Submitted by : SPOGMAI jan

Reg no :

2430-0081

Course :

Information security

Assignment no 3

Question no 1

Solution:-

The condition under which we always get M back is As we know

$$C = M^e \bmod n$$

Then $M = (M^e)^d \bmod n = M^{ed} \bmod n$

So if we take

$$ed = 1 \bmod (n)$$

We can get back our original message.

This means that

$$d = e^{-1} \bmod (n)$$

So if $d = e^{-1} \bmod (n)$ then we get back original message.

Question no 2

Solution:-

Give that $e = 13, n = 629, M = 3$

Required that find private keys

$\phi(n) = ?$

$d = ?$

$C = ?$

So $629 = 17 \times 37$

$\phi(n) = (17-1)(37-1) = 16 \cdot 36$

$= 576$

$ed = 1 \bmod \phi(n) \Rightarrow 13d = 1 \bmod 576 \Rightarrow$ using extended euclidean

$d = 133$

Now encrypting M = 3.

$C = M^e \bmod 629 = 3^{13} \bmod 629$

$C = 427$

So ciphertext = 437

Part b

1) To decrypt or find the private key an attacker must need d.

2) To find d the attacked must know $\phi(n)$ which depend on p and q.

3) Moder RSA uses 2048-bits or large number.

4) So $n \approx 2048$ probabilitgies.

5) So factoring this computationely impossible

So the main ~~reeson~~ resson due to which RSA algorithms are difficult to crack is.

1) factoring n is extremely hard due to high probabilitges.

2) Without $\phi(n)$ the private key cannobe computed.