IMPLEMENTASI ALGORITMA SUPER ENKRIPSI (*AFFINE CIPHER* DAN *ROUTE CIPHER*) PADA PESAN TEKS

SKRIPSI

OLEH
RENA ALVIONITA
NIM. 14610089

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2021

IMPLEMENTASI ALGORITMA SUPER ENKRIPSI (*AFFINE CIPHER* DAN *ROUTE CIPHER*) PADA 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
Rena Alvionita
NIM.14610089

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2021

IMPLEMENTASI ALGORITMA SUPER ENKRIPSI (*AFFINE CIPHER* DAN *ROUTE CIPHER*) PADA PESAN TEKS

SKRIPSI

OLEH
RENA ALVIONITA
NIM.14610089

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 11 Juni 2021

Pembimbing I,	Pembimbing II,
Muhammad Khudzaifah, M.Si	Muhammad Nafie Jauhari, M.Si
NIP. 19900511 20160801 1 057	NIP. 19870218 20160801 1 056

Mengetahui,
Ketua Program Studi Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001

IMPLEMENTASI ALGORITMA SUPER ENKRIPSI (*AFFINE CIPHER* DAN *ROUTE CIPHER*) PADA PESAN TEKS

SKRIPSI

Oleh
Rena Alvionita
NIM.14610089

Telah Dipertahankan di Depan Dewan Penguji Skripsi
Dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
Untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 18 Juni 2021

Penguji Utama	: Dr. Heni Widayani, M.Si	.....
Ketua Penguji	: Juhari, M.Si	.....
Sekretaris Penguji	: Muhammad Khudzaifah, M.Si	.....
Anggota Penguji	: Muhammad Nafie Jauhari, M.Si	.....

Mengetahui,
Ketua Program Studi Matematika

Dr. Usman Pagalay, M.Si
NIP.1965041420003121 1 001

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Rena Alvionita

NIM : 14610089

Jurusan : Matematika Fakultas Sains dan Teknologi

Judul : Implementasi Algoritma Super Enkripsi (*Affine Cipher dan Route Cipher*) pada Pesan Teks

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

Malang, 11 Juni 2021

Yang membuat pernyataan,

Rena Alvionita

NIM. 14610089

MOTO

"Boleh jadi kamu membenci sesuatu padahal ia amat baik bagimu, dan boleh jadi pula kamu menyukai sesuatu padahal ia amat buruk bagimu, Allah mengetahui sedang kamu tidak mengetahui." (QS/Al Baqarah:216)

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:

Kedua orangtua ayahanda Triswanto dan ibunda Jumani, beserta temanku Izah yang selalu memberikan nasihat dan semangat bagi penulis.

KATA PENGANTAR

Assalamua'laikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah Swt. atas rahmat, taufik serta hidayah-Nya, sehingga penulis mampu menyelesaikan penyusunan skripsi yang berjudul "Implementasi Algoritma Super Enkripsi (*Affine Cipher* dan *Route Cipher*) pada Pesan Teks" sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang matematika di Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Dalam proses penyusunan skripsi ini, penulis banyak mendapat bimbingan dan arahan dari berbagai pihak. Untuk itu ucapan terima kasih yang sebesar-besarnya dan penghargaan yang setinggi-tingginya penulis sampaikan terutama kepada:

1. Prof. Dr. H. Abd. Haris, M.Ag, selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Usman Pagalay, M.Si, selaku ketua Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Ari Kusumastuti M.Si, M.Pd selaku sekertaris Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang yang selalu memberi motivasi dan semangat kepada penulis.

5. Muhammad Khudzaifah, M.Si, selaku dosen pembimbing I yang telah banyak memberikan arahan, nasihat, motivasi, dan berbagai pengalaman yang berharga kepada penulis.
6. Muhammad Nafie Jauhari, M.Si, selaku dosen pembimbing II yang telah banyak memberikan arahan dan berbagi ilmu kepada penulis.
7. Dr. Heni Widayani, M.Si, selaku dosen penguji utama yang telah banyak memberikan arahan dan nasihat kepada penulis.
8. Juhari, M.Si, selaku ketua penguji yang telah banyank memberikan nasihat kepada penulis.
9. Segenap sivitas akademika Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang terutama seluruh dosen, terima kasih atas segala ilmu dan bimbingannya.
10. Ayah dan Ibu yang selalu memberikan do'a, semangat, serta nasihat kepada penulis sampai saat ini.

Akhirnya penulis berharap semoga skripsi ini bermanfaat bagi penulis dan bagi pembaca.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, 24 Juni 2021

Penulis

DAFTAR ISI

DAFTAR GAMBAR

ABSTRAK

Alvionita, Rena. 2021. **Implementasi Algoritma Super Enkripsi (*Affine Cipher* dan *Route Cipher*) Pada Pesan Teks.** Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si. (II) Muhammad Nafie Jauhari, M.Si.

Kata Kunci: Enkripsi, Dekripsi, Super Enkripsi, *Affine Cipher*, *Route Cipher*.

Super enkripsi merupakan suatu algoritma yang menggabungkan dua atau lebih dari *cipher* substitusi dan transposisi untuk memperoleh algoritma yang lebih sulit dipecahkan. Penelitian ini bertujuan untuk mengetahui bagaimana keamanan enkripsi dan dekripsi pada pesan teks menggunakan algoritma super enkripsi (*affine cipher* dan *route cipher*). Proses super enkripsi pada penelitian ini yaitu dengan menggabungkan *affine cipher* dan *route cipher*. *Affine cipher* adalah salah satu teknik kriptografi yang termasuk dalam teknik kriptografi klasik dengan menggunakan substitusi dan *route cipher* adalah salah satu teknik kriptografi yang termasuk dalam teknik kriptografi klasik dengan menggunakan transposisi dalam melakukan penyandiannya. Pada proses super enkripsi ini, *plaintext* akan dienkripsi dua kali dengan menggunakan algorima *affine cipher* terlebih dulu dan dilanjutkan dengan enkripsi *route cipher*. Selanjutnya hasil *ciphertext* yang diperoleh dari proses enkripsi kedua algoritma tersebut akan didekripsikan untuk memperoleh pesan asli (*plaintext*) semula. Pengamanan pesan menjadi sangat efektif dengan menggunakan algoritma super enkripsi, karena pesan tersebut dienkripsi dan didekripsi dengan dua tahap. Sehingga pesan tersebut tidak akan mudah diketahui oleh pihak lain.

ABSTRACT

Alvionita, Rena. 2021. ***Implementation of Super Encryption Algorithm (Affine Cipher and Route Cipher) in Text Messages.*** Thesis. Mathematics Study Program, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University of Malang. Advisors: (I) Muhammad Khudzaifah, M.Si. (II) Muhammad Nafie Jauhari, M.Si.

Keywords: Encryption, Decryption, Super Encryption, Affine Cipher, Route Cipher.

Super encryption is an algorithm that combines two or more *cipher* substitution and transposition to obtain an algorithm that is more difficult to crack. This study aims to determine the security of encryption and decryption of text messages using a super encryption algorithm (affine cipher and route cipher). The super encryption process in this research is by combining affine cipher and route cipher. Affine cipher is one of the cryptography techniques in classical cryptography techniques using substitution. Route cipher these techniques are include in classical cryptography techniques using transposition in encoding. In this super encryption process, the plaintext will be encrypted twice using the algorithm affine cipher first and followed by route cipher encryption. Furthermore, the results of the ciphertext obtained from the encryption process of the two algorithms will be decrypted to obtain the original message (*plaintext*). Message security becomes effective by using a super encryption algorithm because the message is encrypted and decrypted in two stages. So that the message will not be easily known by other parties.

ملخص

ألفيونيتا ، رينا. .2021. **تنفيذ خوارزمية التشفير الفائق (التشفير الفرعي وتشفير المسار) في الرسائل النصية**. البحث العلمي. قسم الرياضيات ، كلية العلوم والتكنولوجيا ، جامعة مولانا مالك إبراهيم الإسلامية الحكومية بمالانج. المشرف: المشرف الأول (١) محمد حذيفة، الماجستير، المشرف الثاني (٢) محمد نافع جوهري، الماجستير.

الكلمات الرئيسية: التشفير, وصف, التشفير الفائق, أفيني التشفير, طريق التشفير.

التشفير الفائق عبارة عن خوارزمية تجمع بين الإثنين أو الأكثر من أصفار الاستبدال والتبديل للحصول على خوارزمية يصعب فكها. أهداف هذه الدراسة لتحديد أمن التشفير وفك التشفير للرسائل النصية باستخدام خوارزمية تشفير فائق (أفيني الشفرات والطريق الشفرات).عملية التشفير الفائقة في هذا البحث هو الجمع بين الشفرات أفيني والشفرات الطريق. التشفير الأفيني هو أحد تقنيات التشفير المتضمنة في تقنيات التشفير الكلاسيكية باستخدام الاستبدال وأشفار المسار هي إحدى تقنيات التشفير المضمنة في تقنيات التشفير الكلاسيكية باستخدام التحويل في التشفير. في عملية التشفير الفائق هذه ، النص العادي سيتم تشفير مرتين باستخدام خوارزمية التشفير الأفيني أولاً ثم يليه تشفير المسار .علاقة على ذلك ،نتائج النص المشفر الذي سيتم فك تشفيرتم الحصول عليه من عملية التشفير للخوارزميتين للحصول على الرسالة الأصلية) نص عادي .(يصبح أمان الرسائل فعالاً للغاية باستخدام خوارزمية تشفير فائقة، لأن الرسالة يتم تشفيرها وفك تشفيرها على مرحلتين. حتى لا تعرف الرسالة بسهولة من قبل الأطراف الأخرى.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan pesan ataupun keamanan informasi ialah suatu perihal yang sangat berarti. Dalam upaya melindungi suatu data biar tidak gampang dikenal oleh pihak yang tidak berkepentingan dituntut terdapatnya suatu mekanisme yang baik dalam mengamankan pesan. Ilmu yang berkaitan untuk melindungi keamanan pesan merupakan kriptografi. Kriptografi adalah ilmu yang menekuni bagimana melaksanakan enkripsi serta dekripsi, dengan menggunakan model matematika tertentu. Kriptografi diilhami dengan metode enkripsi ataupun metode penyandian yang mengganti suatu pesan yang bisa dibaca (*plaintext*) menjadi suatu pesan yang acak serta susah diartikan. Sedangkan untuk membaca pesan yang terenkripsi dibutuhkan proses terbalik dari enkripsi yang disebut sebagai metode dekripsi (Kurniawan, 2008).

Kerahasiaan serta keamanan suatu pesan merupakan perihal yang sangat berarti dalam pertukaran pesan ataupun informasi, baik untuk tujuan keamanan bersama ataupun untuk keamanan pribadi. Sudah seharusnya informasi hanya boleh disampaikan kepada orang yang berhak menerimanya saja, seperti firman Allah dalam surat an- Nisa'/4 (58):

"*sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada mereka yang berhak menerimanya".*

Mereka yang ingin supaya datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara mengamankan pesan informasi yang akan dikomunikasikan. Fungsi matematika yang digunakan untuk

enkripsi dan dekripsi disebut algoritma kriptografi (Kurniawan, 2008). Salah satu algoritma kriptografi yang dapat dimanfaatkan adalah algoritma super enkripsi. Super enkripsi merupakan salah satu kriptografi yang menggabungkan *cipher* substitusi dan *cipher* transposisi untuk mendapatkan *cipher* yang lebih kuat tidak mudah dipecahkan.

Affine Cipher adalah suatu metode yang mana setiap huruf-huruf alfabetnya diubah ke dalam bentuk angka-angka dan kemudian disandikan dengan suatu persamaan. *Affine Cipher* merupakan metode penyandian pesan yang mana dalam penyandian tersebut menggunakan algoritma kriptografi klasik. Algoritma kriptografi klasik terdiri dari teknik substitusi dan teknik transposisi. Teknik substitusi yaitu proses mensubstitusi karakter-karakter yang ada pada *plaintext.* Sedangkan teknik transposisi yaitu proses pertukaran huruf-huruf. Algoritma *Route Cipher* adalah salah satu algoritma transposisi, yang memiliki perluasan kunci sama seperti *rail fance cipher* (Kromodimoeljo, 2010). Algoritma *Route Cipher* juga sering disebut dengan Spiral *Cipher*.

Penelitian mengenai kriptografi sudah banyak bermunculan, salah satunya tentang *Affine Cipher*. Pada penelitian Maulana (2019) menjelaskan tentang proses enkripsi dan dekripsi pada polinomial menggunakan metode *Affine Cipher.* Proses enkripsi pada penelitian tersebut dilakukan dengan menentukan polinomial tak tereduksi, kemudian pesan yang masuk dikonversi dengan tabel ASCII. Sedangkan proses dekripsi diperoleh dengan memasukkan *invers* kunci dari proses enkripsi ke persamaan dekripsi *Affine Cipher.* Penelitian lain, yaitu tentang implementasi algoritma *Route Cipher* dalam pengamanan file PDF. Pada penelitian Bangun (2019) algoritma *Route Cipher* melakukan enkripsi terhadap

file PDF dengan menggunakan kunci yang dapat membentuk matriks, kemudian menentukan arah enkripsi berdasarkan persetujuan antara penerima dan pengirim. Prosedur pengamanan *file* PDF adalah dengan menghitung nilai-nilai dari karakter isi teks *file* dengan menggunakan kunci yang menghasilkan *ciphertext* yang didapat berdasarkan algoritma yang digunakan.

Berdasarkan uraian di atas, maka peneliti ingin melakukan suatu kajian penelitian yang berjudul "*Implementasi Algoritma Super Enkripsi* (*Affine Cipher dan Route Cipher*) *Pada Pesan Teks"*.

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka rumusan masalah penelitian ini sebagai berikut:

1. Bagaimanakah proses enkripsi pada pesan teks menggunakan algoritma super enkripsi (*Affine Cipher* dan *Route Cipher*)?
2. Bagaimanakah proses dekripsi pada pesan teks menggunakan algoritma super enkripsi (*Affine Cipher* dan *Route Cipher*)?

1.3 Tujuan Penelitian

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

1. Mengetahui proses enkripsi pesan teks menggunakan algoritma super enkripsi (*Affine Cipher* dan *Route Cipher*).
2. Mengetahui proses dekripsi pesan teks menggunakan algoritma super enkripsi (*Affine Cipher* dan *Route Cipher*).

1.4 Manfaat Penelitian

Adapun beberapa manfaat yang terdapat pada penelitian ini, adalah sebagai berikut:

1. Sebagai bahan referensi serta memperdalam pengetahuan tentang implementasi algoritma super enkripsi (*Affine Cipher* dan *Route Cipher*) pada pesan teks.
2. Mengetahui keamanan pesan teks menggunakan algoritma super enkripsi (*Affine Cipher* dan *Route Cipher*).

1.5 Batasan Masalah

Adapun batasan masalah dalam penelitian yang akan dibahas sebagai berikut:

1. Hanya mengenkripsi bentuk alfabet (huruf kapital dan huruf kecil).
2. Kunci yang digunakan untuk enkripsi dan dekripsi, yaitu $m = 5$ dan $b = 8$ (yang mana m relatif prima dengan $n = 26$) untuk *cipher* substitusi. Sedangkan pada *cipher* transposisi $k = 7$.

1.6 Metode Penelitian

Metode penelitian yang akan digunakan penulis adalah studi literatur dengan mempelajari dan menelaah beberapa buku, jurnal, dan referensi lain yang mendukung penelitian ini. Adapaun langkah-langkah penelitian yang penulis gunakan adalah sebagai berikut.

Proses enkripsi dengan menggunakan metode super enkripsi:

a. Menentukan data atau pesan teks (*plaintext*).
b. Menentukan kunci.

c. Mengkonversi alfabet ke $\mathbb{Z}_{26}$.
d. Melakukan perhitungan dengan substitusi.
e. Melakukan perhitungan dengan transposisi dari hasil perhitungan substitusi.
f. Mengkonversi $\mathbb{Z}_{26}$ ke alfabet.
g. Mendapatkan pesan teks yang sudah disandikan (*ciphertext*).

Proses dekripsi dengan menggunakan metode super enkripsi:

a. Memasukkan pesan yang sudah disandikan (*ciphertext*).
b. Menentukan kunci.
c. Melakukan perhitungan dengan transposisi.
d. Mengkonversi alfabet ke $\mathbb{Z}_{26}$.
e. Melakukan perhitungan dengan substitusi dari hasil perhitungan transposisi.
f. Mengkonversi $\mathbb{Z}_{26}$ ke alfabet.
g. Mendapatkan pesan teks asli (*plaintext*).

1.7 Sistematika Penulisan

Sistematikaa penulisan yang digunakan pada penelitian ini terdiri dari empat bab, yaitu:

Bab I Pendahuluan

Pada bab ini diuraikan tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

Bab II Kajian Pustaka

Pada bab ini menjelaskan tentang gambaran umum dari teori yang mendasari pembahasan.

Bab III Pembahasan

Pada bagian ini merupakan bab inti dari penulisan penelitian yang dilakukan berisi penyelesaian.

Bab IV Penutup

Pada bab ini berisi kesimpulan dari hasil pembahasan yang diperoleh.

BAB II

KAJIAN PUSTAKA

2.1 Teori Bilangan

Menurut pengertiannya, kajian tentang sifat-sifat bilangan asli disebut dengan teori bilangan bulat. Dalam pengertian yang lebih luas, teori bilangan mempelajari bilangan dan sifat-sifatnya. Teori bilangan adalah salah satu cabang matematika dan dapat disebut sebagai "aritmatika lanjut (*advanced aritmetics*)*"* karena saling berkaitan dengan sifat-sifat bilangan asli (Muhsetyo, 1997).

2.1.1 Bilangan Bulat

Bilangan bulat adalah bilangan yang tidak mempunyai pecahan desimal. Himpunan semua bilangan bulat yang dinotasikan dengan $\mathbb{Z}$ diambil dari kata *Zahlen* dari bahasa Jerman atau dinotasikan dengan I yang diambil dari huruf pertama kata *Integer* dari bahasa Inggris, adalah himpunan $\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$. Himpunan bilangan bulat dibagi menjadi tiga bagian, yaitu bilangan bulat positif, yaitu bilangan bulat yang lebih besar dari nol yang dituliskan $\mathbb{Z}^+$, nol, dan bilangan bulat negatif, yaitu bilangan bulat yang lebih kecil dari nol yang dituliskan $\mathbb{Z}^-$ (Abdussakir, 2009).

2.1.2 Keterbagian

Definisi:

Misalkan $a, b \in \mathbb{Z}$ dengan $a \neq 0$, maka a disebut membagi b ditulis sebagai $a|b$ apabila $b = ak$, untuk suatu $k \in \mathbb{Z}$. Berdasarkan dari definisi di atas, suatu bilangan bulat a dengan $a \neq 0$, dikatakan membagi bilangan bulat b jika ada Notasi $a|b$ dibaca dengan "a membagi b" atau "b habis dibagi a"

atau "a pembagi b" atau "a faktor dari b", atau b kelipatan dari a". Jika a tidak membagi b, maka ditulis sebagai $a \nmid b$. Jika $a|b$ dan $0 < a < b$, maka a disebut pembagi sejati dari b (Irawan, dkk, 2014).

Contoh:

$3|12$, karena ada $4 \in \mathbb{Z}$ sehingga $12 = 3 \cdot 4$

$3 \nmid 8$, karena tidak ada $k \in \mathbb{Z}$ sehingga $8 = 3k$

2.1.3 Pembagi Bersama Terbesar

Definisi:

Misalkan a dan b adalah dua buah bilangan bulat tidak nol. Pembagi bersama terbesar (PBB) dari a dan b adalah bilangan bulat terbesar d sedemikian sehingga $d|a$ dan $d|b$. Dalam hal ini dinyatakan bahwa PBB $(a, b) = d$ (Munir, 2005).

Teorema:

Jika c adalah PBB dari a dan b, maka $c(a + b)$.

Bukti:

Karena c adalah PBB dari a dan b, maka ca dan cb. Karena ca, maka berarti $a = cd_2$ untuk suatu bilangan bulat d_2.

$$a + b = cd_1 + cd_2 = c(d_1 + d_2)$$

Terlihat bahwa c habis membagi $a + b$.

Contoh:

Faktor pembagi $24 = 1, 2, 3, 4, 6, 8, 12, 24$;

Faktor pembagi $18 = 1, 2, 3, 6, 9, 18$;

Faktor pembagi bersama dari 24 dan 18 adalah $1, 2, 3, 6$.

PBB $(24, 18) = 6$.

2.1.4 Relatif Prima

Definisi:

Dua buah bilangan bulat a dan b dikatakan relatif prima jika PBB $(a, b) = 1$ (Munir, 2005).

Contoh:

Faktor pembagi $10 = 1, 2, 5, 10$;

Faktor pembagi $21 = 1, 3, 7, 21$;

Faktor pembagi bersama dari 10 dan 21 adalah 1

Jadi, 10 dan 21 adalah relatif prima karena PBB $(10, 21) = 1$.

Tetapi 20 dan 5 tidak relatif prima, karena Faktor pembagi $20 = 1, 2, 4, 5, 10, 20$;

Faktor pembagi $5 = 1, 5$;

Faktor pembagi bersama dari 10 dan 21 adalah 1 dan 5

PBB $(20, 5) = 5 \neq 1$.

Jika a dan b relatif prima, maka terdapat bilangan bulat m dan n sedemikian sehingga

$$ma + nb = 1$$

Bilangan 10 dan 21 adalah relatif prima karena PBB $(10, 21) = 1$, atau dapat ditulis

$$(-2) \cdot 10 + (1) \cdot 21 = 1$$

dengan $m = -2$ dan $n = 1$. Tetapi 20 dan 5 tidak relatif prima karena PBB $(20, 5) = 5 \neq 1$ sehingga 20 dan 5 tidak dapat dinyatakan dalam $m \cdot 20 + n \cdot 5 = 1$ (Munir, 2005).

2.1.5 Kongruensi Modulo

Definisi:

Jika sebuah bilangan bulat M yang tidak nol, membagi selisih $a - b$, maka dikatakan a kongruen dengan b modulo M, dan ditulis:

$$a \equiv b \ (mod\ M)$$

Jika $a - b$ tidak membagi M, maka dikatakan tidak kongruen dengan $b\ mod\ M$, dan dapat ditulis $a \not\equiv b \ (mod\ M)$ (Irawan, dkk, 2014).

Teorema:

Misalkan m adalah bilangan bulat positif.

1. Jika $a \equiv b \ (mod\ m)$ dan c adalah sebarang bilangan bulat maka:

$$ac \equiv bc \ (mod\ m)$$

2. Jika $a \equiv b \ (mod\ m)$ dan $c \equiv d \ (mod\ m)$, maka

$$(a + c) \equiv (b + d) \ (mod\ m)$$

Bukti:

1. $a \equiv b\ mod\ m$ berarti:

$$\Leftrightarrow a = b + km$$

$$\Leftrightarrow a - b = km$$

$$\Leftrightarrow (a - b)c = ckm$$

$$\Leftrightarrow ac = bc + ckm$$

$$\Leftrightarrow ac \equiv bc \ (mod\ m)$$

2. $a \equiv b \ (mod\ m) \Leftrightarrow a = b + k_1 m$

   $c \equiv d \ (mod\ m) \Leftrightarrow c = d + k_2 m$

$$\Leftrightarrow (a + c) = (b + d) + (k_1 + k_2)m$$

$$\Leftrightarrow (a + c) = (b + d) + km, \quad (k = k_1 + k_2)$$

$$\Leftrightarrow (a + c) = (b + d) \ (mod\ m)$$

Contoh:

$22 \equiv 4\ (mod\ 9)$, karena $(22 - 4)$ terbagi oleh 9

$35 \equiv 6\ (mod\ 7)$, karena $(35 - 6)$ tidak terbagi oleh 7

$-8 \equiv 25\ (mod\ 11)$, karena $\big((-8) - 25\big)$ terbagi oleh 11

$-8 \equiv 25\ (mod\ 7)$, karena $\big((-8) - 25\big)$ tidak terbagi oleh 7

Kekongruenan $a \equiv b\ (mod\ m)$ dapat juga dituliskan dalam hubungan

$$a = b + km$$

yang mana k adalah bilangan bulat.

Contoh:

$22 \equiv 4\ (mod\ 9)$ dapat ditulis sebagai $22 = 4 + 2 \cdot 9$

$-8 \equiv 25\ (mod\ 11)$ dapat ditulis sebagai $-8 = 25 + \big((-3)11\big)$

2.1.6 Aritmetika Modulo

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi $a\ mod\ m$ memberikan sisa apabila a dibagi dengan bilangan m disebut modulus atau modulo, dan hasil operasi modulo m terletak didalam himpunan $\{0,1,2, \cdots m - 1\}$ (Munir, 2019).

Contoh:

i. $23\ mod\ 5 = 3$ $\quad (23 = 5 \cdot 4 + 3)$

ii. $27\ mod\ 3 = 0$ $\quad (27 = 3 \cdot 9 + 0)$

iii. $6\ mod\ 8 = 6$ $\quad (6 = 8 \cdot 0 + 6)$

2.1.7 Balikan (*Invers*) Modulo

Definisi:

Jika a dan m adalah relatif prima dan $m > 1$, maka kita dapat menemukan balikan (*invers*) dari a modulo m. Balikan dari a modulo m adalah bilangan bulat $\bar{a}$ sedemikian sehingga (Munir, 2005)

$$a\bar{a} \equiv 1(mod\ m)$$

Bukti:

Berdasarkan dari definisi relatif prima diketahui bahwa PBB $(a, m) = 1$, dan terdapat bilangan bulat p dan q sedemikian sehingga

$$pa + qm = 1$$

yang mengimplikasikan bahwa

$$pa + qm = 1(mod\ m).$$

Karena $qm \equiv 0\ (mod\ m)$, maka

$$pa \equiv 1(mod\ m)$$

Kekongruenan yang terakhir ini berarti menyatakan bahwa p adalah balikan dari a modulo m.

Pembuktian di atas juga menjelaskan bahwa untuk mencari balikan dari a modulo m, harus membuat kombinasi linear dari a dan m sama dengan 1. Koefisien a dari kombinasi linear tersebut merupakan balikan dari a modulo m (Munir, 2005).

Contoh:

Tentukan balikan dari $4\ mod\ 9$ dan $25\ mod\ 10$.

Penyelesaian:

1. Karena PBB $(4, 9) = 1$, maka $4^{-1}\ (mod\ 9)$ ada. Dari algoritma *Euclidean* diperoleh bahwa

$$9 = 2 \cdot 4 + 1$$

susun persamaan di atas menjadi

$$(-2) \cdot 4 + 1 \cdot 9 = 1$$

Dari persamaan terakhir ini diperoleh -2 adalah balikan dari $4\ (mod\ 9)$. Dengan kata lain, $4^{-1}\ (mod\ 9) = -2\ (mod\ 9)$.

2. Karena PBB $(25, 10) = 5 \neq 1$, maka balikan dari $25\ (mod\ 10)$ tidak ada.

2.1.8 Kekongruenan Linear

Kekongruenan linear adalah kongruen yang berbentuk,

$$ax = b\ (mod\ m)$$

dengan m adalah bilangan bulat positif, a dan b sebarang bilangan bulat, dan x adalah peubah bilangan bulat. Cara yang sangat sederhana untuk mencari nilai-nilai x tersebut adalah dengan menggunakan persamaan $a = b + km$. Dapat disusun menjadi $x = \frac{b+km}{a}$ dengan k adalah sebarang bilangan bulat. Dengan mencoba nilai-nilai dari $k = 0,1,2,\cdots$, dan $k = -1,-2,\cdots$, maka dapat menemukan semua nilai x bilangan bulat. Solusi kekongruenan linear tidaklah unik, artinya banyak nilai x yang akan memenuhi (Munir, 2019).

Adapun cara lain adalah dengan mengalikan kedua ruas dengan balikan modulo dari a. Caranya serupa dengan pencarian solusi pada persamaan linear biasa, seperti pada $4x = 12$. Untuk mencari solusi persamaan tersebut, mengalikan kedua ruas dengan balikan perkalian dari 4, yaitu $\frac{1}{4}$.

$$4x = 12$$

$$\frac{1}{4} \cdot 4x = \frac{1}{4} \cdot 12$$

$$1 \cdot x = 3$$

$$x = 3$$

Contoh:

Tentukan $4x \equiv 3(mod\ 9)$.

Kekongruenan $4x \equiv 3(mod\ 9)$ dapat ditulis sebagai $4x = 3 + 9k)$, atau $x = \frac{3+9k}{4}$.

Untuk,

$k = 0 \rightarrow x = \frac{(3+9\cdot 0)}{4} = \frac{3}{4}$ (bukan solusi karena bukan bilangan bulat)

$k = 1 \rightarrow x = \frac{(3+9\cdot 1)}{4} = 3$ (solusi)

Sebenarnya jika sudah ditemukan nilai x pertama kali, maka tidak perlu menghitung nilai x yang lain. Pada contoh di atas, nilai x pertama ditemukan adalah 3, maka solusinya secara umum dapat dinyatakan sebagai $x \equiv 3(mod\ 9)$ atau $x = 3 + 9k,\ k$ sebarang bilangan bulat (Munir, 2019).

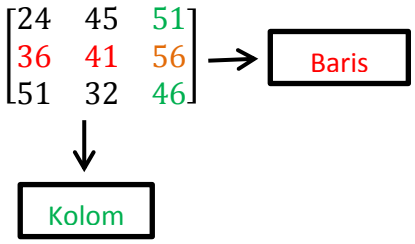
2.2 Matriks

Matriks adalah kumpulan dari bilangan yang disusun dengan cara tertentu dalam bentuk baris dan kolom sehingga membentuk empat persegi panjang atau bujur sangkar yang ditulis diantara dua tanda kurung, yaitu ( ) atau [ ] (Ruminta, 2014).

2.2.1 Ordo Matriks

Seperti yang sudah dijelaskan sebelumnya bahwa matriks terdiri atas unsur-unsur yang tersusun secara baris dan kolom. Apabila banyak baris dari suatu matriks adalah *m*, dan banyak kolom pada suatu matriks adalah *n*, maka matriks tersebut memiliki ordo matriks $m \times n$. *m* dan *n* hanyalah sebuah notasi,

sehingga tidak boleh dilakukan sebuah perhitungan (penjumlahan maupun perkalian). Pada contoh berikut diketahui bahwa:



Gambar 2.1. Ordo Matriks

dengan,

m = banyak baris yaitu 3

n = banyak kolom yaitu 3

$m \times n$ = ordo matriks yaitu 3×3

Notasi pada matriks menggunakan huruf kapital, sedangkan elemen-elemen didalamnya dinotasikan dengan huruf kecil sesuai dengan penamaan matriks dan diberi indeks *ij*. Indeks tersebut menyatakan posisi elemen pada matriks, yaitu baris ke-I dan kolom ke-*j*. Ada beberapa jenis matriks yang perlu diketahui adalah sebagai berikut:

1) Matriks Nol, matriks yang semua elemennya adalah nol.
2) Matriks Baris, matriks yang hanya memiliki satu baris.
3) Matriks Kolom, matriks yang hanya memiliki satu kolom.
4) Matriks Persegi, natriks yang memiliki jumlah kolm dan baris yang sama.
5) Matriks Identitas, matruks konstanta dengan elemen diagonal utama adalah I.

2.2.2 *Transpose* Matriks

Transpose matriks merupakan perubahan baris menjadi kolom dan sebaliknya. Jika $A_{m\times n}$ adalah sebuah matriks dengan ukuran $n \times m$, maka

transpose dari A dinyatakan oleh A^T, A^t, atau A' didefinisikan menjadi matriks $n \times m$ yang merupakan hasil dari pertukaran baris dan kolom matriks A,

Jika A dinyatakan: $A_{m\times n} = (a_{i,j})$, maka *transpose* matriks A dinyatakan: $A^T = (b_{i,j})$, dimana $(b_{i,j}), = (a_{i,j})$ (Ruminta, 2014).

Contoh:

$$\begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix} \text{di}\textit{transpose} \text{ menjadi } \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$$

2.3 Kriptografi

Kriptografi berasal dari bahasa yunani, menurut bahasa dibagi menjadi dua kripto dan graphia, kripto berarti *secret* (rahasia) dan graphia berarti *writing* (tulisan). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain (Ariyus, 2006). Kriptografi klasik merupakan suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Teknik ini sudah digunakan pada beberapa abad yang lalu. Dua teknik dasar yang biasa digunakan pada algoritma jenis ini adalah sebagai berikut:

1. Teknik Substitusi: penggantian setiap karakter plaintext dengan karakter lain.
2. Teknik Transposisi (permutasi): teknik ini menggunakan permutasi karakter (Ariyus, 2006).

Kriptografi modern adalah kriptografi pada era digital. Komputer digital merepresentasikan data dalam bentuk biner (0 dan 1), sehingga informasi dalam bentuk apapun bisa dienkripsi asalkan direpresentasikan dalam bentuk biner. Jika pasa kriptografi klasik enkripsi hanya sebatas huruf, maka dengan algoritma

kriptografi modern dapat mengenkripsi semua karakter, gambar, suara, video, objek 3-D, atau data digital lainnya (Munir, 2019).

2.3.1 Keamanan Pesan

Pesan (*message*) adalah data atau informasi yang dapat dibaca atau dimengerti maknanya. Nama lain untuk pesan adalah plainteks (*plaintext*) atau teks-jelas (*cleartext*). Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran telekomunikasi, dan kain sebagainya) atau yang disimpan di dalam media perekaman (kertas, *storage*, dan lain sebagainya). Pesan yang disimpan tidak hanya berupa teks, tetapi juga dapat berbentuk citra (*image*), suara/bunyi (*voice*), dan video. Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut *ciphertext. Cipherteks* harus dapat ditransformasikan kembali menjadi plainteks semula agar pesan yang diterima dapat dibaca.

Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan. Entitas disini dapat berupa orang, kartu kredit, dan sebagainya. Pengirim tentu ingin pesannya dapat dikirim secara aman, yaitu ia yakin bahwa pihak lain tidak dapat membaca isi pesan yang ia kirim. Solusinya adalah dengan cara menyandikan pesan menjadi *ciphertext* (Munir, 2006).

2.3.2 Algoritma Kriptografi

Algoritma ditinjau dari asal usul kata, kata algoritma mempunyai sejarah yang menarik, kata ini muncul di dalam kamus Webster sampai akhir tahun 1957

hanya menemukan kata algorism yang mempunyai arti proses perhitungan dengan bahasa Arab. Algoritma berasal dari nama penulis buku Arab yang terkenal yaitu Abu Ja'far Muhammad ibnu Musa al-Khuwarizmi (al-Khuwarizmi dibaca oleh orang barat menjadi algorism). Kata algorism lambat laun berubah menjadi algorithm.

Algoritma adalah urutan langkah-langkah logis untuk penyelesaian masalah yang disusun secara sistematis. Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut (Ariyus, 2006).

Algoritma kriptografi terdiri dari tiga fungsi dasar yaitu:

a) Enkripsi: Enkripsi merupakan hal yang sangat penting dalam kriptografi yang merupakan pengamanan data yang dikirimkan agar terjaga rahasianya. Pesan asli disebut *plaintext* yang dirubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *cipher* atau kode. Sama halnya dengan kita tidak mengerti akan sebuah kata, maka kita akan melihatnya di dalam kamus atau daftar istilah-istilah. Beda halnya dengan enkripsi, untuk merubah *plaintext* kebentuk *ciphertext* kita menggunakan algoritma yang dapat mengkodekan data yang kita inginkan.
b) Dekripsi: Dekripsi merupakan kebalikan dari enkripsi, pesan yang telah dienkripsi dikembalikan kebentuk asalnya *(plaintext)* disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan yang digunakan untuk enkripsi.
c) Kunci: kunci yang dimaksud disini merupakan kunci yang dipakai untuk melakukan enkripsi dan dekripsi, kunci terbagi menjadi dua bagian yaitu

kunci pribadi (*private key*) dan kunci umum (*public key*).

Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan dari kunci yang dipakainya (Ariyus, 2006):

1. Algoritma Simetri (menggunakan satu kunci untuk enkripsi dan deripsinya).
2. Algoritma Asimetri (menggunakan kunci yang berbeda untuk enkripsi dan dekripsi).
3. Hash Function.

2.4 Algoritma *Affine Cipher*

Affine cipher termasuk dalam *monoalphabetic substitution cipher* dimana setiap huruf-huruf alfabetnya dapat diubah ke dalam angka-angka kemudian disandikan dengan suatu persamaan (Kromodimoeljo, 2010). Kunci pada *Affine cipher* adalah dua *integer* m dan b, nilai m yang dapat dipakai adalah anggota elemen pada $\mathbb{Z}_{26}$ yang memiliki *invers* memenuhi $gcd(m, 26) = 1$ (Sadikin, 2012).

Affine cipher merupakan perluasan dari *caesar cipher*, dengan cara mengalikan plainteks P dengan sebuah nilai m lalu menambahkan hasilnya dengan sebuah nilai b. elemen m disebut nilai pergeseran multiplikatif, sedangkan b disebut nilai pergeseran aditif. Secara matematis enkripsi palinteks P yang menghasilkan cipherteks C dinyatakan dengan fungsi matematis:

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

yang dalam hal ini, n adalah ukuran alfabet, m adalah bilangan bulat yang harus relatif prima dengan n (jika tidak relatif prima, maka dekripsi tidak bisa dilakukan) dan b adalah jumlah pergeseran. *Caesar cipher* adalah kasus khusus

dari *affine cipher* dengan $m = 1$, sehingga menjadi $C = (P + b)\ mod\ m$, yang dalam hal ini $b = k$. Untuk melakukan dekripsi, persamaan (1) harus dipecahkan untuk memperoleh P. Solusinya hanya ada jika balikan dari $m(mod\ n)$, dinyatakan dengan m^{-1}. Jika m^{-1} ada maka dekripsi dilakukan dengan persamaan

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

Contoh:

Misalkan *plaintext* KRIPTO dienkripsi dengan *affine cipher* dengan mengambil $m = 7$ (karena 7 relatif prima dengan 26) dan $b = 10$. Karena alfabet yang digunakan 26 huruf, maka $n = 26$. Enkripsi plaintext *dihitung* dengan kekongruenan:

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

$$C = (7P + 10)\ mod\ 26$$

Misalkan

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

maka plainteks KRIPTO ekivalen dengan 10 17 8 15 19 14. Perhitungan enkripsi adalah sebagai berikut:

$p_1 = 10 \rightarrow c_1 = (7 \cdot 10 + 10)\ mod\ 26 = 80\ mod\ 26 = 2$ (huruf C)

$p_2 = 17 \rightarrow c_2 = (7 \cdot 17 + 10)\ mod\ 26 = 129\ mod\ 26 = 25$ (huruf Z)

$p_3 = 8 \rightarrow c_3 = (7 \cdot 8 + 10)\ mod\ 26 = 66\ mod\ 26 = 14$ (huruf O)

$p_4 = 25 \rightarrow c_4 = (7 \cdot 15 + 10)\ mod\ 26 = 115\ mod\ 26 = 11$ (huruf L)

$p_5 = 8 \rightarrow c_5 = (7 \cdot 19 + 10)\ mod\ 26 = 143\ mod\ 26 = 13$ (huruf N)

$p_6 = 8 \rightarrow c_6 = (7 \cdot 14 + 10)\ mod\ 26 = 108\ mod\ 26 = 4$ (huruf E)

Cipherteks yang dihasilkan adalah C Z O L N E.

Untuk melakukan dekripsi, pertama-tama harus ditentukan $7^{-1}(mod\ 26)$, yang dapat dihitung dengan memecahkan kekongruenan linear

$$7x \equiv 1\ (mod\ 26)$$

Solusinya adalah $x \equiv 15\ (mod\ 26)$ sebab $7 \cdot 15 = 105 \equiv 1(mod\ 26)$. Jadi, untuk dekripsi digunakan kekongruenan

$$P = 15(C - 10)\ mod\ 26$$

Perhitungan dekripsi adalah sebagai berikut:

$c_1 = 2 \rightarrow p_1 = 15(2 - 10)\ mod\ 26 = -120\ mod\ 26 = 10$ (huruf K)

$c_2 = 25 \rightarrow p_2 = 15(25 - 10)\ mod\ 26 = 225\ mod\ 26 = 17$ (huruf R)

$c_3 = 14 \rightarrow p_3 = 15(14 - 10)\ mod\ 26 = 60\ mod\ 26 = 8$ (huruf I)

$c_4 = 11 \rightarrow p_4 = 15(11 - 10)\ mod\ 26 = 15\ mod\ 26 = 15$ (huruf P)

$c_5 = 13 \rightarrow p_5 = 15(13 - 10)\ mod\ 26 = 45\ mod\ 26 = 19$ (huruf T)

$c_6 = 4 \rightarrow p_6 = 15(4 - 10)\ mod\ 26 = -90\ mod\ 26 = 14$ (huruf O)

Plainteks yang diungkap kembali adalah K R I P T O.

2.5 Algoritma *Route Cipher*

Route Cipher adalah salah satu jenis *cipher* yang merupakan perluasan *rail fance cipher*. Cara ini mirip karena menggunakan rute seperti rail fence, tetapi dalam hal ini rute bisa berupa apa saja seperti melingkar kedalam atau rute khusus. Biasanya kunci berupa cara baca (Irdayani, 2019). Pada algoritma *route cipher*, *plaintext* ditulis ke dalam sebuah *array* atau beberapa kata yang tersusun, kemudian dibaca sebagai perintah yang menentukan sebuah rute yang melalui

array. Dimana *plaintext* ditulis ke dalam sebuah *array* kemudian *ciphertext* dibaca dalam beberapa perintah.

Langkah-langkah algoritma *route cipher* adalah sebagai berikut:

1. Membuat matriks dengan jumlah baris yang akan diisi *plaintext,* yaitu dengan membagi jumlah *plaintext* dengan kunci.
2. Melakukan penentuan arah transposisi *plaintext*, contohnya jika arah yang ditentukan adalah spiral, maka *ciphertext* dihasilkan dengan membaca *plaintext* dalam matriks dengan arah spiral.
3. Untuk proses dekripsinya, algoritma route *cipher* hanya membaca posisi berdasarkan urutan kata yang disusun dalam matriks berdasarkan susunan dari arah yang digunakan untuk membentuk *ciphertext* (Bangun, 2019).

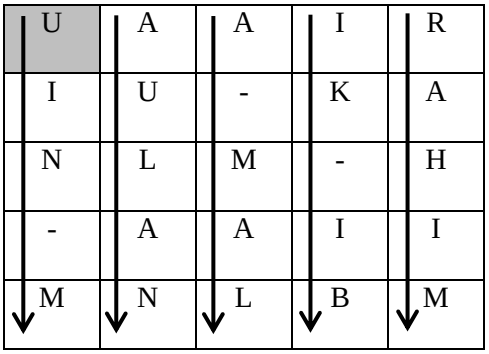
Algoritma *route cipher* merupakan salah satu teknik kriptografi yang termasuk di dalam teknik kriptografi klasik yang menggunakan transposisi dalam melakukan penyandian terhadap *plaintext*. *Route cipher* melakukan transposisi dengan cara menuliskan teks asli secara kolom dari atas ke bawah dalam sebuah kisi-kisi imajiner dengan ukuran yang telah disepakati. Teks sandinya dibaca dengan arah *(route)* sesuai perjanjian, misalnya dibaca secara spiral dengan searah atau berlawanan arah jarum jam, mulai dari kiri atas dan kanan atas, mulai dari kanan bawah dan lain sebagainya cara pembacaannya (Bangun, 2019).

Contoh:

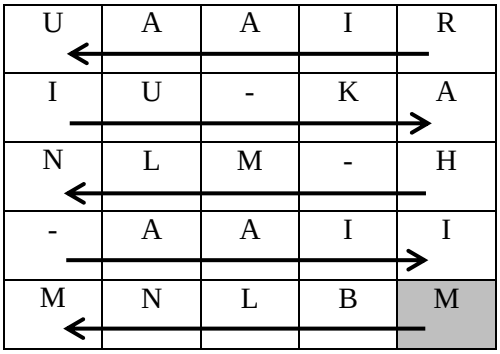
a. Proses Enkripsi

Plaintext: UIN MAULANA MALIK IBRAHIM Penulisan *plaintext* secara vertikal dari kolom atas ke bawah. Inputkan kunci untuk membentuk baris (*array*)

yang berdasarkan kunci, di dalam contoh ini kunci yang digunakan adalah 5 baris, spiral arah jarum jam mulai dari kanan bawah.



Kemudian *ciphertext* didapatkan dengan menyusun teks sesuai dengan arah yang sudah ditentukan dan mendapatkan hasil sebagai berikut:

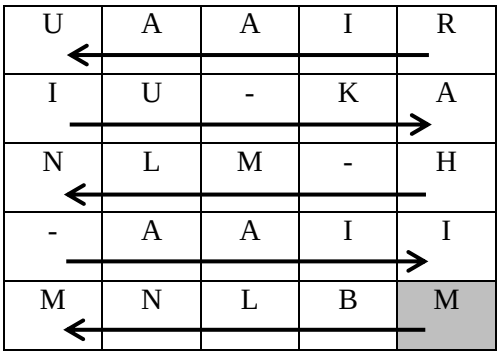


Ciphertext yang dihasilkan adalah MBLNM-AAIIH-MLNIU-KARIAAU.

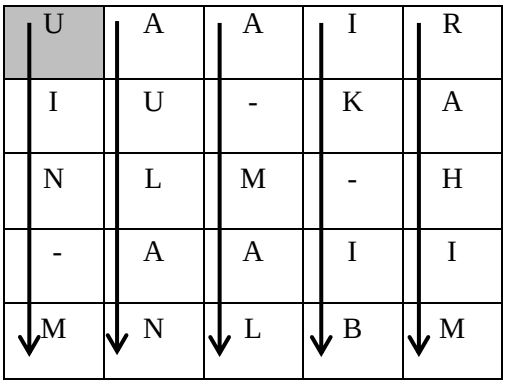
b. Proses Dekripsi

Ciphertext = MBLNM-AAIIH-MLNIU-KARIAAU

Inputkan kunci untuk membentuk baris (*array*) yang berdasarkan kunci, di dalam contoh ini kunci yang digunakan adalah 5. Penulisan *ciphertext* secara spiral arah jarum jam mulai dari kanan bawah.



Pembacaan *plaintext* perkolom mulai dari kolom pertama dan simbol (−) diubah menjadi spasi. Selanjutnya pembacaan plainteks akan dijabarkan dalam gambar dibawah ini.



Kemudian pembacaan *plaintext* didapatkan hasil sebagai berikut:

UIN MAULANA MALIK IBRAHIM

2.6 Super Enkripsi

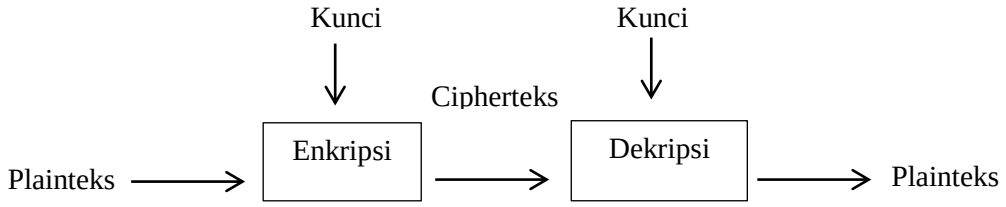
Cipher substitusi dan *cipher* transposisi dapat dikombinasikan untuk memperoleh *cipher* yang lebih kuat (*super*) daripada hanya satu *cipher* saja. Enkripsi dan dekripsi bisa dilakukan dengan urutan *cipher* substitusi kemudian *cipher* transposisi atau sebaliknya (Munir, 2019). Konsep super enkripsi dapat diperluas penggunaannya dari teks ke citra warna.

Adapun tahapan-tahapan dalam proses super enkripsi sebagai berikut:

1. Mengenkripsi *plaintext* menggunakan *affine cipher* dan menjadi suatu *ciphertext*.
2. Mengenkripsi kembali *ciphertext* tersebut menggunakan transposisi *route cipher*.
3. Mendekripsi *ciphertext* dari hasil proses enkripsi *route cipher* dengan transposisi *route cipher* terlebih dahulu.
4. Mendekripsi kembali hasil proses dekripsi *route cipher* tersebut dengan *affine cipher*.
5. Menghasilkan *plaintext* seperti pesan awal yang dikirim.

2.7 Proses Enkripsi dan Dekripsi Pesan

Enkripsi merupakan proses penyandian pesan asli (*plaintext*) menjadi *ciphertext.* Sedangkan dekripsi adalah proses mengembalikan *ciphertext* menjadi *plaintext*.



Gambar 2.2 Skema Enkripsi dan Dekripsi Pesan

Gambar diatas merupakan proses enkripsi menerima masukan berupa *plaintext* dan kunci, yang menghasilkan *ciphertext*. Sebaliknya, proses dekripsi menerima masukan berupa *ciphertext* dan kunci, hasilnya merupakan *plaintext* semula. Enkripsi dan dekripsi dapat digunakan baik pada pesan yang dikirim maupun pada pesan yang disimpan. Istilah *encryption of data in motion* mengacu pada pada enkripsi pesan yang ditransmisikan melalui saluran komunikasi, istilah

encryption of data at rest mengacu pada enkripsi dokumen yang disimpan di dalam memori (*storage*) (Munir, 2019).

2.7.1 Enkripsi Pesan dengan *Affine Cipher*

Plainteks: MATEMATIKA UIN MALANG

Kunci: $m = 5$ dan $b = 8$

Karakter dari alfabet yang digunakan : $(n) = 26$

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

maka plainteks MATEMATIKA UIN MALANG ekivalen dengan 12 0 19 4 12 0 19 8 10 0, 20 8 13, 12 0 11 0 13 6.

M	A	T	E	M	A	T	I	K	A	U	I	N	M	A	L	A	N	G
12	0	19	4	12	0	19	8	10	0	20	8	13	12	0	11	0	13	6

Persamaan algoritma *affine cipher*,

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

Perhitungan enkripsi adalah sebagai berikut:

$p_1 = 12 \rightarrow c_1 = (5 \cdot 12 + 8)\ mod\ 26 = 68\ mod\ 26 = 16$ (huruf Q)

$p_2 = 0 \rightarrow c_2 = (5 \cdot 0 + 8)\ mod\ 26 = 8\ mod\ 26 = 8$ (huruf I)

$p_3 = 19 \rightarrow c_3 = (5 \cdot 19 + 8)\ mod\ 26 = 103\ mod\ 26 = 25$ (huruf Z)

$p_4 = 4 \rightarrow c_4 = (5 \cdot 4 + 8)\ mod\ 26 = 28\ mod\ 26 = 2$ (huruf C)

$p_5 = 12 \rightarrow c_5 = (5 \cdot 12 + 8)\ mod\ 26 = 68\ mod\ 26 = 16$ (huruf Q)

$p_6 = 0 \rightarrow c_6 = (5 \cdot 0 + 8)\ mod\ 26 = 8\ mod\ 26 = 8$ (huruf I)

$p_7 = 19 \rightarrow c_7 = (5 \cdot 19 + 8)\ mod\ 26 = 103\ mod\ 26 = 25$ (huruf Z)

$p_8 = 8 \rightarrow c_8 = (5 \cdot 8 + 8)\ mod\ 26 = 48\ mod\ 26 = 22$ (huruf W)

$p_9 = 10 \rightarrow c_9 = (5 \cdot 10 + 8)\ mod\ 26 = 58\ mod\ 26 = 6$ (huruf G)

$p_{10} = 0 \rightarrow c_{10} = (5 \cdot 0 + 8)\ mod\ 26 = 8\ mod\ 26 = 8$ (huruf I)

$p_{11} = 20 \rightarrow c_{11} = (5 \cdot 20 + 8)\ mod\ 26 = 108\ mod\ 26 = 4$ (huruf E)

$p_{12} = 8 \rightarrow c_{12} = (5 \cdot 8 + 8)\ mod\ 26 = 48\ mod\ 26 = 22$ (huruf W)

$p_{13} = 13 \rightarrow c_{13} = (5 \cdot 13 + 8)\ mod\ 26 = 73\ mod\ 26 = 21$ (huruf V)

$p_{14} = 12 \rightarrow c_{14} = (5 \cdot 12 + 8)\ mod\ 26 = 68\ mod\ 26 = 16$ (huruf Q)

$p_{15} = 0 \rightarrow c_{15} = (5 \cdot 0 + 8)\ mod\ 26 = 8\ mod\ 26 = 8$ (huruf I)

$p_{16} = 11 \rightarrow c_{16} = (5 \cdot 11 + 8)\ mod\ 26 = 63\ mod\ 26 = 11$ (huruf L)

$p_{17} = 0 \rightarrow c_{17} = (5 \cdot 0 + 8)\ mod\ 26 = 8\ mod\ 26 = 8$ (huruf I)

$p_{18} = 13 \rightarrow c_{18} = (5 \cdot 13 + 8)\ mod\ 26 = 73 mod\ 26 = 21$ (huruf V)

$p_{19} = 6 \rightarrow c_{19} = (5 \cdot 6 + 8)\ mod\ 26 = 38\ mod\ 26 = 12$ (huruf M)

Ciphertext yang dihasilkan adalah QIZCQIZWGI EWV QILIVM.

2.7.2 Enkripsi Pesan dengan *Route Cipher*

Plaintext : MATEMATIKA-UIN-MALANG

Kunci : 7 baris, spiral arah jarum jam mulai dari kanan atas

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

Kemudian *ciphertext* didapatkan dengan menyusun teks sesuai dengan arah yang sudah ditentukan.

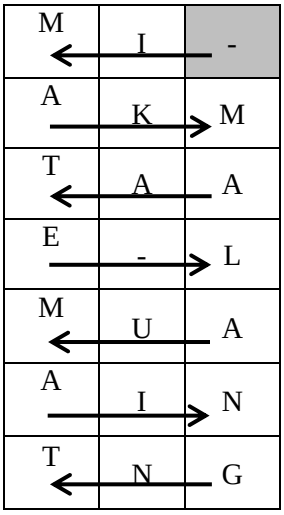
M	I	-
A	K	M
T	A	A
E	-	L
M	U	A
A	I	N
T	N	G

Ciphertext yang dihasilkan adalah -IMMAKMAATE-LAUMAINGNT.

2.7.3 Dekripsi Pesan dengan *Route Cipher*

Ciphertext : -IMMAKMAATE-LAUMAINGNT

Kunci : 7 baris, spiral arah jarum jam mulai dari kanan atas



Kemudian pembacaan *plaintext* perkolom mulai dari kolom pertama, simbol $(-)$ diubah menjadi spasi.

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

Pembacaan *plaintext* yang dihasilkan adalah: MATEMATIKA UIN MALANG.

2.7.4 Dekripsi Pesan dengan *Affine Cipher*

Ciphertext : QIZCQIZWGI EWV QILIVM

Kunci: $m = 5$ dan $b = 8$

Karakter dari alfabet yang digunakan : $(n) = 26$

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

Untuk melakukan dekripsi , pertama harus ditentukan $m^{-1}(mod\ n)$ yang dapat dihitung dengan memecahkan kekongruenan linear.

Misalkan $5^{-1}(mod\ 26) = x$, maka menurut definisi balikan modulo,

$$5x \equiv 1(mod\ 26) \quad \text{atau} \quad 5x = 1 + 26k$$

Maka $x = \frac{(1+26k)}{5}$ dengan k sebarang bilangan bulat, $k = 0, \pm1, \pm2, \pm3, \cdots$

- $k = 0 \rightarrow x = \frac{(1+26\cdot0)}{5} = \frac{1}{5}$
- $k = 1 \rightarrow x = \frac{(1+26\cdot1)}{5} = \frac{27}{5}$
- ⋮
- $k = 4 \rightarrow x = \frac{(1+26\cdot4)}{5} = \frac{105}{5} = 21$

Dengan mencoba bermacam-macam nilai k, maka untuk $k = 21$ diperoleh solusi x bilangan bulat. Jadi, $5^{-1}(mod\ 26)$ adalah $x \equiv 21(mod\ 26)$ karena $21 \cdot 5 = 105 \equiv 1(mod\ 26)$.

Jadi, untuk dekripsi digunakan kekongruenan

$$P = 21(C - 8) mod\ 26$$

Perhitungan enkripsi adalah sebagai berikut:

$c_1 = 16 \rightarrow p_1 = 21(16 - 8)\ mod\ 26 = 168\ mod\ 26 = 12$ (huruf M)

$c_2 = 8 \rightarrow p_2 = 21(8 - 8)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)

$c_3 = 25 \rightarrow p_3 = 21(25 - 8)\ mod\ 26 = 357\ mod\ 26 = 19$ (huruf T)

$c_4 = 2 \rightarrow p_4 = 21(2 - 8)\ mod\ 26 = -126\ mod\ 26 = 4$ (huruf E)

$c_5 = 16 \rightarrow p_5 = 21(16 - 8)\ mod\ 26 = 168 mod\ 26 = 12$ (huruf M)

$c_6 = 8 \rightarrow p_6 = 21(8 - 8)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)

$c_7 = 25 \rightarrow p_7 = 21(25 - 8)\ mod\ 26 = 357\ mod\ 26 = 19$ (huruf T)

$c_8 = 22 \rightarrow p_8 = 21(22 - 8)\ mod\ 26 = 294\ mod\ 26 = 8$ (huruf I)

$c_9 = 6 \rightarrow p_9 = 21(6 - 8)\ mod\ 26 = -42\ mod\ 26 = 10$ (huruf K)

$c_{10} = 8 \rightarrow p_{10} = 21(8 - 8)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)

$c_{11} = 4 \rightarrow p_{11} = 21(4 - 8)\ mod\ 26 = -84\ mod\ 26 = 20$ (huruf U)

$c_{12} = 22 \rightarrow p_{12} = 21(22 - 8)\ mod\ 26 = 294\ mod\ 26 = 8$ (huruf I)

$c_{13} = 21 \rightarrow p_{13} = 21(21 - 8)\ mod\ 26 = 273\ mod\ 26 = 13$ (huruf N)

$c_{14} = 16 \rightarrow p_{14} = 21(16 - 8)\ mod\ 26 = 168 mod\ 26 = 12$ (huruf M)

$c_{15} = 8 \rightarrow p_{15} = 21(8 - 8)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)

$c_{16} = 11 \rightarrow p_{16} = 21(11 - 8)\ mod\ 26 = 63\ mod\ 26 = 11$ (huruf L)

$c_{17} = 8 \rightarrow p_{17} = 21(8 - 8)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)

$c_{18} = 21 \rightarrow p_{18} = 21(21 - 8)\ mod\ 26 = 273\ mod\ 26 = 13$ (huruf N)

$c_{19} = 12 \rightarrow p_{19} = 21(12 - 8)\ mod\ 26 = 84\ mod\ 26 = 6$ (huruf G)

Pembacaan *plaintext* yang dihasilkan adalah:

MATEMATIKA UIN MALANG

2.8 Kajian Keagamaan

Dalam ayat al-Qur'an dijelaskan bahwasanya Allah SWT memerintahkan kepada hamba-Nya untuk menyampaikan pesan atau amanah hanya kepada yang berhak saja serta menetapkan hukum dengan sangat adil, yaitu terdapat dalam al-Qur'an surah an-Nisa'/4:58,

Artinya: "Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (*menyuruh kamu*) *apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha Mendengar lagi Maha Melihat".*

Di dalam tafsir Ibnu Katsir (2003) Allah SWT mengabarkan bahwa Dia memerintahkan untuk menunaikan amanah kepada ahlinya. Hal ini adalah perintah Allah SWT yang menganjurkan menetapkan hukum diantara manusia dengan adil. Maka dari itulah Muhammad ibnu Ka'b, Zaid ibnu Aslam, dan Syahr ibnu Hausyab mengatakan bahwa ayat tersebut diturunkan hanya berkenaan dengan para umara, yakni para penguasa yang memutuskan perkara diantara manusia (Katsir, 2003).

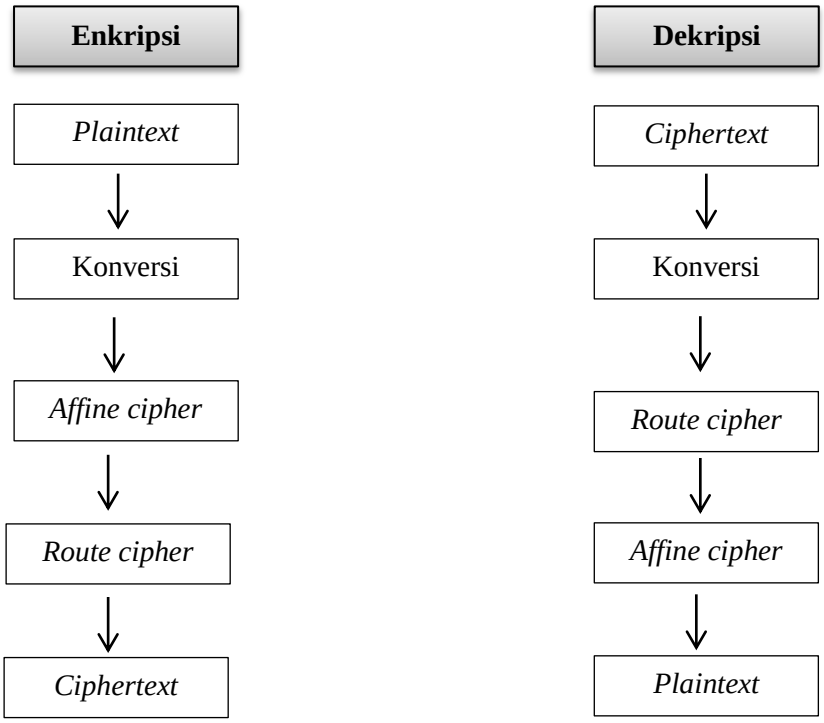
BAB III

PEMBAHASAN

Pada saat melakukan proses penyandian, penulis menentukan pesan asli (*plaintext*) yang akan disandikan menggunakan metode *Affine Cipher* dan *Route Cipher*. Dalam hal ini pesan asli (*plaintext*)-nya adalah "MATEMATIKA UIN MALANG".

3.1 Enkripsi dengan Algoritma Super Enkripsi (*Affine Cipher* dan *Route Cipher*)

Secara sederhana proses enkripsi dan dekripsi pada algoritma super enkripsi dapat digambarkan sebagai berikut:



Gambar 3.1 Skema Enkripsi dan Dekripsi Algoritma Super Enkripsi

Secara matematis dapat dijelaskan sebagai berikut. Proses enkripsi dengan menggunakan metode super enkripsi:

a. Menentukan *plaintext.*
b. Menentukan dua parameter kunci m dan b, dimana m harus relatif prima dengan n dan $1 < b \leq n, (n = 26)$.
c. Mengkonversi *plaintext* yang berbentuk alfabet ke $\mathbb{Z}_{26}$.
d. Melakukan perhitungan dengan menggunakan persamaan enkripsi algoritma *affine cipher*,

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

e. Melakukan perhitungan menggunakan transposisi *route cipher* dengan kunci dan arah cara baca yang sudah ditentukan.
f. Mengkonversi $\mathbb{Z}_{26}$ ke dalam bentuk alfabet.
g. Mendapatkan pesan teks yang sudah disandikan (*ciphertext*).

Proses dekripsi dengan menggunakan metode super enkripsi:

a. Memasukkan pesan teks yang sudah disandikan (*ciphertext*).
b. Menentukan kunci k arah cara baca transposisi *route cipher*.
c. Melakukan perhitungan menggunakan transposisi *route cipher* dengan kunci dan arah cara baca yang sudah ditentukan.
d. Mengkonversi alfabet ke $\mathbb{Z}_{26}$.
e. Melakukan perhitungan dengan menggunakan persamaan dekripsi algoritma *affine cipher*,

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

dan dekripsi hanya bisa dilakukan apabila m mempunyai invers. Maka harus mencari m^{-1} terlebih dahulu sebelum melakukan dekripsi.

f. Mengkonversi $\mathbb{Z}_{26}$ ke dalam bentuk alfabet.

g. Mendapatkan pesan teks asli (*plaintext*).

3.1.1 Algoritma *Affine Cipher*

Algoritma *affine cipher* menggunakan dua parameter sebagai kunci. Kedua parameter tersebut yang nantinya akan digunakan pada proses enkripsi dan dekripsi. Parameter yang digunakan pada proses enkripsi dan dekripsi adalah sebagai berikut.

1. m adalah parameter yang dipakai sebagai pengali dengan P (*plaintext*). Untuk mendapatkan pesan semula pada proses dekripsi maka solusinya hanya ada jika balikan dari $m(mod\ n)$, dinyatakan dengan m^{-1}. Jika $m^{-1}(mod\ n)$ ada maka dekripsi dapat dilakukan. Karena m sebagai parameter pada proses enkripsi dan dekripsi maka bersifat rahasia hanya diketahui oleh pengirim dan penerima saja.
2. b adalah parameter yang dipakai sebagai penjumlah dengan hasil kali m dan P (*plaintext*) untuk menghasilkan *ciphertext*, sedangkan b sebagai pengurang pada dekripsi untuk menghasilkan *plaintext* semula. Karena b sebagai parameter pada proses enkripsi dan dekripsi maka bersifat rahasia hanya diketahui oleh pengirim dan penerima saja.
3. P (*plaintext*) adalah pesan asli yang hanya diketahui oleh pengirim dan akan diketahui oleh penerima melalui proses dekripsi.
4. C (*ciphertext*) adalah pesan acak yang telah dienkripsi oleh pengirim.
5. n adalah jumlah karakter alfabet yang digunakan untuk mengkonversi huruf menjadi angka pada proses enkripsi dan dekripsi.

Keamanan algoritma *affine cipher* terdapat pada dua parameter bilangan

bulat m dan b yang mana kedua parameter tersebut dirahasiakan. Kunci m harus relatif prima dengan n (jumlah karakter alfabet), yaitu 26. Jika $1 < m \leq n$ maka kemungkinan terdapat 12 bilangan bulat yang relatif prima dengan n dan jika $1 < b \leq n$ maka terdapat 26 kemungkinan kunci yang dapat digunakan. Kombinasi dari kedua kunci tersebut, yaitu $12 \cdot 26 = 312$ pasangan kunci yang dapat digunakan. Dalam melakukan proses enkripsi dan dekripsi perlu pembentukan kunci terlebih dahulu kemudian dilakukan proses enkripsi dan dekripsi. Berikut ini langkah-langkah pembentukan kunci:

1. Menentukan parameter m, yang mana pada penelitian ini penulis menggunakan $m = 5$. Parameter tersebut didapatkan dengan cara mencari bilangan bulat yang relatif prima dengan $n = 26$. Faktor pembagi $5 = \{1, 5\}$ dan faktor pembagi $26 = \{1, 2, 13, 26\}$. Faktor pembagi bersama dari 5 dan 26 adalah 1, maka 5 da n 26 adalah relatif prima karena PBB $(5, 26) = 1$.
2. Menentukan parameter b, yang mana pada penelitian ini penulis menggunakan $b = 8$ dimana $1 < b \leq n$.

3.1.2 Algoritma *Route Cipher*

Algoritma *route cipher* merupakan salah satu jenis *cipher* transposisi yang menggunakan kunci berupa cara baca. Pada algoritma *route cipher*, penyandiannya dilakukan dengan menuliskan *plaintext* atau pesan asli secara kolom dari atas ke bawah. Kemudian *ciphertext* dibaca dengan arah (*route*) sesuai perjanjian, misalnya (1) secara spiral dengan arah jarum jam mulai dari kanan atas, kanan bawah, kiri atas dan kiri bawah atau (2) secara ular tangga mulai dari kanan atas, kanan bawah, kiri atas, serta kiri bawah dan lain-lain cara pembacaannya.

Langkah-langkah algoritma *route cipher* adalah sebagai berikut:

1. Membuat matriks dengan jumlah baris yang akan diisi *plaintext,* yaitu dengan membagi jumlah *plaintext* dengan kunci.
2. Menentukan arah transposisi *plaintext,* contohnya jika arah yang ditentukan adalah spiral, maka *ciphertext* dihasilkan dengan membaca *plaintext* dalam matriks dengan arah spiral.
3. Proses dekripsi algoritma route *cipher*, yaitu hanya membaca posisi berdasarkan urutan kata yang disusun dalam matriks berdasarkan susunan dari arah yang digunakan untuk membentuk *ciphertext.*

Langkah-langkah pembentukan kunci pada algoritma *route cipher* adalah sebagai berikut:

1. Menghitung jumlah karakter *plaintext* terlebih dahulu, kemudian membaginya dengan kunci k. Dalam penelitian ini jumlah karakter *plaintext* yang digunakan sebanyak 21 karakter dengan menggunakan $k = 7$ sebagai baris. Membagi jumlah karakter *plaintext* dengan *k,* sehingga jumlah kolom yang dihasilkan adalah 3. Setelah menentukan baris dan kolom maka dibuatlah sebuah matriks berordo 7×3, untuk mengisi jumlah karakter *plaintext* yang ditulis secara kolom dari atas ke bawah.
2. Menentukan arah transposisi *plaintext,* pada penelitian ini menggunakan spiral arah jarum jam dan dimulai dari kanan atas. Maka *ciphertext* yang dihasilkan dengan membaca *plaintext* dalam matriks sesuai arah yang sudah ditentukan tersebut.
3. Selanjutnya untuk mengembalikan *plaintext* semula, yaitu dengan membaca urutan kata secara kolom dari atas ke bawah.

3.1.3 Proses Enkripsi

Super enkripsi akan dilakukan dengan proses enkripsi menggunakan kedua cipher, yaitu *affine cipher* dan *route cipher* secara berurutan. Adapun proses enkripsi menggunakan *affine cipher* adalah sebagai berikut:

Plainteks: MATEMATIKA UIN MALANG

Kunci: $m = 5$ dan $b = 8$

Karakter dari alfabet yang digunakan : $(n) = 26$

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

Gambar 3.2 Kode Karakter Alfabet

maka plainteks MATEMATIKA-UIN-MALANG ekivalen dengan 12 0 19 4 12 0 19 8 10 0 20 8 13 12 0 11 0 13 6.

M	A	T	E	M	A	T	I	K	A	U	I	N	M	A	L	A	N	G
12	0	19	4	12	0	19	8	10	0	20	8	13	12	0	11	0	13	6

Perhitungan enkripsi adalah sebagai berikut:

$p_1 = 12 \rightarrow c_1 = (5 \cdot 12 + 8)\ mod\ 26 = 68\ mod\ 26 = 16$ (huruf Q)

$p_2 = 0 \rightarrow c_2 = (5 \cdot 0 + 8)\ mod\ 26 = 8\ mod\ 26 = 8$ (huruf I)

$p_3 = 19 \rightarrow c_3 = (5 \cdot 19 + 8)\ mod\ 26 = 103\ mod\ 26 = 25$ (huruf Z)

$p_4 = 4 \rightarrow c_4 = (5 \cdot 4 + 8)\ mod\ 26 = 28\ mod\ 26 = 2$ (huruf C)

$p_5 = 12 \rightarrow c_5 = (5 \cdot 12 + 8)\ mod\ 26 = 68\ mod\ 26 = 16$ (huruf Q)

$p_6 = 0 \rightarrow c_6 = (5 \cdot 0 + 8)\ mod\ 26 = 8\ mod\ 26 = 8$ (huruf I)

$p_7 = 19 \rightarrow c_7 = (5 \cdot 19 + 8)\ mod\ 26 = 103\ mod\ 26 = 25$ (huruf Z)

$p_8 = 8 \rightarrow c_8 = (5 \cdot 8 + 8)\ mod\ 26 = 48\ mod\ 26 = 22$ (huruf W)

$p_9 = 10 \rightarrow c_9 = (5 \cdot 10 + 8)\ mod\ 26 = 58\ mod\ 26 = 6$ (huruf G)

$p_{10} = 0 \rightarrow c_{10} = (5 \cdot 0 + 8)\ mod\ 26 = 8\ mod\ 26 = 8$ (huruf I)

$p_{11} = 20 \rightarrow c_{11} = (5 \cdot 20 + 8)\ mod\ 26 = 108\ mod\ 26 = 4$ (huruf E)

$p_{12} = 8 \rightarrow c_{12} = (5 \cdot 8 + 8)\ mod\ 26 = 48\ mod\ 26 = 22$ (huruf W)

$p_{13} = 13 \rightarrow c_{13} = (5 \cdot 13 + 8)\ mod\ 26 = 73\ mod\ 26 = 21$ (huruf V)

$p_{14} = 12 \rightarrow c_{14} = (5 \cdot 12 + 8)\ mod\ 26 = 68\ mod\ 26 = 16$ (huruf Q)

$p_{15} = 0 \rightarrow c_{15} = (5 \cdot 0 + 8)\ mod\ 26 = 8\ mod\ 26 = 8$ (huruf I)

$p_{16} = 11 \rightarrow c_{16} = (5 \cdot 11 + 8)\ mod\ 26 = 63\ mod\ 26 = 11$ (huruf L)

$p_{17} = 0 \rightarrow c_{17} = (5 \cdot 0 + 8)\ mod\ 26 = 8\ mod\ 26 = 8$ (huruf I)

$p_{18} = 13 \rightarrow c_{18} = (5 \cdot 13 + 8)\ mod\ 26 = 73 mod\ 26 = 21$ (huruf V)

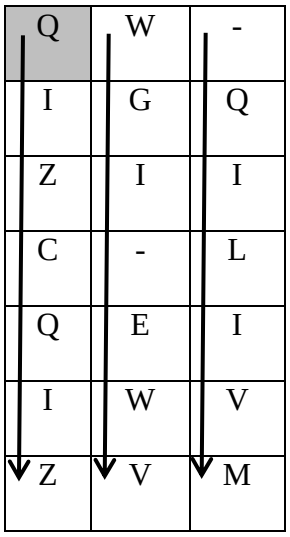
$p_{19} = 6 \rightarrow c_{19} = (5 \cdot 6 + 8)\ mod\ 26 = 38\ mod\ 26 = 12$ (huruf M)

Ciphertext yang dihasilkan adalah QIZCQIZWGI EWV QILIVM.

Selanjutnya *ciphertext* tersebut dienkripsi kembali dengan menggunakan *cipher* transposisi, yaitu *route cipher*. Berikut proses enkripsinya *route cipher*.

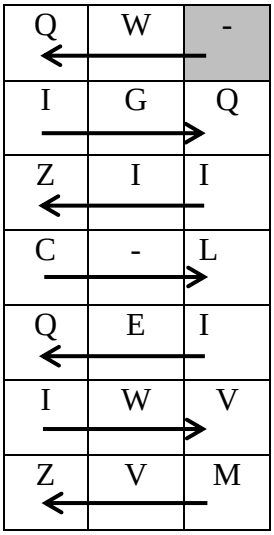
Plaintext : QIZCQIZWGI-EWV-QILIVM

Kunci : 7 baris, spiral arah jarum jam mulai dari kanan atas



Gambar 3.3 Proses Enkripsi *Route Cipher*

Kemudian *ciphertext* didapatkan dengan menyusun teks sesuai dengan arah yang sudah ditentukan.



Gambar 3.4 Pembacaan *Ciphertext Route Cipher*

Ciphertext yang dihasilkan adalah –WQIGQIIZC-LIEQIWVMVZ.

3.2 Dekripsi dengan Algoritma Super Enkripsi (*Affine Cipher* dan *Route Cipher*)

Untuk mengembalikan *ciphertext* tersebut menjadi *plaintext* yang berisi makna pesan sesungguhnya. Maka membutuhkan proses dekripsi secara

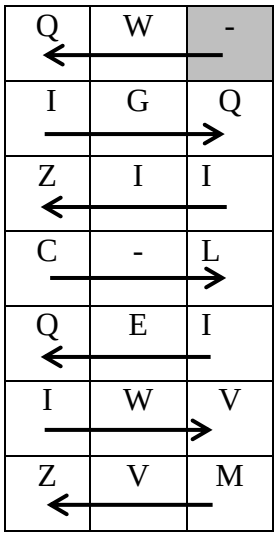
berurutan, yang mana mendahulukan proses dekripsi *affine cipher* kemudian dilanjutkan dengan dekripsi *route cipher*. Dalam proses dekripsi ini menggunakan *ciphertext* yang diperoleh dari proses enkripsi *affine cipher* dan *route cipher* pada pembahasan sebelumnya.

Adapun proses dekripsi menggunakan *route cipher* adalah sebagai berikut:

Ciphertext : –WQIGQIIZC-LIEQIWVMVZ

Kunci : 7 baris, spiral arah jarum jam mulai dari kanan atas

Penulisan *ciphertext* ditulis secara spiral dengan arah jarum jam mulai dari kanan atas.



Gambar 3.5 Proses Dekripsi *Route Cipher*

Pembacaan *plaintext* perkolom dimulai dari kolom pertama dan simbol (−) akan diubah menjadi spasi. Berikut ini adalah gambar pembacaan *ciphertext* yang akan dihasilkan *plaintext. Ciphertext* tersebut akan digunakan pada proses dekripsi pada tahap selanjutnya.

Gambar berikut ini adalah cara pembacaan *plaintext* pada proses dekripsi menggunakan algoritma *route cipher.*

Q	W	-
I	G	Q
Z	I	I
C	-	L
Q	E	I
I	W	V
Z	V	M

Gambar 3.6 Pembacaan *Plaintext* Algoritma *Route Cipher*

Ciphertext yang dihasilkan adalah QIZCQIZWGI-EWV-QILIVM.

Berdasarkan hasil pembacaan *plaintext* yang diperoleh dari proses dekripsi pada *route cipher*, maka *plaintext* tersebut akan digunakan sebagai *ciphertext* pada proses dekripsi menggunakan algoritma *affine cipher* berikut ini.

Ciphertext : QIZCQIZWGI-EWV-QILIVM

Kunci: $m = 5$ dan $b = 8$

Karakter dari alfabet yang digunakan : $(n) = 26$

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

Untuk melakukan dekripsi, pertama harus ditentukan $m^{-1}(mod\ n)$ yang dapat dihitung dengan menggunakan kekongruenan linear.

Misalkan $5^{-1}(mod\ 26) = x$, maka menurut definisi balikan modulo,

$$5x \equiv 1(mod\ 26) \quad \text{atau} \quad 5x = 1 + 26k$$

Maka $x = \frac{(1+26k)}{5}$ dengan k sebarang bilangan bulat, $k = 0, \pm1, \pm2, \pm3, \cdots$

- $k = 0 \rightarrow\ x = \frac{(1+26\cdot0)}{5} = \frac{1}{5}$
- $k = 1 \rightarrow\ x = \frac{(1+26\cdot1)}{5} = \frac{27}{5}$
- ⋮
- $k = 4 \rightarrow\ x = \frac{(1+26\cdot4)}{5} = \frac{105}{5} = 21$

Dengan mencoba bermacam-macam nilai k, maka untuk $k = 21$ diperoleh solusi x bilangan bulat. Jadi, $5^{-1}(mod\ 26)$ adalah $x \equiv 21(mod\ 26)$ karena $21 \cdot 5 = 105 \equiv 1(mod\ 26)$.

Jadi, untuk dekripsi digunakan kekongruenan

$$P = 21(C - 8) mod\ 26$$

Perhitungan dekripsi adalah sebagai berikut:

$c_1 = 16\ \rightarrow\ p_1 = 21(16 - 8)\ mod\ 26 = 168\ mod\ 26 = 12$ (huruf M)

$c_2 = 8 \rightarrow p_2 = 21(8 - 8)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)

$c_3 = 25 \rightarrow p_3 = 21(25 - 8)\ mod\ 26 = 357\ mod\ 26 = 19$ (huruf T)

$c_4 = 2 \rightarrow p_4 = 21(2 - 8)\ mod\ 26 = -126\ mod\ 26 = 4$ (huruf E)

$c_5 = 16 \rightarrow p_5 = 21(16 - 8)\ mod\ 26 = 168 mod\ 26 = 12$ (huruf M)

$c_6 = 8 \rightarrow p_6 = 21(8 - 8)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)

$c_7 = 25 \rightarrow p_7 = 21(25 - 8)\ mod\ 26 = 357\ mod\ 26 = 19$ (huruf T)

$c_8 = 22 \rightarrow p_8 = 21(22 - 8)\ mod\ 26 = 294\ mod\ 26 = 8$ (huruf I)

$c_9 = 6 \rightarrow p_9 = 21(6-8)\ mod\ 26 = -42\ mod\ 26 = 10$ (huruf K)

$c_{10} = 8 \rightarrow p_{10} = 21(8-8)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)

$c_{11} = 4 \rightarrow p_{11} = 21(4-8)\ mod\ 26 = -84\ mod\ 26 = 20$ (huruf U)

$c_{12} = 22 \rightarrow p_{12} = 21(22-8)\ mod\ 26 = 294\ mod\ 26 = 8$ (huruf I)

$c_{13} = 21 \rightarrow p_{13} = 21(21-8)\ mod\ 26 = 273\ mod\ 26 = 13$ (huruf N)

$c_{14} = 16 \rightarrow p_{14} = 21(16-8)\ mod\ 26 = 168 mod\ 26 = 12$ (huruf M)

$c_{15} = 8 \rightarrow p_{15} = 21(8-8)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)

$c_{16} = 11 \rightarrow p_{16} = 21(11-8)\ mod\ 26 = 63\ mod\ 26 = 11$ (huruf L)

$c_{17} = 8 \rightarrow p_{17} = 21(8-8)\ mod\ 26 = 0\ mod\ 26 = 0$ (huruf A)

$c_{18} = 21 \rightarrow p_{18} = 21(21-8)\ mod\ 26 = 273\ mod\ 26 = 13$ (huruf N)

$c_{19} = 12 \rightarrow p_{19} = 21(12-8)\ mod\ 26 = 84\ mod\ 26 = 6$ (huruf G)

Pembacaan *plaintext* yang dihasilkan adalah:

MATEMATIKA UIN MALANG

Proses super enkripsi pada penelitian ini, yaitu dengan menggabungkan *cipher* substitusi dan *cipher* transposisi. Adapun *cipher* substitusinya menggunakan algoritma *affine cipher* dan *cipher* transposisinya menggunakan algoritma *route cipher*. Tahap awal yang dilakukan adalah mengenkripsi suatu *plaintext* dengan menggunakan algoritma *affine cipher* terlebih dahulu dan menghasilkan suatu *ciphertext*, selanjutnya *ciphertext* tersebut dienkripsikan kembali menggunakan algoritma *route cipher* yang menghasilkan *ciphertext* juga. Kemudian hasil *ciphertext* tersebut didekripsikan dengan proses algoritma *route cipher* terlebih dahulu, sehingga menghasilkan *plaintext* yang akan didekripsikan kembali menggunakan algoritma *affine cipher*. Dengan demikian, diperoleh hasil pendekripsian dari algoritma *affine cipher* yang merupakan pesan asli yang

diterima oleh penerima pesan. Penggunaan algoritma super enkripsi pada penelitian ini sesuai dengan tujuannya, yaitu untuk menciptakan *cipher* yang lebih kuat daripada hanya menggunakan satu *chiper* saja, sehingga tidak mudah untuk dipecahkan. Penggabungan kedua algoritma ini juga bertujuan mengamankan pesan dengan efektif sehingga dapat dipastikan pesan tersebut tidak akan mudah diketahui oleh pihak lain.

3.3 Penerapan Tentang Berpesan dalam Islam

Dalam penyampaian pesan atau amanah kita tidak boleh mengkhianatinya, seperti firman Allah Swt dalam surat al-Anfal/8:27.

Artinya:"Wahai orang-orang yang beriman! Janganlah kamu mengkhianati Allah dan Rasul dan (juga) janganlah kamu mengkhianati amanat yang dipercayakan kepadamu, sedang kamu mengetahui".

Ali bin Abi Thalib berkata, dari Ibnu Abbas mengenai firman Allah dan "*dan* (*juga*) *janganlah kamu mengkhianati amanat yang dipercayakan kepadamu".* Amanah merupakan segala macam bentuk perbuatan yang diamanatkan oleh Allah Swt kepada hamba-hamba-Nya. Maksud dari amanat tersebut adalah kewajiban, Dia berkata: "*janganlah kamu mengkhianati",* yang berarti jangan melanggar amanat itu (Katsir, 2003).

Sebagai manusia yang hidup dan mati atas izin Allah Swt, janganlah sekali-kali berkhianat dan sudah seharusnya sebagai manusia wajib menyampaikan apapun yang telah diamanatkan oleh guru, orang tua, saudara, dan juga teman sejawat.

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan pembahasan sebelumnya penelitian ini dapat disimpulkan sebagai berikut :

1. Proses enkripsi pada super enkripsi merupakan gabungan dari proses enkripsi *affine cipher* dan proses enkripsi *route cipher*. Pada proses pertama, yaitu mengenkripsi *plaintext* dengan menggunakan algoritma *affine cipher*. Sedangkan pada proses kedua mengenkripsi kembali *ciphertext* dari *affine cipher* dengan menggunakan algoritma *route cipher*.
2. Proses dekripsi pada super enkripsi merupakan proses pengembalian *ciphertext* menjadi *plaintext* yang berisi pesan teks semula. Pada proses dekripsi ini dengan diawali mendekripsikan *ciphertext* dengan menggunakan algoritma *route cipher*. Selanjutnya hasil dari proses dekripsi *route cipher* didekripsikan kembali menjadi *plaintext* dengan menggunakan algoritma *affine cipher*.

4.2 Saran

Pada penelitian ini membahas tentang super enkripsi yang menggabungkan *cipher* substitusi dan *cipher* transposisi, yaitu *affine cipher* dan *route cipher* pada pesan teks. Kedua *cipher* tersebut merupakan algoritma kriptografi klasik yang menggunakan satu kunci dalam mengamankan pesan teks. Untuk pengembangan penelitian-penelitian selanjutnya diharapakan menggunakan algoritma kriptografi modern yang dapat mengenkripsi semua karakter, gambar, suara, video, objek 3-D, atau data digital lainnya.

DAFTAR RUJUKAN

Abdussakir. 2009. *Matematika 1 Kajian Integratif Matematika dan Al-Qur'an.* Malang: UIN Maliki Press.

Ariyus, D. 2006. *Kriptografi Keamanan Data dan Komunikasi.* Yogyakarta: Graha Ilmu.

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

Irdayani. 2019. Keamanan Citra Menggunakan Algoritma Route. *Majalah Ilmiah INTI*, VI (2): 1-4.

Katsir, I. 2003. *Tafsir Ibnu Katsir Jilid 2. Terjemahan M. Abdul Ghoffar E.M.* Bogor: Pustaka Imam as-Syafi'i.

Kromodimoeljo, S. 2010. *Teori dan Aplikasi Kriptografi.* Jakarta: SPK IT Consuling.

Kurniawan, A. 2008. *Konsep Dan Implemenasi Cryptography Dengan NET.* Jakarta: PC Media.

Maulana, P. A. 2019. *Proses Enkripsi Dan Dekripsi Pada Polinomial Dengan Menggunakan Metode Affine Cipher.* Skripsi Tidak Dipublikasikan. Malang: UIN Maulana Malik Ibrahim.

Muhsetyo, G. 1997. *Dasar-Dasar Teori Bilangan.* Jakarta: PGSM.

Munir, R. 2005. *Matematika Diskrit.* Bandung: Informatika.

Munir, R. 2006. *Kriptografi.* Bandung: Informatika .

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

Ruminta. 2014. *Matriks Persamaan Linier Dan Pemrograman Linier.* Bandung: Rekayasa Sains.

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

Wibowo, S., Nilawati, F.E., dan Suharnawi. 2014. Implementasi Enkripsi Dekripsi Algoritma Affine Cipher Berbasis Android. *Techno.COM*, 13, (4): 215-221. (Online), (https://publikasi.dinus.ac.id), diakses 25 Mei 2021.

RIWAYAT HIDUP

Rena Alvionita, lahir di Malang pada tanggal 26 Nopember 1995, biasa dipanggil Rena, tinggal di Dusun Sumberkunci rt 06/ rw 07, Desa Babadan, Kecamatan Ngajum, Kabupaten Malang. Anak kedua dari Bapak Triswanto dan Ibu Jumani. Pendidikan dasarnya ditempuh di TK Muslimat Al-Amin Sumberkunci Babadan, kemudian melanjutkan ke SD Negeri Babadan 03 dan lulus pada tahun 2008. Kemudian di tahun yang sama melanjutkan pendidikan ke SMP Darusssalam Dawuhan Jatirejoyoso Kepanjen dan lulus pada tahun 2011, setelah itu melanjutkan pendidikannya ke MA Miftahul Huda Mojosari Kepanjen dan lulus pada tahun 2014. Selanjutnya pada tahun 2014 penulis mulai menempuh kuliah dengan mengambil Program Studi Matematika, Fakultas Sains dan Teknologi di Universitas Islam Negeri Maulana Malik Ibrahim Malang.

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

BUKTI KONSULTASI SKRIPSI

Nama : Rena Alvionita
NIM : 14610089
Fakultas/ Jurusan : Sains dan Teknologi/Matematika
Judul Skripsi : Implementasi Algoritma Super Enkripsi (*Affine Cipher* dan *RouteCipher*) pada Pesan Teks
Pembimbing I : Muhammad Khudzaifah, M. Si
Pembimbing II : Muhammad Nafi Jauhari, M. Si

No	Tanggal	Hal	Tanda Tangan
1.	27 April 2021	Konsultasi Bab I dan Bab II	1.
2.	29 April 2021	Revisi Bab I	2.
3.	3 Mei 2021	Konsultasi Bab II dan Keagamaan	3.
4.	21 Mei 2021	Revisi Bab II dan Keagamaan	4.
5.	24 Mei 2021	Konsultasi Bab III	5.
6.	31 Mei 2021	Revisi Bab III	6.
7.	5 Juni 2021	Konsultasi Bab IV	7.
8.	18 Juni 2021	Revisi Bab I, II, III dan IV	8.
9.	18 Juni 2021	ACC Keseluruhan	9.

Malang, 18 Juni 2021
Mengetahui,
Ketua Program Studi Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001