Implementasi Kombinasi Algoritma Rot13 dan Vernam Cipher untuk Keamanan Data Teks

Rafli Abi Assyarif, Gusti Eka Yuliastuti , Citra Nurina Prabiantissa

Institut Teknologi Adi Tama Surabaya
e-mail: abiraden55@gmail.com

ABSTRACT

Data security is a crucial issue and very influential in various sectors, including at every level of each sector concerned. Encryption is one of the strategies to protect data, but there are significant bottlenecks in terms of execution time and resource usage, especially for strong encryption methods. Researchers combined two classic encryption techniques to overcome the barriers that previously existed, namely ROT13 and the Vernam Cipher. This technique offers real-time encryption with a shorter execution duration but still has a high level of security due to the use of two encryption algorithms. In the ROT13 method, data were scrambled by rotating 13 alphabetical positions from their initial position and then processed again using the Vernam Cipher method, which is also known as a one-time pad cipher, to make it more difficult for encryption to be penetrated. The Avalanche Effect test on this method produces an average value above 60%, indicating that the level of security provided was strong enough even with a relatively short execution time. The combination of both encryption methods has been applied to a MySQL database containing population data and has been proven to function efficiently.

Kata kunci: *encryption, ROT13, Verman Cipher*

ABSTRAK

Keamanan data merupakan isu krusial yang sangat berpengaruh pada berbagai sektor serta setiap tingkatan dari masing-masing sektor yang bersangkutan. Enkripsi merupakan salah satu strategi yang digunakan dalam melindungi data tetapi terdapat hambatan dalam hal waktu eksekusi dan penggunaan sumber daya yang signifikan, khususnya untuk metode enkripsi kuat. peneliti menggabungkan dua teknik enkripsi klasik dengan tujuan untuk mengatasi hambatan yang ada sebelumnya yaitu ROT13 dan Vernam Cipher. Teknik ini menawarkan enkripsi real-time dengan durasi eksekusi yang lebih pendek namun tetap memiliki tingkat keamanan yang tinggi sebab penggunaan dua algoritma enkripsi. Dalam metode ROT13 data diacak dengan melakukan rotasi 13 posisi alfabet dari posisi awal kemudian diproses kembali menggunakan metode Vernam Cipher yang juga dikenal sebagai cipher one-time pad yang semakin mempersulit enkripsi untuk ditembus. Pengujian metode ini ditunjukkan melalui pengujian Avalanche Effect yang menghasilkan nilai rata-rata di atas 60% sehingga mengindikasikan bahwa tingkat keamanan yang diberikan cukup kuat meskipun dengan waktu eksekusi yang relatif singkat. Implementasi gabungan metode enkripsi ini telah diaplikasikan pada database MySQL yang berisi data penduduk dan terbukti berfungsi secara efisien.

Kata kunci: enkripsi, ROT13, Verman Cipher

PENDAHULUAN

Teknologi komputer pada disaat ini sudah hadapi pertumbuhan yang sangat pesat yang di iringi dengan kumpulan informasi serta data yang besar. Pada penyimpanan informasi dan data, diperlukan proses pengamanan supaya informasi dan data bisa dilindungi dari bermacam ancaman semacam dapat dengan gampang seorang memandang, mengganggu, mencuri maupun menyalahgunakan informasi ataupun data berarti dari sesuatu lembaga ataupun industri. Salah satu metode dalam melaksanakan pengamanan informasi dan data merupakan mengenakan metode kriptografi [1].

Kriptografi sudah banyak digunakan oleh banyak bidang khususnya dalam bidang informatika, seperti membuat penyandian pada text password yang digunakan pengguna untuk

login ke dalam sistem berbasis digital agar tidak dapat dimengerti oleh orang yang tidak berkepentingan [2]. Hal yang sama juga dilakukan seperti pada file data–text yang sangat rentan dalam fleksibilitas dan mobilitas yang sangat tinggi. Sehingga butuh sualtu mekanisme untuk mengamankan data–text[3]. Kriptografi memiliki dua konsep yang penting, yaitu enkripsi dan dekripsi. Enkripsi mengubah informasi atau data menjadi bentuk yang hampir tidak dikenali seperti informasi awal menggunakan algoritma tertentu, sedangkan dekripsi mengubah bentuk tersamar tersebut menjadi informasi awal [2].

ROT13 (rotate 13) adalah enkripsi substitution cipher yang umum digunakan di sistem operasi UNIX. Pada sistem enkripsi ROT13 sebuah huruf digantikan dengan huruf yang letaknya di atas 13 posisi darinya[2]. Algoritma ROT13 merupakan algoritma turunan dari algoritma caesar chiper yang yang ditemukan dan digunakan oleh Julius Caesar pada tahun 50 SM. Algoritma ROT13 merupakan sebuah algoritmal kriptografi sederhana yang menggunakan sandi abjad-tunggal dengan pergeseran sejauh 13 karakter. algoritma ROT13 biasanya digunakan di sistem operasi unix, penyandian file text menggunakan algoritma ROT 13. Algoritma ROT13 dapat mengurangi masalah-masalah yang sering terjadi seperti pencurian file text, penyalahgunaan file text, dan merusak file text[4].

Vernam cipher merupakan algoritma kriptografi yang ditemukan oleh mayor j. Mougborne dan g. Vernam. Algoritma vernam cipher diadopsi dari one time pad cipher, dimana dalam hal ini karakter diganti dengan bit (0 atau 1). Dengan kata lain, vernam cipher merupakan versi lain dari one-time pad cipher. Algoritma kriptografi vernam cipher merupakan algoritma kriptografi berjenis symmetric key. Kunci yang digunakan untuk melakukan enkripsi dan deskripsi menggunakan kunci yang sama. Dalam melakukan proses enkripsi, algoritma vernam cipher menggunakan cara stream cipher dimana cipher berasal dari hasil operasi XOR antara bit plaintext dan bit key. Pada cipher aliran, bit hanya mempunyai dua buah nilai, sehingga proses enkripsi hanya menyebabkan dua keadaan pada bit tersebut, yaitu berubah atau tidak berubah. Dua keadaan tersebut ditentukan olehkunci enkripsi yang disebut dengan aliran bit kunci (keystream)[5].

TINJAUAN PUSTAKA

Implementasi Enkripsi

Adapun implementasi yang diterapkan pada kombinasi dua metode enkripsi yaitu ROT13 dan Vernam yaitu dengan menerapkan kombinasi kedua enkripsi tersebut kedalam enkripsi database dimana value data yang nantinya akan dimasukkan kedalam database akan dienkripsi terlebih dahulu sehingga nantinya pada saat data tersebut berada didalam database sudah dalam keadaan terenkripsi.

Enkripsi ROT13

Caesar Cipher ROT13 adalah fungsi yang menggunakan kode kaisar dengan pergeseran k=13. ROT13 didesain untuk keamanan pada sistem operasi UNIX yang sering digunakan pada forum online, berfungsi untuk menyelubungi isi artikel sehingga hanya orang yang berhak yang dapat membacanya. Sistem enkripsi ROT13 kali ini dengan menggeser maju karakter sebanyak 13 kali, terhitung 1 adalah karakter didepannya, dan pergeseran karakter berdasarkan urutan karakter pada tabel index sebagai dekripsinya, dengan menggeser mundur karakter sebanyak 13 kali [7]

Dalam perhitungan matematis, enkripsi dengan menggunakan algoritma ROT13 dapat dihitung manual dengan rumus sebagai berikut

$$Ci = (Pi + Ki) \text{ Mod } 26 \quad (1)$$

Sedangkan untuk dekripsi perhitungan manual dari algoritma ROT13 adalah sebagai berikut

$$Pi = (Ci-Ki) \text{ Mod } 26 \quad (2)$$

Keterangan :

Ci = Ciphertext

Pi = Plaintext

Ki = Key

Mod = Jumlah karakter yang digunakan

Vernam Cipher

Vernam cipher atau *one-time-pad* adalah metode enkripsi simetris yang fundamental tetapi unik dan tidak dapat dipecahkan, "simetris" berarti menggunakan kunci yang sama untuk enkripsi seperti halnya untuk dekripsi . *Vernam cipher* adalah metode atau teknik enkripsi yang menghasilkan kerahasiaan sempurna. Didukung oleh beberapa penelitian yang menyatakan bahwa metode vernam cipher (atau one-time pad) telah menjadi dan memainkan peran penting dalam kriptografi karena merupakan sistem kerahasiaan yang sempurna [8].

Proses Enkripsi metode ini adalah sebagai berikut :

Misalkan :

Plaintext : T

Key : 1

Kemudian rubah Plaintext dan Key menjadi biner, Kemudian lakukan proses enkripsi dengan menggunakan logika Ex-OR.

T : 01010100

1 : 00110011 $\oplus$

01100111

Setelah didapatkan hasil dari proses enkripsi dengan logika Ex-OR, maka nilai-nilai biner tersebut dikonversikan kembali ke dalam bentuk karakter. Jadi ciphertext dari plaintext T adalah g yang didapat dari biner (01100111). Sedangkan untuk proses dekripsi sama dengan pada proses enkripsi yaitu dengan melakukan proses Ex-OR pada ciphertext dan key.

Avalanche Effect

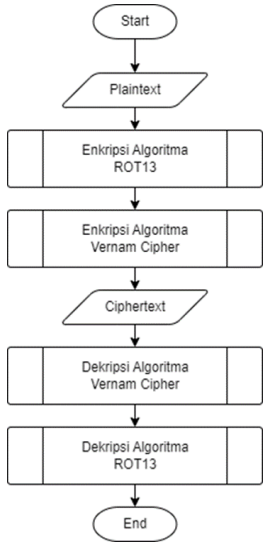
Avalanche Effect adalah sebuah metode untuk mencari dan mengetahui berapa persen pengubahan pesan pada saat proses enkripsi dilakukan dengan melihat rasio antara jumlah bit dari ciphertext yang berubah dan jumlah bit dari plaintext sebelum dirubah dalam proses enkripsi, semakin besar persen yang dihasilkan semakin bagus juga enkripsi yang dihasilkan dan sebaliknya. Pengujian Avalanche Effect dianggap baik apabila terjadi perubahan bit yang menunjukkan antara 45-60% (50 % adalah hasil yang dianggap baik dalam pengujian). Perubahan sebesar 50% akan mengakibatkan masalah yang cukup sulit untuk para pembobol melakukan serangan terhadap data yang dimiliki sesuai pada persaman [9].

$$Avalanche\ effect = \frac{\text{jumlah bit berubah}}{\text{jumlah bit total}} * 100\% \qquad 3$$

METODE

Rancangan Sistem

Untuk menjalankan penelitian, peneliti akan mengikuti langkah-langkah yang terstruktur dan valid agar proses penelitian dapat berlangsung dengan lancar dan mencapai alur penelitian yang diinginkan. Berikut adalah gambar alur (flowchart) yang menggambarkan tahap-tahap penelitian yang dilakukan oleh peneliti.:



Gambar 1 Rancangan sistem

Gambar 1 merupakan alur gambaran umum sistem yang dimulai dengan Multi enkripsi dengan menggunakan algoritma ROT13 dan algoritma Vernam cipher. Kemudian untuk dekripsi dilakukan dengan cara Multi dekripsi menggunakan algoritma Vernam Cipher dan dilanjut menggunakan algoritma ROT13

Enkripsi gabungan

ROT13 adalah metode enkripsi sederhana yang menggeser setiap huruf dalam teks sebanyak 13 posisi dalam alfabet. Verman cipher adalah metode enkripsi simetris yang menggunakan kunci acak yang sama panjang dengan teks. Langkah pertama dalam menggabungkan kedua metode ini adalah melakukan enkripsi ROT13 terhadap teks asli. Kemudian, hasil dari enkripsi ROT13 akan diproses kembali menggunakan verman cipher dengan kunci acak yang telah ditentukan.

HASIL DAN PEMBAHASAN

Untuk menguji keamanan data yang dienkripsi, peneliti menggunakan metode avalanche effect sebagai ukuran. Avalanche effect adalah perbandingan antara jumlah bit yang berubah dalam ciphertext akibat perubahan dalam plaintext. Semakin tinggi persentase bit ciphertext yang berubah, semakin sulit data dienkripsi untuk ditebak. Jika persentase bit ciphertext mencapai setengah (50%), maka data dienkripsi sangat aman. Dalam pengujian ini, penulis akan mengukur efek avalanche (perubahan plaintext) pada proses enkripsi untuk melihat seberapa banyak bit yang berubah dalam plaintext dan menilai seberapa baik kualitasnya. Dalam rangka melakukan pengujian metode enkripsi, peneliti melakukan percobaan dengan melakukan rangkaian pengujian avalanche effect gabungan sesuai dengan rumus sebelumnya pada 30 sampel data berupa nama penduduk dibawah ini.

Tabel 1. Data Penduduk

No	Nama Penduduk	Persentase
1	SAMPINING	62,50%
2	NAIN FAHRUROZZI	65,62%

No	Nama Penduduk	Persentase
3	MASKUR	71,43%
4	WARNITI	68,75%
5	AYUNDA TIARA EKA	63,24%
6	SAROPAH	62,50%
7	SRI WULANDARI	55,36%
8	DIDIK ISWANTO	66,67%
9	WARSITI	70,31%
10	AMAT	72,50%
11	JUPRI	72,92%
12	DAIB	72,50%
13	SENADI	66,07%
14	SUMARMI	64,06%
15	KUSWANAH	60,50%
16	DENAN	66,67%
17	KASTANI	67,19%
18	SISWANDI	61,11%
19	SUTIK	64,58%
20	MARNI	75,00%
21	WARTI	77,08%
22	RITA	70,00%
23	NANDA AKBAR S	63,33%
24	SISWO	64,58%
25	TRIYANTO	63,89%
26	ICKSAN	67,86%
27	SATRI	75,00%
28	YATI	72,50%
29	WINARSIH	56,94%
30	MUSRIATI	65,28%
Rata-Rata		66,86%

Data tabel 1 menunjukkan bahwa persentase rata-rata hasil pengujian avalanche effect metode kombinasi antara ROT13 dengan Verman Cipher sebesar 66,86% dimana hasil tersebut sudah tergolong kedalam hasil yang baik karena sudah diatas standar minimal yaitu 50%.

KESIMPULAN

Berdasarkan penelitian dan praktek uji coba yang telah dilakukan, dapat diambil beberapa kesimpulan sebagai berikut ini:

1. Kombinasi enkripsi antara ROT13 dengan Verman Cipher menghasilkan enkripsi yang tergolong cukup kuat hal ini dapat dibuktikan dari nilai rata-rata pengujian avalanche effect yang diperoleh yaitu 66,86% dan sudah melebihi batas minimal dari standar umum avalanche effect yang biasa digunakan yaitu lebih dari 50%.
2. Kombinasi enkripsi antara ROT13 dengan Verman Cipher menghasilkan enkripsi dengan keunikan yang berbeda dengan metode enkripsi lainnya karena karakter huruf pada plaintext bisa berubah menjadi karakter lain berupa simbol ketika dikonversi menjadi ciphertext.
3. Kombinasi metode enkripsi ROT13 dan Verman Cipher menghasilkan ciphertext acak dengan panjang bit bervariasi sesuai dengan plaintext yang akan dienkripsi sehingga lebih sulit bagi penyerang untuk mengidentifikasi pola atau mencari kelemahan dalam algoritma enkripsi karena teks menjadi lebih kompleks dan sulit untuk dianalisis.

DAFTAR PUSTAKA

[1] A. H. Erik Iman Heri Ujianto, "Implementasi Enkripsi Data Menggunakan Kombinasi AES Dan RSA," *InfoTekJar J. Nas. Inform. Dan Teknol. Jar.*, vol. 5, Mar. 2021, doi: https://doi.org/10.30743/infotekjar.v5i2.3585.

[2] permana Angga Aditya, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android," *LP2M Lemb. Penelit. Dan Pengemb. Masy.*, vol. 4, Mar. 2018, doi: http://dx.doi.org/10.36722/sst.v4i3.280.

[3] C. N. P. Gusti E Yuliastuti, "Implementasi Kriptografi dengan Metode Elliptic Curve Cryptography (ECC) untuk Aplikasi Chatting Berbasis Android," *Pros. Semin. Nas. Sains Dan Teknol. Terap.*, vol. 9, no. 1, pp. 570–576.

[4] H. Hendrik, "Kombinasi Algoritma Huffman dan Algoritma ROT 13 Dalam Pengamanan File Docx," *J. Inf. Syst. Res. JOSH*, vol. 2 NO 1, OKTOBER 2020.

[5] Z. Shabrizqi, "Penerapan Algoritma Vegenere Cipher Dan Vernam Cipher Dalam Penggamanan File Text," *JURIKOM J. Ris. Komput.*, vol. Vol 6, 2019, doi: http://dx.doi.org/10.30865/jurikom.v6i3.1345.

[6] N. S. Dewi Kusumaningsih, "ADVANCED ENCRYPTION STANDARD UNTUK KEAMANAN BASIS DATA DI KANTOR KECAMATAN KARANG TENGAH," *SKANIKA*, vol. 1, Jul. 2018.

[7] M. Z. Z. M. ZAINUDIN ZUHRI, "IMPLEMENTASI ALGORITMA ROT13 DAN ELGAMAL UNTUK ENKRIPSI DAN DEKRIPSI PESAN RAHASIA," *Simki-Techsain*, Aug. 2018.

[8] F. S. Gading Nur Salmi, "Implementation of the data encryption using caesar cipher and vernam cipher methods based on CrypTool2," *J. Soft Comput. Explor.*, no. Vol. 3 No. 2 (2022): September 2022, Sep. 2022, doi: https://doi.org/10.52465/joscex.v3i2.86.

[9] Muslih, "PENGUJIAN AVALANCHE EFFECT PADA KRIPTOGRAFI TEKS MENGGUNAKAN AUTOKEY CIPHER," *STEKOM*, vol. 2 No 1 2022, 2022.