MATH 314 Spring 2018 - Class Notes

10/24/2018

Scribe: Tepliakova Ksenia

Summary: Cipher feedback (CFB).

Notes:

C_0 - any strings transmitted in cleartext

Plain text blocks $P_0, P_2 ... P_n$

Encryption function: $C_i = E_k(C_{i-1} \bigoplus P_i)$

Decryption function: $P_i = D_k(C_i) \bigoplus C_{i-1}$

Stream Ciphers

Encryption is done by xoring plaintext with a random (pseudo-random) string of bits

Cipher Feed Back(CFB):

C_0- sent in a clear text

C_i- encryption of the previous cipher text

Encryption: $C_i = E_k(C_{i-1}) \bigoplus P_i$

Decryption: $P_i = E_k(C_{i-1}) \bigoplus C_i$

Output Feed Back:

$O_0 -$ Sent in clear text

$O_i = E_k(O_{i-1})$

$C_i = O_i \bigoplus P_i$

Counter(CTR)

$X_i = i$written in binary (add 1 each time)

$C_i = E_k(X_i \bigoplus P_i)$

$P_i = C_i \bigoplus E_k$

NIST put out a new call for proposals for replacement for DES

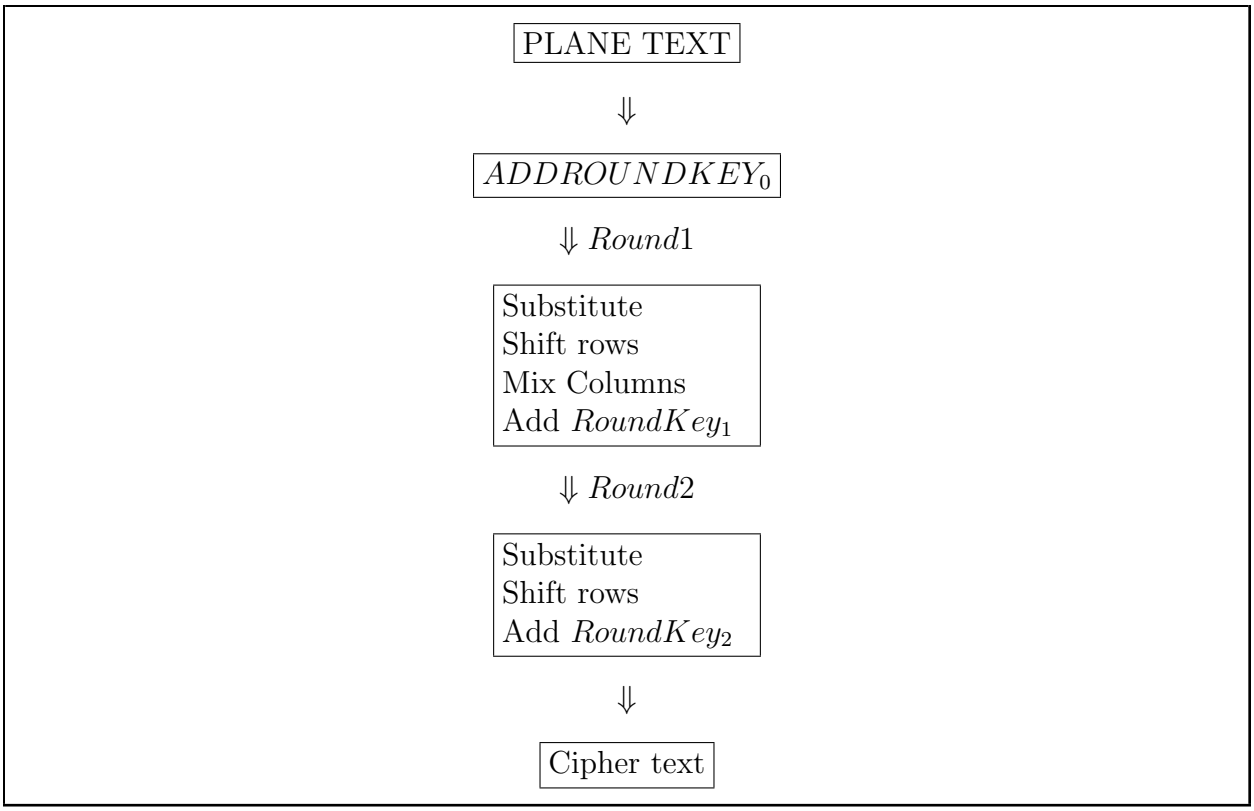
Selected system called Rijndale[Raindoll]. Now it is called AES(Advance Encryption Standart)

One round of AES has 4 steps:

1. Substitute(Sbox)(Confusion)
2. Shift row step(Diffusion)
3. Mix columns(Diffusion)
4. Add Round Key(Confusion)

AES start with an initial add round key step. Then it repeats all steps 9 rounds plus one round without Mix Column step.

Simplified SAES (2 rounds):


PLANE TEXT
⇓
$ADDROUNDKEY_0$
⇓ $Round1$
Substitute
Shift rows
Mix Columns
Add $RoundKey_1$
⇓ $Round2$
Substitute
Shift rows
Add $RoundKey_2$
⇓
Cipher text

`Sbox for SAES`

- Input 4 bits
- Output 4 bits

Input 4 bits b_0, b_1, b_2, b_3
`write a polynomial:` $b_0x^3 + b_1x^2 + b_2x + b_3 = f(x)$ `Think of this as polynomial` $F(x)\epsilon F_{16}$

1. Compute inverse polynomial:
   $F(x)^{-1} = C_0x^3 + C_1x^2 + C_2x + C_3$
2. Take 4 bits and feed them into matrix equation:

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix} \bigoplus \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} \tag{1}$$

Example: Find Sbox value of 0100.

1. Write this as a polynomial: $0 * x^3 + 1 * x^2 + 0 * x + 0 = F(x) = x^2$
2. Find inverse $(modx^4 + x + 1$
3. Use Euclide: $\gcd(x^4 + x + 1, x^2 :)$
   $x^4 + x + 1 = x^2(x^2) + (x + 1)$
   $x^2 = (x + 1)(x + 1) + 1$
   $1 = x^2 + ((x^4 + x + 1) + x^2(x^2))(x + 1)$
   $1 = x^2 + (x + 1)(x^4 + x + 1) + (x^3 + x^2)(x^2)$ $1 = (x^3 + x^2 + 1)x^2 + (x + 1)(x^4 + x + 1)$
   $f^{-1}(x) = x^3 + x^2 + 0 * x + 1$

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \tag{2}$$

$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \bigoplus \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \tag{3}$$