Tutorials 6

Cryptography

Question 1: CRT (two equations)

- Find an x that solves the following simultaneous congruences:

$$x \equiv 3 \pmod{7}$$
$$x \equiv 5 \pmod{9}$$

Q1 (solution)

9	7		
1	0	9	a
0	1	7	b
1	-1	2	$c = a - b$
-3	4	1	$d = b - 3c$

- Find α_1, α_2 by extended Eucli. Algo.

$$7(4) + 9(-3) = 1$$

- Substitute into formula for calculation

$$c \equiv a_1 m_2 \alpha_1 + a_2 m_1 \alpha_2 \pmod{m_1 m_2}$$

$$\begin{aligned} c &= 3(9)(-3) + 5(7)(4) \pmod{63} \\ &= -81 + 140 \pmod{63} \\ &= 59 \end{aligned}$$

Question 2: CRT (three equations)

- Find an x that solves the following simultaneous congruences:

$$x \equiv 1 \pmod{5}$$
$$x \equiv 3 \pmod{7}$$
$$x \equiv 6 \pmod{9}$$

Q.2 (solution)

a^{-1} is said to be a multiplicative inverse of $a \pmod n$ if
$$a\, a^{-1} \equiv 1 \pmod n.$$

- Define $M_i = \frac{M}{m_i}$, compute $\alpha_i = M_i^{-1}(mod\ m_i)$
  - $M_1 = 7\times 9 = 63, \alpha_1 = 63^{-1} = 2(mod\ 5)$
  - $M_2 = 5\times 9 = 45, \alpha_2 = 45^{-1} = -2 = 5(mod\ 7)$
  - $M_1 = 35, \alpha_3 = 35^{-1} = -1 = 8(mod\ 9)$

$$x \equiv 1 \pmod 5$$
$$x \equiv 3 \pmod 7$$
$$x \equiv 6 \pmod 9$$

Theorem: a has a multiplicative inverse modulo n iff

$$\gcd(a, n) = 1.$$

i.e. a and n are co-prime

$$63\times\alpha_1 \equiv 1(mod\ 5)$$
$$63\alpha_1 + 5k = 1$$

63	5		
1	0	63	a
0	1	5	b
1	12	3	$c = a - 12b$
-1	13	2	$d = b - c = -a + 13b$
2	-25	1	$e = c - d = 2a - 25b$

$$63\times 2 + 5\times(-25) = 1$$

Q.2 (solution)

- Define $M_i = \frac{M}{m_i}$, define $\alpha_i = M_i^{-1}(mod\ m_i)$
  - $M_1 = 7\times 9 = 63, \alpha_1 = 63^{-1} = 2(mod\ 5)$
  - $M_2 = 5\times 9 = 45, \alpha_2 = 45^{-1} = 5(mod\ 7)$
  - $M_1 = 35, \alpha_3 = 35^{-1} = 8(mod\ 9)$
- Substitute into formula $c = \sum_i a_i M_i \alpha_i$
  - $c = a_1 M_1 \alpha_1 + a_2 M_2 \alpha_2 + a_3 M_3 \alpha_3$

  $= 1\times 63\times 2 + 3\times 45\times 5 + 6\times 35\times 8(mod\ 5\times 7\times 9)$

  $= 2481(mod\ 315)$
- $x = 276$

Question 3: OTP

- The one-time pad encryption of plaintext cat (when converted from ASCII to binary) under key *k* is

10010100 10000111 01011100

a) What is the key *k*?

b) Is it secure if the same key is used to encrypt another 3-letter word? Why or why not?

Letter	ASCII Code	Binary
a	097	01100001
b	098	01100010
c	099	01100011
d	100	01100100
e	101	01100101
f	102	01100110
g	103	01100111
h	104	01101000
i	105	01101001
j	106	01101010
k	107	01101011
l	108	01101100
m	109	01101101
n	110	01101110
o	111	01101111
p	112	01110000
q	113	01110001
r	114	01110010
s	115	01110011
t	116	01110100
u	117	01110101
v	118	01110110
w	119	01110111
x	120	01111000
y	121	01111001
z	122	01111010

Q.3 (solution)

- The key can be obtained by taking XOR between the plaintext and the ciphertext:

```
01100011 01100001 01110100    (cat in ASCII)
10010100 10000111 01011100    (ciphertext)
-----------------------------------------
11110111 11100110 00101000
```

- It is insecure. For example, if hat is encrypted, the second and third bytes will be the same as the ciphertext of cat.

Question 4: Affine Cipher

Consider the encryption function as follows:

$$E(x) = ax + b \pmod{m}.$$

If the cipher is used to encrypt messages in English (i.e. an alphabet of 26 letters), then m is chosen as 26.

a) How can we ensure that decryption can be done?

b) What is the value of $\phi(26)$?

c) How many possible keys are there?

d) Suppose $a = 9$, $b = 6$, and the ciphertext (which contains only one single letter) is 20. Find the plaintext.

Q4 (solution)

$E(x) = ax + b \pmod{m}$.
$m = 26, a = 9, b = 6$

a) a and m are co-primes, so that a^{-1} exists. (see p.10)

b) $26 = \mathrm{p}\times q = 13\times 2$
$\phi(26) = (p-1)(q-1) = 12\times 1 = 12$

c) m=26. a and m are co-primes.
a: {1,3,5,7,9,11,15,17,19,21,23,25}
There are 12 possible values for a and 26 possible values for *b.*
Therefore the number of possible keys is $12\times 26 = 312$.

d) The encryption function for a single letter is $E(x) = ax + b \pmod{m}$
The decryption function is $\mathrm{D}(x) = a^{-1}(x-b) \pmod{m}$
For $a = 9,\ a^{-1} \equiv 3 \mod 26$.

$$9x + 6 = 20 \pmod{26}$$
$$x = 3(20-6) \pmod{26}$$
$$= 42 \mod 26$$
$$= 16$$

Question 5: RSA

Use the RSA algorithm to encrypt the message m represented by the decimal number 32 with $N = 85$ and $e = 61$.

a) Compute the ciphertext, C.

b) Factorize N, and check your answer in (a) by decryption.

- In practice, N is a very large number, so that factorization is extremely time consuming.

Q5 (solution)

1. To encrypt message M, Alice uses Bob's public key K_B^+: (N, e) to compute
$$C = M^e \pmod N$$

2. After receiving the ciphertext, Bob uses his private key K_B^-: (N, d) to compute
$$M' = C^d \pmod N$$

(a) Encryption

$$C = M^e \bmod N = 32^{61} \bmod 85$$

$$32^2 \equiv 4 \bmod 85$$
$$32^4 \equiv 16 \bmod 85$$
$$32^8 \equiv 1 \bmod 85$$
$$32^{16} \equiv 1 \bmod 85$$
$$32^{32} \equiv 1 \bmod 85$$

❖ **Encryption:**
M=32
N=85
e=61

❖ **Decryption:**
C=2
N=85
d=?

$$32^{61} (mod\ 85) = 32^{32} 32^{16} 32^{8} 32^{4} 32^{1} \pmod{85}$$
$$= 16 \times 32 \pmod{85} = 2$$

Q5 (solution)

M=32
C=2
e=61
N=85
d=?

(b) Decryption

- Generate 2 primes, p and q.
  Compute $N = p \times q$ and $\phi(N) = (p-1)(q-1)$
  - $N = p \times q \quad 85 = 5 \times 17.$
  - $\phi(N) = (p-1)(q-1) = 4 \times 16 = 64.$

- Solve the following equation to find **d**: $ed \equiv 1 \bmod \phi(N)$
  - $ed \equiv 1 \bmod 64$
    $61d \equiv 1 \bmod 64 \quad \Rightarrow \quad d = 21.$

61d+64k=1
d=21, k=-20

- Compute the decrypted message by $M' \equiv C^d (mod\ N)$
  - $M' = C^d \bmod N$
    $= 2^{21} \bmod 85$
    $= (2^5)^4(2) \bmod 85$
    $= (32^4)(2) \bmod 85$
    $= 16 \times 2 = 32 = M$