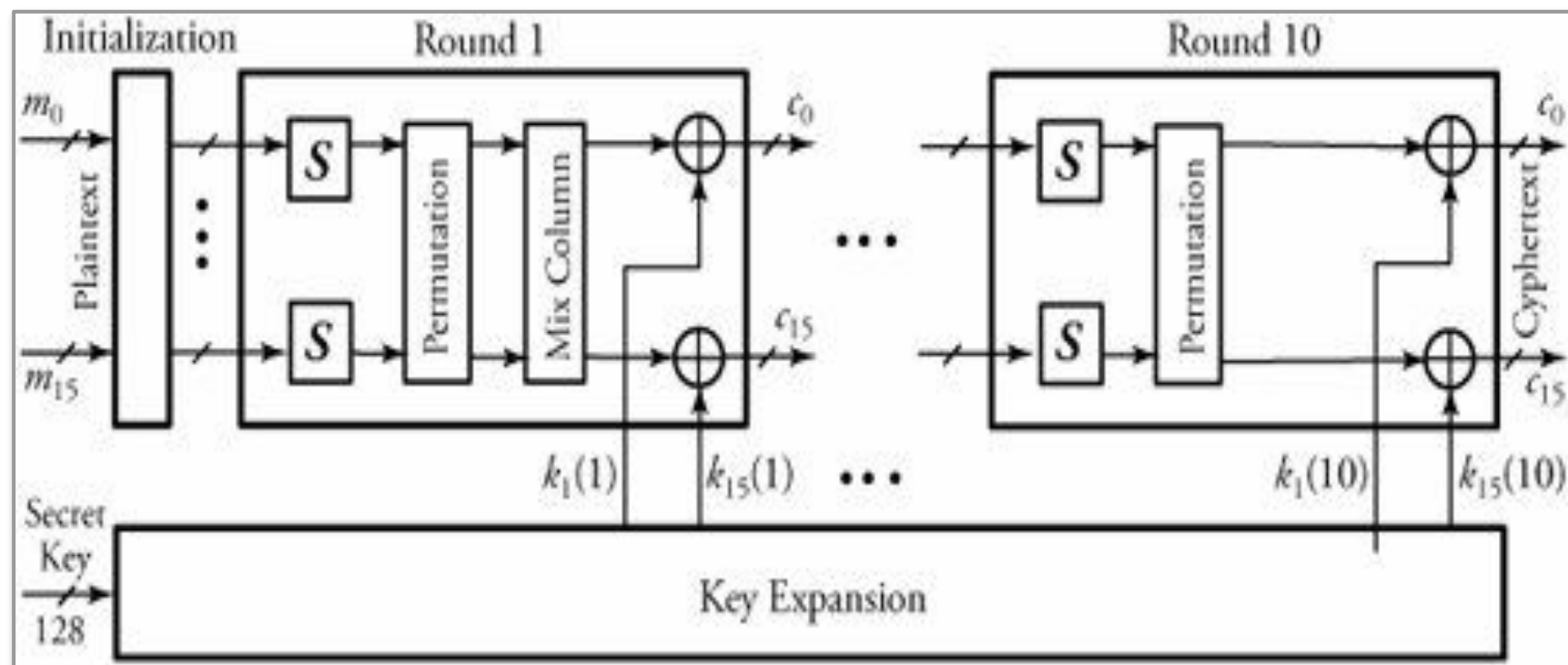





Advanced encryption Standard (AES)

- AES is a private key encryption algorithm
- AES supports 128 - bit symmetric block messages and uses 128, 192, or 256 - bit keys.
- The number of rounds in AES is variable from 10 to 14 rounds depending on the key and block sizes.
- Figure given below, illustrates the encryption overview of this protocol,
- using a 128 - bit key.



Overview of Advanced Encryption Standard (AES) protocol

- There are 10 rounds of encryptions for the key size of 128 bits.
- All rounds are identical except for the last round, which has no mix-column stage.
- A single block of 128-bit plaintext (16 bytes) as an input arrives from the left.
- The plaintext is formed as 16 bytes m_0 through m_{15} and is fed into round 1 after an initialization stage.
- In this round, substitute units indicated by S in the figure perform a byte-by-byte substitution of blocks.
- The ciphers, in the form of rows and columns, move through a permutation stage to shift rows to mix columns.

- 
- At the end of this round, all 16 blocks of ciphers are Exclusive-ORed with the 16 bytes of round 1 key $k_0(1)$ through $k_{15}(1)$.
 - The 128-bit key is expanded for ten rounds.
 - The AES decryption algorithm is fairly simple and is basically the reverse of the encryption algorithm at each stage of a round.

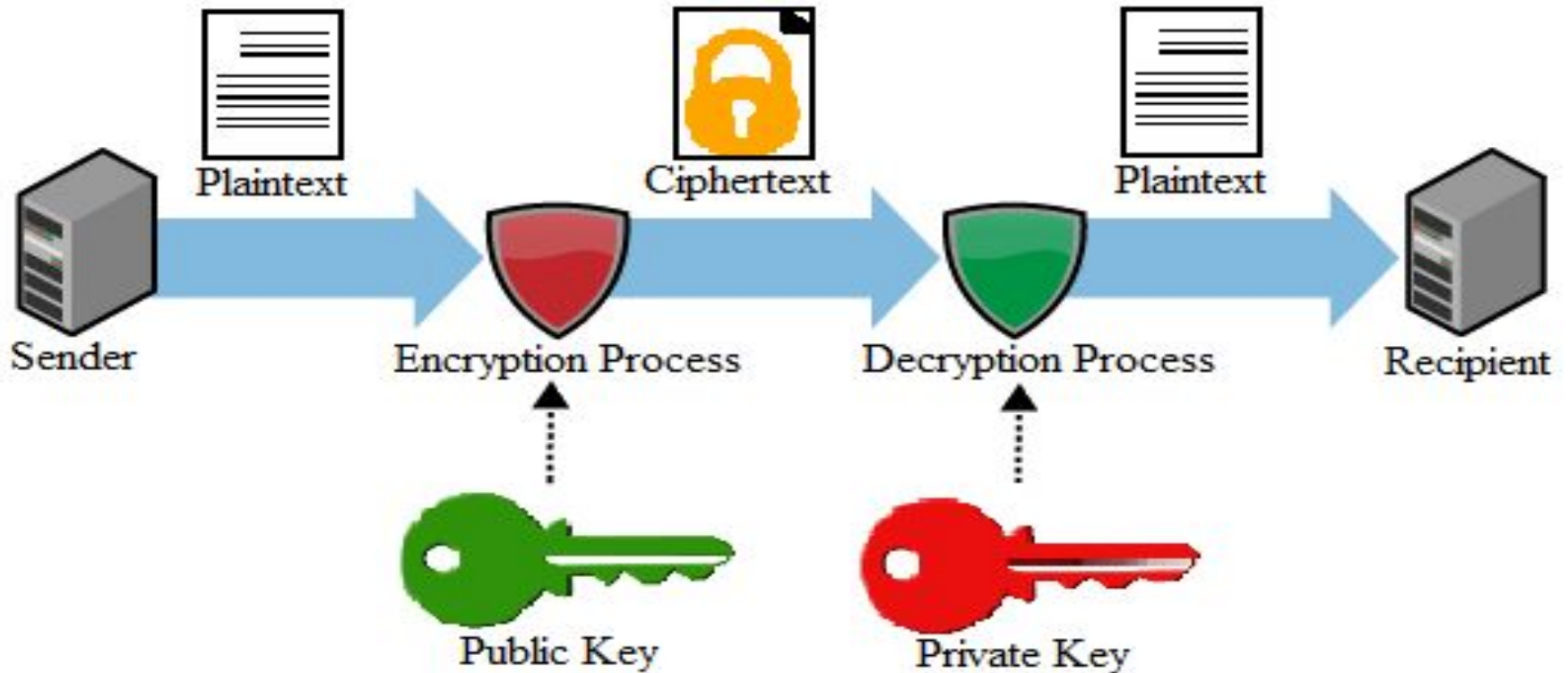


Exam Question:

Explain how to generate the cipher text using AES encryption algorithm?[10M]***

Public-Key Encryption Protocols


Public Key: encryption process



Public key encryption

- Public-key algorithm is based on mathematical functions rather than on substitution or permutation, although the security of any encryption scheme indeed depends on the length of the key and the computational work involved in breaking an encrypted message.
- In the public-key encryption methods, either of the two related keys can be used for encryption; the other one, for decryption.
- It is computationally infeasible to determine the decryption key given only the algorithm and the encryption key.
- . Each system using this encryption method generates a pair of keys to be used for encryption and decryption of a message that it will receive. Each system publishes its encryption key by placing it in a public register or file and sorts out the key as a public one.



- 
- A decorative graphic on the left side of the slide, consisting of several overlapping green triangles and quadrilaterals that create a 3D effect.
- Rivert, Shamir, and Aldeman (RSA) protocol
 - Diffie-Hillman key-exchange protocol.

RSA algorithm

- Assume that a plaintext **m** must be encrypted to a ciphertext **c**. The RSA algorithm has three phases for this: key generation, encryption, and decryption.
- **Key Generation Phase:** User generates Private and public keys in this step

Choose any two prime numbers p and q such that

- They are different.
- They are very large.

Calculate 'n' and totient function $\phi(n)$ where-

- $n = p \times q$
- $\phi(n) = (p-1) \times (q-1)$

Choose any value of 'e' such that-

- $2 < e < \phi(n)$
- $\gcd(e, \phi(n)) = 1$
- The public key = $\{e, n\}$

RSA algorithm

- Determine decryption key 'd' such that

$$ed = 1 \bmod \phi(n)$$

OR

$$d = \frac{1 + k \phi(n)}{e}$$

- You already know the value of 'e' and $\phi(n)$.
- Choose the least positive integer value of 'k' which gives the integer value of 'd' as a result.
- The private key = {d, n}
- Start substituting different values of 'k' from 1.

Encryption Phase:

- Sender represents the message to be sent as an integer between 0 and $n-1$.
- Sender encrypts the message using the public key of receiver.
- It raises the plain text message 'P' to the e^{th} power modulo n .
- This converts the message into cipher text 'C'.

$$\text{Ciphertext } C = P^e \bmod n$$

- The ciphertext 'C' is sent to the receiver over the communication channel.

Decryption Phase:

At receiver side,

- Receiver decrypts the cipher text using his private key.
- It raises the ciphertext 'C' to the d^{th} power modulo n .
- This converts the cipher text back into the plain text 'P'.

$$\text{Plain Text } P = C^d \bmod n$$

RSA Algorithm:

Link: https://www.youtube.com/watch?v=wXB-V_Keiu8 (Experimental solution for RSA-Understanding of How RSA works -in a simpler way) *****

Link: <https://www.youtube.com/watch?v=trkJnhFmKDE> (English)

Link: https://www.youtube.com/watch?v=QvDvM5l0lno&list=PLkLgTq6RIpMQKV1urc_1a-UJiyYpDOdua&index=110 (Hindi)

Question: 1. Explain working of RSA algorithm with an example
2. Solving a problem based on RSA algorithm

$$p=11, q=3 \quad m=2$$

$$n = p \times q = 11 \times 3 = \underline{\underline{33}}$$

$$\phi(n) = (p-1)(q-1) = 10 \times 2 = 20.$$

$$e: \gcd(e, \phi(n)) = 1$$

$$\boxed{e=3} \leftarrow \text{encryption key.}$$

$$d = e^{-1} \bmod \phi(n)$$

$$\text{or}$$

$$\underset{\substack{\uparrow \\ \text{int.}}}{d} = \frac{1 + k \times \phi(n)}{e}$$

$$\boxed{d=7} \leftarrow \text{decryption key.}$$

Encryption:

$$\begin{aligned} \text{Cipher text } C &= p^e \bmod n \\ &= 2^3 \bmod 33 \\ &= \underline{\underline{8}} \end{aligned}$$

Decryption:

$$\begin{aligned} \text{plaintext } P &= C^d \bmod 33 \\ &= 8^7 \bmod 33 \end{aligned}$$

$$\begin{aligned} &= \left[\frac{(8^2 \bmod 33) \times (8^2 \bmod 33) \times (8^2 \bmod 33) \times (8 \bmod 33)}{(8^2 \bmod 33)} \right] \bmod 33 \\ &= [31 \times 31 \times 31 \times 8] \bmod 33 \end{aligned}$$

$$= \underline{\underline{2}}$$

①

when $e=3$,

$$\gcd(3, 20) = 1$$

$$\text{So, } \boxed{e=3}$$

$$\frac{1 + 1 \times 20}{e} = \frac{21}{3}$$

$$= \underline{\underline{7}}$$

$$\boxed{d=7}$$



$$p=3, q=11 \quad M=00111011$$

$$n=33, \phi(n)=20, e=3, d=7.$$

divide M into blocks.

$$\text{block size } b = \log_2 33$$

$$\boxed{b=6}$$

$$\boxed{b = \log_2 n}$$

$$b_1 = 001110 \rightarrow m_1 = \underline{\underline{14}}$$

$$b_2 = 000011 \rightarrow m_2 = \underline{\underline{3}}$$

Encryption

$$\begin{aligned} C_1 &= m_1^e \bmod n \\ &= 14^3 \bmod 33 \\ &= \underline{\underline{5}} \end{aligned}$$

$$\begin{aligned} C_2 &= m_2^e \bmod n \\ &= 3^3 \bmod 33 \\ &= \underline{\underline{27}} \end{aligned}$$

Decryption:

$$\begin{aligned} m_1 &= C_1^d \bmod n \\ &= 5^7 \bmod 33 = 14 \end{aligned}$$

$$m_2 = C_2^d \bmod 33$$

$$p=3, q=5, m=9$$

$$n=15, \phi(n)=8$$

$$e \rightarrow \gcd(e, \phi(n))=1$$

$$e=3$$

$$d \rightarrow e^{-1} \bmod \phi(n)$$

or

$$\frac{1+k \times \phi(n)}{e}$$

$$d=3$$

$$C = q^3 \bmod 15 = 9$$

$$P = q^3 \bmod 15 = 9.$$

$$4. \quad p=5, q=7, m=11$$

$$n=35, \phi(n)=24$$

$$e=5, d=5.$$

$$C=11 \quad P=11$$

$$5. \quad p=5 \quad q=11 \quad m=5$$

$$n=55, \phi(n)=40$$

$$e=3, d=27.$$

$$C=15$$

$$\underline{\underline{P=5}}$$