Jurnal Infotronik Volume 6 No. 1, Juni 2021 P-ISSN: 2548-1932
e-ISSN: 2549-7758

PERBANDINGAN METODE STREAM CIPHER DAN HILL CIPHER DALAM KEAMANAN DATA

Kamil Hidayatuloh[1], Yustantina[2], Kusmadi[3]

[1,2]Teknik Informatika, Fakultas Teknik, Universitas Sangga Buana
[3]Teknik Elektro, Fakultas teknik, Universitas Sangga Buana
[1]hidayatullohkamil@gmail.com, [2]yustantina31@gmail.com, [3]kusmadi@usbypkp.ac.id

ABSTRAK

Keamanan data atau informasi menjadi topik yang selalu diperbincangkan khalayak ramai, kerahasiaan data dan informasi menjadi hal yang sangat penting untuk dijaga. Tetapi Kejahatan cyber semakin sering kita dengar di media massa. Pelaku kejahatan memanfaatkan celah keamanan yang terdapat dalam sistem, untuk dimasuki dan dilakukan manipulasi sebuah data atau informasi. Kriptografi saat ini menjadi salah satu solusi yang banyak diminati karena sudah terbukti bisa mengamankan data dan informasi secara efektif. Bahkan, kriptografi sudah ada di dalam kehidupan kita saat ini, mulai dari transaksi di mesin ATM, Credit Card, mengakses internet, percakapan melalui telepon genggam sampai transaksi di dalam perdagangan elektronik (e-commerce). Pada penelitian ini digunakan metode algoritma Stream Cipher dan Hill Cipher. Berdasarkan hasil perbandingan antara kedua metode algoritma tersebut, dapat disimpulkan bahwasannya algoritma Stream Cipher dapat menjadi pilihan untuk mengamankan dan meminimalisir kebocoran data dan Informasi.

Kata Kunci: *Kriptografi;, Enkripsi; Dekripsi; Stream Cipher; Hill Cipher*

I. PENDAHULUAN

Perkembangan teknologi informasi saat ini telah membuat penyimpanan data menjadi lebih mudah dan efisien. Namun hal ini diikuti juga dengan resiko yang besar, seperti kebocoran informasi.

Kebocoran Informasi tentunya akan sangat merugikan, apalagi informasi tersebut berkaitan dengan dengan sebuah data, mulai dari pencurian data oleh orang yang tidak bertanggung jawab, sampai dengan terlibatnya orang yang memegang data tersebut.

Masalah keamanan data atau sebuah informasi ini perlu dilakukan pencegahan salah satunya dengan Kriptografi. Menurut terminologi kriptografi merupakan ilmu dan seni untuk menjaga sebuah tulisan rahasia agar tidak dapat dibaca oleh orang yang tidak memiliki hak untuk membacanya.

Ada banyak jenis Kriptografi yang banyak digunakan, salah satunya yang akan kita bahas yaitu tentang Perbandingan proses Metode Stream Cipher dan Metode Hill Cipher.

Di Dalam Kriptografi ada banyak istilah-istilah yang akan sering didengar, diantaranya: Pesan (plainteks), Cipherteks (ciphertext), Enkripsi (encryption), dan Dekripsi (decryption).

Penelitian ini bertujuan untuk lebih mengetahui tentang bagaimana keamanan data dalam proses enkripsi juga deskripsi dari suatu pesan menggunakan Metode Stream Cipher dan Metode Hill Cipher.

II. TINJAUAN PUSTAKA

2.1. Sejarah Kriptografi

Kriptografi sudah digunakan sejak 4000 SM oleh bangsa Mesir, pada saat itu untuk menyampaikan pesan bangsa mesir menggunakan ukiran rahasia yang disebut hieroglyph. Terdapat kisah seorang ahli militer, Julius Caesar pada saat itu ingin memberikan sebuah pesan yang rahasia kepada seorang jenderal di medan perang. Pesan tersebut hanya bisa dikirim oleh seorang kurir. Sebelum pesanya diberikan kepada kurir, Julius Caesar mengacak pesan tersebut menjadi sebuah pesan yang tidak dapat dipahami oleh orang lain kecuali oleh jendral tersebut. Alasannya karena Julius Caesar tidak ingin pesannya itu terbaca oleh orang lain, sebab pesan tersebut mengandung pesan rahasia. Julius Caesar mengacak alphabet a=d, b=e, c=f dan seterusnya.

P-ISSN: 2548-1932
e-ISSN: 2549-7758

Apa yang dilakukan Julius Caesar merupakan implementasi dari kriptografi. Pesan awal sebelum diacak dan dirapikan oleh Julius Caesar disebut plaintext, sedangkan pada saat Julius Caesar mengacak pesan tersebut disebut sebagai proses enkripsi. Hasil dari enkripsi disebut sebagai ciphertext. Maka saat pesan diartikan oleh jenderal, proses itu disebut sebagai dekripsi.

Selain itu, Bangsa Yunani sudah memanfaatkan teknik kriptografi sejak 400 tahun SM. Hanya saja, alat yang digunakan bangsa Yunani ini berbeda dengan bangsa Mesir Kuno. Alat yang digunakan bangsa Yunani disebut *Scytale*. Scytale adalah suatu alat seperti pita panjang berbahan daun papyrus yang disusun pada sebatang silinder, pesan tersebut ditulis secara horizontal, apabila kertas dilepaskan, maka pesan akan berubah menjadi huruf-huruf yang sulit untuk diterjemahkan.[1]

2.2. Pengertian Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu kripto = tersembunyi/rahasia sedangkan graphia = tulisan. Jadi, bisa kita artikan bahwa kriptografi merupakan tulisan secara tersembunyi untuk menyampaikan pesan yang harus dijaga kerahasiaannya. Pesan yang dikirim bisa berbentuk video, audio gambar dan teks.

Di Indonesia, ilmu kriptografi juga disebut dengan sandi sastra. Menurut kronologi waktunya, kriptografi dibedakan menjadi kriptografi klasik dan kriptografi modern. Perbedaan diantaranya adalah dalam proses pembuatan pesan.

2.3. Istilah Kriptografi

Secara umum ada beberapa istilah yang sering digunakan dalam Kriptografi, diantaranya:

1. Kriptografi
   Ilmu maupun seni mengamankan pesan yang dilakukan seorang kriptographer.
2. Kriptanalisis
   Ilmu dan seni membuka (breaking) cipherteks.
3. Plainteks
   Pesan asli yang hendak dikirimkan atau data asli.
4. Cipherteks
   Pesan yang sudah terenkripsi atau pesan dari hasil enkripsi.
5. Enkripsi
   Proses pengubah plainteks menjadi cipherteks.
6. Dekripsi
   Kebalikan dari proses enkripsi yaitu mengubah pesan cipherteks menjadi plainteks, sehingga pesan seperti semula/asli.
7. Algoritma Kriptografi
   Kumpulan perintah perintah logis dan matematis, yang tersusun untuk melindungi suatu pesan tetap aman dari gangguan pihak lain.
8. Kunci
   Kunci, yang dimaksud adalah kunci yang dirahasiakan dalam proses enkripsi dan dekripsi. Ada 2 jenis kunci, yaitu kunci public (public key) dan kunci rahasia (private key).

2.4. Tujuan Kriptografi

Tujuan dari kriptografi adalah melindungi data dari serangan yang disengaja ataupun tidak, ada beberapa aspek keamanan dalam kriptografi, yaitu Kerahasiaan data, Keutuhan data, Otentik dan Anti-Penyangkalan. [1]

2.5. Metode Stream Cipher

Vernam adalah seseorang yang pertama kali memperkenalkan Stream Cipher melalui algoritmanya yang disebut dengan Vernam Cipher.

Stream Cipher sering disebut sebagai sandi aliran. Keunggulan dari metode ini yaitu relative lebih cepat dalam proses enkripsi-dekripsi dan juga tidak dibatasi panjang plainteksnya. Metode ini merupakan algoritma kunci simetri. Plainteks dalam Stream Cipher beroperasi dalam bit per bit, jadi dalam proses enkripsinya hanya ada 2 kemungkinan yang terjadi, yaitu berubah atau tidak berubah.

2.6. Metode Hill Cipher

Pada tahun 1929 Lester S. Hill menciptakan sebuah teknik Kriptografi untuk mengamankan sebuah data, yaitu metode Hill Cipher dengan maksud agar kode tidak dapat dipecahkan dengan teknik analisis frekuensi.

P-ISSN: 2548-1932
e-ISSN: 2549-7758

Hill Cipher adalah salah satu algoritma kriptografi dengan kunci simetris yang menggunakan perkalian matriks dan invers terhadap matriks yang berukuran m x n sebagai kunci untuk melakukan enkripsi dan dekripsi. Metode ini dikategorikan sebagai block cipher. Dasar dan teknik Hill Cipher merupakan aritmatika modulo. [2]

III. HASIL DAN PEMBAHASAN

Cara kerja metode Stream Cipher dan Hill Cipher, akan dibahas pada bagian ini, yaitu berupa gambaran perubahan dari pesan asli menjadi menjadi pesan rahasia atau enkripsi dan mengembalikan Kembali menjadi pesan biasa atau dekripsi.

3.1. Stream Cipher

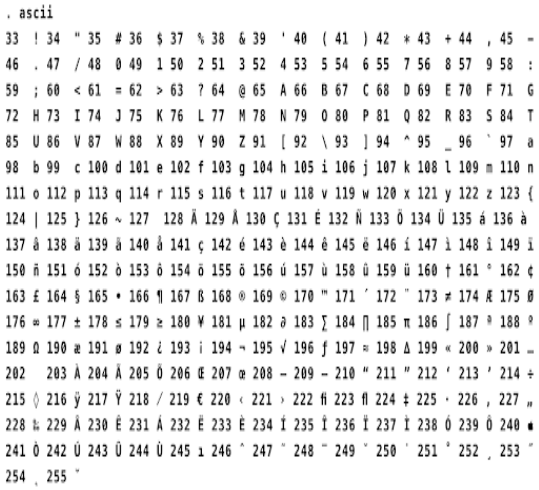
Jika karakter yang digunakan merupakan kode ascii, maka bisa dinyatakan sebagai modulo 256. [3]

1. Enkripsi
   Rumus : **C = (P + K) mod 256**
   Keterangan:
   C : Ciphertext
   K : Kunci
   P : Plaintext

   Plaintext : BAJU
   Kunci : 1234
   a. Mengubah Plaintext ke kode ASCII:
      B = 66
      A = 65
      J = 74
      U = 85
   b. Mengubah kunci ke kode ASCII:
      1 = 49
      2 = 50
      3 = 51
      4 = 52
   c. Perhitungan Enkripsi:
      P1 = (B + 1) mod 256
         = (66 + 49) mod 256
         = 115 mod 256 = 115 = s
      P1 = (A + 2) mod 256
         = (65 + 50) mod 256
         = 115 mod 256 = 115 = s
      P1 = (J + 3) mod 256
         = (74 + 51) mod 256
         = 125 mod 256 = 125 = }
      P1 = (U + 4) mod 256
         = (85 + 52) mod 256
         = 137 mod 256 = 137 = ë

   Cipertext: ss}ë

Kode ASCII:



2. Dekripsi
   Rumus : **P = (C – K) mod 256**

   Perhitungan Dekripsi:
   C1 = (s – 1) mod 256
      = (115 – 49) mod 256
      = 66 mod 256 = 66 = B
   C1 = (s – 2) mod 256
      = (115 – 50) mod 256
      = 65 mod 256 = 65 = A
   C1 = (} – 3) mod 256
      = (125 – 51) mod 256
      = 74 mod 256 = 74 = J
   C1 = (ë – 4) mod 256
      = (137 – 52) mod 256
      = 85 mod 256 = 85 = U

   Plaintext: BAJU

3.2. Hill Cipher

Proses dari metode ini yaitu, pesan pesan harus dikonversi dulu menjadi angka dari 0 - 25 sebelum menjadi deretan block.

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
J	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*
9	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
S	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	
18	**19**	**20**	**21**	**22**	**23**	**24**	**25**	

1. Enkripsi
   Rumus : ***C = K.P***
   Keterangan:
   C : Ciphertext
   K : Kunci

P : Plaintext

- Plaintext : BAJU
  $Kunci\ (K)$: (2 1 3 4)

Maka:

a. Membagi P jadi matriks 2 x 1 dan mengkonversikan menjadi angka yang sesuai dengan table

$$\left(\frac{B}{A}\right) = \left(\frac{1}{0}\right)$$

$$\left(\frac{J}{U}\right) = \left(\frac{9}{20}\right)$$

b. Mengalikan angka yang telah dikonversi dengan K

$$(2\ 1\ 3\ 4\ )\ x\ \left(\frac{1}{0}\right) = \left(\frac{2}{3}\right)$$

$$(2\ 1\ 3\ 4\ )\ x\ \left(\frac{9}{20}\right) = \left(\frac{38}{107}\right)$$

c. Melakukan operasi Mod 26

$$\left(\frac{2}{3}\right) mod\ 26 = \left(\frac{2}{3}\right)$$

$$\left(\frac{38}{107}\right) mod\ 26 = \left(\frac{12}{3}\right)$$

d. Mengubah matriks angka menjadi huruf

$$\left(\frac{2}{3}\right) = \left(\frac{C}{D}\right)$$

$$\left(\frac{12}{3}\right) = \left(\frac{M}{D}\right)$$

e. Hasil pesan BAJU yang telah dienkripsi menjadi CDMD.

2. Dekripsi
   Proses dekripsi metode ini sama dengan proses enkripsi, hanya saja pada metode ini K (kunci) nya harus di invers dulu.

Penurunan rumus:

$$C = K\ x\ P$$

$$K^{-1}\ x\ C = K^{-1}\ x\ K\ x\ P$$

$$K^{-1}\ x\ C = 1\ x\ P$$

$$P = K^{-1}\ x\ C$$

Maka rumusnya menjadi:

$$P = K^{-1}\ x\ C$$

Keterangan:
P : Plaintext
K^{-1} : Invers matriks kunci
C : Ciphertext

Untuk melakukan proses dekripsi, harus mencari nilai invers dari K (kunci) dengan prinsip Determinan.

$$Kunci\ (K) : (2\ 1\ 3\ 4\ )$$

$$Kunci\ K^{-1} : (6\ 5\ 15\ 16\ )$$

Matriks K-1 ini yang akan menjadi kunci pada proses dekripsi.

a) Membagi P jadi matriks 2 x 1 dan mengkonversikan menjadi angka yang sesuai dengan table

$$\left(\frac{C}{D}\right) = \left(\frac{2}{3}\right)$$

$$\left(\frac{M}{D}\right) = \left(\frac{12}{3}\right)$$

b) Mengalikan setiap angka dengan K-1

$$(6\ 5\ 15\ 16\ )\ x\ \left(\frac{2}{3}\right) = \left(\frac{27}{78}\right)$$

$$(6\ 5\ 15\ 16\ )\ x\ \left(\frac{12}{3}\right) = \left(\frac{87}{228}\right)$$

c) Melakukan operasi Mod 26

$$\left(\frac{27}{78}\right) mod\ 26 = \left(\frac{1}{0}\right)$$

$$\left(\frac{87}{228}\right) mod\ 26 = \left(\frac{9}{20}\right)$$

d) Mengubah matriks angka menjadi huruf

$$\left(\frac{1}{0}\right) = \left(\frac{B}{A}\right)$$

$$\left(\frac{9}{20}\right) = \left(\frac{J}{U}\right)$$

e) Maka hasil proses dekripsi menjadi BAJU. [2]

IV. PENUTUP

4.1. Kesimpulan

Berdasarkan pembahasan yang telah dipaparkan, maka kesimpulannya sebagai berikut:

1. Teknik Kriptografi merupakan alternatif yang baik dalam mengamankan data.
2. Dalam metode Stream Cipher data dapat diubah menjadi kode ASCII dengan perhitungan rumus sehingga dapat mengamankan data.
3. Hill Cipher harus dengan menggunakan matriks. Jika kunci nya semakin besar, maka akan semakin kuat tingkat keamanannya.

DAFTAR PUSTAKA

[1] M. K. Harahap, "Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 61–64, 2016, doi: 10.30743/infotekjar.v1i1.43.

[2] A. R. Yuliandaru, "Teknik Kriptografi Hill Cipher Menggunakan Matriks," 2016.

[3] M. A. Nasuton *et al.*, "Penerapan Metode Hill Cipher Dan Stream Cipher Dalam Mengamankan Database MySQL," pp. 532–544, 2010.

[4] D. Lestari, M. Z. Riyanto, U. N. Yogyakarta, and U. A. Dahlan, "A-5 suatu algoritma kriptografi stream cipher berdasarkan fungsi chaos," no. November, pp. 978–979, 2012.

[5] D. Lombu, S. D. Tarihoran, and I. Gulo, "Kombinasi Mode Cipher Block Chaining Dengan Algoritma Triangle Chain Cipher Pada Penyandian Login Website," *J-SAKTI (Jurnal Sains Komputer. dan Inform.*, vol. 2, no. 1, p. 1, 2018, doi: 10.30645/j-sakti.v2i1.51.