Unit 2

AES

Introduction

- Joan Daemen & Vincent Rijmen From Belgium.
- In Oct 2000 Rijndael was released.
- In Nov 2001 became U.S government standard(FIPS 197).
- ***Features of AES***

1. *Flexible*
2. *Adapted to modern processor*
3. *Suited to Smart Card*
4. *Protection against cryptanalysis attacks.*

Algorithm Steps

1. **Do the following one-time initialization:**

a) *Expand the 16-byte key to get the actual key block to be used.*

b) *Do one time initialization of the 16-byte PT block (called as state).*

c) *XOR the state with key block.*

2. **For each round do the following:**

a) *Apply S-box to each of the PT bytes.*

b) *Rotate row k of the PT block(i.e. state) by k bytes.*

c) *Perform Mix columns operation.*

d) *XOR the state with key block.*

Expand the 16-byte key to get the actual key block to be used.

- 16 byte
- Array size 4*4
- 11 such array
- 1 for initialization & remain 10 for 1 round each.
- Original key copied as it is
- *Key Expansion* = 11*4*4 =176 bytes
- In the context of AES a word means 4 bytes
- So initial 16-byte key (16/4 = 4 word key)
- Will be expanded into 176 bytes key (176/4 = 44 words)

Key Expansion /Add round Key Algorithm

- *If the word in the W array is multiple of four.*
- TMP = W [i-1] previous word
  = W [4-1] word 4 place earlier
  = W [3]

Since i=4,

I mod 4 is 0 this is multiple of 4.

TMP = S-box (Rotate(TMP)) XOR W [i-4] XOR Rcon

- *Otherwise*

TMP= W[i-1] previous word XOR W[i-4] word 4 place earlier

Process in each Round

a) Confusion
b) Diffusion
c) Matrix Multiplication using Galois Field
d) O/P of Step (c) XOR Add round key

- *For step (C):*
- O/P value from step (B) & a constant matrix is used.