Exp No: 5

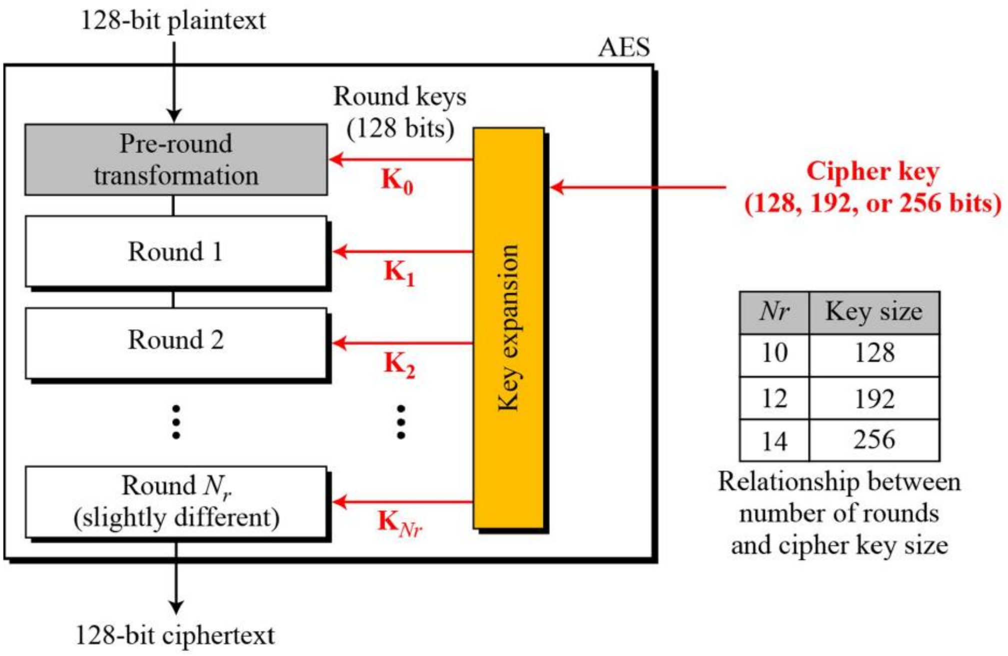
AES algorithm

Aim

To implement AES encryption and decryption

Description to Implement

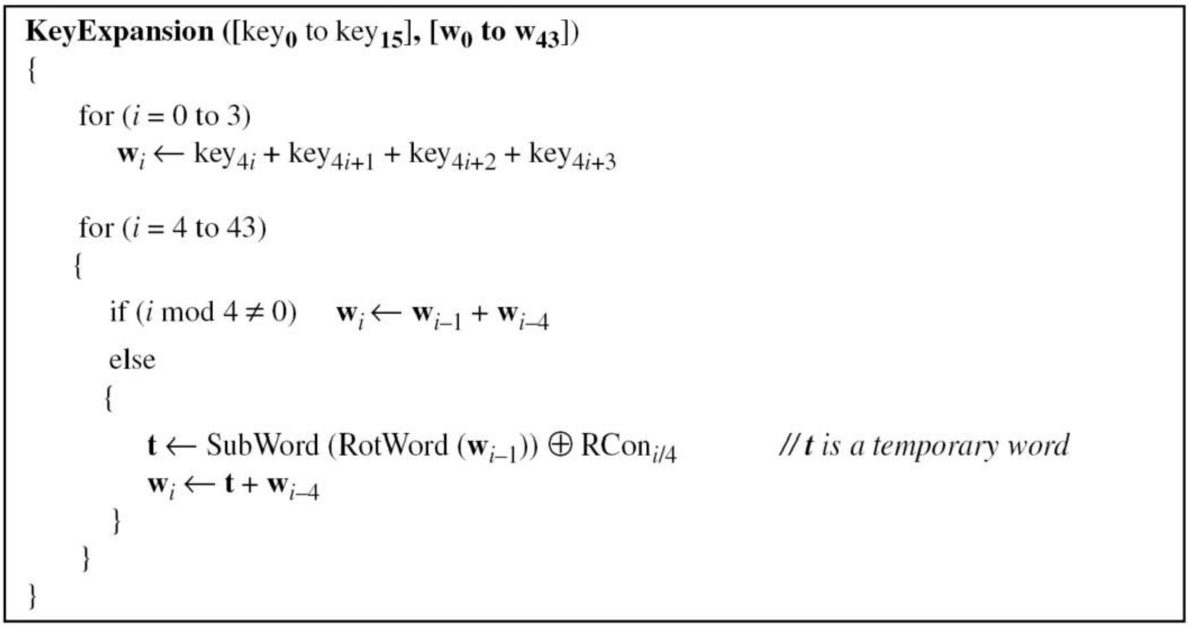
The general structure of the AES consists of key schedule and round function



Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

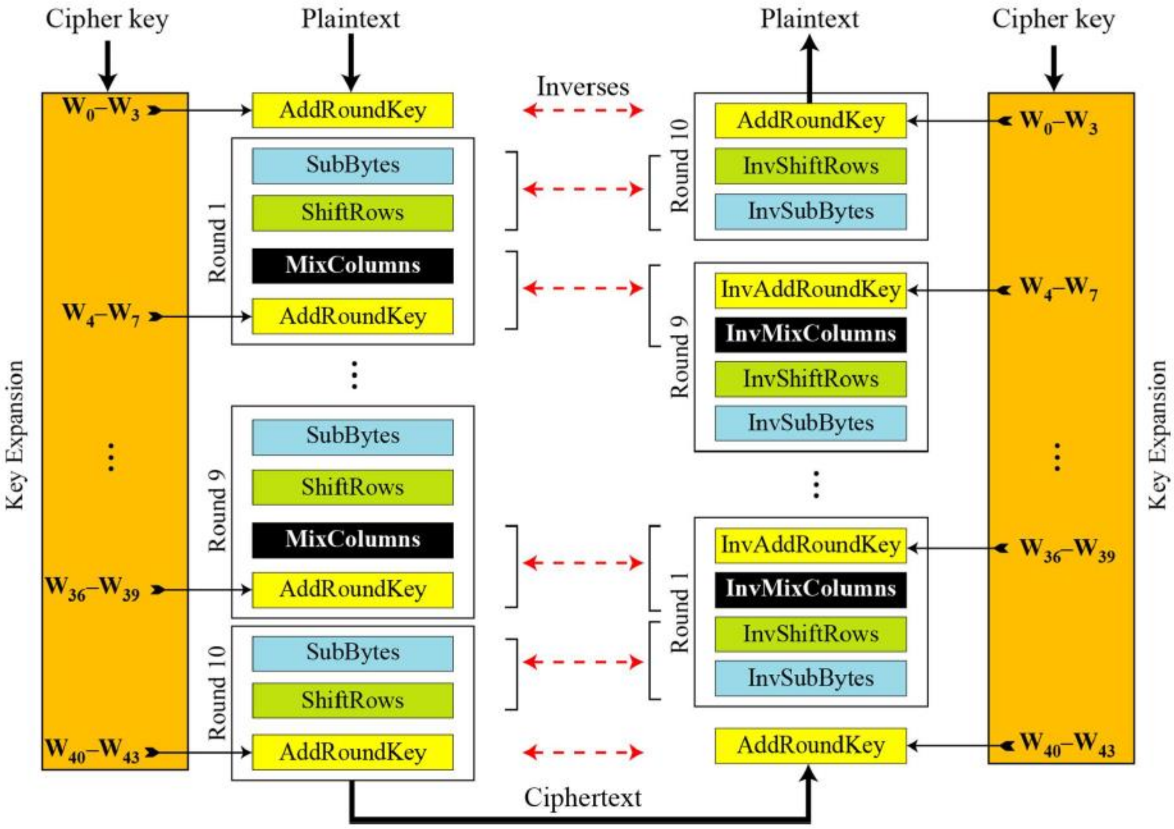
Key Expansion



```
KeyExpansion ([key_0 to key_15], [w_0 to w_43])
{
     for (i = 0 to 3)
         w_i ← key_4i + key_4i+1 + key_4i+2 + key_4i+3

     for (i = 4 to 43)
     {
         if (i mod 4 ≠ 0)     w_i ← w_i−1 + w_i−4
         else
         {
             t ← SubWord (RotWord (w_i−1)) ⊕ RCon_i/4          // t is a temporary word
             w_i ← t + w_i−4
         }
     }
}
```

Encryption-Decryption


Cipher key
Plaintext
Inverses
Plaintext
Cipher key
Key Expansion
W_0–W_3
W_4–W_7
W_{36}–W_{39}
W_{40}–W_{43}
AddRoundKey
Round 1
SubBytes
ShiftRows
MixColumns
AddRoundKey
Round 9
SubBytes
ShiftRows
MixColumns
AddRoundKey
Round 10
SubBytes
ShiftRows
AddRoundKey
Ciphertext
Round 10
AddRoundKey
InvShiftRows
InvSubBytes
Round 9
InvAddRoundKey
InvMixColumns
InvShiftRows
InvSubBytes
Round 1
InvAddRoundKey
InvMixColumns
InvShiftRows
InvSubBytes
AddRoundKey
W_0–W_3
W_4–W_7
W_{36}–W_{39}
W_{40}–W_{43}
Key Expansion