30_PENGAMANAN DATA NASABAH DENGAN METODE ENKRIPSI RC4 &

by Al Amin Imam Husni

Submission date: 11-Apr-2023 05:30AM (UTC+0700)
Submission ID: 2060945665
File name: 30_PENGAMANAN_DATA_NASABAH_DENGAN_METODE_ENKRIPSI_RC4.pdf (912K)
Word count: 1467
Character count: 8957

PENGAMANAN DATA NASABAH DENGAN METODE ENKRIPSI RC4 & STEGANOGRAFI LSB

Arif Kurniawan[1], Imam Husni Al Amin[2]
[1,2]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Stikubank
e-mail: [1]arif@mhs.unisbank.ac.id dan [2]imam@edu.unisbank.ac.id

ABSTRAK

Sistem informasi Koperasi adalah salah satu website yang memiliki proses simpan-pinjam sekaligus penyimpanan hasil proses ke database dan penyimpanan data nasabah. Data nasabah ini sangat penting bagi kepercanyaan nasabah kepada pihak koperasi, maka data nasabah ini harus diamanankan . Keamanan dalam sebuah data termasuk hal yang sangat penting dalam penyebaran sistem secara online. Terdapat banyak kemungkinan data bisa diambil atau disalah gunakan oleh orang lain.

Penelitian ini bertujuan untuk melakukan keamanan pada data nasabah agar bisa terjaga dengan aman. Penelitian ini menggunakan metode Enkripsi RC4 dan Steganografi LSB. Hasil dari penelitian ini adalah Sistem Informasi Koperasi simpan-pinjam dengan penyimpanan proses dan data nasabah yang menerapkan enkripsi RC4 dan Steganografi LSB pada keamanan data nasabahnya.

Kata kunci: sistem informasi koperasi, keamanan data, kriptografi RC4, steganografi LSB

Abstract

Cooperative information system is one website that has a process of saving and borrowing as well as storage of process proceeds to the database and storage of customer data. This customer data is very important for customer's question to the cooperative, then this customer data must be secured. Security in a data is very important in the deployment of the system online. There are many possible data that can be taken or misused by others.

This study aims to perform security on customer data to be safely maintained. This research uses method of RC4 Encryption and LSB Steganography. The result of this research is Saving and Loan Cooperative Information System with process storage and customer data that apply RC4 encryption and LSB Steganography on customer data security.

Keywords: *cooperative information system, data security, RC4 cryptography, LSB steganography*

1. PENDAHULUAN

Keamanan data adalah cara untuk memastikan data yang disimpan aman dari orang lain yang tidak berwenang dan bahwa akses ke sana adalah sesuai dikendalikan. Jadi keamanan data membantu untuk memastikan privasi. Hal ini juga membantu dalam melindungi data pribadi..

Keamananan data bisa dilakukan menggunakan Kriptografi dan Steganografi. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara untuk menyamarkan arti pesan agar menjaga data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa diketahui isinya oleh pihak ketiga. Dalam kriptografi, terdapat 2 proses utama, enkripsi dan dekripsi. Enkripsi adalah proses penyandian pesan asli atau plainteks menjadi cipherteks. Sedangkan dekripsi adalah proses penyandian kembali cipherteks menjadi plainteks[1]

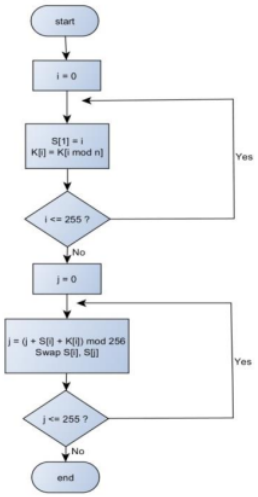
RC4 merupakan salah satu jenis stream cipher yang didesain oleh Ron Riverst di laboratorium RSA (RSA Data Security inc) pada tahun 1987. RC4 sendiri merupakan kepanjangan dari Ron Code atau Rivest's Cipher. RC4 stream cipher ini merupakan teknik enkripsi yang dapat dijalankan dengan panjang kunci yang variabel dan beroperasi dengan orientasi byte[2].

LSB atau kepanjangan dari Least significant bit adalah bagian dari barisan data biner yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. Sedangkan most significant bit adalah sebaliknya, yaitu angka yang paling berarti/paling besar dan letaknya disebelah paling kiri[3].

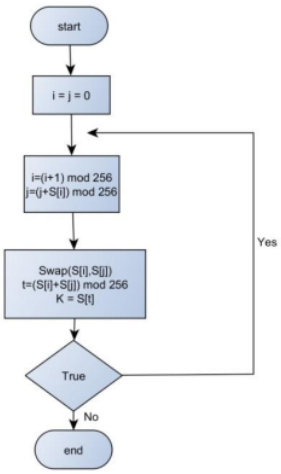
2. METODE PENELITIAN

2.1. Metode Kriptografi RC4

RC4 (Rivest Cipher 4) adalah sebuah synchrone stream cipher, yaitu cipher yang memiliki kunci simetris dan mengenkripsi plainteks secara digit per digit atau byte per byte dengan cara mengkombinasikan dengan operasi biner (biasanya XOR) dengan sebuah angka semiacak [3].



Gambar 1.
key scheduling algorithm (KSA)



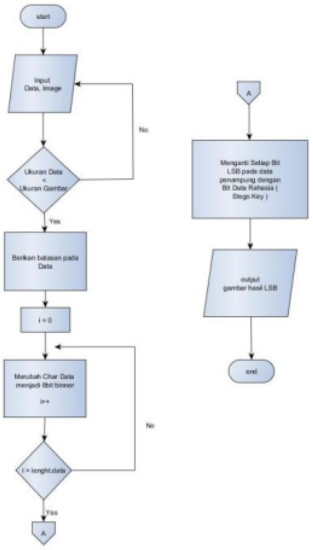
Gambar 2.
pseudo random number generator algorithm (PRGA)

Pada Gambar 1. menjelaskan untuk menginisialisasi permutasi dalam larik "S". "panjang K" didefinisikan sebagai jumlah byte dalam kunci dan dapat berada dalam rentang $1 \leq$ panjang $K \leq 256$, biasanya antara 5 dan 16, sesuai dengan panjang kunci 40 - 128 bit. Pertama, array "S" diinisialisasi ke permutasi identitas. S kemudian diproses untuk 256 iterasi dengan cara yang mirip dengan PRGA utama, tetapi juga mencampur dalam byte kunci pada saat yang sama.

Pada Gambar 2. menjelaskan untuk memodifikasi keadaan dan menghasilkan byte dari keystream. Dalam setiap iterasi, PRGA akan menambah i, mencari elemen i dari S, S [i], dan menambahkannya ke j, menukar nilai S [i] dan S [j], dan kemudian menggunakan jumlah S [i] + S [j] (modulo 256) sebagai indeks untuk mengambil elemen ketiga S, (nilai keystream K di bawah) yang bitwise eksklusif OR'ed (XOR'ed) dengan byte berikutnya dari pesan untuk menghasilkan byte berikutnya baik ciphertext atau plaintext. Setiap elemen S bertukar dengan elemen lain setidaknya sekali setiap 256 iterasi.

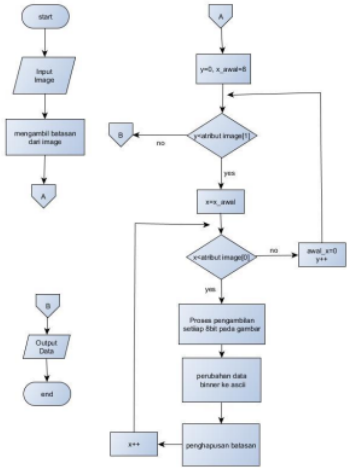
2.2. Metode Steganografi LSB

LSB atau kepanjangan dari Least significant bit adalah bagian dari barisan data biner yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. Sedangkan most significant bit adalah sebaliknya, yaitu angka yang paling berarti/paling besar dan letaknya disebelah paling kiri[3].



Gambar 3. Flowchart LSB

Pada Gambar 3. diatas menjelaskan untuk melakukan proses steganography LSB dengan cara memasukan data yang akan disisipkan dan gambar untuk tempat penyisipannya. Selanjutnya melakukan proses pengecekan bahwa jumlah bit pada data lebih besar dari gambar, jika benar maka proses akan berhenti dan melakakukan proses penyisipan kembali. Jika bit data tidak lebih besar dari gambar maka akan dilakukan proses selanjutnya melakukan proses pembuatan setiap character data dijadikan binner 8bit, dilakukan perulangan sebanyak sejumlah character pada data yang ada. Pada proses terakhir Menganti Setiap Bit LSB pada gambar penampung dengan hasil dari setiap character binner 8bit tersebut.

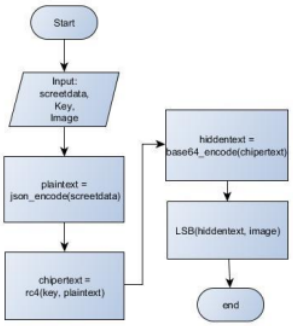


Gambar 4. Flowchart Recovery LSB

Gambar 4. Menjelaskan untuk melakukan proses recovery LSB dengan cara memasukan gambar hasil LSB sebelumnya. Selanjutnya melakukan proses pengambilan batasan pada gambar. Pengecekan setiap horizontal (x) dan vertical(y) pada pixel gambar secara berulang agar mendapat semua pixel yang terdapat data nya, setiap pengecekan dilakukan proses pengambilan data setiap 8bit binner nya terus dirubah menjadi dalam bentuk ascii/text dan melakukan proses penghapusan pada data tersebut, proses dilakukan perulangan terus sampai diambil semua data ascii nya, jika sudah selesai maka akan keluar data nya.

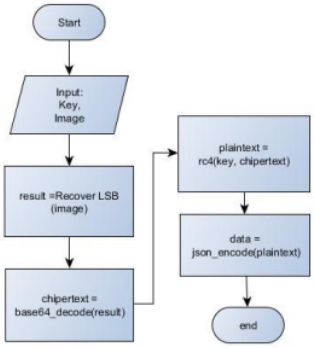
2.3. Flowchart Pengamanan Data Nasabah

Dari pembahasan pada sebelumnya tentang metode RC4 dan LSB disini penulis akan menjabarkan bagaimana cara kedua metode tersebut bisa digabungkan.



Gambar 5. Flowchart pengmanan data

Gambar 5. Menjelaskan untuk melakukukan pengamanan data nasabah dilakukan pemasukan data yaitu screetdata, key dan Image setelah itu screetdata tersebut dirubah menjadi dalam bentuk json, hasil dari json itu disebut plaintext atau data yang akan di enkripsi, lalu melalui proses rc4 untuk mendapatkan chipertext atau hasil dari enkripsi tersebut, hasil tersebut kita lakukakan base64 agar bisa dibaca dengan mudah, dan terakhir lakukan penyembunyian data tersebut kedalam gambar dengna metode LSB.

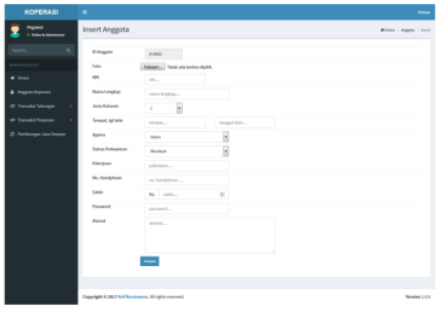


Gambar 6. Flowchart pengembalian data

Gambar 6. Menjelaskan untuk melakukan pengembalian pada data nasabah yang terenkripsi dilakukan pemasukan data yang diperlukan yaitu key dan Image setelah itu gambar tersebut melalui proses recovey LSB untuk mengambil data mentah dari gambar, data tersebut dikembalikan dari bentuk base64 menjadi bentuk chipertext, chipertext tersebut dilakukan proses rc4 dengan memasukan key yang sudah disiapkan akan menghasilkan plaintext, hasil dari plaintext dikembalikan dari bentuk json menjadi data aslinya.

3. HASIL DAN PEMBAHASAN

Halaman Input anggota dapat diakses oleh administrasi Anggota merupakan halaman yang digunakan untuk menyimpan data nasabah anggota koperasi. Mengacu pada penelitian yang dibuat, data anggota yang disimpan pada halaman anggota ini akan dilakukan proses pengamanan data anggota tersebut. Halaman anggota dapat dilihat pada gambar 7.



Gambar 7. input anggota

Dilihat pada gambar 7. ada beberapa inputan yang harus diisi pada anggota koperasi yaitu NIK, nama anggota, foto, jenis kelamin, tempat, tanggal lahir, agama, status perkawinan, pekerjaan, no handphone, saldo, password dan alamat.

Setelah Form di submit maka data pribadi yaitu NIK, jenis kelamin, tempat, tanggal lahir, agama, status perkawinan, pekerjaan, no handphone, foto dan alamat akan dirubah dalam bentuk json dan dilakukan proses enkripsi RC4. Hasil dari RC4 itu akan disembunyikan dengan metode Stegnagrafi LSB, dimana data pribadi tersebut akan disimpan pada foto.

id_anggota	nama_anggota	saldo	gambar	password
A-0001	Arif Kurniawan	830000	A-0001.png	fcc237deadb8a4a7288918556e153473
A-0002	Firmansyah	2070000	A-0002.png	715346c62b65d3c114c0e6234962efc4
A-0003	Pevita	0	A-0003.png	e7a76855450798cb63b4736be8c3aba9

Gambar 8. Data Anggota pada DB

Terlihat pada gambar 8. data yang tersimpan hanya data selain data pribadi yaitu id_anggota, nama_anggota, saldo, gambar dan password

4. KESIMPULAN

Dari hasil penelitian tentang pengamanan data nasabah dengan metode enkripsi RC4 & steganografi LSB dapat disimpulkan bahwa telah terbangun Sistem informasi koperasi simpan-pinjam pada KSPPS BMT NU Sejahtera Sukorejo Kabupaten Kendal yang Menggunakan enkripsi RC4 dan steganografi LSB sehingga membuat data nasabah yang disimpan di database lebih aman.

5. SARAN

Adapun saran-saran yang dapat digunakan untuk pengembangan dari Pengamanan Data Nasabah Dengan Metode Enkripsi RC4 & Steganografi Least Significant Bit bahwa pengembangan sistem informasi koperasi ini belum ada sistem notifikasi ke user melalui sms gateway, email maupun yang lainnya.

DAFTAR PUSTAKA

[1] Suryani, Karina Novita. (2009) *"Algoritma RC4 Sebagai Metode Enkripsi"*. Sekolah Teknik Elektro dan Informatika ITB.

[2] Irfanti, Asti Dwi. (2007). "*Metode pengamanan enskripsi RC4 stream cipher untuk aplikasi pelayanan gangguan"*. Jurusan Teknik Informatika, Fakultas Teknologi Industri, UPN Veteran Jawa Timur.

[3] Utomo, Tri Prasetyo. (2012). "*Steganografi gambar dengan metode least significant bit untuk proteksi komunikasi pada media online"*. Jurusan Teknik Informatika Fakultas, Sains dan Teknologi, UIN Sunan Gunung Djati Bandung.

[4] Amin, Imam Husni Al. (2013). "*Sistem ujian intranet dengan teknik random menggunakan codeigniter"*. Vol. 5, No. 2, Dinamika Informatika.

[5] Amin, Imam Husni Al dan Nur Hasan. (2015). "*Impementasi CRM Untuk Meningkatkan Loyalitas Pelanggan Pada Layanan Catering"*. Vol. 9, No. 1, Hal 11-27, Dinamika Informatika.

30_PENGAMANAN DATA NASABAH DENGAN METODE ENKRIPSI RC4 &

ORIGINALITY REPORT

22%	22%	8%	16%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

6%

★ docgo.net

Internet Source

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		