CRYPTOGRAPHY CONCEPTS
CIA - 2

Team :

1. Tejaswini Uma Sudhir (21011102103)
2. Rohit VR (21011102109)

GitHub Repository :

https://github.com/tejucodes10/Crypto-Concepts-CIA2

Algorithm Implementation :

Diffie - Hellman Algorithm

Code :

Attached in the zip file as well as in the github repository

Algorithm :

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

1. Initialise the prime number `P` and primitive root `G`.
2. Alice chooses a private key `a`.
3. Bob chooses a private key `b`.
4. Alice calculates her public key `x` using the formula:
x = G^a mod P .
5. Bob calculates his public key `y` using the formula:
y = G^b mod P .
6. Alice and Bob exchange their public keys `x` and `y`.

7. Alice calculates the secret key `ka` using Bob's public key `y` and her private key `a` using the formula:
ka = y^a mod P .
8. Bob calculates the secret key `kb` using Alice's public key `x` and his private key `b` using the formula:
kb = x^b mod P .
9. Both Alice and Bob now have the same secret key `ka` and `kb`, which they can use for secure communication.
10. If `ka` is equal to `kb`, the Diffie-Hellman Key Exchange is successful.

Example:

Step 1: Alice and Bob get public numbers P = 23, G = 9

Step 2: Alice selected a private key a = 4 and Bob selected a private key b = 3

Step 3: Alice and Bob compute public values

Alice: x =(9^4 mod 23) = (6561 mod 23) = 6

Bob: y = (9^3 mod 23) = (729 mod 23) = 16

Step 4: Alice and Bob exchange public numbers

Step 5: Alice receives public key y =16 and Bob receives public key x = 6

Step 6: Alice and Bob compute symmetric keys

Alice: ka = y^a mod p = 65536 mod 23 = 9

Bob: kb = x^b mod p = 216 mod 23 = 9

Step 7: 9 is the shared secret.