**LaporaN KEMANAN KOMPUTER**

**kriptografi**

****

**Disusun Oleh :**

ERIK SAIFUL RIZAL (1300631030)

**Program studi manajemen informatika d3**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH JEMBER**

**2015**

DASAR TEORI

Kriptografi menyebabkan timbulnya kriptanalisis, yaitu ilmu pengetahuan dan seni untuk membongkar data acak. Praktisi dari kriptanalisis disebut kriptanalis. Kriptanalis berkembang sejalan dengan kriptografi. Setiap ada algoritma kriptografi baru yang dibuat oleh kriptografer, langsung diikuti oleh adanya upaya percobaan kriptanalisis. Percobaan kriptanalisis ini disebut attack (serangan).

Kriptanalisis mencoba megembalikan data jelas tanpa akses ke ke kunci kriptografi. Ukuran keberhasilan suatu upaya kriptanalisis adalah sampai sejauh mana keberhasilan diketahuinya data jelas atau kunci kriptografi.

Asumsi dasar dari suatu kriptosistem adalah bahwa seorang kriptanalis mengetahui keseluruhan mekanisme enkripsi kecuali kuncinya.Kriptanalisis adalah ilmu (sains) untuk membuka (recovering) suatu pesan tanpa akses ke kunci. Kriptanalisis yang sukses dapat memperoleh teks terang atau kunci. Juga dapat menemukan kelemahan suatu sistem kripto berdasarkan analisis sebelumnya (Schneier, Applied Cr., 1996).

Kriptanalisis adalah studi tentang prinsip2/metode2 pembukaan teks sandi tanpa mengetahui kuncinya. Stalling (Cr and Netsec, 2003).

Kriptanalisis adalah teknik matematik dalam upaya menggagalkan (defeat) suatu teknik kriptografik, dan lebih luas lagi suatu servis pengamanan informasi.(Menezes Cs, Handbook of Applied Cr., 1996)

Kriptanalis bertujuan untuk memcahkan cipherteks menjadi plainteks semula tanpa memiliki akses ke kunci ynag digunakan. Kriptanalis berusaha menemukan kelemahan dari system kriptografi yang pada akhirnya mengarah untuk menemukan kunci dan mengungkap plainteks.

Dalam membahas serangan terhadap kriptografi, kita selalu menganggap bahwa kriptanalis mengetahui algoritma yang digunakan dalam penyandian plainteks., sehingga satu-satunya keamanan siste terdapat pada panjang kunci. Asumsi ini juga diungkapkan dalam prnsip Kerckhoff ynag berbumyi “ Semua algoritma kriptografi harus publik hanya kunci yang rahasia.”

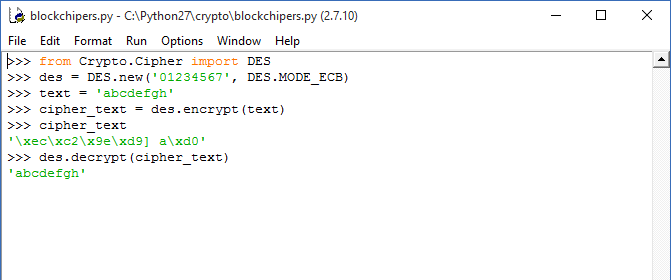
Dengan kata lain kriptanalis mengetahui enkripsi dan dekripsi secara detil. Merahasiakan Algoritma Kriptografi bukan cara yang praktis tetapi malah cara yang pmborosan sebab bila algoritma sandi diketahui oleh pihak lawan, maka kita harus membuat algoritma baru. Oleh karena itu lebih baik uncinya yang rahasia. Jika kunci berhasil dicuri maka kriptografer cukup membangkitkan kunci baru dan seterusnya.

Ada saat ini tidak mengherankan bila semua algoritma kriptografi sudah dipublikasikan ke khalayak umum. Algoritma tersebut sudah dapat dipelajari secara umum oleh semua pihak termasuk di luar lingkubngan persandian. Menurut Scheiner [SCH96], algoritma yang terbaik adalah algoritma yang sudah dipublikasikan dan sudah dipecahkan.Dengan mempublikasikan algoritma baru, kriptografer memperoleh konsultasi gratis dari sejumlah kriptologis akademisi yang ingin sekali memecahkan algoritma sehingga mereka dapat mempublikasikan paper yang memperlihatkan kecerdasan mereka. Jadi banyak pakar yang mencoba mmecahkan suatu algoritma selama beberapa tahun setelah dipublikasikan dan tidak seorangpun berhasil, maka bisa disebut algoritma tersebut tangguh.

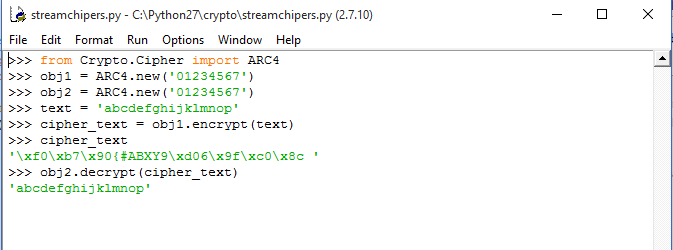
Karena keamanan sistem tergantung kunci, maka agar lebih aman maka kunci harus diperpanjang.

PRAKTIKUM

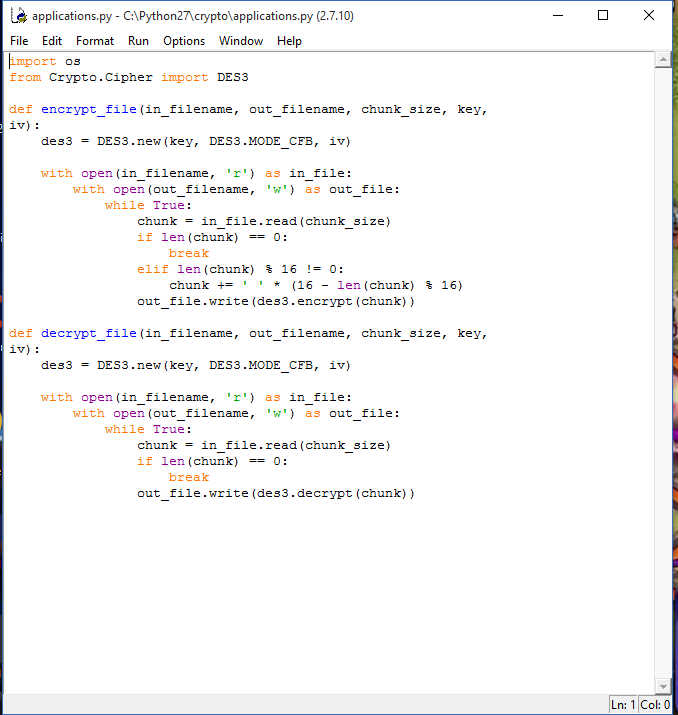
Block ciphers :

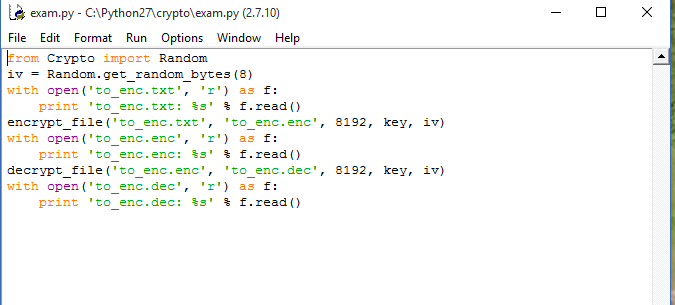


Stream Cipher

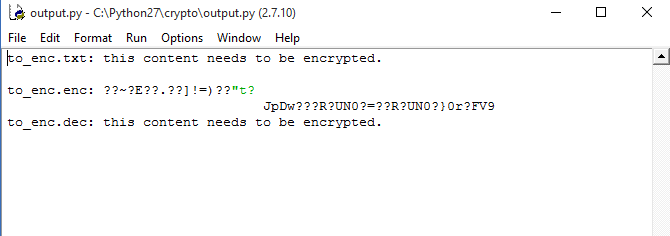


Application

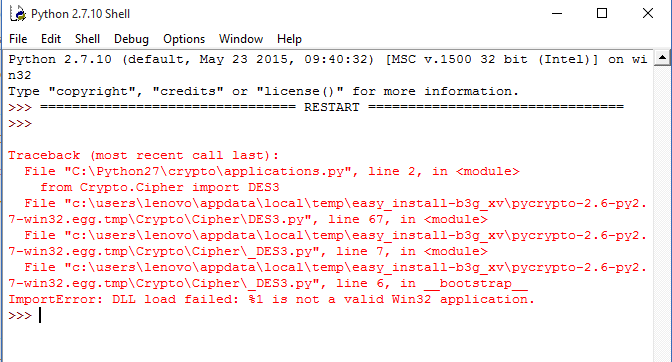




Output



Apabila di Run



Dalam hal ini Laptop/PC saya masih banyak masalah seperti modul tidak bias terinstal

