sheet (s)

Rabin crypto system (Public key encryption)

Choose large p,q satisfy

p ~~mod~~ $4 \equiv 3$

$q \bmod 4 \equiv 3$

Public: $N = p * q$

Encr:

$C = m^2 \bmod N$

Dec:

$m = \sqrt{C} \bmod N$

Solu

$mp = \sqrt{C} \bmod p = \pm C^{\frac{p+1}{4}} \bmod p$

$mq = \sqrt{C} \bmod q = \pm C^{\frac{q+1}{4}} \bmod q$

Prob 1

$p = 7 , q = 11 , C = 58 \Rightarrow m ?$ 1,2,3,4

$mp = \pm 58^2 \bmod 7 = \pm 4 \bmod 7$

$mc = \pm 58^3 \bmod 11 = \pm 5 \bmod 11$

$m_1 = [4 * 11 * (11^{-1} \bmod 7) + 5 * 7 * (7^{-1} \bmod 11)] \bmod 77$

$m_2 = [-4 * 11 * (11^{-1} \bmod 7) + 5 * 7 * (7^{-1} \bmod 11)] \bmod 77$

$m_3 = [4 * 11 * (11^{-1} \bmod 7) - 5 * 7 * (7^{-1} \bmod 11)] \bmod 77$

$m_4 = [-4 * 11 * (11^{-1} \bmod 7) - 5 * 7 * (7^{-1} \bmod 11)]$ "

$11 = 1*7 + 4$

$7 = 1*4 + 3$

$4 = 1*3 + 1$

$1 = 4 - 1*3$

$= 4 - 1*(7 - 1*4)$

$= 2*4 - 1*7$

$= 2*(11 - 1*7) - 1*7 = 2*11 - 3*7$

~~$= 3*7 + 2*11 - (11 - (1*7))$~~

~~$1 = 2*7 + 1*11$~~

$7^{-1} \bmod 11 = 8$, $N^{-1} \bmod 7 = 2$

$m_1 = [4*11*2 + 5*7*8] = 368 \bmod 77 = 60$

$m_2 = [-4*11*2 + 5*7*8] = 192 \bmod 77 = 38$

$m_3 = [4*11*2 + 5*7*8] = -192 \bmod 77 = 39$

$m_4 = [-4*11*2 - 5*7*8] = -368 \bmod 77 = 17$

$$f(x) = a x^2 + b x + \overset{\text{secret}}{M} \quad \text{mod } p$$

$(1,10) \Rightarrow 10 = a + b + M \quad \text{mod } 17 \rightarrow \textcircled{1}$

$(2,16) \Rightarrow 16 = 4a + 2b + M \quad \text{mod } 17 \rightarrow \textcircled{2}$

$(3,2) \Rightarrow 2 = 9a + 3b + M \quad \text{mod } 17 \rightarrow \textcircled{3}$

~~$4 * \textcircled{1} \Rightarrow 40 = 4a + 4b + 4$~~

$\textcircled{2} - \textcircled{1} \Rightarrow 6 = 3a + b \Rightarrow b = 6 - 3a$

sub in $\textcircled{3} \Rightarrow 2 = 9a + 3(6 - 3a) + M \quad \text{mod } 17$

$2 = \cancel{9a} + 18 - \cancel{9a} + M \quad \text{mod } 17$

$M = -16 \text{ mod } 17 = 1$ Secret

$10 = a + 6 - 3a + 1 \quad \text{mod } 17$

$3 = -2a \quad \text{mod } 17$

$\frac{3}{15} \text{ mod } 17 = a \Rightarrow a = 3 * 8 \text{ mod } 17$

$= 24 \text{ mod } 17 = 7$

$17 = 1 * 15 + 2$

$15 = 2 * 7 + 1$

$1 = 15 - 2 * 7$

$= 15 - 7 * (17 - 1 * 15)$

$= 15 - 7 * 17 + 8 * 15$

$= -7 * \underset{\rightarrow 0}{17} + 8 * 15$

$b = 6 - 3 * 7 \text{ mod } 17 = 6 - 21 \text{ mod } 17 = -15 \text{ mod } 17$

$= 2$