Tutorial -3

SOEN-321

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

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

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

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

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

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

$$m_p = c^d \; mod \; p = 156^{107} \; mod \; 17$$
$$m_p = 3^{107} \; mod \; 17 = 7 *$$

$$m_q = c^d \; mod \; q = 156^{107} \; mod \; 11$$
$$m_q = 2^{107} \; mod \; 11 = 7 *$$

<u>CRT:</u>

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

$n_1 = 17$ $n_2 = 11$

$m_1 = 11$ $m_2 = 17$

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

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

*Calculation steps in next slide >>

Problem 1 (b) – Calculation Steps

$\underline{3^{107}\ mod\ 17}$

107=1101011
$3^1 = 3\ mod\ 17$
$3^2 = 9\ mod\ 17$
$3^4 = 13\ mod\ 17$
$3^8 = 16\ mod\ 17$
$3^{16} = 1\ mod\ 17$
$3^{32} = 1\ mod\ 17$
$3^{64} = 3\ mod\ 17$

$3^{107} = 3^1 \times 3^2 \times 3^8 \times 3^{32} \times 3^{64}\ mod\ 17$
$3^{107} = 3 \times 9 \times 16 \times 1 \times 1 = 432\ mod\ 17$
$3^{107} = 7\ mod\ 17$

$\underline{2^{107}\ mod\ 11}$

107=1101011
$2^1 = 2\ mod\ 11$
$2^2 = 4\ mod\ 11$
$2^4 = 5\ mod\ 11$
$2^8 = 3\ mod\ 11$
$2^{16} = 9\ mod\ 11$
$2^{32} = 4\ mod\ 11$
$2^{64} = 5\ mod\ 11$

$2^{107} = 2^1 \times 2^2 \times 2^8 \times 2^{32} \times 2^{64}\ mod\ 11$
$2^{107} = 2 \times 4 \times 3 \times 4 \times 5 = 480\ mod\ 11$
$2^{107} = 7\ mod\ 11$

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

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

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

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

Problem 2

Consider an RSA system with n=899. If the attacker knows that the system was (poorly) constructed using twin primes (i.e., p and q are twin primes). Show how that attacker can break this system.

$n = 899$

Twin primes => $q = p + 2$

$n = pq = p(p+2) = p^2 + 2p$
$p^2 + 2p - n = 0$
$899 = p^2 + 2p$
$p^2 + 2p - 899 = 0$

$p = 29$
$q = 29 + 2 = 31$

$$p = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$p = \frac{-2 \pm \sqrt{2^2 - 4 \times -899}}{2}$$

$$p = \frac{-2 \pm 60}{2}$$

$$p = 29 \; or \; \cancel{p = -31}$$

Problem 3

Consider an RSA system with n= 21311. Show how the attacker can factor n if she knows that Φ(n)=21000

$$n = pq \qquad q = \frac{n}{p}$$

$$\phi(n) = (p-1)(q-1) = (p-1)\left(\frac{n}{p} - 1\right)$$

$$\phi(n) = n - p - \frac{n}{p} + 1$$

-Multiply by p

$$p\phi(n) = np - p^2 - n + p$$

-Subtract pΦ(n)

$$np - p^2 - n + p - p\phi(n) = 0$$
$$p^2 - np - p + p\phi(n) + n = 0$$
$$p^2 + (\phi(n) - n - 1)p + n = 0$$
$$p^2 + (21000 - 21311 - 1)p + 21311 = 0$$
$$p^2 - 312p + 21311 = 0$$

$$p = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$p = \frac{312 \pm \sqrt{312^2 - 4 \times 21311}}{2}$$

$$p = \frac{312 \pm 110}{2}$$

$$p = 211 \ or \ p = 101$$

Problem 4

Consider an RSA system with n=143, e1=7 and e2=17. Suppose the same message m was sent to the two users above and the attacker observed the ciphertext c1=42 and c2=9. Show how the attacker can recover the message.

<u>Common modulus attack (Set 3 – Slide 24)</u>
Use extended euclidean algorithm to find a, b such that
$ae_1 + be_2 = 1$

$\underline{egcd(17,7)}$
$17 = 2 \times 7 + 3$
$7 = 2 \times 3 + 1$
$1 = 7 - 2 \times 3$
$1 = 7 - 2 \times (17 - 2 \times 7)$
$1 = 5 \times 7 - 2 \times 17$
$a = 5, b = -2$

$m = c_1^a \, c_2^b \; mod \; n$
$m = 42^5 \times 9^{-2} \; mod \; 143$

$42^5 \; mod \; 143 = 100$
$9^{-2} \; mod \; 143 = 16^2 \; mod \; 143 = 113$ *

$m = 100 \times 113 \; mod \; 143 = 25600 \; mod \; 143$
$m = 3 \; mod \; 143$

*Calculation steps for inverse in next slide

Problem 4 – Calculation steps

$9^{-2}\ mod\ 143 = (9^{-1})^2\ mod\ 143$

$\underline{9^{-1}\ mod\ 143}$
$143 = 15 \times 9 + 8$
$9 = 1 \times 8 + 1$

$1 = 9 - 1 \times 8$
$1 = 9 - 1 \times (143 - 15 \times 9) = 16 \times 9 - 143\ mod\ 143$
$1 = {\color{red}16} \times 9\ mod\ 143$