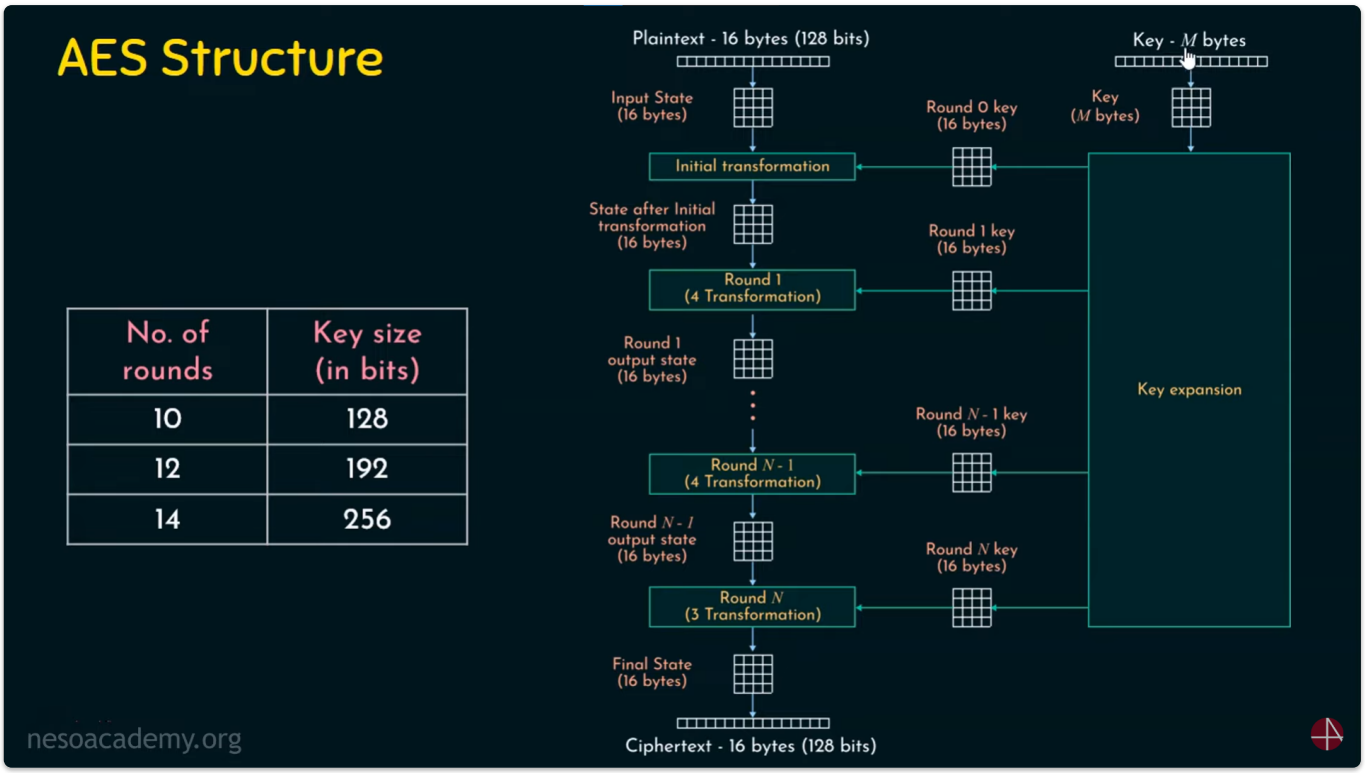
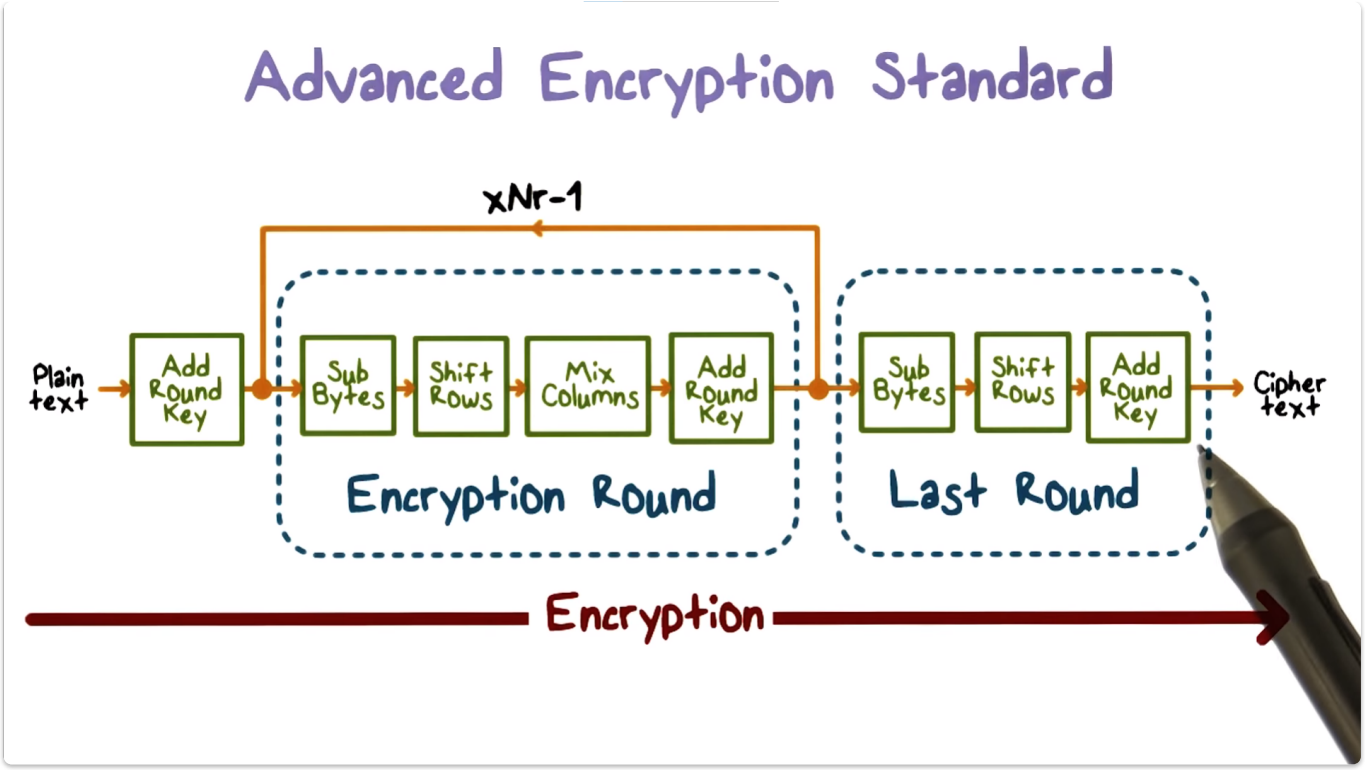
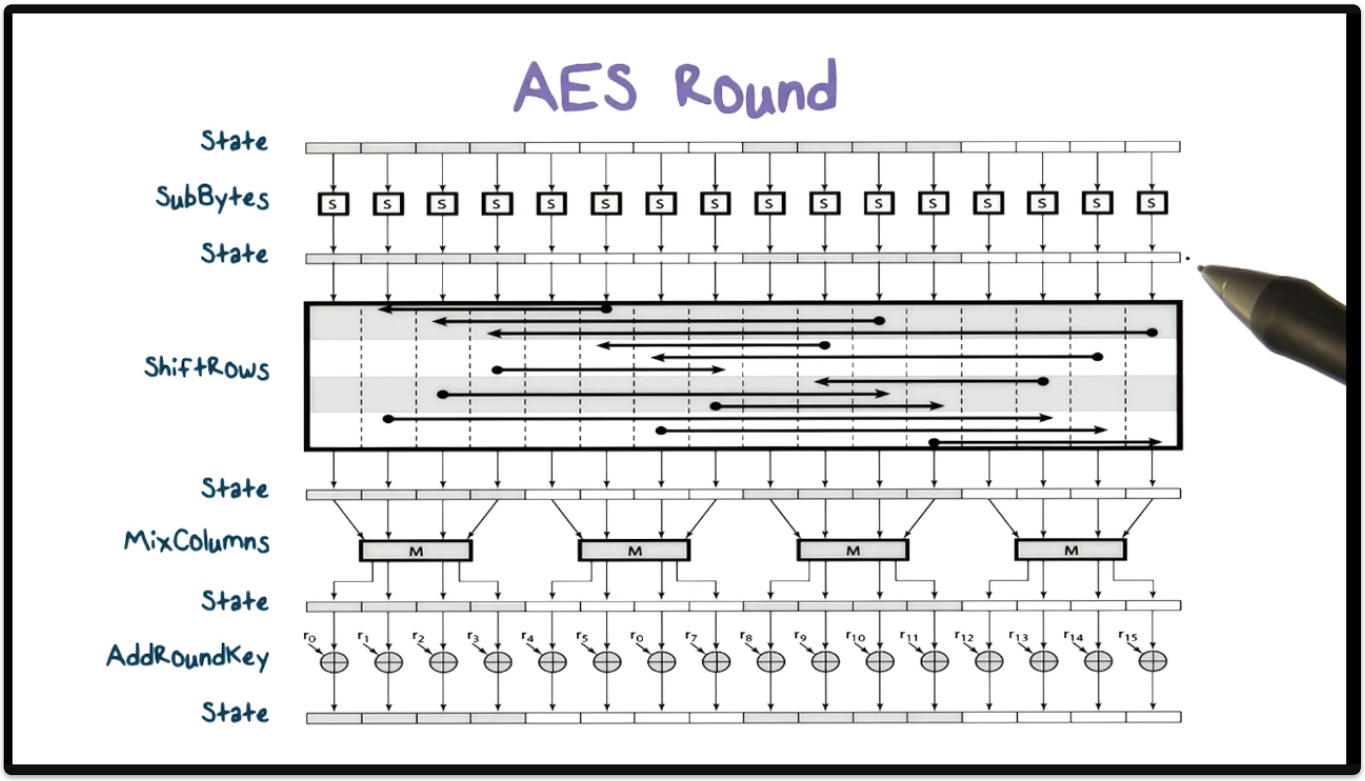
AES

Both AES and DES are Symmetric key Block Ciphers

- S-P (Substitution - Permutation) : Confusion & Diffusion
- S-Box and P-Box
- {above ones are Concepts of DES and AES}

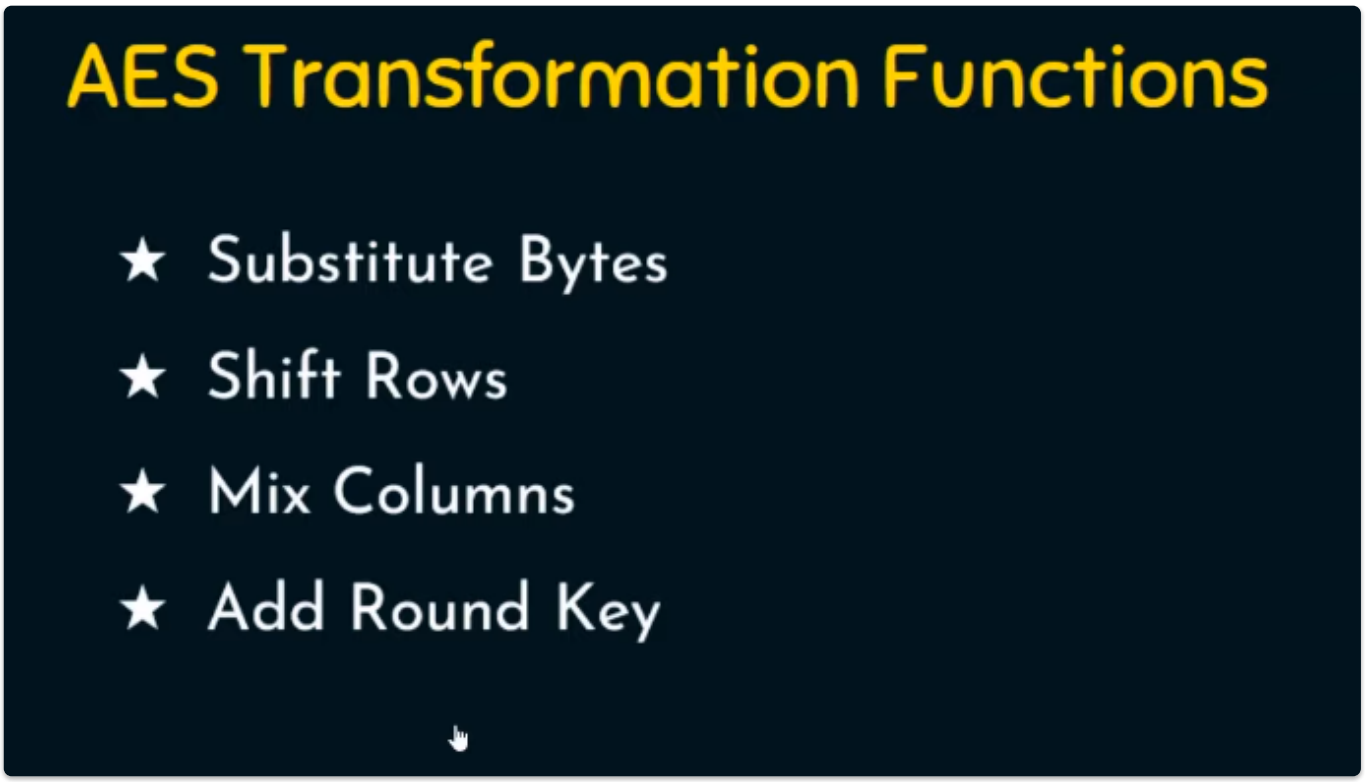






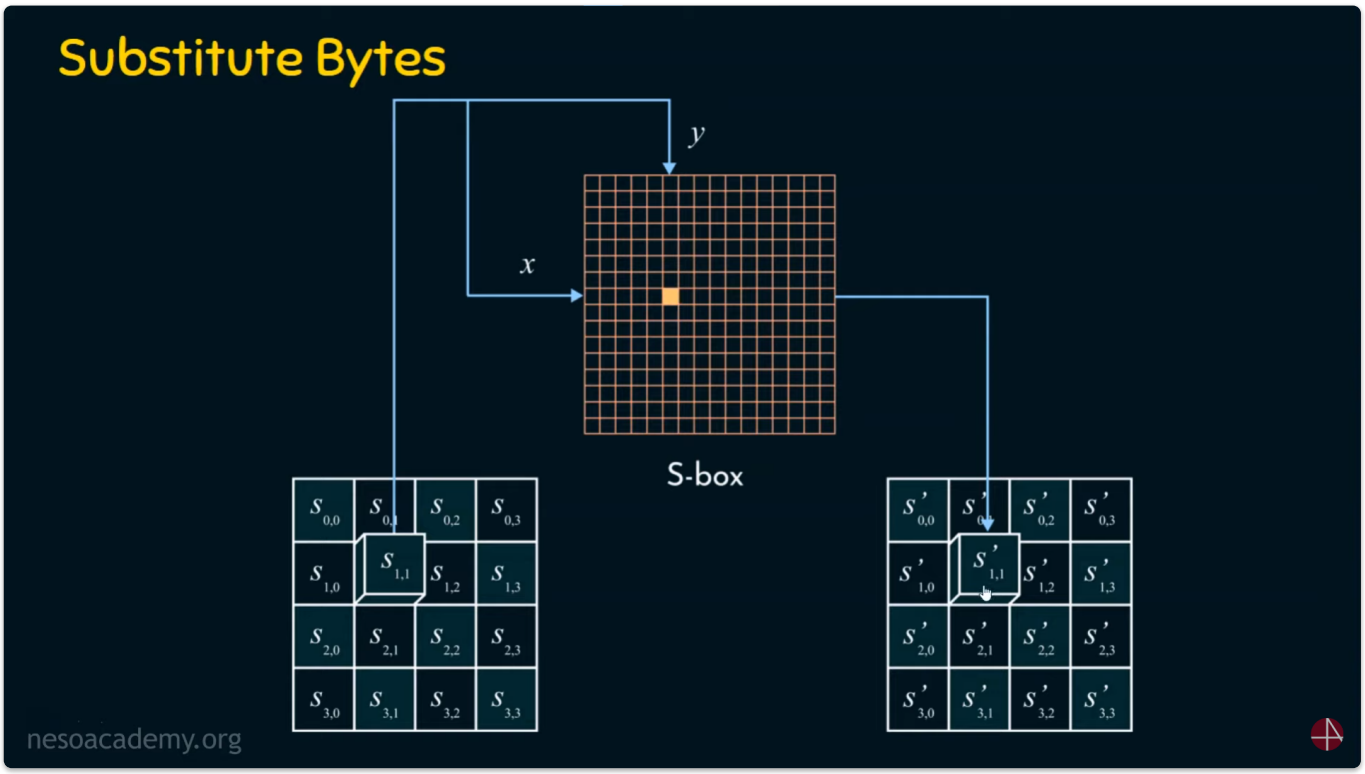
- Add Round Key step : Always involves XOR Operation {in both DES and AES}

ROUND OF AES

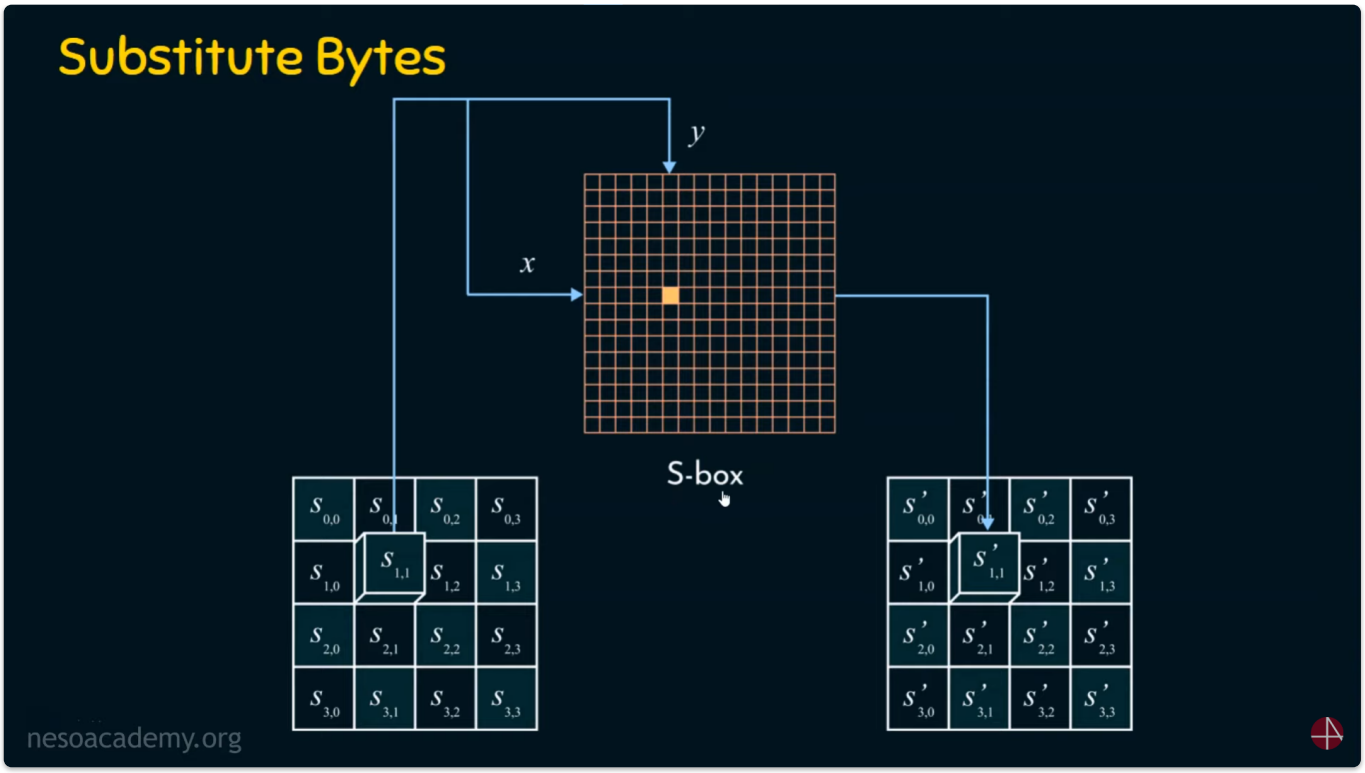


Exception : Round 10 {Last Round} doesn't do "Mix Columns" Function.

1



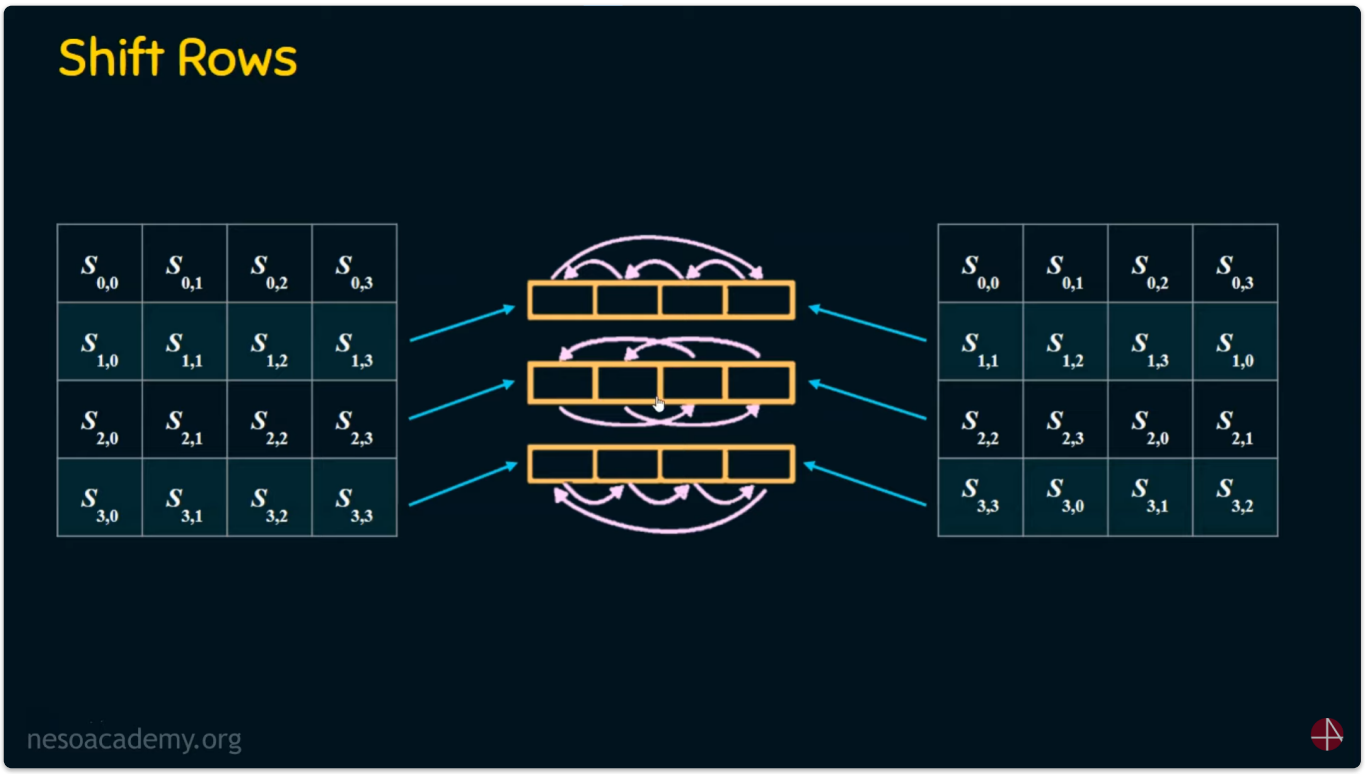
2



S-Box Lookup Table is Given, 8 Bits of One Box tells us Index inside Lookup Table,

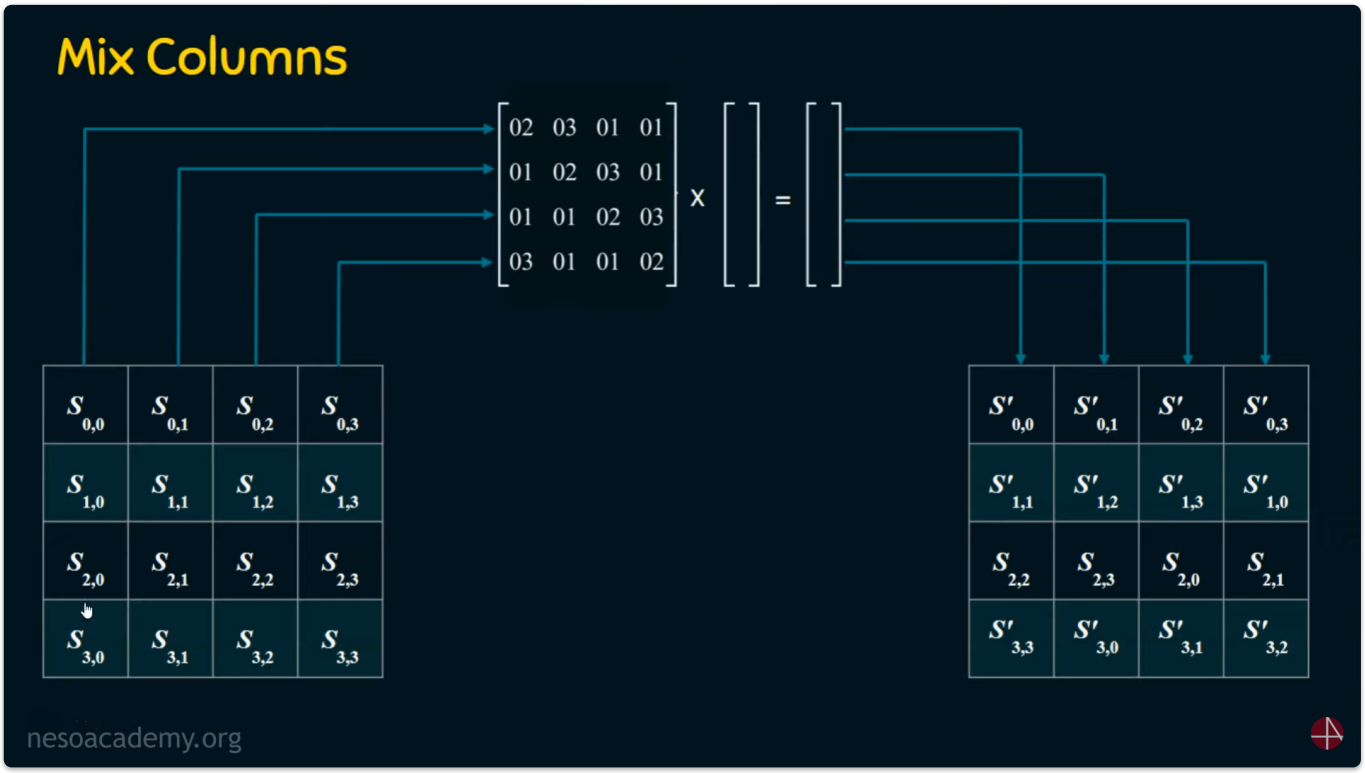
for example, S0,0 = 1010 1111 so Starting 4 Bits = Row and Ending 4 Bits = Column of Lookup Table

3



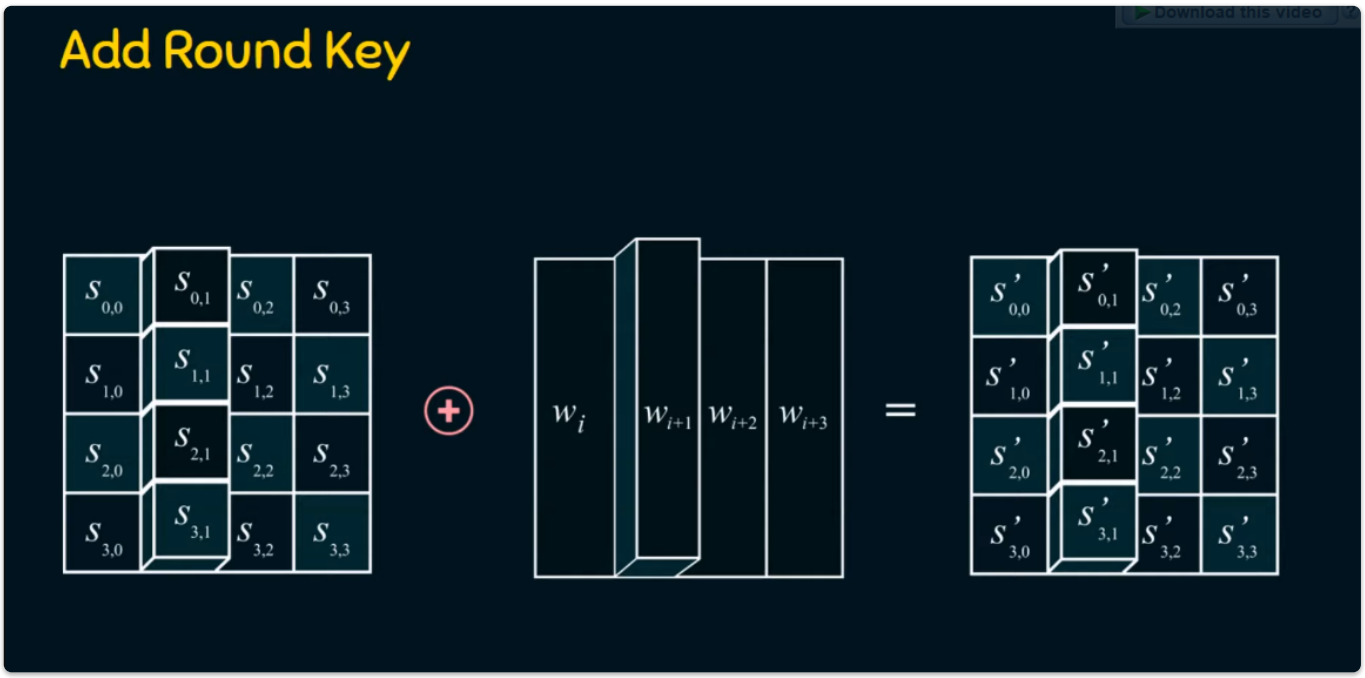
Left Shift is happening simply, Nth Row is Shifted Nth Block to the Left.

4



Constant 4x4 Matrix is Given,
Simply Multiply Each Column of our State Matrix with Entire Constant Matrix
And Resulting 4x1 is the Column of our New Matrix

5

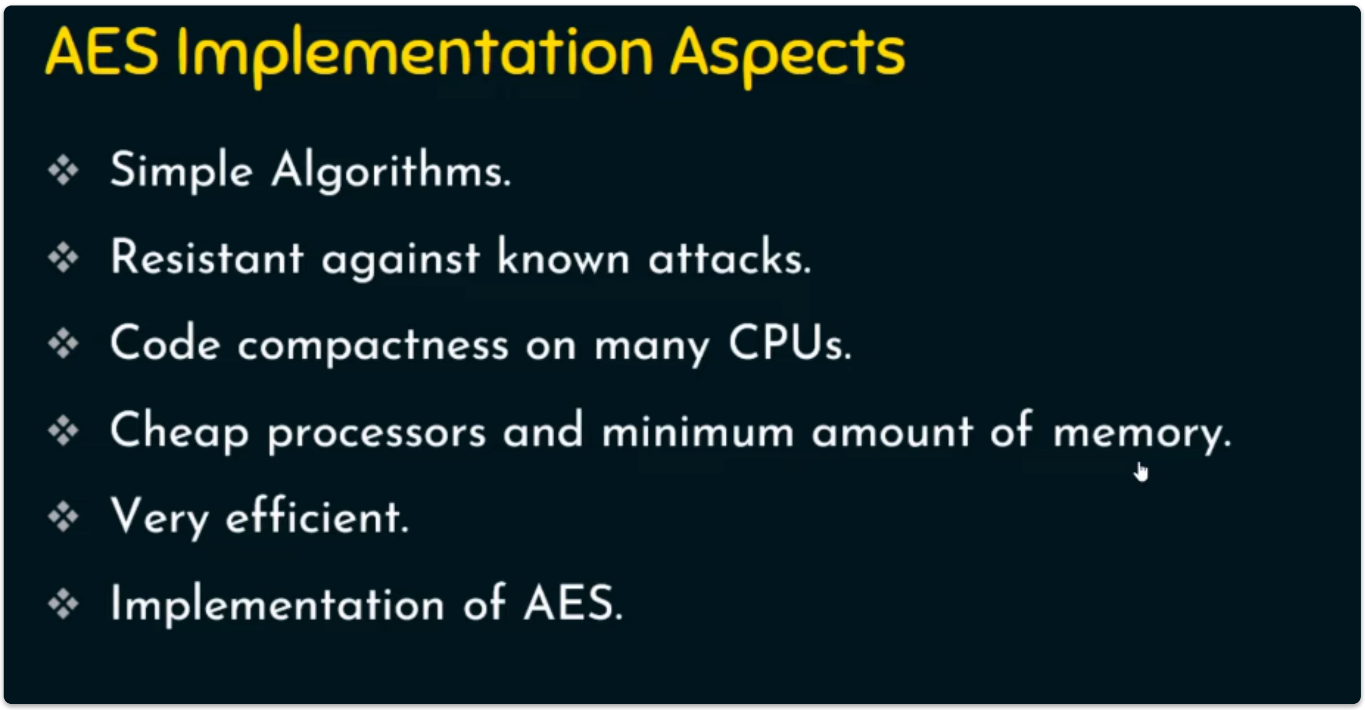


1st Column of State Matrix is XOR with 1st Column or Word of Round Key

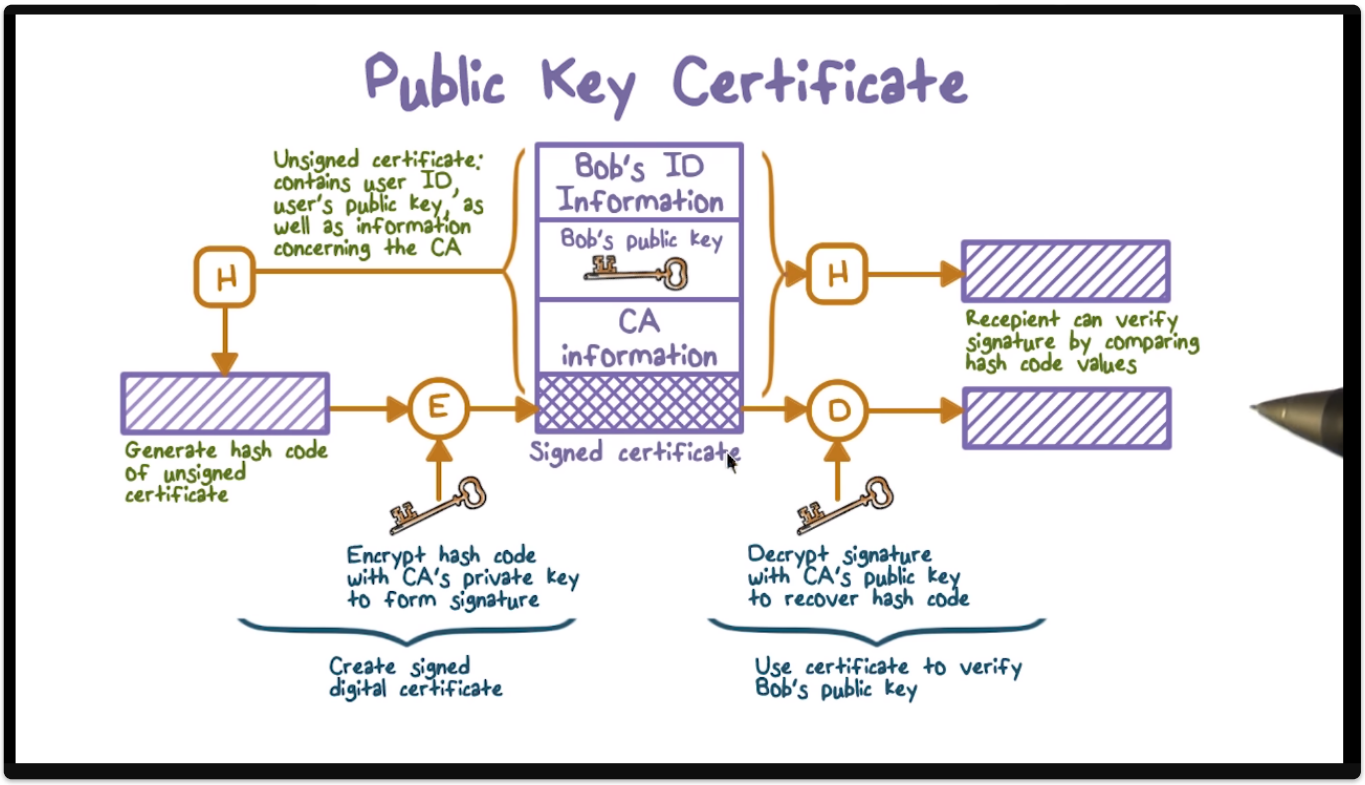
Hence, We will have 4x4 {128-bit} Cipher Text after Completing 10 Rounds.

SECURITY OF AES

BENEFITS OF AES



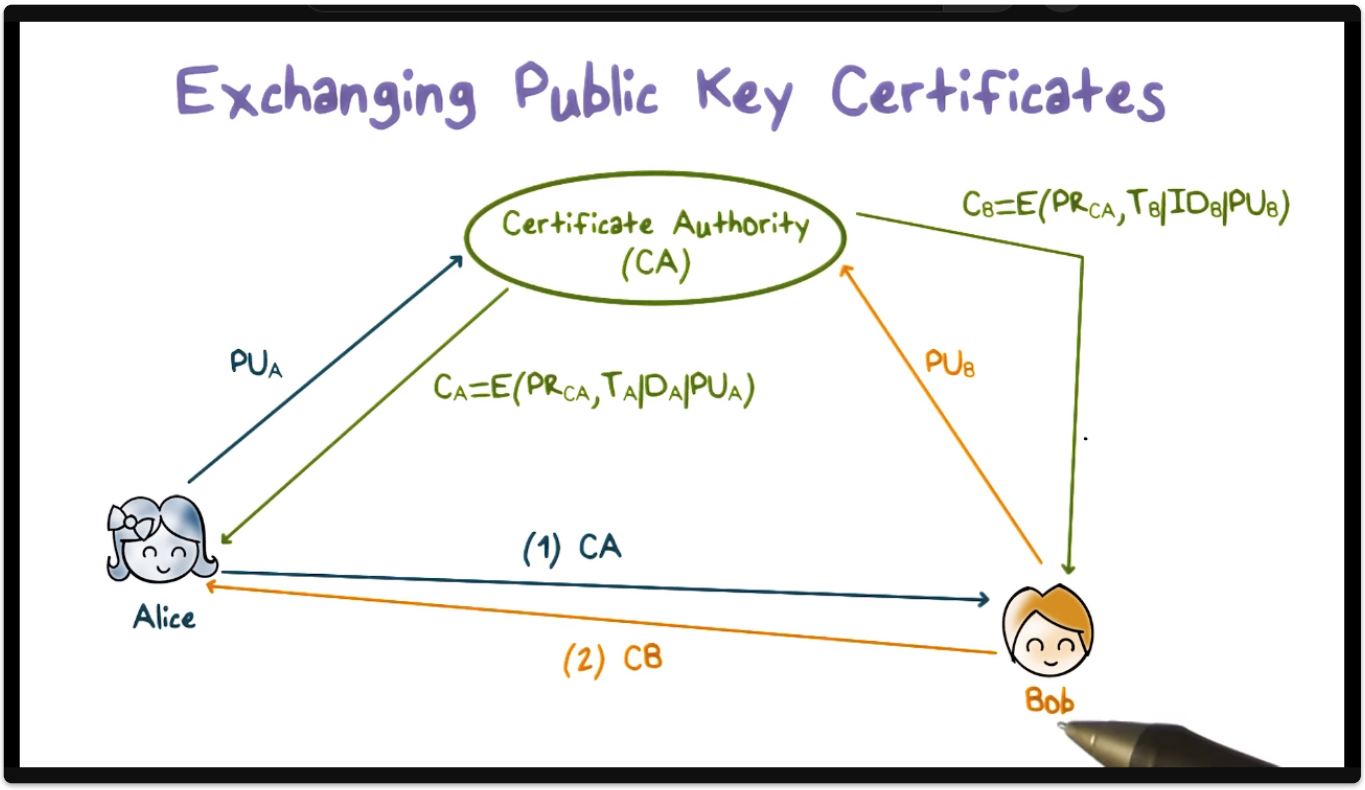
Digital Signature



CA = Certificate Authority's Assigned Information

Alice sends her Public Key to CA Certificate Authority so that
they assign Alice some Digital Certificate containing information like

1. Time of Creation
2. Validity Period
3. ID of Alice
4. A Public Key => Which was generated using CA's Private Key

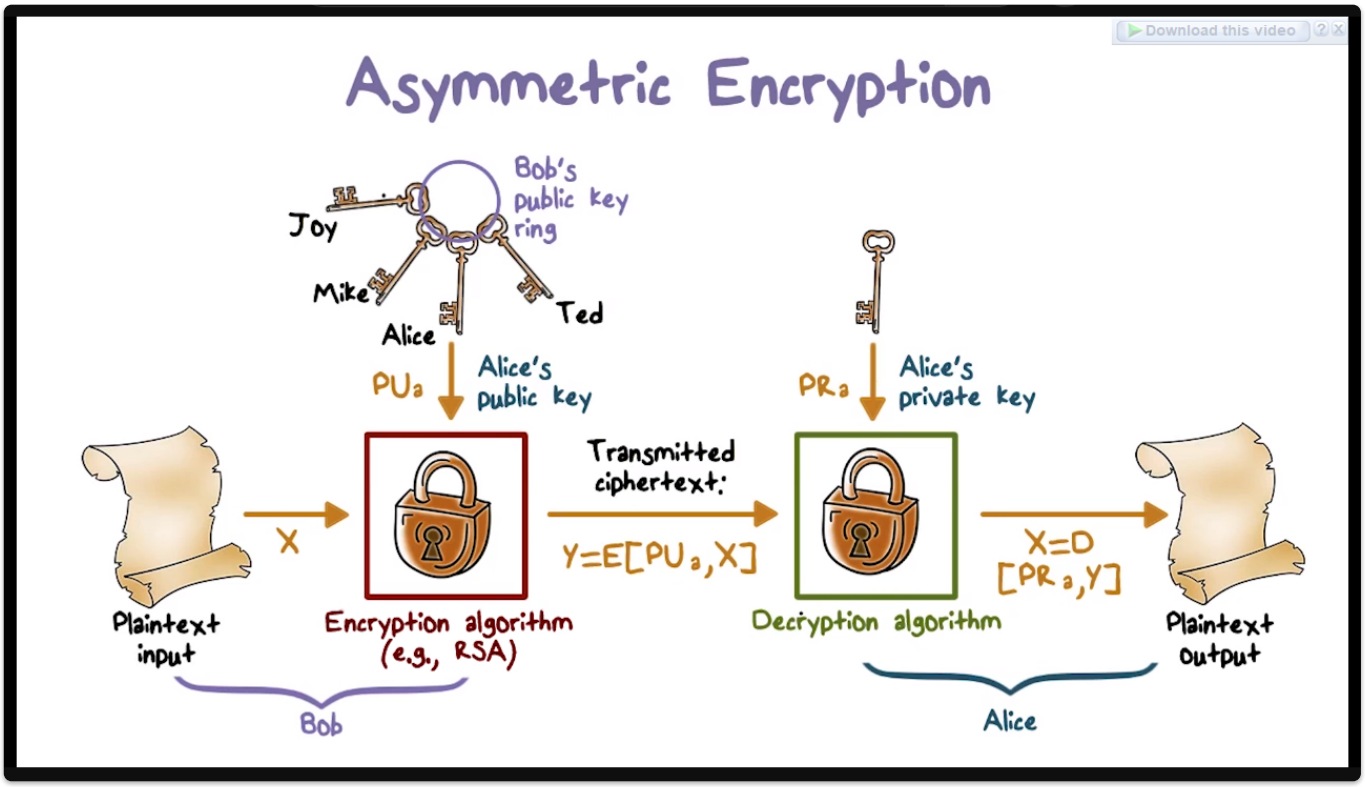


Bob can do the same and then
Both Alice and Bob can exchange these CA provided Public Keys with each other and Get Verified by CA Certificate Authority

So Public Keys are Exchanged through an Authority called CA

==How Asymmetric Encryption Works ? ==

- *Algorithm used is RSA



- Alice (Someone who will receive a Message here)
- Alice will generate a Pair of Keys (Private and Public Key)
- If Alice receives a Message Encrypted using this Public Key.
- Then it would be a Piece of Cake to just Decrypt that Message
- using Private Key initially generated as a Pair to the Public Key.
- So these two Keys (Private and Public) for Alice were
  Generated using Mathematics in such a way that,
  1. Content Encrypted by Public Key would be easily,
  2. Decrypted by Private Key
  3. These Keys are a Pair (Only Compatible with each other).

Now Alice can Share Her Public Key to the Entire World, So Everyone Knows each other's Public Keys

Bob will Use Alice's Public Key and Encrypt the Message and Send that Message to Alice. Since only Alice has her Private Key, Only She can Decrypt the Message

That's all