Chosen Plaintext Attack

CPA Security

La seguridad semántica es la noción de encriptar mensajes individuales, pero que es insuficiente para cifrar multiples mensajes. Utilizar un cifrado determinístico y una única clave de cifrado para múltiples mensajes no es seguro. Lo recomendable es usar cifrados probabilísticos.

Ataque multiclave

Si el adversario no es capaz de encontrar de forma eficiente cualquier diferencia estadística entre parejas de mensajes para una secuencia arbitraria de peticiones entonces la semántica es segura.

Construcción de cifrados CPA seguros

1. Se combina un cifrado SS con un PRF usado para generar claves de un solo uso
2. Se usan variantes probabilísticas del conutermode block cipher

PRFs para CPA security Se usa un PRF F y un input aleatorio para generar diferentes claves.

Cifrado:

$c<-E'(k',m)=E(F(k',x),m)$

donde x es un input aleatorio. La salida de esto es (c,x)

Descifrado de (c,x):

$D(K',(c,x))=D(F(k',x),c)$

Randomized Counter Mode

CPA Secure Ciphers