Page No.
Date

Devanshu Surana
PC-23, Panel C
10322010755

ICS Lab A4

P.1 30/11/23

FAQ's

1. What is the discrete logarithmic problem?

Ans. It is a mathematical problem in the field of number theory and cryptography. It involves finding the exponent (the discrete logarithm) to which a given numbe (the base) must be raised to produce another given number within a finite mathematical group. It is considered difficult to solve, especially in large prime groups, and forms the basis of several crypto-graphic algorithms, including Diffie-Hellman and ElGamal encryption.

2. What is man in middle attack?

Ans. A man-in-the-middle (MiTM) attack is a type of cyber attack in which the attacker secretly inter-cepts and relays messages between two parties who believe they are communicating directly with each other.

3. Explain RSA Algorithm.

Ans. RSA algorithm is a asymmetric cryptography algorithm It is a widely used public key cryptography method that uses two keys (public and private) for encrypti-on and decryption, based on the mathematical difficulty of factoring large numbers.

Page No.
Date

RSA Algorithm:

Generating Public Key:
Select two prime no's
Suppose P = 53 and Q = 59
Now first part of public key
n = P * Q = 3127
We also need a small exponent say e:
e must be an integer
Not be a factor of $\phi(n)$
$1 < e < \phi(n)$ [$\phi(n)$ is discussed below]
let's consider it to be equal to 3.
Our public key is made of n and e.

Generating Private Key:
We need to calculate $\phi(n)$:
such that: $\phi(n) = (P-1)(Q-1)$
so, $\phi(n) = 3016$
Now calculate Private key d:
$d = (k * \phi(n) + 1)/e$ for some integer k.
for k = 2, value of d = 2011

Now we are ready with our public key (n = 3127 and e = 3) and private key (d = 2011). Now we will encrypt "HI".

Convert letters to numbers: H = 8 & I = 9
Thus encrypted data $c = (89^e) \bmod n$
Thus our encrypted data comes out to be 1394.
Now we will decrypt 1394:
Decrypted data = $(c^d) \bmod n$
Thus our Encrypted data comes out to be 89

8 = H and I = 9 i.e. "HI"