PROSES ENKRIPSI DAN DEKRIPSI DENGAN MENGGUNAKAN METODE SUPER ENKRIPSI

SKRIPSI

OLEH
LUQMAN EL HAKIM
NIM. 12610046

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2019

PROSES ENKRIPSI DAN DEKRIPSI DENGAN MENGGUNAKAN METODE SUPER ENKRIPSI

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
Luqman El Hakim
NIM. 12610046

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2019

PROSES ENKRIPSI DAN DEKRIPSI DENGAN MENGGUNAKAN METODE SUPER ENKRIPSI

SKRIPSI

Oleh
Luqman El Hakim
NIM. 12610046

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 24 Mei 2019

Pembimbing I	Pembimbing II
Muhammad Khudzaifah, M.Si	Evawati Alisah, M.Pd
NIDT. 19900511 20160801 1 057	NIP. 19720604 199903 2 001

Mengetahui,
Ketua Jurusan Matematika

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

PROSES ENKRIPSI DAN DEKRIPSI DENGAN MENGGUNAKAN METODE SUPER ENKRIPSI

SKRIPSI

Oleh
Luqman El Hakim
NIM. 12610046

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Sains (S.Mat)
Tanggal 27 Mei 2019

Penguji Utama	:	Hisyam Fahmi, M.Kom	.....
Ketua Penguji	:	Angga Dwi Mulyanto, M.Si	.....
Sekretaris Penguji	:	Muhammad Khudzaifah, M.Si	.....
Anggota Penguji	:	Evawati Alisah, M.Pd	.....

Mengetahui,
Ketua Jurusan Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama	**: Luqman El Hakim**
NIM	: 12610046
Jurusan	: Matematika
Fakultas	: Sains dan Teknologi
Judul	: Proses Enkripsi Dan Dekripsi Dengan Menggunakan Metode Super Enkripsi

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, 27 Mei 2019
Yang membuat pernyataan,

Luqman El hakim
NIM. 12610046

MOTO

“Tidak ada kenyamanan di masa tua bagi mereka yang malas di masa muda.”
(Bob Sadino)

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:

Kedua orang tua tercinta Hajali dan Nadia Choirijjah, adik tersayang Arif Fatchur Rochman.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah Swt atas rahmat, taufik, serta hidayah-Nya sehingga penulis mampu menyelesaikan penyusunan skripsi ini 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. 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 Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Muhammad Khudzaifah, M.Si, selaku dosen pembimbing I yang telah banyak memberikan arahan, nasihat, dan motivasi kepada penulis.
5. Evawati Alisah, M.Pd, selaku dosen pembimbing II yang telah memberikan arahan, nasihat, dan berbagai pengalaman kepada penulis.

6. Dr. Usman Pagalay, M.Si, selaku dosen pembimbing akademik yang telah memberikan arahan dan nasihat kepada penulis baik dalam hal akademik maupun non akademik.
7. 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.
8. Bapak dan Ibu yang selalu memberikan doa, semangat, serta motivasi kepada penulis sampai saat ini.
9. Seluruh teman-teman di Jurusan Matematika, khususnya Pinglan Anta Maulana, Much. Fuad Hasan, Aan Sa'adillah, Muh. Amir Hamzah, Mukhammad Lukman, Grafik Akbar Muttaqin, Achmad Sirojuddin, Icha Risqie Meirissa, Firma Lianaharu, Erny Widiastuti, Maya Puspita Sari, Vany Linda F., Eka Fenia D.P., Okta Dwi Cahyono, dan Ahmad Khusaeri, terima kasih atas kenang-kenangan indah yang dirajut bersama dalam menggapai impian.
10. Semua pihak yang ikut membantu dalam menyelesaikan skripsi ini baik moril maupun materiil.

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

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, Mei 2019

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

El-Hakim, Luqman. 2019. **Proses Enkripsi Dan Dekripsi Dengan Menggunakan Metode Super Enkripsi.** Skripsi. Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si (II) Evawati Alisah, M.Pd.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi, *Plaintext*, *Ciphertext*, Super Enkripsi

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan yang diperoleh dengan menyandikannya menjadi pesan yang tidak mempunyai makna. Enkripsi adalah sebuah proses penyandian yang mengubah teks-asli atau pesan yang dapat dimengerti (*plaintext*) menjadi teks-kode atau pesan yang tidak bisa dimengerti (*ciphertext*). Dekripsi adalah sebuah proses pembalikan yang mengubah teks-kode atau pesan yang tidak bisa dimengerti (*ciphertext*) menjadi sebuah teks-asli atau pesan yang dapat dimengerti (*plaintext*). Untuk melakukan suatu proses penyandian dan proses pembalikan menggunakan algoritma yang sama (Munir, 2006). Suatu sistem yang digunakan untuk mangamankan data agar kerahasiaan data tersebut terjamin dan tersampaikan dengan kerahasiaan yang terjaga, maka perlu menggunakan metode kriptografi untuk mengamankan data yang akan dikirimkan. Adanya kriptografi, diharapkan dapat menjaga kerahasiaan data pada suatu isntansi atau kalangan tertentu.

Tujuan dari penelitian ini adalah menjelaskan proses Enkripsi dan Dekripsi menggunakan metode Super Enkripsi. Hasil penelitian adalah: Penjabaran mengenai proses enkripsi pesan menggunakan metode Super Enkripsi dan dilanjutkan dengan penjabaran proses dekripsi pesan menggunakan metode Super Enkripsi.

Penelitian ini bertujuan untuk mengetahui proses enkripsi dan dekripsi pada super enkripsi. Hasil penelitian adalah:

1. Pada proses enkripsi pesan dengan menggunakan metode super enkripsi ada dua tahap pengerjaan. Pesan asli (*plaintext*) yaitu "P", setiap karakternya dikonversi kedalam tabel konversi. Kunci yang digunakan untuk mengenkripsi pesan yaitu "K". Selanjutnya melakukan proses enkripsi menggunakan *caesar cipher* (metode kaisar), setelah diperoleh hasil dari proses substitusi dengan caesar cipher menggunakan persamaan $c \equiv (p + k) mod\ n$ kemudian dienkripsi kembali dengan teknik transposisi menggunakan transpose matriks. Sehingga didapatkan pesan sandi (*ciphertext*) yaitu "C"
2. Untuk mendapatkan pesan asli (*plaintext*), terlebih dahulu mencari kunci yang digunakan untuk proses dekripsi dan menemukan "K", kemudian melakukan proses dekripsi pada pesan yang sudah disandikan (ciphertext) "C" menggunakan teknik substitusi dengan persamaan $p \equiv (c - k) mod\ n$. Setelah diperoleh hasil dari teknik substitusi, didekripsi kembali menggunakan teknik transposisi dengan transpose matriks. Sehingga diperoleh pesan asli (*plaintext*) yaitu "P".

Penelitian selanjutnya diharapkan untuk Menggunakan kombinasi lain untuk metode super enkripsi serta menggunakan algoritma program untuk mendapatkan hasil yang lebih akurat.

ABSTRACT

El-Hakim, Luqman. 2019. **Encryption And Decripsion Process Using The Super Encryption Method**. Essay. Mathematics Department, Faculty of Science and Technology, State Islamic University Maulana Malik Ibrahim Malang. Advisor: (I) Muhammad Khudzaifah, M.Si (II) Evawati Alisah, M.Pd.

Keywords: Cryptography, Encryption, Decryption, Plaintext, Ciphertext, Super Encryption

Cryptography is a science as well as art to maintain the security of messages obtained by encoding them into messages that have no meaning. Encryption is an encoding process that converts original text or understandable messages (plaintext) into text-codes or incomprehensible messages (ciphertext). Decryption is a reversal process that converts text-codes or messages that cannot be understood (ciphertext) into an original text or an understandable message (plaintext). To do an encoding process and reversal process using the same algorithm (Munir, 2006). A system used to secure data so that the confidentiality of the data is guaranteed and conveyed with confidentiality maintained, it is necessary to use cryptographic methods to secure the data to be sent. The existence of cryptography, is expected to maintain the confidentiality of data at an institution or certain circles.

The purpose of this study is to explain the encryption and decryption process using the Super Encryption method. The results of the study are: The description of the message encryption process using the Super Encryption method and continued with the translation of the message decryption process using the Super Encryption method.

This study aims to determine the process of encryption and decryption in super encryption. The results of the study are:

1. In the message encryption process using the super encryption method there are two stages of work. The original message (plaintext) is "P", each character is converted into a conversion table. The key used to encrypt messages is "K". Then do the encryption process using caesar cipher (caesar method), after the results obtained from the substitution process by caesar cipher using the $c \equiv (p + k) \bmod n$ equation are then encrypted again with the transposition technique using matrix transpose. So that you get a password (ciphertext), namely "C"
2. To get the original message (plaintext), first look for the key used for the decryption process and find "K", then decrypt the encrypted message (ciphertext) "C" using the substitution technique with the equation $p \equiv (c - k) \bmod n$. After the results of the substitution technique were obtained, it was decrypted again using the transposition technique with matrix transpose. So that the original message (plaintext) is obtained "P".

Future tudies are expected to use other combinations for the super encryption method and use program algorithms to get more accurate results.

ملخص

الحكيم ، لقمان. 2019. عملية التشفير والانصهار باستخدام طريقة التشفير الفائقة. بحث جامعي. شعبة الرياضيات. كلية العلوم والتكنولوجيا. الجامعة الاسلامية الحكومية مولانا مالك إبراهيم مالانج.. المستشار: (I) محمد خديفة ، ماجستير (II) إيفواتي أليسا ، ماجستير

الكلمات المفتاحية: التشفير ، فك التشفير ، نص عادي ، نص مشفر ، تشفير سوبر

التشفير هو علم وكذلك فن للحفاظ على أمان الرسائل التي يتم الحصول عليها من خلال ترميزها في رسائل لا معنى لها. التشفير هو عملية تشفير تحول النص الأصلي أو الرسائل المفهومة (نص عادي) إلى رموز نصية أو رسائل غير مفهومة (نص مشفر). فك التشفير هو عملية عكسية تقوم بتحويل الرموز النصية أو الرسائل التي لا يمكن فهمها (نص مشفر) إلى نص أصلي أو رسالة مفهومة (نص عادي). للقيام بعملية الترميز وعكس العملية باستخدام نفس الخوارزمية (منير ، 2006). نظام يستخدم لتأمين البيانات بحيث يتم ضمان سرية البيانات ونقلها مع الحفاظ على السرية ، من الضروري استخدام طرق التشفير لتأمين البيانات المراد إرسالها. وجود تشفير ، من المتوقع أن يحافظ على سرية البيانات في مؤسسة أو دوائر معينة.

الغرض من هذه الدراسة هو شرح عملية التشفير وفك التشفير باستخدام طريقة التشفير السوبر. نتائج الدراسة هي: وصف عملية تشفير الرسائل باستخدام طريقة التشفير الفائق واستمر في ترجمة عملية فك تشفير الرسائل باستخدام طريقة التشفير الفائق.

تهدف هذه الدراسة إلى تحديد عملية التشفير وفك التشفير في التشفير الفائق. نتائج الدراسة هي: في عملية تشفير الرسائل باستخدام طريقة التشفير الفائق ، هناك مرحلتان من العمل. الرسالة الأصلية (نص عادي) هي "P" ، يتم تحويل كل حرف إلى جدول تحويل. المفتاح المستخدم لتشفير الرسائل هو "K". ثم تقوم بعملية التشفير باستخدام تشفير قيصر (طريقة الإمبراطور) ، بعد ذلك يتم تشفير النتائج التي تم الحصول عليها من عملية الاستبدال بواسطة تشفير قيصر باستخدام معادلة $c \equiv (p + k) \, mod \, n$ مرة أخرى باستخدام تقنية التحويل باستخدام تبديل المصفوفة. بحيث تحصل على كلمة مرور (نص مشفر) ، وهي "C"

للحصول على الرسالة الأصلية (نص عادي) ، ابحث أولاً عن المفتاح المستخدم لعملية فك التشفير وابحث عن "K" ، ثم فك تشفير الرسالة المشفرة (نص مشفر) "C" باستخدام تقنية الاستبدال مع المعادلة $c \equiv (p + k) mod \, n$ ، بعد الحصول على نتائج تقنية الاستبدال ، تم فك تشفيرها مرة أخرى باستخدام تقنية النقل مع تبديل المصفوفة. بحيث يتم الحصول على الرسالة الأصلية (نص عادي) من المتوقع أن تستخدم "P". من المتوقع أن تستخدم الدراسات المستقبلية مجموعات أخرى لطريقة التشفير الفائق واستخدام خوارزميات البرنامج للحصول على نتائج أكثر دق

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan merupakan bentuk tindakan untuk mempertahankan sesuatu hal dari berbagai macam gangguan dan ancaman. Selanjutnya, untuk mengatasi permasalahan tersebut dapat diselesaikan dengan kriptografi.

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan yang diperoleh dengan menyandikannya menjadi pesan yang tidak mempunyai makna. Kriptografi dapat digunakan untuk menyamarkan informasi yang bersifat rahasia dari orang atau pihak yang tidak berhak membacanya. Dalam kriptografi terdapat dua proses penyandian, yaitu enkripsi dan dekripsi. Enkripsi adalah sebuah proses penyandian yang mengubah teks-asli atau pesan yang dapat dimengerti (*plaintext*) menjadi teks-kode atau pesan yang tidak bisa dimengerti (*ciphertext*). Dekripsi adalah sebuah proses pembalikan yang mengubah teks-kode atau pesan yang tidak bisa dimengerti (*ciphertext*) menjadi sebuah teks-asli atau pesan yang dapat dimengerti (*plaintext*). Fungsi matematika yang digunakan untuk enkripsi dan dekripsi disebut algoritma kriptografi. Untuk melakukan suatu proses penyandian dan proses pembalikan menggunakan algoritma yang sama (Munir, 2006).

Masalah menjaga keamanan pesan merupakan sesuatu yang sangat penting bagi perusahaan atau organisasi. Dalam ajaran agama Islam sudah diterangkan tentang pentingnya menjaga amanah, yang tercantum dalam firman Allah Swt di surat an-Nisa ayat 58:

إِنَّ اللَّهَ يَأْمُرُكُمْ أَنْ تُؤَدُّوا الْأَمَانَاتِ إِلَىٰ أَهْلِهَا وَإِذَا حَكَمْتُمْ بَيْنَ النَّاسِ أَنْ تَحْكُمُوا بِالْعَدْلِ ۚ إِنَّ اللَّهَ

نِعِمَّا يَعِظُكُمْ بِهِ ۗ إِنَّ اللَّهَ كَانَ سَمِيعًا بَصِيرًا

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.(QS. An-Nisa':58).

Dalam ayat ini dijelaskan yang paling menonjol dalam beramal adalah menyampaikan amanah atau dalam hal ini bisa diartikan menjaga kerahasiaan data yang akan disampaikan.

Suatu sistem yang digunakan untuk mengamankan data agar kerahasiaan data tersebut terjamin dan tersampaikan dengan kerahasiaan yang terjaga, maka perlu menggunakan metode kriptografi untuk mengamankan data yang akan dikirimkan. Adanya kriptografi, diharapkan dapat menjaga kerahasiaan data pada suatu instansi atau kalangan tertentu. Kriptografi yang akan kita gunakan adalah substitusi dan dirangkap dengan transposisi, sehingga pola keamanan yang akan digunakan tidak mudah untuk ditebak atau diketahui.

Pada penelitian sebelumnya telah dibahas tentang cipher substitusi dan cipher transposisi pada data Algoritma Kriptografi Klasik (Rinaldi Munir, 2004). Selanjutnya telah dibahas tentang super enkripsi pada data Perancangan Super Enkripsi Menggunakan Metode Substitusi S-Box AES dan Metode Transposisi dengan Pola Vertical-Horizontal (Frengky Merani dan Danny Wowor, 2016). Sehingga peneliti ingin melakukan suatu kajian yang berjudul "Proses Enkripsi dan Dekripsi Menggunakan Metode Super Enkripsi".

1.2 Rumusan Masalah

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

1. Bagaimanakah proses enkripsi pesan menggunakan metode super enkripsi?
2. Bagaimanakah proses dekripsi pesan menggunakan metode super enkripsi?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah, maka tujuan penelitian ini sebagai berikut:

1. Untuk mengetahui proses enkripsi pesan menggunakan metode super enkripsi.
2. Untuk mengetahui proses dekripsi pesan menggunakan metode super enkripsi.

1.4 Manfaat Penelitian

Beberapa manfaat yang terdapat dalam penelitian ini, di antaranya sebagai berikut:

1. Memperoleh penyelesaian enkripsi pesan menggunakan metode super enkripsi.
2. Memperoleh penyelesaian dekripsi pesan menggunakan metode super enkripsi.

1.5 Batasan Masalah

Peneliti membatasi masalah dalam penelitian yang akan dibahas yaitu

1. Hanya mengenkripsi alfabet.

2. Kunci yang digunakan untuk enkripsi dan dekripsi yaitu kunci $k = 7$ untuk teknik substitusi dan $k = 3$ untuk teknik transposisi.

1.6 Metode Penelitian

Metode yang digunakan penulis adalah studi literatur dengan mempelajari dan menelaah beberapa buku, jurnal, dan referensi lain yang mendukung penelitian ini. Adapun metode penelitian yang penulis gunakan yaitu mengumpulkan, merangkum serta menginterpretasikan data-data yang diperoleh menggunakan studi kepustakaan. Langkah-langkah penelitian yang penulis gunakan adalah:

Proses enkripsi dengan metode super enkripsi

1. Menentukan data pesan *(plaintext)*
2. Menentukan kunci
3. Mengkonversi alfabet ke $\mathbb{Z}_{27}$
4. Melakukan perhitungan dengan substitusi
5. Melakukan perhitungan transposisi dari hasil pehitungan substitusi
6. Mengkonversi $\mathbb{Z}_{27}$ ke alfabet
7. Mendapatkan pesan yang sudah disandikan *(ciphertext)*

Proses dekripsi dengan metode super enkripsi

1. Memasukan pesan yang sudah disandikan (*ciphertext*)
2. Menentukan kunci
3. Mengkonversi alfabet ke $\mathbb{Z}_{27}$
4. Melakukan perhitungan dengan substitusi
5. Melakukan perhitungan transposisi dari hasil pehitungan substitusi
6. Mengkonversi $\mathbb{Z}_{27}$ ke alfabet
7. Mendapatkan pesan asli *(plaintext)*

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam skripsi 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

Bagian ini menjelaskan tentang gambaran umum dari teori yang mendasari pembahasan. Di antaranya tentang keamanan data, kriptografi, Teknik substitusi, Matriks, Teknik transposisi.

Bab III Pembahasan

Bab ini merupakan bab inti dari penulisan skripsi yang dilakukan yaitu berisi penyelesaian.

Bab IV Penutup

Pada bab ini berisi kesimpulan dari hasil dan pembahasan yang telah diperoleh, serta dilengkapi saran-saran yang berkaitan dengan penelitian yang dilakukan.

BAB II

KAJIAN PUSTAKA

2.1 Aritmatika Modulo

Aritmatika modulo (*modular arithmetic*) memainkan peranan penting dalam perhitungan bilangan bulat, khususnya pada aplikasi kriptografi. Operator yang digunakan pada aritmatika modulo adalah mod. Operator mod memberikan sisa pembagian. Misalnya 43 dibagi 5 memberikan hasil 8 dan sisa 3. Sehingga ditulis $43 \ mod \ 5 \ = \ 3$ (Munir, 2006).

2.2 Kongruensi

Kongruensi merupakan cara lain untuk mengkaji keterbagian dalam himpunan bilangan bulat.

Definisi 1

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

$$a \equiv b(mod\ M) \tag{2.1}$$

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

Dari definisi diatas, dapat ditelaah:

Jika $M > 0$ dan $M|(a - b)$ maka ada suatu bilangan bulat t sehingga $a - b = Mt$. Sehingga $a \equiv b(mod\ M)$ dapat dinyatakan sebagai $a - b = Mt$, ini sama artinya dengan $a \equiv b(mod\ M)$ atau beda antara a dan b merupakan kelipatan M.

Dalam kongruensi juga terdapat beberapa teorema sebagai berikut:

Teorema 1

Andaikan a, b dan c adalah bilangan bulat dan m bilangan asli, maka berlaku:

1. Refleksi $a \equiv a(mod\ m)$
2. Simetris, jika $a \equiv b(mod\ m)$, maka:

   $b \equiv a(mod\ m)$ dan $a - b \equiv 0(mod\ m)$ adalah pernyataan yang ekuivalen.

Transitif, jika $a \equiv b(mod\ m)$ dan $b \equiv c(mod\ m)$ maka $a \equiv c(mod\ m)$ (Irawan dkk, 2014).

Bukti :

1. Jika $m \neq 0$ maka $m|0$ yang dapat dituliskan sebagai $m|a - a$.

   Menurut definisi berlaku $a \equiv a(mod\ m)$ untuk semua bilangan bulat a dan $m \neq 0$.

   Cara lain: $a \equiv a(mod\ m)$, sebab $a - a = 0$dan $m|0$
2. $a \equiv b(mod\ m)$berarti $m|a - b$, menurut definisi 1 ada keterbagian bilangan bulat t sehingga:

   $m|a - b$ dapat dinyatakan $a - b = tm$

$$\Leftrightarrow -(a - b) = -tm$$

$$\Leftrightarrow b - a = (-t)m$$

Menurut definisi 1, ini berarti $b \equiv a(mod\ m)$.

$a \equiv b(mod\ m)$ berarti $m|a - b$, menurut definisi ada bilangan bulat t sehingga $m|a - b$ dapat dinyatakan $a - b = tm$

untuk setiap $(a - b) - 0 = tm$ maka $(ab) \equiv 0(mod\ m)$.

Teorema 2

Jika $a \equiv b(mod\ m)$, maka $a + c \equiv b + c(mod\ m)$ (Irawan dkk, 2014)

Bukti:

$a \equiv b(mod\ m)$ berarti $m|a - b$

menurut definisi pada keterbagian ada bilangan bulat t sehingga:

$m|a - b$ dapat dinyatakan $a - b = tm$

$$\Leftrightarrow (a - b) + 0 = tm$$

$$\Leftrightarrow (a - b) + (c - c) = tm$$

$$\Leftrightarrow (a + c) + (b + c) = tm$$

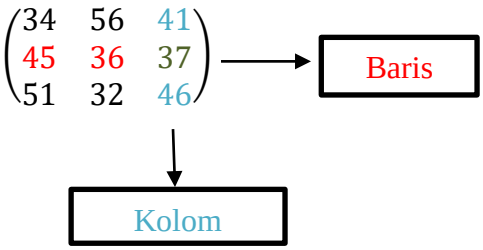
Sesuai definisi maka diperoleh $a + c \equiv b + c(mod\ m)$

2.3 Matriks

Matriks adalah kumpulan bilangan yang disusun secara khusus dalam bentuk baris dan kolom sehingga membentuk empat persegi panjang atau bujur sangkar yang ditulis di antara dua tanda kurung, yaitu ( ) atau [ ] (Ruminta, 2014)

2.3.1 Ordo Matriks

Dijelaskan sebelumnya matriks terdiri dari unsur-unsur yang tersusun secara baris dan kolom. Jika banyak baris suatu matriks adalah m, dan banyak kolom suatu matriks adalah n, maka matriks tersebut memiliki ordo matriks atau ukuran $m\ x\ n$. Perlu diingat bahwa m dan n hanya sebuah notasi, sehingga tidak boleh dilakukan sebuah perhitungan (penjumlahan, perkalian). Pada contoh matriks dibawah 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

Penamaan/notasi matriks menggunakan huruf kapital, sedangkan elemen-elemen di dalamnya dinotasikan dengan huruf kecil sesuai dengan penamaan matriks dan diberi indeks ij. Indeks tersebut menyatakan posisi elemen matriks, yaitu pada baris i dan kolom j.

Untuk mengetahui matriks dalam matematika lebih dalam, ada beberapa jenis matriks yang perlu diketahui. Jenis-jenisnya adalah:

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 : matriks yang memiliki jumlah baris dan kolom yang sama.
5. Matriks identitas : matriks konstanta dengan elemen diagonal utama adalah 1.

2.3.2 Transpose Matriks

Transpose matriks merupakan perubahan baris menjadi kolom dan sebaliknya. Jika $\boldsymbol{A}_{m\times n}$ adalah sebuah matriks dengan ukuran $(n \times m)$, maka transpose dari $\boldsymbol{A}$, dinyatakan oleh $\boldsymbol{A}^{\boldsymbol{T}}$, $\boldsymbol{A}^{\boldsymbol{t}}$, atau $\boldsymbol{A}'$, didefinisikan menjadi matriks $n \times m$ yang merupakan hasil dari pertukaran baris dan kolom dari matriks $\boldsymbol{A}$.

Jika matriks **A** dinyatakan: $\boldsymbol{A}_{m\times n} = (\boldsymbol{a}_{ij})$,

maka transpose matriks $\boldsymbol{A}$ dinyatakan: $\boldsymbol{A}^T = (\boldsymbol{b}_{ij})$, dimana $\boldsymbol{b}_{ij} = \boldsymbol{a}_{ji}$

Contoh:

$\begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$ ditranspose menjadi $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$.

Sifat-sifat dari transpose matriks:

1) Jika $\boldsymbol{A}$ dan $\boldsymbol{B}$ adalah dua matriks yang berorde sama maka: $(\boldsymbol{A} \pm \boldsymbol{B})^T = \boldsymbol{A}^{\boldsymbol{T}} \pm \boldsymbol{B}^T$
2) Jika α skalar dan $\boldsymbol{A}$ matriks, maka: $(\alpha \boldsymbol{A})^T = \alpha \boldsymbol{A}^T$
3) Jika $\boldsymbol{A}$ matriks, maka $(\boldsymbol{A}^T)^T = \boldsymbol{A}$
4) Jika $\boldsymbol{A}$ matriks bujur sangkar dan n positif, maka:

$$(\boldsymbol{A}^n)^T = (\boldsymbol{A}^T)^n$$

5) Jika $\boldsymbol{A}$, $\boldsymbol{B}$ dua matriks dengan ukuran masing-masing $m \times n$ dan $n \times p$, maka $(\boldsymbol{AB})^T = \boldsymbol{B}^T \boldsymbol{A}^T$ (Ruminta, 2014).

2.4 Kriptografi

Kriptografi adalah ilmu mengenai teknik enkripsi dimana "naskah asli" (*plaintext*) diacak menggunakan suatu kunci enkripsi menjadi "naskah acak yang sulit dibaca" (*ciphertext*) oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi dalam waktu yang tidak terlalu lama adalah sangat kecil.

Teknik enkripsi yang digunakan dalam kriptografi klasik adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk *public key cryptography*, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan–bilangan yang sangat besar (Kromodimoeljo, 2010).

Prinsip-prinsip yang mendasari kriptografi yakni :

1. Kerahasiaan (*Confidelity*) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki izin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.
2. Keutuhan data (*Data Integrity*) yaitu layanan yang mampu mengenali / mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).

3. Keotentikan (*Authentication*) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
4. Anti-penyangkalan (*Non-repudiation*) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya) (Menezes, 1996).

2.5 Kriptografi Klasik dan Kriptografi Modern

Kriptografi klasik merupakan suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Teknik ini sudah digunakan beberapa abad yang lalu. Dua teknik dasar yang biasa digunakan pada algoritma jenis ini adalah sebagai berikut:

1. Teknik substitusi, penggantian setiap karakter teks-asli dengan karakter lain.
2. Teknik transposisi (permutasi), dilakukan dengan menggunakan permutasi karakter (Ariyus, 2008).

Salah satu teknik enkripsi menggunakan kunci simetri adalah teknik substitusi, yaitu mengganti setiap karakter *plaintext* dengan karakter lain. Terdapat empat cara dalam menggunakan teknik substitusi, yaitu:

1. *Monoalphabet*, dimana setiap karakter *ciphertext* mengganti satu macam karakter *plaintext* tertentu.
2. *Polialphabet,* dimana setiap karakter *ciphertext* mengganti lebih dari satu macam karakter *plaintext*.
3. *Monograf/unilateral*, dimana satu enkripsi dilakukan terhadap satu karakter *plaintext*.
4. *Poligraf/multilateral*, dimana satu enkripsi dilakukan terhadap lebih dari satu karakter *plaintext* (Menezes, 1996).

Kriptografi modern merupakan suatu algoritma yang digunakan pada saat sekarang ini, yang mana kriptografi modern mempunyai kerumitan yang sangat komplek, karena dalam pengoperasiannya menggunakan komputer (Ariyus, 2006).

2.6 Algoritma Kriptografi

Definisi terminologi algoritma adalah urutan langkah-langkah logis untuk menyelesaikan masalah yang disusun secara matematis. Sedangkan kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut.

Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu:

1. Enkripsi, merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaannya. Pesan asli disebut *Plaintext*, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *cipher* atau kode.
2. Dekripsi, merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks-asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma untuk enkripsi.
3. Kunci, yang dimaksud adalah kunci yang dipakai untu melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci rahasia (*private key*) dan kunci umum (*public key*).

Keamanan dari algoritma kriptografi tergantung pada bagaimana algoritma itu bekerja. Oleh sebab itu algoritma semacam ini disebut dengan algoritma terbatas.

Algoritma terbatas merupakan algoritma yang dipakai sekelompok orang untuk merahasiakan pesan yang mereka kirim. Jika salah satu dari anggota itu keluar dari kelompoknya maka algoritma yang dipakai diganti dengan yang baru. Jika tidak maka hal itu bisa menjadi masalah di kemudian hari.

Keamanan dari kriptografi modern didapat dengan merahasiakan kunci yang dimiliki dari orang lain, tanpa harus merahasiakan algoritma itu sendiri. Kunci memiliki fungsi yang sama dengan *password*. Jika keseluruhan dari keamanan algoritma tergantung pada kunci yang dipakai maka algoritma ini bisa dipublikasikan dan dianalisis oleh orang lain. Jika algoritma yang telah dipublikasikan bisa dipecahkan dalam waktu yang singkat oleh orang lain maka algoritma tersebut tidak aman untuk digunakan (Ariyus, 2008).

2.7 Kode Kaisar (*Caesar Code*)

Substitusi kode yang pertama dalam dunia penyandian terjadi pada pemerintahan Yulis Caesar yang dikenal dengan kode kaisar, dengan mengganti posisi huruf awal dari alfabet atau di sebut juga dengan algoritma ROT3.

Tabel 2.1 *CAESAR CIPHER* ROT3

PLAIN TEXT	*ENCODED TEXT*
ABC	DEF
Hello	Khoor
Attack	Dwwdfn

Secara lebih detail, coba perhatikan contoh berikut:

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25

Menjadi:

d	e	f	g	h	i	j	k	l	m	n	o	p
3	4	5	6	7	8	9	10	11	12	13	14	15

q	r	s	t	u	v	w	x	y	z	a	b	c
16	17	18	19	20	21	22	23	24	25	0	1	2

Jika penggeseran yang dilakukan sebanyak tiga kali maka kunci untuk deskripsinya adalah 3. Penggeseran kunci yang dilakukan tergantung keinginan pengirim pesan. Bisa saja kunci yang dipakai $a = 7,8,9$, dan seterusnya (Ariyus, 2008).

Dalam kode kaisar, untuk teks-asli diberikan simbol "P" dan teks-kodenya "C" dan kunci "K" dan jumlah karakter konversinya "n". Jadi rumusnya sebagai berikut:

$$C \equiv (P + K)\ mod\ n \tag{2.2}$$

Rumus dekripsinya sebagai berikut:

$$P \equiv (C - K)\ mod\ n \tag{2.3}$$

2.8 Teknik Transposisi

Teknik ini menggunakan teknik ini pesan yang asli tidak dapat dibaca kecuali oleh orang yang memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula, sebagai contoh:

Ada 6 kunci untuk melakukan permutasi kode :

1	2	3	4	5	6
3	5	1	6	4	2

Gambar 2.2 Pemutasi

Dan 6 kunci untuk inversi dari permutasi tersebut:

1	2	3	4	5	6
3	6	1	5	2	4

Gambar 2.3 Inversi dari Permutasi

Seandainya melakukan permutasi terhadap kalimat di bawah ini:

"SAYA SEDANG BELAJAR KEAMANAN KOMPUTER"

Terlebih dahulu kalimat tersebut dibagi menjadi 6 blok dan apabila terjadi kekurangan dari blok bisa ditambah dengan huruf yang disukai. Dalam contoh ini ditambah huruf X. Hal ini berguna untuk mempersulit analisis dari kode tersebut.

SAYASE DANGBE LAJARK EAMANA NKOMPU TERXXX

Setelah dibagi menjadi 6 blok maka dengan menggunakan kunci di atas setiap blok akan berubah menjadi seperti di bawah ini:

YSSEAA NBDEGA JRLKAA MNEAAA OPNUMK RXTXXE

Jadi teks-kode yang dihasilkan:

"YSSEAANBDEGAJRLKAAMNEAAAOPNUMKRXTXXE"

Untuk menghasilkan ke bentuk teks-asli maka dilakukan inversi terhadap *ciphertext* dengan mengikuti kunci nomor dua di atas. Ada banyak teknik untuk permutasi ini, seperti zig-zag, segitiga, spiral, dan diagonal.

1. Zigzag.

Memasukkan teks-asli dengan pola zig-zag seperti contoh di bawah ini:

			a					g					a					a					m					x
		y		s				n		b				j		r				m		n				o		p				r	
	a				e		a				e		a				k		a				a		k				u		e		
s						d						l						e						n					t				

Gambar 2.4 Teknik Permutasi Pola Zigzag

Teks-kode dari teknik ini dengan membaca dari baris atas k baris bawah

“AGAAMXYSNBJRMNOPRAEAEAKAAKUESDLENTX”

2. Segitiga.

   Masukkan teks-asli dengan pola segitiga dan dibaca dari atas ke bawah.

					S					
				A	Y	A				
			B	E	L	A	J			
		R	K	E	A	M	A	N		
	A	N	K	O	M	P	U	T	E	
R	X	X	X	X	X	X	X	X	X	X

Gambar 2.5 Teknik Permutasi Pola Segitiga

   Teks-kodenya adalah:

   “RAXRNXBKKXAEEOXSYLAMXAAMPXJAUXNTXEXX

3. Spiral.

   Teks-asli dimasukkan secara spiral dan dapat dibaca dari atas ke bawah. Lihat contoh dibawah ini:

S	A	Y	A	S	E
A	M	A	N	A	D
E	E	R	X	N	A
K	T	X	X	K	N
R	U	P	M	O	G
A	J	A	L	E	B

Gambar 2.6 Teknik Permutasi Pola Spiral

   Teks-kodenya adalah:

   “SAEKRAAMETUJYARXPAANXXMLSANKOEEDANGB”

4. Diagonal.

   Dengan menggunakan pola ini teks-asli dimasukkan dengan cara diagonal.

   Coba perhatikan contoh di bawah ini:

S	D	L	E	N	E
A	A	A	A	K	R
Y	N	J	M	O	X
A	G	A	A	M	X
S	B	R	N	P	X
E	E	K	A	U	X

Gambar 2.7 Teknik Permutasi Pola Diagonal

Teks-kodenya adalah:

"SDLENEAAAAKRYNJMOCAGAAMXSBRNPXEEKAUX"

Teknik transposisi (permutasi) memiliki bermacam-macam pola yang bisa digunakan untuk menyembunyikan pesan dari tangan orang-orang yang tidak berhak. Kombinasi tersebut merupakan dasar dari pembentukan algoritma kriptografi yang kita kenal sekarang ini (modern).

2.9 Super Enkripsi

Super enkripsi merupakan salah satu kriptografi berbasis karakter yang menggabungkan cipher substitusi dan cipher transposisi untuk mendapatkan cipher yang lebih kuat (tidak mudah dipecahkan). Enkripsi dan dekripsi dapat dilakukan dengan urutan cipher substitusi, kemudian cipher transposisi, atau sebaliknya.

Konsep super enkripsi dapat diperluas penggunaannya dari teks ke citra warna. Ini dimungkinkan mengingat sebuah citra merupakan deretan piksel-piksel yang terdiri atas komponen *red* I, *green* (G), *blue* (B) yang merupakan bilangan-bilangan bulat sehingga dapat dioperasikan dalam sebuah matriks. Contoh dari super enkripsi adalah seperti dibawah ini:

Diketahui teks-asli:

"KENAIKAN HARGA BBM MEMBUAT RAKYAT KECIL MENDERITA"

1. Menggunakan teknik substitusi kode dengan memakai algoritma kode kaisar dengan kunci 6.

a	b	c	d	e	f	g	h	i	j	k	l	m
g	h	i	j	k	l	m	n	o	p	q	r	s

n	o	p	q	r	s	t	u	v	w	x	y	z
t	u	v	w	x	y	z	a	b	c	d	e	f

Gambar 2.8 Teknik Substitusi dengan Kunci 6

Teks-kode yang didapat:

"QKTGOQGTNGXMGHHSSKSHAGZQKIORSKTJKXOZG"

2. Menggunakan teknik transposisi kode (permutasi kode) dengan menggunakan teknik diagonal permutasi dengan kunci 4.

Q	K	T	G
O	Q	G	T
N	G	X	M
G	H	H	S
S	K	S	H
A	G	Z	Q
K	I	O	R
S	K	T	J
K	X	O	S
G	X	X	X

Gambar 2.9 Teknik Transposisi dengan Kunci 4

Maka didapat hasil akhir sebagai berikut:

"QONGSAKSKGKQGHKGIKXXTGXHSZOTOXGTMSHQRJSX"

Teks dari enkripsi super sangat penting dan banyak dari algoritma enkripsi modern menggunakan teknik ini sebagai dasar pembuatan suatu algoritma (Ariyus, 2008).

2.2 Keamanan Data

Keamanan *database* adalah suatu cara untuk melindungi *database* dari ancaman, baik dalam bentuk kesengajaan atau pun bukan. Ancaman adalah segala situasi atau kejadian baik secara sengaja maupun tidak yang bersifat merugikan dan mempengaruhi sistem serta secara konsekuensi terhadap perusahaan/organisasi yang memiliki sistem *database*. Keamanan *database* tidak hanya berkenaan dengan data yang ada pada *database* saja, tetapi juga meliputi bagian lain dari sistem *database*, yang tentunya dapat mempengaruhi *database* tersebut. Hal ini berarti keamanan *database* mencakup perangkat keras, perangkat lunak, orang dan data. Agar memiliki suatu keamanan yang efektif dibutuhkan kontrol yang tepat. Seseorang yang mempunyai hak untuk mengontrol dan mengatur *database* biasanya disebut *administrator database*, sehingga administrator yang memegang peranan penting pada suatu sistem *database*, oleh karena itu administrator harus mempunyai kemampuan dan pengetahuan yang cukup agar dapat mengatur suatu sistem (Shona, 2017).

2.3 Pengertian Amanah

Amanah secara etimologis (pendekatan kebahasaan/lughawi) dari bahasa Arab dalam bentuk mashdar dari (amina-amanatan) yang berarti jujur atau dapat dipercaya. Adapaun Amanah menurut pengertian terminologi (istilah) terdapat beberapa pendapat, diantaranya menurut Ahmad Musthafa al-Maraghi, Amanah adalah sesuatu yang harus dipelihara dan dijaga agar sampai kepada yang berhak memilikinya. Dari pengertian tersebut dapat diambil suatu pengertian bahwa amanah adalah menyampaikan hak apa saja kepada pemiliknya, tidak mengambil

sesuatu melebihi haknya dan tidak mengurangi hak orang lain, baik berupa harga maupun jasa.

Di dalam tafsir jalalain pada QS. An-Nisaa'/4:58 Allah Swt berfirman "*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".* Hal itu mencakup seluruh amanah yang wajib bagi manusia, berupa hak-hak Allah Swt terhadap para hamba-Nya, seperti shalat, zakat, puasa, kafarat, nadzar dan selain dari itu, yang kesemuanya adalah amanah yang diberikan tanpa pengawasan hamba-Nya yang lain. Itulah yang diperintahkan oleh Allah Swt untuk ditunaikan. Barang siapa yang tidak melakukannya di dunia ini, maka akan dimintai pertanggungjawabannya di hari Kiamat. Hal ini menandakan betapa pentingnya menyampaikan pesan dengan baik seperti metode mengamankan pesan dengan metode super enkripsi.

BAB III

PEMBAHASAN

3.1 Proses Enkripsi dengan Metode Super Enkripsi

Pada bab ini akan dijelaskan tentang proses enkripsi dengan metode kode kaisar, teknik transpose dan juga super enkripsi

3.1.1 Enkripsi dengan Kode Kaisar

Proses enkripsi dengan menggunakan kode kaisar adalah menentuan teks-asli dan juga menentukan kunci untuk kemudian diolah. Untuk teks-asli diberikan simbol "P" dan teks-kodenya "C" dan kunci "K". Jadi rumusnya dapat ditulis sebagai berikut:

$$C \equiv E(P) \equiv (P + K) \ mod\ n \tag{3.1}$$

Pada proses substitusi, sebelumnya penulis melakukan konversi menggunakan tabel konversi sendiri. Seperti dibawah ini:

Tabel 3.1 Tabel Konversi Alfabet ke $\mathbb{Z}_{27}$

Karakter	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Kode	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Karakter	p	q	r	s	t	u	v	w	x	y	z	Spasi
Kode	15	16	17	18	19	20	21	22	23	24	25	26

Contoh, jika diberikan teks asli sebagai berikut:

BANJIR MERENDAM PASURUAN

Dengan mengguakan kunci lima maka akan didapat teks-kode berikut:

GFSONWRJWJSIFRUFXZWZFS

3.1.2 Enkripsi dengan Metode Transposisi

Pada kode transposisi menggunakan tranpose matriks. Jika A adalah matriks $m \times n$, maka tranpose dari **A** (*transpose of* $\boldsymbol{A}$), dinyatakan dengan $\boldsymbol{A^T}$, didefinisikan sebagai matriks $n \times m$ yang didapatkan dengan mempertukarkan baris-baris dan kolom-kolom dari $\boldsymbol{A}$, sehingga kolom pertama dari $\boldsymbol{A^T}$ adalah baris pertama dari $\boldsymbol{A}$, kolom kedua dari $\boldsymbol{A^T}$ adalah baris kedua dari $\boldsymbol{A}$, dan seterusnya. Dapat dituliskan sebagai berikut:

$$\boldsymbol{A}_{ij} = \boldsymbol{A^T}_{ji}$$

Contoh:

$$\boldsymbol{A} = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

Menjadi:

$$\boldsymbol{A^T} = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix}$$

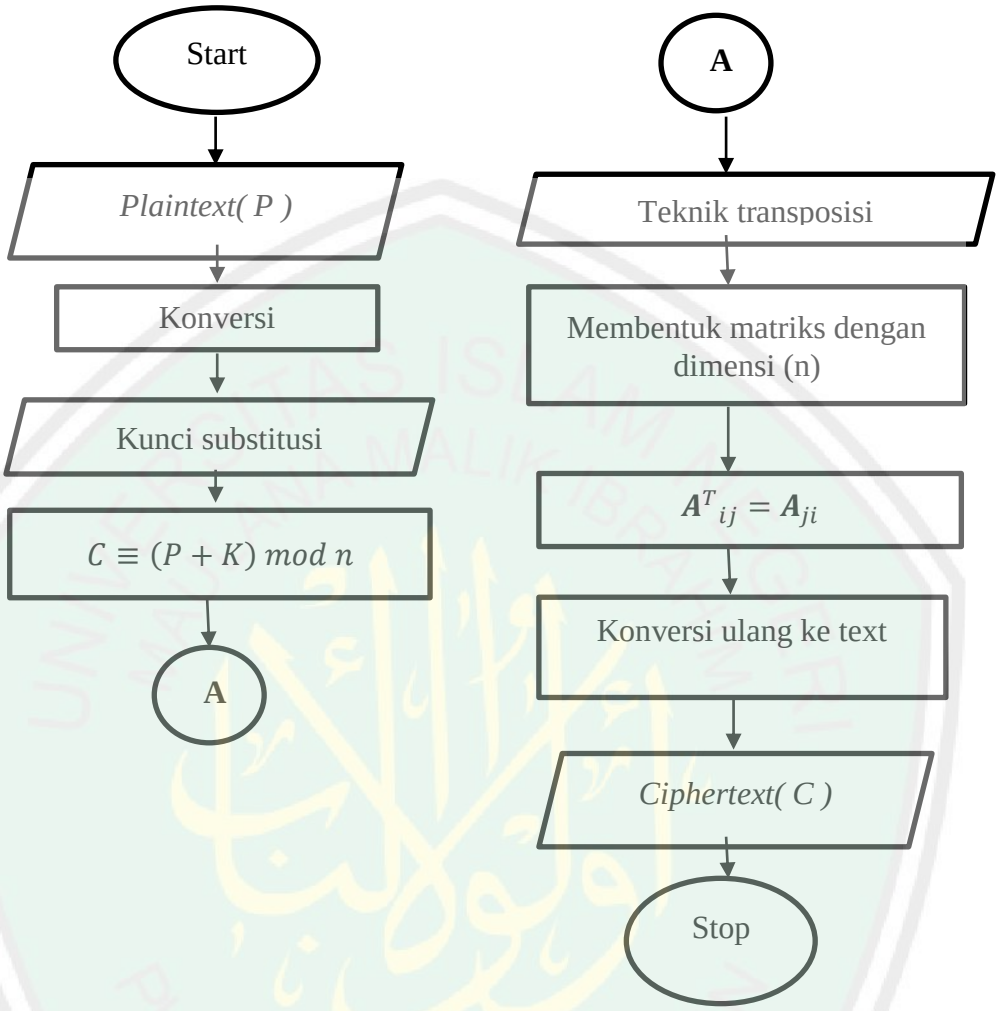
Contoh:

$$\boldsymbol{A} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}$$

Menjadi:

$$\boldsymbol{A^T} = \begin{bmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{bmatrix}$$

3.1.3 Flowchart



Gambar 3.1 Flowchart proses enkripsi

3.1.4 Enkripsi dengan Metode Super Enkripsi

1. *Plaintext*

Pada saat melakukan proses enkripsi, penulis menentukan pesan asli yang akan dienkripsi dengan menggunakan metode super enkripsi. Dalam hal ini penulis menggunakan pesan asli " AKU DAN KAU"

2. Kunci

Pada penentuan kunci, penulis menentukan atau mengambil sebarang bilangan. Dalam hal ini penulis mengambil dua kunci, kunci pertama yaitu untuk kunci substitusi dan kunci kedua yaitu untuk kunci pada proses transpose matriks. Ambil kunci pertama $K = 7$ dan kunci kedua $K = 3$

3. Konversi

Langkah konversi ini dilakukan setelah menentukan kunci yang akan dipakai. Penulis melakukan konversi *plaintext* ke $\mathbb{Z}_{27}$, seperti pada tabel 3.1. seperti berikut :

Tabel 3.2 Tabel Konversi Alfabet ke $\mathbb{Z}_{27}$ pada Proses Enkripsi

Karakter	a	k	u	spasi	d	a	n	spasi	k	a	u
Kode	0	10	20	26	3	0	13	26	10	0	20

4. Substitusi $(C \equiv (P + K) mod\ n)$

Pada langkah substitusi penulis menggunakan kunci pertama yaitu K=7, kemudian dimasukkan ke rumus substitusi.

Tabel 3.3 Enkripsi dengan Teknik Substitusi

Plaintext	Teknik substitusi
$a = 0$	$C = (0 + 7)\ mod\ 27$ $C = 7\ mod\ 27$ $C = 7$
$k = 10$	$C = (10 + 7)\ mod\ 27$ $C = 17\ mod\ 27$ $C = 17$
$u = 20$	$C = (20 + 7)\ mod\ 27$ $C = 27\ mod\ 27$ $C = 0$
$spasi = 26$	$C = (26 + 7)\ mod\ 27$ $C = 33\ mod\ 27$ $C = 6$
$d = 3$	$C = (3 + 7)\ mod\ 27$ $C = 10\ mod\ 27$ $C = 10$

Lanjutan Tabel 3.3 Enkripsi dengan Teknik Substitusi

Plaintext	Teknik substitusi
$a = 0$	$C = (0 + 7)\ mod\ 27$ $C = 7\ mod\ 27$ $C = 7$
$n = 13$	$C = (13 + 7)\ mod\ 27$ $C = 20\ mod\ 27$ $C = 20$
$spasi = 26$	$C = (26 + 7)\ mod\ 27$ $C = 33\ mod\ 27$ $C = 6$
$k = 10$	$C = (10 + 7)\ mod\ 27$ $C = 17\ mod\ 27$ $C = 17$
$a = 0$	$C = (0 + 7)\ mod\ 27$ $C = 7\ mod\ 27$ $C = 7$
$u = 20$	$C = (20 + 7)\ mod\ 27$ $C = 27\ mod\ 27$ $C = 0$

5. Transposisi

Pada teknik transposisi menggunakan transpose matriks, dengan membentuk matriks menggunakan kunci $K = 3$. Kunci tersebut adalah kunci untuk membentuk matriks dimana jumlah barisnya adalah 3.

$$\boldsymbol{A} = \begin{bmatrix} 7 & 17 & 0 \\ 6 & 10 & 7 \\ 20 & 6 & 17 \\ 7 & 0 & \times \end{bmatrix}$$

$$\boldsymbol{A}^T = \begin{bmatrix} 7 & 6 & 20 & 7 \\ 17 & 10 & 6 & 0 \\ 0 & 7 & 17 & \times \end{bmatrix}$$

6. Konversi kembali

Dari hasil enkripsi dengan teknik transposisi, kemudian dilakukan konversi kembali yaitu dari $\mathbb{Z}_{27}$ ke alfabet.

Tabel 3.4 Konversi Kembali dari $\mathbb{Z}_{27}$ ke Alfabet

Karakter	7	6	20	7	17	10	6	0	0	7	17	×
Kode	h	g	u	h	r	k	g	a	a	h	r	×

7. Hasil

Sehingga hasil yang diperoleh dari proses enkripsi dengan menggunakan metode super enkripsi adalah “hguhrkgaahr×”.

3.2 Dekripsi dengan menggunakan Metode Super Enkripsi

Pada bab ini dijelaskan proses dekripsi dengan metode kaisar, teknik transpose dan metode super enkripsi.

3.2.1 Dekripsi dengan Kode Kaisar

Proses dekripsi pada kode kaisar menggunakan rumus pada persamaan (2.1):

$$C \equiv (P + K) mod\ n$$

$$P + K \equiv C\ mod\ n \quad \text{(karena simetris)}$$

$$P + K - K \equiv C - K\ mod\ n \quad \text{(teorema 2)}$$

$$P \equiv (C - k)\ mod\ n \tag{3.2}$$

3.2.2 Dekripsi dengan Metode Transposisi

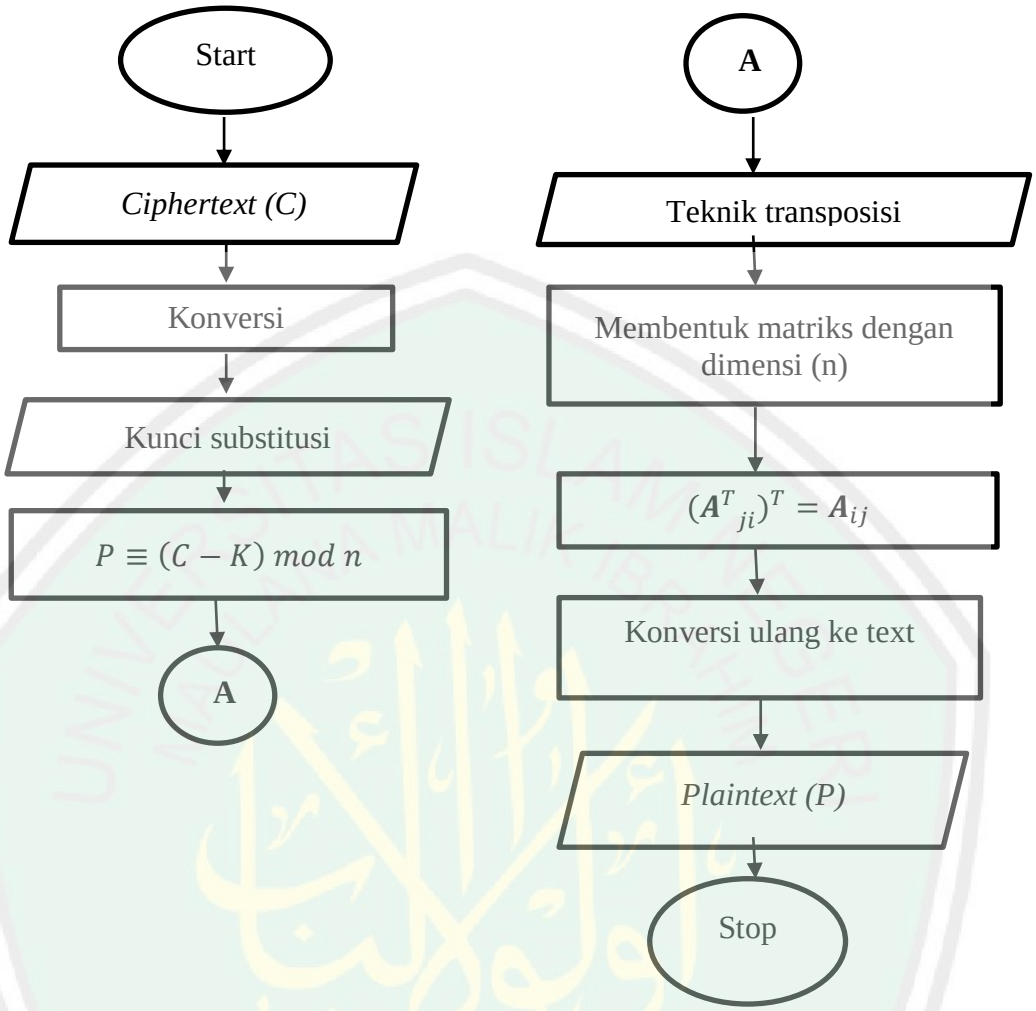
Dengan menggunakan definisi dari transpose matriks, maka dapat ditulis:

$$\boldsymbol{A}_{ij} = \boldsymbol{A}^{T}{}_{ji}$$

maka:

$$(\boldsymbol{A}^{T}{}_{ji})^{T} = \boldsymbol{A}_{ij}$$

3.2.3 Flowchart



Gambar 3.2 Flowchart Proses Dekripsi

3.2.4 Dekripsi dengan Metode Super Enkripsi

1. *Ciphertext*

Pada proses dekripsi, pesan yang tersandi *(ciphertext)* didapat dari hasil enkripsi sebelumnya yaitu “hguhrkgaahr×”

2. Kunci

Pada penentuan kunci, penulis menentukan atau mengambil sebarang bilangan. Dalam hal ini penulis mengambil dua kunci, kunci pertama yaitu untuk kunci substitusi dan kunci kedua yaitu untuk kunci pada proses transpose matriks. Ambil kunci pertama $K = 7$ dan kunci kedua $K = 3$

3. Konversi

Langkah konversi ini dilakukan setelah menentukan kunci yang akan dipakai. Penulis melakukan konversi *plaintext* ke $\mathbb{Z}_{27}$, seperti pada tabel 3.1.

Tabel 3.5 Tabel Konversi Alfabet ke $\mathbb{Z}_{27}$

Karakter	h	g	u	h	r	k	g	a	a	h	r	×
Kode	7	6	20	7	17	10	6	0	0	7	17	×

4. Substitusi $(P \equiv (C - K) mod\ n)$

Pada langkah substitusi penulis menggunakan kunci pertama yaitu K=7, kemudian dimasukkan ke rumus substitusi.

Tabel 3.6 Tabel Dekripsi menggunakan Teknik Substitusi

Plaintext	Teknik substitusi
$h = 7$	$P = (7 - 7)\ mod\ 27$ $P = 0\ mod\ 27$ $P = 0$
$g = 6$	$P = (6 - 7)\ mod\ 27$ $P = 26 mod\ 27$ $P = 26$
$u = 20$	$P = (20 - 7)\ mod\ 27$ $P = 13\ mod\ 27$ $P = 13$
$h = 7$	$P = (7 - 7)\ mod\ 27$ $P = 0\ mod\ 27$ $P = 0$
$r = 17$	$P = (17 - 7)\ mod\ 27$ $P = 10\ mod\ 27$ $P = 10$
$k = 10$	$P = (10 - 7)\ mod\ 27$ $P = 3 mod\ 27$ $P = 3$

Lanjutan Tabel 3.6 Tabel Dekripsi menggunakan Teknik Substitusi

Plaintext	Teknik Substitusi
$g = 6$	$P = (6 - 7)\ mod\ 27$ $P = 26\ mod\ 27$ $P = 26$
$a = 0$	$P = (0 - 7)\ mod\ 27$ $P = 20\ mod\ 27$ $P = 20$
$a = 0$	$P = (0 - 7)\ mod\ 27$ $P = 20\ mod\ 27$ $P = 20$
$h = 7$	$P = (7 - 7)\ mod\ 27$ $P = 0\ mod\ 27$ $P = 0$
$r = 17$	$P = (17 + 7)\ mod\ 27$ $P = 10\ mod\ 27$ $P = 10$

5. Transposisi

Pada teknik transposisi menggunakan transpose matriks, dengan membentuk matriks menggunakan kunci $K = 3$. Kunci tersebut adalah kunci untuk membentuk matriks dimana jumlah barisnya adalah 3.

$$\boldsymbol{A} = \begin{bmatrix} 0 & 26 & 13 & 0 \\ 10 & 3 & 26 & 20 \\ 20 & 0 & 10 & \times \end{bmatrix}$$

$$\boldsymbol{A}^T = \begin{bmatrix} 0 & 10 & 20 \\ 26 & 3 & 0 \\ 13 & 26 & 10 \\ 0 & 20 & \times \end{bmatrix}$$

6. Konversi kembali

Dari hasil dekripsi dengan teknik transposisi, kemudian dilakukan konversi kembali yaitu dari $\mathbb{Z}_{27}$ ke alfabet.

Tabel 3.7 Konversi Kembali dari $\mathbb{Z}_{27}$ ke Alfabet

Karakter	0	10	20	26	3	0	13	26	10	0	20	×
Kode	a	k	u	spasi	d	a	n	spasi	k	a	u	×

7. Hasil

Sehingga hasil yang diperoleh dari proses dekripsi dengan menggunakan metode super enkripsi adalah “AKU DAN KAU”

3.3 Integrasi Agama dengan Kriptografi

Allah Swt menurunkan wahyu kepada Nabi Muhammad Saw. yaitu kitab suci al-Qur’an melalui perantara malaikat Jibril, kejadian tersebut merupakan penerapan dari penyandian, selain proses turunnya wahyu, penyandian juga berkaitan dengan penyampaian pesan bagi yang berhak menerimanya yaitu amanah. Setiap manusia hendaknya selalu amanah dalam banyak hal salah satunya amanah dalam menjaga rahasia. Manusia merupakan khalifah yang seharusnya memimpin diri sendiri bahkan orang lain untuk menjadikan dunia ini lebih baik.

Oleh karena itu setiap manusia harus menunaikan amanahnya dengan baik supaya manusia dapat mempertanggungjawabkan perbuatannya kelak di hari akhir dengan baik juga, karena setiap perbuatan pasti dimintai pertanggungjawaban.

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan pembahasan yang telah dilakukan dapat ditarik kesimpulan sebagai berikut:

1. Pada proses enkripsi pesan dengan menggunakan metode super enkripsi ada dua tahap pengerjaan. Pesan asli (*plaintext*) yaitu "P", setiap karakternya dikonversi kedalam tabel konversi. Kunci yang digunakan untuk mengenkripsi pesan yaitu "K". Selanjutnya melakukan proses enkripsi menggunakan *Caesar Cipher* (metode kaisar), setelah diperoleh hasil dari proses substitusi dengan *Caesar Cipher* menggunakan persamaan $c \equiv (p + k) mod\ n$ kemudian dienkripsi kembali dengan teknik transposisi menggunakan transpose matriks. Sehingga didapatkan pesan sandi (*ciphertext*) yaitu "C".
2. Untuk mendapatkan pesan asli (*plaintext*), pada proses dekripsi pesan yang sudah disandikan (*ciphertext*) "C" didekripsi dengan menggunakan teknik dan kunci "K" yang sama dengan proses enkripsi. Tetapi menggunakan persamaan $p \equiv (c - k) mod\ n$ untuk proses substitusi. Setelah diperoleh hasil dari teknik substitusi, didekripsi kembali menggunakan teknik transposisi dengan transpose matriks. Sehingga diperoleh pesan asli (*plaintext*) yaitu "P".

4.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, ada beberapa saran untuk peneliti berikutnya:

1. Menggunakan kombinasi lain untuk metode super enkripsi.
2. Menggunakan algoritma program untuk mendapatkan hasil yang lebih akurat.

DAFTAR RUJUKAN

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

Ariyus, D. 2008. *Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi*. Yogyakarta: C.V Andi Offset.

Irawan, W. H., Hijriyah, N., dan Habibi, A. R. 2014. *Pengantar Teori Bilangan*. Malang: UIN Malang Press.

Katsir, I. 2003. *Terjemah Tafsir Ibnu Katsir*, Jilid 2. Jakarta: Pustaka Imam Syafii.

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

Menezes, A. J., dkk. 1996. *Handbook of Applied Cryptography*. CRC Press.

Merani, F., Wowor D. 2016. *Perancangan Super Enkripsi Menggunakan Metode Substitusi S-Box AES Dan Metode Transposisi Dengan Pola Vertical-Horizontal. Artikel Ilmiah*. Salatiga: Universitas Kristen Satya Wacana Salatiga.

Munir, Rinaldi. 2006. *Diktat Kuliah IF 2153 Matematika Diskrit*, Edisi Keempat. Departemen Teknik Informatika, Institut Teknologi Bandung.

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

Shona, Khoirul F., 2017. *Security In All Platform Keamanan Data*. Semarang: Universitas Katolik Soegijapranata.

RIWAYAT HIDUP

Luqman El Hakim lahir di Pasuruan pada tanggal 5 Desember 1993, kebanyakan orang memanggilnya Luqman. Untuk teman SMP hingga SMA lebih mengenalnya dengan sebutan "gendut". Tinggal di daerah perumahan yaitu di Perum Keboncandi Permai Blok F-9 RT.02 RW.12 Desa Karangsentul Kecamatan Gondangwetan Kabupaten Pasuruan, merupakan anak pertama dari dua bersaudara dari pasangan bapak Hajali dan ibu Nadia Choirijjah. Awal pendidikan formalnya dimulai di TK Al Kautsar yang ada di Kota Pasuruan. Pendidikan dasarnya ditempuh selama enam tahun di SD Al Kautsar yang lulus pada tahun 2006. Setelah itu melanjutkan pendidikannya di SMP Negeri 5 Pasuruan selama tiga tahun yang lulus pada tahun 2009. Kemudian dia melanjutkan ke SMA Negeri 1 Gondangwetan yang ada di Kabupaten Pasuruan dan lulus pada tahun 2012. Setelah lulus dari bangku SMA, pendidikannya berlanjut di luar kota yaitu Kota Malang untuk menimba ilmu di Universitas Islam Negeri Maulana Malik Ibrahim Malang dengan mengambil program studi matematika.

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

BUKTI KONSULTASI SKRIPSI

Nama : Luqman El Hakim
NIM : 12610046
Fakultas/Jurusan : Sains dan Teknologi/Matematika
Judul Skripsi : Proses Enkripsi Dan Dekripsi Dengan Menggunakan Metode Super Enkripsi
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Evawati Alisah, M.Pd

No	Tanggal	Hal	Tanda Tangan	
1.	12 Maret 2019	Konsultasi Bab I dan Bab II	1.	
2.	21 Maret 2019	Revisi Bab I dan Bab II		2.
3.	2 April 2019	Konsultasi Agama Bab I dan Bab II	3.	
4.	13 Mei 2019	ACC Bab I, Bab II, Bab III, dan Konsultasi Bab IV		4.
5.	13 Mei 2019	ACC Agama Bab I dan Bab II	5.	
6.	13 Mei 2019	Revisi Bab II dan Bab III		6.
7.	13 Mei 2019	Revisi Agama Keseluruhan	7.	
8.	24 Mei 2019	ACC Bab IV		8.
9.	24 Mei 2019	ACC Agama Keseluruhan	9.	
10.	24 Mei 2019	ACC Keseluruhan		10.

Malang, 24 Mei 2019
Mengetahui,
Ketua Jurusan Matematika

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