Peningkatan Keamanan Data dengan Metode *Cropping Selection Pseudorandom*

Pratiwi[#1], Dwi Atmodjo WP[#2]

[#] *Program Studi Teknik Informatika Fakultas Teknologi Informasi*

IKPIA Perbanas Jakarta

[1]wiek.pratiwi@gmail.com

[2]dwiatmojo@gmail.com

Abstraksi - Keamanan data adalah hal yang sangat penting untuk dipertimbangkan pada setiap kegiatan yang berhubungan dengan data rahasia atau terbatas pada komunitas tertentu. Data yang berkaitan dengan informasi sensitif dan berharga akan beresiko jika diakses oleh orang yang tidak berhak. Dalam dunia perbankan banyak data pelanggan yang harus dilindungi dan hati-hati mempertimbangkan faktor keamanan seperti e-banking, sms banking, internet banking, dll Salah satu cara untuk meningkatkan keamanan data dengan kriptografi. Teknik kriptografi ini digunakan untuk melakukan enkripsi dan dekripsi data, mengkonversi atau mengubah data menjadi kode kode tertentu. Hal ini dilakukan agar informasi yang tersimpan dan ditransmisikan melalui jaringan yang paling aman, misalnya melalui Internet. Teknik ini lebih aman karena tidak dapat dibaca oleh siapa pun kecuali oleh mereka yang berhak. Penelitian ini bertujuan untuk meningkatkan keamanan data dengan metode enkripsi keamanan Tanam Pemilihan Pseudorandom. Keuntungan dari teknik enkripsi ini yang menggunakan algoritma enkripsi sangat ringan namun aman dalam arti bahwa hasil enkripsi dapat menyembunyikan data asli menjadi bentuk yang sulit diterjemahkan. Hal lain yang membuat ini metode yang sangat aman dari enkripsi adalah proses algoritma acak atau random sehingga menjadi sulit untuk memprediksi dan dibongkar. Hasil yang dicapai dengan algoritma ini diperoleh akurasi di atas 97% untuk kembali ke bentuk awal.

Kata Kunci : Encryption, Pseudorandom, Crooping Selection, Stream Cipher

Abstract - Data security is a very important thing to be considered at every activity related to confidential data or are limited to a particular community. The data relating to sensitive information and valuable would be at risk if accessed by unauthorized people. In the banking world a lot of customer data that must be protected and carefully considered the safety factor like e-banking, sms banking, internet banking, etc. One of the ways to improve data security with cryptography. This cryptographic technique used to perform the encryption and decryption of data, convert or transform data into a code specific code. This is done so that the information stored and transmitted over the network most safely, for example via the Internet. This technique more safety because it can't be read by anyone except by those who are entitled. This study aims to improve data security with encryption security method Cropping Selection Pseudorandom. The advantage of this encryption technique that uses encryption algorithm is very light but safe in the sense that the results of the encryption can hide the original data into a form that is difficult to translate. Another thing that makes this a very safe method of encryption is the process of random or random algorithm so that it becomes difficult to predict and dismantled. The results achieved with this algorithm obtained an accuracy of above 97% to returns to the initial form.

Keywords : Encryption, Pseudorandom, Crooping Selection, Stream Cipher

I. PENDAHULUAN

Keamanan data menjadi hal yang sangat penting pada saat ini karena untuk setiap pengambilan keputusan, kebijakan harus berdasarkan data. Banyak data yang berisikan informasi penting dan terbatas untuk diketahui pihak yang terkait saja. Pada dunia perbankan banyak kegiatan yang melibatkan data nasabah yang harus diproteksi dan serta sifatnya rahasia. Diungkapan oleh Tedy Heryanto (1999) bahwa banyak kegiatan yang akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak (unauthorized person)[1]. Faktor keamanan data menjadi sangat penting dan harus diperhatikan. Salah satu cara untuk meningkatkan keamanan data diperlukan kriptografi dengan metode enkripsi.

Mengingat bahwa data yang dienkripsi adalah data yang penting maka banyak pihak-pihak yang justru berburu untuk mendapatkan data ini guna didekripsi sehingga dapat dimanfaatkan untuk keperluan lain. Proses dekripsi ini menjadi semakin mudah dengan banyaknya situs-situs online

yang menyediakan layanan enkripsi dan dekripsi tanpa bayar (gratis). Dibawah ini adalah 10 situs online yang menyediakan layanan dekripsi secara gratis, yaitu :
http://blowfish.online-domain-tools.com
http://encoders-decoders.online-domain-tools.com
http://encryption.online-toolz.com
http://www.xarg.org
http://www.yellowpipe.com
tripledes.online-domain-tools.com
http://www.freewarefiles.com
http://www.richkni.co.uk
http://cryptool.shareme.in
http://web.forret.com

Kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah data (plainteks) menggunakan suatu metode enkripsi sehingga yang tidak dapat dibaca secara langsung terutama oleh pihak yang tidak berhak. Metode Enkripsi dilakukan dengan membaca data (plaintext) yang disandikan sehingga Setiap teknik enkripsi memiliki titik lemah. Begitu kelemahan ditemukan maka segera dikembangkan lapisan keamanan baru untuk para user. Salah satu kelemahan yang paling umum terjadi ketika metode enkripsi atau biasa disebut cipher atau alogaritma yang semestinya menghasilkan kode acak[2] .

Individu maupun organisasi yang membutuhkan proteksi tambahan bagi alogaritma enkripsinya sering mengimbuhkan kode ektra ke outputnya. Misalnya, tambahkan karakter pada password yang paling umum dan mudah ditebak, sehingga hacker tidak lagi gampang menerkanya.Enkripsi juga dapat digunakan untuk memverifikasi integritas dari file atau software. Data biner mentah dari file atau aplikasi dijalankan melalui algoritma enkripsi khusus untuk menghasilkan sejumlah digit unik untuk file itu. Apabila ada hacker yang memasukkan kode berbahaya atau korupsi data acak, akan menghasilkan sebuah digit berbeda, sehingga akan diketahui.
Sebuah algoritma matematika untuk menjalankan enkripsi (enchypering) dan dekripsi (*dechypering*) informasi koding binary. Enkripsi mengkonversikan data menjadi bentuk yang sulit ditebak, disebut chyper. Proses dekripsi cypher mengkonversikan data kedalam bentuk aslinya, disebut plain-text. (terjemahan bebas)[3].

Rumusan masalah dalam penelitian ini adalah :

- Sistem keamanan data yang masih memiliki celah untuk ditembus.
- Proses pengamanan data tidak cukup dengan penggunaan password karena banyaknya situs online yang menyediakan layanan encryption/decryption dan password recovery secara gratis.
- Diperlukan model algoritma enkripsi yang baru dan khas dengan melakukan rekasaya terhadap Pseudorandom Generator (PRNG) sedemikian sehingga diperoleh model baru algoritma enkripsi yang belum tersedia decryptornya di situs online maupun software utility pemecah sandi.

II. PENELITIAN SEBELUMNYA

Pengamanan data dan dokumen adalah sangat penting, dan harus dilakukan dengan tuntas. Salah satu bentuk pengamanan data dengan kriptografi menggunakan teknik enkripsi. Pada teknik enkripsi tersebut tidak hanya menyediakan satu metoda saja, tetapi beberapa jenis sehingga dapat memilih yang paling aman.
beberapa penelitian mengenai hal ini telah ada sebelumnya, yaitu:

TABEL I.
PENELITIAN TERKAIT SEBELUMNYA

No	Judul	Penulis	Tema Penelitian
1	Pengamanan Data Menggunakan Metode Enkripsi Einstein	Semuil Tjiharjadi ,Marvin Chandra Wijaya	Algoritma simetri kriptografi Enkripsi dengan metode Einstein
2	Design Web Secure Login dengan Algoritma Enkripsi Simetri RC 6	Arkhan Subari, Mustafid, Kodrat Iman Satoto	AlgoritmaEnkripsi RC 6 untuk keamanan web login
3	Aplikasi Kriptografi dengan Algoritma Message Digest 5 (MD5)	Aghus Sofwan, Agung Budi P, Toni Susanto	Algoritma MD5 memberi garansi bahwa pesan yang disampaikan akan sama dengan yang diterima
4	Analisis Keamanan Sistem Informasi Dengan Metode Enkripsi Menggunakan Algoritma Blowfish	B. Irawan, Irzaman	Analisa Algoritma Blowfish yaitu metode block chipper berbasis bit

A. Kemanan Komputer

Keamanan komputer merupakan kegiatan preventif dari kejahatan yang menggunakan sebagai media. Kemanan yang diperlukan meliputi keamanan fisik (ruangan server dan pendukung infrastruktur), keamanan akses (manusia sebagai pengguna), keamanan data (virus dan pencurian data) dan kemanan sistem operasi komputer. Dalam membangun keamanan komputer harus mempertimbangkan aspek

confidentialy, integrity, authentication, non-repudiation dan *availability*[4].

Aspek *confidentialy* ditujukan untuk menjaga agar data pada komputer tidak jatuh ke tangan yang tidak berhak untuk mencegah penyalahgunaannya. Aspek integrity terkait dengan konsistensi informasi data agar tidak dimodifikasi atau dirusak oleh pihak lain. Pada aspek ini sering digunakan metode enkripsi untuk penyandian. Aspek authentication terkait dengan identifikasi kebenaran pihak pengguna dan kebenaran sumber data. Sedangkan pada aspek non-repudiation untuk menjada penyangkalan akses data oleh pihak yang seharusnya bertanggung jawab pada data tersebut.Aspek availability menekankan bagaimana ketersediaan informasi jika pengguna tidak dapat mengakses data pada komputer yang disebabkan adanya kejahatan komputer tersebut.

Dalam upaya meningkatkan keamanan komputer dilakukan tindakan pencegahan yaitu dengan menggunakan password untuk mencegah kemungkinan pengguna yang tidak berhak melakukan akses terhadap data (*confidentialy*)dan mencegah data tidak dimanipulasi/dirusak (*integrity*) dan memberi authentication pada pihak yang memang berhak untuk akses data tersebut.

B. Enkripsi

Pada prinsipnya Enkripsi adalah proses mengacak atau merubah pesan awal menjadi bentuk dan susunan lain sedemikan sehingga tidak dapat dikenali pesan awal oleh pihak lain. Beberapa proses enkripsi menyertakan kunci didalam proses pangacakannya agar data yang dienkripsi dapat didekripsikan kembali. Proses penyandian pesan dari pesan awal (plaintext) ke pesan baru (ciphertext) dinamakan enkripsi / nchipering Sedangkan proses mengembalikan pesan dari chipertext ke plaintext dinamakan dekripsi /dechipering. Proses enkripsi dan deskripsi ini dapat diterapkan pada pesan yang dikirim, diterima ataupun yang disimpan dalam bentuk dokumen. Algoritma proses enkripsi ini klasik selalu terdiri dari dua bagian yaitu enkripsi dan dekripsi. Ilmu yang mempelajari teknik enkripsi disebut kriptografi[5].

C. Kriptografi

Berdasarkan kata yang membentuk yaitu “Crypto” yanng berarti rahasia dan “graphy” yang berarti tulisan bisa diartikan bahwa Kriptografi adalah tulisan yang dirahasiakan atau dengan kata laian tulisan yang memiliki sifat rahasia sedemikian sehingga hanya orang-orang yang berhak saja yang bisa menterjemahkan tulisannya. William Stallings mendefinisikan kriptografi sebagai “*the art and science of keeping messages secure*”.

Dalam kehidupan sehari-hari kriptografi digunakan sebagai dasar bagi keamanan komputer dan jaringan karena yang menjadi pokok dari fungsi komputer dan jaringan adalah pengelolaan data dan informasi. Data dan Informasi yang bersifat confidential perlu mendapatkan perhatian yang serius mengingat nilai dari infromasi yang terkandung didalamnya sedemikian sehingga diperlukan tata cara untuk menyembunyikan pesan yang tersimpan didalamnya[6].

Secara umum kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plainteks) dengan suatu kunci tertentu menggunakan suatu algoritma enkripsi tertentu sedemiian sehingga menghasilkan informasi baru (chipertext) yang tidak dapat dibaca secara langsung. Chipertext tersebut dapat dikembalikan menjadi informasi awal (plainteks) melalui proses deskripsi.

D. Pseudorandom

Bilangan Random atau Acak adalah adalah bilangan yang dihasilkan dari suatu proses dan hasilnya tidak dapat diketahui secara pasti. Disebut pseudorandom atau random yang semu karena barisan bilangan ini dihasilkan melalui suatu rumus atau formula tertentu, sedemikian sehingga bilangan acak yang dihasilkan oleh pseudorandom tidak benar-benar acak. Pseudorandom telah digunakan pada kriptografi yaitu dalam sistem radio komunikasi, alat pengukur jarak pada frekuensi radio. Tujuan aplikasi pertama adalah kerahasiaan. Pseudorandom akan dicobakan untuk keamanan data elektronik namun dengan sifatnya yang belum benar-benar random perlu dilakukan rekayasa yang tepat untuk mendapatkan tingkat kemanan data yang memadahi[7].

Formula yang sering digunakan pada proses menghasilkan bilangan acak dengan pesudorandom (PRNG) adalah :$x_n = ax_{n-1}$ modulo m dimana Modulo adalah sisa hasil bagi.

III. METODE PENELITIAN

A. Jenis Penelitian

Penelitian ini bersifat Explorasi yaitu dilakukan ketika tidak ada atau sedikit kajian penelitian atas suatu masalah. Fokusnya adalah mendapatkan wawasan lebih luas dari penelitian terkait sebelumnya.

Metode penelitian yang digunakan dalam penelitian ini adalah action reasearch. Menurut Gurito dkk (2010), Action reasearch adalah bentuk penelitian terapan (applied research) yang bertujuan mencari cara efektif yang menghasilkan perubahan disengaja dalam suatu lingkungan yang sebagian dikendalikan (dikontrol). Tujuan utama action reasearh adalah memasuki suatu situasi, melakukan perubahan, dan memantau hasilnya

Metodologi yang digunakan untuk penelitian ini meliputi beberapa tahapan seperti pada gambar 4. Pada penelitian ini dilakukan tahapan mulai dari analisis kebutuhan, desain prototype yang akan dibuat, kemudian membangun prototype. Setelah prototype dibuat akan dilakukan pengujian yang selanjutnya akan di evaluasi

B. Defenisi Konseptual dan Operasional Variabel.

Pseudorandaom : adalah adalah bilangan yang dihasilkan dari suatu proses dan hasilnya tidak dapat diketahui secara pasti.

Enkripsi : adalah proses mengacak atau merubah pesan awal menjadi bentuk dan susunan lain sedemikan sehingga tidak dapat dikenali.

Kriptografi : adalah tulisan yang dirahasiakan atau dengan kata laian tulisan yang memiliki sifat rahasia sedemikian sehingga hanya orang-orang yang berhak saja yang bisa menterjemahkan tulisannya. William Stallings mendefinisikan kriptografi sebagai "*the art and science of keeping messages secure*".

C. Variabel-variabel.

Variabel-variabel yang digunakan dalam penelitia ini adalah :

Plain Text adalah Text yang akan di enkripsi.

Chiper Text adalah Text hasil enkripsi.

RandSeed adalah angka awal sebagai bibit angkat random.

D. Instrumen penelitian

Instrumen yang digunakan dalam penelitian ini selain variable adalah aplikasi Programming Langguage yang dipakai untuk mensimulasikan proses enkripsi dan dekripsi.

E. Populasi dan sample

Sample data enkripsi dan dekripsi yang daiabil dari beberapa situs online yang menyediakan layanan dekripsi secara gratis, yaitu :

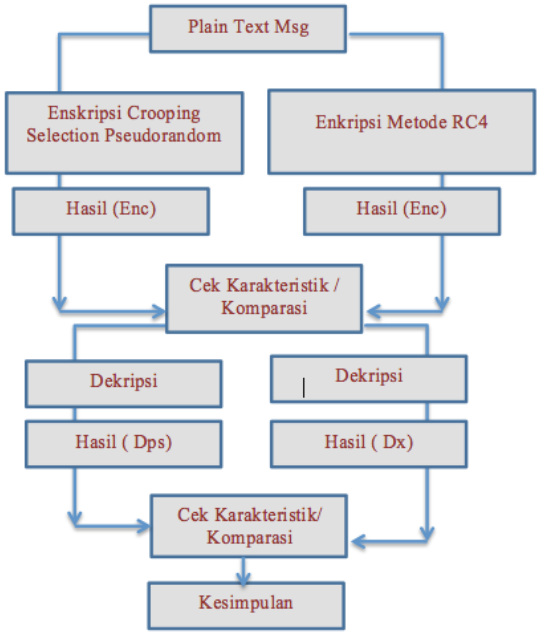
http://blowfish.online-domain-tools.com
http://encoders-decoders.online-domain-tools.com
http://encryption.online-toolz.com
http://www.xarg.org
http://www.yellowpipe.com
tripledes.online-domain-tools.com
http://www.freewarefiles.com
http://www.richkni.co.uk
http://cryptool.shareme.in
http://web.forret.com

F. Metode Pengumpulan data.

Data yang diperlukan diperoleh dari aplikasi yang akan dihasilkan dalam penelitian ini dan dari Situs online diatas.

G. Metode Analisa

Pada penelitian ini dilakukan dengan tahapan mulai dari pemilihan metode enkripsi yang akan digunakan sebagai sarana untuk melakukan enkripsi / dekripsi text. Hasil dari proses ini akan dibandingkan dengan enkripsi dengan metode pseudo random. Jika hasilnya memiliki karakteristik yang sulit untuk di dekripsi maka metode pseudo random layak untuk digunakan sebagai alternative untuk meningkatkan kompleksitas keamanan data elektronik. Dalam proses komparasi akan digunakan metode similarity yang dapat memberikan gambaran tentang tingkat kesamaannya dengan metode yang dibandingkan.



Gambar 1. Kerangka Penelitian

Penelitian ini diawali dengan melakukan proses enkripsi dan dari sebuah pesan dalam bentuk plain text yang akan dienkripsi dengan metode pseudorandom. Hasil dari metode ini akan dibandingkan dengan enkripsi algoritma Cropping Selection Pseudorandom. Jika memiliki karakteristik yang sama maka Algoritma CSPR bisa dikatakan memiliki peluang yang sejajar untuk digunakan sebagai alternatif peningkatan keamanan metode enkripsi data dengan Pseodorandom.

Konsep similarity (kesamaan object) sudah menjadi isu yang sangat penting di hampir setiap bidang ilmu pengetahuan. Zaka (2009) dalam disertasinya menjelaskan tiga macam teknik yang dibangun untuk menentukan nilai similarity (kemiripan) dokumen.

H. *Distance-based similarity measure*

Distance-based similarity measure mengukur tingkat kesamaan dua buah objek dari segi jarak geometris dari variabel-variabel yang tercakup di dalam kedua objek tersebut. *Metode Distance-based similarity ini meliputi Minkowski Distance, Manhattan/City block distance, Euclidean distance, Jaccard distance, Dice's Coefficient, Cosine similarity, Levenshtein Distance, Hamming distance, dan Soundex distance*.

I. *Feature-Based Similarity Measure*

Feature-based similarity measure melakukan penghitungan tingkat kemiripan dengan merepresentasikan objek ke dalam bentuk feature-feature yang ingin

diperbandingkan. Feature-based similarity measure banyak digunakan dalam melakukan pengklasifikasian atau pattern maching untuk gambar dan teks.

J. *Probabilistic-based similarity measure*

Probabilistic-based similarity measure menghitung tingkat kemiripan dua objek dengan merepresentasikan dua set objek yang dibandingkan dalam bentuk probability. Kullback Leibler Distance dan Posterior Probability termasuk dalam metode ini.

Dalam penelitian ini proses komparasi untuk menentukan kesamaan karakteristiknya digunakan pendekatan Cossine Similarity. Metode ini sangat cocok digunakan karena kita bisa melihat kasusnya sebagai dua buah vektor yang memiliki beberapa variable. Variable variable inilah yang menentukan karakteristik dari vektornya. Secara matematis bisa dijabarkan sebagai berikut. Jika sebuah hasil Enkripsi dipandang sebagai sebuah Vektor x dimana vektor x direpresentasikan sebagai x = {x1, x2, . . .,xn} dan Vektor Y dimana vektor y direpresentasikan sebagai y = {y1, y2,…,yn} maka

$$\text{Cos}(x,y) = \frac{x \cdot y}{\| x \| \, \|y\|}$$

Sedemikian sehingga nilai Cos(x,y) akan berkisar dari 0 sampai 1. Akibatnya semakin tinggi nilai Similarity(x,y) maka dua bisa dikatakan kedua besaran memiliki kemiripan yang signifikan.

Tahap berikutnya adalah proses dekripsi pesan yang telah dienkripsi melalui beberapa algoritma enkripsi akan dikembalikan ke pesan semula. Jika proses pengembalian ini berhasil dalam arti Pesan bisa dikembalikan seperti asalnya maka bisa disimpulkan bahwa akan bisa dibuat sebuah aplikasi yang bisa digunakan untuk menyandikan pesan maupun dokumen.

K. Lokasi penelitian

Penelitian ini obyeknya adalah data yang disimpan di dalam komputer/ laptop pemegang otoritas data maka penelitian ini dilaksanakan dimana saja juga data yang ada di kampus IKPIA Perbanas Jakarta.

IV. PEMBAHASAN

A. Deskripsi Obyek Penelitian

Penelitian ini diawali dengan proses enkripsi dan pesan dalam teks biasa yang akan dienkripsi dengan beberapa metode. Hasil dari metode ini akan dibandingkan dengan enkripsi *Tanam algoritma Seleksi Pseudorandom*.

Kelemahan menggunakan PRNGs Enkripsi menggunakan nomor dasar (*randomseed*) dan urutan angka yang akan dihasilkan digunakan untuk menyembunyikan teks biasa.

Sebagai ilustrasi maka peneliti menggunakan PRNGs *Linear Congruential Generator* (LCG) sebagai pembangkit bilangan acaknya. Formula dasar yang akan digunakan untuk menghasilkan bilangan random adalah :

xn = 3 xn-1 + 5 mod 31

sehingga akan didapatkan bilangan random :

2, 11, 7, 26, 21, 6, 23, 12, 10, 4, 17, 25, 18, 28, 27, 24, 15, 19, 0, 5, 20, 3, 14, 16, 22, 9, 1, 8, 29, 30

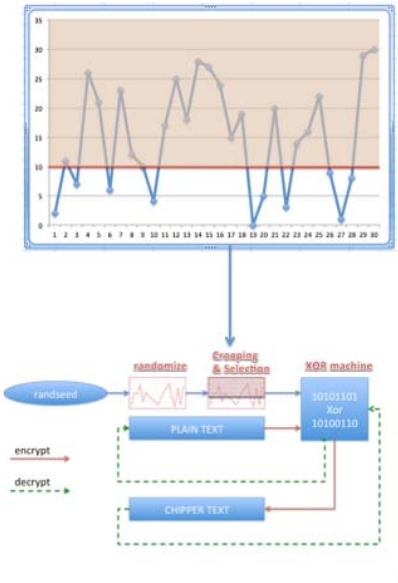
Dalam proses enkripsi bilangan diatas akan langsung digunakan untuk mengubah plain text menjadi cipher text dengan operasi XOR. Namun pada metode CSPs (Crooping Selection Pseudorandom) hasil diatas masih perlu diseleksi dan dibuang yang tidak masuk dalam hasil seleksi. Jika kita menggunakan syarat seleksi adalah yang memenuhi Xn<=10 maka bilangan yang memenuhi adalah :

2,7,6,10,4,0,5,3,9,1,8

Sedangkan urutan bilangan yang digunakan adalah :

X0, X3, X6, X9, X10, X19, X20, X22, X26, X27, X28.

Bilangan hasil seleksi inilah yang akan digunakan untuk melakukan enkripsi plain text. Sehingga algoritma enkripsi dengan CSPs (*Crooping Selection Pseudorandom*) dapat digambarkan sebagai berikut :

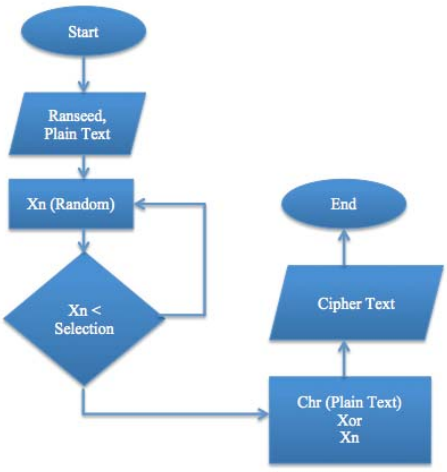


Gbr.2 algoritma enkripsi dengan CSPs (*Crooping Selection Pseudorandom*)

Dibawah ini adalah perbandingan hasil enkripsi menggunakan RC4 dan Crooping Selection Pseudorandom dengan PRNGs yang disediakan oleh Compiler.

Linear congruential generator atau LCG adalah PRNG yang memiliki periode berulang yang pendek sehingga Pembangkit bilangan acak ini kurang aman digunakan untuk cryptografi, dalam hal ini peneliti menggunakan PRNGs yang disediakan oleh compiler Delphi. Dengan menerapkan Crooping Selection pada Pembangkit bilangan acak yang disediakan oleh compiler dengan periode berulang sangat besar (2^{32}), maka penambahan proses Crooping selection akan

membuat proses prediksi nilai random lebih sulit. Ini adalah akibat langsung dari proses seleksinya sedemikan sehingga Xn+1 belum tentu dihasilkan dari nilai X sebelumnya oleh fungsi randomnya.
Algoritma yang digunakan dapat dilihat pada gambar dibawah ini :



Gbr. 3 Algoritma dalam Penelitian

Proses Komparasi dengan antara RC4 dengan Crooping Selection Pseudorandom.
Komponen yang digunakan untuk membentuk Vektor adalah sebagai berikut :
(a.) Bentuk perubahan untuk plain text dengan karakter yang sama.
(b.) Bentuk perubahan untuk plain text dengan karakter yang berbeda.
(c.) Hasil dekripsi.
V(ax,bx,cx)
Seingga dari percobaan diperoleh hasil sebagai berikut

$$\text{Cos}(x,y) = \frac{x \cdot y}{\| x \| \, \|y\|}$$

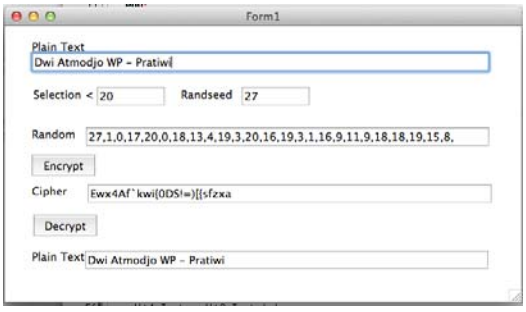
$$\boldsymbol{Cos\ (RC4, CSPs)} = \frac{(1.1+1.1+1.1)}{\sqrt{(1+1+1).(1+1+1)}} = \frac{3}{3} = 1$$

Cos Θ = 1 □ Θ = 90 °

Karena Cos Θ = 90° artinya ketiga karakteristik hasil enkripsi kedua metode diatas memiliki kemiripan yang signifikan.

Gbr. 4 Tampilan Layar

Dibawah ini adalah contoh encrypt dan decrypt dengan algoritma Cropping Selction Pseudorandom .



Gbr. 5 contoh encrypt dan decrypt dengan algoritma Cropping Selction Pseudorandom

V. KESIMPULAN DAN SARAN

1. Salah satu kelemahan dari Pseudorandom Encryption adalah predictable pada bilangan yang dihasilkan. Ini dapat dipahami karena bilangan random hasil daro Pseudorandom urutan n+1 adalah hasil dari bilangan sebelumnya, dengan penambahan crooping dan seleksi bilangan yang dihasilkan menjadi bergantung pada bagian yang diseleksi dan diabaikan, sedemikian sehingga sifat urutan bilangan random berubah, menjadi n+1 belum tentu dihasilkan dari bilangan sebelumnya. Sifat inilah yang akan menambah kehandalan ekripsi dengan pseudorandom.
2. Jika hasil enkripsi dibandingkan dengan metode RC4, dengan mengambil kriteria:
   - Bentuk perubahan untuk plain text dengan karakter yang sama.
   - Bentuk perubahan untuk plain text dengan karakter yang berbeda.

Maka dapat disimpulkan bahwa untuk

- Bentuk perubahan untuk plain text dengan karakter yang sama.
- Antara RC4 dan CSPs masing-masing merubah menjadi bentuk lain yang tidak serupa dengan plain text asal.
- Bentuk perubahan untuk plain text dengan karakter yang berbeda.
- Antara RC4 dan CSPs masing-masing merubah menjadi bentul lain yang tidak serupa dengan plain text asal.
- Hasil Dekripsi.
- Antara RC4 dan CSPs sama-sama dapat dikembalikan menjadi plain text semula.

Sehingga bisa disimpulkan bahwa RC4 dan Crooping Selection memiliki kemiripan dalam hal melakukan enkripsi dari Plain Text ke Cipher Text.

REFERENSI

[1] Alfikri Zakiy Firdaus, Studi dan Analisis Dua Jenis Algoritma Block Cipher: DES dan RC5, 2011

[2] Afiannas R., Cahyani Niken Dwi, Ariyanto Endro, Penggunaan Algoritma Crypt MD5 untuk Kemanan Aplikasi Toko Buku Berbasis Web, 2008

[3] Bogdanov Andrej and Emanuele Viola, Pseudorandom Bits for Polynomials, pp. 41-51, 48th Annual Symposium on Foundation of Computer Science, IEEE, 2007

[4] Bucerzan Dominic, A Cryptographic Algorithm Based on a Pseudorandom Number Generator, 10th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, 2008

[5] Guritno, Suryo, Sudaryono, Rahardja, Untung (2010), Theory an application of IT Reasearch // Metodologi penelitian teknologi Infirmasi, Penerbit Andi, Yogyakart

[6] Nugroho Bayu Kristian, Aplikasi Enkripsi Sms pada Telpon Selular Berbasis J2ME dengan Metode Vigenere Chiper, 2010

[7] Orner Suhaila Sharif and Mansoor, Performance Analysis of Stream and Block Cipher Algorithms, Third International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010