Question

Q $p = 5$ $q = 7$ $m_1 = 10$ $m_2 = 20$

$u = 3$ $r_1 = 3$ $r_2 = 4$

$2 \mid 4, 6$

$2 \mid 2, 3$

$3 \mid 1, 3$

$n = 5 \times 7 = 35$

$g = 36$

$\lambda = 4, 6 \Rightarrow 12$

$$C_1 = \left(\underset{\bmod 35^2}{\underline{(36^{10} \cdot \bmod (35)^2)}} \cdot (3^{35} \cdot \bmod (35)^2) \right)$$

$\Rightarrow$

$36^{10} \cdot \bmod (35)^2 = 36^{10} \bmod$

$(36^5)(36^5) \bmod 1225 = 176 \cdot 176 = 30976 \bmod 1225$

Date : / /

$= 351$

- ~~3^{35}~~ 3^{35} . mod 1225

$(3^{20}) . (3^{15})$ mod 1225

$(751 . 482)$ mod 1225 $= 607$

(351×607) mod 1225

28 46354 $C_1 = 1132$

~~$C_2 = ((36^{20}$~~

$C_2 = ((36^{20}$ mod 1225$) . (4^{35}$ mod 1225$))$
mod 1225

$\Rightarrow 36^{20}$ mod 1225 $\Rightarrow (36^{10}) . (36^{10})$ mod 1225

$(351 . 351)$ mod 1225 $= 701$

4^{35} mod 1225 $\Rightarrow (576 . 1149)$ mod 1225
$= 324$

$(701 . 324)$ mod 1225 $= 499$

62 24 977 536

897560512

Page No.

Date : / /

$C_2 = 499$

$C = (C_1 \cdot C_2) \bmod 1225 = 143$

$x = C^{\lambda} \bmod n^2 \Rightarrow 143^{12} \bmod 1225$

$(143^6)\ (143)^6 \bmod 1225 = 351$

$x = 351$

$L_{(x)} = \frac{351 - 1}{n} = \frac{350}{35} = 10$

678 0377207

$m = 10 \cdot 3 \bmod \cancel{1225}\ 35$

$= \cancel{10}\ \cancel{30}\ 30$