

Nama : Moh. Samsul Huda

Nim : 1310651199

Kelas : A

Soal 1

Resume Domain 5 : Cryptography “Kriptografi”

Kriptografi yaitu menulis sebuah pesan rahasia, ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak. Agar pesan tidak terbaca, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain

Dalam kriptografi ada Confidentiality, integrity, authentication, and nonrepudiation

1. Kerahasiaan (confidentiality), yaitu menjaga supaya pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak,
2. Integritas data (data integrity), yaitu memberikan jaminan bahwa untuk tiap bagian pesan tidak akan mengalami perubahan dari saat data dibuat/dikirim oleh pengirim sampai dengan saat data tersebut dibuka oleh penerima data,
3. Otentikasi (authentication), yaitu berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi maupun mengidentifikasi kebenaran sumber pesan,
4. Nirpenyangkalan (non repudiation), yaitu memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang tertentu sehingga apabila ada seseorang yang mencoba mengakui memiliki dokumen tersebut, dapat dibuktikan kebenarannya dari pengakuan orang tersebut.

Ada tiga jenis dari enkripsi yang modern: symmetric, asymmetric, and Hashing :

Algoritma Kriptografi Simetris adalah teknik yang tertua dan paling terkenal. Kunci rahasia, yang dapat nomor, kata, atau hanya string acak huruf, diterapkan untuk teks pesan untuk mengubah konten dengan cara tertentu. Ini mungkin yang sederhana seperti pergeseran setiap huruf oleh sejumlah tempat dalam abjad. Selama pengirim dan penerima tahu kunci rahasia, mereka dapat mengenkripsi dan mendekripsi pesan semua yang menggunakan kunci ini.

Dalam symmetric ada 2 kategori :

1. Cipher aliran (stream cipher)
Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk bit tunggal yang dalam hal ini rangkaian bit dienkripsikan/didekripsikan bit per bit. Cipher aliran mengenkripsi satu bit setiap kali.
2. Cipher blok (block cipher)
Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk blok bit, yang dalam hal ini rangkaian bit dibagi menjadi blokblok bit yang panjangnya sudah ditentukan sebelumnya. Cipher blok mengenkripsi satu blok bit setiap kali.

Enkripsi asimetris adalah dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan dua kunci yakni kunci publik (public key) dan kunci privat (private key). Kunci publik disebar secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan.

Pada umumnya kunci publik (public key) digunakan sebagai kunci enkripsi sementara kunci privat (private key) digunakan sebagai kunci dekripsi.

Hashing adalah 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” transformasi kriptografi satu arah menggunakan algoritma. Fungsi hash tidak butuh kunci dan sifatnya hanya satu arah, yaitu dari teks masukan menjadi nilai hash yang panjangnya selalu sama. Setelah menjadi nilai hash, tidak ada fungsi yang bisa mengembalikan nilai hash itu menjadi teks semula.

MD5 (Message Digest algorithm 5) adalah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. Pada standart Internet (RFC 1321), MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan, dan MD5 juga umum digunakan untuk melakukan pengujian integritas sebuah berkas.

Beberapa istilah dari kriptografi

- Plaintext adalah pesan yang hendak dikirimkan (berisi data asli).
- Ciphertext adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
- Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.
- Enkripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode (pesan) dari yang bisa dimengerti (plaintexts) menjadi sebuah kode yang tidak bisa dimengerti (ciphertexts).
- Dekripsi adalah proses merubah ciphertexts menjadi plaintexts disebut. Proses enkripsi dan dekripsi memerlukan suatu mekanisme dan kunci tertentu.
- Cipher adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi (Schneier, 1996).
- Kriptanalisis (cryptanalysis) adalah kebalikan dari kriptografi, yaitu suatu ilmu untuk memecahkan mekanisme kriptografi dengan cara mendapatkan kunci dari ciphertexts yang digunakan untuk mendapatkan plaintexts.
- Kriptologi (cryptology) adalah ilmu yang mencakup kriptografi dan kriptanalisis.

Implementasi dari kriptografi

Contohnya pada Digital Signature

Digital signature merupakan 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 kerahasiaan (secret) terhadap kunci 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 tanda tangan biasa, tapi tanda tangan dengan menggunakan cara yang berbeda untuk menandai suatu dokumen sehingga dokumen atau data tidak mengidentifikasi dari pengirim, namun juga memastikan keutuhan dari dokumen tersebut tidak berubah selama proses transmisi, digital signature didasarkan dari isi dari pesan itu sendiri.

Soal 2

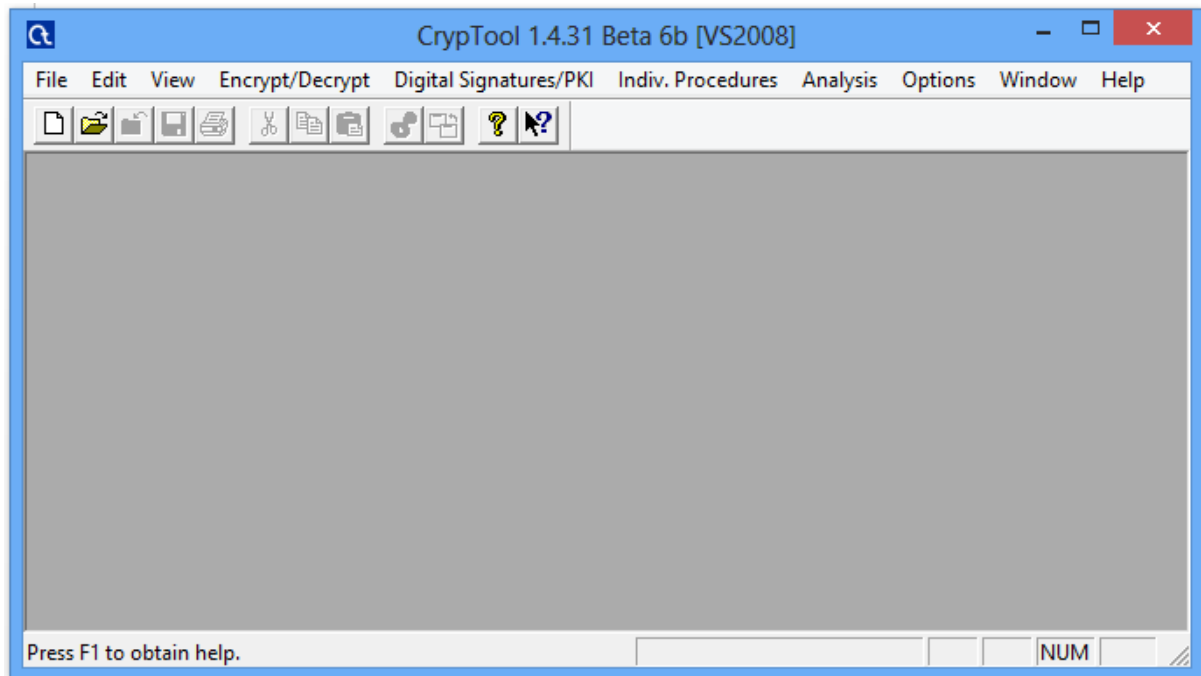
Implementasi Enkripsi Menggunakan sebuah software CrypTool

Kasusnya disini mengubah sebuah text / pesan penting sehingga pesan tersebut tidak bisa dibaca dengan bahasa manusia. Contohnya :

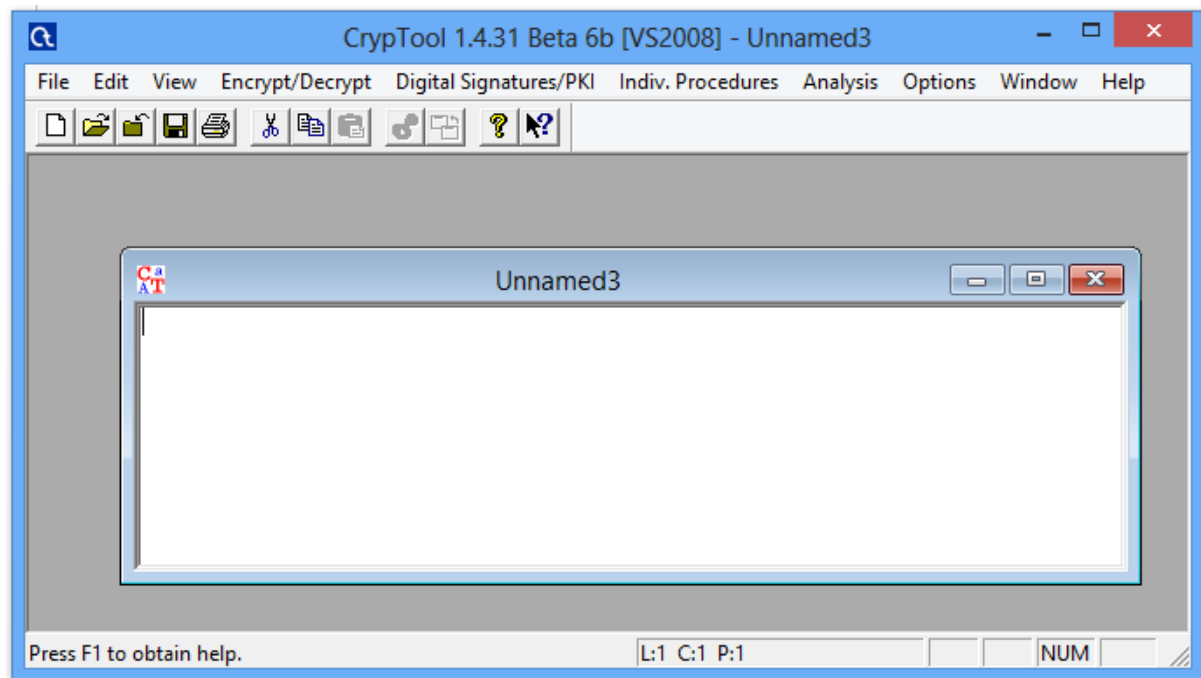
Pertama kita harus punya Software tersebut, Cryptool,
Lalu kita jalankan



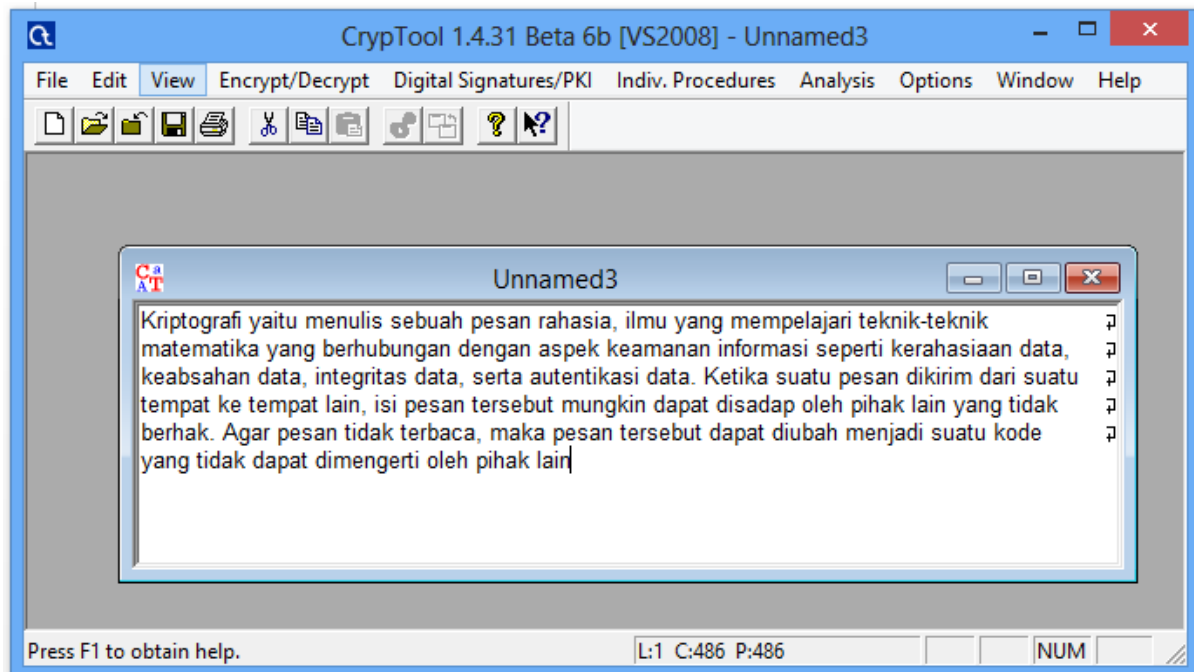
Dan akan muncul tampilan pertama



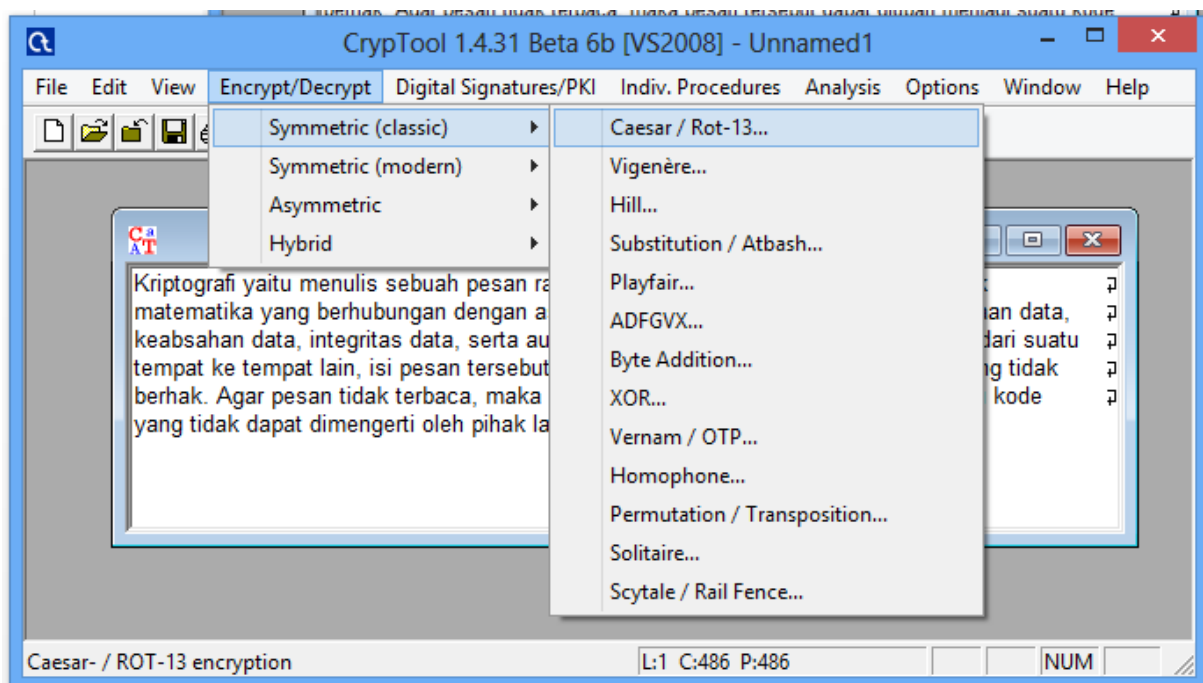
Setelah itu kita klik Menu New diatas / CTRL + N



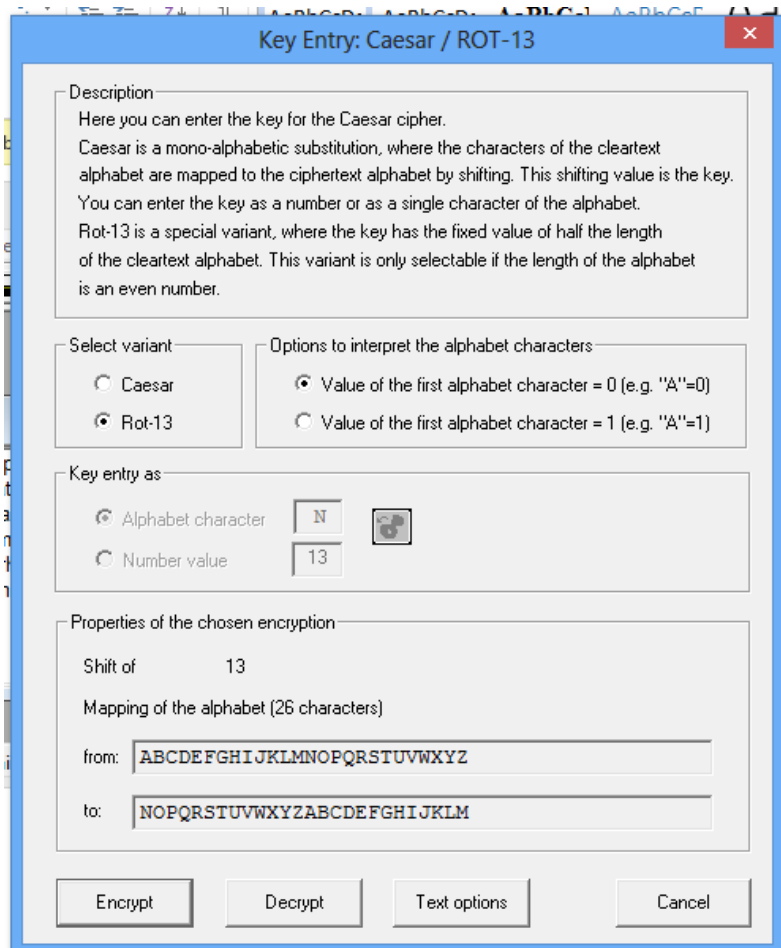
Setelah itu kita ketik pesan tersebut,



Dan kemudian kita klik Menu Encrypt/Decrypt, pilih Symmetric (classic), klik Caesar /Rot-13..

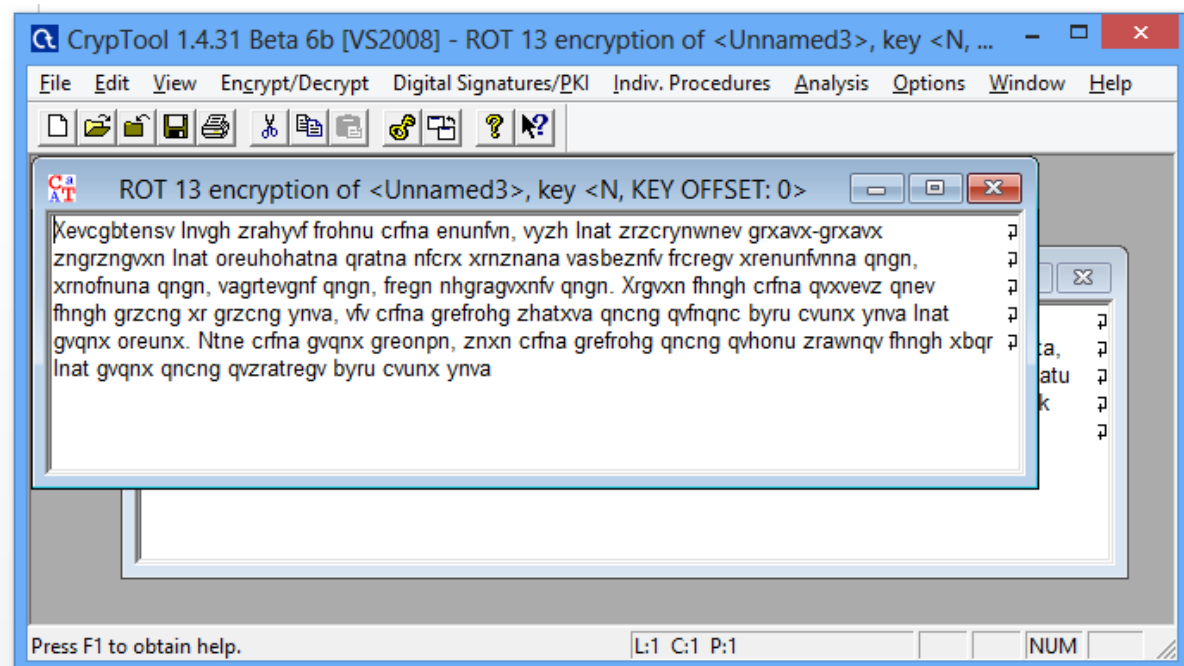


Dan muncul tampilan seperti ini

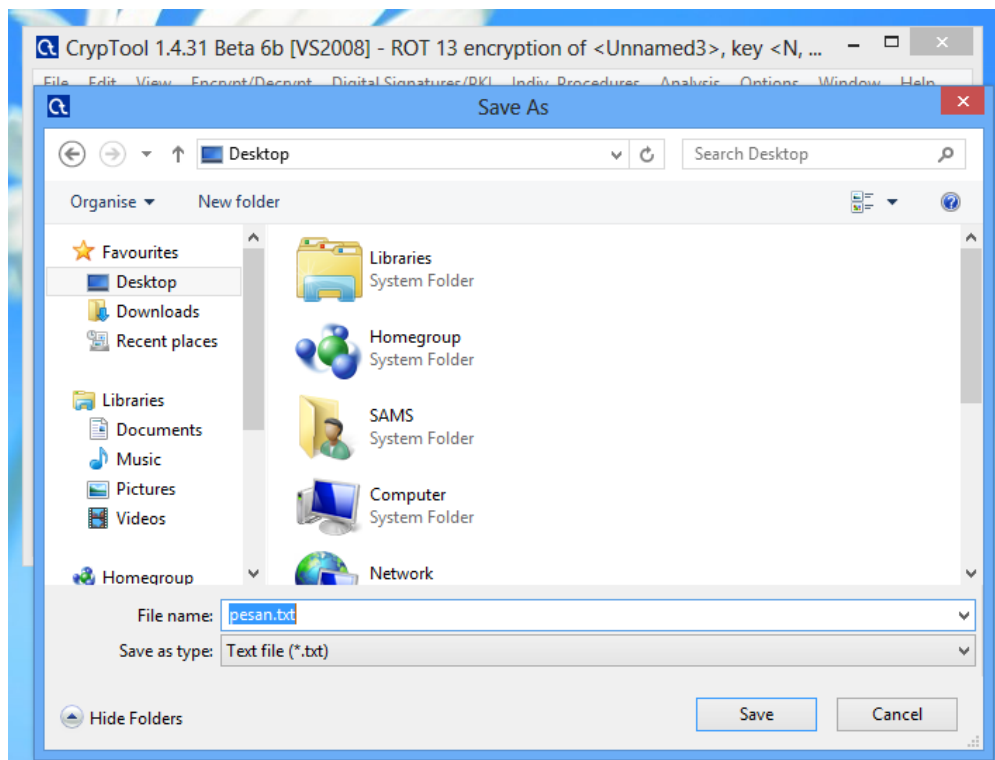


The dialog box is titled "Key Entry: Caesar / ROT-13". It contains a "Description" section explaining the Caesar cipher and ROT-13. Below this, there are two sections: "Select variant" with radio buttons for "Caesar" and "Rot-13" (selected), and "Options to interpret the alphabet characters" with radio buttons for "Value of the first alphabet character = 0 (e.g. 'A'=0)" (selected) and "Value of the first alphabet character = 1 (e.g. 'A'=1)". The "Key entry as" section has radio buttons for "Alphabet character" (selected) and "Number value", with input fields showing "N" and "13" respectively. The "Properties of the chosen encryption" section shows "Shift of 13" and "Mapping of the alphabet (26 characters)" with "from: ABCDEFGHIJKLMNOPQRSTUVWXYZ" and "to: NOPQRSTUVWXYZABCDEFGHIJKLM". At the bottom are buttons for "Encrypt", "Decrypt", "Text options", and "Cancel".

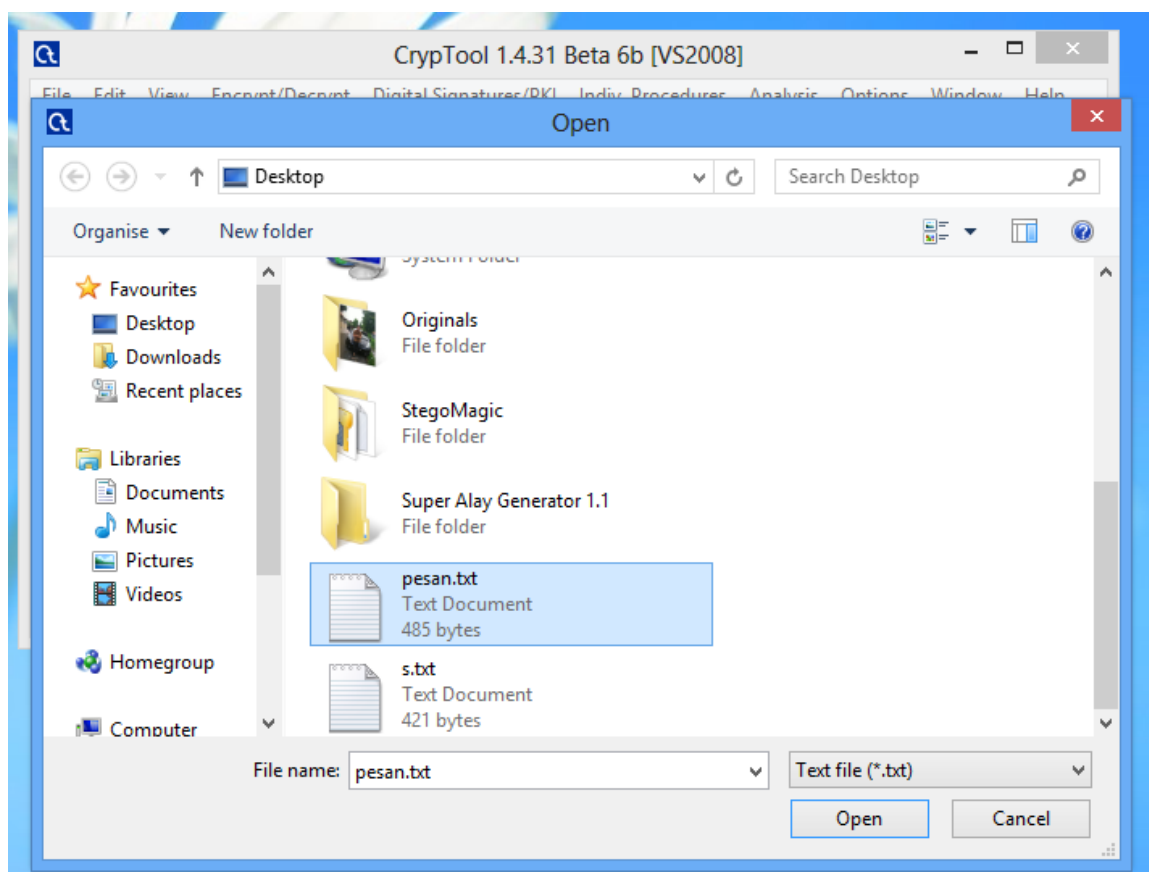
Setelah itu kita pilih Select variant yg Rot-13, lalu klik Encrypt. Dan akan muncul seperti dibawah ini



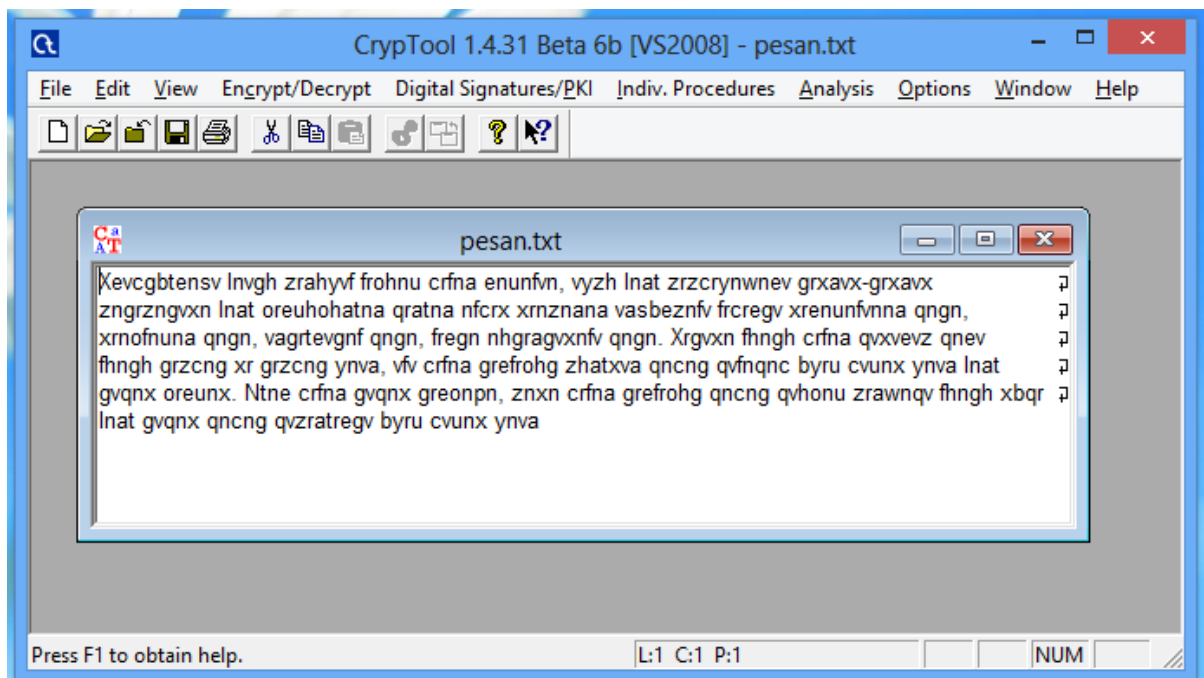
Setelah sudah kita Enkripsi pesan yg tadinya bisa dibaca, sekarang menjadi tulisan tak beraturan / tak bisa dibaca. Kita simpan file tersebut. Klik File Save / CTRL + S



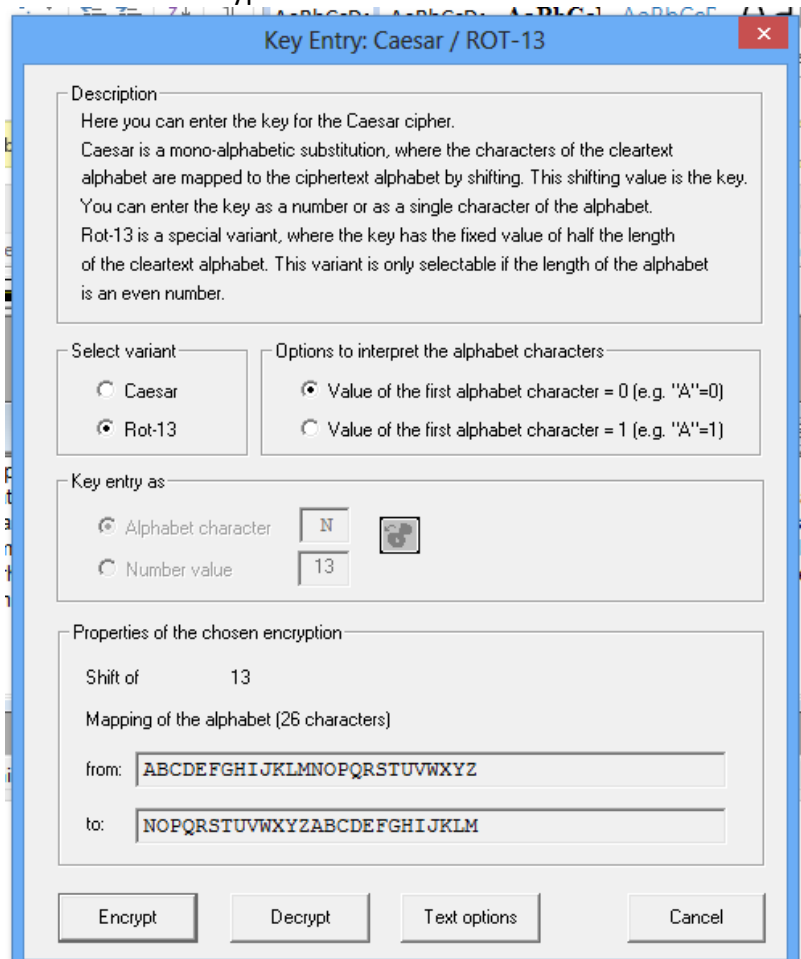
Jika kita mau membuka file tersebut klik File Open / CTRL O



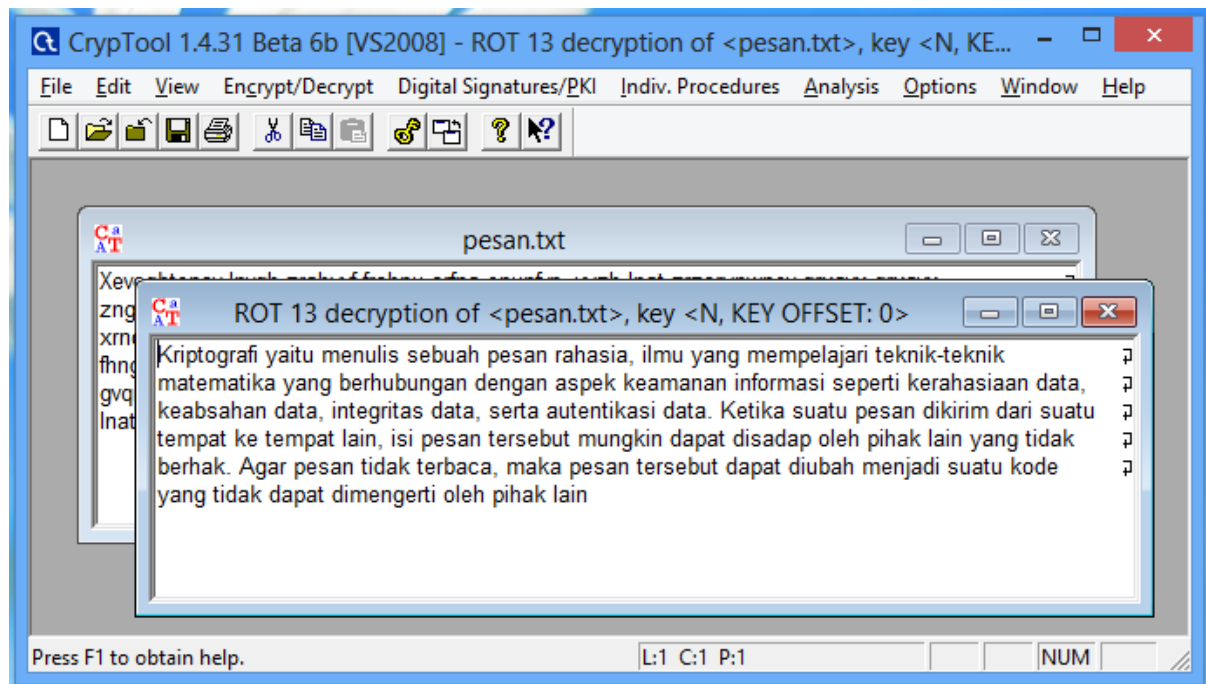
Lalu klik Open, maka akan keluar file yg tadi kita simpan



Dan kita akan mencoba mengembalikan pesan tersebut seperti awal, tahapnya sama seperti kita mau menenkripsi, klik Encrypt/Decrypt, tapi setelah muncul tampilan dibawah, kita klik tombol menu Decrypt



Lalu akan muncul tampilan dibawah, dan pesan yg tadinya tidak bisa dibaca sekarang kembali ke awal.



Analisis

Cryptool adalah software yang berfungsi analisis kriptografi. Fitur yang tersedia disini sudah lumayan lengkap. Bisa dibilang ini Maple-nya Kriptografi.

Cryotool ini sudah sangat lengkap diantaranya :

1. Meliputi banyak algoritma kriptografi klasik dan modern (enkripsi dan dekripsi, pembuatan kunci, password yang aman, otentikasi, protokol yang aman, dll);
2. Visualisasi dari beberapa algoritma (Caesar, Enigma, RSA, Diffie-Hellman, tanda tangan digital, AES, dll);
3. Kriptanalisis dari beberapa algoritma (Vigenère, RSA, AES, dll);
4. Metode pengukuran cryptanalytical(entropi, n-gram, autokorelasi, dll);
5. Didukung dengan tambahan metode (primality tes, faktorisasi, base64 encoding, dll)

Dari percobaan diatas kita ketahui bahwa keamanan dari data penting kita sangatlah penting, untuk menghindari adanya tindak pembobolan pesan yg memang bukan hak dari si pembobol / orang lain.