Tutorials 6

Cryptography

Question 1: CRT (two equations)

- Find an x that solves the following simultaneous congruences:

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

Question 2: CRT (three equations)

- Find an x that solves the following simultaneous congruences:

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 3 \pmod{7} \\ x &\equiv 6 \pmod{9} \end{aligned}$$

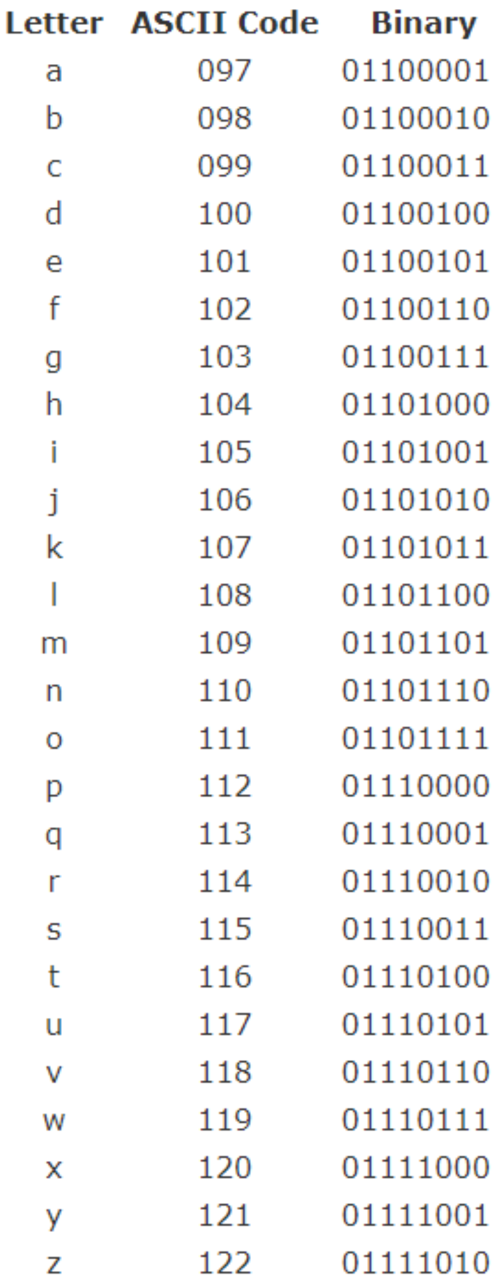
Question 3: OTP

- 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

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.

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.