ISSN : 2460 – 7797
e-ISSN : 2614-8234
Website : jurnal.umj.ac.id/index.php/fbc
Email : fibonacci@umj.ac.id

FIBONACCI
Jurnal Pendidikan Matematika dan Matematika

PENGGUNAAN INVERS MATRIKS DALAM MODIFIKASI FEISTEL CIPHER

Sisilia Sylviani[1)*], Fahmi Candra Permana[2)], Asep Singgih[1)], Nurendra Ari Wiguna[1)]
[1)]Departemen Matematika, FMIPA, Universitas Padjadjaran, Jl. Ir. Soekarno Km. 21, Jatinangor, Sumedang 45363
[2)]Prodi Pendidikan Multimedia, Universitas Pendidikan Indonesia, Bandung

[*]*sisilia.sylviani@unpad.ac.id*

Abstrak

Umumnya, pada algoritma kriptografi modern sistem yang digunakan adalah sistem bit. Namun, hal tersebut membuat cipherteks semakin sulit untuk dipecahkan. Saat ini, Feistel cipher merupakan salah satu algoritma kriptografi modern yang banyak digunakan karena proses pengimplementasiannya yang cukup sederhana. Kelebihan lainnya adalah bahwa algoritma tersebut merupakan salah satu bentuk dari cipherblok yang dibentuk dengan menggunakan struktur yang simetris serta hingga saat ini masih sulit untuk dipecahkan. Adanya modifikasi pada feistel cipher ini bertujuan untuk meningkatkan keamanan dalam proses penyampaian pesan. Dengan modifikasi feistel cipher, pesan yang dikirimkan ke penerima akan sangat sulit dipecahkan karena membutuhkan waktu yang lama dalam memecahkannya.

Kata Kunci*: Kriptografi, Algoritma, Feistel Cipher, Cipherteks, Enkripsi, Dekripsi*

PENDAHULUAN

Kriptografi adalah suatu ilmu yang berfungsi untuk menjaga keamanan pesan ketika pesan dikirim dari sautu tempat ke tempat lain. Pesan yang akan dikirim atau diubah terlebih dahulu kedalam suatu kalimat atau kode rahasia sebelum dikirim yang disebut dengan ciphertext. Setelah sampai ke penerima, cipherteks akan diubah kembali menjadi pesan aslinya. Proses mengubah plaintext atau pesan sebenarnya ke ciphertext disebut enkripsi, dan proses mengubah ciphertext menjadi plaintext disebut dekripsi. Algortima kriptografi ini ada yang simetris dan asimetris. Disebut simetris karena kunci yang digunakan untuk mengenkripsi dan mendekripsi pesan nilainya sama, sedangkan algoritma asimetris kunci enkripsi dan dekripsi nilainya berbeda. Pada kategori kunci simetri modern beroperasi dalam sistem bit dan dapat dikelompokkan menjadi 2 kategori yaitu cipher aliran (stream cipher) dan cipher blok (block cipher). Hampir

DOI: https://dx.doi.org/10.24853/fbc.8.2.143-148

semua algoritma cipher blok bekerja dengan prinsip model Feistel atau Feistel cipher. Model Feistel ini ditemukan oleh Horst Feistel pada tahun 1970. Model ini banyak dipakai dalam algoritma kriptografi seperti Lucifer, DES, Blowfish, dan lain-lain.

METODE PENELITIAN

Feistel Cipher

Feistel Cipher terbentuk dengan menggunakan struktur yang simetris. Nama "Feistel" berasal dari seoarang kriptografer IBM (International Business Machines) berkebangsaan Jerman, Horst Feistel. Penggunaan algoritma tersebut secara komersial pertama kali melalui algoritma Lucifer, yang didesain oleh Feistel sendiri bersama dengan Don Coppersmith. Feistel sendiri menjadi populer setelah pemerintah AS menggunakan algoritma DES (The Data Encryption Standard) sebagai standar enkripsi. Berkat kepopuleran yang didapat feistel cipher pada saat digunakan dalam DES inilah feistel cipher menjadi banyak digunakan oleh algoritma kriptografi yang lainnya.

Algoritma Feistel Cipher

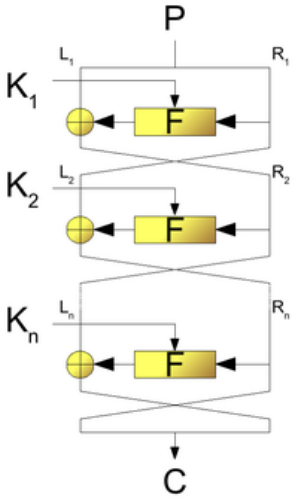
1. Misalkan F merupakan suatu fungsi yang memetakan bagian kanan dari plainteks (plainteks dibagi dua menjadi bagian kiri (L) dan bagian kanan (R)) serta enkripsi yang akan digunakan dan K adalah kunci yang akan digunakan dalam operasi dalam fungsi F, menjadi bagian kiri dari plainteks. Dengan kata lain, F merupakan fungsi yang mengacak bagian kanan pada plainteks dalam langkah sebelumnya. Hal pertama yang dilakukan adalah membagi plainteks yang akan dienkripsi menjadi dua bagian yang memiliki ukuran (matriks) yang sama. Misalkan Kembali potongan pertama sebagai L_0, sedangkan potongan yang kedua disebut R_0.
2. Kemudian, untuk setiap langkah $i = 0,1,2,\dots,n$, dilakukan komputasi sebagai berikut:

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus F(R_i, K_i)$$

Dengan $\oplus$ operasi EXCLUSIVE-OR bit demi bit. Hasil dari cipherteksnya adalah (R_{n+1}, L_{n+1}).

Selanjutnya, proses dekripsi dilakukan melalui langkah yang serupa. Hal yang berbeda terletak pada urutan kunci yang digunakan sebelumnya dibalik. Proses dekripsi yang umumnya digunakan dalam feistel cipher adalah sebagai berikut. Pertama, Kunci yang digunakan untuk setiap langkah adalah $i = n, n-1, n-2, \dots, 0$. Kemudian, dilakukan langkah sebagai berikut :

$$R_i = L_{i+1}$$
$$L_i = R_{i+1} \oplus F(L_{i+1}, K_i)$$



Gambar 1. *skema* Algoritma dari Feistel Cipher

Algoritma Modifikasi Feistel dengan Aritmatika Modular dan Invers Kunci Matriks

Dalam metode ini, kita ambil dan ubah Plaintext (P) ke dalam bentuk sepasang matrik P_0 dan Q_0, dan pergunakan matriks

FIBONACCI : Jurnal Pendidikan Matematika dan Matematika. Vol. 8 (2), pp: 143-148

kunci (K). Dalam metode ini operasi yang mengatur enkripsi dan dekripsi diberikan oleh

$$P_i = (K\ Q_{i-1}\ K\ ) mod\ N$$
$$Q_i = P_{i+1} \oplus P_i$$

$$untuk\ i = 1,2, \dots n$$

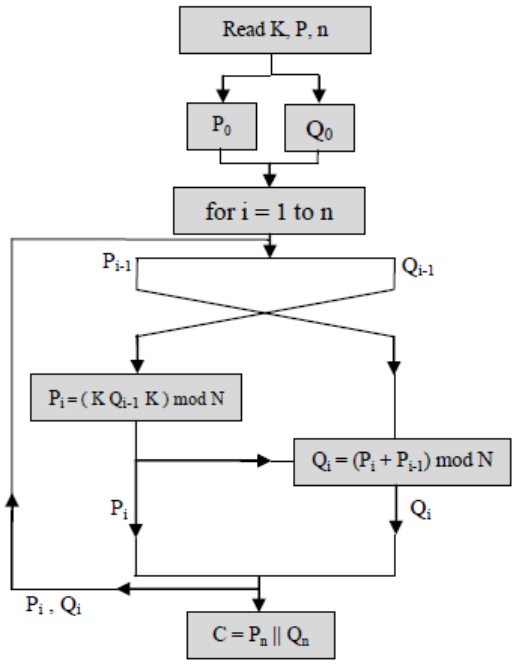
Dan,

$$Q_{i-1} = (K^{-1} P_i\ K^{-1}\ ) mod\ N$$
$$P_{i-1} = Q_i \oplus P_i$$

$$untuk\ i = n, (n-1), \dots$$

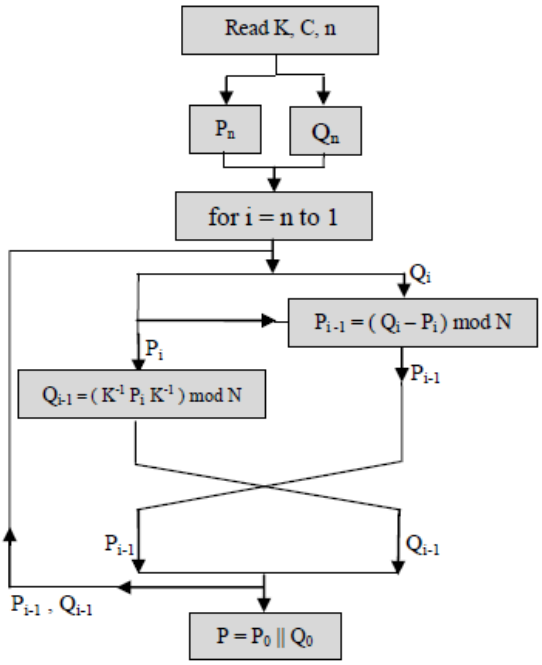
dengan $\oplus$ operasi EXCLUSIVE-OR bit demi bit.

Dalam metode ini, perkalian matriks kunci, dan mod operasi adalah operasi fundamental dalam pengembangan sandi. Inversi matriks kunci memainkan peran penting peran dalam proses dekripsi. Disini N adalah positif integer, dipilih secara tepat, dan n menunjukkan jumlah iterasi digunakan dalam pengembangan cipher. Berikut adalah alur proses enkripsi.



Gambar 2 *Skema* dari algoritma Modfikasi Feistel Cipher (Enkripsi)

Secara sederhananya, proses enkripsi akan dijalankan melalui langkah-langkah berikut :



Gambar 3 *Skema* dari algoritma Modifikasi Feistel Cipher (Dekripsi)

1. Siapkan plaintext P, siapkan matriks kunci K, tentukan banyak iterasi n dan bilangan modulo N, $N \in Z^+$
2. Konversikan karakter-karakter plaintext P kedalam angka yang bersesuaian dan susun kedalam bentuk matriks berukuran $m \times 2m$
3. Bagi dua matriks tersebut menjadi P_0 dan Q_0
4. Lakukan operasi
   $$P_i = (K \cdot Q_i \cdot K)\ mod\ N$$
   $$Q_i = (P_{i-1} + P_i)\ mod\ N$$
   sebanyak n kali dengan i dari 1 sampai n
5. Didapat matriks $C = Pn||Qn$
6. Konversikan entri-entri matriks C kedalam karakter yang bersesuaian.

Sedangkan proses dekripsi dijalankan melalui langkah-langkah berikut.

1. Ketahui ciphertext, matriks kunci K, banyak iterasi n, dan bilangan modulo N, $N \in Z^+$

2. Konversikan ciphertext kedalam angka dan susun kedalam bentuk matriks C
3. Cari invers matriks K
4. Bagi dua matriks C menjadi P_n dan Q_n
5. Lakukan operasi

$$Q_{i-1} = (K^{-1} \cdot P_i \cdot K^{-1}) \; mod \; N$$
$$P_{i-1} = (Q_i - P_i) \; mod \; N$$

sebanyak n kali dengan i dari n sampai 1

6. Didapat P_1 dan Q_1. Gabungkan sehingga didapat matriks P.

Konversikan tiap angka kedalam karakter sehingga didapat plaintext-nya

HASIL DAN PEMBAHASAN

1. Enkripsikan pesan "I LOVE U" dengan metode modifikasi Feistel Cipher Aritmatika Modular jika diberikan matriks kunci

$$K = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

dengan iterasi sebanyak 2 kali dan konversi karakter dengan tabel ASCII.

Jawab:

Konversikan karakter kedalam angka yang bersesuaian. Dengan konversi menggunakan tabel ASCII didapat :

I : 73
$(spasi)$: 32
l : 108
o : 111
v : 118
e : 101
$(spasi)$: 32
u : 117

sehingga didapat matriks P :

$$P = \begin{bmatrix} 73 & 32 & 108 & 111 \\ 118 & 101 & 32 & 117 \end{bmatrix}$$

Bagi dua matriks P, sehingga didapat matriks P_0 dan Q_0

$$P_0 = \begin{bmatrix} 73 & 32 \\ 118 & 101 \end{bmatrix}, Q_0 = \begin{bmatrix} 108 & 111 \\ 32 & 117 \end{bmatrix}$$

Pada iterasi 1, cari matriks P_1 dan Q_1

$$P_1 = (K \cdot Q_1 \cdot K) \; mod \; 128$$
$$Q_1 = (P_0 + P_1) \; mod \; 128$$

Didapat

$$P_1 = \begin{bmatrix} 91 & 111 \\ 112 & 100 \end{bmatrix}, Q_1 = \begin{bmatrix} 36 & 15 \\ 102 & 73 \end{bmatrix}$$

Pada iterasi 2, cari matriks P_2 dan Q_2

$$P_2 = (K \cdot Q_2 \cdot K) \; mod \; 128$$
$$Q_2 = (P_1 + P_2) \; mod \; 128$$

Didapat

$$P_2 = \begin{bmatrix} 51 & 15 \\ 98 & 88 \end{bmatrix}, Q_2 = \begin{bmatrix} 14 & 126 \\ 82 & 60 \end{bmatrix}$$

Sehingga didapat matriks C

$$C = \begin{bmatrix} 51 & 15 & 14 & 126 \\ 98 & 88 & 82 & 60 \end{bmatrix}$$

2. Dekripsikan matriks

$$C = \begin{bmatrix} 51 & 15 & 14 & 126 \\ 98 & 88 & 82 & 60 \end{bmatrix}$$

dengan metode modifikasi Feistel Cipher Invers Matriks kunci jika diketahui matriks kunci K adalah :

$$K = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

dengan iterasi sebanyak 2 kali, dan konversi karakter dengan tabel ASCII

Jawab :

Dari matriks kunci diatas maka didapat invers matriks K

$$K^{-1} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$$

Bagi dua matriks C, sehingga didapat matriks P_2 dan Q_2

$$P_2 = \begin{bmatrix} 51 & 15 \\ 98 & 88 \end{bmatrix}, Q_2 = \begin{bmatrix} 14 & 126 \\ 82 & 60 \end{bmatrix}$$

Pada iterasi 1, cari matriks P_1 dan Q_1

$$Q_1 = (K^{-1} \cdot P_2 \cdot K^{-1}) \; mod \; 128$$
$$P_1 = (Q_2 - P_2) \; mod \; 128$$

Didapat

$$Q_1 = \begin{bmatrix} 36 & 15 \\ 102 & 73 \end{bmatrix}, P_1 = \begin{bmatrix} 91 & 111 \\ 112 & 100 \end{bmatrix}$$

FIBONACCI : Jurnal Pendidikan Matematika dan Matematika. Vol. 8 (2), pp: 143-148

Pada iterasi 2, cari matriks P_0 dan Q_0

$$Q_0 = (K^{-1} \cdot P_1 \cdot K^{-1}) \; mod \; 128$$

$$P_0 = (Q_1 - P_1) \; mod \; 128$$

Didapat

$$P_0 = \begin{bmatrix} 73 & 32 \\ 118 & 101 \end{bmatrix}, Q_0 = \begin{bmatrix} 108 & 111 \\ 32 & 117 \end{bmatrix}$$

Sehingga didapat matriks *P*

$$P = \begin{bmatrix} 73 & 32 & 108 & 111 \\ 118 & 101 & 32 & 117 \end{bmatrix}$$

Yang jika dikonversikan kedalam karakter, didapat kalimat “I LOVE U”

SIMPULAN

Saat ini upaya pengamanan dalam berbagai kebutuhan manusia sangat diperhatikan, terutama dalam kebutuhan penyampaian pesan. Banyak algoritma kriptografi modern yang dimodifikasi agar bisa menciptakan sistem keamanan yang lebih sulit untuk dipecahkan(unbreakable). Meskipun demikian, algoritma feistel cipher masih banyak digunakan sebagai patokan oleh para kriptografer dalam memodifikasi desain algoritma. Modifikasi Feistel Cipher menggunakan Aritmetika Modular dan Invers Matriks Kunci ini memberikan solusi bagi masalah kriptografi, dengan modifikasi ini kita akan mendapatkan beberapa kelebihan dibandingkan algortima lainnya, antara lain :

1. Algoritma enkripsi dan dekripsi yang hampir sama
2. Hasil dekripsi yang mempunyai keamanan tingkat tinggi, karena dilengkapi dengan perpaduan prinsip *diffusion*, *confusion*, dan iterasi.

   sarana untuk memperkuat keamanan
3. Dapat dimodifikasi atau dikombinasi dengan metode lain sehingga akan lebih menambah tingkat keamanan pesan

DAFTAR PUSTAKA

Nadya Arieza dan Sinembala Junita, 2015. Feisty: *Modifikasi Block Cipher AES dengan Jaringan Feistel*. Bandung : Program Studi Teknik Informatika Institut Teknologi Bandung 1

Starsy V.U.K dan Kumar K Anup, 2012. “A Modified Feistel Cipher Involving Modular Aritmethic Addition and Modular Aritmethic Inverse Key Matrix”. India : IJACSA (Internasional Journal of Computer Science and Applications)

Susanto Alvin, 2015. “Analisis Feistel Cipher Sebagai Dasar Berbagai Algoritma Block Cipher.” Bandung : Program Studi Teknik Informatika Institut Teknologi Bandung

Wathoni, M., Efendi, Y., Ramadi, R., Hariyani, M., & Ratriningrum, D. B. 2021. “Penggunaan Aplikasi Qrcode Dan Smarty Template Engine Pada Pengkodean Buku (Studi Kasus Ruang Baca Computer Science Fakultas Ilmu Pendidikan)”. *Fibonacci: Jurnal Pendidikan Matematika dan Matematika*. Vol 7(2), pp: 177-188.