Tutorial -3

SOEN-321

Exercise-2 Problem-4.b

Find x that simultaneously satisfy the following congruent equations

b)

x≡2 mod 7

x≡3 mod 11

$n_1 = 7, n_2 = 11, \; \mathrm{n} = 7 \times 11$= 77
$m_1 = 11, m_2 = 7$

$y_1 = (11)^{-1} \mathrm{mod}\ 7 = 4^{-1} mod\ 7 = 2$
$y_2 = (7)^{-1} \mathrm{mod}\ 11 = 8$

$x = (2 \times 11 \times 2 + 3 \times 7 \times 8) mod\ 77 = 212\ mod\ 77$
$= 58$

Exercise-2 Problem-4.b (cont)

$4^{-1}\, mod\ 7$:

$7 = 1 \times 4 + 3$
$4 = 1 \times 3 + 1$
$1 = 4\ - 3$
$1 = 4 - (7 - 4) = -7 + 2 \times 4\, mod\ 7$
$1 = 2\ \times 4\, mod\ 7$

$7^{-1}\, mod\ 11$:

$11 = 1 \times 7 + 4$
$7 = 1 \times 4 + 3$
$4 = 1 \times 3 + 1$
$1 = 4\ - 3$
$1 = 4 - (7 - 4) = -7 + 2 \times 4$
$1 = -1 \times 7 + 2 \times (11\ - 7)$
$= 2 \times 11\ - 3 \times 7 mod\ 11$
$1 = -3 \times 7 mod\ 11$
$1 = 8 \times 7 mod\ 11$

Exercise-2 Problem 5

Consider an RSA system with p=7, q=11 and e=13. Find the plaintext corresponding to c=17.

$$\mathrm{n} = p \times q = 7 \times 11 = 77$$

$$\phi(n) = (p-1) \times (q-1) = 6 \times 10 = 60$$

$$\mathrm{d} = e^{-1}\, mod\ \phi(n) = 13^{-1}\, mod\ 60 = 37$$

$$\mathrm{m} = c^{d}\, mod\ n = 17^{37}\, mod\ 77 = 52$$

Exercise-2 Problem-5 (cont)

$13^{-1}\ mod\ 60$:

$60 = 3 \times 13 + 8$
$13 = 1 \times 8 + 5$
$8 = 1 \times 5 + 3$
$5 = 1 \times 3 + 2$
$3 = 1\ \times 2 + 1$
$1 = 3\ - 2$
$1 = 3 - (5 - 3) = 3 - 5 + 3 =\ 2 \times 3\ - 5$
$1 = 2\ (8\ - 5) - 5 = 2 \times 8\ - 2 \times 5\ - 5$
$1 = 2 \times 8 - 3 \times 5$
$1 = 2\ \times 8\ - 3\ (13\ - 8) = 5 \times 8\ - 3 \times 13$
$1 = 5(60\ - 4\ \times 13) - 3 \times 13 = 5\ \times 60\ - 23 \times 13$
$1 = -23\ \times 13\ mod\ 60$
$1 = 37\ \times 13\ mod\ 60$

$17^{37}\ mod\ 77$:

$37 = 100101$
$17^{37}\ =\ 17^{32}\ \times\ 17^{4}\ \times 17^{1}$
$17^{1}\ mod\ 77 = 17$
$17^{2}\ mod\ 77 = 58$
$17^{4}\ mod\ 77 = (58)^2\ mod\ 77 =\ 53$
$17^{8}\ mod\ 77 = (53)^2$ mod $77 = 37$
$17^{16}\ mod\ 77 = (37)^2\ mod\ 77 = 60$
$17^{32}\ mod\ 77 = (60)^2\ mod\ 77 =\ 58$
$17^{37}\ mod\ 77 = 58 \times 53 \times 17\ mod\ 77 = 52$

Exercise-2 Problem-6

Consider an RSA system in which the attacker knows that n1 and n2 has the form n1=pq1=16637 and n2=pq2=17399. Show how the attacker can break this system.

p , $\mathrm{q1}$, $\mathrm{q2}$ are prime numbers therefore $\gcd(\mathrm{pq1}, \mathrm{pq2}) = \mathrm{p}$

$\gcd(17399{,}16637)$:
$17399 = 1 \times 16637 + 762$
$16637 = 21 \times 762 + 635$
$762 = 1 \times 635 + 127$
$635 = 5 \times 127 + 0$

Thus p=127

q1= $\frac{17399}{127}$= 137 and q2= $\frac{16637}{127}$ = 131

The attacker can calculate RSA private key (and public key if needed)

Exercise-3 Problem-1(a)

Consider an RSA system with p=17, q=11 and e=3

a. Find m corresponding to c=156

b. Repeat part (a) above using the Chinese remainder theorem

p=17 q=11 e=3 c=156

$$m = c^d \ mod \ n$$
$$d = e^{-1} \ mod \ \phi(n)$$
$$n = pq = 17 \times 11 = 187$$
$$\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$$

$$d = 3^{-1} \ mod \ 160 = 107 \ mod \ 160$$
$$m = 156^{107} mod \ 187 = 7 \ mod \ 187$$

$\underline{3^{-1} \ mod \ 160}$

$$gcd(160, 3)$$
$$160 = 53 \times 3 + 1$$
$$1 = 160 - 53 \times 3 \ mod \ 160$$
$$1 = -53 \times 3 \ mod \ 160$$
$$1 = 107 \times 3 \ mod \ 160$$
$$3^{-1} \ mod \ 160 = 107$$

$\underline{156^{107} mod \ 187}$

$$107 = 1101011$$
$$156^1 = 156 \ mod \ 187$$
$$156^2 = 26 \ mod \ 187$$
$$156^4 = 115 \ mod \ 187$$
$$156^8 = 135 \ mod \ 187$$
$$156^{16} = 86 \ mod \ 187$$
$$156^{32} = 103 \ mod \ 187$$
$$156^{64} = 137 \ mod \ 187$$
$$156^{107} mod \ 187 =$$
$$156^1 \times 156^2 \times 156^8 \times 156^{32} \times 156^{64} =$$
$$156 \times 26 \times 135 \times 103 \times 137 = 7 \ mod \ 187$$

Exercise-2 Problem-1(b)

b. Repeat part (a) above using the Chinese remainder theorem

From part (a):

p=17 q=11 e=3 c=156 n=187 d=107

$$m_p = c^d \, mod \; p = 156^{107} \, mod \; 17$$
$$m_p = (156 \, mod \; 17)^{107 \, mod \, 16} \, mod \; 17$$
$$m_p = 3^{11} \, mod \; 17 = 7$$

$$m_q = c^d \, mod \; q = 156^{107} \, mod \; 11$$
$$m_q = (156 \, mod \; 11)^{107 \, mod \, 10} \, mod \; 11$$
$$m_q = 2^7 \, mod \; 11 = 7$$

<u>CRT:</u>

$$m \equiv m_p \, mod \; p$$
$$m \equiv m_q \, mod \; q$$

$$m = m_p \times y_1 \times m_1 + m_q \times y_2 \times m_2 \, mod \; n$$

$n_1 = 17$ $n_2 = 11$

$m_1 = 11$ $m_2 = 17$

$$y_1 = m_1^{-1} \, mod \; n_1 = 11^{-1} \, mod \; 17 = 14^*$$
$$y_2 = m_2^{-1} \, mod \; n_2 = 17^{-1} \, mod \; 11 = 2^*$$

$$m = 7 \times 14 \times 11 + 7 \times 17 \times 2 = 1316 \, mod \; 187$$
$$m = 7 \, mod \; 187$$

*Calculation steps in next slide >>

Exercise-2 Problem 1(b)

$\underline{17^{-1}\ mod\ 11}$
$17^{-1}\ mod\ 11 = 6^{-1} mod\ 11$
$11 = 6 \times 1 + 5$
$6 = 1 \times 5 + 1$

$1 = 6 - 1 \times 5$
$1 = 6 - 1 \times (11 - 6 \times 1) = 2 \times 6 - 11$ mod 11
$1 = 2 \times 6\ mod\ 11$

$\underline{11^{-1}\ mod\ 17}$
$17 = 1 \times 11 + 6$
$11 = 1 \times 6 + 5$
$6 = 1 \times 5 + 1$

$1 = 6 - 1 \times 5$
$1 = 6 - 1 \times (11 - 1 \times 6) = 2 \times 6 - 11$
$1 = 2 \times (17 - 1 \times 11) - 11 = 2 \times 17 - 3 \times 11\ mod\ 17$
$1 = -3 \times 11\ mod\ 17$
$1 = 14 \times 11\ mod\ 17$