**LaporaN KEMANAN KOMPUTER**

****

**DisusunOleh :**

Cipyanto 1300631020

**UNIVERSITAS MUHAMMADIYAH JEMBER**

**FAKULTAS TEKNIK**

**Prodi manajemen informatika**

**2015**

DASAR TEORI

Kriptografimenyebabkantimbulnyakriptanalisis, yaituilmupengetahuan dan seniuntukmembongkar data acak. Praktisi dari kriptanalisisdisebutkriptanalis. Kriptanalisberkembangsejalandengankriptografi. Setiap ada algoritmakriptografibaru yang dibuatolehkriptografer, langsungdiikutiolehadanyaupayapercobaankriptanalisis. Percobaankriptanalisisinidisebutattack (serangan).

Kriptanalisismencobamegembalikan data jelastanpaakseskekekuncikriptografi. Ukurankeberhasilansuatuupayakriptanalisisadalahsampaisejauh mana keberhasilandiketahuinya data jelasataukuncikriptografi.

Asumsidasar dari suatukriptosistemadalahbahwaseorangkriptanalismengetahuikeseluruhanmekanismeenkripsikecualikuncinya.Kriptanalisisadalahilmu (sains) untukmembuka (recovering) suatupesantanpaakseskekunci. Kriptanalisis yang suksesdapatmemperolehteksterangataukunci. Juga dapatmenemukankelemahansuatusistemkriptoberdasarkananalisissebelumnya (Schneier, Applied Cr., 1996).

Kriptanalisisadalahstuditentang prinsip2/metode2 pembukaantekssanditanpamengetahuikuncinya. Stalling (Cr and Netsec, 2003).

Kriptanalisisadalahteknikmatematikdalamupayamenggagalkan (defeat) suatuteknikkriptografik, danlebihluaslagisuatuservispengamananinformasi.(Menezes Cs, Handbook of Applied Cr., 1996)

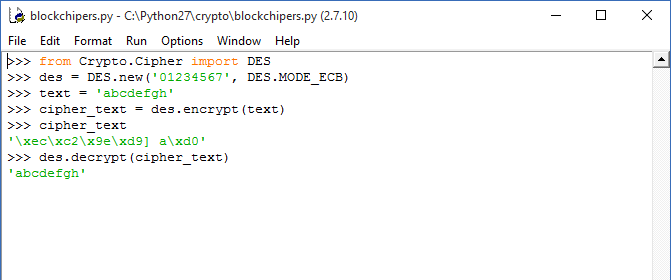
Kriptanalisbertujuanuntukmemcahkancipherteksmenjadiplaintekssemulatanpamemilikiakseskekunciynagdigunakan. Kriptanalisberusahamenemukankelemahandari system kriptografi yang padaakhirnyamengarahuntukmenemukankuncidanmengungkapplainteks.

Dalammembahasseranganterhadapkriptografi, kitaselalumenganggapbahwakriptanalismengetahuialgoritma yang digunakandalampenyandianplainteks., sehinggasatu-satunyakeamanansisteterdapatpadapanjangkunci. Asumsiini juga diungkapkandalamprnsipKerckhoffynagberbumyi“ Semuaalgoritmakriptografiharuspublikhanyakunci yang rahasia.”

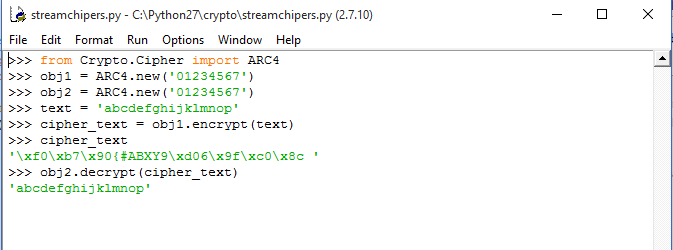
Dengan kata lainkriptanalismengetahuienkripsi dan dekripsisecaradetil. MerahasiakanAlgoritmaKriptografibukancara yang praktistetapimalahcara yang pmborosansebab bila algoritmasandidiketahuiolehpihaklawan, maka kita harusmembuatalgoritmabaru. Olehkarenaitulebihbaikuncinya yang rahasia. Jikakunciberhasildicurimakakriptografercukupmembangkitkankuncibaru dan seterusnya.

PRAKTIKUM

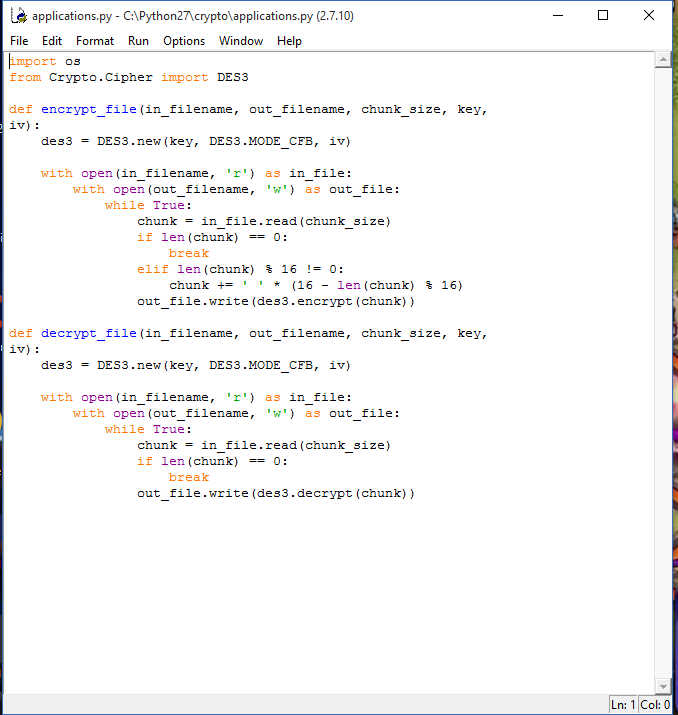
Block ciphers :

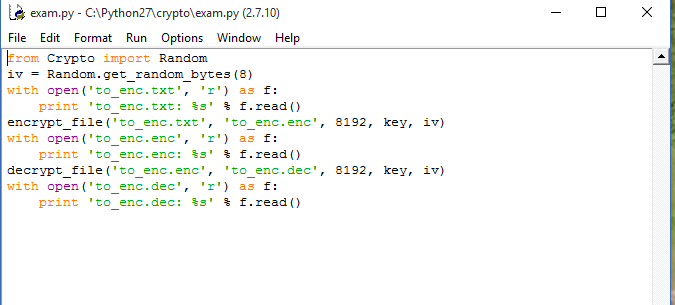


Stream Cipher



Application





Output

