

**PENYANDIAN MODEL KRIPTOGRAFI *PLAYFAIR CIPHER* DENGAN
MENGUNAKAN METODE *SHIFTR*OWS**

SKRIPSI

**OLEH
MUHAMMAD KARIM AMRULLOH
NIM. 14610061**



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

**PENYANDIAN MODEL KRIPTOGRAFI *PLAYFAIR CIPHER* DENGAN
MENGUNAKAN METODE *SHIFTRAWS***

SKRIPSI

**Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Matematika (S.Mat)**

**Oleh
MUHAMMAD KARIM AMRULLOH
NIM. 14610061**

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

**PENYANDIAN MODEL KRIPTOGRAFI *PLAYFAIR CIPHER* DENGAN
MENGUNAKAN METODE *SHIFROWS***

SKRIPSI

Oleh
MUHAMMAD KARIM AMRULLOH
NIM. 14610061

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 3 Mei 2021

Pembimbing I,



Muhammad Khudzaifah, M.Si
NIP. 19901511 20160801 1 057

Pembimbing II,



Mohammad Nafie Jauhari, M.Si
NIP. 19870218 20160801 1 056

Mengetahui,
Ketua Program Studi Matematika



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

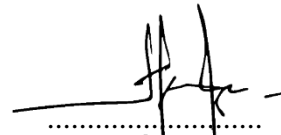
**PENYANDIAN MODEL KRIPTOGRAFI *PLAYFAIR* CIPHER DENGAN
MENGUNAKAN METODE *SHIFTR*OWS**

SKRIPSI

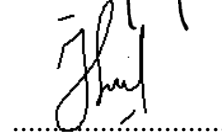
Oleh
MUHAMMAD KARIM AMRULLOH
NIM. 14610061

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Sains (S.Mat)
Tanggal 12 Juni 2021

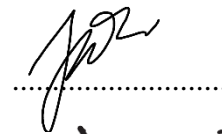
Penguji Utama : Dr. Hairur Rahman, M.Si



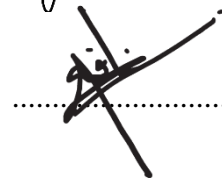
Ketua Penguji : Juhari, M.Si



Sekretaris Penguji : Muhammad Khudzaifah, M. Si



Anggota Penguji : Mohammad Nafie Jauhari, M. Si



Mengetahui,
Ketua Program Studi Matematika



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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Muhammad Karim Amrulloh

NIM : 14610061

Jurusan : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Penyandian Model Kriptografi Playfair Cipher dengan
Menggunakan Metode Shiftrows

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

Malang, 3 Mei 2021
Yang membuat pernyataan,



Muhammad Karim Amrulloh
NIM. 14610061

MOTO

فَإِنَّ مَعَ الْعُسْرِ يُسْرًا

"Karena sesungguhnya sesudah kesulitan itu ada kemudahan" (Al-Insyirah/94:5)

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk abi Muhammad Shobari yang telah mengajarkan kemandirian dan rasa bertanggung jawab. Ummi Aliatul Munafaqoh yang senantiasa dengan ikhlas selalu mendoakan dan mencurahkan kasih sayang serta mengajarkan kedisiplinan, ketaatan dan memberikan motivasi kepada penulis. Kakak Muhammad Amiruddin Lathif dan adik-adik Muhammad Abdullah Munir, Muhammad Abdul Hamid Abror dan juga Muhammad Nafi'uddin lathif yang selalu memberikan dukungan serta semangat kepada penulis.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji dan syukur atas segala nikmat dan rahmat dari Allah SWT yang telah menciptakan makhluk-Nya dengan bentuk yang paling sempurna. Dan tidak lupa penulis haturkan sholawat serta salam kepada junjungan nabi agung Muhammad SAW yang menjadi suri tauladan bagi umat islam hingga akhir zaman.

Rasa syukur atas segala maunah dan ridla dari Allah SWT akhirnya penulis mampu menyelesaikan penulisan skripsi ini dengan judul “Penyandian Model Kriptografi *Playfair Cipher* dengan Menggunakan Metode *ShiftRows*” 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 tak pernah lepas akan jasa para pembimbing serta arahan dari berbagai pihak. Untuk itu ucapan terima kasih penulis ucapkan sebesar-besarnya kepada semua pihak yang telah membantu dalam menyelesaikan penyusunan skripsi ini karena tanpa bantuannya penulis tidak akan dapat menyelesaikannya. Untuk itu ucapan terima kasih yang sebesar-besarnya 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. Muhammad Khudzaifah, M.Si, selaku dosen pembimbing matematika yang telah memberikan arahan, nasihat, dan motivasi kepada penulis.
5. Mohammad Nafie Jauhari, M.Si, selaku dosen pembimbing keagamaan yang telah memberikan bimbingan kepada penulis.
6. Dr. Hairur Rahman, M.Si, selaku dosen penguji I yang telah memberikan kritik dan saran yang membangun kepada penulis.
7. Juhari, M.Si, selaku dosen penguji II yang telah memberikan arahan perbaikan dalam penulisan skripsi kepada penulis.
8. Segenap sivitas akademika Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang terutama seluruh dosen, terima kasih atas segala ilmu dan bimbingannya.
9. Kedua orang tua dan seluruh keluarga penulis yang tak pernah lelah memberikan semangat dan mendoakan keberhasilan penulis.
10. Seluruh teman-teman mahasiswa di Jurusan Matematika angkatan 2014 yang telah memberikan motivasi dan pengalaman berharganya kepada penulis.
11. Semua pihak yang ikut membantu dalam menyelesaikan skripsi ini baik secara moril maupun materiil.

Semoga Allah Swt melimpahkan rahmat dan karunia-Nya kepada kita semua dan semoga skripsi ini bermanfaat bagi penulis dan pembaca.

Wassalamu 'alaikum Warahmatullahi Wabarakatuh

Malang, 3 Mei 2021

Penulis

DAFTAR ISI

HALAMAN JUDUL	
HALAMAN PENGAJUAN	
HALAMAN PERSETUJUAN	
HALAMAN PENGESAHAN	
PERNYATAAN KEASLIAN TULISAN	
HALAMAN MOTO	
HALAMAN PERSEMBAHAN	
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL	xii
DAFTAR GAMBAR.....	xiii
ABSTRAK	xiv
ABSTRACT.....	xv
ملخص	xvi

BAB I PENDAHULUAN

1.1	Latar Belakang.....	1
1.2	Rumusan Masalah	4
1.3	Tujuan Penelitian.....	4
1.4	Manfaat Penelitian	4
1.5	Batasan Masalah.....	5
1.6	Metode Penelitian.....	5
1.7	Sistematika Penulisan	6

BAB II KAJIAN PUSTAKA

2.1	Permutasi.....	7
2.1.1	Definisi Permutasi.....	7
2.1.2	Permutasi Melingkar	7
2.2	Kriptografi.....	7
2.2.1	Definisi Kriptografi.....	7
2.2.2	Sejarah Kriptografi	8
2.2.3	Komponen Kriptografi.....	9
2.2.4	Macam-macam Algoritma Kriptografi	10
2.2.4.1	Kriptografi Simetri	11

2.2.4.2	Kriptografi Asimetri.....	11
2.2.4.3	Fungsi Hash.....	12
2.2.5	Kriptografi Klasik.....	13
2.2.6	Kriptografi Modern.....	13
2.2.7	Super Enkripsi.....	13
2.3	<i>Playfair Cipher</i>	14
2.4	Notasi Heksadesimal	20
2.5	Transformasi <i>ShiftRows</i>	22

BAB III PEMBAHASAN

3.1	Implementasi Proses Enkripsi <i>Playfair Cipher</i> dengan Metode <i>ShiftRows</i>	24
3.2	Implementasi Proses Dekripsi <i>Playfair Cipher</i> dengan Metode <i>ShiftRows</i>	27
3.3	Kajian Agama	30

BAB IV PENUTUP

4.1	Kesimpulan	34
4.2	Saran	34

DAFTAR RUJUKAN	35
-----------------------------	-----------

DAFTAR TABEL

Tabel 2.1	Contoh kunci Playfair Cipher.....	15
Tabel 2.2	Kunci Playfair Cipher.....	16
Tabel 2.3	Notasi Heksadesimal	20

DAFTAR GAMBAR

Gambar 2.1	Proses dan komponen kriptografi	9
Gambar 2.2	Contoh enkripsi bigram pada yang kolom yang sama	17
Gambar 2.3	Contoh enkripsi bigram yang tidak pada baris dan kolom yang sama	18
Gambar 2.4	Contoh dekripsi bigram pada yang kolom yang sama	19
Gambar 2.5	Contoh dekripsi bigram yang tidak pada baris dan kolom yang sama	19
Gambar 2.6	Proses <i>ShiftRows</i>	23

ABSTRAK

Amrulloh, Muhammad Karim. 2021. **Penyandian Model Kriptografi *Playfair Cipher* dengan Menggunakan Metode *ShiftRows***. Skripsi. Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing (I): Muhammad Khudzaifah, M.Si, Pembimbing (II): M. Nafie Jauhari, M.Si.

Kata Kunci: Enkripsi, Dekripsi, *Playfair Cipher*, *ShiftRows*, Kriptografi

Dalam menyampaikan sebuah pesan agar isi pesan tersebut tidak diakses oleh pihak ketiga dibutuhkan suatu teknik kriptografi. Kriptografi adalah ilmu yang membahas teknik di mana sebuah teks diacak menggunakan kunci enkripsi menjadi sesuatu yang sulit dipahami oleh orang yang tidak memiliki kunci dekripsi. Namun kriptografi klasik sendiri sangatlah beresiko jika tidak dikombinasikan dengan algoritma yang lain. Sehingga dalam hal ini digunakan sebuah kriptografi dengan super enkripsi yang terdiri dari kombinasi *cipher* substitusi yaitu algoritma *playfair cipher* dan *cipher* transposisi yaitu algoritma *shiftrows*.

Berdasarkan penelitian ini dapat disimpulkan bahwa keamanan proses enkripsi dan dekripsi pesan pada algoritma *playfair cipher* dengan menggunakan metode *shiftrows* ini terletak pada keamanan dua tahap, yaitu pesan plainteks di proses dengan *playfair cipher*. Hasil tersebut kemudian ditransposisikan dengan menggunakan *shiftrows* sehingga pesan kode *playfair cipher* akan memiliki keamanan yang kuat dan lebih sulit untuk dipecahkan.

ABSTRACT

Amrulloh, Muhammad Karim. 2021. **On the Encryption Playfair Cipher Cryptography Model Using ShiftRows Method**. Thesis. Department of Mathematics, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University of Malang. Advisor (I): Muhammad Khudzaifah, M.Si, Advisor (II): M. Nafie Jauhari, M.Si.

Keywords: Encryption, Decryption, Playfair Cipher, ShiftRows, Cryptography

In sending a message so that the contents of the message are not accessed by third parties, a cryptography is needed. Cryptography is the science of techniques where a text is scrambled using an encryption key into something that is difficult for people who do not have the decryption key to understand. However, classical cryptography itself is very risky if it is not combined with other algorithms. So in this case, a cryptography with super encryption is used which consists of a combination of substitution ciphers, namely the Playfair cipher algorithm and a transposition cipher, namely the shiftrows algorithm.

Based on this research, it can be concluded that the security of the message encryption and decryption process in the playfair cipher algorithm using the shiftrows method lies in the security of two stages, namely the plaintext message is processed with the playfair cipher. The results are then transposed using shiftrows so that the playfair cipher code message will have strong security and be more difficult to crack.

ملخص

امر الله، محمد كريم. 2021. ترميز نموذج تشفير *Playfair* باستخدام طريقة *ShiftRows*. بحث جامعي. شعبة الرياضيات، كلية العلوم والتكنولوجيا جامعة مولانا مالك إبراهيم الإسلامية الحكومية بمالانج. المشرف الأول (1)، محمد حذيفة الماجستير، المشرف الثاني (2)، محمد نافع جوهرى، الماجستير.

الكلمات الرئيسية: التشفير ، فك التشفير ، تشفير *Playfair* ، *ShiftRows*، التشفير

عند نقل رسالة بحيث لا يتم الوصول إلى محتويات الرسالة من لا يعرف الطرف الثالث، هناك حاجة إلى تقنية تشفير. علم التشفير هو علم يتعامل مع التقنيات التي يتم فيها خلط النص باستخدام مفتاح تشفير في شيء يصعب على الأشخاص الذين ليس لديهم مفتاح فك التشفير فهمه. ومع ذلك ، فإن التشفير الكلاسيكي نفسه يمثل مخاطرة كبيرة إذا لم يتم دمجها مع خوارزميات أخرى. لذلك في هذه الحالة ، يتم استخدام التشفير مع التشفير الفائق والذي يتكون من مجموعة من الأصفار البديلة ، وهي خوارزمية تشفير *Playfair* وشفرة التحويل ، وهي خوارزمية *shiftrows*.

بناءً على هذا البحث ، يمكن الاستنتاج لأمن عملية تشفير الرسائل وفك تشفيرها في خوارزمية تشفير *playfair* باستخدام طريقة *shiftrows* يكمن في أمان مرحلتين ، وهما معالجة رسالة النص العادي باستخدام تشفير *playfair*. ثم يتم نقل النتائج باستخدام *shiftrows* بحيث تتمتع رسالة شفرة *playfair* بأمان قوي ويصعب اختراقها.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Berkomunikasi satu sama lain merupakan salah satu sifat dasar manusia sejak ada dimuka bumi ini. Bagi manusia, komunikasi berfungsi sebagai sarana untuk saling memahami satu sama lain. Cara manusia berkomunikasi dari zaman dahulu sampai sekarang terus mengalami perkembangan. Salah satu sarana komunikasi manusia adalah tulisan. Sebuah tulisan berfungsi untuk menyampaikan pesan kepada pembacanya. Pesan itu sendiri merupakan suatu informasi yang dapat dibaca dan dimengerti maknanya (Ariyus, 2008:1).

Ada kalanya suatu pesan bisa bersifat rahasia dan hanya ditujukan pada suatu pihak tertentu. Untuk menjaga keamanan pesan yang bersifat rahasia tersebut. Maka diperlukan suatu sistem yang dapat menyandikan pesan tersebut dan untuk membaca pesan tersebut diperlukan kunci khusus yang hanya diketahui oleh pengirim dan penerima pesan tersebut. Hal tersebut dilakukan agar pesan hanya tersampaikan kepada yang berhak. Seperti yang dijelaskan dalam Al-Qur'an surat an-Nisa' ayat 58 yang berbunyi:

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’/4:58).

Salah satu cara untuk memberikan pengamanan pada pesan teks adalah dengan kriptografi. Ilmu dan seni untuk menjaga kerahasiaan informasi bisa juga disebut dengan pengertian kriptografi secara umum (Schneier, 1996).

Kriptografi yaitu ilmu mengenai teknik enkripsi dimana data diacak menggunakan kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi sehingga mendapatkan data yang asli. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter. Biasanya algoritma tidak dirahasiakan, bahkan enkripsi mengandalkan kerahasiaan algoritma dianggap sesuatu yang tidak baik. Rahasia terletak di beberapa parameter yang menentukan kunci dekripsi itulah yang harus dirahasiakan (parameter menjadi ekuivalen dengan kunci) (Sentot, 2010:5).

Polygram substitution cipher merupakan salah satu metode yang digolongkan dalam kriptografi klasik yang proses enkripsinya menggunakan pemrosesan dalam bentuk blok-blok yang sangat besar. Metode ini merupakan salah satu cara untuk mengatasi kelemahan metode kriptografi klasik lainnya yang mudah tertebak karena terdapat korespondensi satu-satu antara plainteks dengan cipherteks. Metode *polygram substitution cipher* diantaranya adalah *sandi hill cipher* dan *Playfair Cipher* (Setyaningsih, 2009:214).

Berdasarkan penelitian yang dilakukan oleh (Latifah dkk, 2017:1), kriptografi klasik masih tergolong lemah jika diterapkan sendiri-sendiri, akan tetapi lebih kuat jika digabung dengan metode klasik lainnya.

Playfair Cipher termasuk ke dalam kelompok *cipher substitusi polygram cipher*. *Playfair Cipher* melakukan substitusi secara bigram (kelompok yang terdiri

dari dua huruf). *Cipher* ini ditemukan oleh Sir Charles Wheatstone pada tahun 1854, namun dipromosikan oleh Baron Lyon Playfair sehingga nama yang diabadikan adalah nama yang terakhir ini. *Playfair Cipher* digunakan oleh tentara Inggris pada perang Boer (perang dunia I).

Cipher ini mengenkripsi pasangan huruf (bigram atau digraf) menjadi pasangan huruf pula, jadi bukan huruf tunggal seperti pada *cipher* klasik lainnya. Tujuannya adalah untuk membuat analisis frekuensi menjadi sangat sulit sebab frekuensi kemunculan huruf-huruf dalam cipherteks menjadi datar (*flat*). (Munir, 2019:155)

Namun, algoritma kriptografi klasik sendiri memiliki kekurangan. Jika suatu pesan hanya dirahasiakan dengan menggunakan salah satu algoritma saja misalnya *Playfair Cipher*, maka pesan tersebut belum bisa dikatakan aman. Karena algoritma *Playfair Cipher* mudah dipecahkan jika diterapkan sendiri. Maka, penelitian ini akan mengkombinasikan kriptografi *Playfair Cipher* dengan metode *ShiftRows*. Mengkombinasikan dua buah algoritma bertujuan untuk memberikan penyandian baru, sehingga cipherteks yang dihasilkan akan lebih sulit dipecahkan oleh kriptanalisis dibandingkan dengan yang hanya menggunakan satu metode.

Berdasarkan dari latar belakang diatas penulis melakukan penelitian yang berjudul "*Penyandian Model Kriptografi Playfair Cipher dengan Menggunakan Metode ShiftRows*".

1.2 Rumusan Masalah

Merujuk pada latar belakang, maka dapat dirumuskan masalah yang berkaitan dengan penjelasan diatas yaitu:

1. Bagaimana hasil dari proses enkripsi kriptografi model *Playfair Cipher* menggunakan metode *ShiftRows*?
2. Bagaimana hasil dari proses dekripsi kriptografi model *Playfair Cipher* menggunakan metode *ShiftRows*?

1.3 Tujuan Penelitian

Dari rumusan masalah yang telah dipaparkan diatas, maka tujuan penulisan skripsi ini adalah untuk:

1. Mengetahui hasil dari proses enkripsi kriptografi model *Playfair Cipher* menggunakan metode *ShiftRows*.
2. Mengetahui hasil dari proses dekripsi kriptografi model *Playfair Cipher* menggunakan metode *ShiftRows*.

1.4 Manfaat Penelitian

Berdasarkan tujuan penelitian, maka manfaat penelitian ini adalah untuk:

1. Mempermudah dalam mencari hasil dari proses enkripsi kriptografi model *Playfair Cipher* menggunakan metode *ShiftRows*.
2. Mempermudah dalam mencari hasil dari proses dekripsi kriptografi model *Playfair Cipher* menggunakan metode *ShiftRows*.

1.5 Batasan Masalah

Untuk memfokuskan pembahasan, maka penulis memberi Batasan sebagai berikut:

1. Pada proses penyandian kriptografi *playfair*, penulis menggunakan 25 huruf yang terdiri dari 26 huruf alfabet “A sampai “Z” dengan mengubah “J” menjadi “I”.
2. Untuk *ShiftRows* dibagi setiap 6 kolom.

1.6 Metode Penelitian

Informasi yang telah diperoleh dari berbagai literatur kemudian dianalisis dan diolah dalam bentuk laporan penelitian kepustakaan. Berikut akan dijelaskan langkah-langkah analisis adalah:

1. Mengetahui proses enkripsi *Playfair Cipher* dengan menggunakan metode *ShiftRows*.
 - a. Membuat plainteks/pesan rahasia.
 - b. Menyusun algoritma enkripsi *Playfair Cipher* dengan menggunakan metode *ShiftRows*.
 - c. menentukan tabel kunci enkripsi dari *Playfair Cipher*.
 - d. Memproses plainteks dengan mengubah huruf J menjadi I
 - e. Memproses teks dengan tabel kunci enkripsi dari *Playfair Cipher*.
 - f. Memproses teks dengan metode *ShiftRows* yang dibagi menjadi 6 kolom huruf sehingga didapatkan kode cipherteks.
2. Mengetahui proses dekripsi *Playfair Cipher* dengan menggunakan metode *ShiftRows*.

- a. Memasukkan cipherteks yang telah diketahui.
- b. memproses dengan invers *ShiftRows* yang dibagi menjadi 6 kolom huruf.
- c. memproses hasil teks dengan tabel kunci enkripsi dari *Playfair Cipher*.
- d. Didapatkan hasil plainteks.

1.7 Sistematika Penulisan

Untuk mempermudah dalam menulis skripsi ini penulis menggunakan sistematika penulisan lima bab dengan rumusan sebagai berikut:

Bab I Pendahuluan

Pendahuluan ini terdapat latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, metode penelitian, dan sistematika penulisan.

Bab II Kajian Pustaka

Bagian kajian pustaka ini terdiri dari teori-teori atau konsep-konsep yang dapat mendukung di dalam penelitian ini. Teori atau konsep tersebut meliputi konsep kriptografi, dan *Playfair Cipher*.

Bab III Pembahasan

Bagian pembahasan ini akan menjelaskan dan menguraikan secara keseluruhan langkah-langkah yang disebutkan dalam metode penelitian dan menjawab rumusan masalah.

Bab IV Penutup

Bagian ini berisi kesimpulan hasil pembahasan dan saran yang ingin disampaikan peneliti.

BAB II

KAJIAN PUSTAKA

2.1 Permutasi

2.1.1 Definisi Permutasi

Permutasi merupakan bentuk khusus aplikasi aturan perkalian. Misalkan jumlah objek adalah n . maka urutan pertama yang dipilih dari n objek, urutan kedua dipilih dari $n - 1$ objek, urutan ketiga dipilih dari $n - 2$ objek, begitu seterusnya, dan urutan terakhir dipilih dari 1 objek yang tersisa. Menurut kaidah perkalian, permutasi dari n objek adalah

$$n(n - 1)(n - 2) \dots (2)(1) = n! \text{ (Munir, 2012:238)}$$

2.1.2 Permutasi Melingkar

Permutasi Melingkar dari n objek adalah penyusunan objek-objek yang mengelilingi sebuah lingkaran (atau kurva tertutup sederhana). Jumlah susunan objek yang memngelilingi lingkaran adalah $(n - 1)!$.

Pembuktian permutasi melingkar cukup sederhana: objek pertama dapat ditempatkan dimana saja pada lingkaran dengan 1 cara. Sisa $n - 1$ objek lainnya dapat diatur searah jarum jam (misalnya) dengan $P(n - 1, n - 1) = (n - 1)!$ cara. (Munir, 2012:243)

2.2 Kriptografi

2.2.1 Definisi Kriptografi

Kriptografi berasal dari Bahasa Yunani yaitu “*cryptos*” artinya “*secret*” (rahasia) dan “*graphein*” artinya “*writing*” (tulisan). Jadi kriptografi secara harfiah

berarti “*secret writing*” (tulisan rahasia). (Munir, 2019:4)

Menurut (Santi, 2010:28) terdapat empat aspek yang harus terpenuhi dalam keamanan informasi yaitu aspek kerahasiaan (*confidentiality*), integritas data (*data integrity*), otentifikasi (*Authentication*), dan non-repudiiasi (*non-repudiation*).

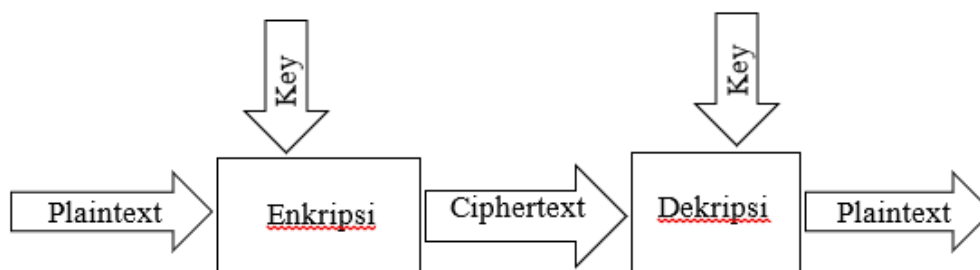
2.2.2 Sejarah Kriptografi

Kriptografi mempunyai sejarah yang sangat menarik dan Panjang.kriptografi sudah digunakan 4000 tahun yang lalu, diperkenalkan oleh orang-orang mesir lewat hieroglyph. Jenis tulisan ini buaknlah bentukstandar untuk menulis pesan. Dikisahkan, pada zaman romawi kuno, padasaat Julius Caesar ingin mengirimkan pesan rahasiakepada seorang jenderal dimedan perang pesan tersebut harus dikirimkan melalui seorang kurir. Karena pesan tersebut mengandung rahasia, Julius Caesar tidak ingin pesan rahasia tersebut sampai terbuka dijalan. Julius Caesar kemudian memikirkan bagaimana mengatasinya. Ia kemudian mengacak pesan tersebut sehingga menjadi suatu pesan yang tidak dapat dipahami oleh siapapun kecuali jenderalnya saja. Tentu sang jenderal telah diberitahu sebelumnya bagaimana cara membaca pesan teracak tersebut. Yang dilakukan Julius Caesar adalah mengganti semua susunan alfabet dari a,b, c, yaitu a menjadi d, b menjadi e,c menjadi f dan seterusnya. (Ariyus, 2008:13).

Dari ilustrasi tersebut, beberapa istilah kriptografi dipergunakan untuk menandai aktifitas-aktifitas rahasia dalam mengirim pesan. Apa yang dilakukan Julius Caesar yang mengacak pesan, disebut sebagai enkripsi. Pada saat sang jenderal merapikan pesan yang teracak itu, proses itu disebut dekripsi. Pesan awal

yang belum diacak dan pesan yang telah dirapikan, disebut *plaintext*, sedangkan pesan yang telah diacak disebut *ciphertext*. (Ariyus, 2008:14)

2.2.3 Komponen Kriptografi



Gambar 2.1 Proses dan komponen kriptografi

Definisi terminologi algoritma adalah urutan langkah-langkah logis untuk menyelesaikan masalah yang disusun secara sistematis. 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 diantaranya enkripsi, dekripsi ciphertexts, dan kriptanalisis. Enkripsi adalah hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaannya. Pesan-asli disebut plaintexts, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan cipher atau kode. Sama halnya dengan kita tidak mengerti akan sebuah kata makna maka kita akan melihatnya dalam kamus atau daftar istilah. Beda halnya dengan enkripsi, untuk mengubah teks-asli kedalam bentuk teks-kode kita menggunakan algoritma yang dapat mengkodekan data yang kita inginkan.

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 yang digunakan untuk enkripsi. Kunci yang dimaksud disini adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci rahasia (*private key*) dan kunci umum (*public key*).

Ciphertext merupakan suatu pesan yang telah melalui proses enkripsi. Pesan yang ada pada teks kode ini tidak bisa dibaca karena berupa karakter-karakter yang tidak mempunyai makna (arti). *Plaintext* sering juga disebut *cleartext*. Teks-asli atau pesan teks biasa ini merupakan pesan ditulis atau diketik yang memilikimakna. Teks asli inilah yang diproses menggunakan algoritma kriptografi untuk menjadi *ciphertext* (teks-kode).

Cryptanalysis bisa diartikan sebagai analisis kode atau suatu ilmu untuk mendapatkan teks asli tanpa harus mengetahui kunci yang sah secara wajar. Jika suatu teks-kode berhasil diubah menjadi teks-asli tanpa harus menggunakan kunci yang sah, proses tersebut dinamakan *breaking code*. Hal ini dilakukan oleh para kriptanalis. Analisis kode juga dapat menemukan kelemahan dari suatu algoritma kriptografi dan akhirnya dapat menemukan kunci teks atau teks-asli dari teks-kode yang dienkripsi dengan algoritma tertentu. (Ariyus, 2008:43).

2.2.4 Macam-macam Algoritma Kriptografi

Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan kunci yang dipakainya:

1. Algoritma Simetri (menggunakan satu kunci untuk enkripsi dan dekripsinya).
2. Algoritma Asimetri (menggunakan kunci yang berbeda untuk enkripsi dan dekripsi).

3. Hash Function. (Ariyus, 2008:44)

2.2.4.1 Algoritma Simetri

Algoritma ini sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi. Algoritma ini sudah ada sejak lebih dari 4000 tahun yang lalu. Bila mengirim pesan dengan menggunakan algoritma ini, si penerima pesan harus diberitahu kunci dari pesan tersebut agar bisa mendekripsikan pesan yang dikirim. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci. Jika kunci tersebut diketahui oleh orang lain maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan. Algoritma yang memakai kunci simetri diantaranya adalah:

1. Data Encryption Standard (DES),
2. RC2, RC4, RC, RC6,
3. International Data Encryption Algorithm (IDEA),
4. Advanced Encryption Standard (AES),
5. One Time Pad (OTP),
6. A5, dan lain sebagainya. (Ariyus, 2008:44)

2.2.4.2 Algoritma Asimetri

Algoritma asimetri sering juga disebut dengan algoritma kunci public, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu:

1. Kunci umum (*public key*): kunci yang boleh siapa orang tahu (dipublikasikan).

2. Kunci rahasia (*private key*): kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang).

Kunci-kunci tersebut berhubungan satu sama lain. Dengan kunci public orang dapat mengenkripsi tetapi tidak bias mendekripsinya. Hanya orang yang memiliki kunci rahasia yang dapat mendekripsi pesan tersebut. Algoritma asimetri bias mengirimkan pesan dengan lebih aman daripada algoritma simetri. Contoh, Bob mengirim pesan ke Alice menggunakan algoritma asimetri. Hal yang harus dilakukan Alice adalah:

1. Bob memberitahukan kunci publiknya ke Alice.
2. Alice mengenkripsi pesan dengan menggunakan kunci public dari Bob.
3. Bob mendekripsi pesan dari Alice dengan kunci rahasianya.
4. begitu juga sebaliknya jika Bob ingin mengirim pesan ke Alice.

Algoritma yang memakai kunci public diantaranya adalah:

1. Digital Signature Algorithm (DSA),
2. RSA,
3. Diffie-Hellman (DH),
4. Elliptic Curve Cryptography (ECC),
5. Kriptografi Quantum, dan lain sebagainya. (Ariyus, 2008:45)

2.2.4.3 Fungsi Hash

Fungsi Hash sering disebut dengan fungsi Hash satu arah (*one-way function*), *message digest*, *fingerprint*, fungsi komponen dan *message authentication code* (MAC), merupakan suatu fungsi matematika yang mengambil masukan Panjang variable dan mengubahnya ke dalam urutan biner

dengan panjang yang tetap. Fungsi hash biasanya diperlukan bila ingin membuat sidik jari dari suatu pesan. Sidik jari pada pesan merupakan suatu tanda bahwa pesan tersebut benar-benar berasal dari orang yang diinginkan. Tentang hal ini akan dibahas lebih lanjut pada bagian berikutnya. (Ariyus, 2008:46)

2.2.5 Kriptografi Klasik

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, 2008:46)

2.2.6 Kriptografi Modern

Kriptografi modern mempunyai kerumitan yang sangat kompleks karena dioperasikan menggunakan komputer. Hal ini akan dibahas lebih detail pada bagian lain. (Ariyus, 2008:46)

2.2.7 Super Enkripsi

Algoritma kriptografi memberikan keamanan namun tidak menjamin keamanan 100 persen, sehingga diajukan solusi yang dirancang untuk meningkatkan keamanan tersebut, melalui kombinasi penggunaan algoritma kriptografi yang berbeda untuk mengenkripsi pesan.

Multiple encryption, dimana salah satu contohnya adalah *double* enkripsi (super enkripsi) adalah proses enkripsi yang dilakukan sebanyak dua kali atau lebih. Pertama enkripsi *plaintext* menjadi *ciphertext*, kemudian enkripsi *ciphertext* itu, mungkin menggunakan *cipher* lain dan kunci.

Super enkripsi adalah salah satu kriptografi berbasis karakter yang menggabungkan *cipher* substitusi dan *cipher* transposisi. Hal tersebut bertujuan untuk mendapatkan *cipher* yang lebih kuat dari hanya menggunakan satu *cipher* saja, sehingga tidak mudah untuk dipecahkan. enkripsi dan dekripsi dapat dilakukan dengan urutan *cipher* substitusi kemudian *cipher* transposisi, atau sebaliknya. Super enkripsi dapat dilakukan dengan menggunakan kedua *cipher* tersebut secara berulang-ulang, namun pada makalah ini hanya akan dibahas mengenai proses enkripsi dan dekripsi satu kali dengan menggunakan *cipher* substitusi dan satu kali dengan menggunakan *cipher* transposisi.

2.3 Playfair Cipher

Playfair Cipher termasuk ke dalam kelompok *cipher* substitusi *polygram cipher*. *Playfair Cipher* melakukan substitusi secara bigram (kelompok yang terdiri dari dua huruf). *Cipher* ini ditemukan oleh Sir Charles Wheatstone pada tahun 1854, namun dipromosikan oleh Baron Lyon Playfair sehingga nama yang diabadikan adalah nama yang terakhir ini. *Playfair Cipher* digunakan oleh tentara Inggris pada perang Boer (perang dunia I).

Cipher ini mengenkripsi pasangan huruf (bigram atau digraf) menjadi pasangan huruf pula, jadi bukan huruf tunggal seperti pada *cipher* klasik lainnya.

Tujuannya adalah untuk membuat analisis frekuensi menjadi sangat sulit sebab frekuensi kemunculan huruf-huruf dalam cipherteks menjadi datar (*flat*).

Kunci enkripsinya adalah 25 buah huruf yang disusun dalam bujursangkar 5 x 5 dengan menghilangkan huruf J dari alfabet (dalam beberapa versi lain huruf I dan J ditulis sebagai I/J). Setiap elemen bujursangkar berisi huruf yang berbeda satu sama lain. Contoh sebuah bujursangkar (persegi) *playfair*:

Tabel 2.1 Contoh kunci *Playfair Cipher*

H	E	Z	K	D
Q	L	A	T	O
C	S	G	N	W
P	I	Y	R	F
V	U	B	X	M

Huruf-huruf di dalam bujur sangkar biasanya hasil permutasi huruf-huruf alfabet. Jumlah kemungkinan bujur sangkar yang dapat dibuat adalah sebanyak permutasi dari 25 alfabet, yaitu

$$25! = 25! = 15.511.210.043.330.985.984.000.000$$

Susunan huruf didalam bujursangkar juga dapat dipilih dari sebuah kalimat kunci yang mudah diingat, misalnya:

JALAN GANESHA SEPULUH

Buang huruf yang berulang dan huruf J jika ada:

ALNGESHPU

Kemudian tambahkan huruf-huruf alfabet lain yang belum ada (kecuali J):

ALNGESHPUBCDFIKMOQRTVWXYZ

Masukkan huruf-huruf di atas kedalam bujursangkar dari atas kebawah dan dari kiri kekanan sehingga membentuk bujursangkar *playfair* sebagai berikut:

Tabel 2.2 Kunci *Playfair Cipher*

A	L	N	G	E
S	H	P	U	B
C	D	F	I	K
M	O	Q	R	T
V	W	X	Y	Z

Sebelum melakukan enkripsi, pesan yang akan dienkrpsi diatur terlebih dahulu dengan aturan berikut:

1. Ganti huruf J (bila ada) dengan huruf I.
2. Tulis pesan dalam pasangan huruf (bigram).
3. Tidak boleh ada pasangan huruf yang sama. Jika ada, sisipkan X ditengahnya (atau huruf lain, misalnya Z).
4. Jika jumlah huruf ganjil, tambahkan huruf X pada bigram terakhir. (Munir, 2019:155)

Misalnya pada plainteks *temui ibu nanti malam* tidak ada huruf J, maka pesan langsung ditulis dalam pasangan huruf (bigram):

TE MU II BU NA NT IM AL AM

Karena ada pasangan huruf yang sama, yaitu II, maka tambahkan huruf X ditengahnya sehingga bigram menjadi:

TE MU IX IB UN AN TI MA LA MX

Menurut (Nurkifli, 2014:367) terdapat beberapa aturan dalam proses enkripsi maupun dekripsi pada *Playfair Cipher*. Berikut merupakan Langkah-langkah enkripsi dan dekripsi *Playfair Cipher*.

Algoritma enkripsi untuk *Playfair Cipher* adalah sebagai berikut:

1. Jika ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya.

2. Jika ada dua huruf terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf di bawahnya.
3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua.
4. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari huruf yang digunakan

Contoh: Plainteks temui ibu nanti malam telah ditulis dalam bigram kapital sebagai berikut: TE MU IX IB UN AN TI MA LA MX

Dan bujur sangkar playfair yang digunakan sama seperti tabel 2.2

Maka cipherteks yang dihasilkan adalah:

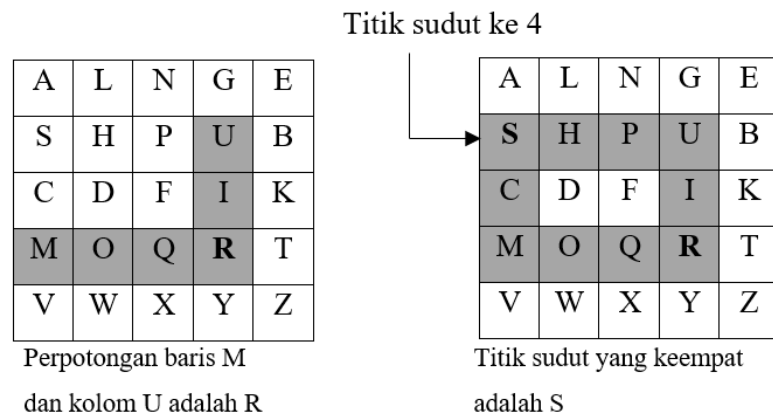
ZB RS FY KU PG LG RK VS NL QV

Penjelasannya adalah sebagai berikut: untuk bigram yang pertama, TE, huruf T dan E terletak pada satu kolom. maka huruf T diganti dengan huruf dibawahnya, Z, begitu juga huruf E diganti dengan huruf dibawahnya, B.

A	L	N	G	E	↻
S	H	P	U	B	
C	D	F	I	K	↻
M	O	Q	R	T	
V	W	X	Y	Z	

Gambar 2.2 Contoh enkripsi bigram pada yang kolom yang sama

Untuk bigram MU, karena tidak terletak pada satu baris atau satu kolom, maka cara enkripsinya ditunjukkan pada bujur sangkar berikut ini:



Gambar 2.3 Contoh enkripsi bigram yang tidak pada baris dan kolom yang sama. Perpotongan baris yang berisi M dengan kolom yang berisi U bertemu pada huruf R. sampai sini kita sudah mempunyai tiga titik sudut yang sudah terbentuk, yaitu M, U, dan R. Titik sudut keempat agar terbentuk persegi Panjang adalah S. Jadi, enkripsi terhadap bigram MU adalah RS. Untuk bigram yang lainnya caranya sama.

Algoritma dekripsi merupakan kebalikan dari algoritma enkripsi. Langkah-langkahnya adalah sebagai berikut:

1. Jika ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kirinya.
2. Jika ada dua huruf terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf di atasnya.
3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua.
4. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari huruf yang digunakan.

Contoh : Cipherteks zbrsfykupglgrkvsnlqv ditulis dalam bigraf kapital sebagai berikut : ZB RS FY KU PG LG RK VS NL QY

Dan bujursangkar playfair yang digunakan sama seperti pada Tabel 2.2

Maka teks yang dihasilkan adalah:

TE MU IX IB UN AN TI MA LA MX

Penjelasannya adalah sebagai berikut: untuk bigram yang pertama, ZB, huruf Z dan B terletak pada satu kolom. maka huruf Z diganti dengan huruf di atasnya, T, begitu juga huruf B diganti dengan huruf di atasnya, E.

A	L	N	G	E
S	H	P	U	B
C	D	F	I	K
M	O	Q	R	T
V	W	X	Y	Z

Gambar 2.4 Contoh dekripsi bigram pada yang kolom yang sama

Untuk bigram MU, karena tidak terletak pada satu baris atau satu kolom, maka cara enkripsinya ditunjukkan pada bujur sangkar berikut ini:

A	L	N	G	E
S	H	P	U	B
C	D	F	I	K
M	O	Q	R	T
V	W	X	Y	Z

Perpotongan baris R dan kolom S adalah M

A	L	N	G	E
S	H	P	U	B
C	D	F	I	K
M	O	Q	R	T
V	W	X	Y	Z

Titik sudut ke 4
Titik sudut yang keempat adalah U

Gambar 2.5 Contoh dekripsi bigram yang tidak pada baris dan kolom yang sama

Perpotongan baris yang berisi R dengan kolom yang berisi S bertemu pada huruf M. sampai sini kita sudah mempunyai tiga titik sudut yang sudah terbentuk, yaitu R, S, dan M. Titik sudut keempat agar terbentuk persegi Panjang adalah U. Jadi, enkripsi terhadap bigram RS adalah MU. Untuk bigram yang lainnya caranya sama.

Setelah itu buang huruf X yang tidak mengandung makna.

Plainteks yang dihasilkan TEMUI IBU NANTI MALAM

2.4 Notasi Heksadesimal

Menurut (Bryant & O'Hallaron. 2010:34) Satu byte terdiri dari 8 bit. Dalam notasi biner nilainya berkisar antara 00000000_2 hingga 11111111_2 . Jika dilihat sebagai bilangan bulat desimal, berkisar dari 0_{10} hingga 255_{10} . Tidak ada notasi yang sangat cocok untuk mendeskripsikan notasi bit. Notasi biner terlalu bertele-tele, sedangkan notasi desimal terlalu tidak menarik saat mengubah pola bit. Sebagai gantinya kita menulis pola bit sebagai basis 16, atau angka heksadesimal. Heksadesimal (atau sederhananya "hex") menggunakan angka 0 sampai 9 dan karakter A sampai F untuk mewakili 16 kemungkinan nilai. Gambar 2.6 menunjukkan nilai desimal dan biner dikaitkan dengan 16 digit heksadesimal, dalam heksadesimal, nilai satu byte berkisar dari 00_{16} hingga FF_{16} . Konstanta numerik yang dimulai dengan 0x atau 0X diinterpretasikan sebagai heksadesimal. Karakter "A" hingga "F" dapat ditulis huruf kapital ataupun huruf kecil.

Tabel 2.3 Notasi Heksadesimal

Hex digit	Decimal Value	Binary value
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101

E	14	1110
F	15	1111

Menurut (Bryant & O'Hallaron. 2010:36) mengonversi antara desimal dan heksadesimal dibutuhkan perkalian atau pembagian untuk menangani kasus umum. Untuk mengonversi desimal x ke heksadesimal, kita dapat berulang kali membagi x dengan 16, dengan ketentuan q adalah hasil bagi dan r adalah sisa, sebagaimana $x = q \cdot 16 + r$. Kemudian kita menggunakan representasi digit heksadesimal yang mewakili r dan kita lanjutkan proses yang sama dengan digit yang tersisa pada proses q . sebagai contoh, perhatikan konversi desimal 314156:

$$314156 = 19634 \cdot 16 + 12 \quad (C)$$

$$19634 = 1227 \cdot 16 + 2 \quad (2)$$

$$1227 = 76 \cdot 16 + 11 \quad (B)$$

$$76 = 6 \cdot 16 + 12 \quad (C)$$

$$4 = 0 \cdot 14 + 4 \quad (4)$$

Dari sini kita dapat membaca representasi heksadesimal sebagai 0x4CB2C.

Sebaliknya, untuk mengubah bilangan heksadesimal ke desimal kita dapat mengalikannya masing-masing digit heksadesimal dengan 16 pangkat n . misalnya, diberikan angka 0x7AF maka kita hitung desimalnya:

$$\begin{aligned} 7 \cdot 16^2 + 10 \cdot 16 + 5 &= 7 \cdot 256 + 10 \cdot 16 + 15 \\ &= 1792 + 160 + 15 \\ &= 1967 \end{aligned}$$

Maka disini kita dapatkan desimal dari 0x7AF adalah 1967

Untuk menghitung biner dengan desimal sendiri sebenarnya sama seperti proses diatas. Hanya saja karena biner adalah dua bilangan maka desimal x dibagi

berulang kali dengan 2. dengan ketentuan q adalah hasil bagi dan r adalah sisa, sebagaimana $x = q \cdot 2 + r$. Sebagai contoh perhatikan desimal 157:

$$157 = 75 \cdot 2 + 1 \quad (1)$$

$$75 = 32 \cdot 2 + 1 \quad (1)$$

$$32 = 16 \cdot 2 + 0 \quad (0)$$

$$16 = 8 \cdot 2 + 0 \quad (0)$$

$$8 = 4 \cdot 2 + 0 \quad (0)$$

$$4 = 2 \cdot 2 + 0 \quad (0)$$

$$2 = 1 \cdot 2 + 0 \quad (0)$$

$$1 = 0 \cdot 2 + 1 \quad (1)$$

Dari sini kita dapat membaca representasi biner sebagai 10000011

Sebaliknya, untuk mengubah bilangan biner ke desimal kita dapat mengalikannya masing-masing digit heksadesimal dengan 2 pangkat n . misalnya, diberikan angka 1001 maka kita hitung desimalnya:

$$\begin{aligned} 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 &= 1 \cdot 8 + 0 \cdot 4 + 0 \cdot 2 + 1 \cdot 1 \\ &= 8 + 1 \\ &= 9 \end{aligned}$$

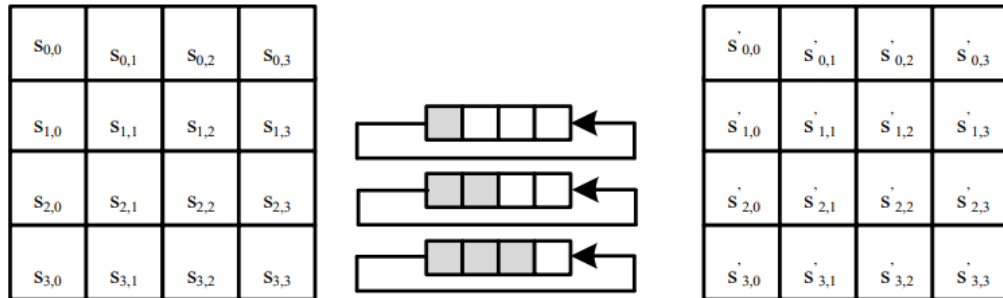
Maka disini kita dapatkan desimal dari 1001 adalah 9

2.5 Transformasi *ShiftRows*

Transformasi *ShiftRows*: beroperasi pada tiap baris dari tabel *state*. Proses ini bekerja dengan cara mengeser byte-byte pada 3 baris terakhir (baris 1, 2, dan 3) dengan jumlah perputaran bergantung pada jumlah baris dan tidak melebihi Nb , dengan nilai Nb adalah 4 word dapat dilihat pada tabel 1. Dimana *byte* pada baris

ke-1 akan digeser ke kiri sebanyak 1 kali, *byte* pada baris ke-2 akan digeser ke kiri sebanyak 2 kali, dan *byte* pada baris ke-3 akan digeser ke kiri sebanyak 3 kali.

Sedangkan baris 0 tidak mengalami pergeseran.(Pardosi dkk. 2015:138)



Gambar 2.6 Proses *ShiftRows*

Jadi pada transformasi *ShiftRows*, setiap dari baris bergeser kekiri dengan jumlah yang ditentukan. Nomor barisnya dimulai dari nol. Baris pertama tidak digeser sama sekali, baris berikutnya digeser satu dan berlaku seterusnya.

BAB III
PEMBAHASAN

3.1 Implementasi Proses Enkripsi *Playfair Cipher* dengan Metode *ShiftRows*

1. Dibuatlah plainteks

ISLAM ITU DIBANGUN DIATAS LIMA PERKARA YAITU SYAHADAT
SHALAT ZAKAT PUASA DAN HAJI

2. Diubahlah plainteks menjadi pasangan huruf (bigram)

IS LA MI TU DI BA NG UN DI AT AS LI MA PE RK AR AY AI TU SY AH
AD AT SH AL AT ZA KA TP UA SA DA NH AI IX

3. Ditentukanlah sebuah kunci enkripsi *Playfair Cipher*

RUKUN ISLAM

Maka didapat

RUKNISLAM

Dibentuklah tabel kunci

R	U	K	N	I
S	L	A	M	B
C	D	E	F	G
H	O	P	Q	T
V	W	X	Y	Z

4. Kemudian plainteks yang sudah diubah menjadi pasangan huruf (bigram)

diroses dengan menggunakan kunci enkripsi *Playfair Cipher* maka diperoleh hasil proses enkripsi berikut:

Plainteks: IS LA MI TU DI BA NG UN DI AT AS LI MA PE RK AR AY AI
TU SY AH AD AT SH AL AT ZA KA TP UA SA DA NH AI IX

Ciphertext: RB AM BN OI GU SM IF KI GU BP ML BU BM XP UN SK MX
BK OI MV SP LE BP CV MA BP XB AE HQ KL LM EL RQ BK KZ

5. Setelah itu kode cipherteks diproses dengan metode *ShiftRows* 6 kolom

Karena metode *ShiftRows* menggeser byte maka kode cipherteks disubstitusi kedalam basis heksadesimal berdasarkan tabel ASCII

KARAKTER	ASCII CODE	HEKSAD ESIMAL
A	65	41
B	66	42
C	67	43
D	68	44
E	69	45
F	70	46
G	71	47
H	72	48
I	73	49
J	74	4A
K	75	4B
L	76	4C
M	77	4D

N	78	4E
O	79	4F
P	80	50
Q	81	51
R	82	52
S	83	53
T	84	54
U	85	55
V	86	56
W	87	57
X	88	58
Y	89	59
Z	90	5A

Maka didapat

52	42	41	4D	42	4E
4F	49	47	55	53	4D
49	46	4B	49	47	55
42	50	4D	4C	42	55
42	4D	58	50	55	4E
53	4B	4D	58	42	4B
4F	49	4D	56	53	50
4C	45	42	50	43	56
4D	41	42	50	58	42
41	45	48	51	4B	4C
4C	4D	45	4C	52	51
42	4B	4B	5A	58	58

Selanjutnya diproses dengan metode *ShiftRows* dan diperoleh

52	42	41	4D	42	4E
49	47	55	53	4D	4F
4B	49	47	55	49	46
4C	42	55	42	50	4D
55	4E	42	4D	58	50
4B	53	4B	4D	58	42
4F	49	4D	56	53	50
45	42	50	43	56	4C

42	50	58	42	4D	41
51	4B	4C	41	45	48
52	51	4C	4D	45	4C
58	42	4B	4B	5A	58

Setelah itu substitusi kembali menggunakan tabel ASCII dan diperoleh suatu kode cipherteks

“RBAMBNIGUSMOKIGUIFLBUBPMUNBMXPKSKMXBOIMVSPEBPCV
LBPXBMAQKLAEHRQLMELXBKKZX”

3.2 Implementasi Proses Dekripsi *Playfair Cipher* dengan Metode *ShiftRows*

1. Didapatkan kode cipherteks

“RBAMBNIGUSMOKIGUIFLBUBPMUNBMXPKSKMXBOIMVSPEBPCV
LBPXBMAQKLAEHRQLMELXBKKZX”

2. Setelah itu kode cipherteks diproses dengan invers metode *ShiftRows* 6 kolom

Karena metode *ShiftRows* menggeser byte maka kode cipherteks disubstitusi kedalam basis heksadesimal berdasarkan tabel ASCII

KARAKTER	ASCII CODE	HEKSAD ESIMAL
A	65	41
B	66	42
C	67	43
D	68	44
E	69	45

F	70	46
G	71	47
H	72	48
I	73	49
J	74	4A
K	75	4B

L	76	4C
M	77	4D
N	78	4E
O	79	4F
P	80	50
Q	81	51
R	82	52
S	83	53

T	84	54
U	85	55
V	86	56
W	87	57
X	88	58
Y	89	59
Z	90	5A

Maka didapat

52	42	41	4D	42	4E
49	47	55	53	4D	4F
4B	49	47	55	49	46
4C	42	55	42	50	4D
55	4E	42	4D	58	50
4B	53	4B	4D	58	42
4F	49	4D	56	53	50
45	42	50	43	56	4C
42	50	58	42	4D	41
51	4B	4C	41	45	48
52	51	4C	4D	45	4C
58	42	4B	4B	5A	58

Selanjutnya diproses dengan invers metode *ShiftRows* dan diperoleh

52	42	41	4D	42	4E
4F	49	47	55	53	4D
49	46	4B	49	47	55
42	50	4D	4C	42	55
42	4D	58	50	55	4E
53	4B	4D	58	42	4B
4F	49	4D	56	53	50
4C	45	42	50	43	56
4D	41	42	50	58	42
41	45	48	51	4B	4C
4C	4D	45	4C	52	51
42	4B	4B	5A	58	58

Setelah itu substitusi kembali menggunakan tabel ASCII dan diperoleh suatu kode cipherteks

“RBAMBNOIGUSMIFKIGUBPMLBUBMXPUNSKMXXBKOIMVSPLEBPC
VMABPXBAEHQKLLMELRQBKKZ”

3. Kemudian diubah menjadi pasangan huruf (bigram)

RB AM BN OI GU SM IF KI GU BP ML BU BM XP UN SK MX BK OI MV
SP LE BP CV MA BP XB AE HQ KL LM EL RQ BK KZ

4. Ditentukanlah sebuah kunci dekripsi *Playfair Cipher*

RUKUN ISLAM

Maka didapat

RUKNISLAM

Dibentuklah tabel kunci

R	U	K	N	I
S	L	A	M	B
C	D	E	F	G
H	O	P	Q	T
V	W	X	Y	Z

5. Kemudian hasil diproses kembali dengan menggunakan kunci *Playfair Cipher*

Cipherteks: RB AM BN OI GU SM IF KI GU BP ML BU BM XP UN SK MX

BK OI MV SP LE BP CV MA BP XB AE HQ KL LM EL RQ BK KZ

Plainteks: IS LA MI TU DI BA NG UN DI AT AS LI MA PE RK AR AY AI

TU SY AH AD AT SH AL AT ZA KA TP UA SA DA NH AI IX

6. Kemudian buang huruf X yang tidak mempunyai makna dan kembalikan huruf I yang sebenarnya J.

Maka diperoleh kembali kode plainteks

ISLAM ITU DIBANGUN DIATAS LIMA PERKARA YAITU SYAHADAT

SHALAT ZAKAT PUASA DAN HAJI

3.3 Kajian Agama

Penelitian ini membahas tentang penyandian kata, penyandian biasanya digunakan untuk menyandikan data-data guna untuk menyimpan data yang bersifat rahasia, yang tidak semua orang berhak mengetahui, ilmu matematika yang membahas tentang penyandian sering disebut dengan kriptografi. Kriptografi ini

yang menyandikan teks asli menjadi teks kode berupa teks yang tidak bisa dibaca atau acak.

Begitu juga semua manusia punya sesuatu yang disembunyikannya, apakah yang disembunyikan itu berupa hal positif seperti perbuatan baik, tekad untuk melakukan sesuatu, cita-cita, harapan ataupun yang negatif seperti perbuatan dosa dan maksiat, hal tersebut disebut dengan rahasia. Rahasia yang disimpan manusia bisa saja hanya berkaitan dengan kepentingan pribadi dan keluarga, teman, dan mungkin rahasia negara. Bahkan Allah Swt. sebagai Khaliq juga menentukan nasib hamba-Nya tanpa diketahui oleh yang lain, semua menjadi rahasia Allah Swt.

Dari pernyataan di atas bahwa semua hal yang bersifat rahasia itu harus disimpan baik-baik agar tidak semua orang yang tidak berhak mengetahui menjadi mengetahui. Islam juga menganjurkan untuk menyimpan rahasia, yang dijelaskan dalam al-Quran surat al-Anfal ayat 27 yang berbunyi:

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَخُونُوا اللَّهَ وَالرَّسُولَ وَتَخُونُوا أَمَانَاتِكُمْ وَأَنْتُمْ تَعْلَمُونَ

“Wahai orang-orang yang beriman! Janganlah kamu mengkhianati Allah dan Rasul dan (juga) janganlah kamu mengkhianati amanat yang dipercayakan kepadamu, sedang kamu mengetahui.” (QS. al-Anfal/8:27).

Di dalam tafsir Ibnu Katsir dijelaskan bahwa Allah SWT memerintahkan agar amanat-amanat itu disampaikan kepada yang berhak menerimanya. Di dalam hadits al-Hasan, dari Samurah, disebutkan bahwa Rasulullah SAW bersabda:

أَدِّ الْأَمَانَةَ إِلَى مَنِ اسْتَمَنَّكَ، وَلَا تَخُنْ مَنْ خَانَكَ

“Sampaikanlah amanat itu kepada orang yang mempercayaimu, dan janganlah kamu berkhianat terhadap orang yang berkhianat kepadamu.” (H.R. Tirmidzi)

Islam juga mewajibkan setiap mukmin untuk memiliki hati dan jiwa yang kuat, dengan hati yang kuat, semua hak Allah SWT dan hak manusia dapat

dipelihara dengan baik, dan segala tindakan dapat dijauhkan dari sikap lalai. Inilah sebabnya mengapa Islam mewajibkan setiap Muslim untuk memiliki sifat dapat dipercaya (amanah). Makna dan kandungan amanah dalam Islam sangat luas, semua makna dan kandungan tertuju pada satu pemahaman, yaitu setiap orang merasakan bahwa Allah SWT menyertainya dalam setiap urusan yang ditugaskan kepadanya. Dan setiap orang memahami dengan baik jika mereka kelak akan diminta pertanggung jawaban atas apa yang mereka lakukan.

Pada saat yang sama, pemahaman umum tentang kepercayaan sering ditempatkan pada pemahaman yang sempit, terbatas pada pemeliharaan barang, meskipun maknanya jauh lebih besar dari yang diduga. Amanah yang penulis maksud di sini adalah amanah dalam arti luas, yaitu tanggung jawab manusia, yang bukan hanya tanggung jawab kepada Allah yang menciptakannya, tetapi juga tanggung jawab kepada sesama makhluk. Amanah adalah segala sesuatu yang dilakukan manusia, baik itu urusan agama maupun urusan dunia, yang berkaitan dengan perkataan dan perbuatan, dan puncak amanah adalah penjagaan dan pelaksanaan. Selain ayat Al-Quran dan hadits diatas juga ada hadist Rasulullah shallallahu ‘alaihi wa sallam bersabda:

الرَّجُلُ إِذَا حَدَّثَ الرَّجُلَ بِحَدِيثٍ ثُمَّ التَّفَتَ عَنْهُ فَهِيَ أَمَانَةٌ

“Jika seseorang mengabarkan kepada orang lain suatu kabar, kemudian ia berpaling dari orang yang dikabari tersebut maka kabar itu adalah amanah (atas orang yang dikabari)”. (HR At-Tirmidzi (1959) dan Abu Dawud (4868). Hadits ini dihasankan oleh Syaikh al-Albani dalam as-Shahihah (1090)).

Makna berpaling yaitu si penyampai kabar tatkala hendak menyampaikan kabarnya menengok ke kanan dan ke kiri karena khawatir ada yang mendengar. Sikapnya memandangi ke kanan dan ke kiri menunjukkan bahwa dia takut kalau ada orang lain yang ikut mendengar pembicaraannya, dan dia menghususkan kabar ini

hanya kepada yang akan disampaikan kabar tersebut. Seakan-akan dengan sikapnya itu ia berkata kepada orang yang diajak bicara, “Rahasiakanlah kabar ini!” (Lihat Tuhfatul Ahwadzi (VI/81) dan ‘Aunul Ma’bud (XIII/178).

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan hasil analisis yang telah dilakukan, maka dapat disimpulkan bahwa:

1. Proses enkripsi dengan menggunakan metode *Playfair Cipher* dengan menggunakan kunci yang telah ditentukan diproses enkripsinya, kemudian hasil enkripsi tersebut diproses enkripsi lagi dengan metode *ShiftRows* yang dibagi setiap 6 kolom dengan menggeser bertingkat setiap bertambahnya baris.
2. Proses dekripsi dengan menggunakan invers dari *Shiftrows* yang dibagi 6 kolom diproses dekripsinya, kemudian didekripsi lagi dengan menggunakan algoritma *Playfair Cipher* dengan kunci yang telah ditentukan.

4.2 Saran

Pada penelitian selanjutnya diharapkan yang akan dipertimbangkan untuk penyandian adalah algoritma lain yang bisa mendukung algoritma-algoritma yang ada di penelitian ini seperti model kriptografi *Hill Cipher*, *Vigenere Cipher*, *Myszkowski Cipher*, *One-time Pad Cipher*.

DAFTAR RUJUKAN

- Ariyus, Doni. 2008. *Pengantar Ilmu Kriptografi*, Bandung: Andi.
- Bryant, E. Randal dan David R. O'Hallaron. 2010. *Computer Systems: A Programmer's Perspective (2nd Edition)*, New Jersey: Prentice Hall.
- Latifah R, dkk. 2017. *Modifikasi Algoritma Caesar Cipher dan Rail Fence Untuk Peningkatan Keamanan Teks Alfanumerik dan Karakter Khusus*. Seminar Nasional Sains Dan Teknologi 2017.
- Munir, Rinaldi. 2019. *Kriptografi*, Bandung: Informatika Bandung.
- Nurkifli, E. H. 2014. *Modifikasi Algoritma Playfair dan Menggabungkan dengan Linear Feedback Shift Register (LFSR)*. Seminar Nasional Teknologi Informasi dan Komunikasi 2014.
- Pardosi I, dkk. 2015. *Aplikasi Penyembunyian Pesan pada Citra dengan Metode AES Kriptografi dan Enhanced LSB Steganografi*. ISSN. 1412-0100 Vol 16, No 2, Oktober 2015
- Santi, R. C. N. 2010. *Implementasi Algoritma Enkripsi Playfair pada File Teks*. Jurnal Teknologi Informasi DINAMIK.
- Schneier, Bruce. 1996. *Applied Cryptography, Second Edition*. New Jersey: John Wiley & Sons Inc.
- Sentot, Kromodimoeljo. 2010. *Teori & Aplikasi Kriptografi*. Jakarta: SPK IT Consulting.
- Setyaningsih, Emy. 2009. *Penyandian Citra Menggunakan Metode Playfair Cipher*. Yogyakarta: Volume 2 Nomor 2 Desember 2009.

RIWAYAT HIDUP



Muhammad Karim Amrulloh dilahirkan di Jombang pada hari Selasa tanggal 06 Februari 1996, merupakan anak kedua dari lima bersaudara, pasangan dari Bapak Muhammad Shobari dan Ibu Aliatul Munafaqoh. Pendidikan dasarnya ditempuh di Jombang di MIN Kauman Utara yang ditamatkan pada tahun 2008.

Pada tahun yang sama melanjutkan pendidikan menengah pertama di MTsN Tambakberas dan lulus pada tahun 2011. Kemudian melanjutkan pendidikan menengah atas di MAN Tambakberas dan menamatkan pendidikan tersebut pada tahun 2014. Pendidikan berikutnya ditempuh di Universitas Islam Negeri Maulana Malik Ibrahim Malang melalui jalur UM-PTAIN dengan mengambil Jurusan Matematika di Fakultas Sains dan Teknologi.



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 : Muhammad Karim Amrulloh
NIM : 14610061
Fakultas/Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Penyandian Model Kriptografi *Playfair Cipher* dengan Menggunakan Metode *ShiftRows*
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : M. Nafie Jauhari, M.Si

No	Tanggal	Hal	Tanda Tangan
1	19 Januari 2021	Konsultasi Bab I, Bab II	1.
2	19 Januari 2021	ACC Bab I, Bab II	2.
3	08 Maret 2021	Konsultasi Bab III	3.
4	16 Maret 2021	Revisi Bab III	4.
5	20 Maret 2021	ACC Bab III	5.
6	30 April 2021	Konsultasi Bab II, Bab III, Bab IV	6.
7	7 Mei 2021	ACC Bab II, Bab III, Bab IV	7.
8	13 Juni 2021	Konsultasi Keagamaan	8.
9	15 Juni 2021	ACC Keagamaan	9.
10	16 Juni 2021	ACC Keseluruhan	10.

Malang, 17 Juni 2021
Mengetahui,
Ketua Program Studi Matematika

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