Implementasi Multi Enkripsi Menggunakan Algoritma *Hill Cipher* dan Algoritma ECB (*Electronic Code Book*)

Fadhil Dias Maulana[1], Gusti Eka Yuliastuti[2], Citra Nurina Prabiantissa[3]
Teknik Informatika, Institut Teknologi Adhi Tama Surabaya[1,2,3]
e-mail: fadhildias10@gmail.com[1]

ABSTRACT

Nowadays, computer technology has developed so rapidly in all aspects of human work to meet human needs, such as large data and information collection. Therefore, security procedures are needed for storing data and information so that they are protected from various threats such as data theft on important information of an agency or company. Cryptography is a branch of science that can be used to secure data until now. It continues to be developed through various algorithms. Researchers carried out analysis and implementation of multi-encryption using the Hill Cipher and the ECB algorithms. The main objective of this research was to secure resident data. The testing was carried out in encryption, description, and Avalanche Effect. The results showed that encryption and description tests worked well. Meanwhile, the Avalanche Effect test indicated that the multi-encryption test combining the Hill Cipher algorithm and the ECB algorithm was very good to encrypt population data compared to each single algorithm because the average Avalanche Effect resulted from the multi-encryption test was 53.21%. It was higher than the average Avalanche Effect from every single algorithm, namely the Hill Cipher and ECB algorithms.

Keywords: *Avalanche Effect, ECB, Hill Cipher, Cryptography, Multiple encryption.*

ABSTRAK

Pada saat ini teknologi komputer telah berkembang sedemikian pesat mencakup semua aspek pekerjaan manusia yang memenuhi kebutuhan manusia,seperti kumpulan data dan informasi yang besar.Sehingga diperlukan prosedur keamanan untuk penyimpanan data dan informasi agar terlindung dari berbagai ancaman seperti pencurian data pada informasi instansi atau perusahaan yang penting.Kriptografi merupakan salah satu cabang ilmu yang dapat digunakan untuk mengamankan data hingga saat ini terus dikembangkan melalui berbagai algoritma. Peneliti melakukan analisis dan implementasi multi enkripsi menggunakan algoritma *Hill Cipher* dan algoritma ECB.Tujuan utama penelitian ini adalah untuk mengamankan data penduduk.Penulis melakukan pengujian dengan melakukan uji coba enkripsi kemudian dekripsi dan juga pengujian *Avalanche Effect*.Hasil pengujian menunjukkan pengujian enkripsi dan dekripsi bisa dilakukan dengan baik.Sedangkan untuk pengujian *Avalanche Effect* didapatkan bahwa pengujian multi enkripsi dari kombinasi algoritma *Hill Cipher* dan algoritma ECB sangat bagus untuk digunakan untuk mengenkripsi data penduduk dibandingkan masing-masing algoritma tunggal karena hasil rata-rata *Avalanche Effect* dari pengujian multi enkripsi didapatkan yaitu 53.21% yang mana itu lebih tinggi daripada rata-rata *Avalanche Effect* masing-masing algoritma tunggal yaitu algoritma *Hill Cipher* dan ECB.

Kata kunci: *Avalanche Effect* , ECB , *Hill Cipher*, Kriptografi, Multi enkripsi.

PENDAHULUAN

Pada saat ini teknologi komputer telah berkembang sedemikian pesat, sehingga sekarang mencakup semua aspek pekerjaan manusia yang memenuhi kebutuhan manusia, seperti kumpulan data dan informasi yang besar[1].Diperlukan prosedur keamanan untuk penyimpanan data dan informasi agar terlindung dari berbagai ancaman seperti seseorang yang dapat dengan mudah melihat, merusak, mencuri, atau menyalahgunakan data atau informasi instansi atau perusahaan yang penting[2].Pengamanan informasi menjadi sangat penting dalam rangka menjaga privasi dan keamanan informasi tersebut salah satunya adalah data penduduk. Data penduduk menyimpan data

dari setiap penduduk yang mana dalam data tersebut mempunyai data-data yang sangat penting. Sehingga pengamanan suatu data menjadi sangat penting untuk dijadikan perhatian dan dengan hal tersebut maka keamanan sangat penting yang mana perlu didalami dan diperhatikan[3]. Adapun solusi untuk mengatasi permasalahan tersebut yakni dengan menerapkan kriptografi[4]

Dengan menggunakan metode penyandian yaitu kriptografi memungkinkan penyembunyian informasi yang dianggap rahasia sehingga tidak dapat dipahami oleh siapa pun selain pencipta dan penerimanya.Saat ini, berbagai algoritma kriptografi, termasuk RSA, AES, MD5, Vigenere, DES, Blowfish, MD2, dan lainnya, digunakan untuk menjaga keamanan data. Penulis mencoba membahas algoritma kriptografi *Hill Cipher*dan algoritma ECB (Elecetronic Code Book) pada bagian ini karena masih ada algoritma kriptografi lain selain yang telah disebutkan di atas. Algoritma *Hill Cipher* adalah algoritma kriptografi klasik yang menggunakan matriks perkalian sebagai proses enkripsi dan dekripsi yang membuat sangat sulit dipecahkan[5].Tetapi pada algoritma *Hill Cipher*hanya dapat mengenkripsi data berupa huruf saja.Maka dari itu dibutuhkan algoritma yang bisa melakukan enkripsi dan dekripsi pada data yang berupa angka. Oleh karena itu algoritma ECB (*Electronic Code Book*) digunakan untuk mengatasi kelemahan algoritma *Hill Cipher*.

TINJAUAN PUSTAKA

Algoritma *Hill Cipher*

Metode kriptografi ini dibuat agar dapat membuat cipher (kode) yang sangat sulit dipecahkan menggunakan teknik analisis frekuensi. *Hill Cipher*tidak mengubah setiap huruf yang serupa pada plaintext dengan huruf lainnya yang serupa pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya. Teknik *Hill Cipher*menggunakan aritmatika modulo terhadap matriks.Dalam pengerjaannya, *Hill Cipher*memakai teknik perkalian matriks dan teknik invers terhadap matriks. Secara matematis,proses enkripsi pada *Hill Cipher* adalah: $\boldsymbol{C} = \boldsymbol{K} . \boldsymbol{P}$

Keterangan :

C = Ciphertext

K = Kunci

P = Plaintext

Selanjutnya untuk proses dekripsi algoritma *Hill Cipher* pada dasarnya sama dengan proses enkripsinya.Namun matriks kunci harus dibalik(invers) terlebih dahulu. Secara matematis,proses dekripsi *Hill Cipher* adalah $\boldsymbol{P} = \boldsymbol{K}^{-1} . \boldsymbol{C}$

Keterangan :

P = plaintext.

K^{-1} = invers matriks kunci

C = ciphertext

Algoritma ECB (*Electronic Code Book*)

Pada mode operasi ECB sebuah blok input plaintext dipetakan secara statis ke sebuah blok output ciphertext. Sehingga tiap plaintext yang sama akan menghasilkan ciphertext yang selalu sama pula.Sifat- sifat dari mode operasi ECB :

a) Sederhana dan efisien
b) Memungkinkan implementasi parallel
c) Tidak menyembunyikan pola Plaintext

Pada sistem, setiap blok plainteks pi, dienkripsi secara individual dan independen menjadi blok cipherteks ci. Secara matematis, enkripsi dengan mode ECB dinyatakan sebagai Ci = Ek (Pi) sedangkan dekripsi sebagai Pi = Dk (Ci) Dalam hal ini, K adalah kunci dan Pi dan Ci masing-masing blok plainteks dan cipherteks ke-1[6].

Avalanche Effect

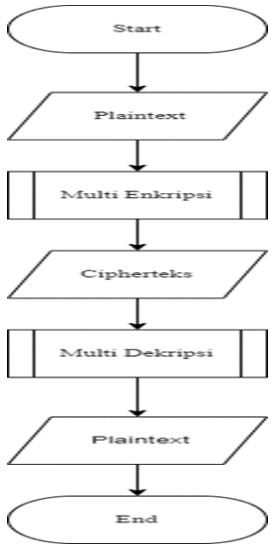
Avalanche Effect adalah sebuah metode untuk mencari dan mengetahui berapa persen pengubahan pesan pada saat proses enkripsi dilakukan dengan melihat rasio antara jumlah bit dari cipherteks yang berubah dan jumlah bit dari plainteks sebelum dirubah dalam proses enkripsi.Pengujian *Avalanche Effect* dianggap baik apabila terjadi perubahan bit yang menunjukkan antara 45-60% (50 % adalah hasil yang dianggap baik dalam pengujian).Perubahaan sebesar 50% akan mengakibatkan masalah yang cukup sulit untuk para pembobol melakukan serangan terhadap data yang dimiliki sesuai pada persaman[7]. Rumus dari *Avalanche Effect* seperti persamaan 1 :

$$Avalanche\ Effect = \frac{Jumlah\ bit\ berbeda}{total\ bit} \times 100\% \quad (1)$$

METODE

Flowchart Sistem

Pada gambar 1 menjelaskan flowchart sistem tentang sistem kombinasi algoritma *Hill Cipher* dan algoritma ECB.Yang pertama menginputkan data atau plaintext, kemudian melakukan multi enkripsi menggunakan algoritma *Hill Cipher* dan algoritma ECB.Setelah itu nantinya akan menghasilkan yaitu cipherteks dari multi enkripsi tadi.Kemudian cipherteks di multi dekripsi menngunakan algoritma ECB dan algoritma *Hill Cipher* dan setelah itu akan menghasilkan palinteks atau data yang awal.



Gambar 1. Flowchart Sistem

HASIL DAN PEMBAHASAN

Pengujian proses enkripsi dan dekripsi

Pengujian proses multi enkripsi ini menggunakan 2 kunci dari algoritma *Hill Cipher* dan ECB yang telah disusun dengan mengambil data penduduk dan didapatkan hasil seperti tabel 1 berikut

Tabel 1. Pengujian proses enkripsi dan dekripsi

Data Pengujian proses					Hasil
No	Plaintext	Key	Enkripsi	Dekripsi	
1	5415140349610072 AGUS BLOK 23 085732124112	$\begin{bmatrix}5 & 2\\6 & 3\end{bmatrix}$ / AKI	e8 fe f0 e8 f4 fa e2 f0 fa f0 fa f0 e2 f6 fc e6 18 30 1c 24 06 0a 08 14 d6 f6 e4 e2 e6 f8 ec f0 f6 e0 f2 fa e0 f4 f6	5415140349610072 AGUS BLOK 23 085732124112	Berhasil

Pada tabel 1 menunjukkan hasil proses enkripsi dan dekripsi menggunakan 2 algoritma yaitu algoritma *Hill Cipher* dan algoritma ECB.Tabel ini terdapat plaintext yang terdiri dari data penduduk berupa NIK,nama penduduk,alamat,dan no telepon. Kemudian terdapat 2 key yang akan digunakan untuk enkripsi dan dekripsi.Hasil dari enkripsi dari algoritma multi enkripsi berupa hexadecimal.Kemudian proses dekripsi menggunakan 2 kunci yang sama yang digunakan saat proses enkripsi. Jika dalam hasil terdapat tulisan "Berhasil" maka proses dekripsi berhasil ,dengan kata lain data kembali ke data awal atau data asli.

Pengujian *Avalanche Effect*

Pengujian ini dilakukan untuk mendapatkan hasil data dari keseluruhan proses. Pada pengujian ini terdapat 3 pengujian yaitu pengujian algoritma *Hill Cipher* pada tabel 2,algoritma ECB pada tabel 3,dan algoritma multi enkripsi pada tabel 4 yang mana nantinya akan dibandingkan 3 pengujian tersebut

Tabel 2 Pengujian algoritma *Hill Cipher*

Pengujian *Avalanche Effect*			
No	Jumlah bit berbeda	Total bit keseluruhan	Hasil (%)
1	10	336	2.97%
2	15	336	4.46%
3	21	352	5.96%
4	11	328	3.35%
5	9	336	2.67%
Total Rata-Rata			3.88%

Pada tabel 2 merupakan hasil pengujian *Avalanche Effect* dari algoritma *Hill Cipher*.Pengujian tersebut menggunakan sampel data penduduk sebanyak 5 data penduduk.Dari hasil pengujian *Avalanche Effect* didapatkan nilai terkecil *Avalanche Effect* adalah 2.67% dan nilai

terbesar *Avalanche Effect* didapatkan adalah 5.96%.Dan untuk rata-rata pengujian *Avalanche Effect* didapatkan adalah 3.88%

Kemudian terdapat pengujian *Avalanche Effect* dari algoritma ECB seperti pada tabel 3

Tabel 3. Pengujian algoritma ECB

Pengujian *Avalanche Effect*			
No	Jumlah bit berbeda	Total bit keseluruhan	Hasil (%)
1	167	336	49.70%
2	177	328	53.96%
3	175	336	52.08%
4	186	352	52.84%
5	166	312	53.20%
Total Rata-Rata			52.35%

Pada tabel 3 merupakan hasil pengujian *Avalanche Effect* dari algoritma ECB.Pengujian tersebut menggunakan sampel data penduduk sebanyak 5 data penduduk.Dari hasil pengujian *Avalanche Effect* didapatkan nilai terkecil *Avalanche Effect* adalah 49.70% dan nilai terbesar *Avalanche Effect* didapatkan adalah 53.96% Dan untuk rata-rata pengujian *Avalanche Effect* didapatkan adalah 52.35%

Kemudian terdapat pengujian *Avalanche Effect* dari kombinasi antara algoritma *Hill Cipher* dan algoritma ECB seperti pada tabel 4

Tabel 4. Pengujian Multi enkripsi

Pengujian *Avalanche Effect*			
No	Jumlah bit berbeda	Total bit keseluruhan	Hasil (%)
1	171	336	50.89%
2	168	312	53.84%
3	180	336	53.57%
4	182	328	55.48%
5	183	344	53.19%
Total Rata-Rata			53.39%

Pada tabel 4 merupakan hasil pengujian *Avalanche Effect* multi enkripsi dari algoritma *Hill Cipher* dan algoritma ECB Pengujian tersebut menggunakan sampel data penduduk sebanyak 5 data penduduk.Dari hasil pengujian *Avalanche Effect* didapatkan nilai terkecil *Avalanche Effect* adalah 50.89% dan nilai terbesar *Avalanche Effect* didapatkan adalah 55.48% Dan untuk rata-rata pengujian *Avalanche Effect* didapatkan adalah 53.39%

Analisis Hasil Pengujian

Dari perbandingan 3 pengujian *Avalanche Effect* pada tabel 2,tabel 3, dan tabel 4 didapatkan bahwa algoritma multi enkripsi sangat bagus untuk digunakan untuk mengenkripsi data penduduk dibandingkan 2 pengujian algorima tunggal yaitu pengujian *Avalanche Effect* dari algoritma *Hill Cipher* dan pengujian *Avalanche Effect* algoritma ECB karena hasil rata-rata *Avalanche Effect* dari pengujian multi enkripsi didapatkan yaitu 53.21% yang mana itu lebih tinggi

dibandingkan 2 pengujian algoritma tunggal seperti algoritma *Hill Cipher* yang memiliki rata-rata *Avalanche Effect* yaitu 3.88% dan algoritma ECB memiliki rata-rata *Avalanche Effect* yaitu 52.53%

KESIMPULAN

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

1. Proses enkripsi dan dekripsi dengan menggunakan metode gabungan seperti algoritma *Hill Cipher* dan algoritma ECB dapat dilakukan
2. Hasil perbandingan antara pengujian *Avalanche Effect* dari algoritma *Hill Cipher*,algoritma ECB,dan algoritma multi enkripsi didapatkan bahwa algoritma multi enkripsi sangat bagus digunakan dalam mengenkripsi data penduduk karena pengujian multi enkripsi ini memiliki hasil rata-rata *Avalanche Effect* yaitu 53.21%.Hasil tersebut lebih baik dibandingkan masing-masing algoritma tunggal seperti algoritma *Hill Cipher* yang memiliki rata-rata *Avalanche Effect* yaitu 3.88% dan algoritma ECB memiliki rata-rata *Avalanche Effect* yaitu 52.22%.
3.

DAFTAR PUSTAKA

[1] Y. Wiharto and A. Irawan, “ENKRIPSI DATA MENGGUNAKAN ADVANCED ENCRYPTION STANDARD 256,” vol. 7, no. 2, p. 9, 2018.
[2] A. Hermawan and E. I. H. Ujianto, “Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA,” vol. 5, p. 6, 2021.
[3] R. V. H. Chandra, A. Kusyanti, and M. Data, “Analisis Performa Proses Enkripsi dan Dekripsi Menggunakan Algoritme AES-128 Pada Berbagai Format File,” p. 7, 2019.
[4] D. H. Sulaksono, C. N. Prabiantissa, G. E. Yuliastuti, and A. R. Taqwa, “Implementasi Kriptografi dengan Metode Elliptic Curve Cryptography (ECC) untuk Aplikasi Chatting Berbasis Android,” 2021.
[5] A. H. Hasugian, “IMPLEMENTASI ALGORITMA *HILL CIPHER* DALAM PENYANDIAN DATA,” p. 9, 2013.
[6] A. Mufid, “TEKNIK ENKRIPSI DAN DESKRIPSI MENGGUNAKAN ALGORITHMA *ELECTRONIC CODE BOOK* (ECB),” 2010.
[7] Muslih Muslih and Lekso Budi Handoko, “PENGUJIAN *AVALANCHE EFFECT* PADA KRIPTOGRAFI TEKS MENGGUNAKAN AUTOKEY CIPHER,” *Semin. Nas. Teknol. Dan Multidisiplin Ilmu SEMNASTEKMU*, vol. 2, no. 1, pp. 127–134, Dec. 2022, doi: 10.51903/semnastekmu.v2i1.162.