MODEL KEAMANAN DATA PEMBANGKIT BILANGAN ACAK DENGAN MODIFIKASI URUTAN

Pratiwi[1], Dwi Atmodjo WP[2]
Program Studi Teknik Informatika
Fakultas Teknologi Informasi, Institut Perbanas Jakarta
Jakarta, 12940, Indonesia
pratiwi@perbanas.id, wiek.pratiwi@gmail.com
dwi.atmodjo@perbanas.id, dwiatmodjo@gmail.com

ABSTRACT

Security on data by owned becoming a need and necessity that is very important in all aspects of social life. Security of data and information is a key factor that determines whether the data forefront of the information is still useful and can be used. 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 is with cryptography. This cryptographic technique used to perform the encryption and decryption of data, convert or transform data into a code specific code. This study aims to improve data security level with Pseudorandom Modification Sequence. This algorithm was more safety because it couldn't be read by anyone except by those who are entitled. 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.. The results achieved with this algorithm obtained an accuracy of above 95% to returns to the initial form.

Keywords:
data security, encryption method, pseudorandom modification sequence.

1. PENDAHULUAN

Perkembangan data elektronik pada saat ini berkembang sangat pesat seiring perkembangan teknologi informasi. Saat ini, sangatlah mudah untuk bertukar informasi mengenai segala hal, termasuk berbagi ilmu mengenai bagaimana caranya mengakses data secara ilegal. Tak dapat dipungkiri hal ini menyebabkan banyaknya data yang cukup penting harus dipikirkan faktor keamanannya. Faktor keamanan yang dipikirkan dimulai dari mengamankan data yang dimiliki, proses perjalanan data, juga memastikan data diterima oleh orang yang tepat atau berhak mengakses data tersebut.

Keamanan data adalah hal yang sangat penting untuk dipertimbangkan pada setiap kegiatan yang berkaitan dengan data rahasia atau terbatas pada komunitas tertentu. Banyak hal yang menjadi pertimbangan untuk dibuatnya model keamanan data. Tingkat keamanan data informasi yang akan digunakan bermacam – macam bergantung pada kegunaan data informasi tersebut. Data informasi yang digunakan dan dipertukarkan apabila mempunyai kriteria tingkat keamanan yang tinggi harus dijaga keamanan datanya agar tidak terjadi penyalahgunaan dan pembajakan. Data yang berhubungan 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 dan sebagainya.

Dalam upaya untuk meningkat-kan keamanan data dilakukan dengan kriptografi. Teknik kriptografi ini digunakan untuk melakukan enkripsi dan dekripsi data, menyandikan atau mengubah data menjadi kode kode tertentu. Hal ini dilakukan agar informasi yang tersimpan tetap aman dapat dikirim melalui jaringan internet dan diterima oleh orang yang berhak secara aman pula. Teknik ini dirasa lebih aman karena hanya dapat dibaca oleh mereka yang berhak akan data ini. Penulis melakukan penelitian ini bertujuan untuk meningkatkan tingkat keamanan data dengan teknik psedorandom (bilangan acak) dengan melakukan modifikasi urutan. Keuntungan dari

teknik enkripsi ini yaitu 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 adalah proses algoritma random atau acak sehingga menjadi sulit untuk memprediksi dan dibongkar.

Hal yang sangat penting dalam mengamankan data dan dokumen harus dilakukan oleh siapapun yang berkecimpung dalam pengolahan data, terutama data data yang sifatnya terbatas diketahui kalangan tertentu. Salah satu bentuk pengamanan data dengan kriptografi menggunakan teknik enkripsi dan ternik ini tidak hanya menyediakan beberapa jenis metoda dan dapat memilih yang paling aman. Beberapa penelitian mengenai hal ini telah ada sebelumnya, yaitu Aplikasi Teori Bilangan di Dalam Masalah Kriptogtafi yang membahas Aplikasi dari teori bilangan, sebagai salah satu cabang ilmu matematika, di dalam Kriptografi [1] (Yosafat Eka Prasetyo Pangalela). Penelitian lain yang dilakukan Semuil Tjiharjadi, Marvin Chandra Wijaya mengenai Pengamanan data menggunakan Algoritma Stream Cipher Seal [2]. Penelitian tentang Kriptografi dengan MD 5 juga dilakukan oleh Rezza Mahyudin dan Agus dan Agung [3][4]

KEAMANAN DATA

Keamanan data pada komputer merupakan kegiatan preventif dari kejahatan yang menggunakan pencurian data dengan media jaringan internet seperti email, chatting dan sosial media lainnya. Dalam membangun keamanan data pada komputer juga harus mempertimbangkan berbagai aspek seperti confidentialy, integrity, authentication, non-repudiation dan availability[5].

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 menjaga 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.

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.

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.

Enkripsi, merupakan hal yang sangat penting dalam kriptografi yang merupakan pengamanan data yang dikirimkan terjaga rahasianya, pesan asli disebut *plaintext* yang dirubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *cipher* atau kode. Dekripsi, merupakan kebalikan dari enkripsi, pesan yang telah

dienkripsi dikembalikan ke bentuk asalnya (*plaintext*) disebut dengan dekripsi pesan [6]. Algoritma. yang digunakan untuk dekripsi tentu berbeda dengan yang digunakan untuk enkripsi. Dalam proses enkripsi dan dekripsi dikenal pengertian key (kunci), yang dimaksud di sini adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi jadi 2 (dua) bagian yaitu kunci pribadi (*private key*) dan kunci umum (*public key*).

PSEUDORANDOM MODIFICATION SEQUENCE

Struktur umum pembangkitan bilangan acak semu terdiri atas tiga bagian utama. Pada tahap pertama, jumlah informasi pada pesan (entropi) sistem operasi mulai dikumpulkan dari berbagai kejadian yang ditangkap oleh kernel pada komputer. Pada tahap kedua, entropi yang berhasil dikumpulkan diberikan kepada sebuah entitas penampung (pool). Entitas ini akan melakukan pencampuran dan penanganan kejadian yang diberikan oleh sistem operasi. Tahap terakhir terjadi bila bilangan acak tersebut dibutuhkan oleh pengguna. Bilangan acak diberikan kepada pengguna dengan melalui beberapa algoritma pembangkit bilangan. Setelah bilangan acak diberikan, dimulai lagi tahap pertama. Algoritma pembangkit bilangan acak adalah algoritma dengan masukan minimum dapat menghasilkan suatu deret bilangan acak. Bila masukannya sama, maka akan menghasilkan urutan bilangan acak yang sama pula.

2. METODOLOGI

Penulis melakukan penelitian bersifat deskriptif analitis, yakni diawali dg menggambarkan situasi yang ada yaitu penggunaan teknik kriptografi dalam pengamanan dalam suatu informasi. Metode yang digunakan dalam penelitian ini adalah experiment reasearch. Metode eksperimen murni banyak digunakan pada penelitian dasar (basic research) sedangkan metode penelitian kuasi eksperimen banyak digunakan pada penelitian terapan (applied research). Dengan demikian, peneliti memiliki maksud menguji pengaruh percobaan terhadap karakteristik setelah percobaan.

Gambar 1. Tahapan Penelitian

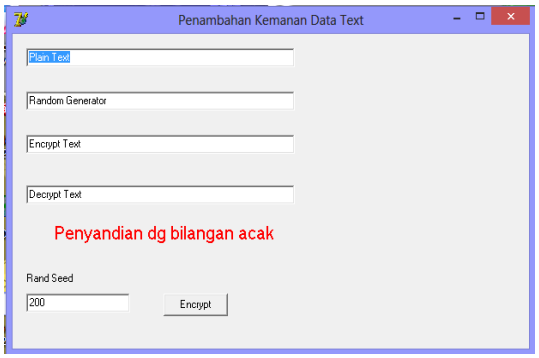
Metodologi yang digunakan untuk penelitian ini meliputi beberapa tahapan seperti pada gambar 1. Pada penelitian ini dilakukan tahapan mulai dari analisis kebutuhan, desain prototype yang akan dibuat, kemudian membangun prototype. Setelah prototype dibuat akan dilakukan pengujian yang selanjutnya akan di evaluasi.

Variabel-variabel yang digunakan dalam penelitian ini adalah *Plain Text* yaitu teks yang akan di enkripsi dan *Chiper Text* yaitu Text hasil enkripsi, serta *RandSeed* adalah angka awal sebagai bibit angkat random. Adapun sampel data enkripsi dan dekripsi yang diambil dari beberapa situs online yang menyediakan layanan dekripsi secara gratis, yaitu seperti : http://encryption.online-toolz.com, http://www.xarg.org,http://www.yellowpipe.com.

3. HASIL DAN PEMBAHASAN

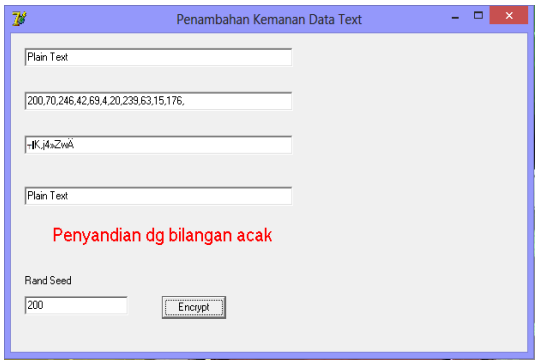
Aplikasi *pseudorandom modification sequence* pada gambar 1 dicobakan pada beberapa data

berupa teks, bilangan dan kombinasi pada keduanya. Pada program penyandian bilangan acak dilakukan pada *Plain Text* yang kemudian dilakukan enkripsi cropping selection pseudorandom yang kemudian dimodifikasi pada urutan secara acak kemudian dilakukan dekripsi sehingga diperoleh *plain text* semula .

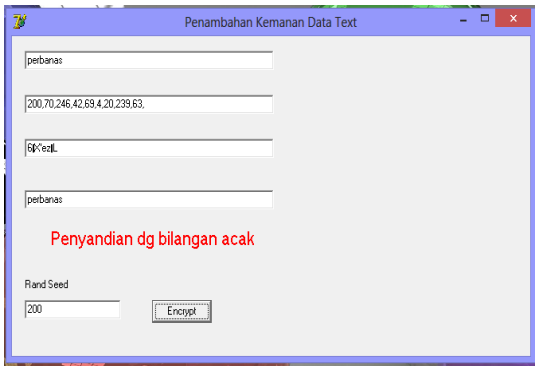


Gambar 2. Tampilan Menu Aplikasi *pseudorandom modification sequence.*

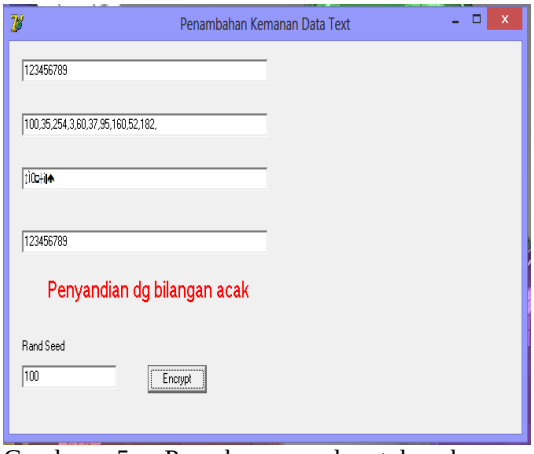
Dibawah ini adalah contoh enkripsi dan dekripsi dengan *pseudorandom modification sequence*, yang ditunjukan dengan data berupa kalimat atau kata-kata terlihat pada gambar 3 dan 4 , juga pada bilangan yang terlihat pada gambar 5 dan terakhir dilakukan pada kombinasi kalimat dan bilangan.



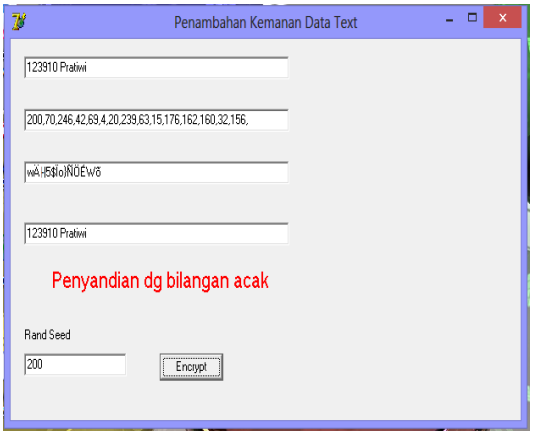
Gambar 3. Percobaan pada teks berupa kata-kata satu.



Gambar 4. Percobaan pada Plain Text kedua.



Gambar 5. Percobaan pada teks berupa bilangan/angka.



Gambar 6. Percobaan pada teks berupa kombinasi teks dan bilangan/angka

4. KESIMPULAN

Salah satu kelemahan dari *Pseudorandom Encryption* adalah dapat diprediksi pada bilangan yang dihasilkan. Dengan penambahan crooping dan seleksi bilangan yang dihasilkan menjadi bergantung pada bagian yang diseleksi dan diabaikan, sedemikian sehingga sifat urutan bilangan random berubah. Modifikasi urutan inilah yang akan menambah kehandalan ekripsi dengan pseudorandom yang kemudian disebut *pseudorandom modification sequence*.
Untuk model keamanan ini, dibutuhkan waktu yang cukup lama untuk menghasilkan deret bit ukuran besar. Hal ini dikarenakan pemrosesan bit yang satu-per satu. Penggabungan operasi metode matematis dan modifikasi urutan bit menghasilkan kehandalan dibandingkan hanya dengan satu metode saja.

DAFTAR PUSTAKA

[1] E. Yosafat Prasetyo, "Aplikasi Teori Bilangan di Dalam Masalah Kriptogtafi (Yosafat Eka Prasetyo Pangalela)." Informatika STEI ITB, 2010.

[2] S. Tjiharjadi and M. W. Chandra, "Pengamanan Data Dengan Menggunakan Algoritma Stream Cipher Seal," *Konf. Nas. Sist. Dan Inform. 2009*, Nov. 2009.

[3] R. Mahyudin, "Algoritma Message Digest 5 (MD5) Dalam Aplikasi Kriptografi." 2006.

[4] A. Sofwan and A. Budi, "Aplikasi Kriptografi Dengan Algoritma Message Diggest 5 (MD5)." Universitas Diponegoro Semarang, 2006.

[5] E. Rahmawati Agustina and A. Kurniati, "Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi Pada e-Voting di Indonesia," *Semin. Nas. Inform. 2009 UPN Yogyak.*, Mei 2009.

[6] T. Puji Rahayu, Yakub, and I. Limiady, "Aplikasi Enkripsi Pesan Teks (Sms) Pada Perangkat Handphone Dengan Algoritma Caesar Cipher." SENTIKA 2012, 10-Mar-2012.