APLIKASI ENKRIPSI DAN DESKRIPSI DATA MENGGUNAKAN ALGORITMA RC4 DENGAN MENGGUNAKAN BAHASA PEMROGRAMAN PHP

Devina Ninosari[1], Yessi Mardiana[2]

[1, 2] Universitas Dehasen Bengkulu, Bengkulu

Email : [1]devinans@unived.ac.id, [2]yessimardiana@unived.ac.id,

ABSTRAK

Keamanan dan kerahasian data saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan data saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi agar tidak dapat di baca atau di mengerti oleh sembarang orang, kecuali untuk penerima yang berhak, maka dirancang aplikasi sistem pengaman data dengan metode enkripsi menggunakan algoritma 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 semi acak
Keywords: Enkripsi, RC4, XOR

ABSTRACT

Security and confidentiality of data is currently a very important issue and continues to grow. Some cases involving data security is now a job that requires handling and security costs so much. To maintain the security and confidentiality of messages, data, or information that can not be read or understood by any person, except for recipients who are entitled, then the application of a safety system designed by the method of data encryption using the RC4 algorithm.
RC4 (Rivest Cipher 4) is a Synchrone stream cipher, which has a symmetric key cipher and encrypt the plaintext digits are digits per byte by byte or by combining with a binary operation XOR with a random numbers.
Keywords: Encryption, RC4, XOR Operation

1. PENDAHULUAN

Di era globalisasi saat ini, mendapatkan informasi sangatlah mudah. Setiap orang dengan mudah mendapatkan data ataupun berita yang diinginkan. Hal ini didukung dengan teknologi informasi dan komunikasi yang berkembang pesat dari tahun ke tahun. Akan tetapi kemudahan mendapatkan informasi juga memberikan ancaman. Beberapa ancaman yang diberikan adalah masalah tentang keamanan, kerahasiaan, dan keotentikan data. Contohnya seperti *password*, data kerahasiaan perusahaan atau instansi [1].

Salah satu metode *enkripsi* yang terkenal adalah metode RC4.RC4 pertama kali dibuat oleh Ron Rivest di Laboraturium RSA pada tahun 1987. Awalnya RC4 adalah sebuah rahasia dagang, akan tapi pada September 1994, kode tersebut dikirim oleh seseorang yang tidak diketahui ke milist Chypermunks dan menyebar ke banyak situs internet. Kode yang bocor tersebut akhirnya dikonfirmasi sebagai RC4 karena memiliki output yang sama dengan *software* dengan *license* RC4 di dalamnya. Karena algoritma sudah diketahui, RC4 tidak lagi menjadi rahasia dagang. Nama "RC4" sekarang adalah sebuah merek dagang, namun sering disebut sebagai "*ARCFOUR*" atau "ARC4" (artinya diduga RC4, karena algoritma ini tidak pernah dirilis secara resmi oleh RSA), untuk menghindari kemungkinan masalah tentang merek dagang.

SMKS 08 Grakarsa Bengkulu merupakan Sekolah Menengah Kejuruan Swasta yang ada di Kota Bengkulu.Untuk keamana datanya SMKS 08 Brakarsa B memerlukan sebuah sistem enkripsi data agar data tersebut terhindar dari campur tangan pihak ketiga yang dapat memanipulasi data tersebut. Oleh karena itu di SMKS 08 Grakarsa Bengkulu dirancang sebuah sistem kriptografi menggunakan algoritma RC4.

2. TINJAUAN PUSTAKA

2.1 Pengertian Metode Sequential Search

Algoritma adalah cara yang dapat ditempuh oleh komputer dalam mencapai suatu tujuan, terdiri atas langkah-langkah yang

terdefinisidengan baik, menerima *input*, melakukan proses dan menghasilkan *output* [2].

Berikut ini adalah contoh menuliskan algoritma :TUKAR ISI BEJANA;

Algoritma TUKAR_ISI_BEJANA

Diberikan dua buah bejana, A dan B. Bejana A berisi larutan berwarna merah, bejana B berisi larutan berwarnabiru. Pertukarkan isi kedua bejana itu sedemikian sehingga bejana A berisi larutan berwarna biru dan bejana B berisi larutan merah.

Deskripsi:

1. Tuangkan larutan dari bejana A ke dalam bejana C
2. Tuangkan larutan dari bejana B ke dalam bejana
3. Tuangkan larutan dari bejana C ke dalam bejana.

2.2 Pengertian Kriptografi

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mengajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (A. Menezes, P. Van Oorschot and S. Vanstone – Handbook of Applied Cryptography) [3].

kata Kriptografi berasal dari bahasa yunani dan memiliki makna seni dalam menulis pesan rahasia (*The art of secret writing*), dimana kriptografi terdiri dari 2 kata yaitu □□□□□□□□□□□□□yang berarti *rahasia* atau *tersembunyi* dan □□□□□□yang□berarti *tulisan* [4].

Ada empat tujuan mendasar dari ilmu kriptografi ini juga merupakan aspek keamanan informasi yaitu Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/ mengupas informasi yang telah disandi Integritas data adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah.

Pengertian Algoritma RC4

Algoritma RC4 merupakan salah satu jenis *stream cipher*, yaitu memproses unit atau *input* data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah *byte* atau bahkan kadang kadang bit (*byte* dalam hal RC4). Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel.

Algoritma ini tidak harus menunggu sejumlah *input* data, pesan atau informasi tertentu sebelum diproses, atau menambahkan *byte* tambahan untuk mengenkrip. Contoh *stream cipher* adalah *RC4*, *Seal*, *A5*, *Oryx*, dan lain-lain. Tipe lainnya adalah *block cipher* yang memproses sekaligus sejumlah tertentu data, biasanya 64 *bit* atau 128 *bit blok*, contohnya :*Blowfish*, *DES*, *Gost*, *Idea*, *RC5*, *Safer*, *Square*, *Twofish*, *RC6*, *Loki97*, dan lain-lain [5].

RC4 merupakan merupakan salah satu jenis *stream cipher*, yaitu memproses unit atau *input* data pada satu saat. Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah *input* data tertentu sebelum diproses, atau menambahkan *byte* tambahan untuk mengenkrip. Metode enkripsi RC4 sangat cepat kurang lebih 10 kali lebih cepat dari DES.Algoritma RC4 memiliki dua *fase*, setup kunci dan pengenkripsian. Setup untuk kunci adalah fase pertama dan yang paling sulit dalam algoritma ini. Dalam setup S- bit kunci (S merupakan panjang dari kunci), kunci enkripsi digunakan untuk menghasilkan variabel enkripsi yang menggunakan dua buah *array*, state dan kunci, dan sejumlah-S 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 [1].

2.3 Pengertian PHP

PHP adalah bahasa pelengkap HTML yang memungkinkan dibuatnya aplikasi dinamis yang memungkinkan adanya pengolahan data dan pemrosesan data. Semua *sintax* yang diberikan akan sepenuhnya dijalankan pada *server* sedangkan yang dikirimkan ke *browser* hanya hasilnya saja. Kemudian merupakan bahasa berbentuk *script* yang ditempatkan dalam *server* dan diproses di *server*. Hasilnya akan dikirimkan ke *client*, tempat pemakai menggunakan *browser*. PHP dikenal sebagai sebuah bahasa *scripting*, yang menyatu dengan tag-tag *HTML*, dieksekusi di *server*, dan digunakan untuk membuat halaman *web* yang dinamis seperti halnya *Active Server Pages* (ASP) atau *Java Server Pages* (JSP).

PHP merupakan sebuah software *Open Source* [2].

3. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode pengembangan sistem. Adapun langkah-langkah penelitian adalah:

1. Analisis sistem aplikasi kriptografi pesan menggunakan algoritma Rivest Code 4 (RC4).
2. Implementasi dan pengujian sistem, yakni melakukan pengujian terhadap sistem yang telah dirancang.

4. PEMBAHASAN

4.1 Hasil Dan Pembahasan

Aplikasi Enskripsi Dan Deskripsi Data mengunakan algoritma RC4 Dengan menggunakan Bahasa Pemprograman PHP. Sistem ini terdiri dari beberapa menu. Adapun tampilan dari menu-menu tersebut adalah sebagai berikut:

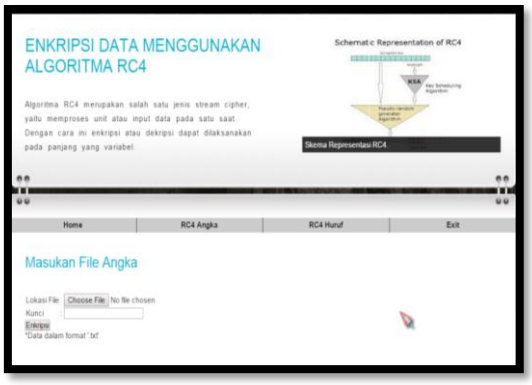
4.1.1 Tampilan Halaman Utama

Halaman ini merupakan tampilan awal sistem.Pada halaman ini disediakan sedikit informasi mengenai algoritma RC 4. Adapun tampilan halaman home dapat dilihat pada gambar berikut 4.1

Gambar 4.1 Tampilan Halaman Utama

4.1.2 *Tampilan Halaman RC4 Angka Open File RC4 Angka*

Pada halaman ini terdapat *form* yang disediakan untuk memasukkan file angka yang berfotmat *.txt* ke sistem. Sehingga data tersebut dapat dienkripsi dan deskripsi.Adapun tampilan halaman *open file* angka dapat dilihat pada Gambar 4.2



Gambar 4.2 Tampilan Halaman Open File Angka

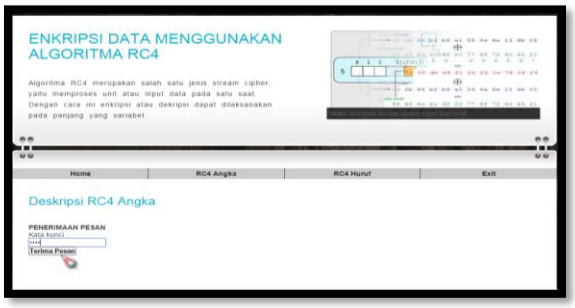
4.1.3 Tampilan Halaman Enskripsi RC4 Angka

Halaman ini digunakan untuk mengekripsi data angka dengan memasukkan angka yang akan dienkripsi ke dalam kotak kosong yang telah disediakan, kemudian masukkan kunci enkripsi minial 5 karakter. Setelah itu klik "kirim" Tampilan halaman enkripsi dapat dilihat pada Gambar berikut 4.3

Gambar 4.3 Tampilan Halaman Enkripsi RC4 Angka

4.1.4 Tampilan Hasil Pencarian Buku Berdasarkan Judul

Halaman ini digunakan untuk mendeskripsi data angka dengan memasukkan kata kunci pada saat enkripsidata sebelumnya. Tampilan halaman deskripsi data angaka dapat dilihat pada Gambar berikut pada gambar 4.4



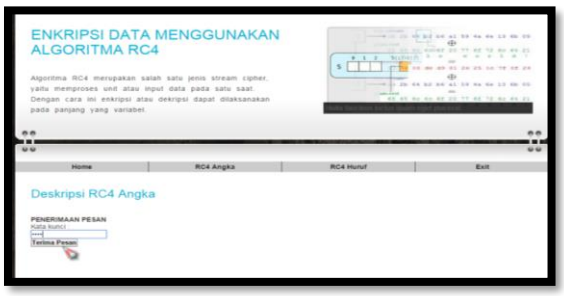
Gambar 4.4 Tampilan Hasil Halaman Deskripsi RC4 Angka

Setelah kata kunci dimasukkan, maka data akan dideskripsi sehingga hasilnya kembali ke *Plaintext*. Seperti pada gambar berikut seperti gambar 4.5.

Gambar 4.5 Tampilan Halaman Hasil Deskripsi RC4 Angka

4.1.5 Tampilan Halaman *Open File*RC4 Huruf

Pada halaman ini terdapat *form* yang disediakan untuk memasukkan *file*huruf yang berfofmat *.txt* ke sistem. Sehingga data tersebut dapat dienkripsi dan deskripsi.Adapun tampilan halaman *open file* huruf dapat dilihat 4.6.



Gambar 4.6 Tampilan Halaman *Open File* RC4 Huruf

Halaman ini digunakan untuk mengekripsi data huruf dengan memasukkan huruf yang akan dienkripsi ke dalam kotak kosong yang telah disediakan, kemudian masukkan kunci enkripsi minial 5 karakter. Setelah itu klik "kirim" Tampilan halaman enkripsi huruf dapat dilihat pada gambar 4.7.

Gambar 4.7 Tampilan Hasil Tampilan Halaman Enkripsi RC4 Huruf

Selanjutnya Halaman ini digunakan untuk mendeskripsi data huruf dengan memasukkan kata kunci pada saat enkripsi data sebelumnya. Tampilan halaman deskripsi data huruf dapat dilihat pada gambar 4.8.

Gambar 4.8 Tampilan Halaman Deskripsi RC4 huruf

4.1.6 Hasil Pengujian Sistem RC4 Huruf

Selanjutnya untuk mengetahui Hasil Pengujian sistem dapat dilihat seperti gambar 4.9

Gambar 4.9 Hasil Hasil Pengujian Sistem RC4

5. KESIMPULAN

Dari hasil dan pembahasan serta pengujian siatam maka dapat diambil beberapa kesimpulan bahwa bahasa pemrograman PHP dapat memberikan kemudahan dalam pembuatan enkripsi dan deskripsi data menggunakan Algoritma RC4 pada SMA Grakarsa Kota Bengkulu Pembuatan sistemenkripsi dan deskripsi data menggunakan Algoritma RC4 dengan menggunakan bahasa pemrograman. PHP pada SMA Grakarsa Kota Bengkulu dapat memberikan kemudahan dalam proses enkripsi data sehingga dapat menjaga kerahasiaan data.

DAFTAR PUSTAKA

[1] Jogiyanto, HM. 2011. *Pengenalan Komputer, Dasar Ilmu Komputer, Pemrograman*, Salemba Empat: Yokyakarta Kurniawan, Rulianto. 2010. *Joomla untuk Orang Awam*. Palembang. Maxikom. 186 halaman.

[2] Ems, TIM. 2012. *Web Progreming for Beginners*. Jakarta: PT Elex Media Komputindo Madcoms. 2008. *PHP dan MySQL untuk Pemula,* Yogyakarta : Andi. 288 halaman.

[3] Alfred J. Menezes, Applied Cryptography, CRC Press ISBN: 0-8493-8523-7 October 1996, 816 pages Handbook

[4] *Mulyono*, Sigit. *2008*. *Perancangan Image Vektor Dengan Adobe. Ilustrator*. UNIKOM. Bandung: BumiAksara.