PENERAPAN ALGORITMA RC4 PADA OPERASI XOR UNTUK KEAMANAN PESAN PADA SMARTPHONE BERBASIS WEB

Muryan Awaludin
Teknik Informatika, STIKOM CKI
Email: muryan_awaludin@yahoo.co.id

Abstract

Utilization of cryptography as the encryption and decryption can be used to secure messages or the data that is important and valuable. A message can be encrypted or into ciphertext using a key and can be safely exchanged without having to worry about the confidentiality of the contents of the message. Decryption key will be to process the encrypted message into plaintext or the original message. XOR operation algorithm is computationally easy to use, but the process XOR algorithm is weak and not strong. To cover up weaknesses reviews these use RC4 algorithm (Rivers Code 4), because RC4 algorithm process is fast and strong . The results of this application in the form of a software is Able to encrypt and decrypt the message form and to generate a unique security key based encrypted message, and provide an accurate report on the presence or absence of changes to the contents of the message, The implementation of the RC4 encryption and decryption process on the website based smartphone helps users in maintaining the security and confidentiality of information storage that is sent and received. The results of this study so that the user can secure messages to be sent to the recipient.

Keywords: Applications, Decryption, Encryption, Message, RC4, Website

1. PENDAHULUAN

RC4 merupakan salah satu stream cipher yang paling populer dari era modern. Dirancang oleh Ron Rivest, itu pertama diperkenalkan pada tahun 1987 sebagai sebuah perangkat lunak proprietary dari RSA DSI. Hal ini digunakan dalam beberapa protokol jaringan populer seperti TLS, WEP dan WPA. Keadaan internal RC4 berisi permutasi dari semua bilangan bulat n-bit, di mana n biasanya 8 dan permutasi adalah atas N = 256 bilangan bulat {0,. . ., 255} (Sarkar, 2014).

Menurut Roos (1995) bahwa keystream byte keluaran pertama kebocoran informasi pada RC4 tentang kunci rahasia ketika pertama dua byte kunci rahasia menambah 0 mod 256. Sebuah studi teoritis yang lebih umum telah dilakukan yang meliputi servations.

Untuk melindungi dan menjaga kerahasia-an informasi agar terhindar dari tindakan-tindakan kejahatan komputer oleh orang-orang yang tidak berhak, maka salah satu cara yang dapat dilakukan adalah dengan memanfaatkan teknik kriptografi. Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain. Pesan asli disebut plaintext dan pesan rahasia disebut chipertext (Jindal & Singh, 2015). Proses untuk mengubah plaintext menjadi ciphertext disebut dengan enkripsi (enciphering). Sebaliknya, proses mengubah ciphertext menjadi plaintext disebut dengan dekripsi (deciphering).

Kunci rahasia cipher diklasifikasikan lebih lanjut sebagai stream cipher dan block cipher. Dalam stream cipher, satu bit atau byte diproses atau dienkripsi pada suatu waktu, aliran kunci yang dihasilkan merupakan urutan pseudo-random bit. Sebuah plaintext (urutan bit /byte) diubah menjadi ciphertext dengan menyem-bunyikan plaintext dengan keystream, meng-gunakan operasi XOR sederhana. Sedangkan di blok cipher, blok bit / byte / kata-kata diproses pada suatu waktu (Jindal & Singh, 2015).

Sebagai upaya mewujudkan implementasi keamanan pesan dengan menggunakan metode enkripsi RC4 (Rivest Code 4) ke dalam suatu aplikasi yang mudah digunakan. Aplikasi ini ditujukan untuk membantu mengatasi masalah keamanan data yang kirim atau disimpan melalui smartphone.

2. METODE PENELITIAN TERKAIT

Pada penelitian yang dilakukan oleh Rita Rio Arjumi Gurning (2014) sistem yang dihasilkan pada penelitian tersebut adalah sebuah sistem yang hanya merubah pesan enkripsi ke dekripsi dengan menggeser kunci awal dan menggunakan kuci caesar cipher. Peneliti melakukan penelitian dengan menguji hanya bebrapa kata. Penelitian ini difokuskan pada pengaman kata atau pesan yang dikirim.

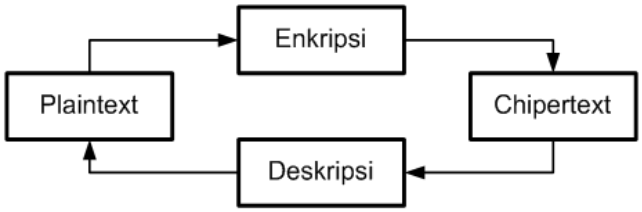
Penelitian yang dilakukan Shohfi Tama, Agung Setyabudi (2016) sistem yang dihasilkan pada penelitian tersebut adalah untuk mengetahui hasil enkripsi suatu kata atau kalimat menjadi ciphertext dan di dekripsi kembali menjadi kata atau kalimat semula atau plantext menggunakan operasi XOR yang berbasis web. Pengujian yang dilakukan dengan mengambil kata yang akan dienkripsi, lalu menghasilkan pesan hasil enkripsi dan mengembalikan hasil semula dengan melakukan proses dekripsi.

Penelitian yang dilakukan oleh Elka Lukman Hakim, Kahiril, Ferry Hari Utami (2014) sistem yang dihasilkan pada penelitian tersebut adalah menerapkan algoritma RC4 pada sebuah aplikasi Website,pada penelitian-nya, peneliti menguji yaitu text asli (pesan sebelum dienkripsi). Dari hasi pengujian tersebut menghasilkan proses enkripsi dan dekripsinya menggunakan algoritma RC4. Panjang kunci tidak terlalu mempengaruhi waktu yang digunakan saat proses terjadi tetapi lebih cenderung dipengaruhi oleh kecepatan komputasi. Semakin panjang kunci yang digunakan maka semakin aman pesan yang di enkripsi. Dan semakin banyak aplikasi yang dijalankan pada laptop maka semakin lama proses enkripsi maupun dekripsi file.

2.1 Dasar Teori

Kriptografi

Kriptografi merupakan ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli(Kromodimoeljo, 2009), seperti yang ditunjukan pada gambar.



Gambar 1 Skema Proses Enkripsi dan Dekripsi

Konsep keamanan umumnya diartikan sebagai gagasan kerahasiaan data yang dikirim, terutama informasi digital ditransmisikan melalui jaringan nirkabel. Namun kebutuhan kerahasiaan informasi memang paradigma sosial.

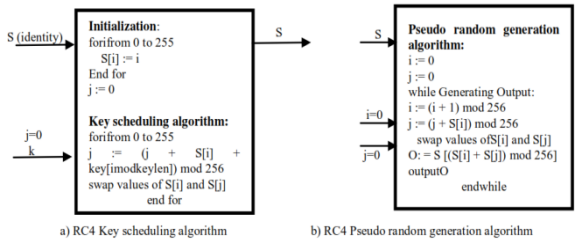
Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter. Biasanya algoritma tidak dirahasiakan, bahkan enkripsi yang mengandalkan kerahasiaan algoritma dianggap sesuatu yang tidak baik. Rahasia terletak di beberapa parameter yang digunakan, jadi kunci ditentukan oleh parameter. Parameter yang menentukan kunci dekripsi itulah yang harus dirahasiakan (parameter menjadi ekuivalen dengan kunci).

RC4 (*Rivest Code 4)*

Algoritma RC4 merupakan salah satu stream cipher tertua dan paling liar digunakan di dunia. Banyak digunakan untuk aplikasi dunia nyata termasuk Microsoft Office, Secure Socket Layer (SSL), Wired Equivalent Privacy (WEP), dll. Sejak debutnya pada tahun 1994 (Chen, 2013) banyak karya kriptanalisis telah dilakukan di atasnya, dan banyak kelemahan telah dimanfaatkan (Supehrdad, et al., 2011) (Subhamoy et al., 2011) (Chen & Miyaji, 2011). Namun, jika RC4 digunakan dengan cara

yang tepat, itu masih dianggap aman. Oleh karena itu masih dianggap menjadi target pembacaan sandi yang berharga tinggi baik di dunia industri dan akademis.

Gambar enkripsi RC4 seperti yang ditunjukan pada gambar 2.



Gambar 2 Enkripsi RC4

Menurut Kromodimoedjo (Kromodimoeljo, 2009), RC4 adalah stream cipher yang dirancang di RSA Security oleh Ron Rivest tahun 1987. Pada mulanya cara kerja RC4 dirahasiakan oleh RSA Security, akan tetapi ini dibocorkan di internet tahun 1994 di milis Cypherpunks. RSA Security tidak pernah merilis RC4 secara resmi, akibatnya banyak yang menyebutnya sebagai ARC4 (alleged RC4 atau tersangka RC4) untuk menghindari masalah trademark. RC4 dirancang agar dapat diimplementasikan di software secara sangat efisien. Ini membuat RC4 sangat populer untuk aplikasi internet, antara lain RC4 digunakan dalam standard TLS (transport layer security) dan WEP (wireless equivalent privacy). Cara membuat keystream dalam RC4 adalah dengan state automaton dan terdiri dari dua tahap :

- Tahap key scheduling dimana state automaton diberi nilai awal berdasarkan kunci enkripsi.

- Tahap pseudo-random generation dimana state automaton beroperasi dan outputnya menghasilkan keystream.

Tahap pertama dilakukan menggunakan key scheduling algorithm (KSA). State yang diberi nilai awal berupa array yang merepresentasikan suatu permutasi dengan 256 elemen, jadi hasil dari algoritma KSA adalah permutasi awal. Array yang mempunyai 256 elemen ini (dengan indeks 0 sampai dengan 255) dinamakan S. Berikut adalah algoritma KSA dalam bentuk pseudo-code dimana key adalah kunci enkripsi dan keylength adalah besar kunci enkripsi dalam bytes (untuk kunci 128 bit, key length = 16) :

```
for i = 0 to 255
S[i] := i
j := 0
for i = 0 to 255
j := (j + S[i] + key[i mod key length]) mod 256
swap(S[i],S[j]) (3)
```

Tahap kedua menggunakan algoritma yang dinamakan pseudo-random generation algorithm (PRGA). Setiap putaran, bagian keystream sebesar 1 byte (dengan nilai antara 0 sampai dengan 255) dioutput oleh PRGA berdasarkan state S. Berikut adalah algoritma PRGA dalam bentuk

pseudo-code:

```
i := 0
j := 0
loop
i := (i + 1) mod 256
j := (j + S[i]) mod 256
swap(S[i],S[j])
K = S[(S[i] + S[j]) mod 256] (4)
```

Byte K di-XOR kan dengan plaintext untuk menghasilkan ciphertext atau di XOR kan dengan ciphertext untuk menghasilkan plaintext. Permutasi dengan 255 elemen mempunyai 255i kemungkinan. Ditambah dua indeks (i dan j) yang masing-masing dapat mempunyai nilai antara 0 dan 255, maka state automaton yang digunakan untuk membuat keystream mempunyai 255! x2552= 21700 kemungkinan internal states. Karena banyaknya jumlah kemungkinan untuk internal state, sukar untuk memecahkan RC4 dengan menganalisa PRGA (teknik paling afisien saat ini harus menjajagi >2700 kemungkinan).

Panjang kunci merupakan faktor utama dalam sekuritas data. RC4 dapat memiliki kunci sampai dengan 128 bit. Protokol keamanan SSL (Secure Socket Layer) pada Netscape Navigator menggunakan algoritma RC4 40-bit untuk

enkripsi simetrisnya. Tahun 1995, Damien Doligez menjebolnya menggunakan 120 komputer Unix yang terhubung pada jaringan dalam waktu 8 hari. Dengan cara seperti ini (Brute Force Attack), dijamin bahwa dalam 15 hari kunci itu pasti ditemukan. Algoritma RC4 memiliki dua fase, setup kunci dan peng-enkripsian. Setup untuk kunci adalah fase pertama dan yang paling sulit dalam algoritma ini. Dalam setup N-bit kunci (N merupakan panjang dari kunci), kunci enkripsi digunakan untuk menghasilkan variabel enkripsi yang menggunakan dua buah array, state dan kunci, dan sejumlah-N hasil dari operasi penggabungan.

Operasi penggabungan ini terdiri dari pemindahan (swapping) byte, operasi modulo, dan rumus lain. Operasi modulo merupakan proses yang menghasilkan nilai sisa dari satu pembagian. Sebagai contoh, 11 dibagi 4 adalah 2 dengan sisa pembagian 3, begitu juga jika tujuh modulo empat maka

akan dihasilkan nilai tiga. Dahulu, variabel enkripsi dihasikan dari setup kunci dimana kunci akan di XOR-kan dengan plain text untuk menghasilkan teks yang sudah terenkripsi. XOR merupakan operasi logik yang membandingkan dua bit biner. Jika bernilai beda maka akan dihasilkan nilai 1. Jika kedua bit sama maka hasilnya adalah 0. Kemudian penerima pesan akan mendekripnya dngan meng XOR-kan kembali dengan kunci yang sama agar dihasilkan pesan dari plain text tersebut. Untuk menunjukan cara kerja dari algoritma RC4, berikut akan dijelaskan dengan menggunakan empat-bit kunci, agar terlihat sederhana.

Buat array state Si berukuran 4 byte, yang memiliki nilai 0 sampai dengan 3

Si = 0 1 2 3
S0 S1 S2 S3

Buat array kunci Ki berukuran 4 byte,yang memiliki nilai pengulangan dari

kunci untuk memuat keseluruhan isi array. (sebagai contoh 1 dan 7)

Ki = 1 7 1 7
K0 K1 K2 K3

Untuk operasi penggabungan akan digunakan variabel i dan f untuk meng-index array Si dan Ki . Pertama inisialisasikan i dan f dengan nilai 0. operasi penggabungan me-rupakan iterasi dari formula (f + Si + Ki) mod 4 diikuti penggantian (swap) nilai Si dan Sf.

Iterasi pertama
for I = 0 (0 + 0 + 1) mod 4 = 1 = f
F s0 k0
Swap S0 dengan S1
Si = 1 0 2 3
S0 S1 S2 S3
Iterasi kedua
for i = 1 (1 + 0 + 7) mod 4 = 0 = f
f S1 K1
Swap S1 dengan S0
Si = 0 1 2 3
S0 S1 S2 S3
Iterasi ketiga
for i = 2 (0 +2 +1) mod 4 = 3 = f
f S2 K2
Swap S2 dengan S3
Si = 0 1 3 2
S0 S1 S2 S3
Iterasi keempat
for i = 3 (3 +0 +7) mod 4 = 2 = f
f S3 K3
Swap S3 dengan S2
Si = 0 1 3 2
S0 S1 S2 S3

Tentukan nilai byte acak untuk enkripsi. Inisialisasi ulang i dan f menjadi 0, set i menjadi (i + 1) mod 4 dan set f menjadi (f + Si) mod 4. Lalu swap Si dan Sf. Set t menjadi (Si + Sf) mod 4, nilai acak untuk enkripsi adalah St

(0 + 1) mod 4 = 1 = i
i
(0 + 2) mod 4 = 2 = f
f Si
Swap S1 dengan S2
Si = 1 0 2 3
S0 S1 S2 S3
t = 3 (0 + 2) mod 4 = 2 = f
S1 S2
S2 = 2

Dua (nilai biner = 00000010), variabel enkripsi ini lalu di XOR-kan dengan plain text untuk menghasilkan ciphertext. Sebagai contoh akan digunakan pesan “HI”

```
          H              I
    0 1 0 0 1 0 0 0 0 1 0 0 1 0 0 1
XOR 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0
    0 1 0 0 1 0 1 0 0 1 0 0 1 0 1 1
```

3. HASIL DAN PEMBAHASAN

Pengujian perlu dilakukan untuk menguji sistem /aplikasi yang telah dibuat apakah sudah sesuai dengan rancangan awal atau tidak. Pengujian yang akan dilakukan yaitu menguji semua proses pada semua halaman yaitu halaman Home, Register, Obrolan, Teman, dan Undang Teman.

Uji coba dilakukan setelah pembuatan perangkat lunak selesai dengan percobaan pada smartphone tampilan pengguna. Dengan melakukan uji coba ini dapat dilakukan untuk mengetahui kemungkinan terjadinya kesalahan dan untuk memastikan fungis-fungsi yang terdapat pada modul-modul aplikasi ini apakah sudah berjalan dengan baik.

Dalam proses pengujiannya metode yang digunakan adalah black box, seerti yang ditunjukan pada Tabel 3.1. Metode ini dipilih karena pengetesan cukup mengetahui semua fungsi–fungsi yang ada dalam sistem berjalan tanpa ada kesalahan dan tidak memerlukan pengetesan secara detail / logis.

Tabel 4.1 Penujian Black Box

No	Deskripsi	Kasus Uji	Kondisi Awal	Hasil yang diinginkan
1	Instal Aplikasi.	Menginstal aplikasi di perangkat Smartphone.	Normal : Aplikasi dapat di instal	Normal : aplikasi muncul pada menu smartphone.
			Tidak Normal : Aplikasi tidak bisa di instal.	Tidak Normal : aplikasi tidak muncul pada menu smartphone
2	Menjalankan Aplikasi.	Menjalankan aplikasi.	Normal : Aplikasi dapat dijalankan	Normal : Halaman Login bisa muncul.
			Tidak Normal : Aplikasi tidak bisa dijalankan.	Tidak Normal : Halaman login tidak muncul.
3	Menu Register	Mamasukan *nick name, email* dan *password.*	Normal : Halaman Register tampil	Normal : bisa memasukan nick name, email, dan password dan muncul halaman login.
			Tidak normal : halaman Register tidak tampil.	Tidak normal : Tidak bisa memasukan nick name, email, dan password
4	Menu Login	Mamasukan *email* dan *password.*	Normal : Halaman login tampil	Normal : bisa memasukan email dan password dan muncul halaman home.
			Tidak normal : halaman login tidak tampil.	Tidak normal : Tidak bisa memasukan email dan password
5	Menu Home	Tampil Menu Utama	Normal : Menampilkan Menu-menu	Normal : dapat menginput

			yang dapat di akses	waktu masuk absen tenant, waktu keluar absen tenant.
			Tidak Normal : Tidak dapat menampilkan Menu-menu yang dapat di akses	Tidak Normal : Menu-menu tidak dapat di akses
6	Menu Obrolan	Dapat mengirim dan menerima pesan enkripsi dan dekripsi	Normal : dapat mengirim dan menerima pesan enkripsi dan dekripsi	Normal : dapat : dapat mengirim dan menerima pesan enkripsi dan dekripsi
			Tidak Normal : tidak dapat mengirim dan menerima pesan enkripsi dan dekripsi	Tidak Normal : tidak dapat mengirim dan menerima pesan enkripsi dan dekripsi
7	Menu Teman	Menampilkan Teman	Normal : dapat menampilkan teman	Normal : dapat Menampilkan semua teman yang telah di undang
			Tidak Normal : tidak dapat menampilkan teman	Tidak Normal : tidak dapat Menampilkan teman yang telah di undang
8	Menu Undang Teman	Memasukkan PIN Teman	Normal : dapat memasukkan PIN teman yang akan di undang berteman	Normal : dapat Menambahkan teman yang telah di undang
			Tidak Normal : tidak dapat memasukkan PIN teman yang akan di undang berteman	Tidak Normal : tidak dapat Menambahkan teman yang telah di undang
9	Menu Keluar	Mengeluarkan Akun	Normal : dapat Mengeluarkan akun.	Normal : dapat menampilkan dan mengeluarkan akun yang digunakan
			Tidak Normal : tidak dapat Mengeluarkan akun.	Tidak Normal : tidak dapat menampilkan dan mengeluarkan akun yang digunakan

4. KESIMPULAN

Berdasarkan uraian-uraian yang telah di paparkan pada bab sebelumnya, maka pada penelitian yang di analisa dapat menarik kesimpulan bahwa:

Dengan mengaplikasikan menggunakan algoritma RC4 (Rivest Code 4) untuk operasi XOR pada smartphone ini, kirim pesan antar user dapat lebih aman dalam proses pengirimannya.

REFERENSI

Sarkar, Santanu. Proving Empirical Key-Corelations in RC4. *Information processing letters, 2014.*

A.Roos,A class of weak keys in the RC4 stream cipher.Twoposts in sci.crypt http://marcel.wanda.ch/Archive/WeakKeys, 1995.

Jindal, Poonam & brahmjit, Singh. RC4 Encryption-A Literature Survey. *International Conference on Information and Communication Technologies (ICICT 2014).*

Chen & Miaji, Novel strategies for searching RC4 key collisions, *Computers and Mathematics with Applications*, 2013

P. Sepehrdad, S. Vaudenay, M. Vuagnoux, Statistical attack on RC4, in: K. Paterson (Ed.), Eurocrypt 2011, in: LNCS, vol. 6632, Springer, Heidelberg, 2011, pp. 343–363.

P. Sepehrdad, S. Vaudenay, M. Vuagnoux, Discovery and exploitation of new biases in RC4, in: A. Biryukov, G. Gong, D. Stinson (Eds.), SAC2010, in: LNCS, vol. 6544, Springer, Heidelberg, 2011, pp. 74–91.

M. Subhamoy, P. Goutam, S. Sourav, Attack on broadcast RC4 revisited, in: FSE2011, in: LNCS, vol. 6733, Springer, Heidelberg, 2011, pp. 199–217.

J. Chen, A. Miyaji, How to find short RC4 colliding key pairs, in: The 14th Information Security Conference, ISC 2011, in: Lecture Notes in ComputerScience, vol. 7001, Springer-Verlag, 2011, pp. 32–46.

Ariyus, Dony. Kriptografi Keamanan Data dan Komunikasi. Graha Ilmu. Yogyakarta. 2006.

B.N. Marbun. Kamus Manajemen. Jakarta. Pustaka Sinar Harapan. 2003.

Cangara, Hafied. Pengantar Ilmu Komunikasi. Raja Grafindo Persada (Rajawali Perss). Jakarta. 2012.

Dhanta, Rizky. Pengantar Ilmu Komputer. Surabaya. INDAH. 2009.

Effendy, Onong Uchjana. Kamus Komunikasi. PT. Mandar Maju. Bandung. 1989.

Firdaus. 7 Jam Belajar Interaktif PHP & MySQL dengan Dreamwever. Palembang. Maxikom. 2007.

HM, Jogiyanto, Analisis dan Desain Sistem Informasi : Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis, Yogyakarta. ANDI Yogyakarta. 1999.

Kadir, Abdul, Algoritma & Pemprograman Menggunakan Java. Yogyakarta. Andi Yogyakarta. 2012.

Kromodimoeljo, Sentot. Teori Dan Aplikasi Kriptografi. SPK IT Consulting. 2009.

Nugroho, Adi. Rekayasa Perangkat Lunak Menggunakan UML dan Java. Yogyakarta. 2010.

Nugroho, Bunafit. Membuat Aplikasi Database SQL Server dengan Visual Basic 6,0. Gava Media, Yogyakarta. 2007.

Nugroho, Bunafit. PHP dan MySQL dengan editor Dreamweaver MX. ANDI Yogyakarta. 2004.

Prasetyo, Didik Dwi. 101 Tip dan Trik Pemrograman PHP. Buku kedua. Jakarta: PT Elex Media Komputindo. 2008.

Siallagan, Sariadin. Pemrograman Java. Yogyakarta. Andi Yogyakarta. 2009.

Simarmata, Janner. Rekayasa Perangkat Lunak . Yogyakarta. Andi Offset. 2010.

Susanto, Azhar. Sistem Informasi Manajemen. Bandung. Linggar Jaya. 2004.

Syafrizal, Melwin. Pengantar Jaringan computer. Yogyakarta. Andi Yogyakarta 2005.

Widodo, Prabowo.P,Dkk. Pemodelan Sistem Berorientasi Obyek Dengan UML. Graha ilmu. Yogyakarta. 2011.