PERBANDINGAN ALGORITMA CIPHER DENGAN ALGORITMA ROT13 PADA PROSES PENGAMANAN DATA

Oleh:
Dahlan Kurniawan [1)]
Nova Mayasari [2)]
Wirda Fitriani [3)]
Universitas Pembangunan Panca Budi, Medan [1,2,3)]
E-mail:
dahlankurniawan@gmail.com [1)]
novamayasari@gmail.com [2)]
wirdafitriani@gmail.com [3)]

ABSTRACT

Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun dekripsi. Teknik ini digunakan untuk mengkonversi data menjadi bentuk kode-kode tertentu, dengan tujuan agar informasi yang tersimpan tidak dapat terbaca oleh siapapun kecuali orang-orang yang berhak. Banyaknya algoritma kriptografi membuat penulis menguji kinerja algoritma Cipher dan algoritma ROT13 dalam mengamankan data. Dengan tujuan mendapatkan keamanan yang efektif dan efesien. Dengan menggunakan aplikasi yang dibangun maka peneliti menguji algoritma cipher dan algoritma ROT13 dengan mengukur kecepatan dalam melakukan enkripsi dan dekripsi. hasil pengujian yang dilakukan dengan menggunakan plainteks yang sama yaitu "DAHLANKURNIAWAN" maka menghasilkan enkripsi 8 miliseconds dan dekripsi 5 miliseconds pada algoritma cipher sedangkan pada algoritma ROT13 enkripsi 5 miliseconds dan dekripsi 5 miliseconds.

Keywords: Kriptografi, Algoritma Cipher. Algoritma ROT13

ABSTRAK

Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun dekripsi. Teknik ini digunakan untuk mengubah data menjadi bentuk kode-kode tertentu, dengan tujuan agar informasi yang disimpan tidak dapat dibaca oleh siapa pun kecuali orang yang berhak. Banyaknya algoritma kriptografi membuat penulis menguji algoritma Cipher dan algoritma ROT13 dalam data. Dengan tujuan mendapatkan keamanan yang efektif dan efesien. Dengan menggunakan aplikasi yang dibangun maka peneliti menguji algoritma cipher dan algoritma ROT13 dengan mengukur kecepatan dalam melakukan enkripsi dan dekripsi. hasil pengujian yang dilakukan dengan menggunakan plainteks yang sama yaitu "DAHLANKURNIAWAN" maka menghasilkan enkripsi 8 milidetik dan dekripsi 5 milidetik pada algoritma cipher sedangkan pada algoritma ROT13 enkripsi 5 milidetik dan dekripsi 5 milidetik.

Kata Kunci: Kriptografi, Algoritma Cipher. Algoritma ROT13

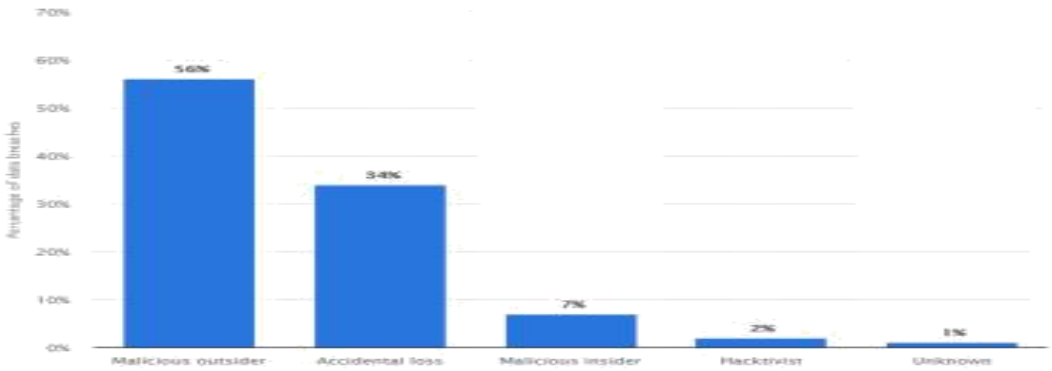
1. PENDAHULUAN

Aspek terpenting dalam menjaga keutuhan dan keaslian information itu sendiri adalah keamanan dan kerahasiaan suatu information. Keamanan information menimbulkan tuntutan akan tersedianya suatu system pengamanan information yang baik, agar dapat mengamankan information dari berbagai kejahatan teknologi yang mungkin akan tersedianya.

Pelaku kejahatan atau yang biasa disebut cybercrime menggunakan celah keamanan yang ada untuk menyadapan dan manipulasi data. Perekonomian dan martabat bangsa Indonesia di mata dunia yang dapat menyebabkan runtuhnya sistem tatanan sosial, lumpuhnya perekonomian negara, lemahnya sistem pertahanan yang ditimbulkan oleh pelaku cybercrime telah merugikan korban dalam jumlah.

Berdasarkan hasil statistik di atas, jenis penyerang menyebabkan pembobolan data global pada awal tahun 2018. Mayoritas serangan, sekitar 56%, berasal dari serangan terhadap orang asing. Sementara serangan orang dalam menyumbang 7%, serangan oleh peretas menyumbang 2%, serangan tidak disengaja 34% serangan oleh orang asing memiliki 1% di semua insiden.

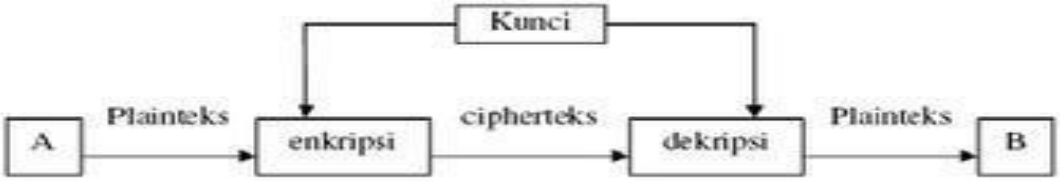
Menurut sebuah laporan oleh perusahaan keamanan Gemalto dalam enam bulan pertama tahun 2018, 4,5 miliar data dicuri. Jumlah data tersebut meningkat 113% dibandingkan periode yang sama tahun lalu. Jumlah pelanggaran data per hari mencapai 6,9 juta data. Hal ini berdasarkan laporan bahwa pencurian data dari tahun 2013 hingga enam bulan pertama tahun 2018 berjumlah 14,6 miliar, di mana hanya 4% yang dienkripsi oleh pemiliknya.



Gambar 1. Statistik Penyerangan Data 2018

2. METODE PENELITIAN

Kriptografi berasal dari kata Yunani cryptos yang berarti rahasia, sedangkan graphein berarti menulis. Jadi kriptografi berarti menulis rahasia (Angriani & Saharaeni, 2019). Kriptografi adalah bidang ilmiah yang mempelajari metode pengiriman pesan secara rahasia (yaitu dienkripsi atau disamarkan) sehingga hanya penerima pesan yang dituju yang dapat menghilangkan penyamaran dan membaca (atau memahami) pesan (Dewi, 2018).



Gambar 2. Sistem Kriptografi

Dalam kriptografi, proses penyandian plainteks menjadi cipherteks disebut pengkodean. Sedangkan proses mengembalikan ciphertext kembali ke plaintext disebut dekripsi. Parameter yang digunakan untuk transformasi enkripsi dan dekripsi disebut kunci. Menurut Paar dan Pelzl (2010), kriptografi bertujuan untuk memberikan layanan keamanan sebagai berikut :

1. Confidentiality. Informasi dirahasiakan dari semua pihak yang tidak berwenang.
2. Integrity. Memungkinkan penerima pesan untuk memverifikasi bahwa data tidak diubah selama transmisi. Penyusup tidak dapat mengganti pesan buruk dengan yang asli.
3. Otentikasi. Memungkinkan penerima pesan untuk mengkonfirmasi keaslian data; Penyusup tidak dapat meniru orang lain.
4. Tidak ditolak. Setiap entitas komunikasi tidak dapat menolak atau menolak data yang dikirim atau diterima

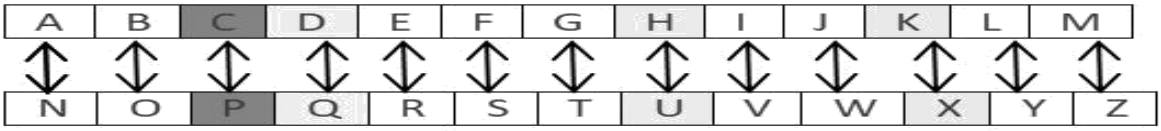
2.2 Algoritma Cipher

Substitusi cipher pertama dalam dunia kriptografi dikenal dengan nama Caesar cipher karena enkripsi ini terjadi pada masa pemerintahan Julius Caesar (Rachmawati & Candra, 2015). Dengan mengganti posisi huruf pertama dengan alfabet yang baik. Caesar cipher adalah salah satu yang tertua dan paling dikenal dalam perkembangan kriptografi.

Caesar cipher adalah cipher substitusi yang membentuk cipher dengan menukar karakter dalam plaintext dengan tepat satu karakter dalam ciphertext. Teknik seperti itu juga dikenal sebagai pengkodean abjad

tunggal. Caesar cipher sangat mudah digunakan. Inti dari algoritma kriptografi ini adalah untuk menggeser semua karakter plaintext dengan nilai perpindahan yang sama (Siregar, 2013). Langkah selanjutnya untuk menghasilkan ciphertext dengan Caesar cipher adalah:

1. Tentukan jumlah offset karakter yang digunakan untuk mengubah ciphertext menjadi plaintext.
2. Mengonversi karakter eksplisit menjadi teks kode berdasarkan offset yang telah ditentukan sebelumnya. Misal kita tahu shift = 3, maka huruf A akan diganti dengan huruf D, huruf B menjadi huruf E, dan seterusnya.



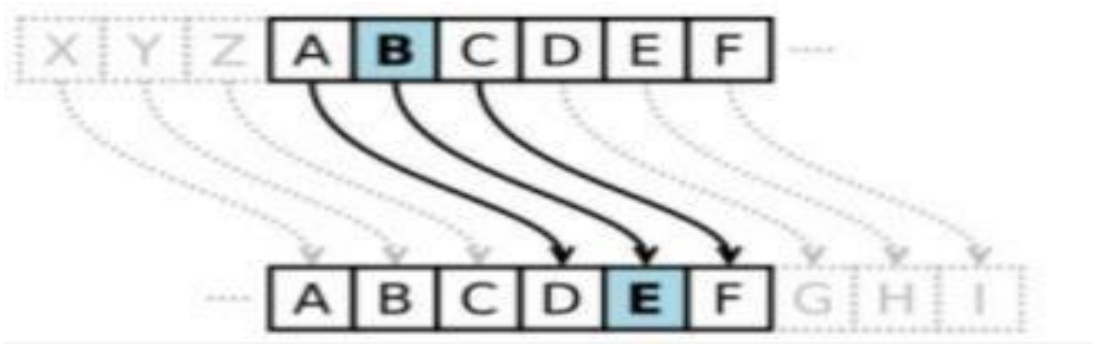
Gambar 3. Algoritma Cipher

Untuk menyandikan sebuah pesan, cukup mencari setiap huruf yang hendak disandikan di alfabet biasa, lalu tuliskan huruf yang sesuai pada alfabet sandi. Untuk memecahkan sandi tersebut gunakan cara sebaliknya. Contoh penyandian sebuah pesan adalah sebagai berikut:

Plainteks
Key
Cipherteks
: DAHLANKURNIAWAN
: 3
: GDKODQNXUQLDZDQ

2.3 Algoritma ROT 13

ROT13 (Rotate 13) adalah cipher pengganti dari cipher yang biasa digunakan pada sistem operasi UNIX. Dalam sistem pengkodean ROT13, sebuah huruf diganti dengan huruf dalam 13 posisi. Metode rot13 adalah metode enkripsi yang mengubah huruf menjadi huruf yang berjarak 13 tempat dari huruf aslinya. Misalnya, `A` akan berubah menjadi `N`, `B` akan berubah menjadi `O`, `C` akan berubah menjadi `P` dan seterusnya (Dewi, 2018).



Gambar 4. Algoritma ROT13

Plainteks : DAHLANKURNIAWAN

Cipherteks : QNUYNAXHEAVAJNA

3. HASIL DAN PEMBAHASAN

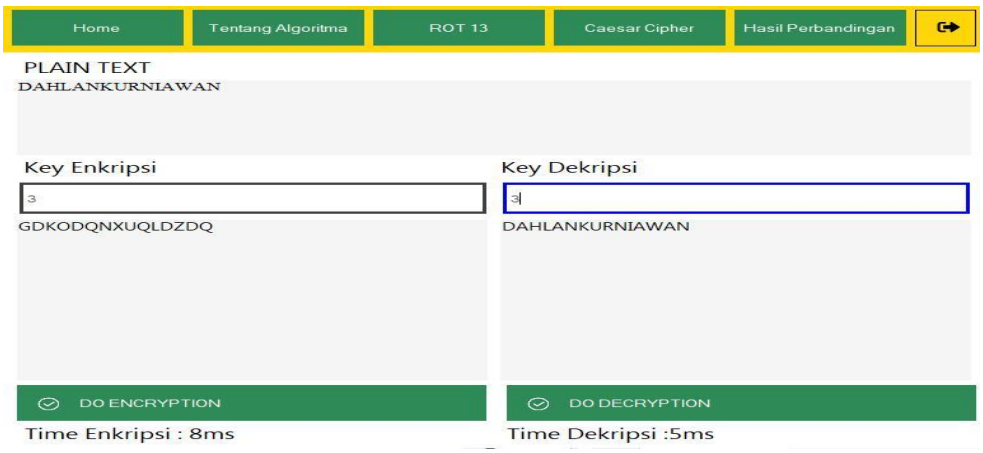
3.1 Test Results

Algoritma cipher dan algoritma ROT13 merupakan dua algoritma yang berbeda dari segi subtitusi dikarenakan pada algoritma cipher melakukan enkripsi dan dekripsi menggunakan kunci sedangkan algoritma ROT13 tidak memerlukan kunci sehingga peneliti ingin menguji kinerja algoritma cipher dan algoritma ROT13 dengan menggunakan aplikasi yang sudah dibangun, cara pengujian menggunakan sistem dalam menghitung cepatnya proses enkripsi dan dekripsi.

Pada gambar dibawah terdapat tampilan aplikasi dalam melakukan proses pengamanan menggunakan algoritma cipher. Pada tahap pengujian plainteks "DAHLANKURNIAWAN" menggunakan kunci "3" dan menghasilkan cipherteks "GDKODQNXUQLDZDQ".

Kinerja Algoritma	**Plainteks**	**Key**	**Durasi Enkripsi**	**Durasi Dekripsi**
Algoritma Cipher	DAHLANKURNIAWAN	3	8 ms	5 ms
	Saya Kuliah Program Studi Sistem Komputer	5	7,5 ms	6,4 ms
	Universitas Pembangunan Pancabudi Medan	3	9,2 ms	6,7 ms
	Jalan Jenderal Gatot Subroto KM 4,5 Kota	10	5 ms	4,2 ms

	Medan Sumatera Utara			
	Rajin Pangkal Kaya Malas Pangkal Miskin	7	4,8 ms	5 ms

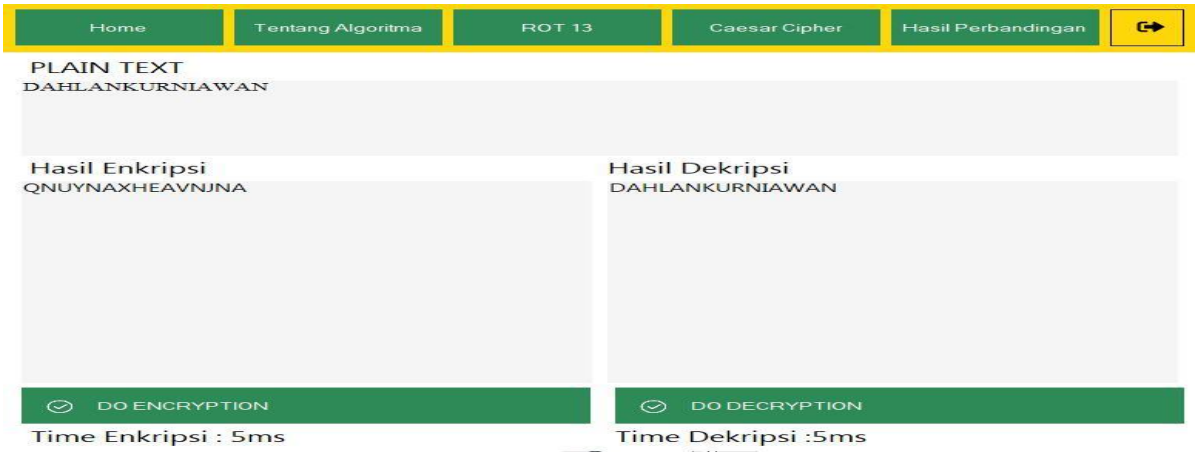


Gambar 5. Pengujian Algoritma Cipher

Algoritma ROT13	Dahlankurniawan		5 ms	5 ms
	Saya Kuliah Program Studi Sistem Komputer		6,2 ms	6,4 ms
	Universitas Pembangunan Pancabudi Medan		5,1 ms	6 ms
	Jalan Jenderal Gatot Subroto KM 4,5 Kota Medan Sumatera Utara		2,8 ms	2 ms
	Rajin Pangkal Kaya Malas Pangkal Miskin		3,8 ms	3 ms

Tabel 1. Perbandingan Pengujian Algoritma Cipher dan Algoritma ROT13

Selanjutnya dilakukan pengujian sebanyak 5 kali pengujian dan menghasilkan pada algoritma cipher melakukan proses enkripsi dengan durasi rata-rata 6,5 miliseconds sedangkan dekripsi dengan durasi rata-rata sebesar 5,46 miliseconds. Algoritma ROT13 melakukan proses enkripsi dengan durasi rata-rata4,58 miliseconds sedangkan dekripsi dengan durasi rata-rata 4,48 miliseconds.



Gambar 6. Pengujian Algoritma ROT13

Pada gambar dibawah terdapat tampilan aplikasi dalam melakukan proses pengamanan menggunakan algoritma ROT13. Pada tahap pengujian plainteks "DAHLANKURNIAWAN" dan menghasilkan cipherteks "GDKODQNXUQLDZDQ".

Dapat disimpulkan dengan plainteks "DAHLANKURNIAWAN" pada algoritma cipher melakukan proses enkripsi dengan durasi 8 miliseconds sedangkan dekripsi sebesar 5 miliseconds. Algoritma ROT13 melakukan proses enkripsi dengan durasi 5 miliseconds sedangkan dekripsi sebesar 5 miliseconds.

Selanjutnya dilakukan pengujian sebanyak 5 kali pengujian dan menghasilkan pada algoritma cipher melakukan proses enkripsi dengan durasi rata-rata 6,5 miliseconds sedangkan dekripsi dengan durasi rata-rata sebesar 5,46 miliseconds. Algoritma ROT13 melakukan proses enkripsi dengan durasi rata-rata4,58 miliseconds sedangkan dekripsi dengan durasi rata-rata 4,48 miliseconds.

4. SIMPULAN

Adapun kesimpulan dari penelitian perbandingan algoritma cipher dan algoritma ROT13 dalam pengamanan data maka dapat diambil beberapa kesimpulan diantaranya :

1. Algoritma cipher lebih lama proses enkripsi daripada proses enkripsi algoritma ROT13 sedangkan proses dekripsi antara algoritma cipher dan algoritma ROT13 sama durasinya. Sehingga dari segi waktu algoritma ROT13 lebih efektif digunakan daripada algoritma cipher.
2. Pengujian dilakukan sebanyak 5 kali pengujian dan menghasilkan pada algoritma cipher melakukan proses enkripsi dengan durasi rata-rata 6,5 miliseconds sedangkan

dekripsi dengan durasi rata-rata sebesar 5,46 miliseconds. Algoritma ROT13 melakukan proses enkripsi dengan durasi rata-rata4,58 miliseconds sedangkan dekripsi dengan durasi rata-rata 4,48 miliseconds.

5. DAFTAR PUSTAKA

Angriani, H., & Saharaeni, Y. (2019). Implementasi Algoritma Caesar Cipher pada Keamanan Data

Sistem E-Voting Pemilihan Ketua Organisasi Kemahasiswaan. *Jurnal Teknologi Informasi Dan Komunikasi*, *9*(2), 123–126.

Dewi, W. T. (2018). *Implementasi Algoritma Kriptografi Caesar Cipher ROT3 dan ROT13 dalam Enkripsi Data Teks Menggunakan PHP*. Universitas Sumatera Utara.

Rachmawati, D., & Candra, A. (2015). Implementasi Kombinasi Caesar dan Affine Cipher untuk Keamanan Data Teks. *Jurnal Edukasi Dan Penelitian Informatika*, *1*(2), 60–63.

Siregar, A. Z. (2013). *Implementasi ADFGVX Cipher dan RSA pada Keamanan File TXT dan DOC*. Universitas Sumatera Utara.