ISSN : 2252-3839 (Print)
ISSN : 2549-2403 (On Line)
DOI : 10.28989/compiler.v8i2.481
http://ejournals.stta.ac.id/index.php/compiler/

MODIFICATION OF VIGENERE ALGORITHM AND ONE TIME PAD USING RIVEST CODE 6 (RC6) KEY EXPANSION

Arif Budiman[1)], Paradise[2)]
[1,2]Universitas AMIKOM Yogyakarta
Jl. Ringroad Utara, Condongcatur, Depok, Sleman, Yogyakarta Indonesia 55283
Email : [1]arif.6122@students.amikom.ac.id, [2]paradise.paradise@students.amikom.ac.id

Abstract

Information technology that is increasingly developing today must be balanced with information security. Good security can minimize the possibility of information being stolen by cryptanalysis, one way is by applying cryptographic techniques. Vigenere Cipher is a key symmetry algorithm that uses a substitution technique that uses two letters encoding the original message. Vigenere cipher and one time pad have disadvantages because they use short keywords and their use will be repeated. The key expansion used is part of the RC6 encryption algorithm combined with Vigenere and One time pad to cover the weaknesses of the algorithm. The purpose of this study is to produce new variations with the modification of the vigenere cipher algorithm and one time pad by adding a key expansion process and tested using the avalance effect. Test results conducted based on modifications can achieve a high level of avalance effect which is 51.76%

Keywords: *Vigenere Cipher, RC6, RC6 key expansion.*

1. Latar Belakang Masalah

Teknologi informasi yang semakin berkembang saat ini harus diimbangi dengan keamaan data informasi. Keamanan informasi didapatkan salah satunya dengan menerapkan teknik kriptografi. Hal ini dilakukan untuk menjamin kerahasiaan informasi yang dikirimkan agar tidak dapat diakses oleh orang yang tidak seharusnya menerima informasi tersebut. Kriptografi merupakan salah satu metode yang digunakan untuk meningkatkan keamanan data karena dapat melakukan proses enkripsi dan dekripsi. terdapat berbagai macam algoritma kriptografi seperti caesar cipher, vigenere cipher, hill cipher, RC6, AES

Vigenere Cipher merupakan algoritma kunci simetri yang menggunakan teknik substitusi yang menggunakan dua huruf menyandikan pesan asli. Vigenere cipher memiliki kelemahan karena menggunakan kata kunci yang pendek dan penggunaanya yang akan diulang. Kunci yang berulang menimbulkan berbagai celah berupa penggeseran yang sama untuk setiap plainteks. Hal ini dapat digunakan untuk mencuri informasi tersebut dengan mencoba setiap kemungkinan yang ada atau biasa disebut dengan brute force attack atau exhaustive attack namun ini dirasa kurang optimal, karena memerlukan waktu yang lama[1]. salah satu metode yang dapat digunakan kriptanalisis adalah dengan menggunakan metode Kasiski. Metode kasiski akan melakukan penebakan panjang kunci melalui serangkaian perhitungan pola huruf n-graf[2][3][4][5]. Oleh karena itu dalam peneltian untuk menggabungkan beberapa algoritma untuk dimodifikasi yaitu vignere dan one time pad untuk proses enkripsi dan penambahan algoritma perpanjangan kunci dari rc6 untuk menghilangan perulangan kunci yang terjadi sehingga keamanan data menjadi lebih baik.

2. Metodologi Penelitian

2.1 Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi digunakan ketika suatu pesan dikirim dari suatu tempat ke tempat lain dengan mengubah isi pesan tersebut menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain[6][7]. Dalam kriptografi terdapat dua proses utama yaituenkripsi dan dekripsi. Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikan rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa didekripsi terlebih dahulu. Sedangkan dekripsi adalah proses membalikan data yang sudah disandikan ke bentuk semula agar diperoleh informasinya[8].

2.1 Vigenere Cipher

Vigenere cipher merupakan algorima symetrik yaitu algoritma kriptografi yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi[4] vigenere cipher merupakan pengembangan dari caesar cipher. pada vigenere cipher karakter pesan pada plainteks dan kunci berkaitan untuk menghasilkan sebuah cipherteks yang terbentuk dari sebuah tabel bujur sangkar vigenere atau tabula recta[1][2]. Misalnya, huruf A pada plainteks dapat menjadi huruf K atau M pada cipherteks yang berkaitan, tergantung pada kunci yang digunakan. Proses enkripsi pada vigenere cipher dapat diketahui menggunakan persamaan berikut :

$$Ci = (Pi + Ki)\ mod\ 26 \qquad (1)$$

Keterangan :

Ci = Cipherteks ke i
Pi = Plainteks ke i
Ki = Kunci ke i

Sedangkan algoritma dekripsi vigenere cipher dapat diketahui menggunakan persamaan (4) :

$$Pi = (Ci - Ki)\ mod\ 26 \qquad (2)$$

Keterangan :

Ci = Cipherteks ke i
Pi = Plainteks ke i
Ki = Kunci ke i

2.2 One Time Pad (Vernam Cipher)

One Time Pad atau dikenal juga dengan sebutan Vernam Cipher merupakan alogitma kriptografi berbasis simetris yang ditemukan oleh mayor Yoseph Mouborgne and Gilbert Vernam pada perang dunia kedua[4].

One time pad cipher merupakan salah satu algoritma kriptografi klasik yang kerahasiaannya mencapai sempurna karena menggunakan kunci yang tidak membentuk barisan yang berulang dan panjang kunci sama dengan panjang teks yang akan dirahasiakan. Dikarenakan menggunakan teknik tersebut one time pad cipher menjadi tidak efisien, karena membutuhkan waktu yang lama untuk menentukan kunci yang sama panjang dengan panjang teks yang akan dirahasiakan. Berikut ini adalah proses pengenkripsian dari one time pad cipher

$$ci \equiv pi + ki\ (mod\ n)\ ,\ i = 1,2,3, \dots , r \qquad (3)$$

Keterangan :

Ci = Cipherteks ke i
Pi = Plainteks ke i
Ki = Kunci ke i

nilai n dapat ditentukan berdasarkan berapa banyak jenis karakter huruf yang digunakan dalam pengenkripsian. Dan berikut ini adalah proses pendekripsian one time pad cipher

$$pi \equiv ci - ki \ (mod\ n)\ ,\ i = 1,2,3, \dots ,r \qquad (4)$$

2.3 RC6

Algoritma RC6 merupakan pengembangan dari RC5 yang dirancang oleh Ronald L Rivest, M.J.B.Robshaw, R. Sidney dan Y.L. Yin. RC6 dirancang untuk menghilangkan segala ketidakamanan yang ditemukan pada RC5 (Kurniawan, 2018).yang menjadi pembeda antara algoritma rc5, rc6 dan algoritma sebelumya yaitu rc4 karena algoritma RC5, dan RC6 termasuk kedalam blok cipher sedangkan RC4 termasuk stream cipher(Suhendar, Septiani, Sajati, & Astuti, 2013) Ada tiga proses dalam algoritma RC6 yaitu Proses Key Expansion (Perpanjangan Kunci), Proses Enkripsi dan Proses Dekrips[4].

Proses perpanjangan kunci dimulai dengan menentukan Kunci S awal yang dihitung menggunakan persamaan berikut

$$Pw = Odd((e - 2) \times 2w) \qquad (5)$$
$$Qw = Odd((ø - 1) \times 2w) \qquad (6)$$

Keterangan :

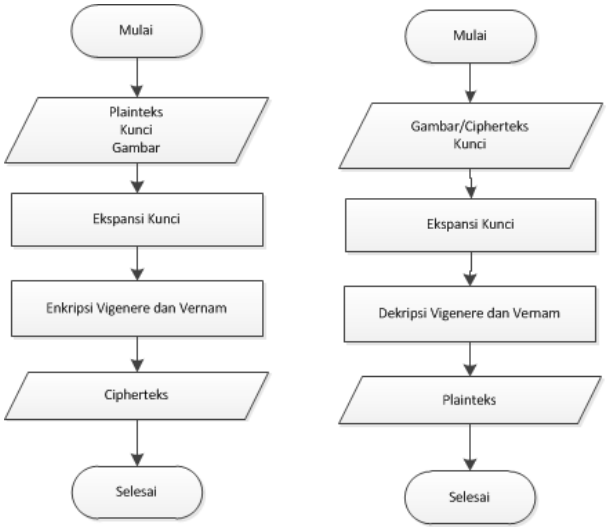
e = 2.718281828459 (logaritma natural)
ø = 1.6180339887 (rasio keemasan)
w = jumlah bit yang digunakan pada masing-masing blok
Odd (x) = bilangan ganjil yang mendekati nilai x

Proses selanjutnya adalah penggabungan kunci antara kunci S dengan Kunci Pengguna menggunakan prosedur berikut :

S[0] = **Pw**
for i = 1 to 2r+3 do
{ S[i] = S[i-1] + **Qw** }
x, y,i,j = 0
for k = 1 to (3 x 2r+4) do
{ S[i] = (S[i] + x + y) <<< 3
x = S[i]
L[j] = (L[j] + x + y) <<<3
y = L[j]
i = (i + 1) mod 2r+4
j = (j + 1) mod c
}

2.4 Enkripsi dan Dekripsi

Enkripsi adalah proses pengkodean yang mengubah pesan, dari yang dapat dipahami, disebut sebagai plaintext, menjadi kode yang sulit dipahami, disebut teks sandi. Sedangkan proses sebaliknya untuk mengubah teks sandi menjadi teks biasa disebut dekripsi. Proses enkripsi dan dekripsi membutuhkan mekanisme dan kunci tertentu[6]. Berikut adalah gambaran proses enkripsi dan dekripsi seperti ditampilkan pada gambar 1



Gambar 1 Enkripsi dan Dekripsi

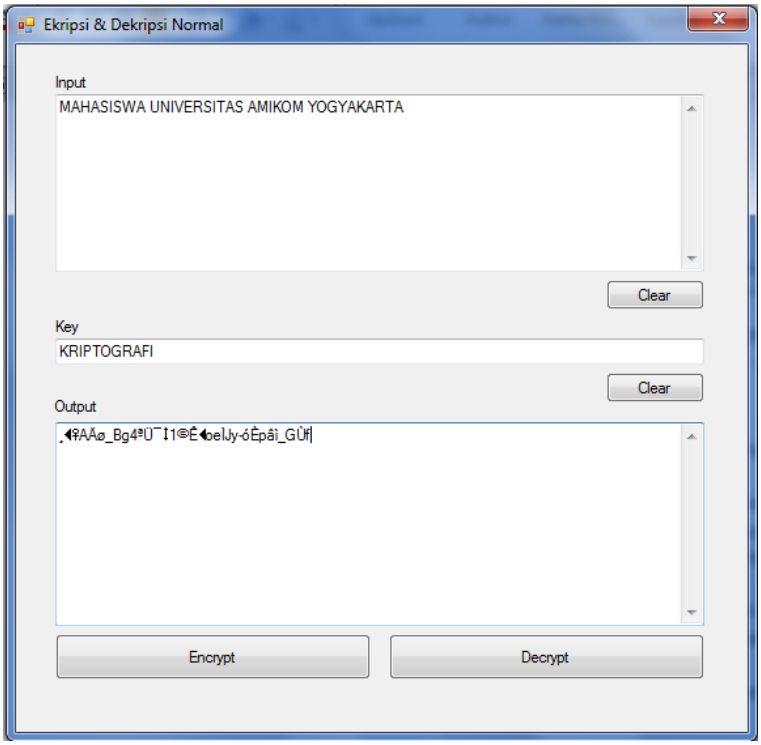
2.5 Avalance Effect

Avalance Effect digunakan untuk untuk menguji seberapa baik sebuah algoritma enkripsi karena algoritma enkripsi yang baik memiliki tingkat avalance effect yang tinggi dengan melihat perubahan cipherteks dengan melakukan sedikit perubahan bit pada plainteks maupun kunci. Untuk menghitung avalance digunakan persamaan berikut :

$$Avalance\ Effect \frac{\sum bit\ berubah}{\sum bit\ total}\ x\ 100\% \qquad (7)$$

3. Hasil dan Pembahasan

Dalam penelitian ini algoritma vignere cipher dikombinasikan dengan algoritma one time pad dan dimodifikasi dengan penambahan proses perpanjangan kunci untuk menghindari pengulangan kunci pada algoritma sebelumnya. Berikut adalah Software algoritma modifikasi yang telah dihasilkan seperti pada gambar 1



Gambar 1 Software Algorima Modifikasi

Gambaran Perbandingan antara algorima Vigenere Cipher, One Time Pad dan Algoritma modifikasi dalam mengenkripsi sebuah informasi yaitu “MAHASISWA UNIVERSITAS AMIKOM YOGYAKARTA” dengam kunci pesan “KRIPTOGRAFI”.

3.1. Hasil dari Vigenere Cipher

Plainteks : MAHASISWA UNIVERSITAS AMIKOM YOGYAKARTA
Kunci : KRIPTOGRAFI
Kunci Akhir : KRIPTOGRAFIKRIPTOGRAFIKRIPTOGRAFIKRI
Cipher Text : WRPPLWYNAZVSMMGLWZRSFUSBWBRCMPAPIBKI

3.2. Hasil dari Time Pad

Plainteks : MAHASISWA UNIVERSITAS AMIKOM YOGYAKARTA
Kunci : KRIPTOGRAFI
Kunci Akhir : KRIPTOGRAFIKRIPTOGRAFIKRIPTOGRAFIKRI
Cipher Text : GIXEEKEEAEDCDUVEKFISKCCSEQKQSGAUQLBQ

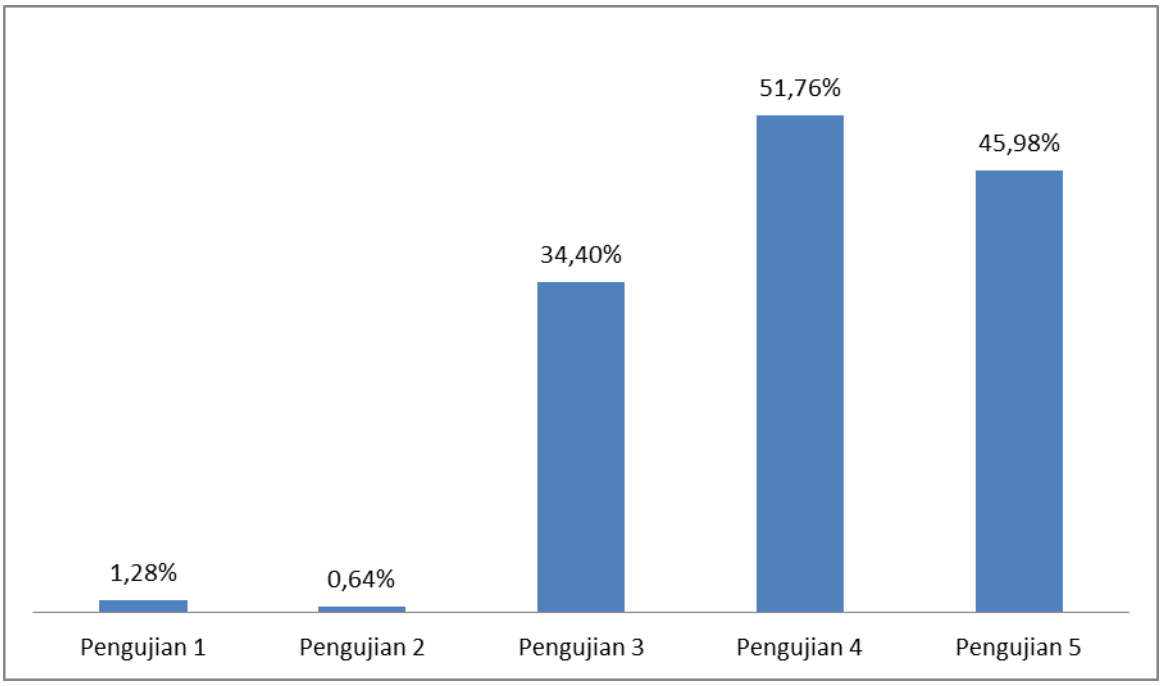
Berdasarkan hasil enkripsi diatas terjadi pengulangan kunci untuk memenuhi panjang dari plainteks pada Vigenere Cipher dan One Time Pad misalnya pada algoritma vigenere cipher perulangan hasil cipherteks terjadi pada huruf A dan I yang menghasilkan hasil yang sama yaitu I, proses ini dalam mengakibatkan ketidakamanan informasinya yang dihasilkan dan rentan untuk dicuri

3.3. Hasil dari Modifikasi Dengan Perpanjangan Kunci

Plainteks : MAHASISWA UNIVERSITAS AMIKOM YOGYAKARTA
Kunci : KRIPTOGRAFI
Cipher Text : Â‡Â¸AÄø_Bg4ªÜ¯1©ÊoeÌJy-óÈpâì_GÙf

Berdasarkan hasil enkripsi diatas dengan menggunakan perpanjangan kunci menunjukan sudah tidak adanya pengulangan kunci namun tetap menggunakan kunci pertama yaitu KRIPTOGRAFI yang digunakan untuk proses enkripsi dan dekripsi:

Untuk mengetahui seberapa baik algoritma yang telah dimodifikasi maka digunakan avalance effect untuk mengetahui setiap perubahan yang terjadi pada pada cipherteks dengan merubah sedikit bit pada plainteks atau kunci, pengujian dilakukan dengan merubah kata UNIVERSITAS menjadi ONIVERSITAS, UMIVERSITAS dan UNIXERSITAS dan merubah kunci KRIPTOGRAFI menjadi KRIBTOGRAFI dan KRIPTOGRAPI. Hasil pengeujian algoritma Modifikasi ditampilkan pada gambar 2



Gambar 2 Avalance Effect

4. Kesimpulan

Kesimpulan dari implementasi modifikasi algoritma vigenere cipher dengan ekspansi kunci rc6 adalah sebagai berikut:

1. Algoritma yang dihasilkan menghasilkan variasi baru untuk keamaanan data.
2. Proses ekspansi kunci RC6 yang diterapkan pada enkripsi algoritma vigenere cipher dan Vernam Cipher dengan memodifikasi jumlah kunci dapat meningkatkan keamanan data.
3. Terdapat Penambahan ukuran terhadap pesan yang dienkripsi pada gambar
4. Tidak Terdapat perbedaan secara visual antara gambar asli dengan gambar yang dienkripsi pesan
5. Hasil Pengujian 4 berdasarkan modifikasi yang dilakukan dapat mencapai tingkat avalance effect yang tinggi yaitu 51,76%

Daftar Pustaka

[1] Tsauri, T. A., & Nurochman, N. (2018). Kriptanalisis Algoritma Vigenere Chiper Dengan Algoritma Genetika Untuk Penentuan Kata Kunci. JISKA (Jurnal Informatika Sunan Kalijaga), 2(2), 115-126

[2] Pratama, G. M., & Tamatjita, E. N. (2015). Modifikasi algoritma vigenère cipher menggunakan metode Catalan number dan double columnar transposition. Compiler, 4(1)

[3] Anas, I., Nanda, P. A., & Hidayat, A. (2018). Implementasi Algoritma Vigeneere Cipher dan GOST dalam Keamanan Data. SinkrOn, 2(2), 18-22

[4] Subandi, A., Lydia, M. S., Sembiring, R. W., Zarlis, M., & Efendi, S. (2018, September). Vigenere cipher algorithm modification by adopting RC6 key expansion and double encryption process. In IOP Conference Series: Materials Science and Engineering (Vol. 420, No. 1, p. 012119). IOP Publishing

[5] Rahim, R., Kurniasih, N., Mustamam, M., Andriany, L., Nasution, U., & Mu, A. H. (2018). Combination Vigenere Cipher and One Time Pad for Data Security. Int. J. Eng. Technol, 7(2.3), 92-94

[6] Triandi, B., Ekadiansyah, E., Puspasari, R., Iwan, L. T., & Rahmad, F. (2018, August). Improve Security Algorithm Cryptography Vigenere Cipher Using Chaos Functions. In 2018 6th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-5). IEEE

[7] Jamaluddin, J., Zarlis, M., & Tulus, T. (2018). Pengamanan Data dengan Kombinasi Teknik Kriptografi Rabin dan Teknik Steganografi Chaotic LSB

[8] Widodo, A. P., Sarwoko, E. A., Suharto, E., & Siahaan, J. F. O. (2016). Pengamanan Data Foto Pada Perangkat Os Android Menggunakan Teknik Kriptografi Hill Cipher. JISKA (Jurnal Informatika Sunan Kalijaga), 1(2)

[9] Kurniawan, D. (2018). Perencanaan Aplikasi Pengamanan Data Text Menggunakan Blowfish Dan RC6. Pelita Informatika: Informasi dan Informatika, 17(3)

[10] Suhendar, A. S. S., Sajati, H., & Astuti, Y. (2013). Perancangan Algoritma Anggi (Aa) dengan Memanfaatkan Diffie-hellman dan Ronald Rivest (Rc4) untuk Membangun Sistem Keamanan Berbasis Port Knocking. Compiler, 2(2)