Date

Activity 2 :-

Q.1 RSA algo is used to encrypt info 3 public key to decrypt msg is {7, 187}. Retrieve original msgs.

$C_1 = 16$, $C_2 = 24$

$PU = \{e, n\} = \{7, 187\}$

$e = 7$, $n = 187$

$n = p \times q$

$187 = 17 \times 11$

so

$p = 17$, $q = 11$

$\phi(n) = (17-1) \times (11-1)$

$= 16 \times 10 = 160$

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

$$d = \frac{(160 \times 1) + 1}{7} = 23$$

so $d = 23$

$PR = \{d, n\} = \{23, 187\}$

$M_1 = C_1^d \bmod n = 16^{23} \bmod 187$

$= [(16^8 \bmod 187) \times (16^8 \bmod 187) \times (16^4 \bmod 187) \times (16^2 \bmod 187) \times (16 \bmod 187)] \bmod 187$

$=$

$= 103$ ($86 \times 86 = 103$) ($69 \times 69 = 86$) ($16 \times 16 = 69$) (16)

$= (103 \times 103 \times 86 \times 69 \times 16) \bmod 187$

$= 1007260896 \bmod 187 = 169$

$M_2 = C_2^d \bmod n = 24^{23} \bmod 187 = 63$

Scanned with CamScanner

b.) Diffie-Hellman key exchange using prime 47 & generator 11.
Alice chooses secret 9 & Bob chooses secret 16.

$q=47,\ \alpha=11,\ X_A=9,\ X_B=16$

Generate public key:- $Y_A=\alpha^{X_A} \bmod q$

$=11^9 \bmod 47$

$=[(11^2 \bmod 47)\times(11^4 \bmod 47)\times(11^2 \bmod 47)\times(11 \bmod 47)] \bmod 47$

$\quad 27 \qquad 37 \qquad 27 \qquad 11$

$=(37\times27\times27\times11) \bmod 47$

$=39$

$Y_B=\alpha^{X_B} \bmod q=11^{16} \bmod 47=3$

Generate Secret key:-

$K=Y_B^{X_A} \bmod q=3^9 \bmod 47=37$ $\quad K=Y_A^{X_B} \bmod q=39^{16} \bmod 47=37$

$K=37$

Q.2 $p=7,\ q=11,\ e=7$

$n=p\times q=77$

$\phi(n)=(p-1)\times(q-1)=60$

$d=\frac{(60\times5)+1}{7}=\frac{301}{7}=43$

$PU=\{e,n\}=\{7,77\}$ $\quad$ Assume $M=2$

$C=M^e \bmod n=2^7 \bmod 77=51$ $\quad M=C^d \bmod n=51^{43} \bmod 77$

Scanned with CamScanner

Date

$[(51^{16} \bmod 77) \times (51^{8} \bmod 77) \times (51^{8} \bmod 77) \times (51^{4} \bmod 77) \times (51^{4} \bmod 77) \times (51^{2} \bmod 77) \times (51 \bmod 77)] \bmod 77$

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

$37 \quad 53 \quad 53 \quad 58 \quad 58 \quad 60 \quad 51$

$= (37 \times 37 \times 53 \times 60 \times 51) = 222024420 \bmod 77 = 2$

Q.3 $p = 61, q = 53, m = 10$; use RSA

$n = p \times q = 61 \times 53 = 3233$

$\phi(n) = 60 \times 52 = 3120$

$e = 7$

$d = \frac{(\phi(n) \times i) + 1}{e} = \frac{(3120 \times 4) + 1}{7} = 1783$

$PU = \{e, n\} = \{7, 3233\}$

$C = M^{e} \bmod n = 10^{7} \bmod 3233 =$

$[(10^{4} \bmod 3233) \times (10^{2} \bmod 3233) \times (10 \bmod 3233)] \bmod 3233$

$301 \quad 100 \quad 10$

$= (301000) \bmod 3233 = 331$

$C = 331$

$M = C^{d} \bmod n = 331^{1783} \bmod 3233 = 10$

b.) $p = 11, q = 13, e = 7, m = 9$; use RSA

$n = p \times q = 143$

$\phi(n) = 120$

$d = \frac{(120 \times 6) + 1}{7} = 103$

$C = M^{e} \bmod n = 9^{7} \bmod 143 = 48$

$M = C^{d} \bmod 143 = 48^{103} \bmod 143 = 9$

Scanned with CamScanner

Date

Q.4.a $p = 23, q = 5$

$p = 23, \alpha = 5, X_A = 2, X_B = 3$

$X_A = 2, X_B = 3$ — randomly generate

public key :-

$Y_A = \alpha^{X_A} \bmod p = 5^2 \bmod 23 = 2$ $\quad Y_B = \alpha^{X_B} \bmod p = 5^3 \bmod 23 = 10$

secret key :-

$K = Y_B^{X_A} \bmod p = 10^2 \bmod 23 = 8$

$K = Y_A^{X_B} \bmod p = 2^3 \bmod 23 = 8$

$K = 8$

b.) $p = 11, \alpha = 2, X_A = 5, X_B = 12$

public key :-

$Y_A = \alpha^{X_A} \bmod p = 2^5 \bmod 11 = 10$ $\quad Y_B = \alpha^{X_B} \bmod q = 2^{12} \bmod 11 = 4$

secret key :-

$K = Y_B^{X_A} \bmod p = 4^5 \bmod 11 = 1$ $\quad K = Y_A^{X_B} \bmod 11 = 10^{12} \bmod 11 = 1$

$K = 1$

Scanned with CamScanner