Cryptography & Network Security Lab-6

In the cellular networks, if the Home Agent (HA) and Foreign Agent (HA) want to communicate with each other they first agree on a **Session-key**. Later, they can use this key for encryption and decryption operations. Implement the public key infrastructure to distribute the shared session-key between HA and FA using **Diffie-Hellman key exchange**. Subsequently, encrypt and decrypt messages between HA and FA using the shared session-key. The steps in Diffie-Hellman key exchange are listed below:

- HA and Fa must agree on two large prime numbers q and α. Where ($\alpha < q$).
- HA selects a private key $\mathbf{H_S}$ ($H_S < q$) and computes the public key $\mathbf{H_P = \alpha^{Hs} \bmod q}$ then sends the public key to FA
- Subsequently, FA picks a private key $\mathbf{F_S}$ ($H_S < q$) and computes the public key $\mathbf{F_P = \alpha^{Fs} \bmod q}$ then sends the public key to HA
- After that, HA computes the shared session key $\mathbf{K_{FH} = F_P^{HS} \bmod q}$ from FA's public key.
- Similarly, FA computes the shared session key $\mathbf{K_{FH} = H_P^{FS} \bmod q}$ from HA's public key.
- Finally, the shared session key $\mathbf{K_{FH}}$ is used to encrypt and decrypt the messages between FA and HA.

Expected Output:

Home Agent (HA):	**Foreign Agent (FA):**
Input primes q and α	Input primes q and α
Select the private key:	Select the private key:
Compute Public key:	Compute Public key:
Receive FA's Public key:	Receive HA's Public key:
Compute session-key: SK	Compute session-key: SK
Enter the plaintext M:	Enter the plaintext:10
Encrypted text **C: M+SK mod 26**	Decrypted text **M: C-SK mod 26**