Name: Tejas Redkar

PRN: 1032210937

Panel - C

Roll No: PC-44

ICS Lab A4

* FAQ's

Q1) What is discrete logarithmic problem?

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

Q2) 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 intercepts & relys messages between two parties who believe they are communicating directly with each other.

Q3) Explain RSA algorithm

Ans RSA algorithm is an asymmetric cryptography algorithm that is widely used public key cryptography method that uses two keys(public & private) for encryption & decryption, based on the mathematical difficulty of factoring large numbers.

RSA Algorithm

Generating Public key:
Select two prime no.s suppose $P=53$ & $Q=59$ Now first part of public key
$n= p*Q = 3127$
We ~~need~~ 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]

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 same integer k
for $k=2$, value of
$d=2011$

Lets consider it to be equal to 3
Our public key is made of n & e

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

Convert letters to numbers
H=8 to 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 & I = 9 i.e. "HI".

A

1/12/23