04/02/2018 Notes

Pushkar R. Tiwari

April 17, 2018

3DES(triple encrytion): It is secure against a meet in the middle attack.
3DES(P)=$\mathrm{E}_3(E_2(E_1(P))) = C$
$E_{K2}(E_{K1}(P)) = D_{K3}(C)$
2^{112} entries $E_{K1}(P) = D_{K2}(D_{K3}(C))$
112 bits of effective security.
3DES uses 2 keys(K_1, K_2)
3DES(P)=$\mathrm{E}_{K1}(E_{K2}(E_{K1}(P))) = C$
Try to do a meet in the middle attack
$\mathrm{D}_{K2}(E_{K1}(P)) = D_{K1}(C)$.....1
$\mathrm{E}_{K1}(P) = E_{K2}(D_{K1}(C))$.....2
Either case has two keys on one side of equation.

3DES is still used in practice today but recommended against.

Modes of Operation:
→How to encrypt things larger than block size.

Electronic Codebook (ECB)
→ Break the message into blocks, encrypt each block seperately to get the ciphertext.

Cipher block chaining (CBC)
→ Start with some C_0(this is a random strig) can be sent in clear text.
Break plaintext into blocks P_1, P_2.....P_k

→ Ciphertext C_i= $\mathrm{E}_k(P_i \oplus \mathrm{C}_{i-1})$ (Even if all of the blocks P_i are the same, the ciphertext C_i will all be different)

To decrypt cipher block C_i
→ i=$\mathrm{D}_k(C_i) \oplus \mathrm{C}_{i-1}$

Cipher-feedback(CFB)
→define some notation
head(P)= First n bits of the string P(DES-n=8 , SDES n=4)
tail(P)=everything after head
head(101100101110)=1011
tail("101100101110")=00101110
Write A||B means concatenate these strings together.
CFB
→ Fix an initial X_1(can be sent in cleartext)
$O_i = head(E_k(X_i))$→ (8 bits)
C_i=$O_i \oplus P_i$→ (8 bits) ← Encryption is like the one time pad. DES is used as a random number generator.
X_{i+1}=tail(X_i)||C_i→ (64 bit)
In this case our plaintext is broken into smaller blocks (8 bits for DES, 4 bits for SDES)

Output-feedback (Doesn't have problems of error propogation)
→ Same idea as CFB
$O_i = head(E_k(X_i))$
$C_i = P_i \oplus O_i$
$X_{i+1} = tail(X_i)||O_i$
$Sometimes, this is called a stream cipher.$
$The\ O_{i's}$ can be precomputed(Don't depend on ciphertext.)
OFB is much faster as a result(at the cost of some security.)

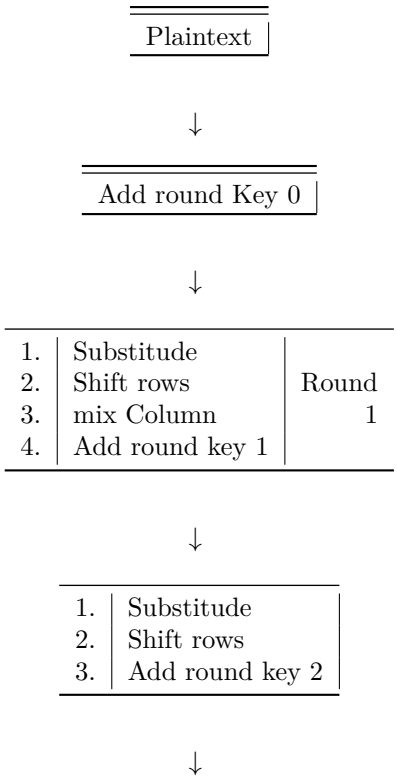
Counter (CTR)
→ Start with any X_0(can be sent cleartext)
X_i=X_{i-1}+1(mod 2^b) : b→blocksize
$C_i = P \oplus E_k(X_i)$
Take home message : ECB → is usually not a good choice for encryption. Pick a different mode of operation.

AES(Advanced Encryption Standard)
→NIST put out a call for proposals to replace DES in the 90s.
The system chosen was rijndael.
This was established as the new standard for data encryption.

Not a feistel cipher
→ Unlike DES the design of AES is completely open to make sure there are no hidden back door.

We'll describe SAES (Simplified AES)
→ 2 rounds(+ initial add round key)

Diagram for SAES



Plaintext and master key are 16 bits in SAES.

Only 1 sbox and it is created using a known formula (takes in 4 bits and output 4 bits)

Take in 4 bits. use them to write a polynomial in F_{16}

$F(x) = \mathrm{b}_0X^3 + b_1X^2 + b_2X + b_3$

Work (modulo X^4+X+1)

→ First we find the inverse of this polynomial in F_{16}

$(\mathrm{b}_0X^3 + b_1X^2 + b_2X + b_3)^{-1} = \mathrm{C}_0X^3 + C_1X^2 + C_2X + C_3$

write these 4-bit as a vector

$$\begin{pmatrix} \mathrm{C}_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix}$$

Multiply on the left by a matrix and add another vector.

$$\begin{pmatrix} 1011 \\ 1101 \\ 1110 \\ 0111 \end{pmatrix} \begin{pmatrix} \mathrm{C}_0 \\ C_1 \\ C_2 \\ C_3 \\ \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \mathrm{d}_1 \\ d_2 \\ d_3 \\ d_4 \\ \end{pmatrix}$$