Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 26-30
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3179
Website https://ejurnal.seminar-id.com/index.php/jussi

Modifikasi Pembentukan Algoritma Rc4 Cipher Dengan Metode Acak Mid-Square Technique Untuk Pengamanan Voice Chat

Bambang Noviansyah

Program Studi Teknik Informatika, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Budi Darma,
Jalan Sisingamanganraja No. 338,Medan, Sumatera Utara, Indonesia
Email: bambangnoviansyah286@gmail.com

Abstrak− Perkembangan teknologi dan gaya hidup manusia memungkinkan pengaksesan sistem informasi dengan cara baru, misalnya mengunakan percakapan online (chat) melalui koneksi internet, yang sering berupa komunikasi teks (text chat) atau suara (voice chat). Instant messaging baru mulai populer saat internet mulai luas dipergunakan pada pertengahan dekade 1990-an. Seiring dengan kebutuhan manusia akan komunikasi yang mudah dan cepat, maka aplikasi yang dapat digunakan yaitu Voice Chat dimana memungkinkan penggunanya melakukan komunikasi suara. Tetapi pada aplikasi voice chatting kurang aman karena mudah disadap oleh pihak lain. Para penyadap dapat dengan mudah mengetahui isi pembicaraan dalam instant messaging dan kurangnya privasi pada pengguna chatting. Algoritma RC4 Memiliki kelemahan dalam penggunaannya untuk mengekripsi sebuah pesan. Kelemahannya adalah Vigenere hanya dapat melakukan proses enkripsi dan dekripsi untuk pesan singkat saja. Salah satu cara yang dapat digunakan yaitu membuat pengamanan pada aplikasi voice chatting dengan menggunakan algoritma Mid-Square Technique.

Kata Kunci: Voice Chat; Algoritma RC4; Algoritma Mid-Square Tehnique.

Abstract−Technological developments and human lifestyles allow access to information systems in new ways, for example using online conversations (chat) via an internet connection, which is often in the form of text communication (text chat) or voice (voice chat). Instant messaging only became popular when the internet began to be widely used in the mid-1990s. Along with the human need for easy and fast communication, the application that can be used is Voice Chat which allows users to carry out voice communication. But the voice chat application is less secure because it is easily intercepted by other parties. Eavesdroppers can easily find out the contents of conversations in instant messaging and the lack of privacy for chat users. The RC4 algorithm has a weakness in its use to encrypt a message. The downside is that Vigenere can only perform encryption and decryption processes for short messages. One way that can be used is to make security for the voice chat application using the Mid-Square Technique algorithm.

Keywords: Voice Chat; RC4 Algorithm; Mid-Square Technique Algorithm..

1. PENDAHULUAN

Perkembangan teknologi, memberikan kemudahan bagi kita untuk melakukan komunikasi dan pertukaran informasi dan juga dapat berdampak kepada pengembangan algoritma kriptografi. Sebuah algoritma yang digunakan untuk melakukan sebuah enkripsi dan dekripsi tidak hanya harus benar saja, namun juga harus efisien digunakan. Sebuah algoritma dikatakan efisien apabila algoritma tersebut menggunakan memori yang relatif lebih kecil dan memiliki waktu proses yang cepat.

Sejauh ini, banyak penelitian yang telah membahas mengenai efisiensi sebuah algoritma. Mengenai pengukuran waktu dan ruang memori yang dibutuhkan dikenal dengan kompleksitas algoritma. Algoritma kriptografi RC4 merupakan salah satu algoritma kunci simetris dibuat oleh RSA Data Security Inc (RSADSI) yang berbentuk stream chipper [1].

Algoritma RC4 Memiliki kelemahan dalam penggunaannya untuk mengekripsi sebuah pesan. Kelemahannya adalah Vigenere hanya dapat melakukan proses enkripsi dan dekripsi untuk pesan singkat saja. Hal ini diakibatkan karena jumlah karakter plaintext dan kunci sama, akan memakan banyak memori dan waktu yang lama dalam melakukan proses enkripsi dan dekripsi.

Kelemahan ini mengakibatkan RC4 tidak lagi menjadi algoritma yang praktis untuk di gunakan. Banyak penelitian sebelumnya hanya membahas mengenai kombinasi algoritma RC4 dengan Algoritma asimetris dalam pembangkitan kunci, bukan kepada efektifitas dan kompleksitas penggunaan algoritma itu sendiri.

Menurut penulis perlu adanya metode dan mengusulkan sebuah modifikasi baru untuk membuat algoritma RC4 menjadi lebih efektif dan efisien digunakan, yaitu dengan cara membuat kunci lebih singkat atau tidak bergantung pada jumlah panjang plaintext.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Guna mempermudah penelitian adapun langkah-langkah yang ditempuh dalam melakukan penelitian, adalah sebagai berikut:

a. Studi pustaka (library research)
b. Pada tahap ini penulis mencari sumber refrensi dan tinjauan pustaka dari berbagai sumber, yang membahas teori-teori yang berhubungan permasalahan yang ada pada penelitian ini, sumber penelitian ini dapat berupa buku, artikel ilmiah, penelitian-penelitian sebelumnya, dan lain sebagainya.
c. Analisa

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 26-30
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3179
Website https://ejurnal.seminar-id.com/index.php/jussi

d. Pada tahap ini menguraikan prosedur modifikasi kunci menggunakan multiplicative random generator serta penenkripsian dan pendekripsian citra digital menggunakan algoritma international data encryption standard.
e. Perancangan dan implementasi
f. Pada tahap ini merupakan perancangan dan pengaplikasian proses enkripsi dan dekripsi citra digital. Selanjutnya akan mengimplementasikan algoritma yang digunakan sesuai dengan hasil analisa.
g. Pengujian
h. Tahap ini merupakan pengujian terhadap analisa yang telah dibahas, pada pengujian ini merupakan pembuktian apakah hasil analisa sesuai dengan hasil yang sebenarnya.
i. Penyusunan laporan dan kesimpulan akhir
j. Pada tahap ini dilakukan proses dokumentasi hasil dari analisa dan pengujian secara tertulis dalam bentuk laporan.

2.2 Kriptografi

Kriptografi berasal dari Bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Kriptografi adalah sebuah teknik penyandian pesan yang dilakukan agar pesan dapat dikirim dan diterima dengan aman. Kriptografi bertujuan untuk menjaga kerahasiaan data dan informasi agar tidak disalah gunakan oleh pihak yang tidak sah. [1] [2] [3] Kriptografi adalah ilmu seni untuk menjaga keamanan pesan. [4] Terdapat berbagai definisi mengenai kriptografi, namun pada intinya kriptografi adalah teknik yang digunakan untuk menjamin keamanan pertukaran data [5].

2.3 Algoritma RC4

RC4 adalah cipher aliran yang digunakan secara luas pada sistem keamanan seperti protokol Secure Socket Layer (SSL). Algoritma kriptografi ini sederhana dan mudah diimplementasikan. RC4 dibuat oleh Ron Rivest dari laboratorium RSA (RC adalah singkatan dari Rivest's Code). RC4 membangkitkan keystream yang kemudian di-XOR-kan dengan plaintext pada waktu enkripsi (atau di-XOR-kan dengan bit-bit ciphertext pada waktu dekripsi). RC4 tidak seperti cipher aliran yang memproses data dalam bit. RC4 memproses data daalam ukuran byte (1 byte = 8 bit). RC4 menggunakan dua buah kotak substitusi (S-box) array 256 byte yang berisi permutasi dari bilangan 0 sampai dengan 255, dan S-box kedua yang berisi permutasi fungsi dari kunci sepanjang variabel. [3]

2.4 Kriptografi

Metode ini ditemukan oleh John von Neumann dan Metropolis (1940). Metode ini digunakan untuk membangkitkan bilangan random sepanjang n digit. Untuk membangkitkan bilangan berikutnya, bilangan yang sekarang dikuadratkan, kemudian dari hasil kuadrat tersebut diambil n digit yang terletak di tengah. Kelemahan cara ini adalah jika mencapai bilangan 0, bilangan-bilangan berikutnya akan terus 0. dalam membangkitkan bilangan acak menggunakan metode ini antara lain [11]:

a. Pilih bilangan bulat positif sebagai seed (Z0) yang berupa bilangan bulat positif yang terdiri dari beberapa digit.
b. Kuadratkan bilangan tersebut sehingga membentuk digit sejumlah dua kali jumlah digit Z0, jika tidak, tambahkan digit 0 di depan bilangan tersebut.
c. Ambil sejumlah digit yang sesuai dengan jumlah digit Z0 yang berada di tengah untuk menjadi Z1.
d. Tambahkan digit desimal di depan Z1.
e. Lakukan sampai langkah ke-n.

2.5 Voice Chat

Voice chat adalah sebuah sistem dimana seseorang dapat meninggalkan pesan kepada orang lain melalui telepon. Sistem ini biasanya diperlukan ketika telepon yang dituju sedang sibuk, di luar jangkauan, atau tidak diangkat oleh pemiliknya. Dalam kondisi seperti itu, si penelepon dapat meninggalkan pesan yang dapat didengarkan kemudian oleh pemilik telepon. Fasilitas voice chat pada telepon genggam pada umumnya telah disediakan oleh penyedia jaringan telepon. Sedangkan, pada telepon biasa, sistem voice chat dapat dijalankan dengan menambah perangkat tertentu, seperti misalnya mesin penjawab telepon. [12]

3. HASIL DAN PEMBAHASAN

3.1 Pembahasan

Perkembangan teknologi dan gaya hidup manusia memungkinkan untuk mengakses sistem informasi dengan cara baru, misalnya menggunakan percakapan online (*chat*) melalui koneksi internet, sering kali dalam bentuk komunikasi teks (*text chat*) atau suara (*voice chat*). Sejalan dengan kebutuhan manusia akan komunikasi yang mudah dan cepat, maka aplikasi yang dapat digunakan adalah *voice chat* yang memudahkan pengguna untuk melakukan komunikasi suara. Namun aplikasi obrolan suara kurang aman karena mudah disadap oleh orang lain. Penyadapan bisa dengan mudah mengetahui isi percakapan dan kurangnya privasi di *chat* tersebut. Salah satu cara yang dapat digunakan adalah dengan membuat pengamanan aplikasi *voice chat* menggunakan algoritma RC4 dan Mid-Square Technique yang menerapkan sistem enkripsi yang dilakukan untuk mencegah terjadinya penyadapan dan kecurangan serta meningkatkan algoritma keamanan

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 26-30
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3179
Website https://ejurnal.seminar-id.com/index.php/jussi

3.2 Analisa Metode *Mid Square Technique*

Contoh penerapan pada penelitian ini dapat dilihat pada kasus dibawah ini. Diketahui suatu Variabel a, c dan m bersifat tetap, variabel ini digunakan untuk menghasilkan nilai acak. Misalkan dilakukan proses *mid square technique* untuk 5 buah nilai acak.

a. X = 1; a = 105; c = 71; M = 1024; t = milidetik
b. Lakukan perulangan sebanyak 5 kali dengan setiap kali perulangan melakukan kalkulasi X[i+1] = ((a * X) + c + t) mod M.
c. X[0] = ((105 * 441) +71 + 891145) mod 1024 = 441
d. X[1] = ((105 * 561) +71 + 891145) mod 1024 = 561
e. X[2] = ((105 * 873) +71 + 891145) mod 1024 = 873
f. X[3] = ((105 * 865) +71 + 891145) mod 1024 = 865
g. X[4] = ((105 * 25) +71 + 891145) mod 1024 = 25
h. Jadi nilai acak yang didapat adalah 441, 561, 873, 865, 25

Nilai acak ini digunakan sebagai kunci enkripsi dan dekripsi pada algoritma *mid square technique.*

3.3 Analisa Metode RC 4

Dalam proses pengamanan menggunakan teknik kriptografi menggunakan enkripsi dan deskripsi. Dalam proses kerja dari enkripsi dan deskripsi dapat dilihat pada poin di bawah ini

3.3.1 Proses Enkripsi

Berikut adalah implementasi algoritma RC4 dengan mode 4 *byte* (untuk lebih menyederhanakan dalam perhitungan manual) serta untuk kebutuhan sistem yang sangat terbatas. S-*Box* dengan panjang 4 *byte*, dengan S[0]=0, S[1]=1, S[2]=2 dan S[3]=3 sehingga *array* S menjadi: 0 1 2 3

Inisialisasi 4 *byte* kunci *array*, K. Misalkan kunci Ulang kunci sampai memenuhi seluruh adalah 2 5 7 3, sehingga array K berisi 2 5 7 3 dan mencoba untuk mengenkripsikan kata **HALO**. Inisialisasi i dan j dengan 0 kemudian dilakukan KSA (*Key-scheduling algorithm*) agar tercipta *state-array* yang acak. Penjelasan iterasi lebih lanjut dapat dijelaskan sebagai berikut :

Iterasi 1
i = 0
j = (0 + S[0] + K [0 mod 4]) mod 4
= (0 + 0 + 2) mod 4 = 2
Swap (S[0], S[2])
Hasil Array S
2 1 0 3

Iterasi 2
i = 1
j = (2 + S[1] + K [1 mod 4]) mod 4
= (2 + 1 + 5) mod 4 =0
Swap (S[1],S[0])
Hasil Array S
1 2 0 3

Iterasi 3
i = 2
j = (0 + S[2] + K [2 mod 4]) mod 4
= (0 + 0 + 7) mod 4 = 3
Swap (S[2], S[3])
Hasil Array S
1 2 3 0

Iterasi 4
i = 3
j = (3 + S[3] + K [3 mod 4]) mod 4
= (3 + 0 + 3) mod 4 = 2
Swap (S[3],S[2])
Hasil Array S
1 2 0 3

Setelah melakukan KSA, akan dilakukan PRGA (*Pseudo-random generation algorithm*). PRGA akan dilakukan sebanyak 4 kali dikarenakan plainteks yang akan dienkripsi berjumlah 4 karakter. Hal ini disebakan karena dibutuhkan 1 kunci dan 1 kali pengoperasian XOR untuk tiap tiap karakter pada *plainteks*. Berikut adalah tahapan penghasilan kunci enkripsi dengan PRGA

Array S
1 2 0 3

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 26-30
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3179
Website https://ejurnal.seminar-id.com/index.php/jussi

Inisialisasi
i = 0
j = 0

Iterasi 1
i = (0 + 1) mod 4 = 1
j = (0 + S[1]) mod 4 = (0+ 2) mod 4 = 2
swap (S[1],S[2])
1 0 2 3
K1 = S[(S[1]+S[2]) mod 4] = S[2 mod 4] = 2
K1 = 00000010

Iterasi 2
i = (1 + 1) mod 4 = 2
j = (2 + S[2]) mod 4 = (2+ 2) mod 4 = 0
swap (S[2],S[0])
2 0 1 3
K2 = S[(S[2]+S[0]) mod 4] = S[3 mod 4] = 3
K2 = 00000011

Iterasi 3
i = (2 + 1) mod 4 = 3
j = (0 + S[3]) mod 4 = (0+ 3) mod 4 = 3
swap (S[3],S[3])
1 0 2 3
K3 = S[(S[3]+S[3]) mod 4] = S[6 mod 4] = 2
K3 = 00000010

Iterasi 4
i = (3 + 1) mod 4 = 0
j = (3 + S[0]) mod 4 = (3+ 1) mod 4 = 0
swap (S[0],S[0])
1 0 2 3
K1 = S[(S[0]+S[0]) mod 4] = S[2 mod 4] = 2
K4 = 00000010

Huruf	Kode ASCII	Binary 8 bit
H		01001000
A		01000001
L		01001100
O		01001111

Setelah menemukan kunci untuk tiap karakter, makadilakukan operasi XOR antara karakter pada *plaintext* dengan kunci yang dihasilkan. Berikut adalah tabel ASCII untuk tiap-tiap karakter pada *plaintext* yang digunakan.

Berikut adalah proses pengXORan dari *plaintext* dengan *key* yang telah didapat :

H A L O	: 01001000 01000001 01001100 01001111
Key	: 00000010 00000011 00000010 00000010
Cipherteks	: 01001010 01000010 01001110 01001101

3.3.2 Proses Dekripsi

Proses dekrsipsi *ciphertext* menggunakan algoritma RC4 ini sama untuk proses *key-schedule*-nya. Untuk mendapatkan *plaintext*, *ciphertext* yang diperoleh di XORkan dengan *pseudo random byte* yang didapat sebelumnya. Maka hasilnya adalah *plaintext* atau teks asli.

Pesan dikirim dalam bentuk *ciphertext* sehingga setelah sampai di penerima pesan dapat kembali diubah menjadi *plaintext* dengan meng-XOR-kan dengan kunci yang sama. Pemrosesan pesan setelah sampai pada penerima dapat dilihat pada dibawah ini. Proses XOR *pseudo random byte* dengan *ciphertext* pada deskripsi yaitu :

Cipherteks	: 01001010 01000010 01001110 01001101
Key	: 00000010 00000011 00000010 00000010
Plainteks	: 01001000 01000001 01001100 01001111.


Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 26-30
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3179
Website https://ejurnal.seminar-id.com/index.php/jussi

4. KESIMPULAN

Dari hasil penelitian yang telah dilakukan maka dapat diambil kesimpulan berdasarkan hasil pengujian yang telah dilakukan maka diperoleh kesimpulan yaitu dengan menererapan Metode RC 4 Cipher dan Mid-square technique untuk pengamanan voice chat akan dapat menambah pengamanan pada dalam melakukan komunikasi. Algoritma RC4 Memiliki kelemahan dalam penggunaannya untuk mengekripsi sebuah pesan. Kelemahannya adalah Vigenere hanya dapat melakukan proses enkripsi dan dekripsi untuk pesan singkat saja. Salah satu cara yang dapat digunakan yaitu membuat pengamanan pada aplikasi voice chatting dengan menggunakan algoritma Mid-Square Technique

REFERENCES

[1] M. Iyas, Jan 2014. [Online]. Available: https://matriasiyas.wordpress.com/2014/01/19/pengertian-algoritma-rc4/.
[2] B. Schneier, Applied Cryptography, Oak Park, 1996.
[3] E. Setyaningsih, Kriptografi & Implementasi Menggunakan Matlab, Yogyakarta, 2015.
[4] R. Munir, Pengantar Kriptografi, Bandung, 2004.
[5] D. Ariyus, Pengantar Ilmu Kriptografi, Andi, 2008.
[6] E. Agustina and A. Kurniati, "Pemanfaatan Kriptografi Dalam Mewujudkan Keamanan Informasi Pada e-Voting di Indonesia," in Seminar Nasional Informatika, 2009.
[7] S. Prabowo, "Kriptografi," Jan 2018. [Online]. Available: http://www.sigitprabowo.id/2013/01/kriptografi-jenis-jenis-serangan-dalam.html.
[8] N. Aleisa, A Comparison of the 3DES and AES Encryptions Standards, 2015.
[9] J. Thakur and N. Khumar, DES,AES ad Blowfish: Symmetric Key Cryptography Algorithm Simulation Based Performance Analysis, 2011.
[10] Mohtashim, April 2015. [Online]. Available: https://tutorialspoint.com/cryptography/cryptography.htm.
[11] Uaies Hafizh, "Teknik Simulasi," 01 November 2011. [Online]. Available: https://uaieshafizh.wordpress.com/2011/11/01/metode-middle-square/.
[12] Wikipedia, "Wikipedia," 27 Maret 2020. [Online]. Available: https://id.wikipedia.org/wiki/Pesan_suara.
[13] F. W. Yudo Untoro, Algoritma Pemograman Dengan Bahasa Java, Yogyakarta, 2010.
[14] M. D. Irwanto, Perancangan Object Oriented Software dengan UML, Yogyakarta, 2007.
[15] M. Yazdi, Pemograman Matlab Pada Sistem Pakar Fuzzy, Yogyakarta, 2017.
[16] S. Al-Hinai, "Algebraic Attacks on Clock-Controlled Stream Chiphers," 2006.
[17] K. Maret 2019. [Online]. Available: https://kiajar.com/pengertian-teks-editorial/.
[18] Mohanmad, "d-HMAC-An improved HMAC algorithm," IJCSIS, vol. Vol.13, no. ISSN 1947-5500, p. No.4, April 2015..