Nama : Risky Putra Sukaryanto

NIM : 1310651212

Kelas : E

1. Aspek keamanan informasi mempunyai ruang lingkup yang luas. Menurut referensi dari ebook CISSP, ruang lingkup materi dari keamanan informasi terdiri dari 10 pokok permasalahan. Dari 10 pokok permasalahan tersebut, silakan buatlah resume salah satu pokok permasalahan dari keamanan informasi mengacu terhadap ebook CISSP yang sudah saya upload di elearning. Resume bukan hasil translate, melainkan inti-intinya saja dari materi yang sudah Anda pahami pada ebook tersebut. Hasil resume **tidak boleh** sama dengan teman-temannya, akan tetapi tema yang dibahas boleh sama

Cryptography

kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat di kirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari puhk ketiga.

Menurut Bruce sceheiner kriptografi adalah ilmu pengetahuan dan seni menjaga pesan agar tetap aman

Konsep kriptografi telah lama di gunakan oleh manusia misalnya pada peradaban mesir dan romawi walaupun masih sederhana, ada pyula prinsip prinsip kriptografi yaitu

Kerahasiaan yaitu layanan agar isi pesan yang di kirim tetap rahasia dan tidak di ketahui oleh pihak lain kecuali pihak pengirim dan pihak penerima , umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk di baca dan di pahami.

Keutuhan data yaitu layanan yang mampu mengenali atau mendeteksi adanya manipulasi data yang tidak sah oleh pihak lain

Keotentikan yaitu layanan yang berhubungan dengan identifikasi baik otentikasi pihak pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data atau informasi

Anti penyangkalan yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang di lakukan sebelumnya bahwa pesan tersebut berasal darinya.

Berbeda dengan kriptografi klasik yang menikitik beratkan kekuatan pada kerahasiaan algoritma yang digunakan yang atrinya apabila algoritma yang di gnakan telah di ketahui maka pesan sudah pasti akan bocor dan dapat di ketahui isnya oleh siapa saja yang mengetehui algoritma tersebut, Kriptografi modern lebih menitik beratkan pada kerahasiaan kunci yang di gunakan pada algoritma tersebut sehingga algoritma tersebut dapat saja di sebarkan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan bagi para pemakainya.

Ada beberapa istilah yang digunakan dalam bahasa kriptografi

- Plaintext adalah pesan yang hendak di kirimkan yang berisi data murni
- Ciphertext adalah pesan yang terenkripsi atau tersandi yang merupakan hasil enkripsi dengan istilah lain data yang sudah teracak.
- Enkripsi adalah proses pengubahan plaintext menjadi ciphertext.
- Dekripsi adalah kebalikan dari enkripsi yaitu mengubah ciphertext menjadi plaintext.
- Kunci adalah suatu bilangan yang di rahasiakan yang di gunakan untuk memecahkan enkripsi dan dekripsi.

Kriptografi itu sendiri terdiri dari dua proses utama yaitu enkripsi dan dekripsi. Proses enkripsi mengubah plaintext menjadi ciphertext dengan menggunakan kunci tertentu sehingga isi informasi pada pesan tersebut sukar di mengerti.

Peranan kunci sangat penting dalam proses enkripsi dan dekripsi disamping pula algoritma yang di gumakan sehingga kerahasiaan sangatlah penting apabila kerahasiaannya terbongkat maka isi dari pesan dapat di ketahui.

Secara sistematis proses enkripsi merupakan pengoprasian fungsi enkripsi menggunakan kunci enkripsi pada plaintext sehingga dihasilkan cipertext .

Notasinta:

$E_e(M) - C$

Sedangkan proses dekripsi merupakan pengoprasian fungsi(D) dekripsi menggunakan kunci dekripsi pada (C) ciphertex sehingga dihasilkan plaintext

Notasinya:

$D_d(C) = M$

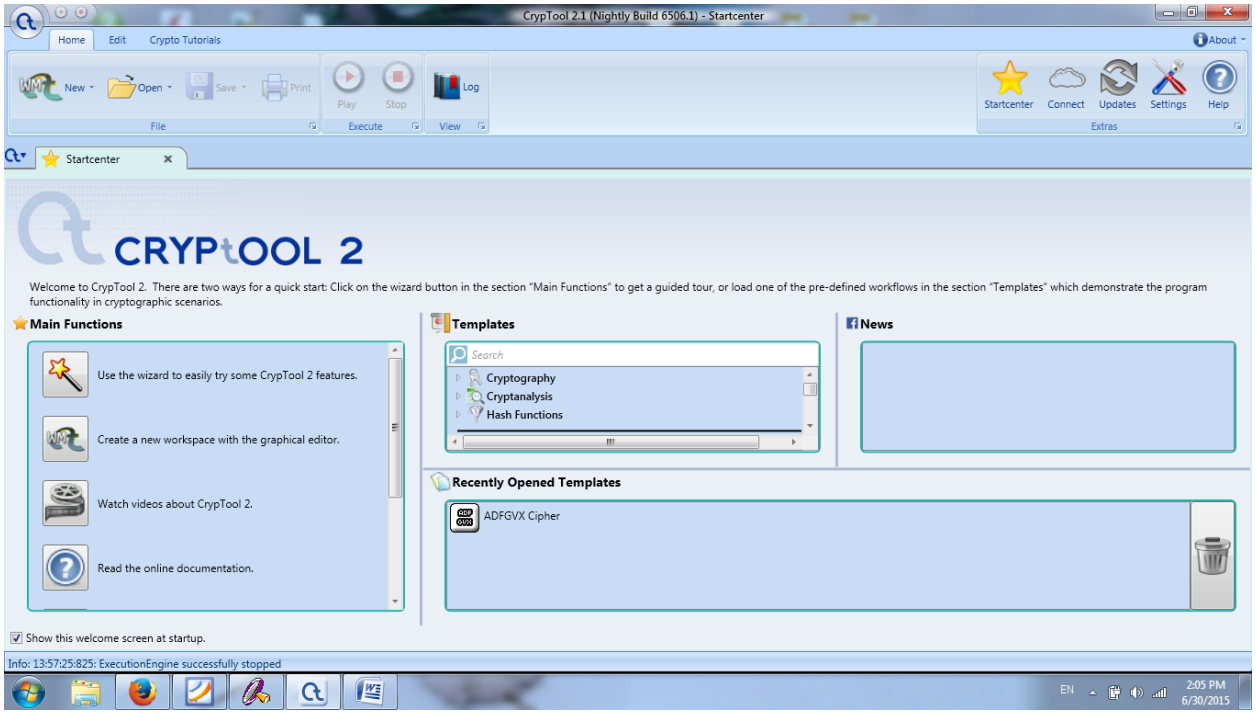
Sehingga dari dua hubungan diatas berlaku

$D_d(E_e(M)) = M$

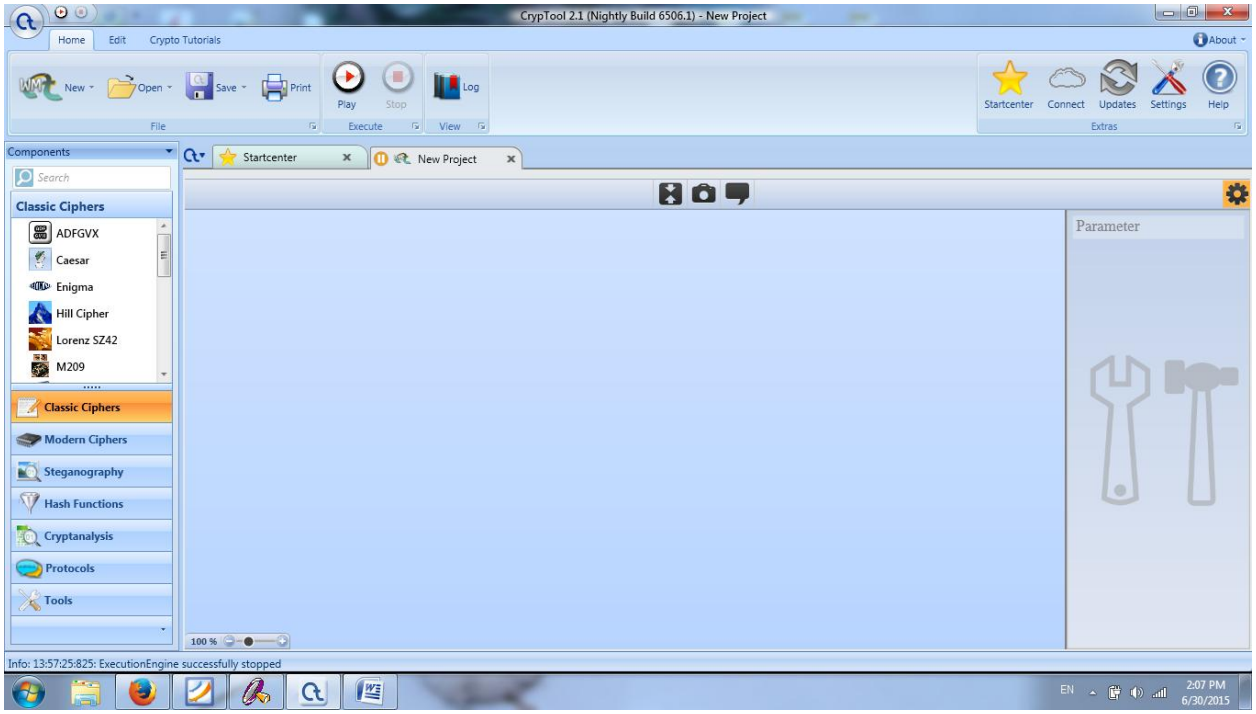
2. Cari software atau tools pendukung keamanan informasi kemudian cobalah fungsional software tersebut untuk menangani kasus tertentu. Buatlah step by step yang terdiri dari screenshot, keterangan gambar, dan analisis. Misalnya penggunaan wireshark dalam melakukan analisis paket data jaringan (pcap file), penggunaan ftk forensic untuk mengetahui file steganografi, dan lain sebagainya. Review software boleh sama, akan tetapi kasusnya harus berbeda dengan temen-temennya.

❖ *Merubah kriptografi Enkripsi dan Dekripsi dengan menggunakan CRYPTOOL*

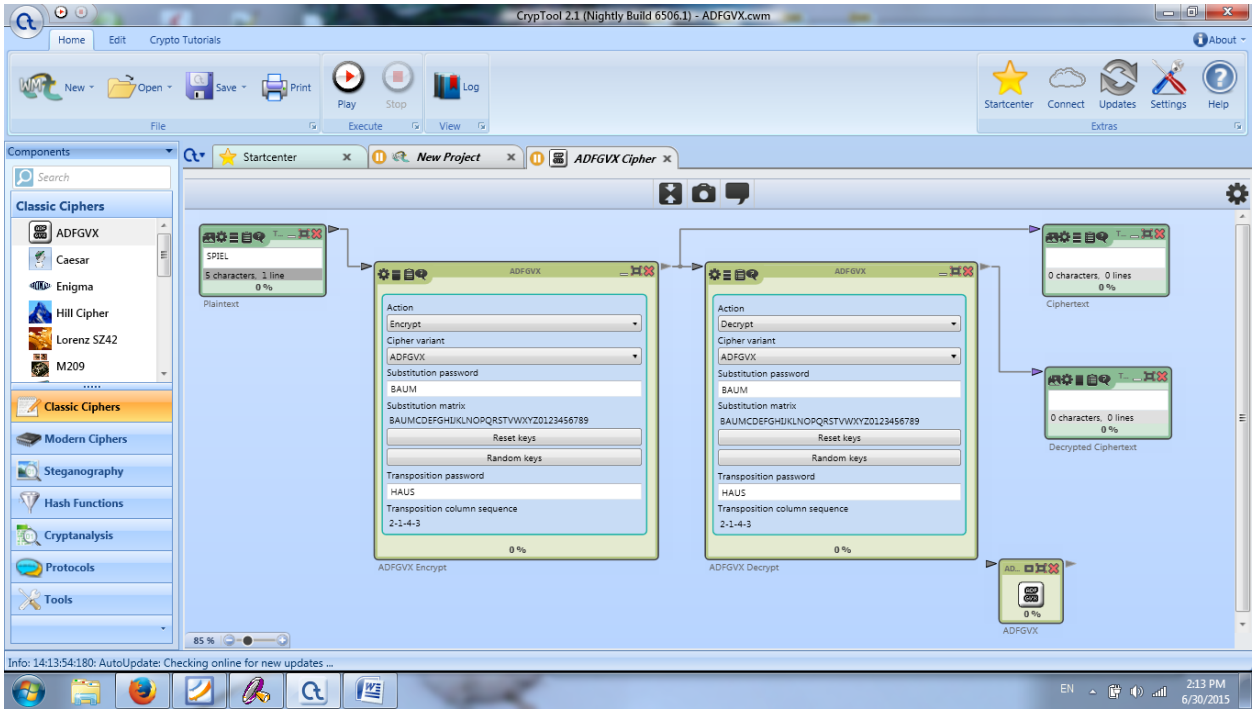
- Langkah pertama yaitu kita instal terlebih dahulu aplikasi cryptoll
- Setelah aplikasi terpasang kita jalankan aplikasinya



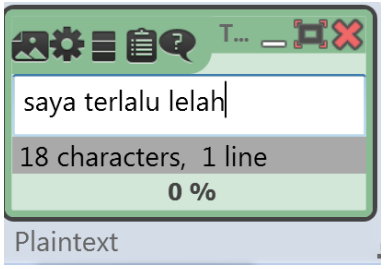
- Stelah itu kita pilih New untuk membuat projek baru
- Setelah itu pilih menu Classic Ciphers



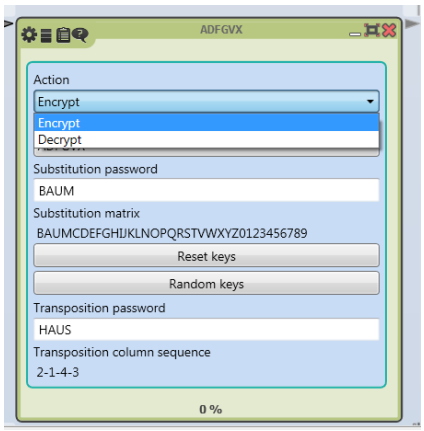
- Setelah memilih classic ciphers kemudian pilih ADFGVX pada nemu classic ciphers



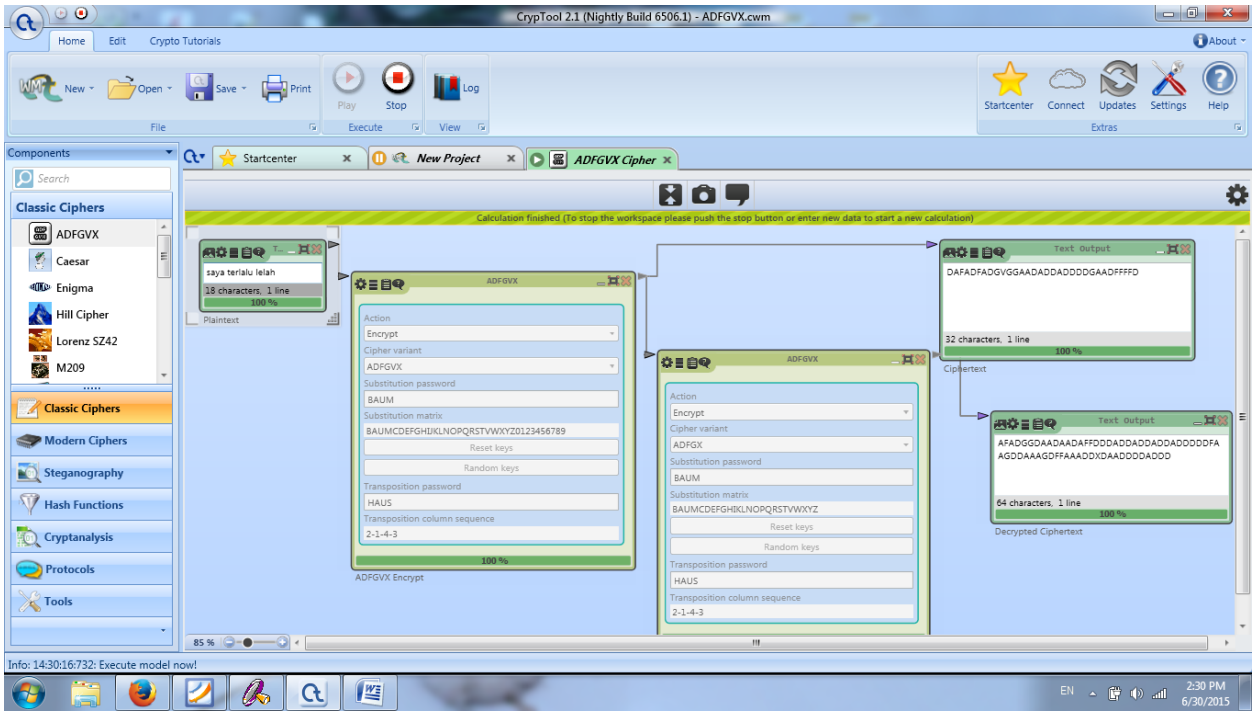
- Dan akhirnya muncul fom fom tersebut
- Kemudia isi fom tersebut dengan plaintext yang akan di rubah



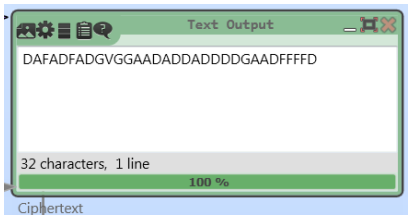
- Pilih menu action sesuai dengan kebutuhan antara enkripsi dan dekripsi



- Kalau semua sudah pas maka kita Play



- Maka hasil akan di dapat pada fom text Output



- Plaintext= “saya terlalu lelah” setelah di rubah menjadi chipertext=”DAFADFADGVGGAADADDADDDDGAADFFFFD”