# IMPLEMENTASI ALGORITMA CIPHER BLOCK CHAINING DAN TRANSPOSISI GRUP SIMETRI $S_4$ PADA PENGAMANAN PESAN TEKS

**SKRIPSI**

**OLEH**
**MARDIAH**
**NIM. 16610003**

**PROGRAM STUDI MATEMATIKA**
**FAKULTAS SAINS DAN TEKNOLOGI**
**UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM**
**MALANG**
**2022**

# IMPLEMENTASI ALGORITMA CIPHER BLOCK CHAINING DAN TRANSPOSISI GRUP SIMETRI $S_4$ PADA PENGAMANAN PESAN TEKS

**SKRIPSI**

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

**Oleh**
**MARDIAH**
**NIM. 16610003**

**PROGRAM STUDI MATEMATIKA**
**FAKULTAS SAINS DAN TEKNOLOGI**
**UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM**
**MALANG**
**2022**

# IMPLEMENTASI ALGORITMA CIPHER BLOCK CHAINING DAN TRANSPOSISI GRUP SIMETRI $S_4$ PADA PENGAMANAN PESAN TEKS

**SKRIPSI**

**Oleh**
**Mardiah**
**NIM. 16610003**

Telah Disetujui Untuk Diuji

Malang, 05 Oktober 2022

| Dosen Pembimbing I | Dosen Pembimbing II |
|---|---|
| Muhammad Khudzaifah, M.Si | Erna Herawati, M.Pd |
| NIDT. 19900511 20160801 1 057 | NIDT. 19760723 20180201 2 222 |

Mengetahui,
Ketua Program Studi Matematika

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

# IMPLEMENTASI ALGORITMA CIPHER BLOCK CHAINING DAN TRANSPOSISI GRUP SIMETRI $S_4$ PADA PENGAMANAN PESAN TEKS

**SKRIPSI**

**Oleh**
**Mardiah**
**NIM. 16610003**

Telah Dipertahankan di Depan Penguji Seminar Hasil Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Mengikuti Ujian Skripsi

Tanggal, 19 Oktober 2022

| | | |
|---|---|---|
| Ketua Penguji | : Prof. Dr. H. Turmudi, M.Si., Ph.D | ..... |
| Anggota Penguji I | : Dr. Heni Widayani, M.Si | ..... |
| Anggota Penguji II | : Muhammad Khudzaifah, M. Si | ..... |
| Anggota Penguji III | : Erna Herawati, M. Pd | ..... |

Mengetahui,
Ketua Program Studi Matematika

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

## PERSYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Mardiah

NIM : 16610003

Jurusan : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Implementasi Algoritma Cipher Block Chaining dan Transposisi Grup Simetri $S_4$ Pada Pengamanan Pesan Teks

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya sendiri, bukan merupakan pengambilan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali secara tertulis dikutip dalam naskah dan disebutkan dalam sumber kutipan atau daftar pustaka. Apabila dikemudian hari pernyataan hasil skripsi ini terbukti terdapat unsur penjiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 19 Oktober 2022

Yang membuat penyataan,


Mardiah

NIM. 16610003

## MOTO

***Bissmillahhirrohmanirrohim***

مَنْ جَدَّ وَجَدَ

مَنْ صَبَرَ ظَفِرَ

مَنْ سَارَ عَلىَ الدَّرْبِ وَصَلَ

***Alhamdulillah***

## PERSEMBAHAN

Dengan rasa syukur penulis persembahkan karya ini kepada:
Untuk orang-orang spesial, terkhusus bagi kedua orang tua penulis yaitu bapak H. Moh. Yunus dan ibu Hj. Sairah (Alm) tercinta yang senantiasa memberikan dukungan dan doa yang tiada hentinya demi keberhasilan penulis. Teruntuk ke dua saudara kandung penulis (Sulbiana, SE dan Mutmainnah, SH) yang juga senantiasa memberikan dukungan baik secara moril maupun materil saat proses mengerjakan skripsi ini.

# KATA PENGANTAR

*Assalamu'alaikum Warahmatullahi Wabarakatuh*

Segala puji dan syukur penulis panjatkan kepada kehadirat Allah Subhanahu Wa Ta'ala, yang telah memberikan nikmat berupa rahmat, taufiq serta hidayah-Nya sehingga penulis dapat menyelesaikan skripsi dengan sebaik-baiknya. Shalawat dan salam semoga senantiasa tercurahkan kepada Nabi Muhammad *Shallallhu 'Alaihi Wasallam*, para sahabat, keluarga dan pengikut-Nya yang taat kepada ajaran agama- Nya, yang telah rela berkorban untuk mengeluarkan manusia dari zaman jahiliyah menuju zaman yang diridhoi oleh Allah Subhanahu Wa Ta'ala yaitu ajaran agama islam.

Alhamdulillah berkat taufiq serta hidayah-Nya, penulis dapat menyelesaikan skripsi ini dengan judul "**Implementasi Algoritma Cipher Block Chaining dan Transposisi Grup Simetri $S_4$ pada Pengamanan Pesan Teks"**. Dalam proses penyelesaian skripsi ini penulis banyak mendapat bimbingan dan bantuan, serta saran dari berbagai pihak. Oleh karena itu penulis menyampaikan ucapan terima kasih kepada:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, S.Pd., M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Muhammad Khudzaifah, M.Si, selaku dosen pembimbing penulis yang telah memberikan banyak waktu, bimbingan, serta arahan selama perkuliahan hingga dapat terselesaikannya skripsi.
5. Erna Herawati, M.Pd, selaku dosen pembimbing Integrasi Sains dan Islam yang telah banyak meluangkan waktunya untuk membimbing penulis tentang sains dan perspektif agama Islam.
6. Prof. Dr. Turmudi, M.Si., Ph. D, selaku dosen wali dan selaku Ketua Penguji yang telah memberikan banyak bimbingan selama menempuh studi di Universitas Islam Negeri Maulana Malik Ibrahim Malang.

7. Dr. Heni Widayani, M.Si, selaku Anggota Penguji I dalam Ujian Skripsi.
8. Seluruh Dosen, Staff Administrasi Jurusan matematika, Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang yang telah memberikan ilmu serta pengalamannya kepada penulis selama studi.
9. Bapak H. Moh Yunus dan Ibu Hj. Sairah (Alm) tercinta yang telah mendidik sepenuh hati dan tidak lupa kepada saudara sosok kakak kandung Sulbiana dan Mutmainnah selalu mencurahkan kasih sayang dengan penuh perhatian, yang telah memberikan dukungan moril maupun spiritual hingga penulis dapat menyelesaikan penulisan skripsi ini.
10. Semua pihak yang terlibat dalam memberikan bantuan dan dukungan dalam menyelesaikan skripsi ini.

Semoga bantuan yang tulus dari berbagai pihak, mendapatkan imbalan yang setimpal dari Allah SWT. Dengan mengucap *Alhamdulillahirabbil 'alamin*, penulis berharap semoga skripsi ini dapat bermanfaat bagi penulis sendiri khususnya dan juga bagi para pembaca pada umumnya, untuk kemajuan ilmu pengetahuan dan pendidikan di masa depan.

*Wassalamualaikum Warahmatullahi Wabarakatuh*

Malang, 05 Oktober 2022

Penulis

## DAFTAR ISI

## DAFTAR TABEL

## DAFTAR GAMBAR

## DAFTAR SIMBOL

| | |
|---|---|
| $C_i$ | = *Ciphertext ke-i* |
| $P_i$ | = *Plaintext ke-i* |
| $E_k$ | = Kunci pada Enkripsi |
| $D_k$ | = Kunci pada Dekripsi |
| $IV$ | = *Initialization Vector* / $C_0$ |
| $S_n$ | = Grup Simetri |
| $N$ | = Banyaknya anggota himpunan yang dipermutasikan |
| $\circ$ | = Operasi Komposisi |
| $(G,*)$ | = Grup dengan Operasi Biner $*$ |
| $\oplus$ | = Operasi XOR |
| $K$ | = Kunci |
| $\|\sigma\|$ | = Orde dari suatu elemen $\sigma$ |

## DAFTAR LAMPIRAN

# ABSTRAK

Mardiah. 2022. **Implementasi Algoritma Cipher Block Chaining dan Transposisi Grup Simetri $S_4$ pada Pengaman Pesan Teks**. Skripsi. Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si. (II) Erna Herawati, M. Pd.

**Kata Kunci: Algoritma, Cipher Block Chaining, Transposisi Grup Simetri $S_4$**

Masalah keamanan informasi menjadi isu yang tidak ada habis-habisnya dibahas sejak dulu hingga zaman sekarang. Informasi yang bersifat rahasia, sensitif, atau bernilai tinggi dijaga keamanannya agar tidak dapat diakses oleh pihak-pihak yang tidak memiliki wewenang. Algoritma *Cipher Block Chaining* merupakan salah satu algoritma substitusi yang sulit dipecahkan. Bentuk umum *Cipher Block Chaining* bekerja dengan mode blok yaitu melakukan pengelompokkan biner-biner plainteks menjadi beberapa kelompok sesuai dengan ketentuan yang ditetapkan oleh pengguna. Grup simetri $S_4$ adalah grup semua permutasi dari empat elemen. Proses enkripsi dilakukan dengan algoritma *Cipher Block Chaining* dilanjutkan dengan algoritma transposisi grup simetri $S_4$ dan cara perhitungannya dilakukan dengan menggunakan protokol perjanjian kunci yang sudah disepakati. Sedangkan untuk proses dekripsi dilakukan dengan algoritma transposisi grup simetri $S_4$ lalu dilanjutkan dengan algoritma *Cipher Block Chaining* dan cara perhitungannya dengan menggunakan invers kunci yang sudah disepakati sebelumnya.

# ABSTRACT

Mardiah. 2022. **On Implementation of Cipher Block Chaining Algorithm and Symmetry Group Transposition $S_4$ for Message Text Security**. Thesis. Department of Mathematics, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University Malang. Supervisor: (I) Muhammad Khudzaifah, M.Sc. (II) Erna Herawati, M. Pd.

**Keyword : Algorithm, Cipher Block Chaining, Symmetry Group Transposition $S_4$**

The information security has become an issue that has been discussed endlessly since ancient times until today. Information that is confidential, sensitive, or of high value is safeguarded so that it cannot be accessed by unauthorized parties. Cipher Block Chaining Algorithm is a substitution algorithm that is difficult to solve. The general form of Cipher Block Chaining works in block mode, which is to group plaintext binaries into several groups according to the conditions set by the user. The symmetry group $S_4$ is the group of all permutations of the four elements. The encryption process is carried out with the Cipher Block Chaining algorithm followed by the $S_4$ symmetric group transposition algorithm and the calculation method is carried out using the agreed key agreement protocol. Meanwhile, the decryption process is carried out with the $S_4$ symmetric group transposition algorithm and then continued with the Cipher Block Chaining algorithm. The calculation method uses the previously agreed key inverse.

**مستخلص البحث**

مر ضيه . ٢٢. ٢. **تنفيذ خوارزمية التشفير Cipher Block Chaining وتبديل المجموعة المتماثل Transposisi Grup Simetri $S_4$ لأمن نص الرسائل**. قسم الرياضيات بكلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف (١): محمد خذيفة ، الماجستير. و المشرفة (٢)إرنا هيراواتي ، الماجستير.

**الكلمات الرئيسية : لخوارزمية, Cipher Block Chaining, Transposisi Grup Simetri $S_4$**

أصبحت قضية أمن المعلومات من القضايا التي تمت مناقشتها إلى ما لا نهاية منذ العصور القديمة وحتى اليوم. تتم حماية المعلومات السرية أو الحساسة أو ذات القيمة العالية بحيث لا يمكن الوصول إليها من قبل أطراف غير مصرح لها. تعد خوارزمية *Cipher Block Chaining* استبدال يصعب حلها. يعمل الشكل العام لتسلسل الكتل المشفرة في وضع الحظر ، وهو تجميع ثنائيات النص العادي في عدة مجموعات وفقًا للشروط التي يحددها المستخدم .مجموعة التناظر $Symmetry\ Group\ S_4$ هي مجموعة جميع تباديل العناصر الأربعة. يتم تنفيذ عملية التشفير باستخدام خوارزمية *Cipher Block Chaining* متبوعة بخوارزمية نقل المجموعة المتماثلة *Transposisi Grup Simetri* $S_4$ ويتم تنفيذ طريقة الحساب باستخدام بروتوكول اتفاقية المفتاح المتفق عليه. أما بالنسبة لعملية فك التشفير ، باستخدام خوارزمية *Transposisi Grup Simetri* $S_4$ متبوعة بخوارزمية نقل المجموعة المتماثلة *Cipher Block Chaining* وطريقة الحساب باستخدام عاكس المفتاح المتفق عليه مسبقًا.

# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Masalah keamanan informasi menjadi isu yang tidak ada habis-habisnya dibahas sejak dulu hingga zaman sekarang. Informasi yang bersifat rahasia, sensitif, atau bernilai tinggi dijaga keamanannya agar tidak dapat diakses oleh pihak-pihak yang tidak memiliki wewenang. Kita sudah sering mendengar kasus-kasus seperti penyadapan percakapan penting, kasus pembobolan atau keamanan informasi sensitif (misalnya data nasabah bank), kasus pencurian dokumen negara yang sangat rahasia, penyadapan surat-surat penting di kantor duta besar negara asing dan lain-lain (Munir, 2019).

Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan yang bersifat pribadi dan rahasia. 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 kriptografi. Untuk melakukan suatu proses penyandian dan proses pembalikan menggunakan algoritma yang sama (Munir, 2019).

Amanah adalah segala sesuatu baik bersifat materi maupun non-materi yang dipercayakan pemberi kepada penerima untuk selalu dijaga dan ditunaikan dengan

sebaik-baiknya. Dalam Al-Qur'an surah Al-Anfal(8):27, telah dijelaskan pentingnya menjaga amanah.

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَخُوْنُوا اللّٰهَ وَالرَّسُوْلَ وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ

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

Berdasarkan firman Allah SWT. dalam surat Al-Anfal ayat 27 dijelaskan bahwa "janganlah kamu menghianati amanah-amanah". Agama Islam memerintahkan bahwa amanah apapun merupakan hal penting yang perlu dijaga maka dapat diartikan bahwa sebuah pesan merupakan amanah yang perlu dijaga kerahasiaannya.

Sehubungan dengan ayat di atas, Rasulullah SAW juga memberi penjelasan atau keterangan dalam hadits yang diriwayatkan oleh Imam Bukhari yaitu sebagai berikut:

عَنْ أَبِي هُرَيْرَةَ رَضِيَ اللّٰهُ عَنْهُ قَالَ قَالَ رَسُولُ اللّٰهِ صَلّٰى اللّٰهُ عَلَيْهِ وَسَلَّمَ إِذَا ضُيِّعَتْ الْأَمَانَةُ فَانْتَظِرْ السَّاعَةَ قَالَ كَيْفَ إِضَاعَتُهَا يَا رَسُولَ اللّٰهِ قَالَ إِذَا أُسْنِدَ الْأَمْرُ إِلَى غَيْرِ أَهْلِهِ فَانْتَظِرْ السَّاعَةَ (رواه البخاري)

*Dari Abu Hurairah r.a mengatakan; Rasulullah shallallahu 'alaihi wasallam bersabda: "Jika amanat telah disia-siakan, tunggu saja kehancuran terjadi." Ada seorang sahabat bertanya; bagaimana maksud amanat disia-siakan? 'Nabi menjawab:"Jika urusan diserahkan bukan kepada ahlinya, maka tunggulah kehancuran itu." (H.R. Bukhâri)*

Hadits ini menjelaskan agar amanah dalam bentuk apapun tidak tersia-siakan perlu diadakan penelitian. Wasiatun (2016) telah meneliti grup simetri-$n$ pada algoritma pembentukan kunci. Penelitian tersebut melakukan proses enkripsi

dan dekripsi menggunakan teknik transposisi dengan menggunakan kunci yang telah disepakati melalui proses pembentukan kunci atas grup simetri-$n$.

*Cipher Block Chaining* (CBC) adalah salah satu pengembangan dari algoritma *Block Cipher*. Algoritma ini melakukan proses enkripsi dan dekripsi berdasarkan operasi XOR antara blok *plaintext* dengan cipher sebelumnya. Salah satu ciri utama dari CBC adalah setiap blok cipher selalu bergantung pada blok-blok sebelumnya. Kesalahn satu bit pada sebuah blok *plaintext* akan merambat pada blok *ciphertext* yang berkoresponden dan semua blok *ciphertext* berikutnya dan inilah yang menjadi kelemahan algoritma ini. Algoritma CBC juga memiliki kelebihan dimana setiap blok *ciphertext* bukan hanya bergantung pada blok *plaintext*nya, tetapi bergantung pula pada blok-blok *plaintext* yang sama pula. (Dafirius lombu dkk, 2018). Salah satu peneliti yang mengkaji *Cipher Block Chaining* telah dilakukan oleh Wijayanto (2021). Hasil enkripsi algoritma *Cipher Block Chaining* dengan persamaan $C_i = E_K\,(P_i \oplus C_{i-1})$ disandikan kembali dengan menggunakan algoritma *Rail Fence Cipher* dengan mengurutkan karakter. Proses dekripsi tersebut dilakukan dengan proses didekripsi lagi menggunakan *One Time Pad Cipher* dengan persamaan $P_i = D_K(C_i) \oplus C_{i-1}$. Panjang kunci pada algoritma *Cipher Block Chaining* harus sama dengan panjang *plaintext* agar bisa dienkripsi kembali dengan menggunakan algoritma *Rail Fence Cipher*.

Proses enkripsi dan dekripsi membutuhkan suatu protokol perjanjian kunci yaitu kesepakatan mengenai kunci rahasia yang dilakukan oleh pihak pengirim dan pihak penerima pesan sehingga kedua belah pihak dapat menyapakati suatu kunci rahasia. Proses enkripsi dilakukan dengan cara mengubah *plaintext* menjadi *ciphertext* dan perhitungannya dilakukan dengan cara mengubah *plaintext* dan

perhitungannya dilakukan dengan menggunakan invers kunci yang sudah disepakati. Penelitisn ini dibahas mengenai enkripsi dan dekripsi pesan dimana dalam perhitungannya menggunakan grup simetri $S_n$ umtuk menentukan kunci rahasia telah dilakukan sebelumnya oleh Wasiatun (2016).

Berdasarkan penelitian Wijayanto (2021) menerapkan algoritma yaitu *Cipher Block Chaining* dan algoritma *Rail Fence Cipher* yang mana pada algoritma kedua ini perlunya kombinasi dari beberapa algortima agar keamanan lebih terjaga. Wasiatun (2016) membahas tentang proses enkripsi dan dekripsi pesan menggunakan $S_n$ untuk mengamankan pesan yang mana tingkat keamanannya peneliti menggunakan satu buah algoritma sangatlah diragukan keamanannya. Oleh karena itu, penelitian ini akan mengembangkan penggabungan dua proses yaitu Implementasi algoritma *Cipher Block Chaining* dan Transposisi Grup Simetri pada Pengamanan Pesan Teks agar keamanan lebih terjaga.

## 1.2 Rumusan Masalah

Berdasarkan pada latar belakang, maka dapat rumusan masalah yang berkaitan dengan penjelasan diatas adalah:

1. Bagaimana proses enkripsi pesan menggunakan algoritma *Cipher Block Chaining* dan transposisi grup simetri $S_4$ untuk mengamankan pesan teks?
2. Bagaimana proses dekripsi pesan menggunakan algoritma *Cipher Block Chaining* dan transposisi grup simetri $S_4$ untuk mengamankan pesan teks?

## 1.3 Tujuan Penelitian

Merujuk pada rumusan masalah di atas, maka tujuan dan penulis skripsi ini adalah untuk:

1. Mengetahui proses enkripsi pesan menggunakan algoritma *Cipher Block Chaining* dan transposisi grup simetri $S_4$ untuk mengamankan pesan teks?
2. Mengetahui proses dekripsi pesan menggunakan algoritma *Cipher Block Chaining* dan trasposisi grup simetri $S_4$ untuk mengamankan pesan teks?

## 1.4 Manfaat Penelitian

Penelitian ini dilakukan dengan harapan dapat bermanfaat bagi berbagai pihak berikut:

1. Bagi Penulis

   Penelitian ini diharapkan menjadi pembelajaran untuk memahami khususnya mengenai Algoritma Cipher Block Chaining dan Transposisi Grup Simetri $S_4$ sehingga dapat menambah dan mengembangkan wawasan yang nantinya juga dapat dijadikan sebagai bahan rujukan untuk penelitian selanjutnya
2. Bagi Mahasiswa

   Penelitian ini diharapkan menambah pengetahuan keilmuan aljabar matematika khususnya tentang keterkaitan dengan kriptografi dalam menggunakan sarana informasi dan komunikasi untuk melakukan informasi yang aman.
3. Bagi Instansi

   Hasil penelitian ini dapat digunakan sebagai tambahan bahan literatur atau bahan pustaka dan bahan pengembangan ilmu matematika. Khususnya yang berhubungan dengan kriptografi.

## 1.5 Batasan Masalah

Agar pembahasan pada penelitian ini tidak meluas, maka penulis memberikan batasan-batasan masalah sebagai berikut:

1. Algoritma *Cipher Block Chaining* (CBC). Proses penyandian teks ini dilakukan dengan mengelompokkan kode biner dari teks asli menjadi beberapa blok seterusnya di-*XOR*-kan ke kunci yang sudah ditentukan, setelah itu hasil *XOR* tersebut digeser 4 bit dari kiri ke kanan. Proses Dekripsi dengan algoritma *Cipher Block Chaining* (CBC) dilakukan dengan teks asli yang sudah dienkripsi digeser dahulu dari kanan ke kiri sebanyak 4 bit setelah itu di-*XOR*-kan dengan *Inisial Vector*. Input yang dibutuhkan oleh sistem adalah teks yang diinput langsung oleh *user* dapat diinputkan merupakan karakter-karakter ASCII.
2. Proses enkripsi transposisi grup simetri menggunakan teknik transposisi (permutasi) dengan melakukan permutasi $\pi$ pada *plaintext*, sedangkan proses dekripsi transposisi grup simetri dengan melakukan invers permutasi $\pi^{-1}$ pada *ciphertext*.
3. Pada pembentukan kunci untuk proses grup simetri adalah algoritma protokol perjanjian kunci Stickel yang perhitungannya berdasarkan grup simetri oleh dua pihak yang berbeda yaitu pengirim pesan dan penerima pesan.

## 1.6 Definisi Istilah

Pada penelitian ini terdapat beberapa istilah yang penting untuk dijelaskan, agar tidak terjadi salah makna serta mendapat kesamaan pemahaman tentang tema dan arah penelitian. Beberapa istilah yang digunakan dalam penelitian ini adalah:

1. Algoritma Cipher Block Chaining

   *Cipher Block Chaining* adalah teks asli yang sama akan dienkripsi ke dalam bentuk *cipher* berbeda, disebabkan *block cipher* yang satu tidak berhubungan dengan *block cipher* lain, melainkan tergantung pada *cipher* sebelumnya.

2. Algoritma Transposisi Grup simetri

   Algoritma transposisi grup simetri merupakan salah satu algoritma teknik transposisi (permutasi).

3. Pengamanan Pesan teks

   Penyandian teks adalah ilmu yang berdasarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi.

# BAB II
# KAJIAN PUSTAKA

## 2.1 Teori Pendukung

### 2.1.1 Grup

#### 2.1.1.1 Definisi Operasi Biner

Definisi operasi biner adalah sebagai berikut:

1. Suatu operasi biner $*$ pada himpunan G merupakan suatu fungsi $*: G \times G \rightarrow G. \forall a, b \in G$ yang dituliskan dengan $a * b$ untuk $*(a, b)$.
2. Suatu operasi biner $*$ pada himpunan $G$ merupakan assosiatif jika untuk semua $a, b, c \in G$ maka berlaku $a * (b, c) = (a * b) * c$.
3. Jika $*$ merupakan operasi biner pada himpunan $G$ maka unsur-unsur $a$ dan $b$ dari $G$ komutatif jika $a * b = b * a$ (Dummit, 2004).

#### 2.1.1.2 Definisi Grup

Suatu grup adalah pasangan berurutan $(G,*)$ yang $G$ merupakan himpunan tak kosong dan $*$ merupakan operasi biner di $G$ yang memenuhi aksioma-aksioma berikut:

1. Operasi $*$ bersifat tertutup di $G$ $\forall a, b \in G$ maka $a * b \in G$.
2. Operasi $*$ bersifat assosiatif di $G$ $(a * b) * c = a * (b * c), \forall a, b, c \in G$
3. Terdapat unsur $e$ di $G$ yang disebut sebagai unsur identitas dari $G$ sedemikian sehingga untuk semua $a \in G$ maka berlaku $e * a = a * e = a$ (terdapat identitas e dari G terhadap operasi $*$.
4. Untuk setiap $a \in G$, terdapat suatu unsur $a^{-1}$ di $G$ yang disebut invers dari $a$ sedemikian sehingga $a * a^{-1} = a^{-1} * a = e$ (terdapat invers dalam $G$ terhadap operasi $*$) (Dummit, 2004).

Grup $(G,*)$ disebut abelian atau komutatif jika $(a * b) = b * a, \forall a, b \in G$ (Dummit, 2004).

**Contoh :**

Misalkan $\boldsymbol{Z}$ adalah himpunan bilangan bulat, maka $(\boldsymbol{Z}, +)$ merupakan suatu grup karena berlaku:

Bukti:

1. Operasi penjumlahan pada $Z$ merupakan operasi biner karena pemetaan $Z \times Z \to Z. \forall a, b \in Z$ maka $a + b \in Z$.

   Jadi $Z$ tertutup terhadap operasi penjumlahan.

2. $\forall a, b, c \in Z$, maka $(a + b) + c = a + (b + c)$.

   Jadi operasi penjumlahan bersifat assosiatif di $Z$.

3. Ambil $0 \in Z$, sehingga $a + 0 = 0 + a = a, \forall a \in Z$.

   Jadi 0 adalah unsur identitas pada operasi penjumlahan.

4. Untuk setiap $a \in Z$ terdapat $(-a) \in Z$. Sehingga $a + (-a) = (-a) + a = 0$.

   Jadi invers dari $a$ adalah $-a$.

Dari (i),(ii),(iii) dan (iv) terbukti bahwa $(Z, +)$ adalah grup.

### 2.1.2 Grup Simetri

Grup simetri adalah suatu grup yang dibentuk dari suatu himpunan yang isinya merupakan permutasi-permutasi dengan operasi perkalian.

Misal Ω adalah sebarang himpunan tak kosong dan misal $S_\Omega$ adalah himpunan yang memuat semua fungsi-fungsi bijektif dari Ω ke Ω (atau himpunan yang memuat semua permutasi dari Ω). Himpunan $S_\Omega$ dengan operasi komposisi " ∘ " atau ($S_\Omega$,∘) merupakan suatu grup. Operasi komposisi " ∘ " merupakan suatu biner pada $S_\Omega$ karena jika $\sigma: \Omega \to \Omega$ dan $\tau: \Omega \to \Omega$ adalah fungsi-fungsi bijektif, maka $\sigma \circ \tau$ juga merupakan suatu bijektif dari Ω ke Ω' selanjutnya operasi " ∘ " adalah komposisi fungsi yang bersifat assosiatif. Indentitas dari $S_\Omega$ merupakan permutasi 1 yang didefinisikan dengan $1(a) = a, \forall a \in \Omega$. Untuk setiap permutasi $\sigma: \Omega \to \Omega$ terdapat fungsi invers $\sigma^{-1}: \Omega \to \Omega$ yang memenuhi $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$. Dengan demikian semua aksioma grup telah dipenuhi oleh $S_\Omega$ dengan operasi komposisi " ∘ ". Grup ($S_\Omega$,∘) disebut sebagai grup simetri pada himpunan $S_\Omega$. Yang perlu diketahui bahwa elemen dari $S_\Omega$ adalah permutasi dari Ω, bukan elemen dari Ω itu sendiri. Unsur-unsur dari $S_\Omega$ adalah simetri-simetri dari Ω.

Pada kasus khusus dengan $\Omega = \{1,2,3, \dots, n\}$ merupakan grup simetri pada Ω yang dinotasikan $S_\mathrm{n}$, yaitu grup simetri dengan derajat n. Order dari $S_\mathrm{n}$ adalah n! (Dummit, 2004).

#### 2.1.2.1 Definisi Grup Simetri $S_4$

Grup simetri $S_4$ adalah grup semua permutasi dari empat elemen. Definisikan $S_4$ sebagai himpunan semua fungsi satu-satu dari {1,2,3,4} ke dirinya sendiri. Grup simetri $S_4$ dibawah operasi komposisi mempunyai $4! = 24$ elemen.

Elemen-elemen dari $S_4$ ditetapkan sebagai berikut:

$f_0 = (1), f_1 = (34), f_2 = (23), f_3 = (234), f_4 = (243), f_5 = (24),$

$f_6 = (12), f_7 = (12)(34), f_8 = (123), f_9 = (1234),\ f_{10} = (1243)$

$f_{11} = (124), f_{12} = (132), f_{13} = (1342), f_{14} = (13), f_{15} = (134),$

$f_{16} = (13)(24), f_{17} = (1324), f_{18} = (1432), f_{19} = (142)$

$f_{20} = (143), f_{21} = (14), f_{22} = (1423), dan\ f_{23} = (14)(23).$

**Contoh :**

Jika $S$ adalah sebuah himpunan tak kosong maka *A(S)* adalah himpunan semua pemetaan satu-satu dan pada dari $S$ ke dirinya sendiri:

Bukti: Jika $\sigma, \tau, \mu$ adalah elemen-elemen dari $A(S)$, maka

1. $\sigma^{\circ}\tau$ berada *di* $A(S)$.
2. $(\sigma^{\circ}\tau)^{\circ}\mu = \sigma^{\circ}(\tau^{\circ}\mu)$.
3. Terdapat sebuah elemen 1 (pemetaan identitas) di *A(S)* sedemikian sehingga $\sigma^{\circ}1 - 1^{\circ}\sigma = \sigma$.
4. Terdapat sebuah elemen $\sigma - 1 \in A(S)$ sedemikian sehingga $\sigma^{\circ}\sigma - 1 = \sigma 1^{\circ}\sigma = 1$.

Berdasarkan contoh maka diperoleh:

1. Komposisi di $S_4$ bersifat tertutup.
2. Komposisi di $S_4$ bersifat asosiatif dimana untuk setiap $x, y, z \in S_4$ berlaku $(x^{\circ}y)^{\circ}\, z = x^{\circ}(y^{\circ}z)$.
3. Terdapat elemen identitas $f_0$ sehingga $f_0\, ^{\circ}\, x = x\, ^{\circ} f_0 = x$ untuk setiap $x \in S_4$.

4. Terdapat elemen invers dari $x$ yakni $x'$ yang mana $x' \circ x = x \circ x' = f_0$ untuk setiap $x \in S_4$.

Sehingga dapat disimpulkan bahwa himpunan $S_4$ adalah sebuah grup terhadap operasi ° (Febyola, 2017).

#### 2.1.2.2 Order dari Unsur Grup Simetri $S_4$

Misalkan $\sigma = (a_1, a_2 \dots a_r)$ adalah suatu *r-cycle*, maka $\sigma^n = (a_1, a_2 \dots a_r)^n$ ini berarti $a_i$ berganti sebanyak $n$ kali dengan $n \geq 1$ dan $n$ adalah nilai terkecil sedemikian sehingga $\sigma^n = e$ dengan $n = r$. Akibatnya, suatu *r-cycle* mempunyai order *r* (Febyola, 2017).

Order dari unsur-unsur $S_4$ ditunjukkan sebagai berikut:

**Tabel 2.1 Tabel Order dari Unsur Grup Simetri-4 $S_4$**

| Order | Unsur |
|---|---|
| 1 | $f_0$ |
| 2 | $f_1, f_2, f_5, f_6, f_7, f_{14}, f_{16}, f_{21}, f_{23}$ |
| 3 | $f_3, f_4, f_8, f_{11}, f_{12}, f_{15}, f_{19}, f_{20}$ |
| 4 | $f_9, f_{10}, f_{13}, f_{17}, f_{18}, f_{22}$ |

### 2.1.3 Kriptografi

#### 2.1.3.1 Pengertian Kriptografi

Kriptografi *(cryptography)* berasal dari bahasa Yunani yaitu: *"cryptos"* artinya *"secret"* (rahasia), sedangkan *"graphein"* artinya *"writing"* (tulisan). Jadi, kriptografi secara harfiah berarti *"secret writing"* (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan didalam berbagai pustaka. Menyatakan bahwa kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti

kerahasiaan, integritas data, otentikasi serta penyangkalan dari pengirim dan penerima pesan (Munir, 2019).

#### 2.1.3.2 Komponen Kriptografi

Di dalam kriptografi, akan sering ditemukan berbagai istilah atau terminologi. Beberapa istilah yang penting untuk diketahui oleh pembaca diberikan berikut ini.

1. *Plaintext* dan *Ciphertext*

   Pesan *(message)* adalah data atau informasi yang dapat dibaca, dipersepsi, dan dimengerti artinya. Pesan berupa teks sering disebut juga *plaintext* atau teks-jelas *(cleartext)*. Agar pesan tidak dapat dipahami isinya oleh pihak lain, maka pesan perlu disandikan menjadi pesan yang tidak dapat dimengerti lagi maknanya. Pesan teks yang disandi disebut *ciphertext*. Pesan yang tersandi harus dapat dikembalikan menjadi pesan semula agar bisa dibaca. Dengan cara *Ciphertext* harus dapat ditrasformasikan kembali menjadi *plaintext* semula agar pesan yang diterima bisa dibaca.

2. Pengirim dan Penerima

   Pengirim *(sender)* adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima *(receiver)* adalah entitas yang menerima pesan. Pengirim atau penerima tidak harus berupa orang, tetapi juga dapat berupa mesin, robot, atau komputer.

3. Enkripsi dan Dekripsi

Enkripsi *(encryption)* atau *enciphering* merupakan proses menyandikan plainteks menjadi cipherteks. Sedangkan proses mengembalikan cipherteks menjadi plainteks semula dinamakan dekripsi *(decryption)* atau *deciphering.*

4. *Cipher* dan Kunci

   Algoritma kriptografi untuk enkripsi dan dekripsi disebut juga *cipher*. *Cipher* dapat diartikan sebagai aturan untuk *enchipering* dan *dechiphering*, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi (Munir, 2019). Kunci yang dimaksud adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci rahasia *(private key)* dan kunci umum *(public key)* (Ariyus, 2008).

5. Kriptanalisis dan Kriptologi

   Kriptanalisis *(cryptanalysis)* adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks, tanpa mengetahui kunci yang digunakan dalam enkripsi-dekripsi. Orang yang melakukan kriptanalisis disebut **kriptanalis**. Kriptografi dan kriptanalisis adalah cabang dari ilmu yang dinamakan kriptologi. **Kriptologi** *(cryptology)* adalah studi mengenai kriptografi dan kriptanalisis.

### 2.1.4 Substitusi

Metode penyandian secara substitusi dan metode penyandian secara transposisi merupakan bagian dari kriptografi klasik. Bentuk penyandian berupa teks (huruf/karakter) adalah bentuk penyandian dari kriptografi klasik. Biasanya

dengan menggunakan alat tulis berupa kertas dan pensil. Namun bila menggunakan mesin sandi, biasanya mesin tersebut masih sangat sederhana.

Seiring berkembangnya zaman, dalam metode penyandian substitusi modern, teks asli yang berbentuk kumpulan karakter dalam sebuah file dapat diganti secara digital pula sehingga menghasilkan kumpulan karakter lain dengan file sandi yang siap dikomunikasikan. Untuk membaca teks aslinya kembali dari teks sandi, cukup dengan memutar balik prosesnya.

Terdapat beberapa macam metode penyandian substitusi, diantaranya adalah:

1. Metode penyandian Substitusi Sederhana
2. Metode Penyandian *Caesar*
3. Metode Penyandian *Vigenere*
4. Metode Penyandian *Hill*
5. Metode Penyandian *OTP*

### 2.1.5 Transposisi

Metode penyandian dengan cara mengubah letak dari teks pesan yang akan disandikan merupakan metode penyandian transposisi. Dengan mengembalikan letak dari pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati ini merupakan cara agar dapat membaca kembali pesan aslinya.

Transposisi sering dikombinasikan dengan teknik lain untuk memperkuat keamanan suatu data. Metode penyandian transposisi mempunyai beberapa algoritma yaitu:

1. Penyandian transposisi *Rail Fence Cipher*
2. Penyandian transposisi *Route cipher*
3. Penyandian transposisi kolom
4. Penyandian transposisi ganda

### 2.1.6 Algoritma Kriptografi

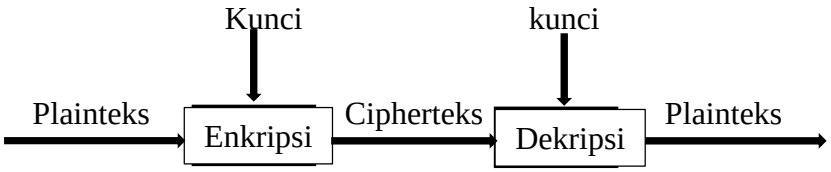
Algoritma kriptografi memerlukan kunci untuk melakukan enkripsi dan dekripsi. Macam-macam algoritma kriptografi dibagi menjadi tiga bagian berdasarkan kunci yang dipakainya:

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).

#### 2.1.6.1 Algoritma Simetri

Kriptografi simetri adalah kriptografi kunci-privat, kriptografi kunci rahasia, atau kriptografi konvensional. Semua kriptografi klasik termasuk ke dalam kelompok kriptografi simetri. Karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi. Bila pengirim pesan dengan menggunakan algoritma ini, si penerima pesan harus diberitahu kunci dari pesan tersebut agar bisa mendekripsikan pesan yang dikirim. Di dalam kriptografi simetri, keamanannya terletak pada kerahasiaan kuncinya. Jika kunci tersebut diketahui oleh orang lain maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan. Algoritma yang memakai kunci simetri diantaranya,

*DES (Data Encryption Standart), Blowfish, twofish, triple-DES, IDEA, OTP, A5, RC4, RC5, RC6,* dan masih banyak yang lain, dan yang menjadi standart saat ini adalah *AES (Advanced Data Standart)* (Munir,2019).



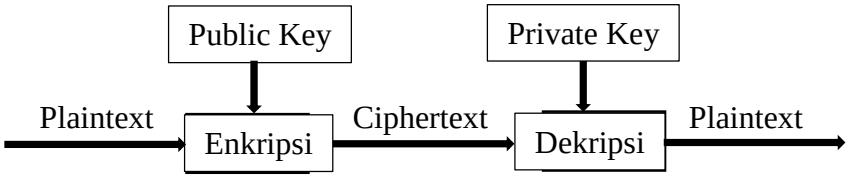

**Gambar 2.1 Algoritma Simetri (Munir, 2019)**

### 2.1.6.2 Algoritma Asimetri

Algoritma asimetri sering disebut juga dengan algoritma kunci publik. Arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu (Ariyus, 2008):

1. Kunci umum (*Public Key*): kunci yang boleh semua orang tahu (dipublikasikan).
2. Kunci rahasia (*Private Key*): kunci yang dirahasikan (hanya boleh dikatahui oleh satu orang).

Kunci tersebut berhubungan satu sama lain. Dengan kunci publik orang dapat mengenkripsi pesan tetapi tidak bisa mendekripsinya. Hanya orang yang memiliki kunci rahasia yang dapat mendekripsi pesan tersebut. Algoritma asimetri bisa mengirim pesan dengan lebih aman dari pada algoritma simetri. Algoritma yang memakai kunci publik diantaranya adalah DSA *(Digital Signature Algorithm), RSA, DH (Diffffie-Hellmann), EEC (Eliptic Curve Cryptography)*, Kriptografi Quantum, dan lain sebagainya.




**Gambar 2.2 Algoritma Asimetri (Munir, 2019)**

### 2.1.7 Super Enkripsi

Super enkripsi merupakan suatu konsep dengan menggunakan kombinasi dari dua atau lebih dari teknik substitusi dan transposisi *cipher* untuk mendapatkan suatu algoritma yang sulit dipecahkan oleh penyusup (Ariyus, 2006). Untuk menjalankan teknik super enkripsi ini, harus mengerti teknik substitusi dan transposisi yang akan dioperasikan.

*Cipher* substitusi dan *cipher* transposisi dapat dikombinasikan untuk memperoleh cipher yang lebih kuat (super) dari pada hanya satu *cipher* saja. Mula-mula *plaintext* dienkripsikan dengan *cipher* substitusi sederhana (misalnya *cipher* alphabet-tunggal), lalu hasilnya dienkripsi lagi dengan *cipher* transposisi (atau bisa juga sebaliknya) (Munir, 2019). Konsep super enkripsi dapat diperluas penggunaannya dari teks ke citra warna. Algoritma kriptografi modern menerapkan prinsip super enkripsi untuk mendapatakan cipherteks yang kompleks.

### 2.1.8 Algoritma kriptografi Klasik dan Kriptografi Modern

Kriptografi klasik merupakan suatu algoritma yang menggunakam suatu 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).

Tiga alasan mengapa kita perlu mempelajari algoritma-algoritma kriptografi klasik meskipun mereka sudah kadaluwarsa adalah: (1) untuk memberikan pemahaman konsep dasar kriptografi, (2) sebagai dasar dari algoritma kriptografi modern, (3) agar dapat memahami potensi-potensi kelemahan *Cipher*.

Kriptografi modern merupakan suatu algoritma yang digunakan pada saat sekarang ini, yang mana kriptografi modern mempunyai kerumitan yang sangat kompleks, karena dalam pengoperasian menggunakan komputer.

### 2.1.9 Bit String Dalam Kriptografi Modern

Pada pengoperasiannya kriptografi modern berbeda dengan kriptografi klasik dikarenakan kriptografi modern sudah menggunakan komputer sehingga data dapat diamankan melalui jaringan komputer dengan cara ditransfer maupun tidak, hal ini sangat berguna untuk melindungi privasi dan integritas data (Ariyus, 2008).

Kriptografi klasik menggunakan subsitusi dan permutasi karakter dari teks-asli. Pada kriptografi modern, karakter yang ada dikonversi ke dalam suatu urutan digit biner (*bits*), yaitu 1 dan 0, yang umum digunakan untuk skema

*encoding* ASCII (*American Standard Code For Information Interchange*). Urutan bit yang mewakili teks-asli yang kemudian dienkripsi untuk mendapatkan teks-kode dalam dalam bentuk urutan bit (Ariyus, 2008).

Algoritma kriptografi modern umumnya beroperasi dalam bit biner. Ini berarti plainteks, kunci dan cipherteks dinyatakan dalam biner (0 dan 1). Beberapa algoritma kriptografi modern memproses data dalam bentuk blok-blok bit dapat ditulis dalam sejumlah cara bergantung pada panjang blok. Bila panjang rangkaian bit tidak habis dibagi dengan ukuran blok yang diterapkan, maka blok yang berakhir ditambah dengan bit-bit semu yang disebut *padding bits* (Munir, 2019).

Algoritma enkripsi bisa menggunakan salah satu dari dua metode. Yang pertama “natural”, pembagian antara aliran kode, di mana urutan dalam bit untuk enkripsi menggunakan metode *bit-by-bit*. Metode kedua adalah blok kode, di mana urutan pembagian dalam bentuk ukuran blok yang diinginkan. ASCII memerlukan 8 bit untuk mendapatkan satu karakter dan blok kode mempunyai 64 bit untuk satu blok. Sebagai contoh sequence 12 bit: $100111010110$. Jika dipecah menjadi 3 block maka didapat $100\ 111\ 010\ 110$. Bagaimanapun bit-string dengan panjang 3 menghadirkan bilangan bulat dari 0 sampai 7 dengan urutan menjadi 4 7 2 6.

$$000 = 0, \qquad 001 = 1, \qquad 010 = 2, \qquad 011 = 3,$$

$$100 = 4, \qquad 101 = 5, \qquad 110 = 6, \qquad 111 = 7$$

Cara yang umum untuk menulis bit-string dengan menggunakan notasi heksadesimal (*HEX*). Untuk *HEX* setring dibagi ke dalam bentuk blok yang berukuran 4 sebagai berikut:

$0000 = 0 \quad 0001 = 1 \quad 0010 = 2 \quad 0011 = 3$

$0100 = 4 \quad 0101 = 5 \quad 0110 = 6 \quad 0111 = 7$

$1000 = 8 \quad 1011 = 9 \quad 1010 = A \quad 1011 = B$

$1100 = C \quad 1101 = D \quad 1101 = E \quad 1111 = F$

Sejak operasi algoritma kode menggunakan string biner maka perlu dibiasakan untuk menggunkan metode kombinasi dua bit yang disebut *Exclusive OR* dan kadang ditulis dengan *XOR* atau $\oplus$. Ini merupakan suatu penambahan modulo 2 dan digambarkan sebagai berikut: $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0$. Operasi *XOR* ini mengkombinasikan dua bit-string dengan panjang yang sama (Ariyus, 2008).

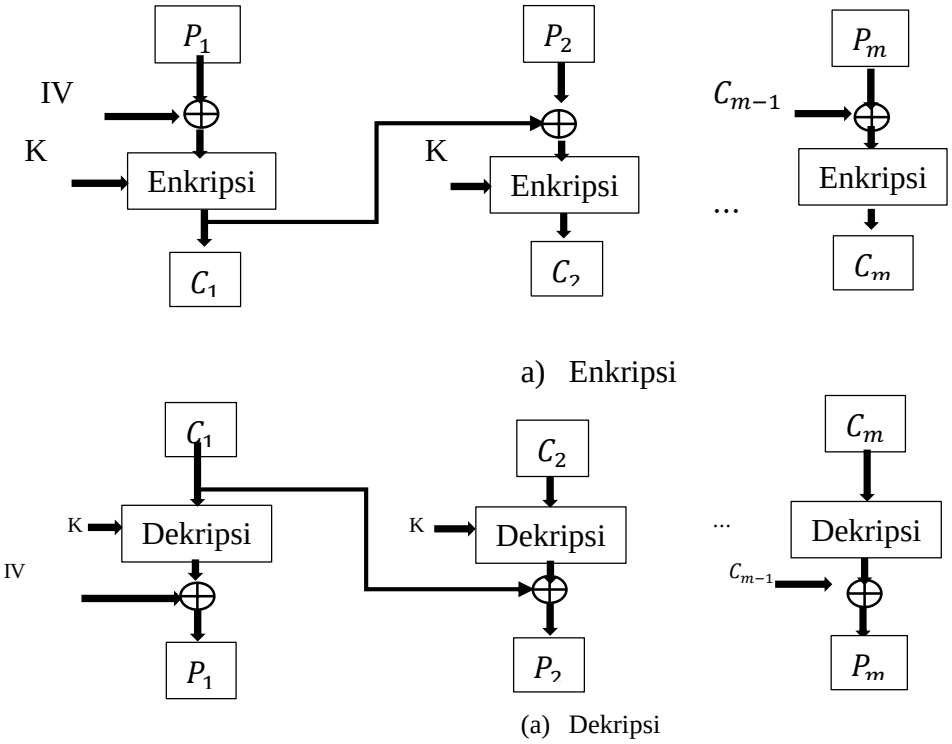
### 2.1.10 Algoritma *Cipher Block Chaining*

*Cipher Block Chaining* adalah teks asli yang sama akan dienkripsi ke dalam bentuk *cipher* berbeda, disebabkan *block cipher* yang satu tidak berhubungan dengan *block cipher* lain, melainkan tergantung pada *cipher* sebelumnya (Ariyus, 2008).

*Cipher Block Chaining* merupakan penerapan mekanisme umpan-balik pada sebuah block *bit* dimana hasil enkripsi block sebelumnya diumpan balikkan ke dalam proses enkripsi block *current*. Caranya, block *plaintext* yang current di-*XOR*-kan terlebih dahulu dengan block *ciphertext* hasil enkripsi sebelumnya,

selanjutnya hasil peng-*XOR*-an ini masuk ke dalam fungsi enkripsi. Dengan algoritma *CBC*, setiap block *ciphertext* tidak hanya bergantung pada block *plaintext* nya tetapi juga pada seluruh block *ciphertext* sebelumnya (Rosmala, 2012).

Di bawah ini akan dijelaskan prosesnya secara lebih rinci:




**Gambar 2.3 Flowchart Algoritma Cipher Block Chaining (Munir, 2019)**

Dekripsi dilakukan dengan memasukkan block cipherteks yang *current* ke fungsi dekripsi, kemudian meng-*XOR*-kan hasilnya dengan block cipherteks sebelumnya. Dalam hal ini, block cipherteks sebelumnya berfungsi sebagai umpan-maju (*feedforward*) pada akhir proses dekripsi. Gambar 2.3 memperlihatkan skema mode operasi *CBC*. Perhatikan bahwa fungsi *E* dapat sama dengan fungsi *D*, atau *E=D*, sehingga tidak dibutuhkan algoritma baru untuk dekripsi. Secara matematis, enkripsi dan dekripsi untuk *m* buah block pesan dengan mode *CBC* dinyatakan sebagai

Enkripsi: $C_i = E_K\ (P_i \oplus C_{i-1}),$ $i = 1,2, \dots, m$

Dekripsi: $P_i = D_K(C_i) \oplus C_{i-1},$ $i = 1,2, \dots, m$

Keterangan:

$C_i$ = *Cipertext* ke-i

$P_i$ = *Plaintext* ke-i

$E_K$ = Kunci pada Enkripsi

$D_K$ = Kunci pada Dekripsi

Kasus khusus adalah enkripsi blok pertama sebab tidak tersedia nilai $C_0$. Untuk mengatasinya, maka $C_0$ diganti dengan sebuah nilai sembarang yang dinamakan *IV (initialization vector)*. Jadi $C_0 = IV$. Nilai *IV* dapat dinyatakan sebagai konstanta atau dibangkitkan secara acak oleh program. Sebaliknya pada dekripsi, block plainteks pertama diperoleh dengan cara meng-*XOR*-kan *IV* dengan hasil dekripsi terhadap block cipherteks pertama. *IV* tidak perlu rahasia. Jadi, untuk *m* buah block plainteks, enkripsi nya adalah:

$C_1 = E_K(P_1 \oplus IV)$

$C_2 = E_K(P_2 \oplus C_1)$

$C_3 = E_K(P_3 \oplus C_2)$

$\vdots$

$C_m = E_K(P_m \oplus C_{m-1})$

Dan dekripsi *m* buah block cipherteks adalah:

$C_1 = D_K(C_1) \oplus IV$

$C_2 = D_K(C_2) \oplus C_1$

$C_3 = D_K(C_3) \oplus C_2$

$\vdots$

$C_m = D_K(C_m) \oplus C_{m-2}$ (Munir, 2019).

Adapun langkah-langkah dalam penyelesaian proses algoritma *cipher block chaining* (CBC) adalah sebagai berikut:

1. Input plainteks atau cipherteks, kemudian konversikan nilai desimal ke biner.
2. Tentukan nilai jumlah bit setiap kelompok, kunci, *initialization vector* ($C_0$)
3. Kelompokkan biner-biner plainteks dan cipherteks kedalam blok sesuai dengan jumlah bit per kelompok yang telah ditentukan sebelumnya.
4. Melakukan proses enkripsi dan dekripsi pada setiap blok/kelompok biner *plaintext* atau *ciphertext* dimana setiap block saling ketergantungan dengan blok yang lain.
5. Lakukan proses pergeseran bit *plaintext* maupun *ciphertext* sesuai dengan jumlah bit yang diterapkan oleh pengguna, hasil pergeseran inilah yang menjadi hasil akhir dari proses enkripsi dan dekripsi.

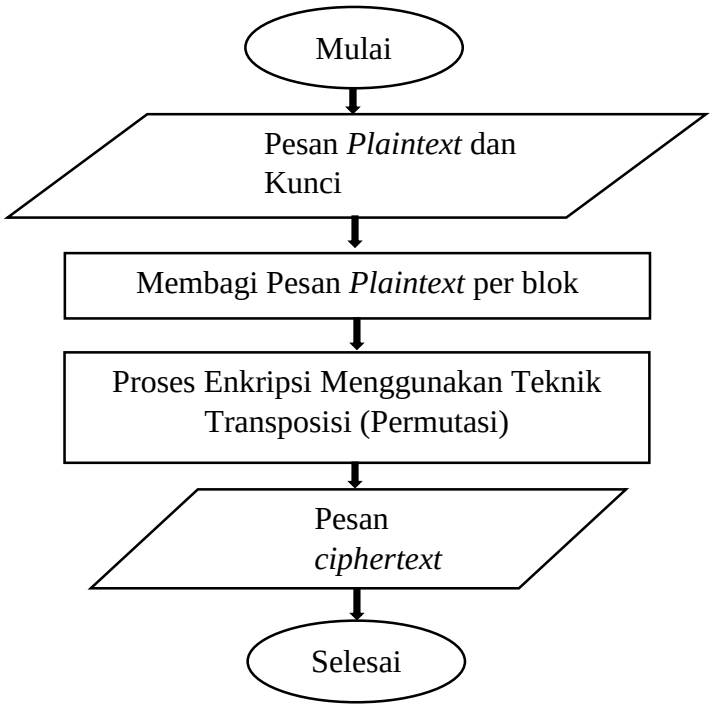
### 2.1.11 Algoritma Transposisi Grup Simetri

Teknik transposisi (permutasi) ini menggunakan permutasi karakter, yang mana dengan menggunakan teknik ini pesan yang asli tidak dapat dibaca kecuali oleh orang yang memiliki kunci untuk mengembalikan pesan tersebut ke bentuk

semula (Ariyus, 2008). Algoritma enkripsi menggunakan teknik transposisi (permutasi) dengan melakukan permutasi $\pi$ pada teks asli (*plaintext*), sedangkan algoritma dekripsi dengan melakukan invers permutasi $\pi^{-1}$ pada teks kode (*ciphertext*) (Sadikin, 2012).

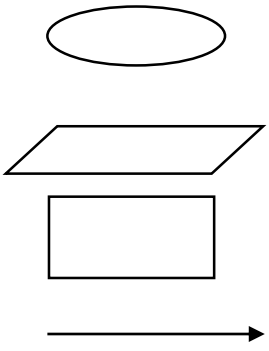
1. Proses Enkripsi Teknik Transposisi (Permutasi)

   Langkah pertama dari proses enkripsi dengan teknik transposisi (permutasi) adalah membagi pesan plaintext menjadi per blok yang terdiri dari beberapa huruf. Kunci pada teknik transposisi (permutasi) ini menggunakan bentuk permutasi-$n$, yang mana dengan menggunakan teknik ini pesan yang asli tidak dapat dibaca kecuali oleh orang yang memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula (Ariyus, 2008). Proses enkripsi menggunakan teknik transposisi (permutasi) ini dapat dijelaskan dalam *flowchart* sebagai berikut:




**Gambar 2.4 Proses Enkripsi Teknik Transposisi (Permutasi) (Ariyus, 2008)**

Keterangan:



: permulaan atau akhir program

: proses input atau output data, parameter dan informasi.

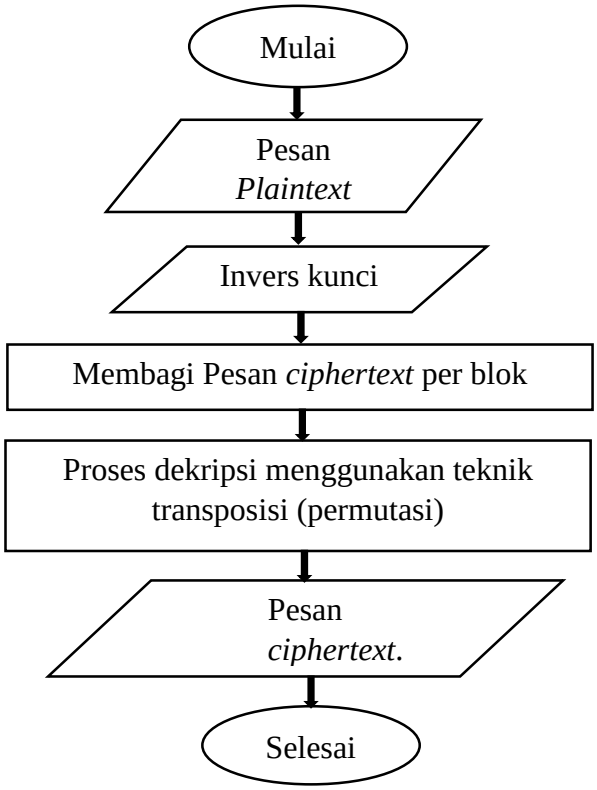
: proses perhitungan atau proses pengolahan data.

: arah aliran program

2. Proses Dekripsi Teknik Transposisi (Permutasi)

Pada dasarnya proses dekripsi sama saja dengan proses enkripsi, akan tetapi pada proses ini penerima pesan ini penerima pesan mendekripsikan pesan ciphertext dengan menginverskan kunci yang telah disepakati.

Proses dekripsi menggunakan teknik transposisi (permutasi) ini dapat dijelaskan dalam *flowchart* sebagai berikut:




**Gambar 2.5 Proses Dekripsi Teknik Transposisi (Permutasi) (Ariyus, 2008)**

**Contoh :**

Ada 6 kunci untuk melakukan permutasi kode:

| $x$ | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ |
|---|---|---|---|---|---|
| $\pi(x)$ | $a_3$ | $a_5$ | $a_1$ | $a_2$ | $a_4$ |

dan 6 kunci untuk invers dari permutasi tersebut:

| $x$ | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ |
|---|---|---|---|---|---|
| $\pi^{-1}(x)$ | $a_3$ | $a_4$ | $a_1$ | $a_5$ | $a_2$ |

Seandainya kita akan melakukan permutasi terhadap kalimat di bawah ini:

| SAYA SEDANG MENAHAN RINDU IBU |
|---|

Terlebih dahulu kalimat tersebut dibagi menjadi 5 blok dan apabila terjadi kekurangan dari blok bisa ditambah dengan huruf yang disukai, misalkan & dan spasi dilambangkan dengan $. Hal ini berguna untuk mempersulit analisis dari kode tersebut.

| | | |
|---|---|---|
| SAYA$ | SEDAN | G$MEN |
| RINDU | $IBU& | AHAN$ |

Setelah dibagi menjadi 5 blok maka dengan menggunakan kunci nomor satu di atas setiap blok akan berubah menjadi seperti di bawah ini:

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

= Y$SAA

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

= DNSEA

Blok III: $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_5 & a_1 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ G & \$ & M & E & N \\ a_3 & a_5 & a_1 & a_2 & a_4 \\ M & N & G & \$ & E \end{pmatrix}$

= MNG$E

Blok IV: $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_5 & a_1 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ A & H & A & N & \$ \\ a_3 & a_5 & a_1 & a_2 & a_4 \\ A & \$ & A & H & N \end{pmatrix}$

= A$AHN

Blok V: $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_5 & a_1 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ R & I & N & D & U \\ a_3 & a_5 & a_1 & a_2 & a_4 \\ D & N & S & E & A \end{pmatrix}$

= DNSEA

Blok VI: $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_5 & a_1 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \$ & I & B & U & \& \\ a_3 & a_5 & a_1 & a_2 & a_4 \\ B & \& & \$ & I & U \end{pmatrix}$

= B&$IU

Jadi *ciphertext* yang dihasilkan

Y$SAADNSEAMNG$EA$AHNDNSEAB&$IU

Sedangkan untuk proses mengembalikan ke bentuk teks-asli maka dilakukan invers terhadap ciphertext dengan mengikuti kunci nomor dua di atas.

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) (Ariyus, 2008).

### 2.1.12 Protokol Perjanjian Kunci

Protokol perjanjian kunci merupakan skema dalam kriptografi yang digunakan untuk mengatasi masalah perjanjian kunci rahasia. Kunci tersebut digunakan pada proses enkripsi dan dekripsi diantara dua pihak yang saling berkomunikasi. Tingkat keamanan dari protokol perjanjian kunci diletakkan pada tingkat kesulitan dari suatu permasalahan matematis dan bertujuan agar kedua belah pihak dapat menentukan kunci yang sama. Protokol perjanjian kunci Diffie-Hellman merupakan salah satu contoh perjanjian kunci yang paling sederhana yang dipublikasikan pada tahun 1976. Skema Protokol Perjanjian Kunci Diffie-Hellman (Myasnikov, 2008) disajikan pada tabel 2.2.

**Tabel 2.2 Skema Protokol Perjanjian Kunci Diffie-Hellman (Myasnikov dkk, 2008)**

| Pengirim pesan atau penerima pesan mempublikasikan suatu grup siklik $G$ dengan elemen pembangun $g \in G$. | |
|---|---|
| Pengirim pesan | Penerima pesan |
| 1. Pengirim pesan memilih secara rahasia suatu bilangan positif $a$<br>2. Pengirim pesan menghitung $g^a$<br>3. Pengirim pesan mengirim $g^a$ kepada pengirim pesan<br>4. Pengirim pesan menerima $g^b$ dari penerima pesan | 1. Penerima pesan memilih secara rahasia suatu bilangan positif $b$<br>2. Penerima pesan menghitung $g^b$<br>3. Penerima pesan mengirim $g^b$ kepada pengirim pesan<br>4. Penerima pesan menerima $g^a$ dari pengirim pesan |

| | |
|---|---|
| 5. Pengirim pesan menghitung $K_1 = (g^a)^b = g^{ab}$ | 5. Penerima pesan menghitung $K_2 = (g^b)^a = g^{ba}$ |
| Pengirim pesan dan penerima pesan telah menyepakati kunci rahasia $K = K_1 = K_2$ | |

Setiap grup siklik merupakan grup komutatif, maka $ab = ba$, sehingga diperoleh $K = K_1 = K_2$. Misalkan pengirim pesan dan penerima pesan telah berhasil menyepakati kunci rahasia yang sama yaitu $K$. Kemudian, kunci rahasia $K$ yang telah disepakati digunakan untuk melakukan proses enkripsi dan dekripsi. Selain pengirim dan penerima, penyadap sebagai penyerang hanya dapat mengetahui nilai $g$, $g^a$ dan $g^b$ . Untuk mendapatkan kunci yang telah disepakati pengirim pesan dan penerima pesan, penyadap harus menentukan nilai $a$ atau $b$. Dengan kata lain, penyadap harus menyelesaikan masalah logaritma diskrit pada $G$, yaitu menentukan $a$ apabila nilai $g$ dan $g^a$ diketahui. Tingkat keamanan dari protokol perjanjian kunci Diffie-Hellman didasarkan pada masalah logaritma diskrit pada grup siklik (Myasnikov, 2008).

Pada protokol perjanjian kunci *Diffie-Hellman* digunakan grup siklik yang merupakan grup komutatif. Akan tetapi, pada penelitian Stickel (2005) dalam Myasnikov (2008) diperkenalkan konsep mengenai protokol perjanjian kunci yang menggunakan grup non-komutatif. Myasnikov (2008) memberikan skema protokol perjanjian kunci Stickel yang didasarkan atas grup non-komutatif disajikan pada tabel 2.3.

**Tabel 2.3 Skema Protokol Perjanjian Kunci Stickel (Myasnikov dkk, 2008)**

<table>
<tr><td colspan="2">Pengirim pesan atau penerima pesan mempublikasikan suatu grup non-komutatif $G$ dan $a, b \in G, ab \neq ba$, dengan $N$ dan $M$ berturut-turut adalah order dari $a$ dan $b$.</td></tr>
<tr><td>Pengirim pesan</td><td>Penerima pesan</td></tr>
<tr><td>1. Pengirim pesan memilih secara rahasia suatu bilangan asli $n < N$ dan $m < M$<br>2. Pengirim pesan menghitung $x = a^n b^m$<br>3. Pengirim pesan mengirim $x$ kepada pengirim pesan<br>4. Pengirim pesan menerima $y$ dari penerima pesan<br>5. Pengirim pesan menghitungm $K_1 = a^n y b^m$</td><td>1. Penerima pesan memilih secara rahasia suatu bilangan asli $r < N$ dan $s < M$<br>2. Penerima pesan menghitung $y = a^r b^s$<br>3. Penerima pesan mengirim $y$ kepada pengirim pesan<br>4. Penerima pesan menerima $x$ dari pengirim pesan<br>5. Penerima pesan menghitung $K_2 = a^r\ x\ b^s$</td></tr>
<tr><td colspan="2">Pengirim pesan dan penerima pesan telah menyepakati kunci rahasia yang sama yaitu $K = K_1 = K_2$</td></tr>
</table>

$n$ dan $m$ merupakan sebarang bilangan asli kurang order $a$, $m$ dan $s$ merupakan sebarang bilangan asli kurang dari order $b$ sehingga dapat ditunjukkan bahwa penerima pesan dan pengirim pesan telah berhasil menyepakati kunci rahasia yang sama, yaitu

$$K_1 = a^n y\ b^m = a^n a^r b^s b^m = a^{n+r} b^{s+m} = a^r a^n b^m b^s = a^r\ x\ b^s = K_2$$

Grup simetri $S_n$ merupakan salah satu contoh grup yang dapat digunakan pada protokol perjanjian kunci Stickel. Penggunaan grup pada Protokol Stickel ini dapat diperumum menjadi sebarang semigrup. Kunci tersebut yang digunakan

pada proses enkripsi dan dekripsi. Proses enkripsi dan dekripsi bertujuan agar pesan yang dikirm tidak dibaca oleh orang yang tidak berhak menerimanya.

## 2.2 Kajian Integrasi Topik dengan Al-Qur'an/Hadits

Pesan rahasia sama halnya dengan amanat yang harus disampaikan kepada yang berhak menerimanya. Sebagaimana firman Allah SWT dalam Al-Qur'an surat An-Nisaa' ayat 58 dijelaskan bahwa:

اِنَّ اللّٰهَ يَأْمُرُكُمْ اَنْ تُؤَدُّوا الْاَمٰنٰتِ اِلٰٓى اَهْلِهَاۙ وَاِذَا حَكَمْتُمْ بَيْنَ النَّاسِ اَنْ تَحْكُمُوْا بِالْعَدْلِ ۗ اِنَّ اللّٰهَ نِعِمَّا يَعِظُكُمْ بِهٖۗ اِنَّ اللّٰهَ كَانَ سَمِيْعًاۢ بَصِيْرًا

*"Sungguh, Allah SWT menyuruhmu menyampaikan amanat kepada yang berhak menerimanya, dan apabila kamu menetapkan hukum di antara manusia hendaknya kamu menetapkannya dengan adil. Sungguh, Allah sebaik-baik yang memberi pengajaran kepadamu. Sungguh, Allah Maha Mendengar, Maha Melihat"(QS.An-Nisaa' ayat 58)".*

Berdasarkan firman Allah SWT. Dalam surat An-Nisaa' ayat 58 menjelaskan bahwa ayat "Sesungguhnya Allah menyuruh kamu untuk menyampaikan amanat (kewajiban-kewajiban yang dipercayakan dari seseorang kepada yang berhak menerimanya) turun ketika Ali r.a. hendak mengambil kunci Ka'bah dari Usman bin Thalhah Al-Hajabi (penjaga kunci) secara paksa yakni ketika Nabi SAW. datang ke Mekah pada tahun pembebasan. Usman ketika itu tidak mau memberikannya lalu katanya, "Seandainya saya tahu bahwa ia Rasulullah SAW tentulah saya tidak akan menghalanginya." Maka Rasulullah SAW. pun menyuruh mengembalikan kunci itu padanya seraya bersabda, "Terimalah ini untuk selama-lamanya tiada putus-putusnya!" Usman merasa heran atas hal itu lalu dibacakannya ayat tersebut sehingga Usman pun masuk Islam. Ketika akan meninggal kunci itu diserahkan kepada saudaranya Syaibah. Ayat ini

walaupun datang dengan sebab khusus tetapi umumnya berlaku disebabkan persamaan di antaranya (dan apabila kamu mengadili di antara manusia) maka Allah menitahkanmu (agar menetapkan hukum dengan adil. Sesungguhnya Allah amat baik sekali) pada *ni`immaa* diidgamkan *mim* kepada *ma*, yakni *nakirah maushufah* artinya *ni`ma syaian* atau sesuatu yang amat baik (nasihat yang diberikan-Nya kepadamu) yakni menyampaikan amanat dan menjatuhkan putusan secara adil. Sesungguhnya Allah Maha Mendengar akan semua perkataan lagi Maha Melihat segala perbuatan.

Amanat adalah segala sesuatu baik bersifat materi maupun non-materi yang dipercayakan pemberi kepada penerima untuk selalu dijaga dan ditunaikan dengan sebaik-baiknya. Dalam Al-Qur'an surah Al-Anfal/8:27, telah dijelaskan pentingnya menjaga amanah.

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَخُوْنُوا اللّٰهَ وَالرَّسُوْلَ وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ

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

Berdasarkan firman Allah SWT. Dalam surat Al-Anfal ayat 27 menjelaskan bahwa "janganlah kamu menghianati amanat-amanat". Agama Islam memerintahkan bahwa apapun merupakan hal penting yang perlu dijaga sehingga dapat diartikan bahwa sebuah pesan merupakan amanat yang perlu dijaga kerahasiaannya.

Sehubungan dengan ayat di atas, Rasulullah SAW juga memberi penjelasan atau keterangan dalam hadits yang diriwayatkan oleh Abu Daud yaitu sebagai berikut:

حَدَّثَنَا مُحَمَّدُ بْنُ الْعَلاَءِ، وَأَحْمَدُ بْنُ إِبْرَاهِيمَ، قَالاَ حَدَّثَنَا طَلْقُ بْنُ غَنَّامٍ، عَنْ شَرِيكٍ، - قَالَ ابْنُ الْعَلاَءِ وَقَيْسٍ عَنْ أَبِي حُصَيْنٍ، عَنْ أَبِي صَالِحٍ، عَنْ أَبِي هُرَيْرَةَ، قَالَ قَالَ رَسُولُ اللَّهِ صلى الله عليه وسلم " أَدِّ الأَمَانَةَ إِلَى مَنِ ائْتَمَنَكَ وَلاَ تَخُنْ مَنْ خَانَكَ "

*"Tunaikanlah amanah terhadap orang yang memberi amanah padamu dan janganlah berkhianat terhadap orang yang telah mengkhianatimu" (HR. Abu Daud)* (Katsir, 2004).

Makna hadist ini umum mencakup semua jenis amanat yang diharuskan bagi manusia untuk menyampaikannya. Amanat tersebut antara lain menyangkut hak-hak Allah SWT. atas hamba-hambanya, seperti shalat, zakat, puasa, kifarat dan semua jenis nazar dan lain sebagainya (yang semisal yang dipercaya kepada seseorang dan tidak seorang hamba pun yang dipercayakan kepada seseorang dan tidak seorang hamba pun yang melihatnya). Juga termasuk pula hak-hak yang menyangkut hamba-hamba Allah sebagian dari mereka atas sebagian yang lain, seperti semua titipan dan lain-lainnya yang merupakan subjek titipan tanpa ada bukti maka Allah SWT memerintahkan agar hal tersebut ditunaikan kepada yang berhak menerimanya. Barang siapa yang tidak melakukan hal tersebut di dunia, maka ia akan dituntut nanti di hari kiamat dan dihukum karenanya (Ad-Dimisyqi, 2001).

## 2.3 Kajian Topik dengan Teori Pendukung

Pada penelitian ini menggunakan beberapa teori pendukung, seperti Algoritma *Cipher Block Chaining* merupakan salah satu algoritma substitusi yang sulit dipecahkan. Bentuk umum *Cipher Block Chaining* bekerja dengan mode blok yaitu melakukan pengelompokkan biner-biner *plaintext* menjadi beberapa kelompok sesuai dengan ketentuan yang ditetapkan oleh pengguna. Lalu

melakukan proses enkripsi dan dekripsi pada setiap blok/kelompok biner *plaintext* atau *ciphertext* dimana setiap blok saling ketergantungan dengan blok lainnya. Kemudian melakukan pergeseran bit dengan jumlah bit yang ditentukan, maka hasil pergeseran inilah yang menjadi hasil akhir dari proses enkripsi dan dekripsi.

Grup simetri $S_4$ adalah grup semua permutasi dari empat elemen. Definisikan $S_4$ sebagai himpunan semua fungsi satu-satu dari {1,2,3,4} ke dirinya sendiri (Febyola, 2017). Proses enkripsi dan dekripsi dengan menggunakan Transposisi Grup Simetri $S_4$ untuk mengamankan informasi akan menghasilkan *ciphertext* yang tidak dibaca oleh orang yang tidak berhak menerimanya. Langkah awal yang dilakukan penulis yaitu menentukan unsur-unsur dari grup simetri-$n$ dan menentukan order dari masing-masing unsur tersebut, kemudian membentuk kunci menggunakan grup simetri-$n$. Transposisi grup gimetri $S_4$ merupakan salah satu contoh grup yang dapat digunakan pada protokol perjanjian kunci Stickel.

# BAB III
# METODE PENELITIAN

## 3.1 Jenis Penelitian

Metode yang digunakan dalam penelitian ini adalah menggunakan penelitian kualitatif yaitu penelitian yang dilakukan dengan cara mengumpulkan data dan informasi yang berhubungan dengan penelitian dengan bantuan materi yang terdapat dalam perpustakaan, seperti buku-buku, jurnal dan lain-lain tentang enkripsi serta dekripsi pada pesan teks beserta algoritma-algoritmanya.

## 3.2 Pra Penelitian

Data yang digunakan oleh penulis berupa data primer dan data sekunder. Data primer pada penelitian ini didapatkan dari hasil pengamatan penulis berupa unsur-unsur dari subgrup pada grup simetri. Sedangkan data sekunder yang digunakan oleh penulis berupa definisi, teorema dan sifat-sifat yang berkaitan dengan pengambilan kesimpulan pada penelitian ini.

## 3.3 Tahapan Penelitian

Bentuk umum *Cipher Block Chaining* bekerja dengan mode blok yaitu melakukan pengelompokan biner-biner *plaintext* menjadi beberapa kelompok sesuai dengan ketentuan yang ditetapkan oleh pengguna (orang yang mengenkripsikan pesan).

Secara umum untuk mencapai tujuan yang diinginkan maka tahapan-tahapan yang digunakan dalam penelitian ini adalah:

1. Memaparkan proses penyandian *Cipher Block Chaining* dan penyandian transposisi grup simetri

2. Menyusun proses penyandian menggunakan *Cipher Block Chaining* dan penyandian transposisi grup simetri

a. Proses enkripsi pada penyandian *Cipher Block Chaining* dan penyandian transposisi grup simetri sebagi berikut:

1) Menentukan *plaintext*
2) Menentukan Kunci *Cipher Block Chaining*
3) Menentukan *initialization vector* ($C_0$)
4) Mengelompokkan biner-biner *plaintext*, IV/$C_0$ dan kunci ke dalam blok sesuai dengan jumlah bit per kelompok yang telah ditentukan sebelumnya
5) Melakukan proses enkripsi pada setiap blok/kelompok biner *plaintext* dimana setiap blok saling ketergantungan dengan blok yang lain.
6) Lakukan proses pergeseran bit *plaintext* sesuai dengan jumlah bit yang diterapkan oleh pengguna, hasil pergeseran inilah yang menjadi hasil akhir dari proses enkripsi dan memperoleh *ciphertext1*.
7) Menerapkan algoritma transposisi grup simetri pada proses pembentukan kunci dengan menggunakan skema protokol perjanjian kunci Stickel.
8) Membagi *ciphertext1* menjadi blok-blok.
9) Mengenkripsi *ciphertext1* dan kunci yang sudah disepakati pada setiap blok/kelompok biner dengan mengunakan protokol perjanjian kunci Stickel dengan teknik transposisi (permutasi) dan memperoleh *ciphertext* akhir.

b. Proses dekripsi pada penyandian *Cipher Block Chaining* dan penyandian transposisi grup simetri sebagi berikut:

1) Menginverskan kunci transposisi grup simetri
2) Membagi *ciphertext* pada setiap blok/kelompok biner.
3) Mengenkripsikan *ciphertext* pada setiap blok/kelompok menggunakan invers kunci transposisi grup simetri dengan teknik transposisi (permutasi) dan memperoleh *ciphertext1*.

3. Mendekripsi ulang *ciphertext1* dengan menggunakan kunci *Cipher Block Chaining* dan menghasilkan *plaintext.*

# BAB IV
# HASIL DAN PEMBAHASAN

Sistem kriptografi atau sering disebut dengan *cipher* merupakan suatu sistem atau kumpulan aturan-aturan yang digunakan untuk melakukan enkripsi dan dekripsi. Sistem kriptografi simetri adalah sistem kriptografi yang menggunakan kunci enkripsi dan dekripsi yang sama. Sistem ini mengharuskan dua pihak yang berkomunikasi menyepakati suatu kunci rahasia yang sama sebelum keduanya saling berkomunikasi. Keamanan dari sistem ini tergantung pada kunci, membocorkan kunci berarti bahwa orang lain yang berhasil mendapatkan kunci dapat mendekripsi *ciphertext*.

## 4.1 Proses Penyandian Algoritma *Cipher Block Chaining*

Bentuk umum *Cipher Block Chaining* bekerja dengan mode blok yaitu melakukan pengelompokkan biner-biner *plaintext* menjadi beberapa kelompok sesuai dengan ketentuan yang ditetapkan oleh pengguna (orang yang mengenkripsikan pesan).

Pertama adalah mencari biner dari setiap huruf pada *ciphertext* dan *keyword*

**Tabel 4.1 konversi Teks ke Desimal dan Biner**

| *Ciphertext* | Desimal | Biner |
|---|---|---|
| D | 68 | 01000100 |
| I | 73 | 01001001 |
| A | 65 | 01000001 |
| H | 72 | 01001000 |

| *Keyword* | Desimal | Biner |
|---|---|---|
| X | 88 | 01011000 |
| Y | 89 | 01011001 |

| IV/$C_0$ | Desimal | Biner |
|---|---|---|
| A | 65 | 01000001 |
| B | 66 | 01000010 |

Kedua adalah pengelompokan dari hasil dan *keyword* untuk dioperasi-enkripsikan

| *Ciphertext* | Desimal | Biner |
|---|---|---|
| DI | 68 73 | 01000100 01001001 |
| AH | 65 72 | 01000001 01001000 |

| *Keyword* | Desimal | Biner |
|---|---|---|
| XY | 88 89 | 01011000 01011001 |

| IV/C0 | Desimal | Biner |
|---|---|---|
| AB | 65 66 | 01000001 01011001 |

Ketiga adalah proses enkripsi pada *Cipher Block Chaining* (CBC) dinyatakan dengan rumus $C_i = E_K(P_i \oplus C_{i-1})$ adapun proses enkripsi adalah sebagai berikut:

$C_i = E_K(P_i \oplus C_{i-1})$

$CP_1$ = Blok P1$\oplus C_0$

= 01000100 01001001

= 01000001 01000010 ⊕

= 00000101 00001011

= 01011000 01011001 ⊕

= 01011101 01010010

Geser empat bit kekiri 11010101 00100101 → Õ%

$CP_2$ =Blok P2⊕$C_{2-1}$

= 01000001 01001000

= 11010101 00100101 ⊕

= 10010100 01101101

= 01011000 01011001 ⊕

= 11001100 00110100

Geser empat bit kekiri 11000011 01001100 → Á***L***

maka, hasil enkripsinya adalah Õ%Á***L***

Proses dekripsi pada *Cipher Block Chaining* (CBC) dinyatakan dengan rumus $P_i = D_K(C_i) \oplus C_{i-1}$ sebelum melakukan dekripsi *ciphertext* menjadi *plaintext* terlebih dahulu menggeser 4 bit *ciphertext* dari kanan. Adapun proses dekripsinya sebagai berikut:

$P_i = D_K(C_i) \oplus C_{i-1}$

$C_0$= 01000001 01000010

$C_1$= 11010101 00100101 → geser empat bit kekanan 01011101 01010010

$C_2$= 11000011 01001100 → geser empat bit kekanan 11001100 00110100

$P_1 = C_1 \oplus C_0$

= 01011101 01010010

= <u>01000001 01000010</u> ⊕

= 00011100 00010000

= <u>01011000 01011001</u> ⊕

= 01000100 01001001

hasilnya adalah **DI**

$P_2 = C_2 \oplus C_{2-1}$

= 11001100 00110100

= <u>11010101 00100101</u> ⊕

= 00011001 00010001

= <u>01011000 01011001</u> ⊕

= 01000001 01001000

hasilnya adalah **AH**

maka, hasil dekripsinya adalah **DIAH**

## 4.2 Kajian Integrasi Algoritma *Cipher Block Chaining* (CBC) dengan Al-Qur'an/Hadits

Algortima *Cipher Block Chaining* merupakan salah satu algoritma substitusi yang sulit dipecahkan. Sistem ini dibuat dengan tujuan mengimplementasikan enkripsi dan dekripsi teks berdasarkan algoritma *Cipher Block Chaining* (CBC) dengan tujuan dapat memperlihatkan prosedur dan hasil yang didapatkan untuk mengamankan pesan teks, khususnya prosedur yang dilakukan pada kegiatan penyandian dan pengembalian teks ke bentuk semula. Input yang dibutuhkan oleh sistem adalah teks yang diinput langsung oleh *user* dapat diinputkan merupakan karakter-karakter ASCII.

Sehubungan dengan analisis algoritma *Cipher Block Chaining* diatas bahwa algoritma ini dapat dibandingkan dengan model kepemimpinan Ratu Balqis dalam A-Qur'an. Ketika itu Ratu Balqis mendapat kiriman surat dari Nabi Sulaiman sebagaimana disebutkan dalam QS. An-Naml (27):32:

قَالَتْ يٰٓاَيُّهَا الْمَلَؤُا اَفْتُوْنِيْ فِيْٓ اَمْرِيْۚ مَا كُنْتُ قَاطِعَةً اَمْرًا حَتّٰى تَشْهَدُوْنِ

*"Dia (Balqis) berkata, "Wahai para pembesar! Berilah aku pertimbangan dalam perkaraku (ini). Aku tidak pernah memutuskan suatu perkara sebelum kamu hadir dalam majelis(ku)."*

Dari ayat tersebut, tersirat bahwa Ratu Balqis membuka surat itu kepada para pembesar-pembesarnya dari bangsanya. Isi dalam surat itu sulit untuk dipecahkan. Jika dipahami secara tekstual maka tidak akan ditemukan jawaban dari surat itu. Dan jika dipahami secara kontekstual terkait tujuan mengapa surat itu dikirm maka baru dapat dipahami maknanya sehingga mereka memulai

membahas dengan bermusyawarah bersama. Maka ketika itu pula Ratu Balqis pernah salah langkah ketika sampai di istana Nabi Sulaiman.

Begitupula dengan algoritma ini, dibuat dengan tujuan mengimplementasikan enkripsi dan dekripsi pesan untuk mengamankan informasi untuk mengharuskan dua pihak yang berkomunikasi menyepakati suatu kunci rahasia yang sama sebelum keduanya saling berkomunikasi.

## 4.3 Proses Penyandian Transposisi Grup Simetri $S_4$

Teknik transposisi (permutasi) ini menggunakan permutasi karakter, yang mana dengan menggunakan teknik ini pesan yang asli tidak dapat dibaca kecuali oleh orang yang memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula (Ariyus, 2008). Algoritma enkripsi menggunakan teknik transposisi (permutasi) dengan melakukan permutasi $\pi$ pada teks asli (*plaintext*), sedangkan algoritma dekripsi dengan melakukan invers permutasi $\pi^{-1}$ pada teks kode (*ciphertext*)

a. Proses Enkripsi Teknik Transposisi (Permutasi)

Langkah pertama dari proses enkripsi dengan teknik transposisi (permutasi) adalah membagi pesan *plaintext* menjadi per blok yang terdiri dari beberapa huruf. Kunci pada teknik transposisi (permutasi) ini menggunakan bentuk permutasi-$n$, yang mana dengan menggunakan teknik ini pesan yang asli tidak dapat dibaca kecuali oleh orang yang memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula.

b. Proses Dekripsi Teknik Transposisi (Permutasi)

Pada dasarnya proses dekripsi sama saja dengan proses enkripsi, akan tetapi pada proses ini penerima pesan ini penerima pesan mendekripsikan pesan *ciphertext* dengan menginverskan kunci yang telah disepakatin.

Berikut ini contoh proses penyandian menggunakan teknik permutasi.

Terdapat kunci untuk melakukan permutasi:

| $x$ | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ |
|---|---|---|---|---|---|
| $\pi(x)$ | $a_2$ | $a_4$ | $a_1$ | $a_5$ | $a_3$ |

dan kunci untuk invers dari permutasi tersebut:

| $x$ | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ |
|---|---|---|---|---|---|
| $\pi^{-1}(x)$ | $a_3$ | $a_1$ | $a_5$ | $a_2$ | $a_4$ |

Misalnya kita akan melakukan permutasi terhadapat kalimat dibawah ini:

SAYA SEDANG MERINDU

Terlebih dahulu kalimat tersebut dibagi menjadi 5 blok dan apabila terjadi kekurangan dari blok bisa ditambah dengan huruf yang disukai, misalkan & dan spasi dilambangkan dengan $. Hal ini berguna untuk mempersulit analisis dari kode tersebut.

SAYA$ SEDAN G$MER INDU&

Setelah dibagi menjadi 5 blok maka dengan menggunakan kunci nomor satu diatas setiap blok akan berubah menjadi seperti di bawah ini:

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

= AAS$Y

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

= EASNE

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

= $EGRM

Blok IV : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_4 & a_1 & a_5 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ I & N & D & U & \& \\ a_2 & a_4 & a_1 & a_5 & a_3 \\ N & U & I & \& & D \end{pmatrix}$

= NUI&D

sehingga diperoleh *ciphertext* yaitu:

AAS$YEASNE$EGRAMNUI&D

Sedangkan untuk proses dekripsi ciphertext dilakukan dengan cara yang sama seperti proses enkripsi namun dengan menggunakan kunci invers atau kedua yang telah ditentukan sebelumnya.

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

$$K^{-1} = \begin{pmatrix} a_2 & a_4 & a_1 & a_5 & a_3 \\ a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix}$$

$$K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_1 & a_5 & a_2 & a_4 \end{pmatrix}$$

Blok I : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_1 & a_5 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ A & A & S & \$ & Y \\ a_3 & a_1 & a_5 & a_2 & a_4 \\ S & A & Y & A & \$ \end{pmatrix}$

= SAYA$

Blok II : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_1 & a_5 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ E & A & S & N & E \\ a_3 & a_1 & a_5 & a_2 & a_4 \\ S & E & D & A & N \end{pmatrix}$

= SEDAN

Blok III : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_1 & a_5 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ \$ & E & G & R & M \\ a_3 & a_1 & a_5 & a_2 & a_4 \\ G & \$ & M & E & R \end{pmatrix}$

= G$MER

Blok IV : $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_1 & a_5 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ N & U & I & \& & D \\ a_3 & a_1 & a_5 & a_2 & a_4 \\ I & N & D & U & \& \end{pmatrix}$

= INDU&

sehingga diperoleh plaintext yaitu:

SAYA SEDANG MERINDU

## 4.4 Kajian Integrasi Algoritma Transposisi Grup Simetri $S_4$ dengan Al-Qur'an/Hadits.

Algoritma grup simetri-*n* merupakan salah satu algoritma teknik transposisi (permutasi). Langkah awal yang dilakukan penulis yaitu menentukan unsur-unsur dari grup simetri-*n* dan menentukan order dari masing-masing unsur tersebut, kemudian membentuk kunci menggunakan grup simetri-*n*. Grup simetri $S_4$ merupakan salah satu contoh grup yang dapat digunakan pada protokol perjanjian kunci Stickel. Penggunaan grup pada protokol Stickel ini dapat diperumum menjadi sebarang semigrup. Kunci tersebut yang digunakan pada proses enkripsi dan dekripsi. Proses enkripsi dan dekripsi bertujuan agar pesan yang dikirim tidak dibaca oleh orang yang tidak berhak menerimanya.

Sehubungan dengan analisis di paragraf sebelumnya, di dalam Al-Qur'an juga dijelaskan tentang anjuran untuk menjaga pesan. Dengan kata lain, pesan adalah sebuah amanat yang harus disampaikan kepada penerimanya, sebagaimana dalam firman Allah SWT. Dalam Al-Qur'an surat an-Nisa'(4):58:

اِنَّ اللّٰهَ يَأْمُرُكُمْ اَنْ تُؤَدُّوا الْاَمٰنٰتِ اِلٰٓى اَهْلِهَاۙ وَاِذَا حَكَمْتُمْ بَيْنَ النَّاسِ اَنْ تَحْكُمُوْا بِالْعَدْلِ ۗ اِنَّ اللّٰهَ نِعِمَّا يَعِظُكُمْ بِهٖۗ ۗ اِنَّ اللّٰهَ كَانَ سَمِيْعًاۢ بَصِيْرًا

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

Berdasarkan firman Allah SWT. Dalam surat An-Nisaa' ayat 58 menjelaskan bahwa Allah menyuruh manusia untuk menyampaikan amanat

kepada orang yang berhak menerimanya. Selain orang yang berhak menerima amanat tersebut maka orang lain tidak boleh mengetahuinya.

Begitupula dengan algoritma ini, dibuat dengan tujuan mengimplementasikan enkripsi dan dekripsi pesan untuk mengamankan informasi dan untuk mempersulit masalah pemecahan pesan, penulis menggunakan grup simetri $S_4$.

## 4.5 Proses Enkripsi Pesan

### 4.5.1 Algoritma Ekripsi *Cipher Block Chaining* dan Algoritma Transposisi Grup Simetri $S_4$

Adapun langkah-langkah dalam penyelesaian algoritma *Cipher Block Chaining* (CBC) dan transposis grup simetri $S_4$ untuk proses enkripsi adalah sebagai berikut:

1. Menginput *plaintext*, kemudian konversikan nilai desimal ke biner.
2. Menentukan nilai jumlah bit setiap kelompok, kunci dan *initialization vector* $(C_0)$.
3. Mengelompokkan biner-biner *plaintext* kedalam blok sesuai dengan jumlah bit per kelompok yang telah ditentukan sebelumnya.
4. Melakukan proses enkripsi pada setiap blok/kelompok biner *plaintext* dimana setiap blok saling ketergantungan dengan blok yang lain.
5. Lakukan proses pergeseran bit *plaintext* sesuai dengan jumlah bit yang diterapkan oleh *user*.
6. Menerapkan algoritma transposisi grup simetri pada proses pembentukan kunci dengan menggunakan skema protokol perjanjian Stickel.

7. Membagi *ciphertext1* menjadi blok-blok dan mengenkripsi *ciphertext1* dan kunci yang sudah disepakati pada blok biner dengan menggunakan protokol perjanjian kunci Stickel dengan teknik transposisi (permutasi) dan memperoleh *ciphertext*.

### 4.5.2 Penerapan *Algoritma Cipher Block Chaining* dan Transposisi Grup Simetri $S_4$ untuk Proses Enkripsi pada Pengamanan Pesan Teks

Proses enkripsi pada *Cipher Block Chaining* (CBC) dinyatakan dengan rumus $C_i = E_K(P_i \oplus C_{i-1})$. Pada pembahasan ini penulis menggunakan *plaintext*= RINDU_IBU. yang akan disandikan menjadi *ciphertext*. *Plaintext* tersebut diubah dahulu ke desimal dan hasilnya sebagai berikut:

1. *Plaintext*= **RINDU_IBU.**

| *Plaintext* | Desimal | Biner |
|---|---|---|
| R | 82 | 01010010 |
| I | 73 | 01001001 |
| N | 79 | 01001110 |
| D | 68 | 01000100 |
| U | 85 | 01010101 |
| _ | 95 | 01011111 |
| I | 73 | 01001001 |
| B | 66 | 01000010 |
| U | 85 | 01010101 |
| . | 46 | 00101110 |

Kunci berikut terlebih dahulu dan diubah ke dalam desimal setelah itu diubah ke dalam bentuk biner.

*Keyword*= AB

| *Keyword* | Desimal | Biner |
|---|---|---|
| A | 65 | 01010000 |
| B | 66 | 01000010 |

Berikut penentuan *initialization vector* atau $C_0$. Dalam penentuan, $C_0$ dapat ditentukan sendiri.

IV/$C_0$=XY

| IV/$C_0$ | Desimal | Biner |
|---|---|---|
| X | 88 | 01011000 |
| Y | 89 | 01011001 |

Selanjutnya adalah pengelompokkan dari hasil dan *keyword* untuk dioperasi enkripsikan.

Pengelompokkan *plaintext*

| *Plaintext* | Biner |
|---|---|
| RI | 01010010 01001001 |
| ND | 01001110 01000100 |
| U_ | 01010101 01011111 |

| | |
|---|---|
| IB | 01001001 01000010 |
| U. | 01010101 00101110 |

Pengelompokkan *Keyword*

| *Keyword* | Biner |
|---|---|
| AB | 01010000 01000010 |

Pengelompokkan IV/$C_0$= *initialization vector*

| IV/$C_0$ | Biner |
|---|---|
| XY | 01011000 01011001 |

Kemudian lakukan proses enkripsi dan dekripsi. Adapun susunan dari algoritma *Cipher Block Chaining* (CBC) dalam proses enkripsi adalah sebagai berikut:

$C_i \quad = E_K(P_i \oplus C_{i-1})$

$CP_1$ = Blok P1$\oplus C_0$

= 01010010 01001001

= <u>01011000 01011001 $\oplus$</u>

= 00001010 00010000

= <u>01010000 01000010 $\oplus$</u>

= 01011010 01010010

geser empat bit kekiri 10100101 00100101 → ¥%

$CP_2$ =Blok P2⊕$C_{2-1}$

= 01001110 01000100

= <u>10100101 00100101</u> ⊕

= 11101011 01100001

= <u>01010000 01000010</u> ⊕

= 10111011 00100011

geser empat bit kekiri 10110010 00111011→ ²;

$CP_3$ =Blok P3⊕$C_{3-1}$

= 01010101 01011111

= <u>10110010 01111011</u> ⊕

= 11100111 00100100

= <u>01010000 01000010</u> ⊕

= 10110111 01100110

geser empat bit kekiri 01110110 01101011→ vk

$CP_4$ =Blok P4⊕$C_{4-1}$

= 01001001 01000010

= <u>01110110 01101011</u> ⊕

= 00111111 00101001

= 01010000 01000010 ⊕

= 01101111 01101011

geser empat bit kekiri 11110110 10110110→ Ö¶

$CP_5$ =Blok P5⊕$C_{5-1}$

= 01010101 00101110

= 11110110 10110110 ⊕

= 10100011 10011000

= 01010000 01000010 ⊕

= 11110011 11011010

geser empat bit kekiri 00111101 10101111→ =⁻

sehingga diperoleh *ciphertext1* adalah: ¥%²; *vk*Ö¶ =⁻

Berdasarkan grup simetri $S_4$ dapat diterapkan algoritma untuk melakukan pembentukan kunci seperti pada tabel sebagai berikut:

**Tabel 4.2 Skema Protokol Perjanjian Kunci Stickel atas Grup Simetri $S_4$**

<table>
<tr><td colspan="2">Pengirim pesan atau penerima pesan mempublikasikan suatu grup simetri $S_4$ dan $\sigma_1, \sigma_2 \epsilon S_4$<br>Pilih $\sigma_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix}$ dan $\sigma_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_4 & a_1 & a_3 \end{pmatrix}$</td></tr>
<tr><td>Pengirim pesan</td><td>Penerima pesan</td></tr>
<tr><td>1. Pengirim pesan memilih secara rahasia suatu bilangan asli $n$ dan m<br>Pilih: $n = 3$ dan $m = 2$<br>2. Pengirim pesan menghitung $x = {\sigma_1}^n \circ {\sigma_2}^m$<br>$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix}^3 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_4 & a_1 & a_3 \end{pmatrix}^2$<br>$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix}$<br>$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix}$</td><td>1. Penerima pesan memilih secara rahasia suatu bilangan asli $r$ dan s<br>Pilih: $r = 3$ dan $s = 1$<br>2. Penerima pesan menghitung $y = {\sigma_1}^r \circ {\sigma_2}^s$<br>$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix}^3 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_4 & a_1 & a_3 \end{pmatrix}^1$<br>$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix}$<br>$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix}$</td></tr>
</table>

| | |
|---|---|
| $x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_1 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_2 & a_1 \end{pmatrix}$<br>$x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_4 & a_3 & a_2 \end{pmatrix}$<br>3. Pengirim pesan mengirim $x$ kepada pengirim pesan<br>4. Pengirim pesan menerima $y$ dari penerima pesan<br>5. Pengirim pesan menghitung<br>$K_1 = a^n \circ y \circ b^m$<br>$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix}^3 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_1 & a_2 & a_4 \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_4 & a_1 & a_3 \end{pmatrix}^2$<br>$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_1 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_1 & a_2 & a_4 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_2 & a_1 \end{pmatrix}$<br>$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_2 & a_3 & a_1 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_2 & a_1 \end{pmatrix}$<br>$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_2 & a_4 \end{pmatrix}$ | $y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_1 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_4 & a_1 & a_3 \end{pmatrix}$<br>$y = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_1 & a_2 & a_4 \end{pmatrix}$<br>3. Penerima pesan mengirim $y$ kepada pengirim pesan<br>4. Penerima pesan menerima $x$ dari pengirim pesan<br>5. Penerima pesan menghitung<br>$K_2 = a^r \circ x \circ b^s$<br>$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \end{pmatrix}^3 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_4 & a_3 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_4 & a_1 & a_3 \end{pmatrix}^1$<br>$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_1 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_4 & a_3 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_4 & a_1 & a_3 \end{pmatrix}$<br>$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_1 & a_4 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_4 & a_1 & a_3 \end{pmatrix}$<br>$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_2 & a_4 \end{pmatrix}$ |
| Pengirim pesan dan penerima pesan telah menyepakati kunci rahasia yang sama yaitu<br>$K = K_1 = K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_2 & a_4 \end{pmatrix}$ | |

Berikut adalah proses enkripsi pada operasi Transposisi grup simetri $S_4$:

a. Proses Ekripsi

Pada langkah proses enkripsi pesan selanjutnya adalah mengimput hasil enkripsi pesan dari operasi *Cipher Block Chaining* ke dalam operasi transposisi grup simetri $S_4$ *ciphertext1* yang ditulis yaitu:

¥%²; *vk*Ö¶ =⁻

Kemudian *ciphertext1* dienkripsi terlebih dahulu oleh pesan dengan menggunakan kunci yang sudah disepakati yaitu:

$$K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_2 & a_4 \end{pmatrix}$$

Karena kunci yang digunakan adalah bentuk permutasi $P_4$ maka *ciphertext* tersebut dibagi menjadi 4 blok dan apabila terjadi kekurangan dari blok bisa ditambah dengan huruf yang disukai, misalkan & dan spasi dilambangkan dengan $. Hal ini berguna untuk mempersulit analisis dari kode tersebut.

| ¥%²; | *vk*Ö¶ | =⁻ && |
|---|---|---|

Setelah dibagi menjadi 4 blok maka dengan menggunakan kunci diatas setiap blok akan berubah menjadi seperti di bawah ini:

Blok I : $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ ¥ & \% & ² & ; \\ a_1 & a_3 & a_2 & a_4 \\ ¥ & ² & \% & ; \end{pmatrix}$

= ¥²%;

Blok II: $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ v & k & Ö & ¶ \\ a_1 & a_3 & a_2 & a_4 \\ v & Ö & k & ¶ \end{pmatrix}$

= *v*Ö*k*¶

Blok III: $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ = & - & \& & \& \\ a_1 & a_3 & a_2 & a_4 \\ = & \& & - & \& \end{pmatrix}$

= =&-&

Dari proses enkripsi di atas diperoleh *ciphertext* akhir yang akan dikirim kepada penerima pesan yaitu:

¥²%; *v*Ö*k*¶ =&-&

## 4.6 Proses Dekripsi Pesan

### 4.6.1 Algoritma Dekripsi Transposisi Grup Simetri $S_4$ dan Algoritma *Cipher Block Chaining*

Adapun langkah-langkah dalam penyelesaian algoritma transposisi grup simetri $S_4$ ke dalam *Cipher Block Chaining* (CBC) dalam proses enkripsi adalah sebagai berikut:

1. Menginverskan kunci transposisi grup simetri $S_4$
2. Membagi *ciphertext* pada setiap blok/kelompok biner.
3. Mengdenkripsi *ciphertext* pada blok/kelompok menggunakan invers kunci transposisi grup simetri dengan teknik transposisi (permutasi) dan memperoleh *ciphertext1*.
4. Mendekripsi ulang *ciphertext1* dengan menggunakan algoritma *Cipher Block Chaining* pada proses dekripsi dan menghasilkan *plaintext*.

### 4.6.2 Penerapan Transposisi Grup Simetri $S_4$ dan *Cipher Block Chaining* untuk Proses Enkripsi pada Pengamanan Pesan Teks

Proses selanjutnya adalah proses dekripsi. Setelah memperoleh *ciphertext* dari pengirim pesan menggunakan algoritma trasnposisi grup simetri $S_4$, maka penerima pesan mengubahnya menjadi *plaintext* menggunakan trasnposisi grup simetri $S_4$ yaitu sebagai berikut:

$$¥^{2}\%;v\ddot{O}k¶ = \&^{-}\&$$

Pada proses ini juga dibutuhkan kunci $K$ untuk mendekripsikan pesan tersebut. Dalam proses ini berbeda dengan proses enkripsi, pada proses ini

pendekripsian *ciphertext* dengan menginverskan kunci yang telah disepakati yaitu:

$$K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_2 & a_4 \end{pmatrix}$$

*ciphertext* tersebut selanjutnya diubah ke dalam blok-blok yang terdiri dari 4 karakter sehingga diperoleh sebagai berikut:

| ¥²%; | *v*Ök¶ | = &-& |
|---|---|---|

kemudian proses dekripsi dilakukan satu persatu dari blok tersebut dengan menggunakan kunci invers.

Blok I: $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ ¥ & ² & \% & ; \\ a_1 & a_3 & a_2 & a_4 \\ ¥ & \% & ² & ; \end{pmatrix}$

= ¥%²;

Blok II: $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ v & Ö & k & ¶ \\ a_1 & a_3 & a_2 & a_4 \\ v & k & Ö & ¶ \end{pmatrix}$

= *vk*Ö¶

Blok III: $K^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_3 & a_2 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ = & & - & \& \\ a_1 & a_3 & a_2 & a_4 \\ = & - & \& & \& \end{pmatrix}$

= =-&&

dari proses dekripsi di atas diperoleh pesan *plaintext1* yaitu:

¥%²; *vk*Ö¶ = -&&

Proses dekripsi pada *Cipher Block Chaining* (CBC) dinyatakan dengan rumus $P_i = D_K(C_i) \oplus C_{i-1}$ sebelum melakukan dekripsi *ciphertext* menjadi *plaintext* terlebih dahulu menggeser 4 bit *ciphertext* dari kanan. Adapun proses dekripsinya sebagai berikut:

$P_i = D_K(C_i) \oplus C_{i-1}$

$C_0$= 01011000 01011001

$C_1$= 10100101 00100101 → geser empat bit kekanan 01011010 01010010

$C_2$= 10110010 00111011→ geser empat bit kekanan 10111011 00100011

$C_3$= 01110110 01101011→ geser empat bit kekanan 10110111 01100110

$C_4$= 11110110 10110110→ geser empat bit kekanan 01101111 01101011

$C_5$= 00111101 10101111→ geser empat bit kekanan 11110011 11011010

$P_1 = C_1 \oplus C_0$

= 01011010 01010010

= <u>01011000 01011001</u> ⊕

= 00000010 00001011

= <u>01010000 01000010</u> ⊕

= 01010010 01001001

hasilnya adalah **RI**

$P_2 = C_2 \oplus C_{2-1}$

= 10111011 00100011

= 10100101 00100101 $\oplus$

= 00011110 00000110

= 01010000 01000010 $\oplus$

= 01001110 01000100

hasilnya adalah **ND**

$P_3 = C_3 \oplus C_{3-1}$

= 10110111 01100110

= 10110010 00111011 $\oplus$

= 00000101 01011101

= 01010000 01000010 $\oplus$

= 01010101 00011111

hasilnya adalah **U_**

$P_4 = C_4 \oplus C_{4-1}$

= 01101111 01101011

= 01110110 01101011 $\oplus$

= 00011001 00000000

= 01010000 01000010 $\oplus$

= 01001001 01000010

hasilnya adalah **IB**

$P_5 = C_5 \oplus C_{5-1}$

= 11110011 11011010

= 11110110 10110110 $\oplus$

= 00000101 01101100

= 01010000 01000010 $\oplus$

= 01010101 00101110

hasilnya adalah **U.**

sehingga diperoleh *plaintext* awal adalah **RINDU_IBU.**.

# BAB V
# PENUTUP

## 5.1 Kesimpulan

Berdasarkan hasil dan pembahasan yang dilakukan pada bab sebelumnya, maka dapat diambil kesimpulan sebagai berikut:

1. Proses enkripsi pertama dilakukan pada *plaintext* menggunakan algoritma *Cipher Block Chaining* menggunakan persamaan $C_i = E_K\ (P_i \oplus C_{i-1})$, $i = 1,2,\dots,m$ hasil enkripsi tersebut dienkripsi kembali menggunakan transposisi grup simetri $S_4$. Karena kunci yang digunakan adalah bentuk permutasi $P_4$ maka *plaintext* tersebut dibagi menjadi 4 blok kemudian proses enkripsi dilakukan satu persatu dari blok tersebut, sehingga diperoleh *ciphertext1*.
2. Proses dekripsi pertama *ciphertext1* dilakukan dengan transposisi grup simetri $S_4$ menggunakan invers dari kunci permutasi $P_4$ sehingga diperoleh pesan *ciphertext*. *Ciphertext* kemudian didekripsi lagi menggunakan algoritma *Cipher Block Chaining* dengan persamaan $P_i = D_K(C_i) \oplus C_{i-1}, i = 1,2,\dots,m$, sehingga diperoleh *plaintext* awal.

## 5.2 Saran

Pada penelitian ini membahas tentang proses enkripsi dan dekripsi pesan menggunakan algoritma *Cipher Block Chaining* dan transposisi grup simetri $S_4$ pada pengamanan pesan teks. Penelitian transposisi grup simetri hanya dibahas sampai $S_4$, maka pada penelitian selanjutnya bisa menggunakan $S_n$ dan menggunakan aplikasi program komputer agar tinggat keamanannya lebih tinggi.

## DAFTAR PUSTAKA


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

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

Andriani, Devi. (2017). *"perancangan aplikasi penyandian teks dengan menggunakan algoritma chiper block chaining".* Jurnal Teknik Informatika Unika: Medan.

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

Azizah, Nur. (2021). "*Impelementasi algoritma super enkripsi (hill cipher dan transposisi columnar) pada pesan teks"*. Skripsi. Malang: UIN Malang.

Dummit, D., & Foote, R. (2004). Abstract Algebra Third Edition. New York: Prentice-Hall International, Inc.

Febyola, Yanita, dan Monika Rianti Helmi. (2017). *"ORDER UNSUR DARI GRUP* $S_4$. Jurnal Matematika FMIPA UNAND Limau Manis Padang, Indonesia. Vol. VI No. 1 Hal. 142 – 147

Gazhali, al. (2019). "*Amanah Dalam Al-Qur'an (Studi Tentang Persepsi Pengurus Bem Iain Palopo)*". Skripsi. Palopo: IAIN Palopo.

Hamidy, Zainuddin. *et al*. "*terjemah hadits shahih bukhari*", Jilid IV. Jakarta: widjaya.

Halim, abdul. Zulheldi dan sobhan. (2019). "*Karakteristik Pemegang Amanah dalam Al-Qur'an"*. Jurnal Studi al-Qur'a dan Hadis. Bandung: UIN Imam Bonjol Padang.

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

Lombu, Dafirius, Siska Dame Tarihoran, dan Irwan Gulo. (2018). *"Kombinasi Mode Cipher Block Chaining Dengan Algoritma Triangle Chain Cipher Pada Penyandian Login Website.* (J-SAKTI) STMIK Budi Darma Medan, Vol (2) No. 1 Maret 2018).

Munir, R. (2019). Kriptografi. Bandung: Informatika Bandung.

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

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

Rosmala, Dewi (2012). "*Implementasi Mode Cipher Block Chaining (CBC) pada pengamanan Data"*, Vol.3, 2012

Sadikin, R. (2012). Kriptografi untuk Keamanan Jaringan. Yogyakarta: C.V ANDI OFFSET.

Wijayanto, Septedi Nugroho. (2021). *"Implementasi Algoritma Rail Pence dan Cipher Block Chainig pada Pengamanan Pesan Text". Skripsi.* Malang: UIN Malang.

Wasiatun, R. (2016). “Enkripsi dan Dekripsi Pesan Menggunakan Grup Simetri untuk Mengamankan Informasi”. Skripsi. Malang: UIN Malang.

**LAMPIRAN**

**Lampiran Tabel ASCII**

| Des | Hex | Biner | ASCII | Des | Hex | Biner | ASCII |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 00000000 | Null | 128 | 80 | 10000000 | Ç |
| 1 | 1 | 00000001 | ☺ | 129 | 81 | 10000001 | Ű |
| 2 | 2 | 00000010 | ☻ | 130 | 82 | 10000010 | É |
| 3 | 3 | 00000011 | ♁ | 131 | 83 | 10000011 | Â |
| 4 | 4 | 00000100 | ♂ | 132 | 84 | 10000100 | Ä |
| 5 | 5 | 00000101 | ♀ | 133 | 85 | 10000101 | À |
| 6 | 6 | 00000110 | ☿ | 134 | 86 | 10000110 | Å |
| 7 | 7 | 00000111 | ● | 135 | 87 | 10000111 | Ç |
| 8 | 8 | 00001000 | ◘ | 136 | 88 | 10001000 | Ê |
| 9 | 9 | 00001001 | ○ | 137 | 89 | 10001001 | Ë |
| 10 | A | 00001010 | ◙ | 138 | 8A | 10001010 | È |
| 11 | B | 00001011 | ☾ | 139 | 8B | 10001011 | Ï |
| 12 | C | 00001100 | ☽ | 140 | 8C | 10001100 | Î |
| 15 | F | 00001111 | ☼ | 143 | 8F | 10001111 | Å |
| 16 | 10 | 00010000 | ► | 144 | 90 | 10010000 | É |
| 17 | 11 | 00010001 | ◄ | 145 | 91 | 10010001 | Æ |
| 18 | 12 | 00010010 | ↕ | 146 | 92 | 10010010 | Æ |
| 19 | 13 | 00010011 | !! | 147 | 93 | 10010011 | ô |
| 20 | 14 | 00010100 | ¶ | 148 | 94 | 10010100 | ö |
| 21 | 15 | 00010101 | § | 149 | 95 | 10010101 | ò |
| 22 | 16 | 00010110 | ▬ | 150 | 96 | 10010110 | û |
| 23 | 17 | 00010111 | ↨ | 151 | 97 | 10010111 | Ù |
| 24 | 18 | 00011000 | ↑ | 152 | 98 | 10011000 | ij |
| 25 | 19 | 00011001 | ↓ | 153 | 99 | 10011001 | Ö |
| 26 | 1A | 00011010 | → | 154 | 9A | 10011010 | Ü |
| 27 | 1B | 00011011 | ← | 155 | 9B | 10011011 | ¢ |
| 28 | 1C | 00011100 | ↗ | 156 | 9C | 10011100 | £ |
| 29 | 1D | 00011101 | ↔ | 157 | 9D | 10011101 | ¥ |
| 30 | 1E | 00011110 | ▲ | 158 | 9E | 10011110 | Pt |
| 31 | 1F | 00011111 | ▼ | 159 | 9F | 10011111 | *ƒ* |
| 32 | 20 | 00100000 | Spasi | 160 | A0 | 10100000 | á |
| 33 | 21 | 00100001 | ! | 161 | A1 | 10100001 | í |
| 34 | 22 | 00100010 | “ | 162 | A2 | 10100010 | ó |
| 35 | 23 | 00100011 | # | 163 | A3 | 10100011 | ú |
| 36 | 24 | 00100100 | $ | 164 | A4 | 10100100 | ñ |

| 37 | 25 | 00100101 | % | 165 | A5 | 10100101 | Ñ |
|---|---|---|---|---|---|---|---|
| 38 | 26 | 00100110 | & | 166 | A6 | 10100110 | a |
| 39 | 27 | 00100111 | ‘ | 167 | A7 | 10100111 | o |
| 40 | 28 | 00101000 | ( | 168 | A8 | 10101000 | |
| 41 | 29 | 00101001 | ) | 169 | A9 | 10101001 | ⌐ |
| 42 | 2A | 00101010 | * | 170 | AA | 10101010 | ¬ |
| 43 | 2B | 00101011 | + | 171 | AB | 10101011 | ½ |
| 44 | 2C | 00101100 | , | 172 | AC | 10101100 | ¼ |
| 45 | 2D | 00101101 | - | 173 | AD | 10101101 | |
| 46 | 2E | 00101110 | . | 174 | AE | 10101110 | « |
| 47 | 2F | 00101111 | / | 175 | AF | 10101111 | » |
| 48 | 30 | 00110000 | 0 | 176 | B0 | 10110000 |  |
| 49 | 31 | 00110001 | 1 | 177 | B1 | 10110001 |  |
| 50 | 32 | 00110010 | 2 | 178 | B2 | 10110010 |  |
| 51 | 33 | 00110011 | 3 | 179 | B3 | 10110011 |  |
| 52 | 34 | 00110100 | 4 | 180 | B4 | 10110100 |  |
| 53 | 35 | 00110101 | 5 | 181 | B5 | 10110101 |  |
| 54 | 36 | 00110110 | 6 | 182 | *B6* | 10110110 |  |
| 55 | 37 | 00110111 | 7 | 183 | B7 | 10110111 |  |
| 56 | 38 | 00111000 | 8 | 184 | B8 | 10111000 |  |
| 57 | 39 | 00111001 | 9 | 185 | B9 | 10111001 |  |
| 58 | 3A | 00111010 | : | 186 | *BA* | 10111010 |  |
| 59 | 3B | 00111011 | ; | 187 | BB | 10111011 |  |
| 60 | 3C | 00111100 | < | 188 | BC | 10111100 |  |
| 61 | 3D | 00111101 | = | 189 | BD | 10111101 |  |
| 62 | 3E | 00111110 | > | 190 | BE | 10111110 |  |
| 63 | 3F | 00111111 | ? | 191 | BF | 10111111 |  |
| 64 | 40 | 01000000 | @ | 192 | C0 | 11000000 |  |
| 65 | 41 | 01000001 | A | 193 | C1 | 11000001 |  |
| 66 | 42 | 01000010 | B | 194 | C2 | 11000010 |  |
| 67 | 43 | 01000011 | C | 195 | C3 | 11000011 |  |
| 68 | 44 | 01000100 | D | 196 | C4 | 11000100 |  |
| 69 | 45 | 01000101 | E | 197 | C5 | 11000101 |  |
| 70 | 46 | 01000110 | F | 198 | C6 | 11000110 |  |
| 71 | 47 | 01000111 | G | 199 | C7 | 11000111 |  |
| 72 | 48 | 01001000 | H | 200 | C8 | 11001000 |  |
| 73 | 49 | 01001001 | I | 201 | C9 | 11001001 |  |
| 74 | 4A | 01001010 | J | 202 | CA | 11001010 |  |
| 75 | 4B | 01001011 | K | 203 | CB | 11001011 |  |
| 76 | 4C | 01001100 | L | 204 | CC | 11001100 |  |

| 77 | 4D | 01001101 | M | 205 | CD | 11001101 | ═ |
|---|---|---|---|---|---|---|---|
| 78 | 4E | 01001110 | N | 206 | CE | 11001110 | ╬ |
| 79 | 4F | 01001111 | O | 207 | CF | 11001111 | ╧ |
| 80 | 50 | 01010000 | P | 208 | D0 | 11010000 | ╨ |
| 81 | 51 | 01010001 | Q | 209 | D1 | 11010001 | ╤ |
| 82 | 52 | 01010010 | R | 210 | D2 | 11010010 | ╥ |
| 83 | 53 | 01010011 | S | 211 | D3 | 11010011 | ╙ |
| 84 | 54 | 01010100 | T | 212 | D4 | 11010100 | ╘ |
| 85 | 55 | 01010101 | U | 213 | D5 | 11010101 | ╒ |
| 86 | 56 | 01010110 | V | 214 | D6 | 11010110 | ╓ |
| 87 | 57 | 01010111 | W | 215 | D7 | 11010111 | ╫ |
| 88 | 58 | 01011000 | X | 216 | D8 | 11011000 | ╪ |
| 89 | 59 | 01011001 | Y | 217 | D9 | 11011001 | ┘ |
| 90 | 5A | 01011010 | Z | 218 | DA | 11011010 | ┌ |
| 91 | 5B | 01011011 | [ | 219 | DB | 11011011 | ▌ |
| 92 | 5C | 01011100 | \ | 220 | DC | 11011100 | ▄ |
| 93 | 5D | 01011101 | ] | 221 | DD | 11011101 | ▐ |
| 94 | 5E | 01011110 | ^ | 222 | DE | 11011110 | ▀ |
| 95 | 5F | 01011111 | _ | 223 | DF | 11011111 | α |
| 96 | 60 | 01100000 | ` | 224 | E0 | 11100000 | Α |
| 97 | 61 | 01100001 | A | 225 | E1 | 11100001 | Β |
| 98 | 62 | 01100010 | B | 226 | E2 | 11100010 | Γ |
| 99 | 63 | 01100011 | C | 227 | E3 | 11100011 | Π |
| 100 | 64 | 01100100 | D | 228 | E4 | 11100100 | Σ |
| 101 | 65 | 01100101 | E | 229 | E5 | 11100101 | σ |
| 102 | 66 | 01100110 | F | 230 | E6 | 11100110 | Μ |
| 103 | 67 | 01100111 | G | 231 | E7 | 11100111 | Τ |
| 104 | 68 | 01101000 | H | 232 | E8 | 11101000 | Φ |
| 105 | 69 | 01101001 | I | 233 | E9 | 11101001 | Θ |
| 106 | 6A | 01101010 | J | 234 | EA | 11101010 | Ω |
| 107 | 6B | 01101011 | K | 235 | EB | 11101011 | δ |
| 108 | 6C | 01101100 | L | 236 | EC | 11101100 | ∞ |
| 109 | 6D | 01101101 | M | 237 | ED | 11101101 | φ |
| 110 | 6E | 01101110 | N | 238 | EE | 11101110 | ε |
| 111 | 6F | 01101111 | O | 239 | EF | 11101111 | ∩ |
| 112 | 70 | 01110000 | P | 240 | F0 | 11110000 | ≡ |
| 113 | 71 | 01110001 | Q | 241 | F1 | 11110001 | ± |
| 114 | 72 | 01110010 | R | 242 | F2 | 11110010 | ≥ |
| 115 | 73 | 01110011 | S | 243 | F3 | 11110011 | ≤ |
| 116 | 74 | 01110100 | T | 244 | F4 | 11110100 | ⌠ |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **117** | **75** | **01110101** | **U** | **245** | **F5** | **11110101** | ⌡ |
| **118** | **76** | **01110110** | **V** | **246** | **F6** | **11110110** | **÷** |
| **119** | **77** | **01110111** | **W** | **247** | **F7** | **11110111** | ≈ |
| **120** | **78** | **01111000** | **X** | **248** | **F8** | **11111000** | ○ |
| **121** | **79** | **01111001** | **Y** | **249** | **F9** | **11111001** | **.** |
| **122** | **7A** | **01111010** | **Z** | **250** | **FA** | **11111010** | **.** |
| **123** | **7B** | **01111011** | **{** | **251** | **FB** | **11111011** | √ |
| **124** | **7C** | **01111100** | \| | **252** | **FC** | **11111100** | **N** |
| **125** | **7D** | **01111101** | **}** | **253** | **FD** | **11111101** | **2** |
| **126** | **7E** | **01111110** | **~** | **254** | **FE** | **11111110** | ■ |
| **127** | **7F** | **01111111** | ⌂ | **255** | **FF** | **11111111** | blank |

## RIWAYAT HIDUP

Mardiah, lahir di Pengalihan pada tanggal 05 Desember 1997. Memiliki nama panggilan Diah atau Mar. Bertempat tinggal di Parit Setia Jaya, Ds. Pancur, Kec. Keritang, Kab. Indragiri Hilir, Riau. Merupakan anak bungsu dari 3 bersaudara dari Bapak H. Moh Yunus dan Ibu Hj. Sairah.

Pendidikan yang pernah ditempuh yaitu SDS 015 Pancur dan lulus pada tahun 2010. Menempuh Pendidikan di MTs Al-Ishlahiyah Pancur, lulus pada tahun 2013. Pada tahun yang sama melanjutkan pendidikan di MA PONPES Dar EL Hikmah Pekanbaru dan lulus pada tahun 2016. Tahun 2016 melanjutkan studi di Universitas Islam Negeri Maulana Malik Ibrahim Malang menempuh Program Studi Matematika. Aktif dalam kegiatan akademis dan organisasi di luar kampus seperti HMJ “Integral” Matematika, dan PSHT UIN Malang.

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

## BUKTI KONSULTASI SKRIPSI

Nama : Mardiah
NIM : 16610003
Fakultas/Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Implementasi Algortima Cipher Block Chaining dan Transposisi Grup Simetri $S_4$ pada Pengamanan Pesan Teks
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Erna Herawati, M. Pd

| No | Tanggal | Hal | Tanda Tangan |
|---|---|---|---|
| 1 | 29 Nov 2021 | Konsultasi Judul Skripsi | 1. |
| 2 | 15 Des 2021 | Konsultasi Bab I dan Bab II | 2. |
| 3 | 23 Des 2021 | Konsultasi Bab I dan Integrasi | 3. |
| 4 | 10 Maret 2022 | Konsultasi Pembaharuan Tamplate dan ACC Seminar Proposal | 4. |
| 5 | 25 Maret 2022 | ACC Seminar Proposal | 5. |
| 6 | 19 April 2022 | Revisi Seminar Proposal | 6. |
| 7 | 08 Juni 2022 | ACC Seminar Hasil Skripsi | 7. |
| 8 | 13 Juni 2022 | ACC Seminar Hasil Skripsi | 8. |
| 9 | 23 Sep 2022 | Konsultasi Kajian Integrasi dan ACC Sidang Skripsi | 9. |
| 10 | 21 Sep 2022 | Konsultasi Revisi Seminar Hasil Skripsi dan ACC Sidang Skripsi | 10. |

Malang, 19 Oktober 2022
Mengetahui,
Ketua Program Studi Matematika

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