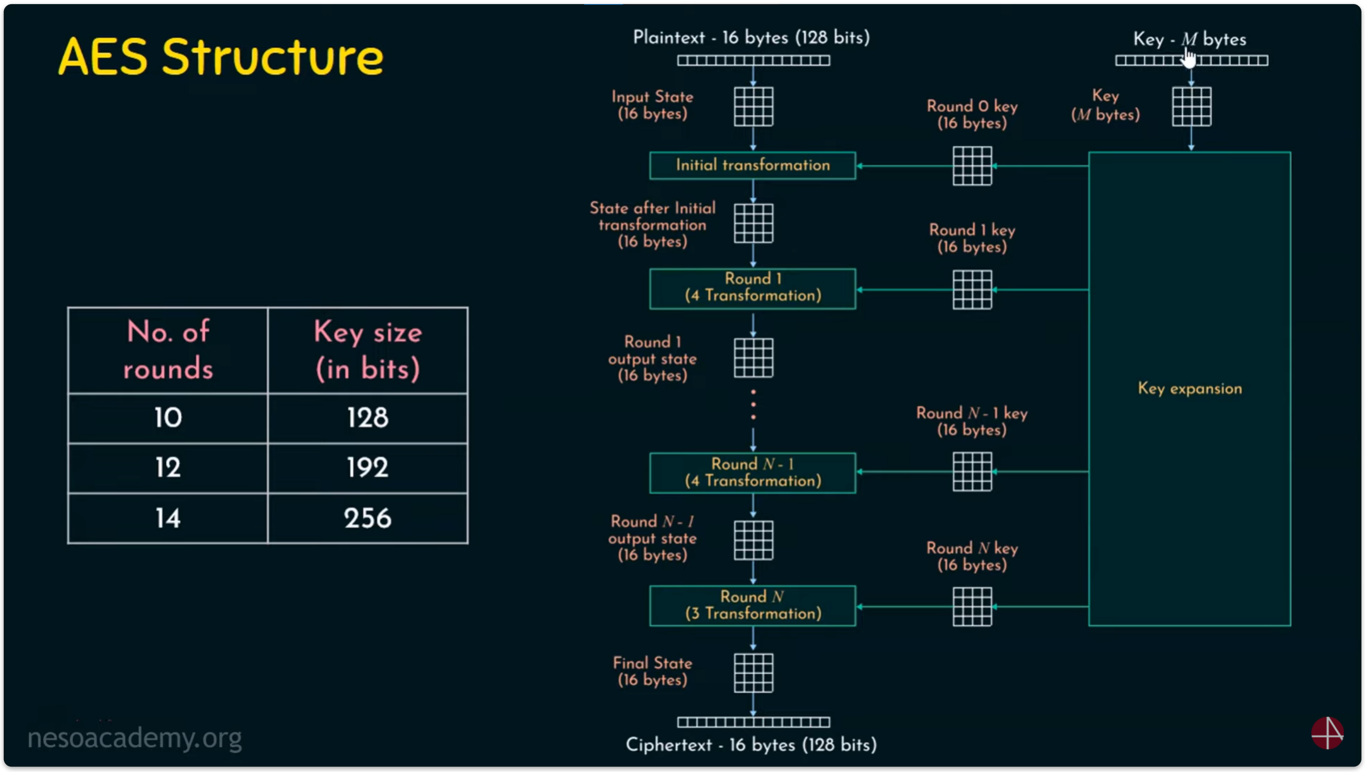
AES

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}



AES Structure

No. of rounds	Key size (in bits)
10	128
12	192
14	256

Plaintext - 16 bytes (128 bits)

Key - M bytes

Input State (16 bytes)

Key (M bytes)

Round 0 key (16 bytes)

Initial transformation

State after Initial transformation (16 bytes)

Round 1 key (16 bytes)

Round 1 (4 Transformation)

Round 1 output state (16 bytes)

Key expansion

Round N - 1 key (16 bytes)

Round N - 1 (4 Transformation)

Round N - 1 output state (16 bytes)

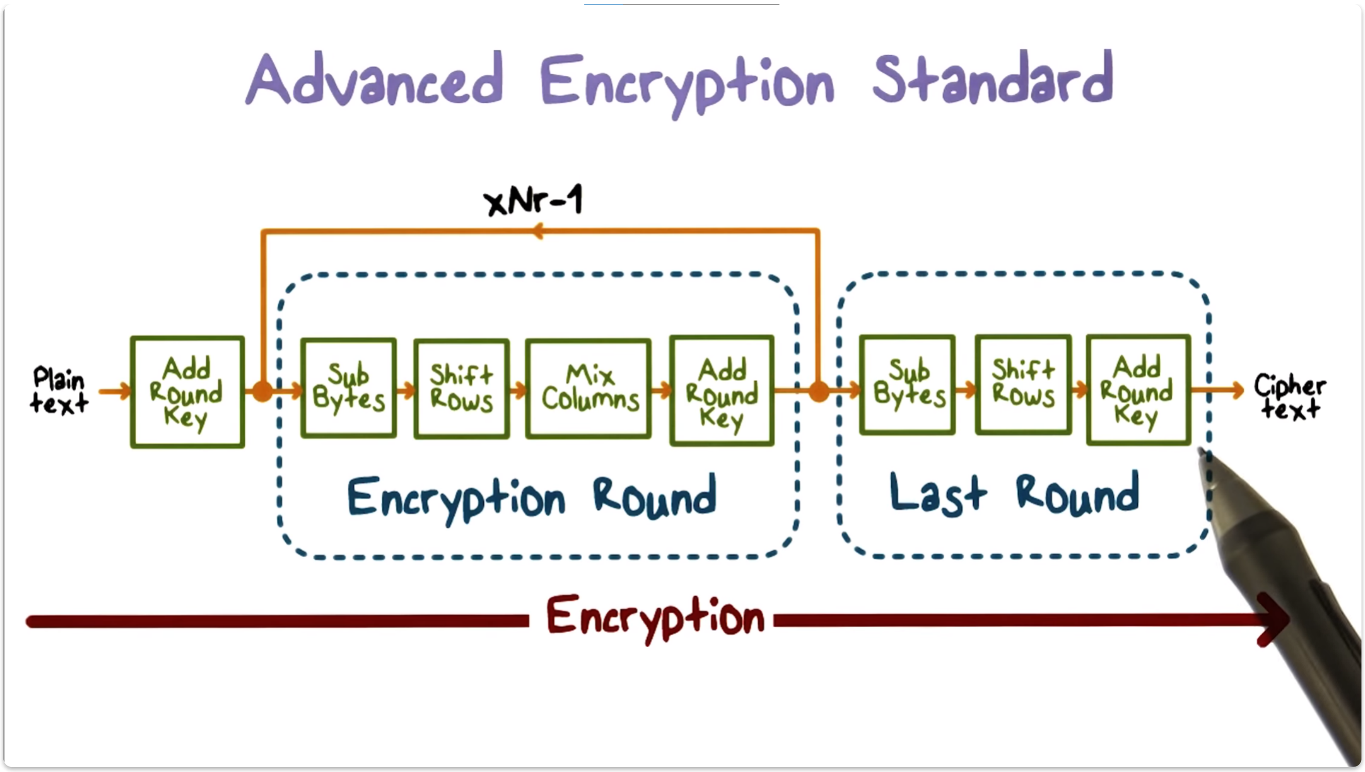
Round N key (16 bytes)

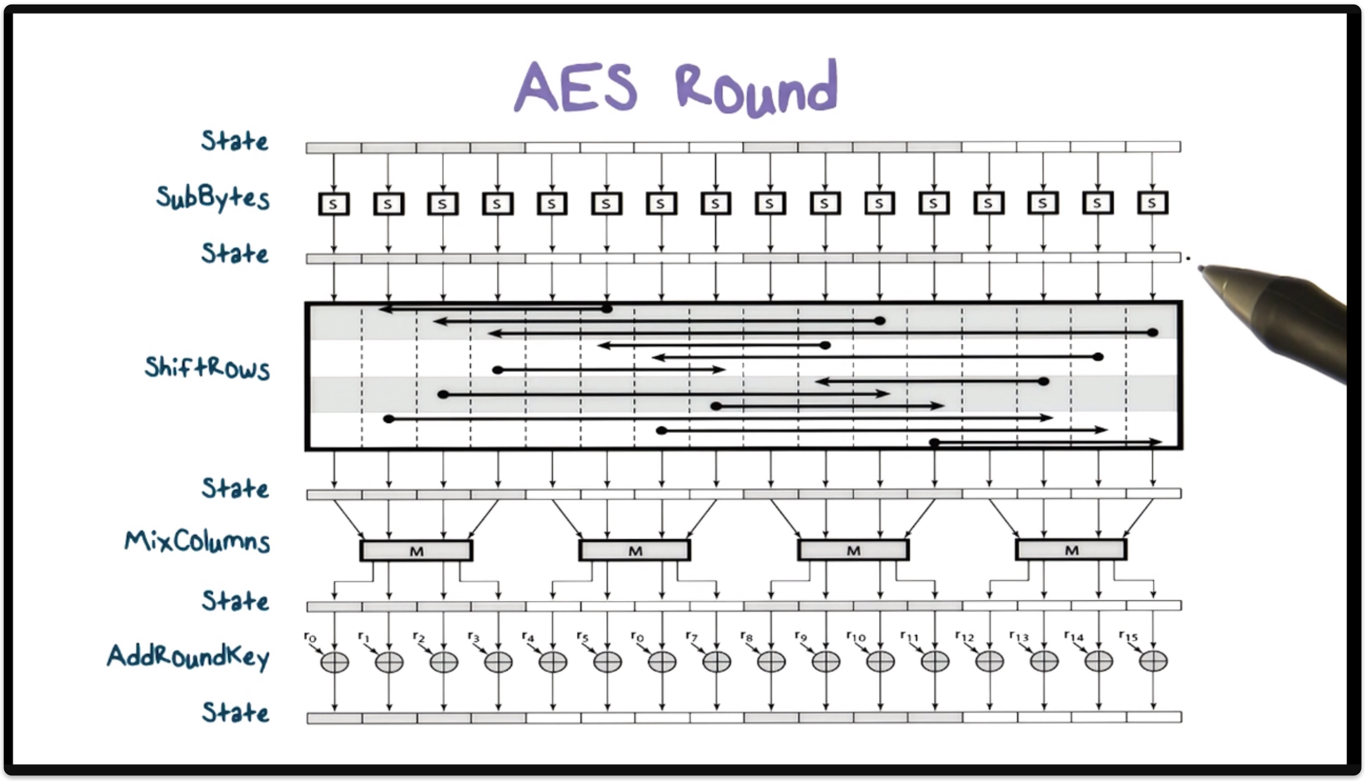
Round N (3 Transformation)

Final State (16 bytes)

Ciphertext - 16 bytes (128 bits)

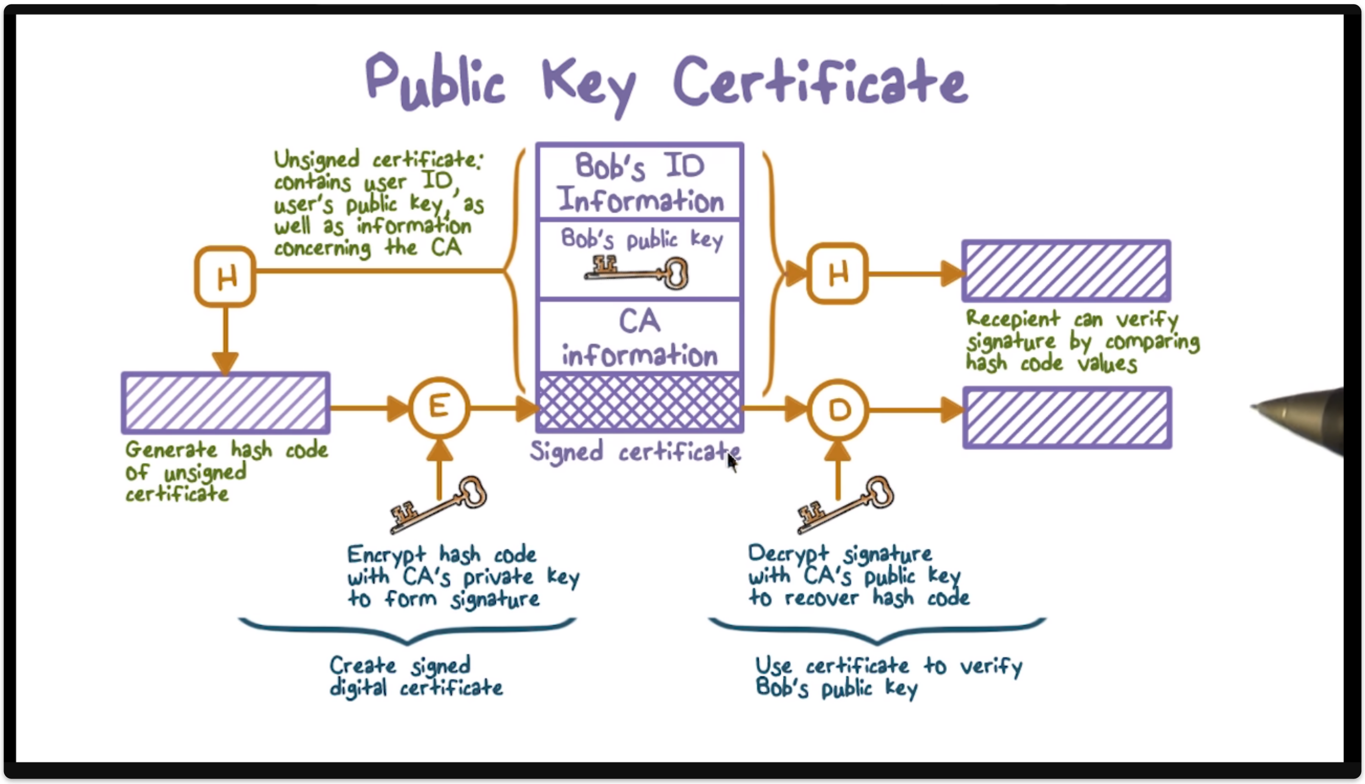
nesoacademy.org





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

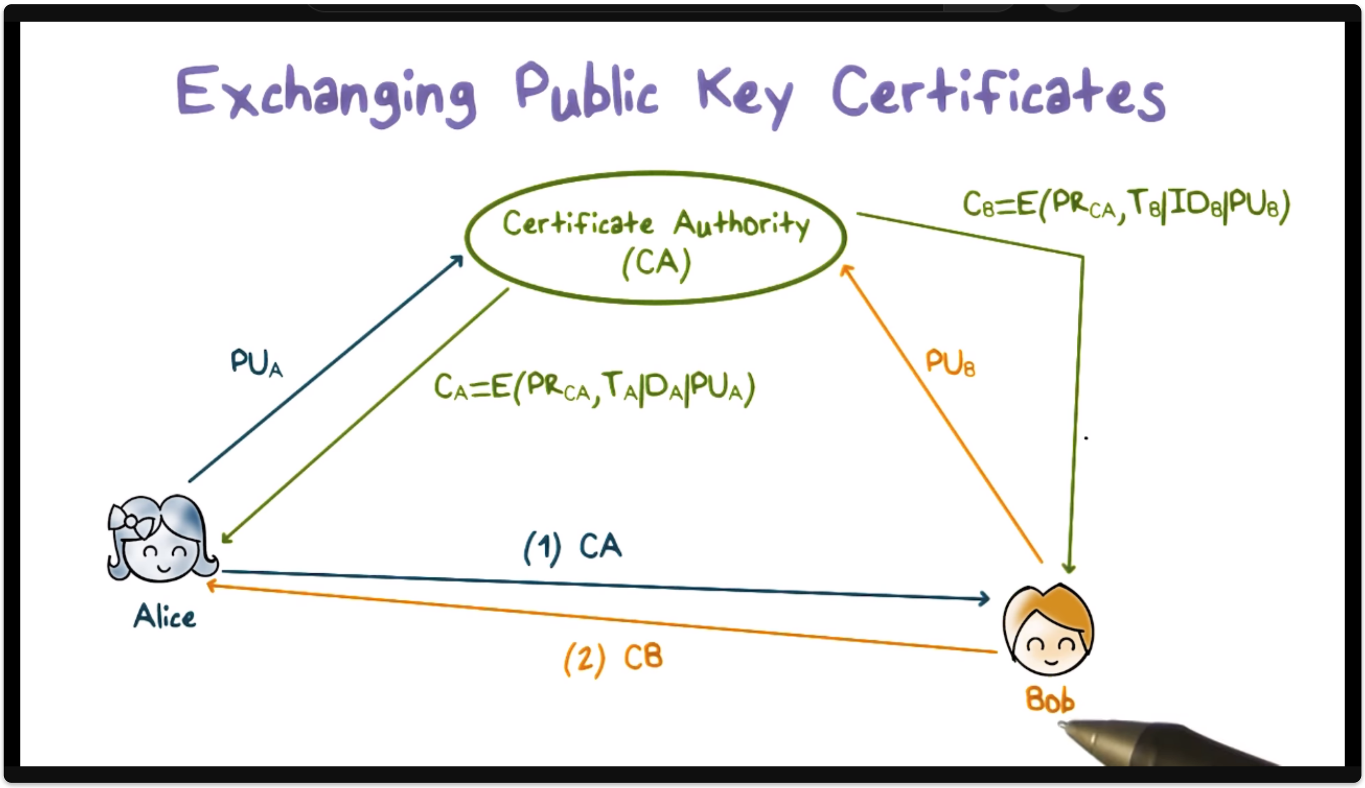
Digital Signature


Public Key Certificate
Unsigned certificate: contains user ID, user's public key, as well as information concerning the CA
H
Bob's ID Information
Bob's public key
CA information
Signed certificate
H
Recepient can verify signature by comparing hash code values
Generate hash code of unsigned certificate
E
D
Encrypt hash code with CA's private key to form signature
Decrypt signature with CA's public key to recover hash code
Create signed digital certificate
Use certificate to verify Bob's public key

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

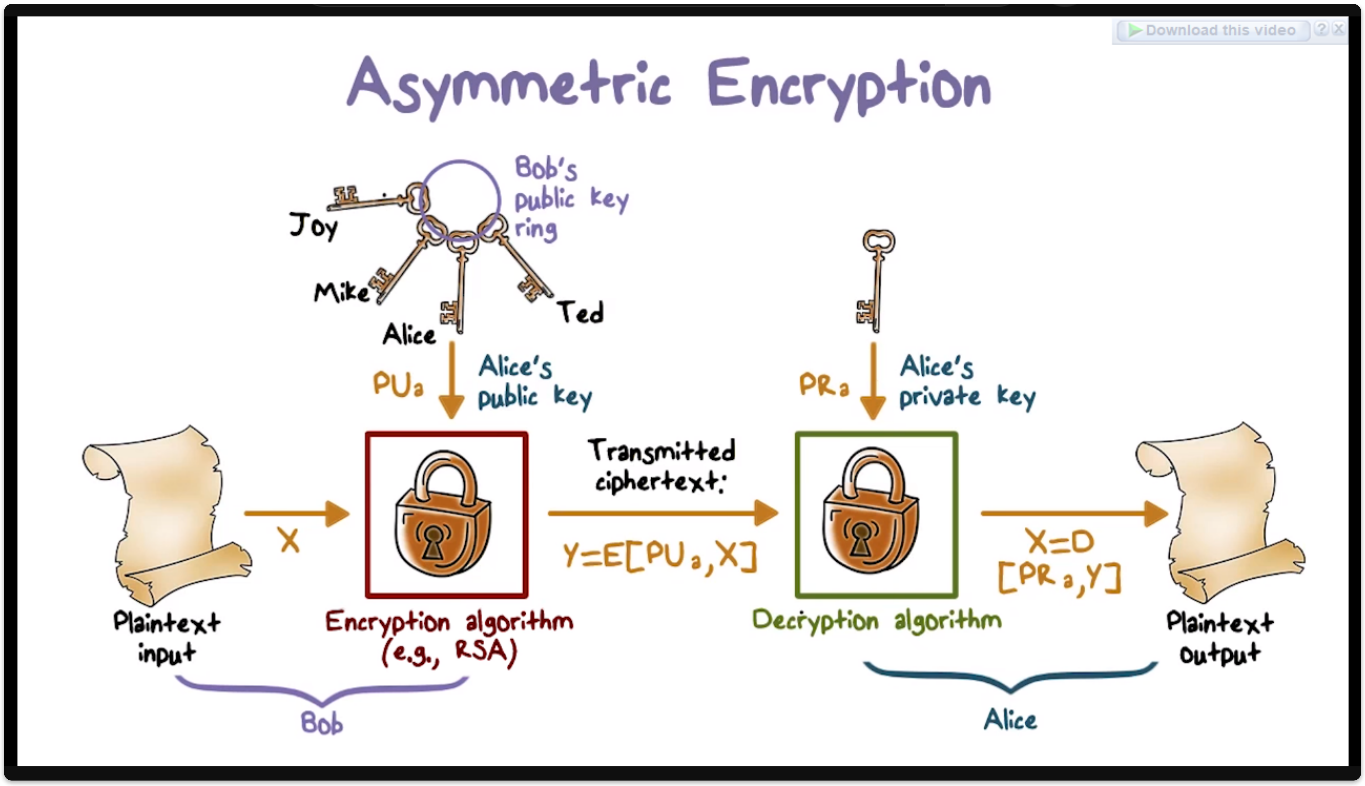

Exchanging Public Key Certificates
Certificate Authority (CA)
$C_B=E(PR_{CA},T_B|ID_B|PU_B)$
PU_A
$C_A=E(PR_{CA},T_A|D_A|PU_A)$
PU_B
(1) CA
Alice
(2) CB
Bob

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