Algoritma *Affine Cipher* dan Modifikasi *Affine Cipher*, serta Kombinasinya dengan *Cipher* Transposisi Grup Simetri untuk Mengamankan Pesan Teks

Ilfi Nur Diana

Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia

email: ilfinurdiana70@gmail.com

Abstrak

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi. Metode kriptografi yang digunakan untuk mengamankan pesan diantaranya adalah *affine cipher* dan *cipher* transposisi grup simetri. *Affine cipher* merupakan salah satu algoritma kriptografi klasik yang menggunakan metode substitusi. Modifikasi *Affine Cipher* membagi teks terlebih dahulu menjadi kelompok yang terdiri dari k karakter lalu kemudian menggunakan *Affine Cipher. Cipher* transposisi grup simetri merupakan salah satu algoritma kriptografi klasik yang menggunakan metode transposisi. *Cipher* transposisi grup simetri menggunakan grup simetri-n sebagai kunci rahasia. Semakin besar nilai n akan semakin banyak pula kemungkinan kunci dari *cipher* transposisi grup simetri. Metode substitusi dan transposisi memiliki tingkat keamanan yang cenderung lebih rendah. Untuk meningkatkan keamanan penyandian pesan maka dilakukan penggabungan algoritma *cipher* substitusi dan *cipher* transposisi yang disebut super enkripsi. Pada penelitian ini dilakukan penggabungan algoritma *affine cipher* dan *cipher* transposisi grup simetri, serta modifikasi *affine cipher* dan *cipher* transposisi grup simetri.

Kata kunci: Affine Cipher, Modifikasi Affine Cipher, Cipher Transposisi Grup Simetri, Super Enkripsi

Abstract

Cryptography is a science that studies mathematical techniques related to aspects of information security. Cryptographic methods used to secure messages include affine ciphers and symmetric group transposition ciphers. Affine cipher is one of the classical cryptographic algorithms that use the substitution method. In Modification of Affine Cipher, we first divide the text into groups of k characters and then use Affine Cipher. Cipher transposition symmetric group is one of the classical cryptographic algorithms that use the transposition method. The cipher transposition symmetric group uses the n-symmetric group as the secret key. The larger value of n, the more possible keys from the cipher transposition symmetric group. Substitution and transposition methods have a lower level of security. On the other hand, the key of the affine cipher can be found by an exhaustive key search. To increase the security of message encoding, a substitution cipher algorithm and a transposition cipher algorithm are combined which is called super encryption. In this study, the

affine cipher algorithm and cipher transposition symmetric group were combined, as well as modification of affine cipher and symmetric group transposition cipher.
Keywords: Affine Cipher, Modification of Affine Cipher, Cipher Transposition Symmetric Group, Super Encryption

Pendahuluan

Teknologi komputer semakin lama semakin berkembang dan semakin maju. Perkembangan teknologi komputer dapat meningkatkan kemudahan dalam berkomunikasi dengan menggunakan akses internet. Namun, internet memiliki jangkauan yang sangat luas dan dapat dilihat oleh banyak orang sehingga rentan terjadi penyadapan penyandian. Penyadapan penyandian dapat mengakibatkan orang lain mengetahui pesan yang kita kirimkan. Hal ini membuat aspek keamanan pada pertukaran informasi menjadi sangat penting. Untuk itu perlu adanya usaha dalam mengamankan pesan informasi yang akan dikomunikasikan [1]. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [2],[3],[4],[5]. Pengamanan pesan menggunakan kriptografi tidak lepas dari metode enkripsi dan dekripsi. Enkripsi merupakan proses menyandikan pesan asli (plainteks) menjadi pesan tersandi (cipherteks). Sedangkan dekripsi merupakan proses mengembalikan cipherteks menjadi plainteks semula [6],[7],[8].

Affine cipher adalah perluasan dari algoritma *caesar cipher* yang diperoleh dengan mengalikan plainteks dengan suatu bilangan m yang relatif prima dengan nilai pergeseran b, kemudian hasilnya dijumlahkan dengan nilai pergeseran b [6]. Berdasarkan Nurjamiyah [9], algoritma *affine cipher* dapat digunakan untuk menyembunyikan pesan rahasia ke dalam teks dengan efektif. *Affine cipher* adalah salah satu metode penyandian pesan menggunakan algoritma kriptografi klasik. Kriptografi klasik merupakan algoritma kriptografi yang berbasis karakter dimana enkripsi dan dekripsi dilakukan pada setiap karakter pesan [10]. Algoritma Modifikasi Affine Cipher merupakan metode Affine Cipher dengan menerapkan modifikasi pada plainteks yang dikelompokan menjadi k karakter setiap kelompoknya, kemudian disusun ulang dengan posisi terbalik. Secara umum algoritma kriptografi klasik dikategorikan menjadi dua, yaitu *cipher* substitusi dan *cipher* transposisi. *Cipher* substitusi merupakan proses penyandian pesan dengan mengganti huruf dari plainteks menjadi huruf, angka, atau simbol lainnya [11]. Sedangkan *cipher* transposisi merupakan proses penyandian pesan dengan cara mengubah susunan huruf-huruf [6].

Cipher transposisi grup simetri merupakan teknik transposisi menggunakan permutasi karakter di mana pengirim dan penerima menyepakati kunci rahasia menggunakan grup simetri-n, kemudian membagi teks asli (plainteks) menjadi blok-blok yang memuat beberapa karakter [12]. Penyandian pesan menggunakan grup simetri S_n untuk mengamankan informasi akan menghasilkan cipherteks yang tidak dapat dimengerti. Dengan menggunakan grup simetri-n maka terdapat kemungkinan sebanyak $n!$ Kunci. Semakin besar nilai n akan semakin banyak pula kemungkinan kunci dari algoritma *cipher* transposisi grup simetri [12].

Metode substitusi dan transposisi memiliki tingkat keamanan yang cenderung lebih rendah [13]. Disisi lain, kunci dari *affine cipher* dapat ditemukan dengan *exhaustive key search*. Jika menggunakan karakter alfabet 26 huruf, maka hanya terdapat 25 kemungkinan untuk nilai b dan hanya terdapat 12 nilai m yang relatif prima dengan 26 [6]. Teknik-teknik klasik penggabungan memberikan *cipher* lebih aman dan kuat [14]. Super Enkripsi adalah metode kriptografi berbasis karakter yang mengkombinasikan dua buah cipher untuk memperoleh cipher yang lebih kuat sehingga tidak mudah untuk dipecahkan, dan juga untuk menangani penggunaan cipher tunggal

yang secara komparatif lemah [15],[16],[17],[18]. Cipher substitusi dan cipher transposisi dapat dikombinasikan untuk memperoleh cipher yang lebih kuat (super) daripada hanya satu cipher saja. Proses penyandian pesan dilakukan dengan mengenkripsikan plaintext menggunakan *cipher* substitusi sederhana, kemudian hasilnya dienkripsi kembali menggunakan *cipher* transposisi (atau sebaliknya) [6]. Penelitian mengenai algoritma super enkripsi yang dilakukan oleh [14] menggabungkan *cipher* substitusi yaitu *hill cipher* dan *cipher* transposisi yaitu transposisi kolom. Penelitian tersebut menyatakan bahwa algoritma super enkripsi dapat menambah keamanan pada pesan teks.

Pada Penelitian ini, peneliti menggunakan algoritma super enkripsi yang mengkombinasikan algoritma *cipher* substitusi dan *cipher* transposisi dalam mengamankan atau menyandikan pesan teks. Adapun algoritma *cipher* substitusi yang digunakan adalah *affine cipher* dan modifikasi *affine cipher* sedangkan algoritma *cipher* transposisi yang digunakan adalah *cipher* transposisi grup simetri. Hal ini dilakukan karena penggabungan dua buah *cipher* akan lebih sulit dipecahkan daripada hanya menggunakan satu *cipher* saja. Selain itu, banyaknya kemungkinan kunci pada *cipher* transposisi grup simetri dapat menguatkan tingkat keamanan dari *affine cipher* maupun modifikasi *affine cipher*.

Metode

Metode penelitian yang digunakan oleh penulis menggabungkan dua buah algoritma yang telah ada untuk memperoleh proteksi ganda untuk pengamanan teks yaitu *affine cipher* dan *cipher* transposisi grup simetri, serta modifikasi *affine cipher* dan *cipher* transposisi grup simetri.

1. Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: "*cryptós*" artinya "*secret*" (rahasia), sedangkan "*gráphein*" artinya "*writing*" (tulisan). Jadi, kriptografi secara harfiah berarti "*secret writing*" (tulisan rahasia) [6]. Kriptografi merupakan ilmu menulis pesan rahasia yang bertujuan untuk menyembunyikan makna pesan tersebut [19]. Kriptografi berkembang sesuai dengan masalah yang dihadapi sehingga muncul beberapa istilah yang digunakan untuk menandai aktifitas-aktifitas rahasia untuk mengirim pesan. Proses mengacak pesan disebut enkripsi dan ketika merapikan pesan teracak disebut dekripsi. Pesan awal yang belum diacak atau yang sudah dirapikan disebut plainteks dan pesan yang sudah diacak disebut cipherteks [20].

2. Algoritma *Affine Cipher*

Proses enkripsi plainteks menggunakan algoritma *affine cipher* dapat dilakukan dengan persamaan berikut [6]:

$$C = (mP + b)\ mod\ n \quad (1)$$

keterangan:

$C =$ cipherteks

$P =$ plainteks

$n =$ banyaknya alfabet

$m =$ bilangan bulat yang relatif prima dengan n

$b =$ jumlah pergeseran

Proses dekripsi menggunakan algoritma *Affine cipher* dapat dilakukan jika ada balikan dari $m\ (mod\ n)$ yang dinyatakan dengan $m^{-1}\ (mod\ n)$. Berdasarkan Munir [6], Persamaan yang digunakan saat proses dekripsi adalah

$$P = m^{-1}\ (C - b)\ mod\ n \quad (2)$$

3. Algoritma Modifikasi Affine Cipher

Algoritma ini merupakan metode Affine Cipher dengan menerapkan modifikasi pada plainteks yang dikelompokan menjadi k karakter setiap kelompoknya, kemudian disusun ulang dengan posisi terbalik [1]. Sebagai contoh jika kata MATEMATIKA akan dibagi kedalam kelompok dengan empat karakter maka menjadi MATE MATI KA kemudian posisi dibalik sehingga menjadi ETAM ITAM AK. Setelah proses modifikasi pada plainteks dilakukan, maka proses pada Affine Cipher dapat dilakukan yaitu seperti tertera pada persamaan (1).

Proses dekripsi juga sama dengan algoritma Affine Cipher pada persamaan (2), dengan setelahnya menambahkan proses pembagian menjadi kelompok dengan empat karakter kemudian dilakukan pembalikan posisi karakter.

4. Algoritma *Cipher* Transposisi Grup Simetri

Proses enkripsi menggunakan algoritma *cipher* transposisi grup simetri yaitu, pertama pengirim dan penerima menyepakati kunci rahasia menggunakan grup simetri-n. Kemudian membagi teks asli (plainteks) menjadi blok-blok yang memuat beberapa karakter. Pesan asli tidak dapat diketahui kecuali oleh seseorang yang mempunyai kunci untuk mendekripsi cipherteks ke bentuk asal [10].

Proses dekripsi menggunakan algoritma *cipher* transposisi grup simetri pada dasamya sama saja dengan proses enkripsinya namun pada proses dekripsi penerima pesan terlebih dahulu menginverskan kunci yang telah disepakati sebelumnya [10].

5. Kombinasi Algoritma Super Enkripsi (Affine Cipher dan Cipher Transposisi Grup Simetri)

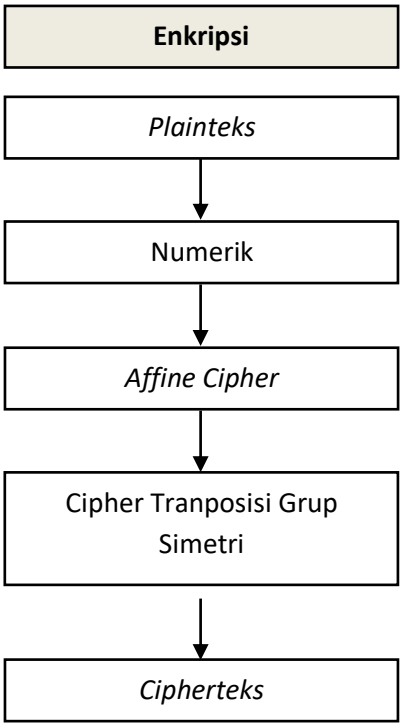
Secara matematis proses enkripsi menggunakan metode super enkripsi dapat dijelaskan sebagai berikut:

1) Menentukan plainteks.
2) Menentukan kunci m dan b di mana m relatif prima dengan n dan $1 < b < n, (n = 26)$.
3) Mengubah plainteks alfabet ke dalam bentuk numerik.
4) Mengubah hasil enkripsi bentuk numerik menjadi alfabet.
5) Menentukan kunci grup simetri K.
6) Membagi plainteks menjadi beberapa blok sesuai dengan jumlah permutasi pada K.
7) Melakukan enkripsi menggunakan algoritma cipher transposisi grup simetri.
8) Memperoleh pesan teks yang telah disandikan (cipherteks).

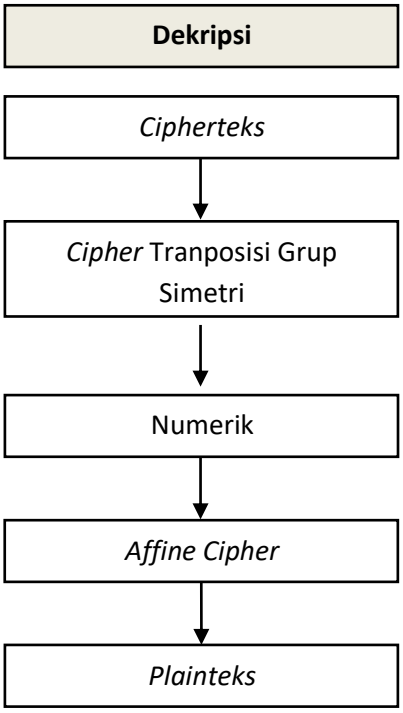
Sedangkan proses dekripsi secara matematis menggunakan metode super enkripsi dapat dijelaskan sebagai berikut:

1) Mendapatkan pesan yang telah disandikan (cipherteks)
2) Menentukan K^{-1} sebagai kunci yang akan digunakan untuk dekripsi dengan cipher transposisi grup simetri
3) Membagi plainteks menjadi beberapa blok sesuai dengan jumlah permutasi pada K.
4) Melakukan dekripsi menggunakan algoritma cipher transposisi grup simetri.
5) Mengubah cipherteks alfabet ke dalam bentuk numerik. cipherteks merupakan plainteks hasil dekripsi menggunakan cipher transposisi grup simetri
6) Menentukan m^{-1}.
7) Melakukan dekripsi menggunakan algoritma *affine cipher*
8) Mengubah hasil dekripsi bentuk numerik menjadi alfabet.
9) Memperoleh pesan teks asli (plainteks).

Proses enkripsi dan deskripsi diilustrasikan seperti pada Gambar 1 dan Gambar 2 berikut:



Gambar 1. Skema Enkripsi Algoritma Super Enkripsi



Gambar 2. Skema Dekripsi Algoritma Super Enkripsi

6. Kombinasi Algoritma Modifikasi Super Enkripsi (Modifikasi Affine Cipher dan Cipher Transposisi Grup Simetri)

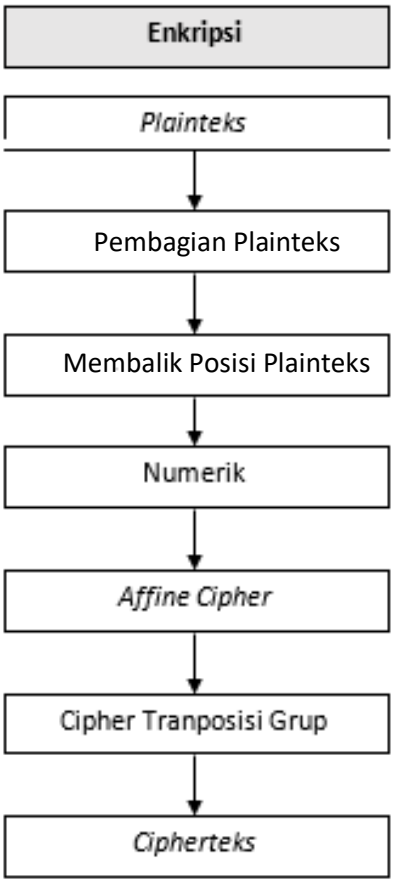
Secara matematis proses enkripsi menggunakan metode super enkripsi dapat dijelaskan sebagai berikut:

1) Menentukan plainteks.
2) Membagi plainteks ke dalam kelompok dengan k karakter.
3) Membalik posisi karakter di setiap kelompoknya
4) Menerapkan proses enkripsi kombinasi *affine cipher dan cipher* transposisi grup simetri pada bagian 5

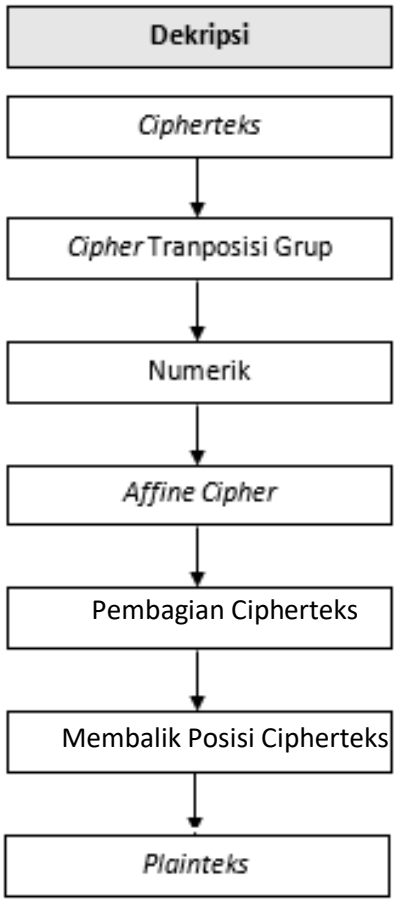
Secara matematis proses dekripsi menggunakan metode super enkripsi dapat dijelaskan sebagai berikut:

1) Mendapatkan pesan yang telah disandikan (cipherteks)
2) Menerapkan proses dekripsi kombinasi *affine cipher dan cipher* transposisi grup simetri pada bagian 5.
3) Membagi plainteks ke dalam kelompok dengan k karakter.
4) Membalik posisi karakter di setiap kelompoknya
5) Memperoleh pesan teks asli (plainteks).

Proses enkripsi dan dekripsi diilustrasikan seperti Gambar 3 dan Gambar 4 berikut:



Gambar 3. Skema Enkripsi Algoritma Modifikasi Super Enkripsi



Gambar 4. Skema Dekripsi Algoritma Modifikasi Super Enkripsi

Hasil dan Diskusi

Pada penelitian ini, penulis menggunakan plainteks "PRAMUKA UIN MALANG" untuk disandikan dengan metode *Affine Cipher* dan Cipher Transposisi Grup Simetri.

1. Enkripsi Menggunakan Algoritma *Affine Cipher* dan *Cipher* Transposisi Grup Simetri

Proses enkripsi dilakukan menggunakan algoritma *affine cipher* terlebih dahulu. Karakter alfabet yang digunakan pada algoritma *affine cipher* sejumlah 26 huruf dimana A=0, B=1, C=2,…, Z=25. Berikut merupakan proses enkripsi menggunakan *Affine Cipher*:

Plainteks: PRAMUKA UIN MALANG

Kunci $m = 11$ dan $b = 14$

Karena karakter yang digunakan sejumlah 26 huruf maka $n = 26$. Berdasarkan karakter alfabet yang digunakan, plainteks PRAMUKA UIN MALANG ekuivalen dengan 15 17 0 12 20 10 0 20 8 13 12 0 11 0 13 6. Menggunakan (1) maka proses perhitungan enkripsi menggunakan algoritma *Affine Cipher* adalah sebagai berikut:

$p_1 = 15 \rightarrow c_1 = (11 \cdot 15 + 14)\ mod\ 26 = 179\ mod\ 26 = 23$ (huruf X)

$p_2 = 17 \rightarrow c_2 = (11 \cdot 17 + 14)\ mod\ 26 = 201\ mod\ 26 = 19$ (huruf T)

$p_3 = 0 \rightarrow c_3 = (11 \cdot 0 + 14)\ mod\ 26 = 14\ mod\ 26 = 14$ (huruf O)

$p_4 = 12 \rightarrow c_4 = (11 \cdot 12 + 14)\ mod\ 26 = 146\ mod\ 26 = 16$ (huruf Q)

$p_5 = 20 \rightarrow c_5 = (11 \cdot 20 + 14)\ mod\ 26 = 234\ mod\ 26 = 0$ (huruf A)

$p_6 = 10 \rightarrow c_6 = (11 \cdot 10 + 14)\ mod\ 26 = 124\ mod\ 26 = 20$ (huruf U)
$p_7 = 0 \rightarrow c_7 = (11 \cdot 0 + 14)\ mod\ 26 = 14\ mod\ 26 = 14$ (huruf O)
$p_8 = 20 \rightarrow c_8 = (11 \cdot 20 + 14)\ mod\ 26 = 234\ mod\ 26 = 0$ (huruf A)
$p_9 = 8 \rightarrow c_9 = (11 \cdot 8 + 14)\ mod\ 26 = 102\ mod\ 26 = 24$ (huruf Y)
$p_{10} = 13 \rightarrow c_{10} = (11 \cdot 13 + 14)\ mod\ 26 = 157\ mod\ 26 = 1$ (huruf B)
$p_{11} = 12 \rightarrow c_{11} = (11 \cdot 12 + 14)\ mod\ 26 = 146\ mod\ 26 = 16$ (huruf Q)
$p_{12} = 0 \rightarrow c_{12} = (11 \cdot 0 + 14)\ mod\ 26 = 14\ mod\ 26 = 14$ (huruf O)
$p_{13} = 11 \rightarrow c_{13} = (11 \cdot 11 + 14)\ mod\ 26 = 135\ mod\ 26 = 5$ (huruf F)
$p_{14} = 0 \rightarrow c_{14} = (11 \cdot 0 + 14)\ mod\ 26 = 14\ mod\ 26 = 14$ (huruf O)
$p_{15} = 13 \rightarrow c_{15} = (11 \cdot 13 + 14)\ mod\ 26 = 157\ mod\ 26 = 1$ (huruf B)
$p_{16} = 6 \rightarrow c_{16} = (11 \cdot 6 + 14)\ mod\ 26 = 80\ mod\ 26 = 2$ (huruf C)

Jadi, cipherteks yang dihasilkan adalah XTOQAUO AYB QOFOBC.

Selanjutnya, cipherteks tersebut dienkripsi kembali menggunakan cipher transposisi grup simetri. Berikut merupakan proses enkripsi menggunakan cipher transposisi grup simetri:

Kunci: $K = (1\ 2\ 3\ 4\ 5\ 4\ 1\ 5\ 3\ 2\ )$

Membagi plainteks menjadi blok-blok yang terdiri dari lima huruf dengan ketentuan jika terdapat kekurangan pada blok maka ditambahkan dengan karakter %. Sedangkan untuk spasi diganti dengan karakter #.

XTOQA	UO#AY	B#QOF	OBC%%

Kemudian, setiap blok diubah menjadi seperti di bawah ini dengan menggunakan kunci yang telah ditentukan.

Blok 1: $K = (1\ 2\ 3\ 4\ 5\ 4\ 1\ 5\ 3\ 2\ ) = (1\ 2\ 3\ 4\ 5\ X\ T\ O\ Q\ A\ 4\ 1\ 5\ 3\ 2\ Q\ X\ A\ O\ T\ )$
Blok 2: $K = (1\ 2\ 3\ 4\ 5\ 4\ 1\ 5\ 3\ 2\ ) = (1\ 2\ 3\ 4\ 5\ U\ O\ \#\ A\ Y\ 4\ 1\ 5\ 3\ 2\ A\ U\ Y\ \#\ O\ )$
Blok 3: $K = (1\ 2\ 3\ 4\ 5\ 4\ 1\ 5\ 3\ 2\ ) = (1\ 2\ 3\ 4\ 5\ B\ \#\ Q\ O\ F\ 4\ 1\ 5\ 3\ 2\ O\ B\ F\ Q\ \#\ )$
Blok 4: $K = (1\ 2\ 3\ 4\ 5\ 4\ 1\ 5\ 3\ 2\ ) = (1\ 2\ 3\ 4\ 5\ O\ B\ C\ \%\ \%\ 4\ 1\ 5\ 3\ 2\ \%\ O\ \%\ C\ B\ )$

Sehingga diperoleh cipherteks yaitu QXAOTAUY#OOBFQ#%O%CB.

2. Dekripsi Menggunakan Algoritma Super Dekripsi (*Affine Cipher* dan *Cipher* Transposisi Grup Simetri)

Pengembalian plainteks menjadi pesan teks semula (plainteks) dilakukan dengan proses dekripsi menggunakan *cipher* transposisi grup simetri terlebih dahulu. Proses dekripsi menggunakan cipher transposisi grup simetri dilakukan dengan cara yang sama seperti proses enkripsi, namun dengan menggunakan kunci invers. Berikut adalah proses dekripsi menggunakan cipher transposisi grup simetri.

Cipherteks: QXAOTAUY#OOBFQ#%O%CB

Kunci: $K = (1\ 2\ 3\ 4\ 5\ 4\ 1\ 5\ 3\ 2\ )$

$K^{-1} = (4\ 1\ 5\ 3\ 2\ 1\ 2\ 3\ 4\ 5\ )$

$K^{-1} = (1\ 2\ 3\ 4\ 5\ 2\ 5\ 4\ 1\ 3\ )$

Membagi plainteks menjadi blok-blok yang terdiri dari lima huruf sebagai berikut:

QXAOT	AUY#O	OBFQ#	%O%CB

Selanjutnya, setiap blok diubah menjadi seperti di bawah ini dengan menggunakan kunci yang telah ditentukan.

Blok 1: $K^{-1} = (1\ 2\ 3\ 4\ 5\ 2\ 5\ 4\ 1\ 3\ ) = (1\ 2\ 3\ 4\ 5\ Q\ X\ A\ O\ T\ 2\ 5\ 4\ 1\ 3\ X\ T\ O\ Q\ A\ )$
Blok 2: $K^{-1} = (1\ 2\ 3\ 4\ 5\ 2\ 5\ 4\ 1\ 3\ ) = (1\ 2\ 3\ 4\ 5\ A\ U\ Y\ \#\ O\ 2\ 5\ 4\ 1\ 3\ U\ O\ \#\ A\ Y\ )$
Blok 3: $K^{-1} = (1\ 2\ 3\ 4\ 5\ 2\ 5\ 4\ 1\ 3\ ) = (1\ 2\ 3\ 4\ 5\ O\ B\ F\ Q\ \#\ 2\ 5\ 4\ 1\ 3\ B\ \#\ Q\ O\ F\ )$

Blok 4: $K^{-1} = (1\ 2\ 3\ 4\ 5\ 2\ 5\ 4\ 1\ 3\ ) = (1\ 2\ 3\ 4\ 5\ \%\ O\ \%\ C\ B\ 2\ 5\ 4\ 1\ 3\ O\ B\ C\ \%\ \%\ )$.
Sehingga diperoleh plainteks yaitu XTOQAUO#AYB#QOFOBC%%. Diketahui karakter # menggantikan spasi dan karakter % menggantikan kekurangan pada blok maka plainteks yang diperoleh adalah XTOQAUO AYB QOFOBC.

Plainteks yang diperoleh dari hasil dekripsi menggunakan cipher tranposisi grup simetri akan digunakan sebagai cipherteks pada proses dekripsi menggunakan *affine cipher*.
Cipherteks: XTOQAUO AYB QOFOBC
Kunci: $m = 11$ dan $b = 14$
Berdasarkan karakter alfabet yang digunakan, maka cipherteks XTOQAUO AYB QOFOBC ekuivalen dengan 23 19 14 16 0 20 14 0 24 1 16 14 5 14 1 2. Untuk melakukan dekripsi, maka harus ditentukan $m^{-1}(mod\ n)$ terlebih dahulu. Menentukan $m^{-1}(mod\ n)$ dapat dihitung dengan menggunakan kekongruenan linier.
Misalkan $11^{-1}(mod\ 26) = x$ maka $x = 19$ karena $11 \cdot 19\ (mod\ 26) = 1$.
Berdasarkan (2) maka proses perhitungan dekripsi menggunakan algoritma *Affine Cipher* adalah sebagai berikut:

$c_1 = 23 \rightarrow p_1 = 19(23 - 14)\ mod\ 26 = 171\ mod\ 26 = 15$ (huruf P)
$c_1 = 19 \rightarrow p_1 = 19(19 - 14)\ mod\ 26 = 95\ mod\ 26 = 17$ (huruf R)
$c_1 = 14 \rightarrow p_1 = 19(14 - 14)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)
$c_1 = 16 \rightarrow p_1 = 19(16 - 14)\ mod\ 26 = 38\ mod\ 26 = 12$ (huruf M)
$c_1 = 0 \rightarrow p_1 = 19(0 - 14)\ mod\ 26 = -266\ mod\ 26 = 20$ (huruf U)
$c_1 = 20 \rightarrow p_1 = 19(20 - 14)\ mod\ 26 = 114\ mod\ 26 = 10$ (huruf K)
$c_1 = 14 \rightarrow p_1 = 19(14 - 14)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)
$c_1 = 0 \rightarrow p_1 = 19(0 - 14)\ mod\ 26 = -266\ mod\ 26 = 20$ (huruf U)
$c_1 = 24 \rightarrow p_1 = 19(24 - 14)\ mod\ 26 = 190\ mod\ 26 = 8$ (huruf I)
$c_1 = 1 \rightarrow p_1 = 19(1 - 14)\ mod\ 26 = -247\ mod\ 26 = 13$ (huruf N)
$c_1 = 16 \rightarrow p_1 = 19(16 - 14)\ mod\ 26 = 38\ mod\ 26 = 12$ (huruf M)
$c_1 = 14 \rightarrow p_1 = 19(14 - 14)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)
$c_1 = 5 \rightarrow p_1 = 19(5 - 14)\ mod\ 26 = -171\ mod\ 26 = 11$ (huruf L)
$c_1 = 14 \rightarrow p_1 = 19(14 - 14)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)
$c_1 = 1 \rightarrow p_1 = 19(1 - 14)\ mod\ 26 = -247\ mod\ 26 = 13$ (huruf N)
$c_1 = 2 \rightarrow p_1 = 19(2 - 14)\ mod\ 26 = -228\ mod\ 26 = 6$ (huruf G)

Jadi, plainteks yang dihasilkan adalah PRAMUKA UIN MALANG.

3. Enkripsi Menggunakan Algoritma Modifikasi Super Enkripsi (Modifikasi *Affine Cipher* dan *Cipher* Transposisi Grup Simetri)

Sama halnya dengan pada proses enkripsi *affine cipher,* dengan menggunakan kunci $m = 11$ dan $b = 14$, serta $k = 5$, maka diperoleh:
Plainteks : PRAMUKA UIN MALANG
Pembagian Plainteks : PRAMU-KA UI-N MAL-ANG
Pembalikan Posisi Plainteks :UMARP-IU AK-LAM N-GNA

Karakter alfabet yang digunakan pada algoritma modifikasi *affine cipher* sejumlah 26 huruf dimana A=0, B=1, C=2,…, Z=25, sehingga proses numerik akan menjadi 20 12 0 17 15-8 20 0 10- 11 0 12 13- 6 13 0 Karena kata yang digunakan beserta bilangan kunci sama dengan proses algoritma super enkripsi sehingga dengan proses modulo pada bagian 2 diperoleh 0 16 14 19 23- 24 0 14 20-5 14 16 1-2 1 14. Yang dikonversi menjadi Cipherteks AQOTX-YA OU-FOQ B-CBO

Selanjutnya, cipherteks tersebut dienkripsi kembali menggunakan cipher transposisi grup simetri. Berikut merupakan proses enkripsi menggunakan cipher transposisi grup simetri:

Kunci: $K = (1\ 2\ 3\ 4\ 5\ 4\ 1\ 5\ 3\ 2\ )$

Membagi plainteks menjadi blok-blok yang terdiri dari lima huruf dengan ketentuan jika terdapat kekurangan pada blok maka ditambahkan dengan karakter %. Sedangkan untuk spasi diganti dengan karakter #.

AQOTX	YA#OU	FOQ#B	CBO%%

Kemudian, setiap blok diubah menjadi seperti di bawah ini dengan menggunakan kunci yang telah ditentukan.

Blok 1: $K = (1\ 2\ 3\ 4\ 5\ 4\ 1\ 5\ 3\ 2\ ) = (1\ 2\ 3\ 4\ 5\ AQOTX\ 4\ 1\ 5\ 3\ 2\ TAXOQ\ )$

Blok 2: $K = (1\ 2\ 3\ 4\ 5\ 4\ 1\ 5\ 3\ 2\ ) = (1\ 2\ 3\ 4\ 5\ YA\#OU\ 4\ 1\ 5\ 3\ 2\ OYU\#A)$

Blok 3: $K = (1\ 2\ 3\ 4\ 5\ 4\ 1\ 5\ 3\ 2\ ) = (1\ 2\ 3\ 4\ 5 FOQ\#B4\ 1\ 5\ 3\ 2\ \#FBQO)$

Blok 4: $K = (1\ 2\ 3\ 4\ 5\ 4\ 1\ 5\ 3\ 2\ ) = (1\ 2\ 3\ 4\ 5\ CBO\%\%4\ 1\ 5\ 3\ 2\ \%C\%OB)$

Sehingga diperoleh cipherteks yaitu TAXOQOYU#A#FBQO%C%OB

4. Dekripsi Menggunakan Algoritma Super Dekripsi (*Affine Cipher* dan *Cipher* Transposisi Grup Simetri)

Pengembalian plainteks menjadi pesan teks semula (plainteks) dilakukan dengan proses dekripsi menggunakan *cipher* transposisi grup simetri terlebih dahulu. Proses dekripsi menggunakan cipher transposisi grup simetri dilakukan dengan cara yang sama seperti proses enkripsi, namun dengan menggunakan kunci invers. Berikut adalah proses dekripsi menggunakan cipher transposisi grup simetri.

Cipherteks: TAXOQOYU#A#FBQO%C%OB

Kunci: $K = (1\ 2\ 3\ 4\ 5\ 4\ 1\ 5\ 3\ 2\ )$

$K^{-1} = (4\ 1\ 5\ 3\ 2\ 1\ 2\ 3\ 4\ 5\ )$

$$K^{-1} = (1\ 2\ 3\ 4\ 5\ 2\ 5\ 4\ 1\ 3\ )$$

Membagi plainteks menjadi blok-blok yang terdiri dari lima huruf sebagai berikut:

TAXOQ	OYU#A	#FBQO	%C%OB

Selanjutnya, setiap blok diubah menjadi seperti di bawah ini dengan menggunakan kunci yang telah ditentukan.

Blok 1: $K^{-1} = (1\ 2\ 3\ 4\ 5\ 2\ 5\ 4\ 1\ 3\ ) = (1\ 2\ 3\ 4\ 5 TAXOQ 2\ 5\ 4\ 1\ 3 AQOTX\ )$

Blok 2: $K^{-1} = (1\ 2\ 3\ 4\ 5\ 2\ 5\ 4\ 1\ 3\ ) = (1\ 2\ 3\ 4\ 5\ OYU\#A\ 2\ 5\ 4\ 1\ 3\ YA\#OU\ )$

Blok 3: $K^{-1} = (1\ 2\ 3\ 4\ 5\ 2\ 5\ 4\ 1\ 3\ ) = (1\ 2\ 3\ 4\ 5\ \#FBQO 2\ 5\ 4\ 1\ 3\ FOQ\#B4\ )$

Blok 4: $K^{-1} = (1\ 2\ 3\ 4\ 5\ 2\ 5\ 4\ 1\ 3\ ) = (1\ 2\ 3\ 4\ 5\ \%C\%OB 2\ 5\ 4\ 1\ 3\ CBO\%\%\ ).$

Sehingga diperoleh plainteks yaitu AQOTXYA#OUFOQ#BCBO%% Diketahui karakter # menggantikan spasi dan karakter % menggantikan kekurangan pada blok maka plainteks yang diperoleh adalah AQOTXYA OUFOQ BCBO.

Plainteks yang diperoleh dari hasil dekripsi menggunakan cipher transposisi grup simetri akan digunakan sebagai cipherteks pada proses dekripsi menggunakan *affine cipher*.

Cipherteks: AQOTXYA OUFOQ BCBO

Kunci: $m = 11$ dan $b = 14$

Berdasarkan karakter alfabet yang digunakan, maka cipherteks AQOTXYA OUFOQ BCBO ekuivalen dengan diperoleh 0 16 14 19 23 24 0 -14 20 5 14 16 - 1 2 1 14. Dengan proses yang sama pada algoritma super enkripsi maka diperoleh numerik 20 12 0 17 15 8 20- 0 10 11 0 12 -13 6 13 0. Lalu dikembalikan ke huruf abjad menjadi UMARPIU AKLAM NGNA. Kemudian dikelompokan ke dalam

kata yang beranggotakan lima karakter menjadi UMARP-IU AK-LAM N-GNA. Proses terakhir adalah proses membalikan posisi karakter sehingga diperoleh PRAMUKA UIN MALANG.

Kesimpulan

Berdasarkan pembahasan mengenai algoritma yang menggabungkan *affine cipher* dan *cipher* transposisi grup simetri, serta modifikasi *affine cipher* dan *cipher* transposisi grup simetri maka dapat ditarik kesimpulan bahwa proses enkripsi dilakukan melalui dua tahap sehingga dapat meningkatkan keamanan dan menghasilkan *cipher* yang sulit dipecahkan. Proses pertama adalah mengenkripsi plainteks menggunakan algoritma *Affine cipher* atau modifikasi *affine cipher*. Kemudian dilanjut dengan proses kedua, yaitu mengenkripsikan kembali cipherteks dari *Affine cipher* menggunakan algoritma *cipher* transposisi grup simetri. Sedangkan proses pengembalian cipherteks menjadi plainteks diawali dengan mendekripsikan cipherteks menggunakan algoritma cipher transposisi grup simetri. Kemudian hasil dari proses dekripsi cipher transposisi grup simetri didekripsikan kembali menjadi plainteks menggunakan algoritma *Affine cipher* atau modifikasi *affine cipher*.

Referensi

[1] A. B. Nasution, “Modifikasi Algoritma Affine Cipher untuk Mengamankan Data,” *J. Teknol. Inf.*, vol. 4, no. 2, pp. 377–382, 2020.

[2] P. C. Van Oorschot, A. J. Menezes, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1996.

[3] B. Anwar, R. Kustini, and I. Zulkarnain, “Penerapan Algoritma RSA (Rivest Shamir Adelman) Untuk Mengamankan Nilai Siswa SMP HKBP P. Bulan,” *J. Teknol. Sist. Inf. dan Sist. Komput. TGD*, vol. 4, no. 1, pp. 88–91, 2021.

[4] D. Djumhadi and A. Hamka, “APLIKASI MOBILE MESSENGER DENGAN KEAMANAN DATA MENGGUNAKAN METODE SHIFT CHIPPER (CAESAR) KRIPTOGRAFI,” *Pros. Semin.*, vol. 3, no. 1, pp. 47–53, 2021.

[5] R. OKTARIA, “PERANCANGAN APLIKASI PEMBELAJARAN KRIPTOGRAFI PADA ALGORITMA DATA ENCRYPTION SYSTEM (DES) MENGGUNAKAN METODE COMPUTER ASSISTED INTRUCTION,” *JTIK (Jurnal Tek. Inform. Kaputama)*, vol. 3, no. 2, pp. 18–28, 2019.

[6] R. Munir, “Kriptografi Edisi Kedua,” *Bandung Inform.*, 2019.

[7] N. P. E. Merliana, “Pemanfaatan Teknologi Kriptografi dalam mengatasi kejahatan Cyber,” *Satya Dharma J. Ilmu Huk.*, vol. 3, no. 2, pp. 23–40, 2020.

[8] S. Suhardi, “Kombinasi Metode Affine Cipher Dan ExclusiveOR (XOR) Dalam Pengamanan Pesan,” 2021.

[9] N. Nurjamiyah, “Implementasi Algoritma Affine Cipher untuk Keamanan Data Teks,” *Query J. Inf. Syst.*, vol. 4, no. 1, 2020.

[10] Y. Permanasari, “Kriptografi Klasik Monoalphabetic,” *Mat. J. Teor. dan Terap. Mat.*, vol. 16, no. 1, 2017.

[11] K. R. Devi and G. N. Harshini, “Analysis and Comparison of Substitution and Transposition Cipher,” *Int. J. Res. Anal. Rev.*, vol. 6, no. 2, pp. 549–555, 2019.

[12] W. Riskiyah, “Enkripsi dan dekripsi pesan menggunakan grup simetri untuk mengamankan informasi.” Universitas Islam Negeri Maulana Malik Ibrahim, 2016.

[13] P. Poonia and P. Kantha, “Comparative Study of Various Substitution and Transposition Encryption Techniques,” *Int. J. Comput. Appl*, vol. 145, no. 10, pp. 24–27, 2016.

[14] R. A. Megantara and F. A. Rafrastara, “Super Enkripsi Teks Kriptografi Menggunakan Algoritma Hill Cipher Dan Transposisi Kolom,” 2019.

[15] E. Setyaningsih, C. Iswahyudi, and N. Widyastuti, “Konsep Super Enkripsi untuk Meningkatkan Keamanan Data Citra,” 2011.

[16] R. Mubarak, “Implementasi Sistem Keamanan Data Berbasis Kriptografi Rivest Code 6,

Vigenere Chipper dan Kompresi Data LZW," *Insa. Pembang. Sist. Inf. dan Komput.*, vol. 8, no. 2, 2020.
[17] M. K. Amrulloh, "Penyandian model kriptografi playfair cipher dengan menggunakan metode shiftrows." Universitas Islam Negeri Maulana Malik Ibrahim, 2021.
[18] F. A. Saputro, "Implementasi algoritma One Time Pad Cipher dan transformasi Rail Fence Cipher pada pesan teks." Universitas Islam Negeri Maulana Malik Ibrahim, 2020.
[19] M. K. Harahap, "Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher dan One Time Pad," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 1, no. 1, pp. 61–64, 2016.
[20] H. Mukhtar, *Kriptografi Untuk Keamanan Data*. Deepublish, 2018.