Nama : Moch Yusuf Kurniawan
Nim : 1310651067
Kelas :A

1. Domain 5: Cryptography

Cryptography adalah menulis pesan rahasia dimana ini komunikasi yang aman yang dapat dipahami oleh satu tujuan saja atau sang penerima pesan saja .

dimana pesan tersebut harus di enskripsi terlebih dahulu dan bila kita ingin mengetahui pesan aslinya maka kita harus mendeskripsikannya dulu.

Istilah dan Arti:

Ciphertext :Teks yang sudah dienkripsi dari aslinya

Cryptanalysis : Ilmu (dan seni) untuk mengembalikan informasi dari ciphertext tanpa diketahui kunci sebelumnya

Cryptography: Ilmu mengenai pengubahan (enciphering) dan pengembalian (deciphering) dari pesan ke dalam kode rahasia atau cipher.

Cryptosystem: Sebuah sistem yang digunakan untuk mengubah informasi

Decryprion : Proses untuk mengembalikan cipher ke plaintext

Enkripsi : Proses untuk mengubah plaintext ke cipher

Key : Kunci atau informasi rahasia yang diketahui oleh Pengirim atau Penerima untuk membuka plaintext

Monoalphabetic Substitution :Sebuah metode enkripsi di mana huruf dalam plaintext selalu diubah dengan huruf yang sama di dalam ciphertext

Plaintext : Sumber informasi (informasi asli) yang akan diamankan

Polyalphabetic Substitution : Sebuah metode enkripsi di mana huruf dalam plaintext tidak selalu diubah dengan huruf yang sama di dalam ciphertext

Substitution and permutation

Cryptographic substitution adalah pergantian pesan yang rahasia sedangkan permutation adalah penataan kembali / penyusunan kembali pada suatu pesan yang akan di kirim agar tidak diketahui oleh orang lain.

Jenis Cryptographic Ada 3 jenis dari enkripsi yang modern: simetris, asimetris, dan hashing.

Enkripsi simetris ini hanya menggunakan satu kunci: dari enskripsi dan deskripsi hanya menggunakan 1 kunci saja (kunci yang sama)

Nama : Moch Yusuf Kurniawan
Nim : 1310651067
Kelas :A

asymmetric cryptography adalah algoritma yang menggunakan kunci berbeda untuk proses enkripsi dan dekripsinya. Kunci enkripsi biasanya dapat disebarkan kepada umum dan dinamakan sebagai kunci publik (public key) sedangkan kunci dekripsi disimpan untuk digunakan sendiri dan dinamakan sebagai kunci pribadi (private key). Oleh karena itulah, Kriptografi ini dikenal pula dengan nama Kriptografi kunci publik (public key cryptography).

hashing adalah : kriptografi satu arah saja .

Symmetric Encryption : key untuk enkripsi sama dengan key untuk dekripsi

Asymmetric Encryption : key untuk enkripsi berbeda dengan key untuk dekripsi

Hash Functions merupakan sebuah algoritma yang mengubah text atau message menjadi sederetan karakter acak yang memiliki jumlah karakter yang sama. Hash juga termasuk salah satu bentuk teknik kriptografi dan dikategorikan sebagai kriptografi tanpa key (unkeyed cryptosystem). Selain itu hash memiliki nama lain yang juga dikenal luas yaitu “one-way function”.

Kita sering sekali menjumpai hash di website-website yang menyediakan layanan untuk download file ataupun program secara resmi. Hash memang umumnya digunakan untuk mengecek integritas dari sebuah pesan atau file. File atau pesan yang sudah berubah akan memiliki nilai hash yang berbeda.

MD5 adalah sebuah pesan algoritma yang sudah terenskripsi

macam – macam serangan kriptografi :

-Known plaintext

-Brute force

-Meet-in-the-middle attack

-Known key

-Differential cryptanalysis

-Linear cryptanalysis

-Side-channel attacks

-Chosen plaintext and adaptive-chosen plaintext

-Chosen ciphertext and adaptive-chosen ciphertext

Nama : Moch Yusuf Kurniawan
Nim : 1310651067
Kelas :A

Digital signature merupaakn sistem keamanan kriptografi simetris (symetric crypthography/secret key crypthography) atau public key cryptography system yang dikenal sebagai kriptografi simetris, menggunakan kunci yang sama dalam melakukan enkripsi dan dekripsi terhadap suatu pesan (message), disini pengirim dan penerima menggunakan kunci yang sama sehingga mereka harus menjaga kerahasian (secret) terhadap kuci tersebut. Salah satu algoritma yang terkenal dalam kriptografi simetris ini adalah Data Encryption stkitard (DES) yang bertujuan untuk memastikan otentisitas dari dokumen tersebut. Suatu digital signature sebenarnya bukan tkita tangan biasa, tapi tkita tangan dengan menggunakan cara yang berbeda untuk menkitai suatu dokumen sehingga dokumen atau data tidak mengidentifikasi dari pengirim, namuni juga memastikan keutuhan dari dokumen tersebut tidak berubah selama proses transmisi, digital signature didasarkan dari isi dari pesan itu sendir

2. STEGANOGRAFI DENGAN SOFTWARE OPEN PUFF

Andi akan mengirimkan suatu pesan rahasia pada manda tapi dia mengenskripsi pesan tersebut agar tidak ada orang yang mengetahui pesan tersebut . tetapi sebelumnya dya sudah mengirim password atau kunci untuk membuka pesan tersebut . agar tidak ada orang yang bisa membua pesan tersebut .

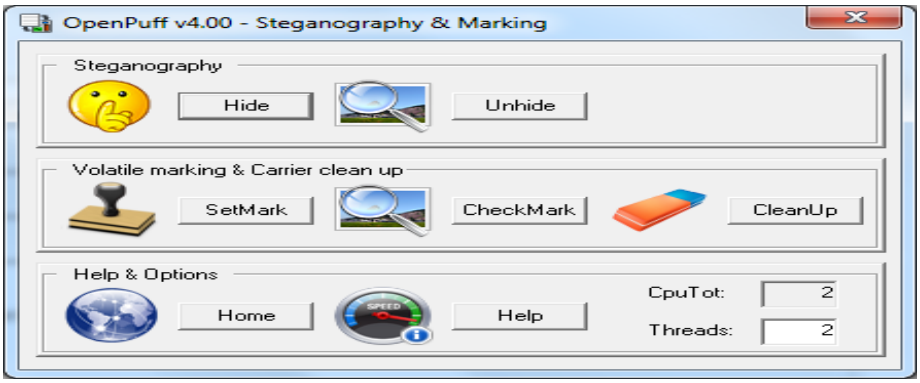
Kasus ini adalah tentang pengiriman pesan yang disisipkan pada sebuah data yang tidak di ketahui bahwa data tersebut telah di sisipkan pesan penting , untuk dikirimkan pada seseorang .

Pada kasus steganografi ini filenya akan di buka menggunakan open puff .

membukanya menggunakan pasword yang sama atau menggunakan kunci yang sama .

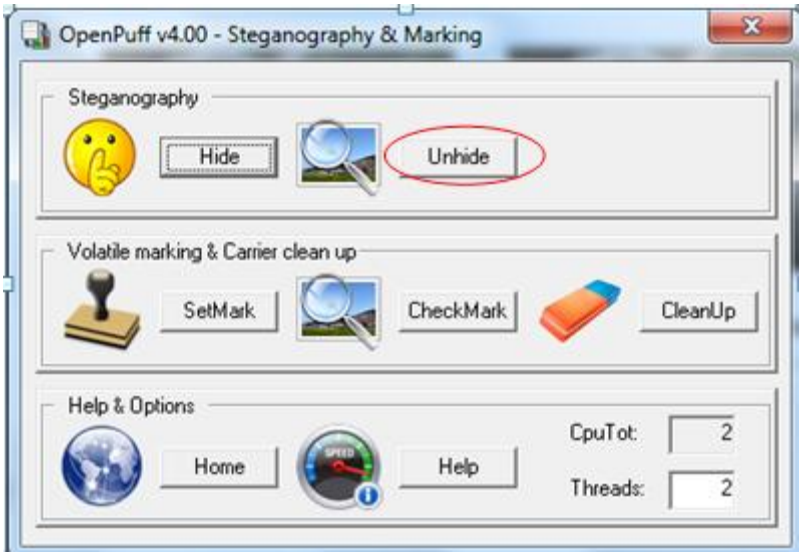
cara penggunaannya sebagai berikut :

* pertama kita buka software open puff terlebih dahulu .

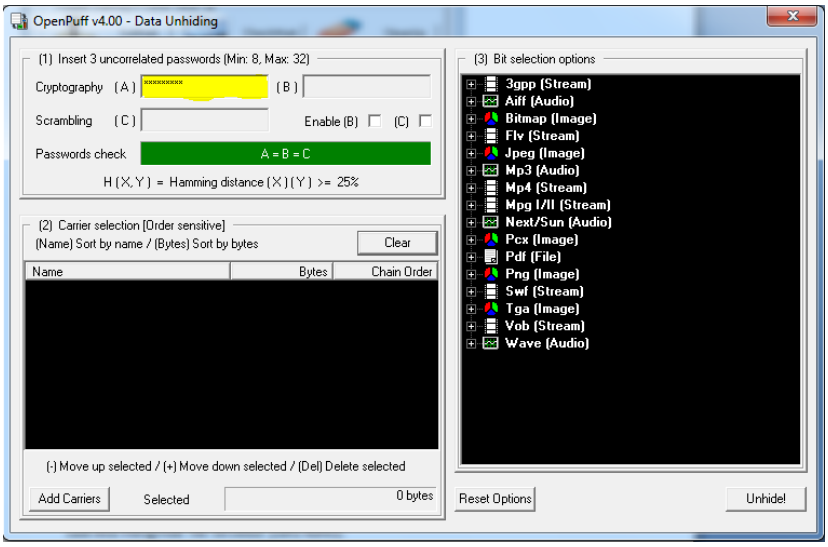


Nama : Moch Yusuf Kurniawan
Nim : 1310651067
Kelas :A

- langkah pertama kita klik ***Unhide*** seperti gambar di bawah .

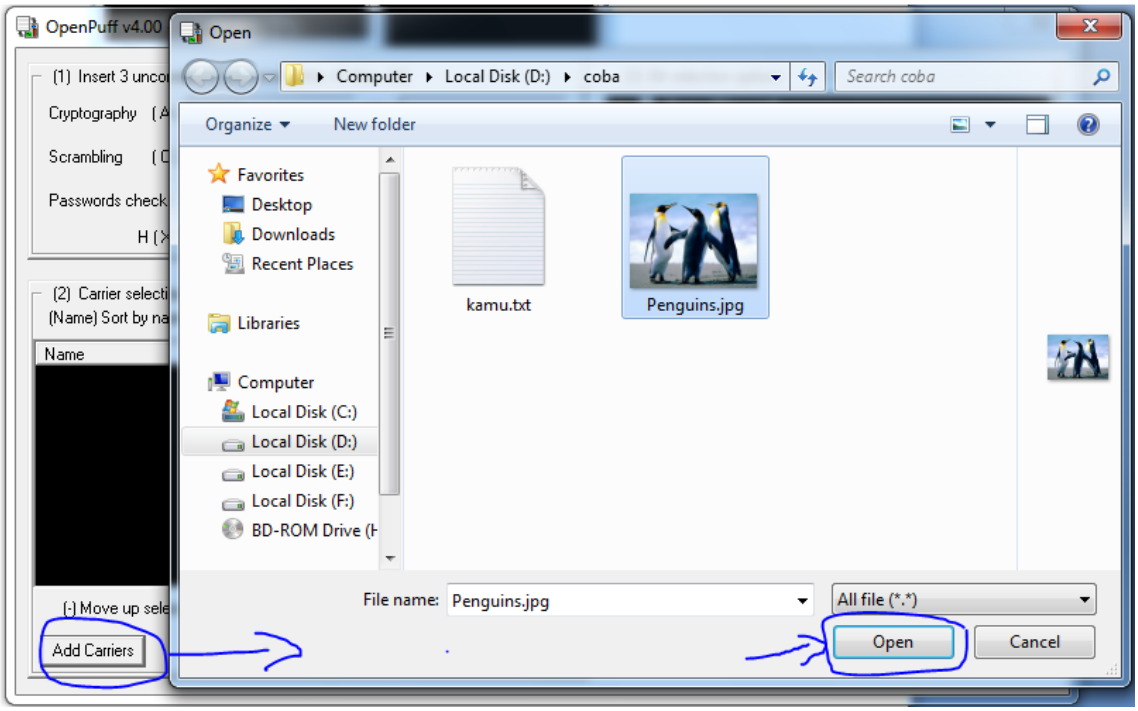


- selanjutnya masukkan password , dimana password tersebut sama dengan password saat kita mengHide file tersebut (satu kunci).

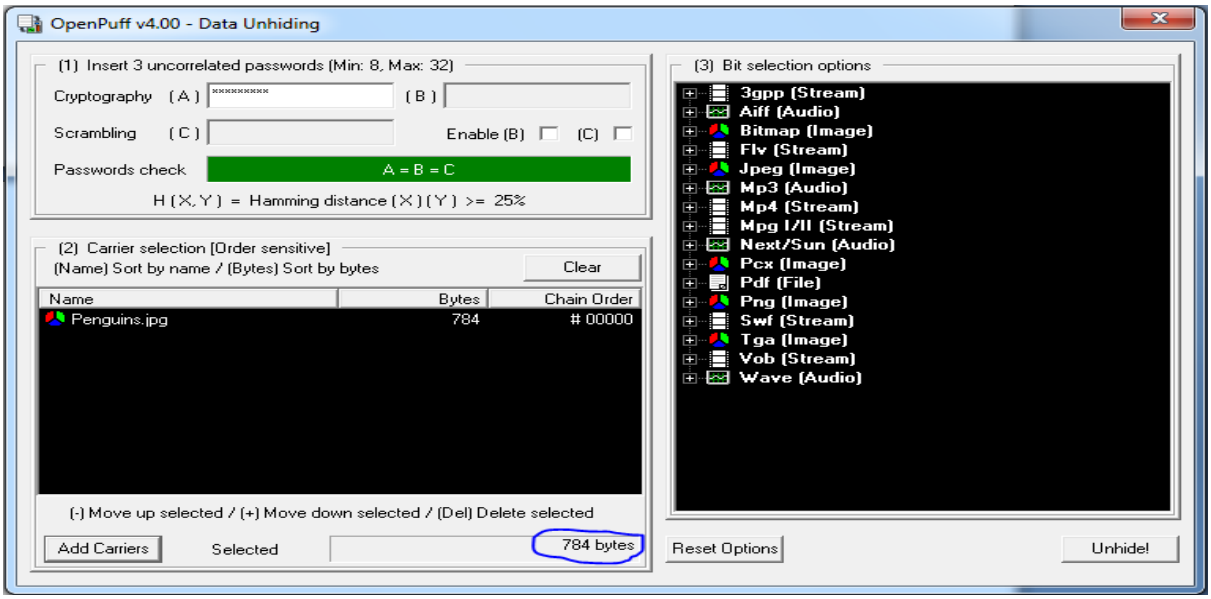


Nama : Moch Yusuf Kurniawan
Nim : 1310651067
Kelas :A

- Selanjutnya upload file yang menjadi file pengangkut/pembawa file penting tadi . Klik add carrier dan cari file pembawa .

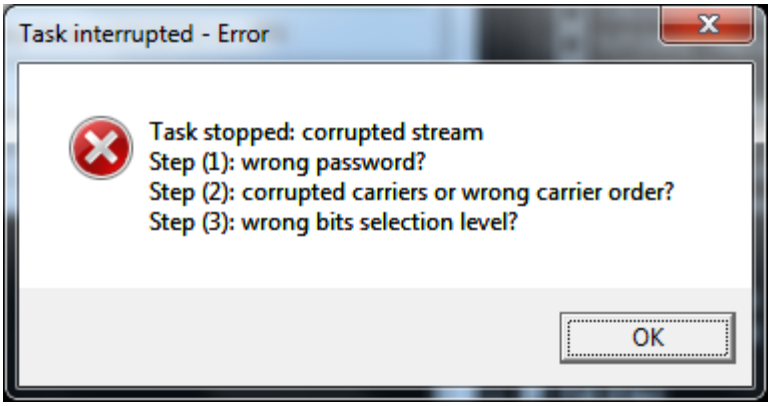


- Setelah itu maka tampilan akan seperti gambar dibawah ini. Dan dapat diketahui juga file tersebut masih sama terdapat informasi file tersebut dapat mengangkut file sebesar 784 bytes.

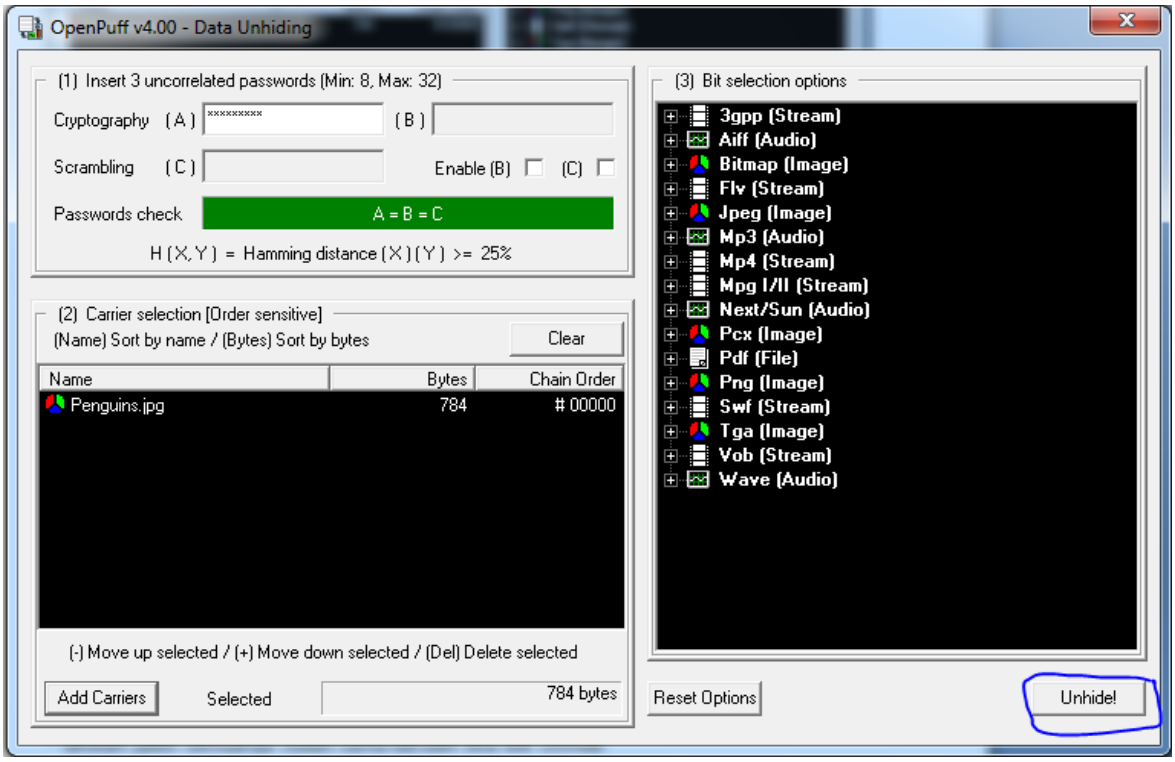


Nama : Moch Yusuf Kurniawan
Nim : 1310651067
Kelas :A

- Sebelum kita klik unhide pastikan bahwa password, file pembawa, dan bit selection levels nya sama dengan saat hiding information. Jika dari kesemuanya itu tidak sama maka tidak akan bisa melakukan unhide. Seperti tampilan gambar dibawah ini.

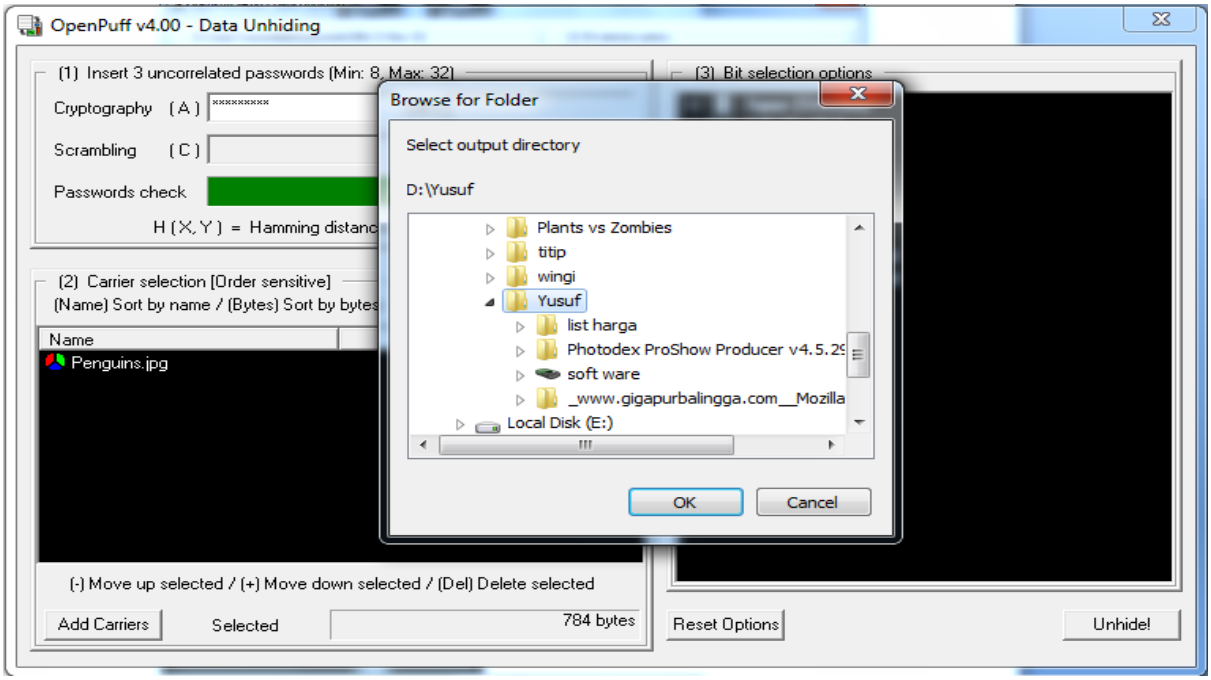


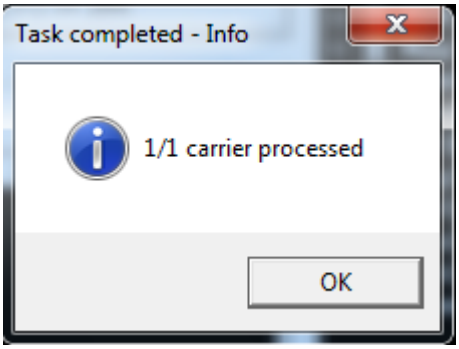
* Setelah yakin semuanya sudah sama barulah kita klik UnHide

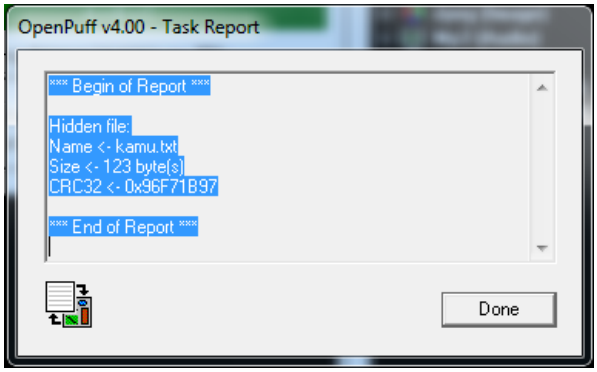


Nama : Moch Yusuf Kurniawan
Nim : 1310651067
Kelas :A

setelah itu kita pilih lokasi file tersebut akan di keluarkan seperti gambar di bawah.







- Setelah berhasil, file pesan yang tadinya terlebur dengan file pembawa dengan melakukan proses unhide information maka file pesan tersebut akan berpisah dengan file pembawanya. Tampilan dibawah ini merupakan file pesan setelah dipisahkan dari file pembawanya .