ALGORITMA BLOWFISH

Analisis Algoritma Blowfish

Sebagian besar dari Blowfish yang menarik adalah f-fungsi yang tidak membalik. Fungsi ini menggunakan aritmatik modular untuk membangkitkan index-index ke dalam S-box. Tidak membalik (non-invertibility) ini dijelaskan sebagai berikut dengan contoh : Ambil fungsi $f(x) = x^2$ mod 7, lihat tabel 1 dibawah ini :

Tabel 1 Contoh fungsi $f(x) = x^2$ mod 7

X	X^2	X^2 Mod 7
1	1	1
2	4	4
3	9	2
4	16	2
5	25	4
6	36	1
7	49	0

Output yang dihasilkan tidak ada fungsi sehingga fungsi yang dihasilkanpun tidak ada fungsi khusus ke f(x). Sebagai contoh jika kita mengetahui bahwa fungsi kita mempunyai sebuah nilai 4 di beberapa nilai X, maka tidak ada cara untuk mengetahui jika nilai X tersebut adalah 2; 5; atau nilai X yang lain yang mempunyai fungsi f(x) = 4. Blowfish melakukan aritmatikanya sebesar mod 2^{32} (2^{32} sama dengan 4 milyar). Ini disebut aritmatik dalam bidang berhingga dan membuat banyak asumsi matematika yang sama yang tidak benar (1+1 tidak sama dengan 2 jika kita berada disebuah bidang ukuran 2 yang berhingga).

S-box adalah array yang besar dari data yang didefinisikan sebelumnya. Selama proses setup key, key tersebut menggabungkan dengan S-box. Detail key-setup ini relatif tidak menarik tetapi kenyataannya bahwa ia menggabungkan key tersebut dengan S-box yang menguatkan algoritma tersebut. Key-setup dalam Blowfish dirancang relatif lamban. Hal ini sangat bermanfaat karena seseorang akan melakukan suatu search-key brute-force yang akan menuju proses key-setup yang lamban untuk setiap key yang dicobanya. Meskipun seseorang melakukan enkripsi dan dekripsi harus hanya menuju proses key-setup satu kali, maka proses enkripsi dan dekripsi relatif cepat.

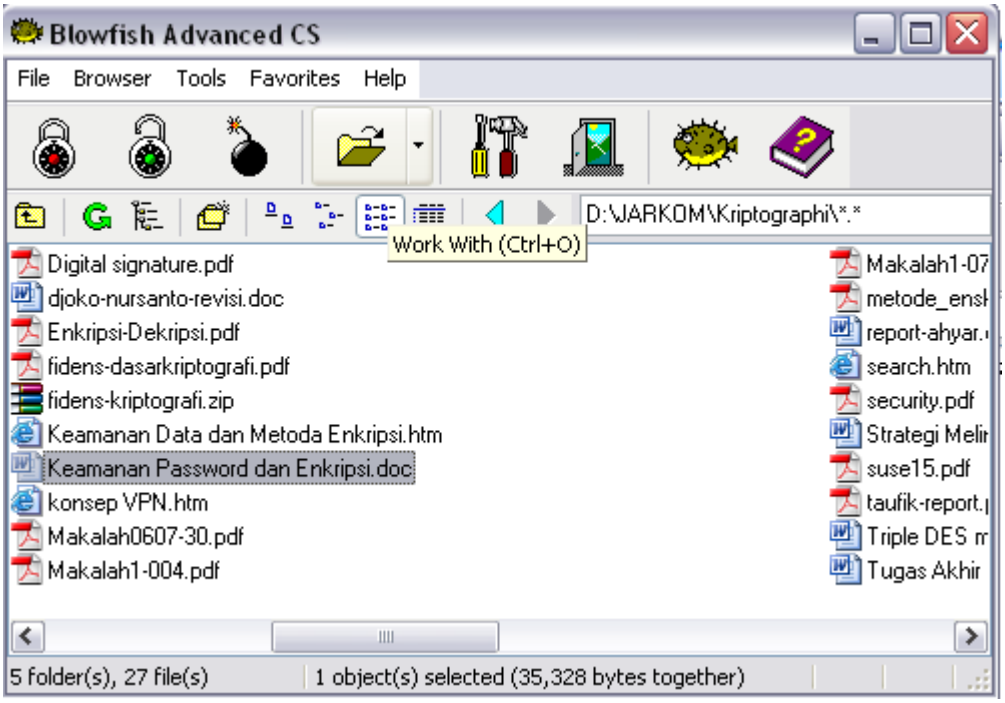
Elemen yang terpenting pada Blowfish yang lain adalah jaringan Feistel. Menggunakan jaringan Feistel yang menghasilkan cipher dengan dua sifat yang dapat diinginkan yaitu dekripsi menggunakan fungsi (f) yang sama dan kemampuan untuk

mengiterasi fungsi tersebut beberapa kali ini disebut round (putaran). Semakin banyak round maka semakin banyak keamanan algoritma tersebut. Jumlah round yang direkomendasikan tergantung pada aloritma khusus; untuk Blowfish adalah 16 round.

Pembuktian Algoritma Blowfish

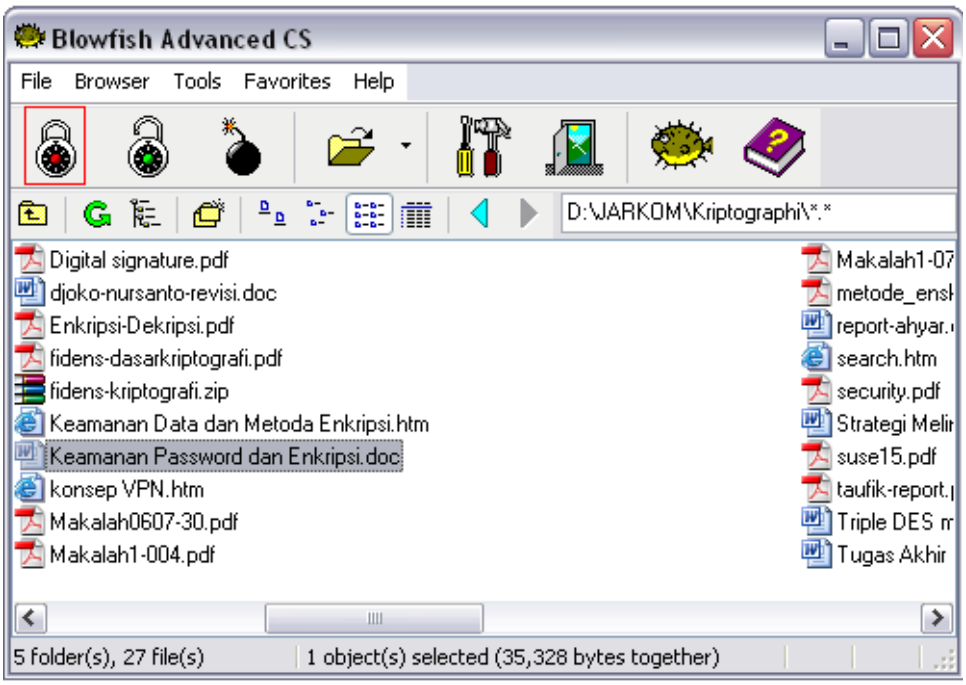
Contoh untuk mengenkripsikan suatu pesan pada file data:

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

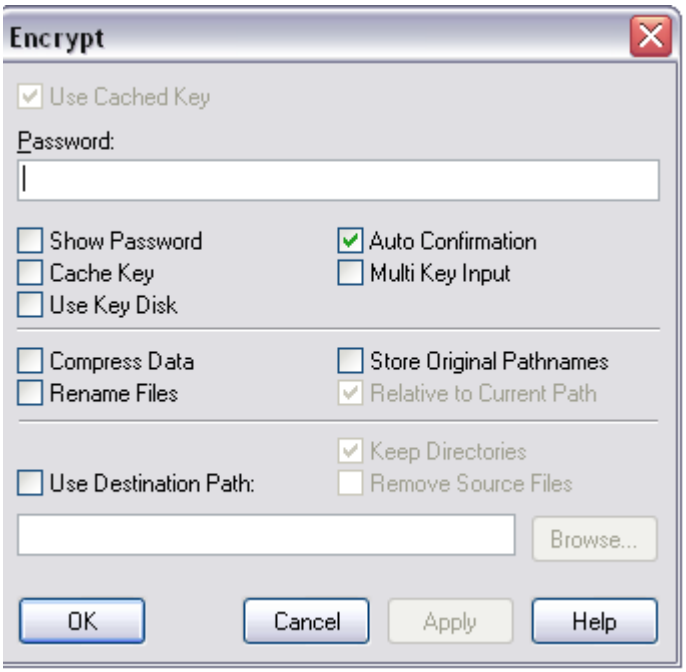


Dari gambar diatas saya memilih untuk meng-enkripsikan file ”Keamanan Password dan Enkripsi”

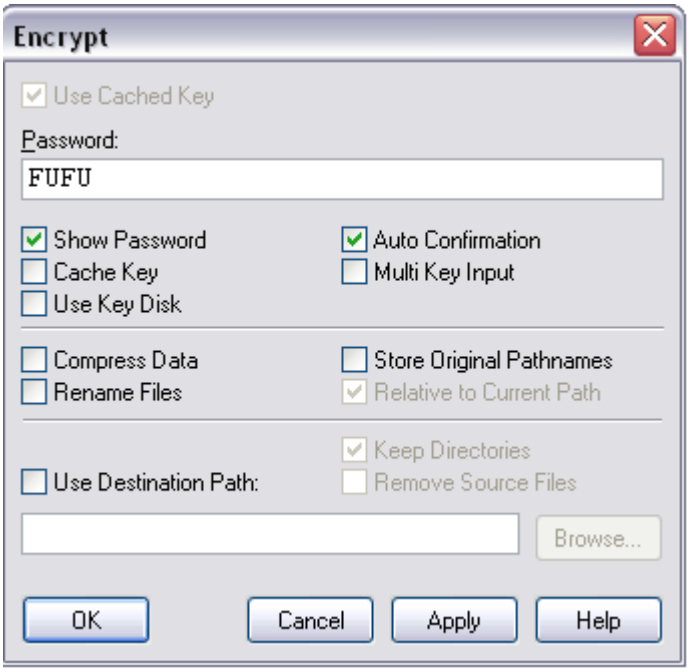
3. Lalu klik gambar kunci yang tertutup



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

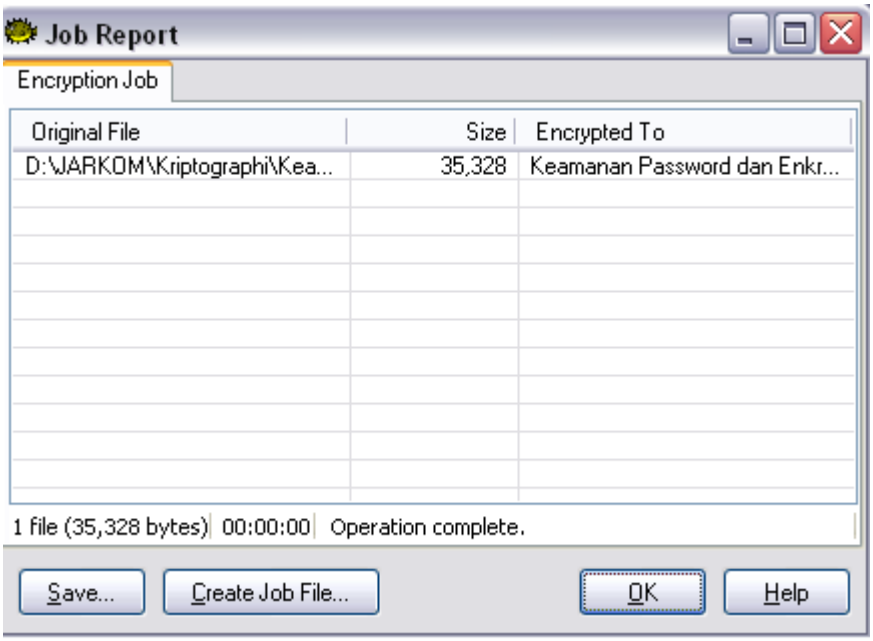


5. Lalu masukkan passwordnya kemudian klik OK

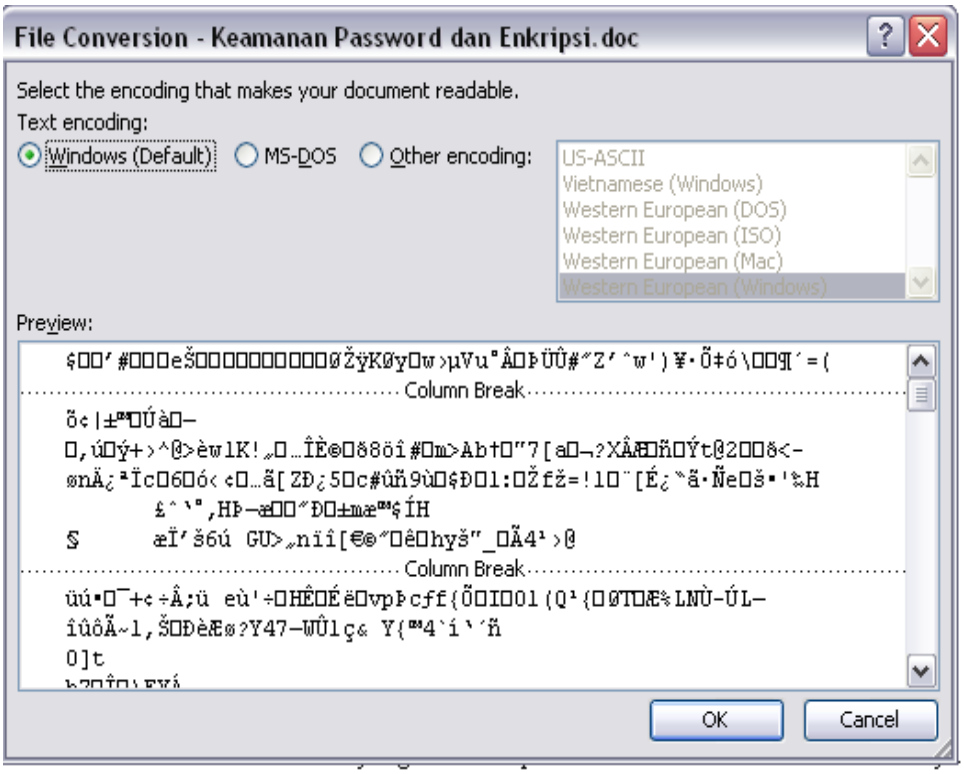


6. Lalu akan keluar tampilan seperti dibawah ini, lalu klik yes

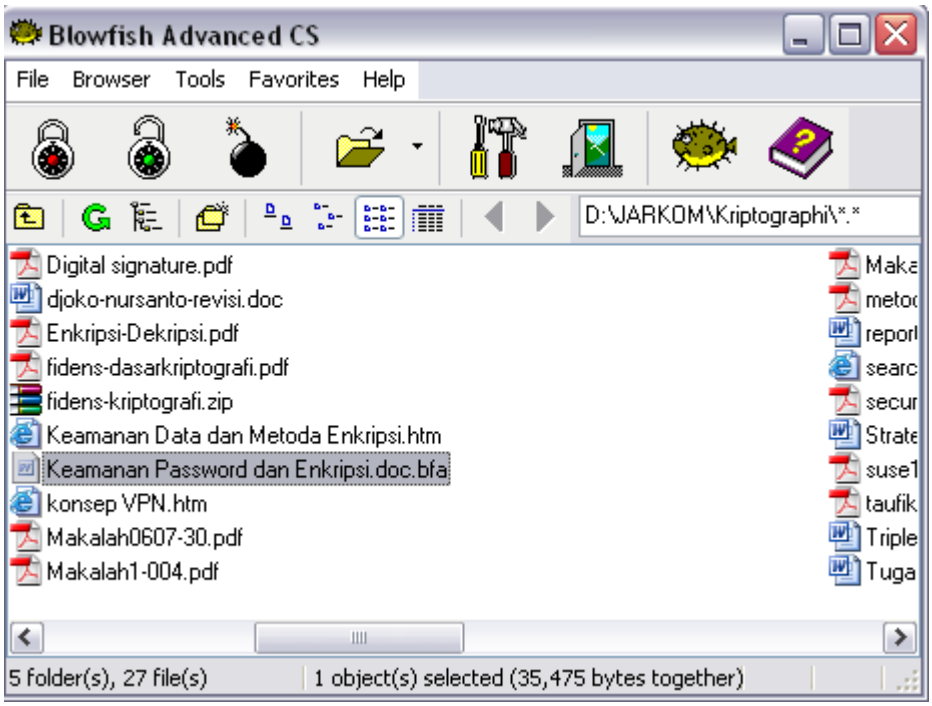
7. Setelah klik yes maka akan keluar tampilan kembali sepeti di bawah ini dan klik OK



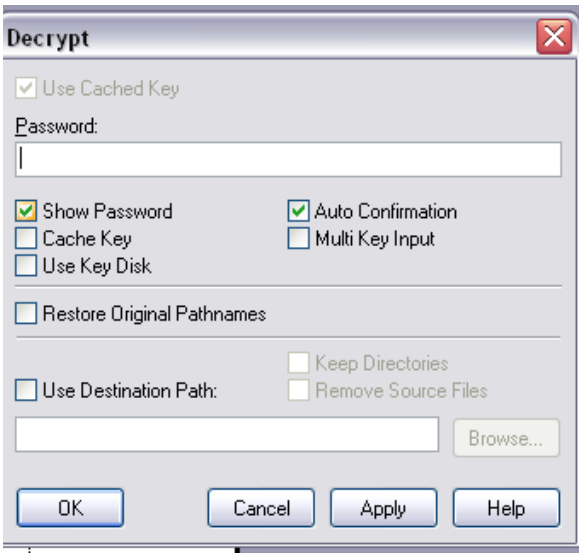
8. Secara otomatis file yang kita enkripdi tadi akan tidak bisa di baca datanya oleh orang lain.
9. Untuk membuktikannya kita buka file tadi lalu lihat apakah yang terjadi pada file tersebut



10. 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.
11. Untuk membuka kembali datanya kita buka kembali toolsnya lalu kita klik tanda kunci yang terbuka

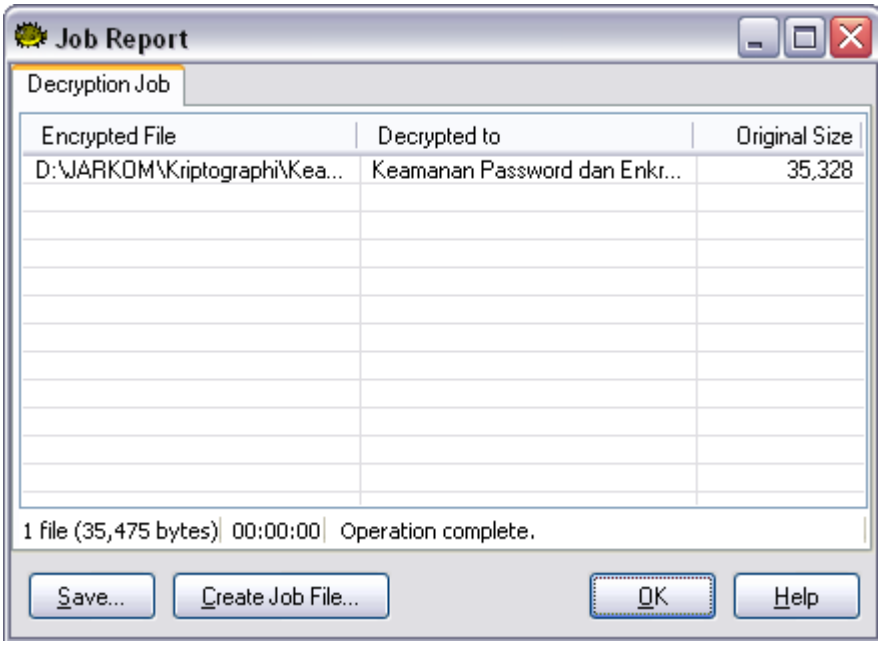


12. masukkan kembali password kita yang tadi lalu kllik OK, dan pasword tadi jangan sampai lupa. Apabila hal tersebut terjadi maka file tersebut tidak akan pernah bisa dibaca kembali.



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

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



15. Maka secara otomatis file yang telah di enkripsi tadi telah berubah menjadi seperti semula sebelum di enkripsi, atau kembali lagi menjadi plaintexs.
16. 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.