akan dioperasikan dengan invers matrik kunci yang sudah disepakati.

b. Hasil perhitungan dekripsi invers matriks dari metode Hill Cipher akan diopersikan dengan kunci invers grup simetri, maka akan didapatkan kembali *plaintext* awal.

BAB IV
PEMBAHASAN

4.1 Proses Enkripsi dan Deskripsi Hill Cipher

Proses enkripsi dan deskripsi Hill Cipher adalah dengan mengubah setiap karakter (alfabet) menjadi bilangan bulat positif, serta penambahan karakter sp (spasi) pada karakter {A,….,Z,sp} ke {0,….,26} sehingga jumlah karakter menjadi 27, maka dapat dirumuskan menjadi

$$C = K.P \ mod\ 27$$

Kemudian dekripsi menjadi

$$P = K^{-1}\ .\ C\ mod\ 27$$

Matriks kunci dinotasikan dengan K sebagai berikut:

$$K = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n1} & \ldots & k_{nn} \end{bmatrix}$$

Matriks K berupa matriks invertible (*multiplicative invers*) K^{-1} sehingga $K \times K^{-1} = \boldsymbol{I}$.

Keterangan:

C : *Ciphertext*

P : *Plaintext*

K : Matriks Kunci

K^{-1} : Invers Matriks Kunci

Algoritma Hill Cipher melibatkan sejumlah parameter yang penting dalam proses enkripsi dan dekripsi, termasuk:

1. *Plaintext* adalah pesan asli yang hanya diketahui oleh pengirim, sedangkan penerima akan mengetahui isi pesan melalui proses dekripsi.

2. Kemudian matriks $P_{1\times a}$ diubah menjadi $P_{n\times m}$ akan disesuaikan ukurannya matriks kunci yang digunakan.

$$jadi\ P_{n\times m} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n1} & \dots & p_{nm} \end{bmatrix} dimana\ p_{11}, p_{12}, p_{13}, \dots\dots . p_{nm}\ \in Z$$

3. Parameter K digunakan sebagai matriks kunci untuk proses enkripsi. Untuk memastikan pesan dapat dikembalikan melalui bentuk aslinya saat proses dekripsi, matriks kunci $K_{n\times n}$ harus memiliki invers yang memenuhi persyaratan $(det(K_{n\times n}) \neq 0$, dan semua elemen dalam matriks kunci $K_{n\times n}$ harus berupa bilangan bulat.

$$jadi\ K_{n\times n} = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n1} & \dots & k_{nn} \end{bmatrix} dimana\ k_{11}, k_{12}, k_{13}, \dots\dots . k_{nn}\ \in Z$$

4. Selanjutnya, matriks kunci $(K_{n\times n})$ akan dikalikan dengan matriks *plainteks* $(P_{n\times n})$, dan hasilnya akan dimodulokan 27 dengan penambahan karakter spasi di dalamnya. Hasil perkalian ini akan disimbolkan dalam bentuk matriks.

$$C_{(nm)} = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n1} & \dots & k_{nn} \end{bmatrix} \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n1} & \dots & p_{nm} \end{bmatrix} mod\ 27$$

$$C_{n\times m} = \begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ s_{n1} & s_{n1} & \dots & s_{nm} \end{bmatrix}$$

Dengan $C_{p(11)} = k_{11}, p_{11} + k_{12}, p_{21} + \cdots + k_{1n}, p_{n1}$

5. Pengubahan matriks $C_{(nm)}$ menjadi matriks baris (T)

6. *Chipertext* berupa pesan yang sudah disandikan oleh pengirim.

$$C_{(nm)} = [\ c_1\ \ c_2\ \ c_3\ \dots .\ \ c_{nm}]$$

7. Proses deskripsi *ciphertext* melibatkan konversi *ciphertext* ke dalam bentuk matriks baris yang terdiri dari elemen-elemen nilai numerik yang ekuivalen.
8. Matriks $C_{(nm)}$ diubah menjadi matriks dengan ukuran yang sama dengan matriks kunci yang digunakan.
9. Dengan mengalikan matriks invers kunci (K^{-1}) dengan matriks *ciphertext*, kemudian melakukan modulokan 27, hasil dari perkalian invers matriks tersebut dibentuk matriks baris. Hasil dari proses dekripsi ini akan menghasilkan *plaintext* pada pesan yang akan dikirim.

Jadi terbukti proses di atas memenuhi fungsi enkripsi dekripsi dari Hill Cipher. Berikut contoh penggunaan algoritma Hill Cipher

Misal diberikan *Plaintext*: DONI YOGA PRATAMA

Tabel 4.1 Tabel konversi Numerik Alfabet Modulo 27

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

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	sp
13	14	15	16	17	18	19	20	21	22	23	24	25	26

A. Simulasi enkripsi Hill Cipher Pengirim Pesan

1) Ubah *plaintext* $P =$ DONI YOGA PRATAMA menjadi bilangan bulat di mana sp (*spaces*) bernilai 27

Tabel 4.2 Tabel Konversi *Plaintext*

D	O	N	I	Sp	Y	O	G	A
3	14	13	8	26	24	14	6	0
sp	P	R	A	T	A	M	A	sp
26	15	17	0	19	0	12	0	26

2) Pembentukan matriks (P) dari bentuk bilangan bulat *plaintext* dengan ukuran 3×6, matriks dibetuk berukuran 3×6 karena mengikuti matriks kuncinya.

$$P = \begin{bmatrix} 3 & 8 & 14 & 26 & 0 & 12 \\ 14 & 26 & 6 & 15 & 19 & 0 \\ 13 & 24 & 0 & 17 & 0 & 26 \end{bmatrix}$$

3) Kalikan matriks *plaintext* (P) dengan kunci K, misal $K = \begin{bmatrix} 3 & 4 & 1 \\ 2 & 1 & 1 \\ 6 & 2 & 3 \end{bmatrix}$

$$C = K \cdot P \; mod \; 27$$

$$C = \begin{bmatrix} 3 & 4 & 1 \\ 2 & 1 & 1 \\ 6 & 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 3 & 8 & 14 & 26 & 0 & 12 \\ 14 & 26 & 6 & 15 & 19 & 0 \\ 13 & 24 & 0 & 17 & 0 & 26 \end{bmatrix} \; mod \; 27$$

$$C = \begin{bmatrix} 78 & 152 & 66 & 155 & 76 & 62 \\ 33 & 66 & 34 & 84 & 19 & 50 \\ 85 & 172 & 96 & 237 & 38 & 150 \end{bmatrix} \; mod \; 27$$

$$C = \begin{bmatrix} 24 & 17 & 12 & 20 & 22 & 8 \\ 6 & 12 & 7 & 3 & 19 & 23 \\ 4 & 10 & 15 & 21 & 11 & 15 \end{bmatrix}$$

4) Ubah kembali matriks (C) kedalam bentuk alfabetnya dan didapatkan *ciphertext.*

5) Maka didapat $C = YGERMKMHPUDVWTLIXP$ sebagai *ciphertext* dalam proses enkripsi Hill Cipher

B. Simulasi deskripsi Hill Cipher Penerima Pesan

1) Ubah *ciphertext* $C = YGERMKMHPUDVWTLIXP$ menjadi bilangan bulat kembali.

Tabel 4.3 Tabel Konversi *Ciphertext*

Y	G	E	R	M	K	M	H	P
24	6	4	17	12	10	12	7	15
U	D	V	W	T	L	I	X	P
20	3	21	22	19	11	8	23	15

2) Buat mariks C dari bilangan bulat *ciphertext.*

$$C = \begin{bmatrix} 24 & 17 & 12 & 20 & 22 & 8 \\ 6 & 12 & 7 & 3 & 19 & 23 \\ 4 & 10 & 15 & 21 & 11 & 15 \end{bmatrix}$$

3) Mengalikan matriks C dengan K^{-1} dengan kunci deskripsi $K^{-1} = \begin{bmatrix} 1 & -10 & 3 \\ 0 & 3 & -1 \\ -2 & 18 & -5 \end{bmatrix} mod\ 27$

$$P = K^{-1}\ .\ C\ mod\ 27$$

$$P = \begin{bmatrix} 1 & -10 & 3 \\ 0 & 3 & -1 \\ -2 & 18 & -5 \end{bmatrix} \cdot \begin{bmatrix} 24 & 17 & 12 & 20 & 22 & 8 \\ 6 & 12 & 7 & 3 & 19 & 23 \\ 4 & 10 & 15 & 21 & 11 & 15 \end{bmatrix} mod\ 27$$

$$P = \begin{bmatrix} -24 & -73 & -13 & 53 & -135 & 177 \\ 14 & 26 & 6 & -12 & 46 & 54 \\ 40 & 132 & 27 & -91 & 243 & 323 \end{bmatrix} mod\ 27$$

$$P = \begin{bmatrix} 3 & 8 & 14 & 26 & 0 & 12 \\ 14 & 26 & 6 & 15 & 19 & 0 \\ 13 & 24 & 0 & 17 & 0 & 26 \end{bmatrix}$$

4) Ubah kembali ke bentuk alfabet.

$$P = \begin{bmatrix} 3 & 8 & 14 & 26 & 0 & 12 \\ 14 & 26 & 6 & 15 & 19 & 0 \\ 13 & 24 & 0 & 17 & 0 & 26 \end{bmatrix} = \begin{bmatrix} D & I & O & sp & A & M \\ O & sp & G & P & T & A \\ N & Y & A & R & A & sp \end{bmatrix}$$

5) Maka akan didapatkan hasil semula dari *plaintext* $P = DONI\ YOGA\ PRATAMA$.

4.1.1 Kelemahan Hill Cipher

Kekuatan Hill Cipher terletak pada kemampuannya untuk menyembunyikkan frekuensi kemunculan huruf, sehingga sulit untuk dianalisis dengan metode analisis frekuensi huruf. Namun, seperti metode enkripsi lainnya, Hill Cipher juga memiliki kelemahan, seperti serangan *known-plaintext*. Serangan tersebut melibatkan pencocokan pasangan *ciphertext* dan *plaintext* yang diketahui, dengan memperhatikan pola bigram atau trigram yang sering muncul dalam *ciphertext*. Hal ini dimungkinkan karena frekuensi kemunculan bigram dan trigram dalam teks berbahasa Inggris sudah diketahui.

4.2 Modifikasi Algoritma Hill Cipher Menggunakan Grup Simetri

Penjelasan sebelumnya telah mengindikasikan bahwa Hill Cipher memiliki kerentanan yang dapat dieksploitasi oleh pihak ketiga. Oleh karena itu, perlu dilakukan modifikasi dengan menggabungkan metode lain untuk menjaga kerahasiaan pesan rahasia tanpa diketahui oleh pihak ketiga. Modifikasi yang akan dilakukan pada algoritma Hill Cipher adalah dengan menambahkan satu angka untuk merepresentasikan spasi. Dengan kata lain, spasi tidak dihapus dan akan diacak sebelum melakukan operasi menggunakan metode Hill Cipher. Tujuan dari menggunakan penyandian grup simetri S_n adalah untuk melindungi keaslian plaintext sehingga pesan tetap aman dan tidak dapat dibaca oleh pihak yang tidak memiliki otoritas.

Metode penyandian grup simetri melibatkan penggunaan grup simetri dalam pembentukan kunci, sementara teknik transposisi (permutasi) digunakan untuk

proses enkripsi dan dekripsi. Teknik transposisi melibatkan permutasi T pada *plaintext* saat proses enkripsi, dan dalam proses dekripsi, permutasi invers T^{-1} diterapkan pada *ciphertext*.

4.2.1 Simulasi Proses Enkripsi dan Deskripsi Modifikasi Algoritma Hill Cipher Menggunakan Grup Simetri S_n.

Protokol perjanjian kunci *Stickel* menggunakan grup simetri S_n, di mana S_n adalah sebuah grup non-komutatif yang terdiri dari permutasi n anggota dalam himpunan yang dipermutasikan. Dalam sistem kriptografi simetri, ketika dua orang terlibat dalam proses enkripsi dan dekripsi pesan, maka akan ada sejumlah $\frac{1}{2}2(2-1)=1$ kunci rahasia yang perlu ditukarkan secara aman. Kunci tersebut akan digunakan dalam proses enkripsi penyandian grup simetri, sementara invers dari kunci akan digunakan dalam proses dekripsi.

A. Simulasi Proses Enkripsi

Proses enkripsi dimulai dengan pihak pengirim dengan menentukan grup simetri S_n. Pengirim pesan dan penerima pesan mempublikasi suatu grup simetri S_n dan $\sigma_{n!}, S_{22} \in S_n, \sigma_{n!} \circ \sigma_{22} \circ \sigma_{n!}$. dimana

$$\sigma_{n!} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & \cdots & a_{n-1} & a_n & a_1 \end{pmatrix}$$

$$dan$$

$$\sigma_{22} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & \cdots & a_{n-2} & a_{n-1} & a_n \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 & \cdots & a_{n-1} & a_n & a_{n-2} \end{pmatrix}$$

Kemudian menentukan R (orde dari σ_1) dan S (orde dari σ_2).

1) Pengirim pesan memilih dan mengirim secara rahasia bilangan asli $M < R \; dan \; N < S$ dan mengirim.

$$r = {\sigma_1}^M \circ {\sigma_2}^N$$

2) Pengirim pesan memilih dan mengirim secara rahasia bilangan asli $P < R \; dan \; Q < S$ dan mengirim

$$s = {\sigma_1}^P \circ {\sigma_2}^Q$$

3) Pengirim pesan akan menerima s dari pihak penerima dan penerima pesan akan menerima r dari pihak pengirim.

4) Kemudian pihak pengirim akan menghitung

$$T_1 = {\sigma_1}^M \circ s \circ {\sigma_2}^N$$

5) Penerima pesan menghitung

$$T_2 = {\sigma_1}^P \circ r \circ {\sigma_2}^Q$$

6) Sehingga dapat diperoleh berdasarkan grup simetri S_n.

$$T_1 = {\sigma_1}^M \circ s \circ {\sigma_2}^N$$
$$= {\sigma_1}^M \circ {\sigma_1}^P \circ {\sigma_2}^Q \circ {\sigma_2}^N$$
$$= {\sigma_1}^{M+P} \circ {\sigma_2}^{N+Q}$$
$$= {\sigma_1}^P \circ {\sigma_1}^M \circ {\sigma_2}^N \circ {\sigma_2}^Q$$
$$= {\sigma_1}^P \circ r \circ {\sigma_2}^Q$$
$$= T_2$$

Jadi, $T = T_1 = T_2$

Kemudian membagi *plaintext* akan dibagi menjadi beberapa blok sebanyak n.

7) Menentukan kunci Hill Cipher

Permutasi *ciphertext* yang dihasilkan dari pemutasian *plaintext* akan diproses menggunakan metode Hill Cipher dengan menggunakan operasi modulo 27. Dalam operasi ini, karakter spasi (sp) akan

diberikan nilai 27 yang merupakan nilai tambahan di luar jangkauan huruf alfabet.

8) Hasil perhitunga dari *step* 7 dikembalikan dalam bentuk karakter berdasarkan modulo 27.

B. Simulasi Proses Dekripsi

Langkah selanjutnya adalah melakukan dekripsi *ciphertext* yang dihasilkan pada proses di atas. Proses dekripsi menggunakan modifikasi algoritma Hill Cipher dengan grup simetri S_n. dilakukan sebagai berikut:

1) Mengkonversi karakter-karakter pada *ciphertext* kedalam angka, dan membentuknya kedalam matrik kolom

2) Mengalikan *ciphertext* yang sudah berbentuk matriks dengan mengalikannya dengan matriks balikan dari Hill Cipher.

3) Hasil dari perhitungan dari *step* 2 akan dikembalikan ke dalam perutasi grup simetri S_n.

4) Menginvers kunci grup simetri Menginvers kunci grup simetri.

$$T^{-1} = \begin{bmatrix} t(\sigma_1) & t(\sigma_2) & \dots & t(\sigma_n) \\ \sigma_1 & \sigma_2 & \dots & \sigma_n \end{bmatrix}$$

$$= \begin{bmatrix} \sigma_1 & \sigma_2 & \dots & \sigma_n \\ t^{-1}(\sigma_1) & t^{-1}(\sigma_2) & \dots & t^{-1}(\sigma_n) \end{bmatrix}$$

5) Membagi *ciphertext* menjadi blok-blok, setelah semua blok selesai dipemutasikan maka akan diperoleh *plaintetx* sebenarnya.

4.2.2 Simulasi Enkripsi dan Deskripsi Modifikasi Algoritma Hill Cipher Menggunakan Grup Simetri S_6.

A. Simulasi Enkripsi

Misal *plaintext* berupa DONI YOGA PRATAMA, maka proses enkripsi sebagai berikut:

1) Membentu grup simetri.

Pada tahap pembentukan kunci, pengirim pesan secara rahasia memilih dua bilangan asli, yaitu M dan N. Kunci grup simetri dibentuk dengan menghitung operasi sebagai berikut:

$$\sigma_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_1 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}$$

2) Kemudian akan ditentukan KPK dari $\sigma_1\ dan\ \sigma_2$

$$R = |(234561| = 6$$

$$S = |(231)(564)| = 3$$

3) Pengirim menghitung

$r = {\sigma_1}^M \circ {\sigma_2}^N$ dengan $M < R = 5\ , dan\ N < S = 2$

$r = {\sigma_1}^M \circ {\sigma_2}^N$

$$r = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_1 \end{pmatrix}^M \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}^N$$

$$r = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_1 \end{pmatrix}^5 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}^2$$

$$r = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_6 & a_1 & a_5 & a_3 & a_4 \end{pmatrix}$$

4) Penerima juga melakukan hal yang sama $P < R = 5\ dan\ Q < S = 1$

$s = {\sigma_1}^P \circ {\sigma_2}^Q$

$$s = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_1 \end{pmatrix}^P \circ$$

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}^Q$$

$$s = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_1 \end{pmatrix}^5 \circ$$

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}^1$$

$$s = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_1 & a_2 & a_4 & a_6 & a_5 & a_3 \end{pmatrix}$$

5) Pengirim pesan akan menerima s dari penerima dan penerima pesan akan menerima r dari pengirim pesan

6) Kemudia pengirim pesan menghitung kunci

$$T_1 = {\sigma_1}^M \circ s \circ {\sigma_2}^N$$

$$T_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_1 \end{pmatrix}^M \circ$$

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_1 & a_2 & a_4 & a_6 & a_5 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}^N$$

$$T_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_1 \end{pmatrix}^5 \circ$$

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_1 & a_2 & a_4 & a_6 & a_5 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}^2$$

$$T_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix}$$

7) Penerima pesan juga menghitung

$$T_2 = {\sigma_1}^P \circ r \circ {\sigma_2}^Q$$

$$T_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_1 \end{pmatrix}^P \circ$$

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_1 & a_6 & a_1 & a_5 & a_3 & a_4 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}^Q$$

$$T_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_1 \end{pmatrix}^5 \circ$$

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_1 & a_6 & a_1 & a_5 & a_3 & a_4 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 \end{pmatrix}^1$$

$$T_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix}$$

8) Membagi *plaintext* menjadi enam karakter masing-masing blok, apabila terdapat spasi maka spasi tidak dihilangkan namun menambah satu angka.

DONIspY	OGAspPR	ATAMAsp
3 14 13 8 26 24	14 6 0 26 15 17	0 19 0 12 0 26

9) Setelah membuat beberapa blok maka akan diubah seperti di bawah ini

Blok 1: $T = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix}$

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ 26 & 24 & 3 & 14 & 13 & 8 \end{pmatrix}$$

Blok 2: $T = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix}$

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ 15 & 17 & 14 & 6 & 0 & 26 \end{pmatrix}$$

Blok 3: $T = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \end{pmatrix}$

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ 0 & 26 & 0 & 19 & 0 & 12 \end{pmatrix}$$

10) Sehingga diperoleh *ciphertext* (C_T)

26 24 3 14 13 8	15 17 14 6 0 26	0 26 0 19 0 12

11) Kemudian mengkalikan dengan matrik $K = \begin{bmatrix} 3 & 4 & 1 \\ 2 & 1 & 1 \\ 6 & 2 & 3 \end{bmatrix}$

$$C = K \cdot C_T \; mod \; 27$$

$$\begin{bmatrix}3 & 4 & 1\\ 2 & 1 & 1\\ 6 & 2 & 3\end{bmatrix}\cdot\begin{bmatrix}26 & 14 & 15 & 6 & 0 & 19\\ 24 & 13 & 17 & 0 & 26 & 0\\ 3 & 8 & 14 & 26 & 0 & 12\end{bmatrix} mod\ 27$$

$$\begin{bmatrix}177 & 102 & 127 & 44 & 104 & 69\\ 79 & 49 & 61 & 38 & 26 & 50\\ 213 & 134 & 166 & 114 & 52 & 150\end{bmatrix} mod\ 27$$

$$\begin{bmatrix}15 & 21 & 19 & 17 & 23 & 15\\ 25 & 22 & 7 & 11 & 26 & 23\\ 24 & 26 & 4 & 6 & 25 & 15\end{bmatrix}$$

Maka didapatkan *ciphertext*

15 25 24 21 22	19 7 4 17 11 6	23 26 25 15 23

Maka *ciphertext* baru yaitu PZYVWspTHERLGXspZPXP

B. Simulasi Dekripsi

1) Mengkonversi kembali *ciphertext* menjadi bentuk matrik

$$\begin{bmatrix}15 & 21 & 19 & 17 & 23 & 15\\ 25 & 22 & 7 & 11 & 26 & 23\\ 24 & 26 & 4 & 6 & 25 & 15\end{bmatrix}$$

2) Langkah selanjutnya mengkalikan *ciphertext* dengan $K^{-1} =$

$$\begin{bmatrix}1 & -10 & 3\\ 0 & 3 & -1\\ -2 & 18 & -5\end{bmatrix} mod\ 27$$

$$P_T = K^{-1}\ .\ C\ mod\ 27$$

$$\begin{bmatrix}1 & -10 & 3\\ 0 & 3 & -1\\ -2 & 18 & -5\end{bmatrix}.\begin{bmatrix}15 & 21 & 19 & 17 & 23 & 15\\ 25 & 22 & 7 & 11 & 26 & 23\\ 24 & 26 & 4 & 6 & 25 & 15\end{bmatrix} mod\ 27$$

$$\begin{bmatrix}-163 & -121 & -39 & -75 & -162 & -170\\ 51 & 40 & 17 & 27 & 53 & 54\\ 300 & 224 & 68 & 134 & 297 & 309\end{bmatrix} mod\ 27$$

$$\begin{bmatrix}26 & 14 & 15 & 6 & 0 & 19\\ 24 & 13 & 17 & 0 & 26 & 0\\ 3 & 8 & 14 & 26 & 0 & 12\end{bmatrix}$$

3) Maka dihasilkan *plaintext* awal $\begin{bmatrix} 26 & 14 & 15 & 6 & 0 & 19 \\ 24 & 13 & 17 & 0 & 26 & 0 \\ 3 & 8 & 14 & 26 & 0 & 12 \end{bmatrix}$

26 24 3 14 13 8	15 17 14 6 0 26	0 26 0 19 0 12

4) Kemudian ubah kembali dengan kunci invers transposisi.

Blok 1: $T^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix}$

$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ 3 & 14 & 13 & 8 & 26 & 24 \end{pmatrix}$

Blok 2: $T^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix}$

$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ 14 & 6 & 0 & 26 & 15 & 17 \end{pmatrix}$

Blok 3: $T^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix}$

$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ 0 & 19 & 0 & 12 & 0 & 26 \end{pmatrix}$

Sehingga *plaintext* (P) yang diperoleh adalah

DONI YOGA PRATAMA

Maka dapat disimpulkan bahwa:

$C = K.P_T$

$C = K.P \circ T$ $(P_T = P \circ T)$

$K^{-1}.C = K^{-1}.K.P \circ T$ (kedua ruas dikalikan K^{-1})

$K^{-1}.C = I.P \circ T$ $(K^{-1}.K = I)$

$(K^{-1}.C) \circ T^{-1} = P \circ T \circ T^{-1}$ (pindah ruas dipermutasi T^{-1})

$(K^{-1}.C) \circ T^{-1} = P$ $(T \circ T^{-1} = I)$

Keterangan :

C : *Ciphertext*

P : *Plaintext*

T : kunci tranposisi grup simetri

K : Matriks kunci

K^{-1} : Invers matriks

C_T : *Ciphertext* grup simetri

P_T :*Plaintext* grup simetri

T^{-1} : Invers grup simetri

4.3 Kajian Keislaman

Mengamankan pesan melalui penyandian adalah tindakan yang dilakukan untuk menjaga kerahasiaan pesan yang akan disampaikan kepada pihak yang berhak menerimanya. Menjaga pesan ini merupakan tanggung jawab yang telah dipercayakan kepada kita untuk tidak mengungkapkannya melalui media apa pun. Dalam suatu kitab Faidh al-Bariy dijelaskan bahwa amanah adalah salah satu corak dari iman. Sifat amanah disampaikan dalam surah Al-Baqarah ayat 283,yaitu:

فَإِنْ أَمِنَ بَعْضُكُمْ بَعْضًا فَلْيُؤَدِّ الَّذِي اؤْتُمِنَ أَمَانَتَهُ وَلْيَتَّقِ اللَّهَ رَبَّهُ.....

"*... Jika sebagai kamu mempercayai sebagian yang lain, maka hendaklah yang dipercaya itu menunaikan amanat (hutang) dan hendaklah ia bertakwa kepada Allah Tuhannya…"(QS. Al-Baqarah/2:283)*

Surah tersebut mengungkapkan tentang betapa pentingnya tanggung jawab (amanah) yang diberikan kepada seseorang yang dipercayakan untuk menjalankannya.

Amanah yang diberikan kepada kita harus dijaga dan dilestarikan tanpa melakukan manipulasi atau pelanggaran yang dapat merusak kepercayaan yang

telah diberikan. Dalam riwayat oleh Ahmad Musthafa Al-Maraghi, dikemukakan bahwa amanah merujuk pada segala sesuatu yang harus dijaga dan dilestarikan agar dapat disampaikan kepada pihak yang berhak menerimanya. Allah SWT menegaskan pentingnya ketaatan kepada-Nya dan Rasul-Nya, serta konsekuensi pahala bagi mereka yang memelihara ketaatan tersebut dan azab bagi mereka yang melanggarnya. Selanjutnya, dijelaskan tentang betapa besar pentingnya aspek yang terkait dengan ketaatan tersebut.

Berdasarkan penjelasan sebelumnya, penting bagi kita untuk menjaga kerahasiaan setiap amanah (pesan) yang akan dikirimkan agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Prinsip yang serupa berlaku untuk algoritma ini, yang telah dirancang dengan maksud menerapkan proses enkripsi dan dekripsi pesan untuk menjaga keamanan informasi. Algoritma ini menuntut kesepakatan antara kedua pihak yang berkomunikasi untuk menggunakan kunci rahasia yang sama sebelum mereka dapat saling berkomunikasi. Dengan demikian, kunci rahasia tersebut menjadi faktor penting dalam menjaga kerahasiaan dan keamanan komunikasi.

BAB V
PENUTUP

5.1 Kesimpulan

Modifikasi algoritma Hill Cipher menggunakan grup simetri dapat mengamankan pesan dengan cara mengacak terlebih dahulu *plaintext* menggunakan kunci perjanjian stickel di mana pengirim dan penerima mendapatkan kunci sama yang sudah disetujui sebelum membawanya ke dalam metode Hill Cipher. Enkripsi dalam penelitian ini menggunakan persamaan $C = K \cdot P_T \ mod\ 27$ sedangkan dalam proses dekripsi menggunakan persamaan $P = K^{-1} .\ C_T \ mod\ 27$.

5.2 Saran

Modifikasi algoritma Hill Cipher menggunakan grup simetri untuk mengamankan pesan dapat mengamankan pesan terbatas pada 26 karakter dengan penambahan karakter sp . Sehingga untuk penelitian selajutnya diharapkan untuk menambahan karakter berupa alfabet, angka dan simbol serta menggunakan metode lainnya.

DAFTAR PUSTAKA

A. Menezes, Van Oorschot, & S. Vanstone. (1996). *Handbook of Applied Cryptography*. CRC Press.

Ad-Dimasyqi. (2001). *Tafsir Ibnu Katsir*. Bandung: Sinar Baru Algensindo.

Al Qur'an dan Terjemahan. (2019). Kementerian Agama RI.

Al-Sheik, A. b. (1994). *Tafsir Ibnu Katsir* (2 ed.). (M. A. E.M, Penerj.) Jakarta: Pustaka Imam asy-Syafe'i.

Arifin, A. (2000). *Aljabar*. Bandung: ITB Bandung.

Ariyus, D. (2008). *Penghantar Ilm Kriptografi Teori Analisis dan Implementasi*. Yogyakarta: C.V ANDI OFFSET.

Dummit, D. S., & Foote, R. M. (2004). *Abstact Algebra Third Edition.* New York: Prentice-Hall International,inc.

Hariati, A., Hardiyati, K., & Putri, W. E. (2018). Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks. *Sikron*, 13-17.

Hasugian, A. H. (2013). Implementasi Algoritma Hill Cipher dalam Penyandian. *Pelita Informatika Budi Darma*, 115-122.

Irawan, W. H. (2014). *Pengantar Teori Bilangan.* Malang: UIN-Malang Press.

Katsir, I. (2004). *"Tafsir Ibnu Katsir" Jilit 2. Terjemahan M. Abdul Ghofar E.M.* Bogor: Pustaka Imam as-Syafi'i.

Meyer, C. H., & Matyas, S. M. (1982). *Cryptography : a new dimension in computer data security.* New York: John Wiley & Sons.

Mukhtar, H. (2018). *Kriptografi Untuk Keamanan Data.* Yogyakarta: Derpublish.

Munir, R. (2019). *Kriptografi edisi dua.* Bandung: Informatika Bandung.

Musthofa, & Lestari, D. (2014). Metode Perjanjian Password Berdasarkan Operasi Matriks Atas Aljabar Min-Plus untuk Keamanan Pengiriman Informasi Rahasia. *J. Sains Dasar*, 3(1) 25-33.

Myasnikov, A., Shpilrain, V., & Ushakov, A. (2008). *Group-based Cryptography.* Basel Switzerland: Birkhauser Verlag.

Rachmawati, D., Budiman, M. A., & Aulia, I. (2018). Super-Encryption Implementation Using Monoalphabetic Algorithm and XOR Algorithm for Data Security. *Journal of Physic*.

Raisinghania, M. D., & Aggarwal, R. S. (1980). *Moderent Algebra.* New Delhi: S. Chand & Company LTD.

Ruffini, P. (1799). *Teoria Generale Delle Equazioni.* S. Tommaso d'Aquaino: Nella Stamperia.

Sadikin, R. (2012). *Kriptografi untuk Keamanan Jaringan.* Yogyakarta: CV Andi Offset.

Sayyid, Q. (2001). *Tafsir Fi Zhilalil Qur'an* (Jilid II ed.). (A. A. As'ad Yasin, Penerj.) Jakarta: Gema Insani Press.

RIWAYAT HIDUP

Doni Yoga Pratama lahir di Trenggalek pada tanggal 21 Juni 1998, biasa dipanggil Doni atau Inod. Alamat berasal di Dusun Tawing Krajan RT/RW:01/01 Desa Tawing, Kecamatan Munjungan, Kabupaten Trenggalek. Merupakan anak pertama dari pasangan Bapak Sugianto dan Ibu Murtini. Pernah menempuh pendidikan dasar di SDN 1 Tawing dan lulus 2010. Kemudian melanjutkan sekolah ketingkat menengah pertama di SMPN 1 Munjungan dan lulus pada tahun 2013. Selanjutnya, menempuh sekolah tingkat menengah ke atas di SMAN 1 Pasir Belengkong pada tahun 2016. Tahun 2016 melanjutkan studi di Universitas Islam Negeri Maulana Malik Ibrahim Malang menempuh Program Studi Matematika aktif dalam kegiatan akademik dan organisasi HMJ “Integral” Matematika.

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 : Doni Yoga Pratama
NIM : 16610009
Fakultas / Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Modifikasi Algoritma Hill Cipher Menggunakan Grup Simetri Untuk Mengamankan Pesan Teks
Pembimbing I : Muhammad Khudzaifah, M.Si.
Pembimbing II : Erna Herawati, M.Pd.

No	Tanggal	Hal	Tanda Tangan
1.	13 Maret 2023	KONSULTASI JUDUL PERTAMA	1.
2.	14 Maret 2023	KONSULTASI JUDUL KEDUA	2.
3.	27 April 2023	KONSULTASI BAB I, II dan III	3.
4.	27 April 2023	KONSULTASI KAJIAN AGAMA	4.
5.	30 April 2023	ACC KAJIAN AGAMA	5.
6.	08 Mei 2023	ACC BAB I, II dan III	6.
7.	22 Mei 2023	KONSULTASI REVISI SEMPRO	7.
8.	23 Mei 2023	KONSULTASI BAB IV dan V	8.
9.	24 Mei 2023	KONSULTASI KAJIAN KEISLAMAN	9.
10.	25 Mei 2023	ACC KAJIAN KEISLAMAN	10.
11.	26 Mei 2023	ACC BAB IV dan V	11.
12.	15 Juni 2023	Konsultasi Revisi Seminar Hasil dan ACC Sidang	12.

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129200012200 5