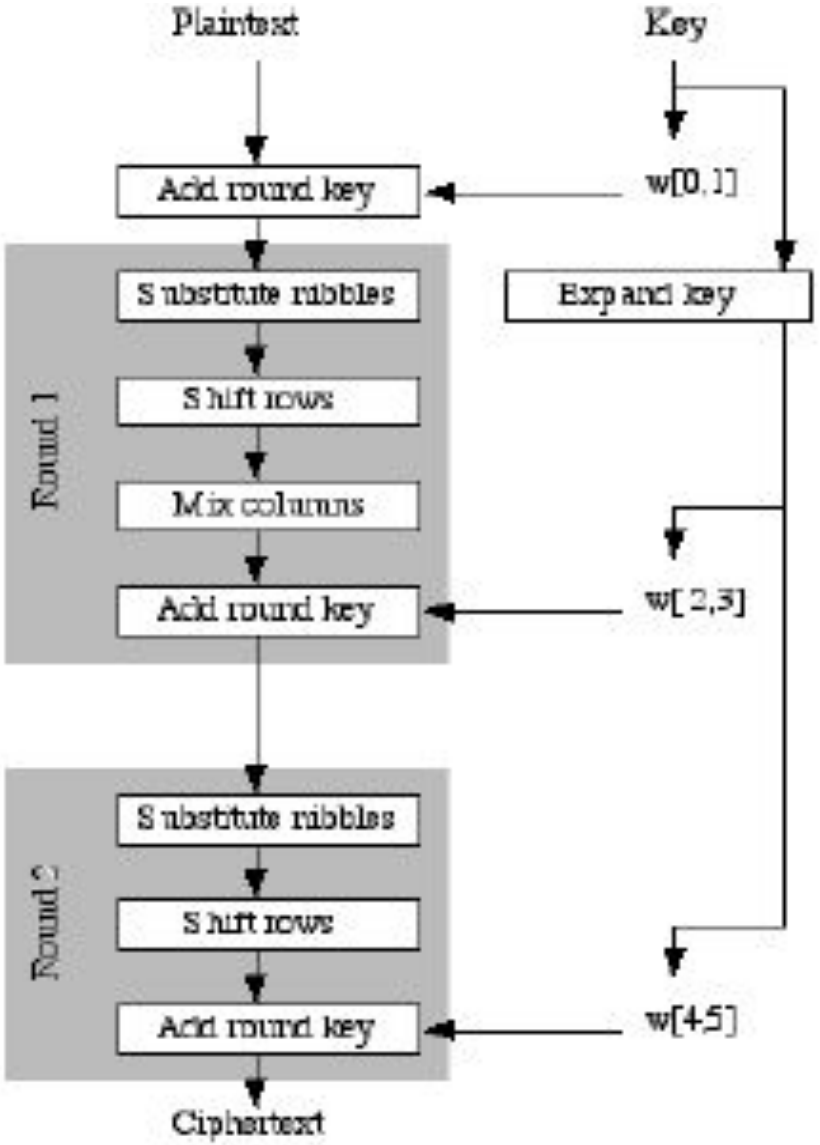
Simplified AES

Dr. S.R. Shinde

S-AES



S-AES Encryption Overview

Key Generation

- Plain text=P[i]= 1101 0111 0010 1000 =16 bit
- Key[i]=0100 1010 1111 0101 =16 bit
- W0[]=0100 1010=for i=0 to 7 W0[i]=Key[i];
- W1[]=1111 0101= W1[i]=Key[i+8];
- K1=W0W1=key=0100 1010 1111 0101
- W2[]= W0 XOR 1000 0000 XOR SubNib(RotNib(W1))
- =0100 1010 XOR 1000 0000 XOR SubNib(RotNib(W1))
- = 1100 1010 XOR SubNib(RotNib(W1))
- = 1100 1010 XOR SubNib(RotNib(1111 0101))
- = 1100 1010 XOR SubNib(0101 1111)

nibble	S-box(nibble)	nibble	S-box(nibble)
0000	1001	1000	0110
0001	0100	1001	0010
0010	1010	1010	0000
0011	1011	1011	0011
0100	1101	1100	1100
0101	0001	1101	1110
0110	1000	1110	1111
0111	0101	1111	0111

- W2[]=1100 1010 XOR SubNib(0101 1111)
- W2[]=1100 1010 XOR 0001 0111
- W2[]=1101 1101
- W3[]= W2 Xor W1
- = 1101 1101 Xor 1111 0101
- = 0010 1000
- W4= W2 XOR 0011 0000 XOR SubNib(RotNib(W3))
- W4[]= 1101 1101 XOR 0011 0000 XOR SubNib(RotNib(W3))

W4[]= 1110 1101 XOR SubNib(RotNib(0010 1000))
W4[]= 1110 1101 XOR SubNib(1000 0010)
W4[]= 1110 1101 XOR 0110 1010
W4[]= 1000 0111
W5[]=W4 XOR W3= 1000 0111 XOR 0010 1000=
W5[]= 1010 1111

Implementation logic

- W2[]= W0 XOR 1000 0000 XOR SubNib(RotNib(W1))
- W4[]= W2 XOR 0011 0000 XOR SubNib(RotNib(W3))
- If (n%2)==0, Count=0
- Wn [i]=Wn-2 XOR SubNib(RotNib(Wn-1));
- While(count<2)
- If (Count==0)

  Wn[i]=Wn[i] XOR 1000 0000;

  Count++;

Else

Wn[i]=Wn[i] XOR 0011 0000;

Count++;

Else

Wn[i]=Wn-2[i] XOR Wn-1[i]

Key

- K1=W0W1=key=0100 1010 1111 0101
- K2=W2 W3= 1101 1101 0010 1000
- K3= W4W5= 1000 0111 1010 1111
- $Key^0 = w^0 w^1$
- = 0100 1010 1111 0101
- $Key^1 = w^2 w^3$
- = 1101 1101 0010 1000
- $Key^2 = w^4 w^5$
- = 1000 0111 1010 1111

Encryption

nibble	S-box(nibble)	nibble	S-box(nibble)
0000	1001	1000	0110
0001	0100	1001	0010
0010	1010	1010	0000
0011	1011	1011	0011
0100	1101	1100	1100
0101	0001	1101	1110
0110	1000	1110	1111
0111	0101	1111	0111

- P= 1101 0111 0010 1000 =16 bit
- K1=W0W1=key=0100 1010 1111 0101
- Add Round Key=ARK1
- ARK1=P Xor K1= 1101 0111 0010 1000
- XOR= 0100 1010 1111 0101
- = 1001 1101 1101 1101
- Substitute Nib= 0010 1110 1110 1110
- Shift Row = 0010 1110 1110 1110

Mix Column

- Shift Row = 0010 1110 1110 1110
- S matrix=

$$M_e = \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0010 & 1110 \\ 1110 & 1110 \end{bmatrix}$$

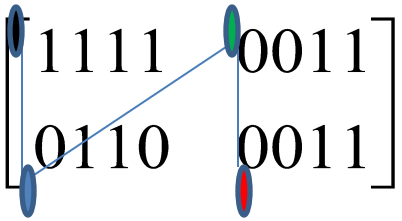
- Mxi Coln Multiplication=Me*S Matrix
- S00= 1*0010 Xor 4* 1110=0010 XOR 0100*1110
- 0100*1110 =x^2*(X^3+X^2+X)= X^5+X^4+X^3=111000 convert into 4 bit binary= X^4+X+1 is polynomial irreducible
- 10011

Polynomial reducer

- 111000/10011
- 111000
- 10011
- 011110=11110
- XoR =10011
- = 01101=1101
- 0010 XOR 0100*1110= 0010 XOR 1101
- = 1111

Mix Column….

- S10= 4*0010 XOR 1*1110
- = 1000 XOR 1110
- = 0110
- S01=1*1110 XOR 4*1110
- = 1110 XOR 1101
- = 0 0 1 1
- S11= 4*1110 XOR 1*1110
- = 1101 XOR 1110
- = 0 0 11
- Mix Coln=1111 0110 0011 0011



Encryption Cont..

nibble	S-box(nibble)	nibble	S-box(nibble)
0000	1001	1000	0110
0001	0100	1001	0010
0010	1010	1010	0000
0011	1011	1011	0011
0100	1101	1100	1100
0101	0001	1101	1110
0110	1000	1110	1111
0111	0101	1111	0111

- Mix Coln=1111 0110 0011 0011
- ARK2= 1111 0110 0011 0011
- XOR = 1101 1101 0010 1000
- = 0010 1011 0001 1011
- Sub Nibble=1010 0011 0100 0011
- Shift Row =1010 0011 0100 0011
- ARK3= 1010 0011 0100 0011
- XOR = 1000 0111 1010 1111
- = 0010 0100 1110 1100
- = Cipher Text =0010 0100 1110 1100

Decryption

- Cipher Text= 0010 0100 1110 1100
- K1=W0W1=0100 1010 1111 0101
- K2=W2 W3= 1101 1101 0010 1000
- K3= W4W5= 1000 0111 1010 1111
- ARK3= 0010 0100 1110 1100
- XOR = 1000 0111 1010 1111=k3
- =1010 0011 0100 0011

nibble	S-box(nibble)	nibble	S-box(nibble)
0000	1001	1000	0110
0001	0100	1001	0010
0010	1010	1010	0000
0011	1011	1011	0011
0100	1101	1100	1100
0101	0001	1101	1110
0110	1000	1110	1111
0111	0101	1111	0111

- ARK3= 1010 0011 0100 0011
- Inv Shift row= 1010 0011 0100 0011
- Inv Nib Sub= 0010 1011 0001 1011
- ARK2= 0010 1011 0001 1011
- XOR = 1101 1101 0010 1000=k2
- = 1111 0110 0011 0011=S00, S10, S01, S11
- Inv Mix coln= $\begin{bmatrix} 9 & 2 \\ 2 & 9 \end{bmatrix} \begin{bmatrix} 1111 & 0011 \\ 0110 & 0011 \end{bmatrix}$

Inverse of Mix Column

- S00=9*1111 XOR 2*0110 =1110 XOR 1100=0010
- S10= 2*1111 XOR 9*0110=1101 XOR 0011=1110
- S01= 9*0011 XOR 2*0011=1000 XOR 0110=1110
- S11=2*0011 XOR 9*0011=0110 XOR 1000= 1110
- 9*1111= (X^3+1)(X^3+X^2+X+1)
- = X^6+X^5+X^4+X^3+ X^3+X^2+X+1
- Re =(X^4+X+1)* X^2=X^6+X^3+X^2
- = X^5+X^4+X^3+X+1
- =X^5+X^2+X
- =X^4+X^3+X^2+1
- = X^4+X+1
- = X^3+X^2+X
- =**1110**

- S10= 2*1111 XOR 9*0110=1101 XOR 0011=1110
- 2*1111 =
- X*(X^3+X^2+X+1)= X^4+X^3+X^2+X
- X^4+ X+1
- = X^3+X^2+1=1101
- 9*0110= (X^3+1)*(X^2+X)=X^5+X^4+X^2+X
- (X^4+X+1) *X = X^5+ X^2+X
- = X^4
- X^4+X+1
- = X+1=0011

- S01= 9*0011 XOR 2*0011=1000 XOR 0110=1110
- (X^3+1)*(X+1)= X^4+X^3+X+1
- = X^4+X+1
- = X^3=1000
- S00=9*1111 XOR 2*0110 =1110 XOR 1100=0010
- S10= 2*1111 XOR 9*0110=1101 XOR 0011=1110
- S01= 9*0011 XOR 2*0011=1000 XOR 0110=1110
- S11=2*0011 XOR 9*0011=0110 XOR 1000= 1110
- Inv Mix Coln= 0010 1110 1110 1110

nibble	S-box(nibble)	nibble	S-box(nibble)
0000	1001	1000	0110
0001	0100	1001	0010
0010	1010	1010	0000
0011	1011	1011	0011
0100	1101	1100	1100
0101	0001	1101	1110
0110	1000	1110	1111
0111	0101	1111	0111

- Inv Mix Coln= 0010 1110 1110 1110
- Inv Shift row= 0010 1110 1110 1110
- Inv Nib Sub =1001 1101 1101 1101
- ARK1 XOR K1=0100 1010 1111 0101
- =1101 0111 0010 1000
- P= 1101 0111 0010 1000