IMPLEMENTASI ALGORITMA RAIL FENCE DAN CIPHER BLOCK CHAINING PADA PENGAMANAN PESAN TEXT

SKRIPSI

OLEH
SEPTEDI NUGROHO WIJAYANTO
NIM. 14610096

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

IMPLEMENTASI ALGORITMA RAIL FENCE DAN CIPHER BLOCK CHAINING PADA PENGAMANAN PESAN TEXT

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
Septedi Nugroho Wijayanto
NIM. 14610096

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

IMPLEMENTASI ALGORITMA RAIL FENCE DAN CIPHER BLOCK CHAINING PADA PENGAMANAN PESAN TEXT

SKRIPSI

Oleh
Septedi Nugroho Wijayanto
NIM. 14610096

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 16 November 2020

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

Mengetahui,
Ketua Program Studi Matematika

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

IMPLEMENTASI ALGORITMA RAIL FENCE DAN CIPHER BLOCK CHAINING PADA PENGAMANAN PESAN TEXT

SKRIPSI

Oleh
Septedi Nugroho Wijayanto
NIM. 14610096

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 16 November 2020

Penguji Utama	: Dr.H.Imam Sujarwo, M.Pd	.....
Ketua Penguji	: Juhari, M.Si	.....
Sekretaris Penguji	: Muhammad Khudzaifah, M.Si	.....
Anggota Penguji	: Muhammad Nafie Jauhari, M.Si	.....

Mengetahui,
Ketua Program Studi Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama	:	Septedi Nugroho W
NIM	:	14610096
Program Studi	:	Matematika
Fakultas	:	Sains dan Teknologi
Judul Skripsi	:	IMPLEMENTASI ALGORITMA RAIL FENCE DAN CIPHER BLOCK CHAINING PADA PENGAMANAN PESAN TEXT

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

Malang, 26 April 2021
Yang membuat pernyataan,

Septedi Nugroho W
NIM.14610096

MOTTO

“Ilmu yang sejati, seperti barang berharga lainnya, tidak bisa diperoleh dengan mudah. Ia harus diusahakan, dipelajari, dipikirkan, dan lebih dari itu, harusselalu disertai doa.”

PERSEMBAHAN

Alhamdulillahi Robbil'alamin, dengan mengucap syukur kepada Allah Azza Wa Jalla, Penulis mempersembahkan skripsi ini untuk kedua orang tua saya tercinta, Bapak Amat Parjono, dan Almh. Ibu Hariyani yang selalu memberikan doa, dukungan, motivasi dan lain sebagainya yang tidak mungkin bisa penulis balas dengan balasan yang setimpal.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Segala puji bagi Allah Azza Wa Jalla Tuhan sekalian alam yang telah melimpahkan rahmat, taufik dan hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi ini sebagai syarat untuk memperoleh gelar sarjana di Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Nehgeri Maulana Malik Ibrahim Malang.

Dalam proses penyusunan skripsi ini, penulis banyak sekali mendapatkan pengarahan dan bimbingan dari berbagai pihak. Maka dari itu ucapan terima kasih yang sebesar-besarnya dari penulis sampaikan terutama kepada:

1. Prof. Dr. H. Abd Haris, M.Ag, selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Usman Pagalay, M.Si, selaku ketua Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Muhammad Khudzaifa, M.Si, selaku dosen pembimbing I yang telah banyak memberikan arahan, nasihat, motivasi, dan berbagai pengalaman yang sangat berharga kepada penulis.
5. Muhammad Nafie Jauhari, M.Si, selaku dosen pembimbing II yang telah banyak memberikan arahan dan berbagai ilmunya kepada penulis.

6. Segenap sivitas akademika Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang terutama seluruh dosen, terima kasih atas segala ilmu dan bimbingannya.
7. Bapak Parjono dan Almh. ibu Hariyani yang selalu memberikan doa, semangat, serta motivasi kepada penulis sampai saat ini.
8. Seluruh teman-teman di Program Studi Matematika angkatan 2014 (MATH EIGEN), seluruh teman-teman LDK At-Tarbiyah, seluruh teman-teman Jaisyu Qur'an Indonesia, terima kasih atas segala pengalaman berharga, kerjasama dan kebersamaan serta dukungan yang terukir indah selama ini.
   Kalian luar biasa.
9. Semua pihak yang tidak dapat disebutkan satu-persatu, yang telah membantu penulis dalam menyelesaikan skripsi ini baik moral maupun materi.

Semoga Allah Swt melimpahkan rahmat dan karunia-Nya kepada kita semua. Akhirnya penulis berharap semoga dengan rahmat dan izin-Nya mudah-mudahan skripsi ini bermanfaat bagi penulis dan bagi pembaca. Amiin.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, 26 April 2021

Penulis

DAFTAR ISI

DAFTAR GAMBAR

ABSTRAK

Wijayanto, Septedi Nugroho. 2020. **IMPLEMENTASI ALGORITMA RAIL FENCE DAN CIPHER BLOCK CHAINING PADA PENGAMANAN PESAN TEXT** Skripsi. Program Studi Matematika Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si. (II) M. Nafie Jauhari, M.Si.

Kata kunci : Enkripsi, Dekripsi ,Cipher Block Chaining, Rail Fence Cipher

Penggunan satu buah algoritma sangatlah diragukan keamanannya. Sehingga perlunya kombinasi dari beberapa algoritma agar keamanan lebih terjaga. Penggabungan dua atau lebih dari teknik subtitusi dan transposisi cipher untuk mendapatkan suatu algoritma yang lebih andal (susah dipecahkan) merupakan sebuah konsep yang dinamakan dengan Super enkripsi. Algoritma Rail Fence Cipher memiliki keunggulan dibanding algoritma lainnya karena dalam tahap proses penulisan plaintext menjadi ciphertext dapat dilakukan pada baris mana saja sehingga menambah kesulitannya dalam proses enkripsi dan dekripsi. Cipher Block Chaining merupakan sebuah algoritma kriptografi klasik yang sangat kuat dengan memiliki sifat menutupi pola plaintext dan sangat acak, hal ini dikarenakan sifat dari algoritma ini memiliki operasi 2 kali kunci serta plaintext serta kunci-kuncinya harus diubah menjadi biner agar bisa dioperasikan dan juga panjang dari kunci algoritma ini haruslah sama dengan panjang plaintext nya.

Penggunaan Super Enkripsi dengan Algoritma Cipher Block Chaining dan Rail Fence Cipher. Hal ini bertujuan untuk mendapatkan sebuah cipher yang lebih kuat dari pada hanya menggunakan satu cipher, sehingga tidak mudah untuk di crack. Enkripsi dan dekripsi dapat dilakukan dengan substitusi urutan cipher kemudian transposisi cipher, atau sebaliknya..Cipher Block Chaining memiliki sifat menutupi pola plaintext dan sangat acak Selanjutnya keamanan yang kedua didapatkan dari metode algoritma Rail Fence Cipher, dimana pesan tersebut ketika sudah disandikan akan membuat semakin sulit untuk dipecahkan.

ABSTRACT

Wijayanto, Septedi Nugroho. 2020. **IMPLEMENTATION OF RAIL FENCE AND CIPHER BLOCK CHAINING ALGORITHM ON TEXT MESSAGE SECURITY** Thesis. Department of Mathematics, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University of Malang. Advisor : (I) Muhammad Khudzaifah, M.Si. (II) M. Nafie Jauhari, M.Si.

Keywords : Encryption, Descryption, Super Encryption, Cipher Block Chaining, Rail Fence Cipher

The safety of one algorithm is doubtful. So the need for a combination of several algorithms so that security is more secure. Combining two or more of the substitution and transposition cipher techniques to get a more reliable algorithm (difficult to crack) is a concept called super encryption. The Rail Fence Cipher algorithm has advantages over other algorithms because in the process of writing plaintext into ciphertext, it can be done on any line, thus increasing the difficulty in the encryption and decryption process. Cipher Block Chaining is a classic cryptographic algorithm that is very strong with the nature of covering the plaintext pattern and is very random, this is because the nature of this algorithm has 2 key operations and plaintext and the keys must be converted into binary so that it can be operated and also the length of the algorithm. the key of this algorithm must be equal to the length of the plaintext.

The use of Super Encryption with Cipher Block Chaining Algorithm and Rail Fence Cipher. This aims to get a cipher that is stronger than using only one cipher, so it is not easy to crack. Encryption and decryption can be done by substituting the cipher sequence then transposing the cipher, or vice versa. Cipher Block Chaining has the property of covering up the plaintext pattern and is very random. Furthermore, the second security is obtained from the Rail Fence Cipher algorithm method, where the message when encoded will make it more difficult to solve.

مستخلص البحث

وجاينطا، سفندي زوغروه و. 2020. **تطبيق خوارزمية سباج السكك الحديدية وسلسل كتلة التشفير في وقاية رسالة النصوص.** البحث الجامعي. قسم الرياضيات كلية العلوم والتكنولوجيا جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف: 1(حمد حذيفة، الماجستير، 2(حمد انفع جوهري، الماجستير. **الكلمات الرئيسية:** التشفير، فك التشفير، سلسل كتلة التشفير، سباج السكك الحديدية التشفرات

إن استخدام الخوارزمية الواحدة أشك وقاية حتى يحتاج إلى المزيج من عدة الخوارزميات حيث تكون الوقاية أقوى. كان الجمع بين اثنين أو أكثر من تقنيات التبادل والتنقل التشفير للحصول على الخوارزمية المطلوبة)أصعبها كشفا(هو المفهوم المسمى بالتشفير المختلط. تتميز خوارزمية تشفير سباج السكك الحديدية مزايا مقارنة بالخوارزميات الأخرى ألن بها عملية كتابة نص عادي إلى نص مشفر أن يمكن إجراؤها على أي سطر مما يزيد من صعوبة بها عملية التشفير وذلك التشفير. أما سلسل كتلة التشفير فعبارة عن خوارزمية كريبتوغرافيا كالسكية أقوى بصفة متغطية على نمط النص العادي و عشوائية جدا، ألن طبيعة هذه الخوارزمية لها عملية مزدوجة لتغطية النص العادي أين تكون مفاتيحها حمولة إلى ثانية لعمليتها وأن يكون طول مفاتيح هذه الخوارزمية نفس طول النص العادي. كان

الهدف من استخدام التشفير المختلط خوارزمية سلسل كتلة التشفير وسباج السكك الحديدية للحصول على تشفير أقوى من استخدام شفرة واحدة فقط ، حتى ال يتيسر كشفها. يمكن إجراء التشفير وذلك التشفير عن طريق استبدال ترتيب التشفير مث نقل التشفير أو العكس. تتميز سلسل كتلة التشفير بطبيعتها المتغطية على أنماط النص العادي وهي عشوائية جدا. عالوة على ذلك، يتم الحصول على الوقاية الثانية من طريق خوارزمية تشفير سباج السكك الحديدية حيث تكون الرسالة عند تشفيرها أصعب كشفها.

BAB I

PENDAHULUAN

1.1. Latar Belakang

Pada era yang sekarang ini penyampaian sebuah informasi sangat mudah dilakukan. Hal itu disebabkan oleh pesatnya perkembangan teknologi dalam penyampaian pesan. Dalam proses penyampaian pesan dapat dilakukan melalui media apa saja sehingga mengakibatkan pihak yang tidak bertanggungjawab dapat mengambil data saat proses pengiriman. Misalnya penyampain pesan dalam bentuk digital menggunakan jaringan internet sangat rentan untuk disadap seperti adanya modifikasi atau perusakan. Oleh sebab itu, dibutuhkan suatu teknik untuk menjaga keaslian dan kerahasiaan sebuah pesan yang akan dikirim. Untuk menyampaikan pesan yang hanya ditujukan kepada pihak tertentu maka, kriptografi merupakan salah satu cabang ilmu yang bisa digunakan.

Menjaga amanah merupakan salah satu tujuan dari merahasiakan data atau pesan. Dalam Al-Qur'an surah Al-Anfal /8:27, telah dijelaskan pentingnya menjaga rahasia.

تَخُوْنُوا اللّٰهَ وَالرَّسُوْلَ وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا

Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui. (QS.Al-Anfal /8:27)

Dalam surah Al-Anfal ayat 27 tersirat bahwa “janganlah kamu mengkhianati amanat-amanat” agama Islam memerintahkan bahwa amanat apapun merupakan hal penting yang perlu dijaga. sehingga kalimat ini mengartikan bahwa sebuah pesan merupakan amanat yang perlu dijaga kerahasiaannya. Maka agar terhindar dari keburukan media sosial perlu adanya solusi agar amanat-manat tersebut sampai kepada pihak yang dituju.

Kriptografi merupakan salah satu bidang studi teknik matematika yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan sebuah pesan, otentikasi entitas serta otentikasi keaslian data dan integritas sebuah data. Kriptografi tidak hanya menyediakan keamanan informasi saja, tetapi juga sebuah himpunan teknik-teknik. (Menezes, Oorschot dan Vantone 1996). Teknik keamanan data harus terus dikembangkan untuk meminimalkan pencurian data. Dikembangkannya prosedur pengamanan data agar data tidak dapat dicuri. Penyandian data dapat diterapkan untuk meningkatkan pengamanan data berupa pesan teks. Penyandian atau enkripsi data merupakan proses pengubahan informasi data agar data tidak mudah terbaca. Hasil dari enkripsi merupakan informasi yang disandikan.

Dalam penelitian oleh (Singh, Nandal, dan Malik, 2015) menyatakan bahwa keamanan pesan tidak akan menjadi akurat apabila hanya dilakukan dengan menggunakan algoritma Rail Fence Cipher saja, sebab pada Teknik transposisi Rail Fence Cipher jika dilakukan dengan terpisah maka cipher akan mudah retak. Serta dalam penelitian yang dilakukan oleh (Fahrizal, Prihanto dan Rudianto, 2016) menyatakan bahwa Saat ini banyak algoritma kriptografi yang digunakan dalam pengamanan data, salah satunya algoritma kriptografi block cipher. Blok cipher

merupakan algoritma kriptografi simetrik yang mengenkripsi satu blok plaintext dengan jumlah bit tertentu dan menghasilkan blok ciphertextdengan jumlah bit yang sama. setiap blok-blok plaintext diExclusive OR dengan blok kunci sebelumnya sebelum dienkripsi, dengan harapan pengamanan datanya lebih terjaga. Dalam mode Cipher Block Chaining (CBC).

Mencermati hal yang telah diuraikan di atas, maka penulis ingin melakukan penelitian dengan judul **"IMPLEMENTASI ALGORITMA RAIL FENCE DAN CIPHER BLOCK CHAINING PADA PENGAMANAN PESAN TEXT"**

1.2. Rumusan masalah

Berdasarkan uraian pada latar belakang tersebut maka rumusan masalah dalam penelitian ini adalah :

1. Bagaimana proses enkripsi pada pesan teks menggunakan Algoritma rail fence dan *Cipher Block Chaining* ?
2. Bagaimana hasil enkripsi pada pesan teks menggunakan Algoritma rail fence dan *Cipher Block Chaining* ?
3. Bagaimana proses dekripsi pada pesan teks menggunakan Algoritma rail fence dan *Cipher Block Chaining*?
4. Bagaimana hasil dekripsi pada pesan teks menggunakan Algoritma rail fence dan *Cipher Block Chaining*?

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah di atas maka tujuan dari penelitian ini adalah:

1. Mengetahui proses enkripsi pada pesan teks menggunakan Algoritma rail fence dan *Cipher Block Chaining*
2. Mengetahui hasil enkripsi pada pesan teks menggunakan Algoritma rail fence dan *Cipher Block Chaining*
3. Mengetahui proses dekripsi pada pesan teks menggunakan Algoritma rail fence dan *Cipher Block Chaining*
4. Mengetahui hasil dekripsi pada pesan teks menggunakan Algoritma rail fence dan *Cipher Block Chaining*

1.4. Manfaat Penelitian

Hasil penelitian ini diharapkan mampu memberikan manfaat bagi pembaca dan peneliti khususnya, selain itu juga diharapkan:

1. Sebagai pembelajaran dan penelitian pengamanan data berupa pesan teks.
2. Sebagai bahan refrensi dalam pengembangan penelitian lebih lanjut.
3. Sebagai sarana pengambangan keilmuan dibidang matematika aljabar.
4. Sebagai aplikasi dalam melindungi privasi pesan teks.

1.5. Metode Penelitian

Penulisan penelitian ini dilakukan dengan studi literatur. Penulisan dimulai dengan mempelajari jurnal-jurnal, tugas akhir, artikel dan buku-buku tentang enkripsi serta deskripsi pada pesan teks beserta algoritma-algoritmanya. Adapun langkah-langkah penyelesaian penelitian ini, sebagai berikut:

1. Menyusun enkripsi dengan Algoritma rail fence dan *Cipher Block Chaining* pada pesan teks.
    a. Menentukan 16 karakter huruf yang akan digunakan sebagai *plaintext*
    b. Mengoperasikan plaintext dengan Algoritma rail fence yaitu dengan menuliskan dan membagi plaintext menjadi 4 baris secara zig-zag
    c. Menyusun hasil enkripsi dari Algoritma rail fence secara berbaris menyamping
    d. Menentukan Initial vektor yang akan digunakan untuk melakukan blok dan operasi pada kunci dan *ciphertext*
    e. Menentukan kunci yang akan digunakan untuk melakukan blok dan operasi pada Initial vector dan *ciphertext*
    f. Merubah karakter ciphertext kedalam bilangan biner dengan menggunakan operasi *Cipher Block Chaining*
    g. Merubah karakter kunci kedalam bilangan biner dengan menggunakan operasi *Cipher Block Chaining*
    h. Merubah karakter Initial vektor kedalam bilangan biner dengan menggunakan operasi *Cipher Block Chaining*
    i. Mengelompokan karakter dan biner dari ciphertext menjadi 8 blok entri menggunakan operasi *Cipher Block Chaining*
    j. Mengelompokan karakter dan biner dari kunci menjadi 8 blok entri menggunakan operasi *Cipher Block Chaining*
    k. Mengelompokan karakter dan biner dari kunci menjadi 1 blok entri menggunakan operasi *Cipher Block Chaining*

l. Mengoperasikan masing-masing blok entri biner ciphertext dengan blok entri biner Initial vektor menggunakan operasi exclusive-OR

m. Mengoperasikan kembali hasil operasi dari masing-masing blok entri biner *ciphertext* dengan blok entri biner Initial vektor dengan masing-masing blok entri biner dari kunci menggunakan operasi exclusive-OR

n. Menggeser 4 bit biner terdepan kebelakang dari hasil operasi exclusive-OR

o. Menggunakan operasi *Cipher Block Chaining*

p. Merubah hasil geser biner menjadi karakter-karakter ASCII menggunakan operasi *Cipher Block Chaining*

2. Menyusun dekripsi dengan Algoritma Super Enkripsi Algoritma rail fence dan Cipher Block Chaining pada pesan teks.

   a. Menggeser 4 bit biner paling belakang kedepan dari hasil enkripsi menggunakan operasi *Cipher Block Chaining*

   b. Mengoperasikan 8 blok entri biner dari hasil enkripsi dengan Initial vektor menggunakan operasi exclusive-OR

   c. Mengoperasikan kembali 8 blok entri biner dari hasil enkripsi dengan Initial vektor menggunakan operasi exclusive-OR dengan 8 blok entri biner kunci menggunakan operasi exclusive-OR

   d. Merubah 8 blok entri biner hasil operasi exclusive-OR kedalam karakter ASCII dengan menggunakan operasi *Cipher Block Chaining*

   e. Menyusun dan membagi karakter entri ciphertext menjadi 4 bagian secara berbaris kebawah

   f. Mengoperasikan ciphertext dengan Algoritma rail fence

g. Implementasi sebagai ketepatan hasil perhitungan dengan computer menggunakan aplikasi PYTHON.

h. Interpretasi hasil

3. Memaparkan proses penyandian Cipher Block Chaining dan Rail Fence.
4. Menganalisa tingkat keamanan algoritma Cipher Block Chaining dan Rail Fence.

1.6. Sistematika Penulisan

Dalam penulisan dalam penelitian ini, penulis menggunakan sistematika yang terdiri dari empat bab, dan masing-masing bab dibagi dalam subbab dengan sistematika penulisan sebagai berikut.

Bab I Pendahuluan

Membahas tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, tinjauan pustaka, metode penulisan dan sistematika penulisan yang menggambarkan secara singkat isi laporan penelitian ini.

Bab II Kajian Pustaka

Membahas tentang teori-teori penunjang yang digunakan dalam bab selanjutnya, meliputi Pesan teks, keamanan Pesan teks, Algoritma kriptografi, Algorima kriptografi klasik, Algoritma Kriptografi modern, Enkripsi, Dekripsi, Super Enkripsi, Algoritma Rail fence dan *Cipher Block Chaining*

Bab III Pembahasan

Bab ini berisi tentang langkah-langkah pemebentukan ciphertext yang melalui tahap super enkripsi substitusi dan transposisi yang dilakukan

melalui metode Algoritma Rail fence Cipher dan *Cipher Block Chaining* sehingga didapatkan suatu ciphertext yang telah terenkripsi dan juga berisi implementasi algoritma kedalam aplikasi PYTHON.

Bab IV Penutup

Bab ini berisi kesimpulan dari pembahasan yang sesuai dengan hasil penelitian, yang selanjutnya dapat digunakan sebagai saran bagi pembaca dan peneliti selanjutnya.

BAB II

KAJIAN PUSTAKA

2.1. Algoritma

Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematik dan logis". Kata logis merupakan kata kunci dalam algoritma. Langka-langka dalam algoritma harus logis dan harus dapat ditentukan bernilai salah atau benar (Rosa dan Shalahuddin 2010).

Algoritma berusaha melakukan langkah-langkah seefisien mungkin untuk mencapai tujuan semaksimal mungkin. Algoritma merupakan implementasi dari kehidupan sehari-hari misalnya antrian dan tumpukan yang terjadi dalam aktifitas sehari-hari merupakan implementasi dari algoritma stack dan algoritma queue. Menurut Thomas H. Cormen (2009:5), Algoritma merupakan prosedur dari komputasi yang mengambil beberapa nilai atau kumpulan nilai sebagai input kemudian di proses sebagai output sehingga urutan langkah komputasi yang mengubah input menjadi output disebut dengan algoritma.

2.2. Kriptografi

Kriptografi merupakan ilmu mengenai teknik enkripsi sebuah data dimana data tersebut diacak menggunakan suatu kunci enkripsi menjadi data yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Sehingga untuk mendapatkan kembali data asli harus melalui proses dekripsi menggunakan kunci dekripsi. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter. Rahasia pada sebuah algoritma terletak di beberapa parameter yang

digunakan, jadi parameter yang menentukan sebuah kunci. Sehingga parameter yang menentukan kunci dekripsi itulah yang harus dirahasiakan. (Sentot, 2009).

Terdapat empat elemen utama didalamnya untuk menjalankan proses kriptografi yang baik, yang berkait satu sama lain. Yaitu :

1. *Plain Text*

   Merupakan sebuah pesan awal atau pesan asli yang akan di kirim pada proses komunikasi. Sehingga pesan awal atau pesan asli yang akan di enkripsi dan di deskripsi disebut dengan Plain Text.

2. *Cipher Text*

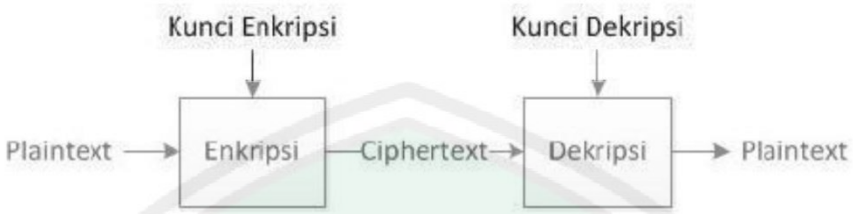
   Merupakan pesan asli (Plain Text) yang telah melalui proses enkripsi didalam kriptografi. Agar pesan asli (Plain Text) dapat dibaca kembali oleh penerima pesan, maka Cipher Text ini diubah kembali dengan memanfaatkan Key yang telah di sediakan.

3. *Cryptography Key*

   Merupakan kunci yang di gunakan untuk melakukan enkripsi dan deskripsi pada sebuah data yang akan melalui proses kriptografi. Tanpa adanya 3. Cryptography Key yang sama maka proses enkripsi dan deskripsi tidak dapat dilakukan dengan baik. Cryptography Key merupakan informasi yang padat menjadi kendali terhadap proses terjadinya sebuah kriptografi.

4. *Encryption Decryption Algorithm*

Algoritma yang di gunakan untuk enkripsi dan dekripsi merupakan komponen yang juga sama pentingnya dalam proses kriptografi



Gambar 2.1

Empat tujuan mendasar dari ilmu kriptografi yang juga merupakan aspek keamanan informasi, yaitu :

a. Kerahasiaan (confidentiality) artinya data tersebut hanya bisa diakses atau diterima oleh pihak-pihak tertentu saja.
b. Otentikasi (authentication) Saat seseorang mengirim atau menerima informasi, kedua belah pihak perlu mengetahui pengirim pesan yang sebenarnya.
c. Integritas data (integrity) Pesan yang sampai pada penerimanya sangat terjaga tanpa ada bagian dari pesan tersebut yang diganti, diduplikasi, dirusak, diubah urutannya dan ditambahkan.
d. Ketiadaan penyangkalan (nonrepudiation) Nonrepudiation sebuah upaya mencegah adanya sifat saling mengingkari antara pengirim maupun penerima bahwa mereka telah mengirimkan atau menerima suatu pesan/informasi (Munir, 2006).

2.3. Algoritma Kriptografi

2.3.1 Algoritma Kriptografi Klasik

Algoritma telah lama digunakan bahkan sejak sebelum era komputerisasi dan mayoritas menggunakan teknik kunci simetris. Metode yang digunakan menyembunyikan pesan ada beberapa teknik yaitu dengan teknik substitusi atau transposisi atau keduanya (Sadikin, 2012). Teknik substitusi merupakan Teknik menggantikan karakter yang ada pada *plaintext* menjadi karakter lain yang hasilnya adalah *ciphertext*. Sedangkan teknik mengubah plaintext menjadi *ciphertext* dengan cara permutasi karakter disebut dengan transposisi.

Terbentuknya berbagai macam algoritma kriptografi modern dilatarbelakangi oleh kombinasi keduanya secara kompleks (Prayudi, 2005).

2.4. Algoritma Kriptografi Modern

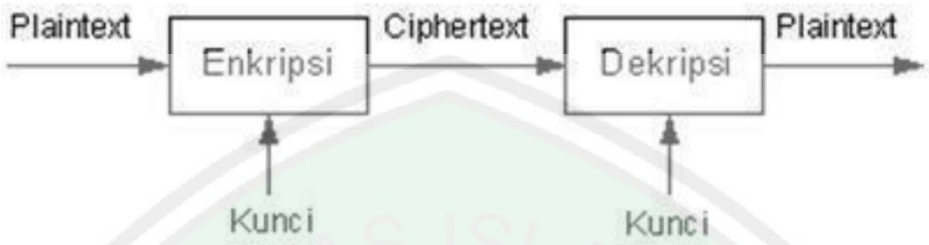
Algoritma Kriptografi Modern merupakan algoritma yang menggunakan pengolahan simbol biner karena berjalan mengikuti operasi komputer digital. Sehingga ilmu pengetahuan matematika sangat dibutuhkan untuk menguasainya (Sadikin, 2012). Algoritma kriptografi modern terbagi menjadi dua macam, yaitu algoritma simetris (symmetric algorithms) dan algoritma asimetris (asymmetric algorithms).

Macam-macam Algoritma Kriptografi

2.5. Algoritma Kriptografi Simetris.

Algoritma yang hanya menggunakan satu kunci pada proses enkripsi dan dekripsi disebut Algoritma kriptografi simetris. Contoh algoritma simetris yaitu

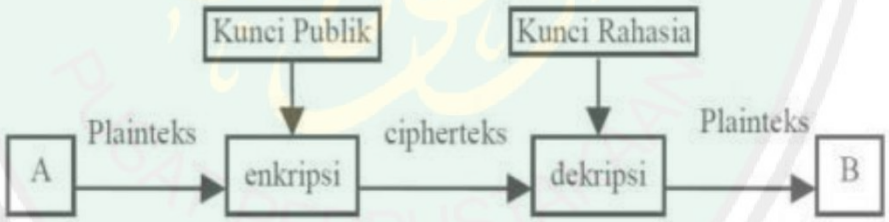
Rijndael, DES (Data Encryption Standard), IDEA, Blowfish, Serpent, GOST, RC5, RC4, RC2, dan lain-lain. Terdapat Skema kriptografi algoritma simetris pada gambar 2.1 (Munir, 2006).



Gambar 2. 2

2.6. Algoritma kriptografi asimetris atau algoritma kunci publik.

Algoritma yang menggunakan kunci publik pada enkripsi dan kunci privat untuk proses dekripsi disebut Algoritma kriptografi asimetris. Contoh algoritma asimetris yaitu ElGamal, Rabin dan RSA. Terdapat skema kriptografi algoritma asimetris pada gambar 2.2 (Munir, 2006).



Gambar 2. 3

2.7. Fungsi Hash

Menurut Munir (2006), Fungsi hash sering disebut dengan satu arah message digest, fingerprint, (one-way function), message authentication code (MAC) dan fungsi kompresi. Fungsi Hash merupakan satu fungsi matematika yang

pengaplikasiannya dengan cara menginput variable dan mengubahnya menjadi urutan biner dengan panjang yang tetap. Pembuatan sidik jari dari suatu pesan merupakan salah satu pengaplikasian dari Fungsi Hash. Pesan yang menggunakan sidik jari merupakan suatu tanda bahwa pesan tersebut benar-benar hanya untuk orang yang di inginkan.

2.8. Subsitusi

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 berkembangannya 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 (Supriyanto & Ardhianto, 2008).

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

2.9. 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 (Supriyanto, Ardhianto, 2008). Metode penyandian transposisi mempunyai beberapa algoritma yaitu :

1. Penyandian transposisi Rail Fence Cipher
2. Penyandian transposisi route
3. Penyandian transposisi kolom
4. Penyandian transposisi ganda

2.10. Enkripsi

Enkripsi merupakan langkah-langkah sistematis yang digunakan dalam menyandikan/ menyembunyikan pesan dari pihak-pihak lain yang tidak berhak menerima pesan tersebut. Keamanan dari algoritma enkripsi tergantung dari bagaimana suatu algorima itu bekerja, maka algoritma semacam ini disebut dengan algoritma terbatas (Ariyus, 2006).

2.11. Deskripsi

Ciphertext yang dirubah menjadi plaintext kembali dengan menggunakan kunci yang juga digunakan pada proses enkripsi disebut dengan deskripsi (Stalling, 2003). Kunci pada algoritma Simetri saat enkripsi dan dekripsi adalah sama,

sedangkan kunci dekripsi pada algoritma Asimetri yang digunakan berbeda dengan enkripsi atau disebut dengan kunci public. Algoritma yang memakai kunci publik diantaranya adalah (Ariyus, 2006):

1. Diffie-Hellman (DH)
2. Elliptic Curve Cryptography (ECC)
3. Digital signature algoritm (DSA)
4. RSA
5. Dan lain sebagainya.

Enkripsi dan dekripsi merupakan bagian penting dari algoritma kriptografi proses tersebut tidak dapat dipisahkan, jika suatu metode enkripsi tidak memiliki pemecahannya atau dekripsinya dapat dikatakan bahwa metode tersebut fail.

Secara sistem operasi kriptografi dekripsi merupakan proses pengembalian pesan dari enkripsi.

Sistem Kriptografi Menurut Stinson (1995), sistem kriptografi (cryptosystem) adalah suatu 5- tuple (P, C, K, E, D) yang memenuhi kondisi sebagai berikut :

1. P adalah himpunan plaintext, 11
2. C adalah himpunan ciphertext,
3. K atau ruang kunci(keyspace), adalah himpunan kunci,
4. E adalah himpunan fungsi enkripsi ek : P → C ,
5. D adalah himpunan fungsi dekripsi dk : C → P ,
6. Untuk setiap k ∈ K terdapat ek ∈ E dan dk ∈ D. Setiap ek : P → C dan dk : C → P merupakan fungsi sedemikian hingga dk(ek(x)) = x, untuk setiap plaintext x ∈ P . Sistem kriptografi terdiri dari sebuah algoritma, seluruh kemungkinan

plaintext, ciphertext dan kunci-kuncinya. Sistem kriptografi merupakan suatu fasilitas untuk mengkonversikan plaintext menjadi ciphertext, dan sebaliknya.

2.12. Super Enkripsi

Agar algoritma tidak mudah ditemukan oleh pihak yang tidak bersangkutan, maka dikembangkan algoritma baru dengan menggabungkan kedua teknik algoritma klasik tersebut. Dengan menggunakan dua atau lebih dari Teknik subtitusi dan transposisi cipher untuk mendapatkan suatu algoritma yang lebih andal (susah dipecahkan) merupakan sebuah konsep yang dinamakan dengan Super enkripsi (Ariyus, 2006). Untuk menjalankan teknik super enkripsi ini, harus mengerti teknik subtitusi dan transposisi yang akan dioperasikan. Super enkripsi dijalankan dengan melakukan enkripsi pesan dengan teknik subtitusi, selanjutnya ciphertext yang telah didapatkan dienkripsi lagi dengan teknik transposisi.

2.13. Rail Fence Cipher

Rail Fence Cipher adalah merupakan salah satu variasi implementasi cipher transposisi. Pada *Rail Fence Cipher*, penulisan *plaintext* secara vertikal ke bawah sepanjang n-rails, dan menulis lagi ke kolom baru setelah penulisan *plaintext* karakter ke-n. *Ciphertext* yang dihasilkan berupa karakter yang dibaca secara horizontal.

Rail Fence Cipher membentuk sebuah lintasan. Karena lintasan ini berbentuk Zig Zag itulah sebabnya metode ini dapat juga disebut Kriptografi Zig-Zag. Rail *Fence Cipher* adalah salah satu dari cipher transposisi umumnya, dalam metode ini, elemen *plaintext* yang disetujui oleh pengirim dan penerima biasanya ditulis ke

dalam bentuk matriks. Hal Ini berarti model matriks disetujui atau diketahui oleh keduanya. Ada banyak cara bagaimana membentuk *ciphertext*, salah satu nya dengan metode Zig-Zag (Ramkesh,2016).

Misalnya Saya akan melakukan penyandian terhadap plaintext berikut :

Sebagai contoh untuk enkripsi, kita mempunyai kunci sebanyak n=3 dan sebuah pesan (plaintext) yaitu "SARASWATI YOGA". Maka proses enkripsi karakter dapat dilihat seperti pada Tabel 2.1 sebagai berikut:

Plaintext: SARASWATI YOGA													
n = 1	S				S				I				A
n = 2		A		A		W		T		Y		G	
n = 3			R				A				O		

Tabel 2. 1

Hasil Enkripsi *Rail Fence Cipher*

Plaintext: SARASWATI YOGA													
n = 1	S				S				I				A
n = 2		A		A		W		T		Y		G	
n = 3			R				A				O		
Ciphertext: SSI AAA WTY GRAO													

Tabel 2. 2

Proses Dekripsi:

Nilai Kunci yang digunakan: Hitung Jumlah Karakter Ciphertext, selanjutnya Bagikan dengan Nilai Kunci Enkripsi, Maka hasilnya sebagai Kunci Dekripsi.

Ciphertext = SSI AAA WTY GRAO

Sebagai contoh untuk dekripsi, setelah sebuah pesan yaitu *plaintext* telah diubah menjadi ciphertext, maka ciphertext dapat ditulis secara horizontal dengan kunci

sebanyak n=3, kemudian *plaintext* dapat dibaca secara vertikal yang dapat dilihat pada Tabel 2.3 sebagai berikut:

Ciphertext: SSIAAAWTYGRAO													
n = 1	S				S				I				A
n = 2		A		A		W		T		Y		G	
n = 3			R				A				O		
Plaintext: SARASWATI YOGA													

Tabel 2.3

Algoritma *Rail Fence Cipher* mempunyai kelebihan dibandingkan algoritma lainnya dalam proses penulisan *plaintext* menjadi *ciphertext* karena penulisan dapat dilakukan pada baris mana saja. Hal ini akan menambah kerumitan dalam proses enkripsi maupun dekripsi.

2.14. Cipher Block Chaining

Algoritma *Cipher Block Chaining* (CBC) merupakan salah satu algoritma subtitusi dengan penerapan mekanisme umpan balik pada sebuah blok bit dimana hasil enkripsi blok sebelumnya diumpan balikkan ke dalam proses enkripsi blok current. Caranya, blok *plaintext* yang current di-XOR-kan terlebih dahulu dengan blok *ciphertext* hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi. Dengan algoritma CBC, setiap blok *ciphertext* tidak hanya bergantung pada blok plaintextnya tetapi juga pada seluruh blok *plaintext* sebelumnya. Dekripsi dilakukan dengan memasukkan blok *ciphertext* yang current ke fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok *ciphertext* sebelumnya. Blok *ciphertext* sebelumnya berfungsi sebagai umpan maju (*feedforward*) pada akhir proses dekripsi (Dewi Rosmala, 2012, 58)

Mode operasi ini menerapkan mekanisme umpan balik (*feedback*) pada sebuah blok. Caranya, *blok plaintext* yang current di-XOR-kan terlebih dahulu dengan blok ciphertext hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi.

Untuk menghasilkan blok cipher pertama, IV (*initialization vector*) digunakan untuk pengoperasian awal menggantikan *blok ciphertext* sebelumnya. Saat proses deskripsi, blok plaintext pertama diperoleh dengan cara meng-XORkan IV dengan hasil dekripsi terhadap blok ciphertext pertama (Munir;2019).

Deskripsi dilakukan dengan memasukkan blok *ciphertext* yang current ke fungsi deskripsi, kemudian hasil blok ciphertext yang di-*current*-kan ke fungsi deskripsi, di-XOR-kan dengan blok *ciphertext* sebelumnya. Dalam hal ini, blok *ciphertext* sebelumnya berfungsi sebagai umpan (*feedforward*) pada akhir deskripsi. Gambar 2.5 memperlihatkan skema mode operasi CBC. Perhatikan bahwa fungsi enkripsi dapat sama dengan fungsi deskripsi, atau enkripsi = deskripsi, sehingga tidak dibutuhkan algoritma baru untuk deskripsi. Secara sistematis, enkripsi dan deskripsi untuk m buah blok pesan dengan mode *Cipher Block Chaining* dinyatakkan sebagai :

Enkripsi : $Ci = Ek(Pi \oplus Ci\text{-}1)$, $i= 1,2,\ldots,m$

Deskripsi : $Pi=Dk(Ci) \oplus Ci\text{-}1$, $i= 1,2,\ldots,m$

Kasus khusus adalah enkripsi blok pertama sebab tidak tersedia nilai C_0. Untuk mengatasinya maka C0 digantin dengan sebuah nilai sembarang yang dinamakan IV (Initialization Vector), Jadi, C0 = IV. Nilai IV dapat dinyatakan sebagai konstanta atau dibangkitkan acak oleh program. Sebaliknya pada deskripsi,

blok plaintext pertama diperoleh dengan cara meng-XOR-kan IV dengan hasil deskripsi terhadap blok ciphertext pertama. IV tidak perlu rahasia.

Jadi, untuk m buah blok plaintext, enkripsinya adalah:

C1 = Ek(P1⊕IV)

C2 = Ek(P2⊕C1)

C3 =

Ek(P3⊕C2)

:

:

Cm = Ek(Pm⊕Cm)

Dan deskripsi m buah blok ciphertext adalah:

P1=Dk(C1) ⊕IV

P2=Dk(C2) ⊕C1

P3=Dk(C3) ⊕C2

:

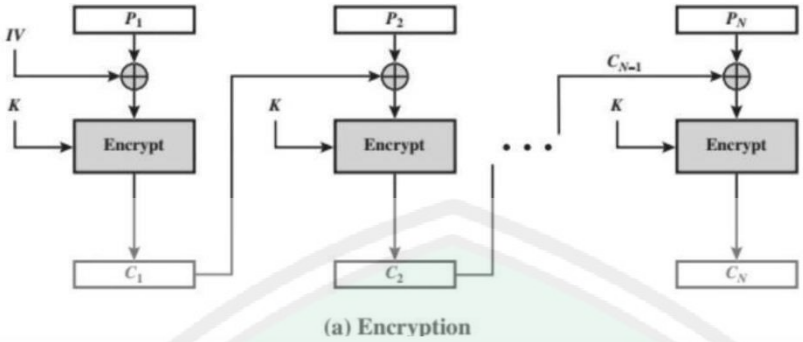
:

Cm = Dk(Cm)⊕Cm-1 (Munir;2019).

2.15. Algoritma dan Flowchart Proses Enkripsi dan Dekripsi dari File Teks

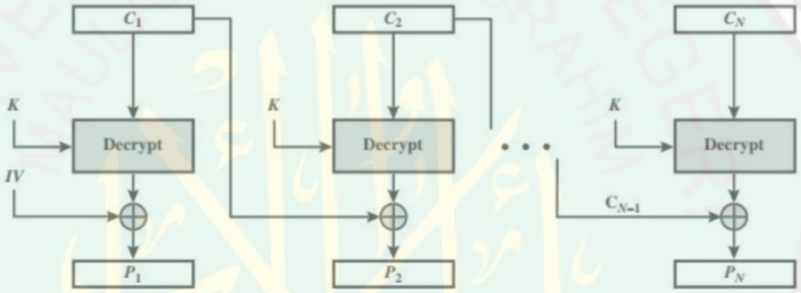
Prosedur ini digunakan untuk melakukan proses enkripsi dan dekripsi. Pada tahap ini juga akan dipanggil beberapa prosedur pendukung yang telah dijelaskan sebelumnya. Di bawah ini akan dijelaskan prosesnya secara lebih rinci :

Flowchart enkripsi Algoritma *Cipher Block Chaining*



(a) Encryption

Gambar 2.4



(b) Decryption

Gambar 2.5

2.16. 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, integritas data (Ariyus, 2006).

Teknik yang digunakan pada kriptografi klasik adalah subsitusi dan transposisi karakter dari plaintext , dan hasil dari subsitusi dan tranposisi akan menghasilkan ciphertext. Karakter yang ada dikonversi kedalam suatu urutan digit biner (bits) yaitu 1 dan 0, yang umum digunakan untuk schema encoding ASCII

(American Standart Code for Information Interchange) digunakan pada kriptografi modern. Squence bit (urutan bit) yang akan mewakili plaintext yang kemudian akan dienkripsi untuk mendapatkan chipertext dalam bentuk sequence bit.

Algoritma enkripsi boleh memakai salah satu dari dua metode, metode yang pertama "natural" pembagian antara stream cipher, dimana urutan bit untuk enkripsi digunakan bit by bit. Metode kedua adalah block cipher, dimana urutan pembagian dalam bentuk ukuran block yang dinginkan. Untuk mendapatkan satu karakter ASCII memerlukan 8 bit biner dan block cipher mempunyai 64 bit untuk satu block. Sebagai contoh sequence 12 bit : 100111010110, dipecah menjadi 3 block maka akan di dapatkan 100 111 010 110. Bagaimanapun, Bit-String dengan panjang 3 menghadirkan bilangan bulat 0 sampai 7 dengan urutan menjadi 4 7 2 6 (Ariyus, 2006).

000 = 0, 001 = 1, 010 = 2, 011 = 3, 100 = 4 ,

101 = 5, 110 = 6, 111 = 7

Binari string merupakan bagian operasi algoritma cipher, maka perlu memahami metode kombinasi dua bit yang disebut dengan Exclusive OR atau disebut XOR yang ditandai dengan $\oplus$. Dengan sebuah 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, 2006).

2.17. Pesan

Pesan merupakan serangkaian isyarat/symbol yang diciptakan oleh seseorang untuk memberikan informasi tertentu dengan harapan bahwa penyampaian pesan

berupa isyarat/simbol itu akan berhasil dalam menimbulkan sesuatu. (Hafied, 2004: 14).

Komunikasi dalam kehidupan manusia merupakan sesuatu hal yang sangat penting, karena dengan komunikasi seseorang dapat menyampaikan segala bentuk ide atau pesan yang akan disampaikan kepada orang lain. Dalam setiap melakukan komunikasi unsur penting diantaranya adalah pesan, karena pesan merupakan sebuah hal yang dapat disampaikan melalui media yang tepat, bahasa yang di mengerti, kata-kata yang sederhana dan sesuai dengan maksud, serta tujuan pesan itu akan disampaikan dan mudah dicerna oleh komunikan.Adapun pesan itu menurut Onong Effendy, menyatakan bahwa pesan adalah : "suatu komponen dalam proses komunikasi berupa paduan dari pikiran dan perasaan seseorang dengan menggunakan lambang, bahasa/lambang-lambang lainnya disampaikan kepada orang lain". (Effendy, 1989:224).

2.17.1 Keamanan Pesan

Pertukaran informasi terjadi setiap saat di internet sehingga sangat memungkinkan terjadinya pencurian informasi oleh pihak-pihak tertentu yang tidak bertanggungjawab. Agar data yang dikirimkan aman dari pihak-pihak yang tidak bertanggungjawab, maka data dapat disembunyikan dengan menggunakan kriptografi dengan Algoritma Transposition Cipher. Algoritma kriptografi disebut juga cipher, yaitu suatu aturan untuk enkripsi dan dekripsi sebuah data, atau fungsi matematika untuk proses enkripsi dan dekripsi. Menurut Alfred kekuatan dari algoritma yang digunakan untuk proses enkripsi dan dekripsi data berhubungan erat dengan penggunaan persamaan matematika. Semakin banyak dan rumit

perhitungan dari persamaan matematika yang digunakan dalam sebuah algoritma maka data sandi semakin aman (Alfred, 1997).

Adapun beberapa hal yang perlu diperhatikan dari keamanan informasi menurut Whitman dan Mattord (2011) sebagai berikut :

a. Physical Security yang memfokuskan pada strategi untuk mengamankan pekerja atau anggota dari organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
b. Personal Security yang overlap dengan „phisycal security' dalam melindungi orang-orang dalam organisasi
c. Operation Security yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
d. Communications Security yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.
e. Network Security yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Masing-masing komponen diatas berkontribusi dalam program keamanan informasi secara keseluruhan. Keamanan informasi adalah perlindungan informasi, termasuk system dan perangkat yang digunakan, menyimpan, dan mengirimkannya.

Keamanan terhadap pesan/informasi adalah hal yang sangat penting, bisa dibayangkan apabila informasi yang menjadi rahasia penting dapat bocor dan

disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, kriptografi yang merupakan salah satu teknik pengamanan pesan diharapkan dapat tetap menjaga kerahasiaan isi dari informasi dan memberikan keyakinan pada penerima pesan bahwa informasi tersebut memang berasal dari pengirim yang tepat begitu pula sebaliknya pengirim yakin bahwa penerima informasi adalah pihak yang tepat. (Yuliana;2014)

Teknik keamanan data terus dikembangkan untuk meminimalkan pencurian data. Peningkatan prosedur pengamanan data sering dikembangkan agar data tidak dapat dicuri. Penyandian data dapat diterapkan untuk meningkatkan pengamanan data berupa teks. Penyandian atau enkripsi data merupakan proses pengubahan informasi data agar data tidak terbaca. Hasil dari enkripsi berupa informasi yang disandikan (cipher text) sedangkan proses pembalikan sandi untuk mendapatkan informasi disebut dekripsi (Nishika dan R.K. Yadav). Algoritma kriptografi digunakan pada proses enkripsi maupun deskripsi. Pada umumnya algoritma kriptografi dibedakan menjadi dua jenis, yaitu kriptografi kunci simetris (symmetric key cryptography) dan kriptografi kunci tidak simetris (asymmetric key cryptgraphy) (Narender T. Dan Anita G).

BAB III

PEMBAHASAN

3.1 Teknik penyandian *Cipher Block Chaining*

Bentuk umum penyandian teks dengan menggunakan *Cipher Block Chaining* adalah menggunakan huruf alphabet A sampai dengan Z berikut ini adalah proses enkripsi algoritma *Cipher Block Chaining* :

Pertama adalah Mencari Biner dari setiap huruf pada Cipertext dan keyword

Ciphertext	Biner
M	01001101
A	01000001
L	01001100
A	01000001
N	01001110
G	01000111

Keyword	Biner
A	01000001
S	01010011
R	01010010
I	01001001
A	01000001
S	01010011

Inivation Vector	Biner
2	00110010
7	00110111

Kedua adalah pengelompokkan dari hasil dan keyword untuk dioperasi enkripsikan

Pengelompokan plaintext

Plaintext	Biner
MA	01001101 01000001
LA	01001100 01000001
NG	01001110 01000111

Pengelompokkan Keyword

Keyword	Biner
AS	01000001 01010011
RI	01010010 01001001
AS	01000001 01010011

Pengelompokan IV/C0 = initial vector

Initial Vector	Biner
27	00110010 00110111

Ketiga adalah pengoperasian Plaintext dengan IV/C0 dan Keyword

Ci = Ek(Pi⊕Ci-1)

CP1 = Blok P1⊕C0

= 01001101 01000001

= 00110010 00110111 ⊕

= 01111111 01110110

= 01000001 01010011 ⊕

= 00111110 00100101

Geser empat bit kekiri 11100010 01010011 →

CP2 = Blok P2⊕C2-1

= 01001100 01000001

= 11100010 01010011 ⊕

= 10101110 00010010

= 01010010 01001001 ⊕

= 11111100 01011011

Geser empat bit kekiri 11000101 10111111→

CP3 = Blok P3⊕C3-1

= 01001110 01000111

= 11000101 10111111 ⊕

= 10001011 11111000

= 01000001 01010011 ⊕

= 11001010 10101011

Geser empat bit kekiri 10101010 10111100→

Maka, hasil enkripsinya adalah

Proses Dekripsi pada Cipher Block Chaining (CBC) dinyatakan dengan rumus Pi= Dk(Ci) ⊕ Ci-1 sebelum melakukan dekripsi chipperteks menjadi plaintext terlebih dahulu menggeser 4 bit ciphertext dari kanan. Adapun proses dekripsinya sebagai berikut :

Pi = Dk(Ci) ⊕ Ci-1

C0= 00110010 00110111

C1= 11100010 01010011 → Geser empat bit kekanan 00111110 00100101

C2= 11000101 10111111→ Geser empat bit kekanan 11111100 01011011

C3= 10101010 10111100→ Geser empat bit kekanan 11001010 10101011

P1 = C1⊕C0

= 00111110 00100101

= 00110010 00110111 ⊕

= 00001100 00010010

= 01000001 01010011 ⊕

= 01001101 01000001

Hasilnya adalah **MA**

P2 = C2⊕C2-1

= 11111100 01011011

= 11100010 01010011 ⊕

= 00011110 00001000

= 01010010 01001001 ⊕

= 01001100 01000001

Hasilnya adalah **LA**

P3 = C3⊕C3-1

= 11001010 10101011

= 11000101 10111111 ⊕

= 00001111 00010100

= 01000001 01010011 ⊕

= 01001110 01000111

Hasilnya adalah **NG**

Maka, hasil enkripsinya adalah **MALANG**

3.1.1 Analisis Algoritma *Cipher Block Chaining*

Algoritma Cipher Block Chaining merupakan salah satu algoritma subtitusi yang sulit dipecahkan. Hal ini dikarenakan hasil enkripsi dari algoritma *Cipher Block Chaining* berupa simbol-simbol serta tombol-tombol kontrol pada komputer. Hal ini pula yang merupakan kelemahan dari algoritma *Cipher Block Chaining*, sehingga menyulitkan bagi para penerjemah jika ingin membuka sebuah teks.

Algoritma dan Flowchart Proses Enkripsi dan Deskripsi teks

3.2 Teknik penyandian Railfence Cipher

Diberikan *Plaintext*

JAWA TIMUR

Enkripsi dilakukan dengan kunci k = 3 ,offset = 0

J	.	.	.	T	.	.	.	R
.	A	.	A	.	I	.	U	.
.	.	W	.	.	.	M	.	.

Namun enkripsi juga dapat dilakukan dengan memulainya bukan dari baris paling atas (offset = 0), namun bisa juga dari baris lainnya. Dengan menggunakan contoh *plaintext* di atas :

.	.	W	.	.	.	M	.	.
.	A	.	A	.	I	.	U	.
J	.	.	.	T	.	.	.	R

Maka *ciphertextnya* adalah JTRAAIUWM

Proses Dekripsi :

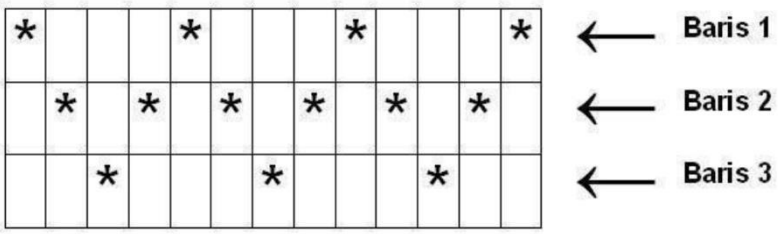
Ciphertext = JTRAAIUWM

jumlah karakter Ciphertext = 9

Key (jumlah baris) = 3

<u>langkah pertama:</u>

gambarkan baris/urutan sesuai dengan jumlah karakter dan key-nya!



langkah kedua:

hitung jumlah karakter pada masing-masing baris!

baris 1 = 3

baris 2 = 4

baris 3 = 2

langkah ketiga:

Sesuaikan jumlah karakter pada masing-masing baris dengan karakter pada *ciphertext* sesuai urutannya.

sehingga dapat ditentukan:

baris 1 = **JTR**

baris 2 = **AAIU**

baris 3 = **WM**

langkah keempat:

gambarkan kembali baris yang sudah ditentukan sesuai karakter pada masing-masing baris.

J . . . T . . . R

. A . A . I . U .

. . W . . . M . .

Dari 4 langkah di atas dapat diketahui bahwa decrypt dari

Chipertext **JTRAAIUWM** adalah **JAWATIMUR**

3.2.1 Analisa keamanan Railfence Cipher

Teknik penyandian railfance cipher adalah teknik penyandian sederhana yang merupakan penyandian dengan teknik transposisi yang merubah posisi dari seiap karakter huruf berdasarkan nilai kunci. Bruteforce menjadi sangat efektif untuk memcahkan pesan yang tersandikan menggunakan teknik railfance cipher yaitu dengan mencoba semua kemungkinan kunci dimana kemungkinan kunci dari teknik railfance cipher sangatlah terbats yaitu sejumlah bilangan bulat yang kurang dari jumlah nilai panjang *plaintext* yang ada. Sehingga teknik ini sangat rentan untuk dipecahlan. Misalakan pesan disandikan dengan railfance cipher dengan kunci 3, maka hanya menggunaka 3 kali percobaan agar plaintext bisa didapakan.

3.3 Penyandian Super Enkripsi Cipher Block Chaining dan Railfence Cipher

Teknik penyandian pesan dimulai dengan proses enkripsi menggunakan *Cipher Block Chaining*, kemudian pesan hasil enkripsi tersebut dienkripsi lagi menggunakan transformasi Railfence Cipher sehingga akan terbentuk keamanan dua lapis, untuk mengembalikan pesan agar terbaca kembali maka dilakukan dekripsi menggunakan Railfence Cipher kemudian pesan didekripsi menggunakan *Cipher Block Chaining*. Proses enkripsi dan dekripsi pesan dilakukan menggunakan kunci dan *plaintext* yang sama.

3.4 Proses Enkripsi Pesan

3.4.1 Penerapan Cipher Block Chaining Untuk Proses Dekripsi

Proses Dekripsi pada Cipher Block Chaining (CBC) dinyatakan dengan rumus Ci = Ek(Pi⊕Ci-1) langkah pertama adalah mengenkripsi pesan tersebut dengan menggunakan rumus dari enkripsi Cipher Block Chaining.

Pertama adalah Mencari Biner dari setiap huruf pada Cipertext dan keyword

Ciphertext	Biner
M	01001101
A	01000001
T	01010100
E	01000101
M	01001101
A	01000001
T	01010100

I	01001001
K	01001011
A	01001001
U	01000001
I	01010101
N	01001110

Keyword	Biner
M	01001101
E	01000101
R	01010010
D	01000100
E	01000101
K	01001011
A	01000001

M	01001101
E	01000101
R	01010010
D	01000100
E	01000101
K	01001011

Inivation Vector	Biner
1	00110001
5	00110101

Kedua adalah pengelompokkan dari hasil dan keyword untuk dioperasi enkripsikan.

Pengelompokan *plaintext*

Plaintext	Biner
MA	01001101 01000001
TE	01010100 01000101
MA	01001101 01000001
TI	01010100 01001001
KA	01001011 01000001
UI	01010101 01001001
N	01001110

Pengelompokkan Keyword

Keyword	Biner
ME	01001101 01000101
RD	01010010 01000100
EK	01000101 01001011
AM	01000001 01001101
ER	01000101 01010010
DE	01000100 01000101
K	01001011

Pengelompokan IV/C0 = initial vector

Initial Vector	Biner
15	00110001 00110101

Ketiga adalah pengoperasian Plaintext dengan IV/C0 dan Keyword

Ci = Ek(Pi⊕Ci-1)

CP1 = Blok P1⊕C0

= 01001101 01000001

= 00110001 00110101 ⊕

= 01111100 01110100

= 0100110101000101 ⊕

= 00110001 00110001

Geser empat bit kekiri 00010011 00010011 →DC3DC3

CP2 = Blok P2⊕C2-1

= 01010100 01000101

= 00010011 00010011 ⊕

= 01000111 01010110

= 01010010 01000100 ⊕

= 00010101 00010010

Geser empat bit kekiri 01010001 00100001→Q!

CP3 = Blok P3⊕C3-1

= 01001101 01000001

= 01010001 00100001 ⊕

= 00011100 01100000

= 01000101 01001011 ⊕

= 01011001 00101011

Geser empat bit kekiri 10010010 10110101→ μ

CP4 = Blok P4⊕C4-1

= 01010100 01001001

= 10010010 10110101 ⊕

= 11000110 11111100

= 01000001 01001101 ⊕

= 10000111 10110001

Geser empat bit kekiri 01111011 00011000→{CAN

CP5 = Blok P5⊕C5-1

= 01001011 01000001

= 01111011 00011000 ⊕

= 00110000 01011001

= 01000101 01010010 ⊕

= 01110101 00001011

Geser empat bit kekiri 01010000 10110111→P.

CP6 = Blok P6⊕C6-1

= 01010101 01001001

= 01010000 10110111 ⊕

= 00000101 11111110

= 01000100 01000101 ⊕

= 01000001 10111011

Geser empat bit kekiri 00011011 10110100→ESC'

CP7 = Blok P7⊕C7-1

= 01001110

= 10110100 ⊕

= 11111010

= 01001011 ⊕

= 10110001

Geser empat bit kekiri 00011011→ESC

Hasil Enkripsi nya adalah DC3 DC3 µ { CAN P . ESC ' ESC

3.4.2 Penerapan *Railfence Cipher* Untuk Proses enkripsi

Pada langkah enkripsi pesan selanjutnya adalah meng-input hasil enkripsi pesan dari operasi Cipher Block Chaining kedalam operasi Rail Fence Cipher maka bentuk operasinya seperti berikut:

Diberikan Plaintext

DC3 DC3 µ { CAN P . ESC ’ ESC

Enkripsi dilakukan dengan kunci k = 3

DC3	.	.	.	.	.	.	**P**	.	.	.	**ESC**
.	**DC3**	.	**!**	.	**µ**	.	**CAN**	.	**.**	.	**‘**	.
.	.	**Q**	.	.	.	**{**	.	.	.	**ESC**	.	.

Maka ciphertextnya DC3 P ESC DC3 ! µ CAN . ‘ { ESC

3.5 Proses Dekripsi Pesan

Maka diperlukan teknik dekripsi pesan agar ciphertext kembali menjadi plaintext yang bisa dibaca dan dipahami. Pada proses dekripsi dilakukan Teknik yang berlawanan dengan proses enkripsi yaitu dilakukan teknik dekripsi *Railfence Cipher* kemudian dilanjutkan dengan *Cipher Block Chaining*

3.5.1 Penerapan *Railfence Cipher* Untuk Proses Dekripsi

Seperti pada proses dekripsi pesan railfence cipher, pertama adalah membuat sebuah matriks dengan ukuran nilai kunci enkripsi x jumlah karakter pesan, kemudian dari kolom 1 dan baris 1 di beri suatu tanda yang mana ini menjadi patokan dalam penginputan pesan tanda ini dibuat bergerak secara zig zag ke arah kanan

Ciphertext = **DC3 P ESC DC3 ! µ CAN . ‘ { ESC**

jumlah karakter Ciphertext = 13

Key (jumlah baris) = 3

langkah pertama:

gambarkan baris/urutan sesuai dengan jumlah karakter dan key-nya!

langkah kedua:

hitung jumlah karakter pada masing-masing baris!

baris 1 = 4

baris 2 = 6

baris 3 = 3

langkah ketiga:

Sesuaikan jumlah karakter pada masing-masing baris dengan karakter pada *ciphertext* sesuai urutannya.

sehingga dapat ditentukan:

baris 1 = **DC3 P ESC**

baris 2 = DC3 ! µ CAN . ‘

baris 3 = Q { ESC

langkah keempat:

gambarkan kembali baris yang sudah ditentukan sesuai karakter pada masing-masing baris.

DC3	.	.	.	.	.	.	**P**	.	.	.	**ESC**												
.	**DC3**	.	**!**	.	**µ**	.	**CAN**	.	**.**	.	**‘**	.											
.	.	**Q**	.	.	.	**{**	.	.	.	**ESC**	.	.											

Dari 4 langkah di atas dapat diketahui bahwa deskripsi dari DC3 P ESC DC3 ! µ CAN . ‘ { ESC adalah DC3 DC3 µ { CAN P . ESC ’ ESC

3.5.2 Penerapan Cipher Block Chaining Untuk Proses Dekripsi

Proses Dekripsi pada Cipher Block Chaining (CBC) dinyatakan dengan rumus Pi= Dk(Ci) ⊕ Ci-1 sebelum melakukan dekripsi chipperteks menjadi plaintext terlebih dahulu menggeser 4 bit ciphertext dari kanan. Adapun proses dekripsinya sebagai berikut :

Pi = Dk(Ci) ⊕ Ci-1

C0= 00110001 00110101

C1= 00010011 00010011 →Geser empat bit kekanan 00110001 00110001

C2= 01010001 00100001→ Geser empat bit kekanan 00010101 00010010

C3= 10010010 10110101→ Geser empat bit kekanan 01011001 00101011

C4= 01111011 00011000→ Geser empat bit kekanan 10000111 10110001

C5= 01010000 10110111→ Geser empat bit kekanan 01110101 00001011

C6 = 00011011 10110100→ Geser empat bit kekanan 01000001 10111011

C7= 00011011→ Geser empat bit kekanan 10110001

P1 = C1⊕C0

= 00110001 00110001

= <u>00110001 00110101</u> ⊕

= 00000000 00000100

= <u>01001101 01000101</u> ⊕

= 01001101 01000001

Hasilnya adalah **MA**

P2 = C2⊕C2-1

= 00010101 00010010

= 00010011 00010011 ⊕

= 00000110 00000001

= 01010010 01000100 ⊕

= 01010100 01000101

Hasilnya adalah **TE**

P3 = C3⊕C3-1

= 01011001 00101011

= 01010001 00100001 ⊕

= 00001000 00001010

= 01000101 01001011 ⊕

= 01001101 01000001

Hasilnya adalah MA

P4 = C4⊕C4-1

= 10000111 10110001

=10010010 10110101 ⊕

= 00010101 00000100

= 01000001 01001101 ⊕

= 01010100 01001001

Hasilnya adalah **TI**

P5 = C5⊕C5-1

= 01110101 00001011

= 01111011 00011000 ⊕

= 00001110 00010011

= 01000101 01010010 ⊕

= 01001011 01000001

Hasilnya adalah **KA**

P6 = C6⊕C6-1

= 01000001 10111011

= 01010000 10110111 ⊕

= 00010001 00001100

= 01000100 01000101 ⊕

= 01010101 01001001

Hasilnya adalah **UI**

P7 = C7⊕C7-1

= 10110001

= 10110100 ⊕

= 00000101

= 01001011 ⊕

= 01001110

Hasilnya adalah **N**

Hasilnya adalah **MATEMATIKAUIN**

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan hasil analisis dan implentasi program yang telah dilakukan dengan menggunakan aplikasi Python diatas, maka dapat disimpulkan bahwa :

1. Teknik super enkripsi dengan menggunakan metode algoritma Cipher Block Chaining dengan menggunakan persamaan Ci = Ek(Pi⊕Ci-1), i= 1,2,…,m di proses enkripsinya, lalu hasil dari enkripsi tersebut disandikan kembali dengan menggunakan algoritma Rail Fence Cipher dengan mengurutkan karakter pada baris atas yang kemudian diikuti oleh karakter selanjutnya pada baris bawah, dan seterusnya sebanyak plaintext dan sifatnya algoritma tersebut yang zig-zag. Proses pengembalian pesan tersebut lalu menggunakan dekripsi dari Algoritma Rail Fence Cipher kemudian didekripsi lagi dengan menggunakan algoritma One Time Pad Cipher yang persamaan dekripsi tersebut menggunakan Pi=Dk(Ci) ⊕Ci-1, i=1,2,…,m
2. Kunci yang digunakan dalam proses pengenkripsian dengan menggunakan algoritma Cipher Block Chaining harus benar-benar acak dan harus sempurna (truly random). Panjang kunci di algoritma Cipher Block Chaining memang haruslah sama dengan panjang plaintext yang akan dienkripsikan agar bias dibangkitkan kembali ketika nanti dienkripsi kembali dengan menggunakan teknik algoritma Rail Fence Cipher.
3. Teknik yang diimplementasikan dengan menggunakan algoritma Cipher Block Chaining dan algoritma Rail Fence Cipher membuat pesantersebut sangatlah

aman. Hal ini dikarenakan penggunaan dua buah jenis Cipher ini sangatlah mendukung satu sama lain agar proses enkripsi dan dekripsi pesan dapat meningkat keamanannya.

4. Implementasi sederhana dengan program Python membuat semakin mudah ketika memasukkan pesan teks secara otomatis.

4.2 Saran

Pada penelitian ini, terdapat beberapa saran yang bias dipertimbangkan untuk pengembangan pada peneltian yang berikutnya, yaitu :

1. Untuk penelitian kedepannya pada proses enkripsi pesan menggunakan Algoritma Rail fence dan Cipher Block Chaining diharapkan adanya modifikasi yang lebih variatif sehingga membuat pesan yang dienkripsi menjadi lebih kuat lagi dari penelitian ini.
2. Untuk pengembangan selanjutnya diharapkan adanya visualisasi yang lebih baik pada aplikasi PYTHON dari hasil enkripsi pesan menggunakan Algoritma Rail fence dan Cipher Block Chaining.
3. Untuk pengembangan yang menggunakan algoritma pada penelitian ini diharapkan adanya modifikasi yang lebih simple dan variatif sehingga membuat pesan yang didekripsi menjadi lebih cepat dan lebih baik lagi.
4. Untuk pengembangan selanjutnya diharapkan adanya visualisasi yang lebih baik pada aplikasi PYTHON dari hasil dekripsi pesan menggunakan Algoritma Rail fence dan Cipher Block Chaining

DAFTAR PUSTAKA

A.S, Rosa, Shalahuddin, M. (2010). Rekayasa Perangkat Lunak (Terstruktur dan Berorientasi Objek). Bandung: Penerbit Modula. 81 -135

Cangara, Hafied. 2004. Pengantar Ilmu Komunikasi. Jakarta : Kencana Prenada Media Group.

Cucu Tri Eka Yuliana, "Implementasi Algoritma Kriptografi Blowfish dan Metode Steganografi End Of File (EOF) untuk Keamanan Data", Skripsi Teknik Informatika Universitas Dian Nuswantoro, Semarang, 2014.

Effendy, Onong Uchjana. 1989. KAMUS KOMUNIKASI. Bandung : PT. Mandar Maju.

Munir, Rinaldi. 2006. Kriptografi. Bandung: Informatika Bandung.

Munir, Rinaldi. 2019. Kriptografi. Bandung: Informatika Bandung.

Narender T. Dan Anita G.,"Comparative Analysis of Symmetric Key Encryption Algorithms". International Journal of Advanced Research in Computer Science and Software Engineering Vol. 4(8), pp. 348-354.

Nishika dan R.K. Yadav, "A Lookup Table Based Secure Cryptographic SMS Communication on Android Environment". International Journal of Computer Science and Mobile Computing Vol. 2(6), pp. 53-59.

Prayudi, Yudi, Idham Halik. 2005. Studi Analisis Algoritma Rivest Code 6 (RC6) Dalam Enkripsi/Dekripsi Data. Seminar Nasional Aplikasi Teknologi Informasi 2005 (SNATI 2005), Yogyakarta.

Sadikin, Rifki. 2012. Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java. Penerbit Andi, Yogyakarta.

Whitman, M.E., & Mattord, H.J, Management of Information Security, Third Edition, Boston: Course Technology, 2010

Alfred J.M., Paul C.O., and Scott A.V, 1997, Handbook of Applied Cryptography. CRC Press LLC, Florida, USA.

Cormen, Thomas et. al. 2009. Introduction to Algorithm Third Edition. Massachusetts: The MIT Press.

Kromodimoeljo, Sentot. (2009). Teori dan Aplikasi Kriptografi. Jakarta : SPK IT Consulting.

Supriyanto, Aji.(2008). Pengantar Teknologi Informasi. Makassar : Salemba Empat.

Ariyus, D. (2006). Kriptografi keamanan data dan komunikasi. Penerbit Graha Ilmu Yogyakarta.

Stallings, William. 2003. Cryptography and Network Security. New Jersey: Pearson Education.

Stinson, Douglas. 1995. Cryptography: Theory and Practice. CRC Press.

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

Ramkesh, N. (2016). ADVANCED RAIL FENCE CIPHER ALGORITHM. International journal of pharmacy and technology, 16541.

https://rivalryhondro.wordpress.com/2017/04/10/rfcipher/

LAMPIRAN

```
# -*- coding: utf-8 -*-

a = input('Masukkan Plain Text: ')

b = input('Masukkan Kata Kunci: ')

c = input('Masukkan Initial Vaktor: ')

d = input('Masukkan Kunci Rail Fence: ')



print("==================================")



i = 0

bb = b

while len(b) < len(a):

    b = b+b[i]

    i = i+1

    if i > len(bb):

    i = 0



if len(b) > len(a):
```

```
bk = ''
i = 0bb = b
while len(bk) < len(a):
    bk = bk+b[i]
    i = i+1
b = bk



plaintext = str(a)
kataKunci = str(b)
IV = str(c)
kunciRail = int(d)



# PecahPlain text
pecahPlain = list()
for i in range(0,len(plaintext),2):
    pecahPlain.append(plaintext[i:i+2])


# PecahKunci
pecahKunci = list()
for i in range(0,len(kataKunci),2):
    pecahKunci.append(kataKunci[i:i+2])
```

```
# Binary Pecah Plain
binPecahPlain = list()
for i in pecahPlain:
    binPlain = ''.join(bin(ord(c)) for c in i).replace('b','')
    binPecahPlain.append(binPlain)


# Binary Pecah Kunci
binPecahKunci = list()
for i in pecahKunci:
    binKunci = ''.join(bin(ord(c)) for c in i).replace('b','')
    binPecahKunci.append(binKunci)


# Binary IV
Bitc = [[0,0,0,0,0,0,0,0],[0,0,0,0,0,0,0,0]]
for i in range(len(IV)):
    Bs = ''.join(bin(ord(c)) for c in IV[i]).replace('b','')
    for j in range(len(Bs)):
        Bitc[i][8-len(Bs)+j] = int(Bs[j])
```

```
binIV = list()
for i in range(2):
    for j in range(8):
        binIV.append(str(Bitc[i][j]))
binIV="".join(binIV)
#binIV = ''.join(bin(ord(c)) for c in IV).replace('b','')



# Jumlahan Biner
def add_biner(x,y):
    hasil = list()
for i in range(len(x)):
    hasilKei = (int(x[i])+int(y[i]))%2
    hasil.append(str(hasilKei))
hasil= "".join(hasil)


return hasil



# Proses Penjumlahan
CP = list()
binIVtambah = binIV
for i in range(len(binPecahPlain)):
```

```
    if len(binPecahPlain[i]) ==16:
        CPS = add_biner(binPecahPlain[i],binIVtambah)
        CPS = add_biner(CPS,binPecahKunci[i])
        CPS1 = list()
        for i in range(4,len(CPS)):
            CPS1.append(CPS[i])
for k in range(4):
        CPS1.append(CPS[k])
    CPS1="".join(CPS1)
else:
    CPS = add_biner(binPecahPlain[i],binIVtambah[8:16])
    CPS = add_biner(CPS,binPecahKunci[i])
    CPS1 = list()
    for i in range(4,len(CPS)):
        CPS1.append(CPS[i])
for k in range(4):
        CPS1.append(CPS[k])
    CPS1="".join(CPS1)
binIVtambah = CPS1
CP.append(CPS1)


# Hasil Enkripsi
CPT = list()
```

```
for i in range(len(CP)):
    X = CP[i]
    if len(X)==16:
        CPT.append(chr(int(X[:8],2)))
        CPT.append(chr(int(X[8:],2)))
    else:
        CPT.append(chr(int(X[:8],2)))
    CPT = "".join(CPT)
print("Hasil Enkripsi CBC")
print(CPT)
print("==================================")



# Enkripsi rail
def encrypts(s,n):

    fence = [[] for i in range(n)]
    rail = 0
    var = 1
for char in s:
    fence[rail].append(char)
    rail += var
```

```
if rail == n-1 or rail == 0:
    var = -var



res = ''
for i in fence:
    for j in i:
        res += j


return res



a = encrypts(CPT,kunciRail)
print("Hasil Enkripsi Rail Fence")
print(a)
print("================================")



# Dekripsi Rail
def decrypts(s,n):
    fence = [[] for i in range(n)]
    rail = 0
```

```
    var = 1
    for char in s:
        fence[rail].append(char)
        rail += var


if rail == n-1 or rail == 0:
    var = -var

rFence = [[] for i in range(n)]


i = 0
l = len(s)
s = list(s)
for r in fence:
    for j in range(len(r)):
        rFence[i].append(s[0])
        s.remove(s[0])
i += 1


rail = 0
var = 1
```

```
r = ''
for i in range(l):
    r += rFence[rail][0]
    rFence[rail].remove(rFence[rail][0])
    rail += var

    if rail == n-1 or rail == 0:
        var = -var
return r

b = decrypts(a,kunciRail)

print("Hasil Dekripsi Rail Fence")
print(b)
print("================================")

"======================================"
"Proses Dekripsi CBC"
"======================================"

DCP = CP #Mengambil Cipper text dari proses Enkripsi
```

```
# Penggeseran bit ke kanan


DCPgeser = list()


for i in range (len(DCP)):
    DCPS = list()
    for k in range (len(DCP[i])-4,len(DCP[i])):
        DCPS.append(DCP[i][k])
    for j in range (len(DCP[i])-4):
        DCPS.append(DCP[i][j])
DCPS = ''.join(DCPS)
DCPgeser.append(DCPS)
DCP = list()
    DCP.append(binIV)
for i inrange(len(CP)):
    DCP.append(CP[i])


# Penjumlahan dekripsi


binDekText = list()
```

```
for i in range(len(CP)):
    if len(DCPgeser[i]) == 16:
        DTS = add_biner(DCPgeser[i],DCP[i])
        DTS = add_biner(DTS,binPecahKunci[i])
        binDekText.append(DTS)
else:
        DTS = add_biner(DCPgeser[i],DCP[i][8:16])
        DTS = add_biner(DTS,binPecahKunci[i])
        binDekText.append(DTS)
TextN = list()
for i in range(len(binDekText)):
    if len(binDekText[i])==16:
        a = chr(int(binDekText[i][:8],2))
        b = chr(int(binDekText[i][8:],2))
        TextN.append(a)
        TextN.append(b)
else:
        a = chr(int(binDekText[i][:8],2))
        TextN.append(a)
TextN = "".join(TextN)

print("Hasil Dekripsi CBC")
print(TextN)
```

RIWAYAT HIDUP

Septedi Nugroho W, biasa dipanggil Tedi, lahir di Jakarta pada tanggal 15 September 1996. Bertempat tinggal di Kelurahan Ujung Menteng RT 12 RW 03 Kecamatan Cakung Provinsi DKI Jakarta Kota Jakarta Timur. Anak pertama dari bapak Parjono dan Almh. Ibu Haryani.

Mulai menempuh pendidikan dasar di SDN Percontohan 04 Pagi Jakarta pada tahun 2002 hingga 2008, menempuh Pendidikan menengah pertama di SMPN 146 Jakarta pada tahun 2008 hingga 2011, dan menempuh pendidikan menengah atasnya di MAN 21 Jakarta pada tahun 2011 hingga 2014. Selanjutnya pada tahun 2014, melanjutkan pendidikan di Universitas Islam Negeri (UIN) Maulana Malik Ibrahim Malang mengambil Program Studi Matematika.

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 : Septedi Nugroho Wijayanto
NIM : 14610096
Fakultas/Program Studi : Sains dan Teknologi/Matematika
Judul Skripsi : IMPLEMENTASI ALGORITMA RAIL FENCE DAN CIPHER BLOCK CHAINING PADA PENGAMANAN PESAN TEXT
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Mohammad Nafie Jauhari, M.Si

No	Tanggal	Hal	Tanda Tangan
1	13 Januari 2020	Konsultasi BAB I & II	1.
2	03 Februari 2020	Revisi BAB I & II	2.
3	17 April 2020	ACC BAB I & II 3	3.
4	26 Agustus 2020	Konsultasi BAB I, II & III	4.
5	30 Agustus 2020	Revisi BAB I, II & III 5	5.
6	11 September 2020	ACC BAB I, II & III	6.
7	20 September 2020	Konsultasi BAB IV	7.
8	5 Oktober 2020	Konsultasi BAB IV	8.
9	8 Oktober 2020	Revisi BAB IV	9.
10	14 Oktober 2020	Revisi BAB IV	10.
11	19 Oktober 2020	Revisi BAB 1, II & III	11.
12	27 Oktober 2020	ACC BAB I, II & III	12.
13	03 November 2020	ACC BAB IV	13.
14	17 November 2020	Konsultasi Keagamaan	14.
15	19 November 2020	ACC Keagamaan	15.
16	23 November 2020	ACC Keseluruhan	16.

Mengetahui,
Ketua Program Studi Matematika

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