10/06/'20

18DCE115

Date
Page 1

CE246 - DATABASE MANAGEMENT SYSTEM

KASHYAP SHAH
4CE2 => B-BATCH
COMPUTER ENGINEERING
9408718809

ANSWERS

Q1 P = 17
q = 13
e = 5
M = 7

RSA algorithm : It is used to implement Assignment cryptography.

$$n = P \times q$$
$$= 17 \times 13$$
$$= 221$$

$$\phi(n) = (P-1)(q-1)$$
$$= 16 \times 12$$
$$= 192$$

public key (e) = 5

$$de = 1 + k\phi(n)$$

$$d = \frac{1 + k\phi(n)}{e}$$

Let $k = 0$, $d = \frac{1+0}{5} = \frac{1}{5}$ → not proper

$k = 1$, $d = \frac{1+192}{5} = \frac{193}{5} = 38.6$ (not proper)

$k = 2$, $d = \frac{1+2(192)}{5} = \frac{1+384}{5} = \frac{385}{5} = 77$

∴ plain text = 7

For cipher Text = $E(M)$ cipher $= M^e \pmod n$

$= 7^5 \bmod 221$

$= 16807 \bmod 221$

$= 11$

$D(c)pt = c^9 \pmod n$

$= 11^{77} \pmod{221}$

Decryption = 7