| CIASSMAte |
|-----------|
| Date : |
| Page: |

Name: Tejas Redkar

PRN: 1032210937

Panel-C

ROILNO: PC-44

ICS Lab A4

FAOIS

Ans It is

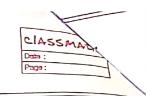
What is discrete logarithmic peroblem?

It is a mathematical peroblem in the yield of number theory & cryptography. It involves yinding the exponent (the discrete logarithm) to which a given number (the base) must be vaised to peroduce another given number within a finite mathematical group. It is considered difficult to wave, especially in large purime groups & forms the basis of several cryptographic algorithms, including diffier Hellman & ElGamal encuryption.

(05)

What is man in middle affack?

A man in the middle (Hi7M) affack is a type of cyber affack in which the affacker isocurably intercepts & welys messages between two parties who believe they are communicating divertly with each other.



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

RSA Algoreithm

Crenerating Purivate Koy: Generating Public key: We need to calculate Select two poume o(n) Such that 00.5 wuppose P=53& $= \phi(n) = (p-1)(0-1) = 0$ Q=59 Now Yivest part Q(n) = 3016of public key Now calculate Puivate n= p* Q - 3127 we need also need a d=(K*Q(n)+1)/e your small exponent saye same integer k e must be an integer york=2, value of Not be a factour of o (n) 1<e<p(n) [\phi(n) in discussed] d=2011

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

Now we are cready with our public key (n=3127 & e=3) & puivale key (d=201) Now we usill encoupt "HI".

Convert letters to numbers
H=8 to I=9

Thus encurypted Data C= (89°) mod n Thus our encurypted Data comes out to be 1394

Now we will decrypt 1394:

Decrypted Data = (ca) mod s

Thus our encoupped Data comes out to be 89

8=H & I=9 i.e. "no HI".

