SEMINAR NASIONAL HASIL PENELITIAN 2021
"Penguatan Riset, Inovasi, dan Kreativitas Peneliti di Era Pandemi Covid-19"
ISBN: 978-623-387-014-6

Kriptografi Menggunakan Aplikasi *Blowfish Advanced CS Pada Sistem Keamanan Data Komputer*

Tasri ponta[1], Sutarsi Suhaeb[2], Sabran[3]
Universitas Negeri Makassar
Email: tasri.ponta43@gmail.com

Abstrak. Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa. Dalam bidang kriptografi terdapat dua konsep yang sangat penting atau utama yaitu enkripsi dan dekripsi. Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah plaintext. Kemudian setelah disamarkan dengan suatu cara penyandian, maka plaintext ini disebut sebagai chipertext. Proses penyamaran dari plaintext ke ciphertext disebut enkripsi *(encryption),* dan proses pengembalian dari ciphertext menjadi plaintext kembali disebut dekripsi *(decryption).* Dalam hal ini file yang dapat di enkripsi adalah file dokumen berupa teks, file citra berupa gambar, serta file audio dan file video dalam format digital. Pada pesan teks, isi file dokumen, atau file dokumen dalam menjaga kerahasiaan informasi datanya memerlukan teknik-teknik enkripsi dan dekripsi yang tidak mudah atau sukar untuk dipecahkan. Proses pengamanan pada pesan teks, isi file dokumen, atau file dokumen dapat dilakukan dengan mengenkripsi pesan teks, isi file dokumen, atau file. Tujuan yang ingin dicapai dalam penelitian ini adalah Bagaimana langkah-langkah menggunakan menggunakan aplikasi *blowfish advanced cs* dan kriptografi pengamanan data pada pesan teks, file, dan dokumen menggunakan menggunakan aplikasi *blowfish advanced cs.* Penelitian ini merupakan jenis penelitian yaitu jenis penelitian kualitatif. Dengan studi kasus yang bertujuan untuk mengetahui tata cara dalam mengimplementasi kriptografi pengamanan data pada pesan teks, file, dan dokumen menggunakan menggunakan aplikasi blowfish advanced cs. Sistem keamanan yang menggunakan aplikasi Blowfish Advance CS pada pesan teks, file, dan dokumen yang meliputi proses enkripsi, deskripsi dan contoh simulasi data dengan menggunakan aplikasi Blowfish advance CS tersebut. Dengan enkripsi, data kita disandikan (encrypted) dengan menggunakan sebuah kunci(key). Untuk membuka (decript) data tersebut digunakan juga sebuah kunci yang sama dengan kunci mengenkripsi tadi atau yang sering disebut dengan private key kriptographi.

Kata Kunci: Kriftografi, Data, Blowfish advance CS

PENDAHULUAN

1. Dokumen Digital

Dokumen merupakan suatu sarana transformasi informasi dari satu orang ke orang lain atau dari suatu kelompok ke kelompok lain. Dokumen meliputi berbagai kegiatan yang diawali dengan bagaimana suatu dokumen dibuat, dikendalikan, diproduksi, disimpan, didistribusikan, dan digandakan. Dokumen digital merupakan setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat

ISBN: 978-623-387-014-6

dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara atau gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya .

2. Kompresi *File* (*File Compress*)

Kompresi *file* adalah suatu cara untuk mengkodekan informasi dengan menggunakan *bit* yang lebih rendah yang digunakan untuk memperkecil ukuran data agar dapat disimpan dengan ruang penyimpanan yang kecil dan juga dapat mempersingkat waktu dalam transfer data.

3. File

File adalah entitas dari data yang disimpan didalam sistem *file* yang dapat diakses dan diatur oleh pengguna. Sebuah *file* memiliki nama yang unik dalam direktori di mana ia berada. Alamat direktori dimana suatu berkas ditempatkan diistilahkan dengan *path*.

Sebuah *file* berisi aliran data (atau data stream) yang berisi sekumpulan data yang saling berkaitan serta atribut berkas yang disebut dengan properties yang berisi informasi mengenai *file* yang bersangkutan seperti informasi mengenai kapan sebuah berkas dibuat.

4. Kriptografi

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (*transposition cipher*) dan algoritma substitusi (*substitution cipher*). *Cipher* transposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan *cipher* substitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain.

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai *plaintext* (teks biasa). Disebut demikian karena informasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja. Algoritma yang dipakai untuk mengenkripsi dan mendekripsi sebuah *plaintext* melibatkan penggunaan suatu bentuk kunci. Pesan *plaintext* yang telah dienkripsi (atau dikodekan) dikenal sebagai *ciphertext* (teks sandi).

5. Blowfish

Blowfish alias "*OpenPGP.Cipher.4*" merupakan enkripsi yang termasuk dalam golongan *Symmetric Cryptosystem* , metoda enkripsinya mirip dengan DES (DES-like Cipher) diciptakan oleh seorang *Cryptanalyst* bernama Bruce Schneier Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang

ISBN: 978-623-387-014-6

kriptografi dan keamanan Komputer) dan dipublikasikan tahun 1994. Sejak saat itu telah dilakukan berbagai macam analisis, dan perlahan - lahan mulai mendapat penerimaan sebagai algoritma enkripsi yang kuat. Dibuat untuk digunakan pada komputer yang mempunyai microposesor besar (32-bit keatas dengan *cache* data yang besar). Sampai saat ini belum ada attack yang dapat memecahkan Blowfish.

Algoritma utama terbagi menjadi dua subalgoritma utama, yaitu bagian ekspansi kunci dan bagian enkripsi-dekripsi data. Pengekspansian kunci dilakukan pada saat awal dengan masukan sebuah kunci dengan panjang 32 bit hingga 448 bit, dan keluaran adalah sebuah array subkunci dengan total 4168 byte.

Bagian enkripsi-dekripsi data terjadi dengan memanfaatkan perulangan 16 kali terhadap jaringan feistel. Setiap perulangan terdiri dari permutasi dengan masukan adalah kunci, dan substitusi data. Semua operasi dilakukan dengan memanfaatkan operator Xor dan penambahan. Operator penambahan dilakukan terhadap empat array lookup yang dilakukan setiap putarannya.

Blowfish juga merupakan *cipher* blok, yang berarti selama proses enkripsi dan dekripsi, Blowfish akan membagi pesan menjadi blok-blok dengan ukuran yang sama panjang. Panjang blok untuk algoritma Blowfish adalah 64-bit. Pesan yang bukan merupakan kelipatan delapan *byte* akan ditambahkan bit-bit tambahan (*padding*) sehingga ukuran untuk tiap blok sama.

Blowfish adalah algoritma yang tidak dipatenkan dan license free, dan tersedia secara gratis untuk berbagai macam kegunaan. Blowfish dirancang dan diharapkan mempunyai kriteria perancangan yang diiginkan sebagai berikut :

1. Cepat, Blowfish melakukan enkripsi data pada microprocessor 32-bit dengan rate 26 clock cycles per byte.
2. Compact, Blowfish dapat dijalankan pada memory kurang dari 5K.
3. Sederhana, Blowfish hanya menggunakan operasi – operasi sederhana, Blowfish hanya menggunakan operasi – operasi sederhana, seperti : penambahan, XOR, dan lookup tabel pada operan32-bit.
4. Memiliki tingkat keamanan yang bervariasi, panjang kunci yang digunakan oleh Blowfish dapat bervariasi dan bisa sampai sepanjang minimal 32-bit, maksimal 448 -bit, Multiple 8 bit, defalutl 128 bit.

Blowfish dioptimasikan untuk berbagai aplikasi dimana kunci tidak sering berubah, seperti pada jaringan komunikasi atau enkripsi file secara otomatis. Dalam pengimplementasiannya dalam komputer bermicroprosesor 32-bit dengan *cache* data yang besar (Pentium dan Power PC) Blowfish terbukti jauh lebih cepat dari DES. Tetapi Blowfish tidak cocok dengan aplikasi dengan perubahan kunci yang sering atau sebagai fungsi hast satu arah seperti pada aplikasi *packet switching*. Blowfish pun tidak dapat digunakan pada aplikasi kartu pintar (*smart card*) karena memerlukan memori yang besar.

Algoritma Blowfish terdiri atas dua bagian :

Key-Expansion Berfungsi merubah kunci (Minimum 32-bit, Maksimum 448-bit) menjadi beberapa array subkunci (subkey) dengan total 4168 byte.

ISBN: 978-623-387-014-6

Enkripsi Data Terdiri dari iterasi fungsi sederhana (*Feistel Network*) sebanyak 16 kali putaran. Setiap putaran terdiri dari permutasi kunci-*dependent* dan substitusi kunci- dan data-*dependent*. Semua operasi adalah penambahan (*addition*) dan XOR pada variabel 32-bit. Operasi tambahan lainnya hanyalah empat penelusuran tabel (*table lookup*) array berindeks untuk setiap putaran.

METODE PELAKSANAAN

Penelitian yang digunakan yaitu jenis penelitian kualitatif. Dengan studi kasus yang bertujuan untuk mengetahui tata cara dalam kriptografi pengamanan data pada pesan teks, file, dan dokumen menggunakan menggunakan aplikasi *blowfish advanced cs*.

1. Lokasi dan Subjek Penelitian

Lokasi penelitian adalah Laboratorium Jurusan Pendidikan Teknik Elektronika, dan subjek penelitian adalah mahasiswa Program Studi Pendidikan Teknik Elektronika FT UNM.

2. Teknik Pengumpulan Data

Dalam penelitian ini, jenis data yang dikumpulkan adalah data primer dan data sekunder. Untuk mengumpulkan data primer dan data sekunder, peneliti menggunakan beberapa teknik pengumpulan data, yaitu :

a. Observasi Observasi adalah pengamatan dan pencatatan yang sistematis terhadap gejala-gejala yang diteliti. Kegiatan ini dilakukan untuk memperoleh keterangan data yang lebih akurat mengenai hal-hal yang diteliti, serta untuk mengetahui relevansi (kesesuaian) antara jawaban responden dengan kenyataan yang terjadi di lapangan.
b. Dokumentasi Yang dimaksud dengan dokumentasi disini adalah cara mengumpulkan data dengan mempelajari dan mencatat bagian-bagian yang diaggap penting yang terdapat baik di lokasi penelitian.
c. Wawancara Wawancara adalah kegiatan tanya jawab lisan antara dua orang atau lebih secara langsung. Wawancara ini dilakukan untuk memperoleh data untuk melengkapi data-data yang diperoleh sebelumnya.

3. Instrumen Pengumpulan Data

Menurut Suharsimi Arikunto menyatakan bahwa instrumen penelitian adalah alat bantu bagi peneliti dalam mengumpulkan data. Dalam penelitian ini, peneliti menggunakan kuesioner sebagai alat untuk melakukan wawancara dan pengamatan terhadap obyek penelitian.

4. Teknik Analisis Data

Menurut Patton yang dikutip oleh Lexy J. Moleong analisis data adalah proses mengatur urutan data, mengorganisasikannya ke dalam suatu pola, kategori dan uraian dasar. Penelitian ini merupakan penelitian deskriptif, dengan lebih banyak

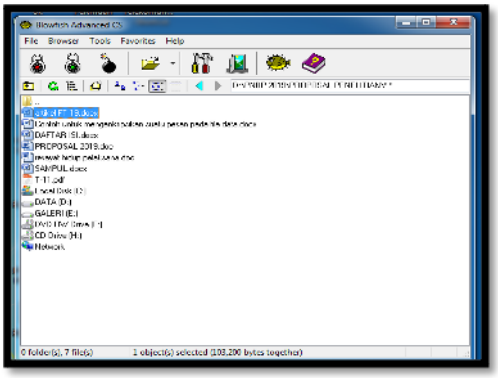
ISBN: 978-623-387-014-6

bersifat uraian dari hasil wawancara dan studi dokumentasi. Data yang telah diperoleh akan dianalisis secara kuantitatif serta diuraikan dalam bentuk deskriptif.

HASIL DAN PEMBAHASAN

A. Pembuktian Algoritma Blowfish

1 Kita terebih dahulu dapatkan toolsnya yang bisa di download secara gratis, saya mendapatkan toolsnya dengan lambang ikan kembung.
2 Lalu kita buka toolsnya dan pilih file apa yang akan kita enkripsikan

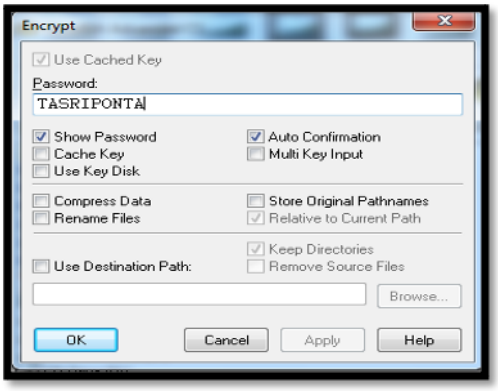


1. Dari gambar diatas saya memilih untuk meng-enkripsikan file "Keamanan Password dan Enkripsi"
2. Lalu klik gambar kunci yang tertutup

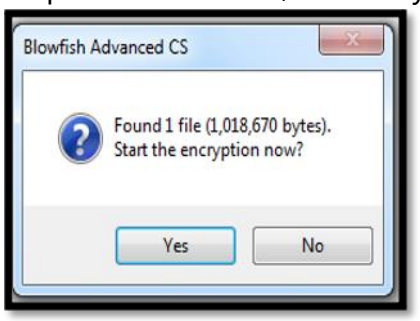
3. setelah di klik maka akan muncul seperti kotak di bawah ini :

ISBN: 978-623-387-014-6

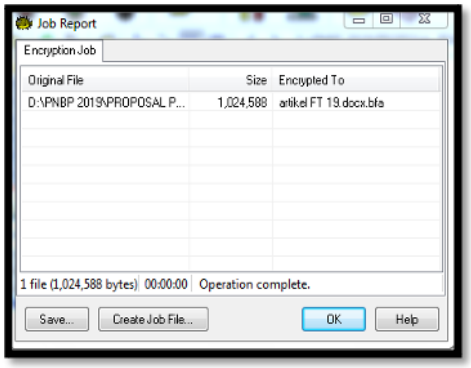
4. Lalu masukkan passwordnya kemudian klik OK



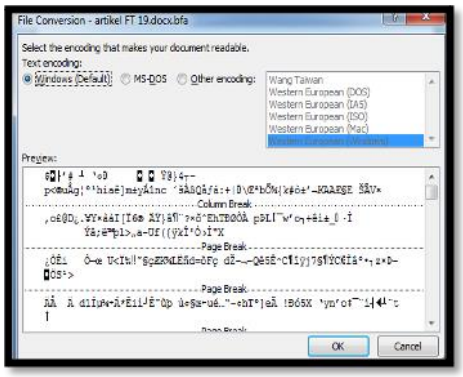
5. Lalu akan keluar tampilan seperti dibawah ini, lalu klik yes



6. Setelah klik yes maka akan keluar tampilan kembali sepeti di bawah ini dan klik OK

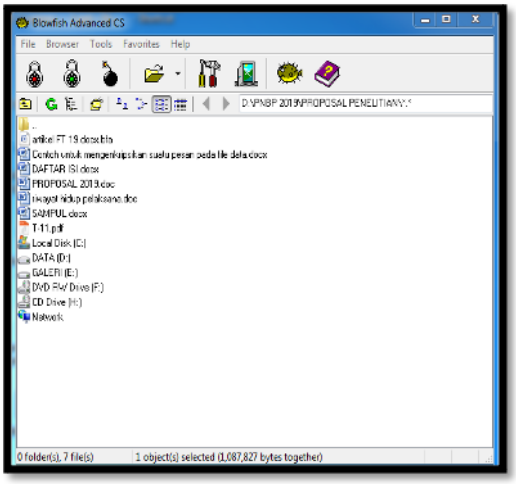


7. Secara otomatis file yang kita enkripdi tadi akan tidak bisa di baca datanya oleh orang lain.
8. Untuk membuktikannya kita buka file tadi lalu lihat apakah yang terjadi pada file tersebut

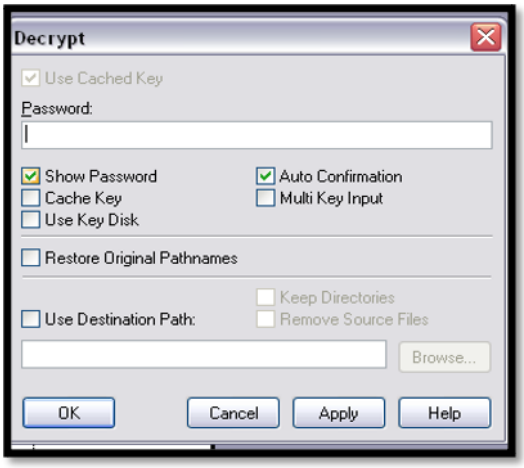


ISBN: 978-623-387-014-6

9. Dan ternyata file tersebut datanya telah aman, data yang ada pada file tersebut telah berubah menjadi sebuah bentuk tuisan aneh yang tdak dapt di mengerti. Dengan itu kita dapat merasa aman dengan data yang kita rahasiakan tersebut.
10. Untuk membuka kembali datanya kita buka kembali toolsnya lalu kita klik tanda kunci yang terbuka.



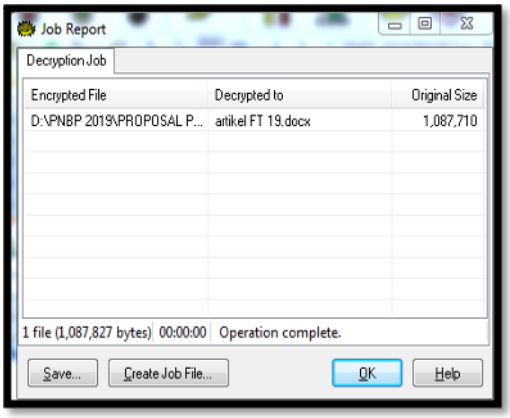
11. masukkan kembali password kita yang tadi lalu kllik OK, dan pasword tadi jangan sampai lupa. Apabila hal tersebut terjadi maka file tersebut tidak akan pernah bisa dibaca kembali.



12. Setelah itu akan keluar kembali tampilan seperti di bawah ini dan klik yes

ISBN: 978-623-387-014-6

13. Maka akan tampil seperti tampilan di bawah ini, lalu klik OK :



14. Maka secara otomatis file yang telah di enkripsi tadi telah berubah menjadi seperti semula sebelum di enkripsi, atau kembali lagi menjadi plaintexs.
15. Untuk membuktikan apakah file yang berisi data "Keamanan Password dan Enkripsi" tadi telah kembali seperi semula maka dapat kembali di buka seperti membuka file seperti biasanya.

KESIMPULAN

Dari analisa algoritma dan simulasi program Blowfish advance CS tersbut dapat disimpulkan sebagai berikut:

1 Pada saat proses key set-up algoritma Blowfish, key ini digabungkannya sehingga menguatkan algoritmanya.
2 Pada saat proses simulasi file/folder data file enkripsi dalam program algoritma Blowfish ini menggunakan key dengan minimum bisa 4 karakter.
3 Kunci yang simetri pada algoritma Blowfish ini sehingga proses simulasi enkripsi dan dekripsi file/folder data selalu menggunakan key yang sama, begitu juga split file dan merger file menggunakan key yang sama.

DAFTAR PUSTAKA

C. Haldankar, and S. Kuwelkar, "Implementation of AED and blowfish algorithm," International Journal of Research in Engineering and Technology, vol. 3, pp. 143-147, May 2014.

Trisnawati, Sistem Keamanan Menggunakan Algoritma Blowfish Advance CS pada File dan Folder Data, Universitas Sriwijaya, 2008.

J. Marcel. T, "Studi perbandingan chiper blok algoritma blowfish dan algoritma camellia," unpublished.

Seminar Matematika Dan Pendidikan Matematika UNY 2017 ISBN. 978-602-73403-2-9 (CETAK), 978-602-73403-3-6 (ON-LINE) .