Tutorial -2

SOEN-321

Problem 1

The cryptanalyst observed the following plaintext/ciphertext pairs (p,c): (1,10) and (2,17).

$$C \quad = (\alpha P + \beta) \quad mod\ 26$$

$$10 \quad = (\alpha + \beta) \quad mod\ 26 \quad (1)$$

$$17 \quad = (2\alpha + \beta) \quad mod\ 26 \quad (2)$$

Subtract (2) – (1)

$$7 = \alpha\ mod\ 26 \rightarrow \alpha = 7$$

Substitute in (1)

$$10 = 1 \times 7 + \beta \ \ mod\ 26$$

$$3 = \beta\ mod\ 26 \qquad \rightarrow \quad \beta = 3$$

What is the ciphertext corresponding to the plaintext p=3:

$$c = 3 \times 7 + 3 \ \ mod\ 26$$

$$c = 24\ mod\ 26 \qquad \rightarrow \quad c = 24$$

Problem 2

Consider the Hill cipher in which the ciphertext is related to the plaintext using the form

$$(c_1 , c_2) = (p_1 , p_2) \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix} mod\ 26$$

The cryptanalyst observed the following plaintext/ciphertext pairs (p1 p2)/(c1 c2): (1 2)/(16 23) and (3 3)/(1 16). Determine the key corresponding to this system.

$$\begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} = \begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 \end{bmatrix} \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix} mod\ 26$$

$$\begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 \end{bmatrix}^{-1} \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

$$\frac{1}{p_1 p_4 - p_2 p_3} \begin{bmatrix} p_4 & -p_2 \\ -p_3 & p_1 \end{bmatrix} \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

Observed pairs: (p_1 , p_2) (c_1 , c_2)
(1 , 2) (16, 23)
(3 , 3) (1 , 16)

$$\begin{bmatrix} 16 & 23 \\ 1 & 16 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix} mod\ 26$$

Problem 2 (cont)

$$\frac{1}{3-6}\begin{bmatrix} 3 & -2 \\ -3 & 1 \end{bmatrix}\begin{bmatrix} 16 & 23 \\ 1 & 16 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

$$\frac{1}{23}\begin{bmatrix} 3 & 24 \\ 23 & 1 \end{bmatrix}\begin{bmatrix} 16 & 23 \\ 1 & 16 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

$$\frac{1}{23} = 23^{-1}\, mod\ 26 = 17\ mod\ 26$$

$$17\begin{bmatrix} 3 & 24 \\ 23 & 1 \end{bmatrix}\begin{bmatrix} 16 & 23 \\ 1 & 16 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

$$17\begin{bmatrix} 3 \times 16 + 24 \times 1 & 3 \times 23 + 16 \times 24 \\ 23 \times 16 + 1 \times 1 & 23 \times 23 + 16 \times 1 \end{bmatrix}$$
$$= \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

$$\begin{bmatrix} 1224 & 7701 \\ 6273 & 9265 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix} \text{ mod 26}$$

$$\begin{bmatrix} 2 & 5 \\ 7 & 9 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

Problem 2 (cont)

Multiplicative inverse

$1 = a \times b \bmod m$: we say a is multiplicative inverse of b

$\frac{1}{b} = b^{-1} = a$

To find a, use Extended Euclidean Algorithm between b and m

$GCD(23,26)$

$26 = 1 \times 23 + 3$

$23 = 7 \times 3 + 2$

$3 = 1 \times 2 + 1$

$1 = 3 - 2$

$1 = 3 - (23 - 7 \times 3)$

$1 = 8 \times 3 - 23$

$1 = 8\,(26 - 23) - 23$

$1 = 8 \times 26 - 9 \times 23\ mod\ 26$

$1 = -9 \times 23\ mod\ 26$

$1 = 17 \times 23\ mod\ 26$

Problem 3

$\gcd(621,345):$

$621 = 1 \times 345 + 276$
$345 = 1 \times 276 + 69$
$276 = 4 \times 69 + 0$

$\gcd(11316,1221):$

$11316 = 9 \times 1221 + 327$
$1221 = 3 \times 327 + 240$
$327 = 1 \times 240 + 87$
$240 = 2 \times 87 + 66$
$87 = 1 \times 66 + 21$
$66 = 3 \times 21 + 3$
$21 = 7 \times 3 + 0$

Problem 3 (cont)

$23^{-1}\ mod\ 67$:

$67 = 2 \times 23 + 21$
$23 = 1 \times 21 + 2$
$21 = 10 \times 2 + 1$
$1 = 21 - 10 \times 2$
$1 = 21 - 10 \times (23 - 21) = 11 \times 21 - 10 \times 23$
$1 = 11 \times (67 - 2 \times 23) - 10 \times 23 =$
$11 \times 67 - 32 \times 23\ mod\ 67$
$1 = -32 \times 23\ mod\ 67$
$1 = 35 \times 23\ mod\ 67$

$32^{-1}\ mod\ 167$:

$167 = 5 \times 32 + 7$
$32 = 4 \times 7 + 4$
$7 = 1 \times 4 + 3$
$4 = 1 \times 3 + 1$
$1 = 4 - 3$
$1 = 4 - (7-4) = -1 \times 7 + 2 \times 4$
$1 = -1 \times 7 + 2 \times (32 - 4 \times 7) = 2 \times 32 - 9 \times 7$
$1 = 2 \times 32 - 9 \times (167 - 5 \times 32)$
$= 47 \times 32 - 9 \times 167\ mod\ 167$
$1 = 47 \times 32\ mod\ 167$

Problem 3 (cont)

$\gcd(16,56):$

$56 = 3 \times 16 + 8$
$16 = 2 \times 8 + 0$

$\gcd(161,535):$

$535 = 3 \times 161 + 52$
$161 = 3 \times 52 + 5$
$52 = 10 \times 5 + 2$
$5 = 2 \times 2 + 1$
$2 = 2 \times 1 + 0$

Problem 3 (cont)

$161^{-1}\ mod\ 536$:

$536 = 3 \times 161 + 53$
$161 = 3 \times 53 + 2$
$53 = 26 \times 2 + 1$
$1 = 53 - 26 \times 2$
$1 = 53 - 26 \times (161 - 3 \times 53)$
$= -26 \times 161 + 79 \times 53$
$1 = -26 \times 161 + 79 \times (536 - 3 \times 161) =$
$79 \times 536 - 263 \times 161\ mod\ 536$
$1 = -263 \times 161\ mod\ 536$
$1 = 273 \times 161\ mod\ 536$

$16^{-1}\ mod\ 533$:

$533 = 33 \times 16 + 5$
$16 = 5 \times 3 + 1$
$1 = 16 - 3 \times 5$
$1 = 16 - 3 \times (533 - 33 \times 16)$
$= -3 \times 533 + 100 \times 16\ mod\ 533$
$1 = -1 \times 7 + 2 \times (32 - 4 \times 7) = 2 \times 32 - 9 \times 7$
$1 = 100 \times 16\ mod\ 533$

Problem 4.a

Find x that simultaneously satisfy the following congruent equations

a)

x≡3 mod 7
x≡5 mod 11
x≡9 mod 13

$n_1 = 7, n_2 = 11, n_3 = 13,\ \mathrm{n} = 7 \times 11 \times 13$=1001

$m_1 = 11 \times 13 = 143, m_2 = 7 \times 13 = 91, m_3 = 7 \times 11$ =77

$$y_1 = (11 \times 13)^{-1}\mathrm{mod}\ 7 = 3^{-1} mod\ 7 = 5$$
$$y_2 = (7 \times 13)^{-1}\mathrm{mod}\ 11 = 3^{-1} mod\ 11 = 4$$
$$y_3 = (7 \times 11)^{-1}\mathrm{mod}\ 13 = 12^{-1} mod\ 13 = 12$$

$$x = (3 \times 143 \times 5 + 5 \times 91 \times 4 + 9 \times 77 \times 12) mod\ 1001 = 2145 + 1820 + 8316\ mod\ 1001$$
$$= 269$$

Problem 4.a (cont)

$3^{-1}\ mod\ 7$:

$7 = 2 \times 3 + 1$
$1 = 7\ - 2 \times 3\ \ mod\ 7$
$1 = -2\ \times 3$
$1 = 5\ \times 3\ mod\ 7$

$3^{-1}\ mod\ 11$:

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

$12^{-1}\ mod\ 13$:

$13 = 1 \times 12 + 1$
$1 = 13\ - 1 \times 12\ \ mod\ 13$
$1 =\ - 1\ \times 12\ mod\ 13$
$1 = 12 \times 12 mod\ 11$

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
$m_1 = 11, m_2 = 7$

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

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

Problem 4.b (cont)

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

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

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

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

Problem 5

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

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

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

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

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

Problem 5 (cont)

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

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

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

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

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 $\mathrm{p}=127$

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

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