# Information Security
## Class Participation

Alizeh Manzar
22F-3846
BCS-7B

## Question #1 :-

prime numbers : 17, 19

encrypt the plain text = 13

$p = 17, \quad q = 19$

$n = p \times q = 17 \times 19 = 323$

$\phi(n) = (p-1)(q-1) = 16 \times 18 = 288$

$e = 1 < e < \phi(n)$

$gcd(e, 288) = 1$, so $e = 7$

~~private~~ public key $< e, n > = (7, 323)$

$C = m^e \bmod n$

$C = 13^7 \bmod 323 = 276$

$M = c^d \bmod n$

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

$d = 247$

$M = 276^{247} \bmod 323$

$M = 13$

## Question # 2 :-

you are given RSA components

$n = 2537 \qquad n = 33$

$d = 937 \qquad d = 7$

$C = 855 \rightarrow$ encrypted using public key

$C = 16$

$M = c^d \bmod n$

$M = 16^7 \bmod 33$

$M = 25$

Question # 3 :-

$p = 17$ , $q = 23$

$M = 88$

$n = p \times q = 17 \times 23 = 391$

$\phi(n) = (p-1)(q-1) = 16 \times 22 = 352$

$e \Rightarrow 1 < e < \phi(n)$

$\gcd(e, 352) = 1$ , so $e = 3$

public key $< e, n > = < 3, 391 >$

$c = m^e \bmod n$

$c = 88^3 \bmod 391$

$c = 350$

$d \times e \bmod \phi(n) = 1$

$d = 235$

$M = c^d \bmod n$

$M = 350^{235} \bmod 391$

$M = 88$