Mathematics in the Real World
Math 107

Lectures 16 & 17: Introduction to cryptography. Modular arithmetics.

Introduction to cryptography. Cryptography studies methods of enciphering and deciphering texts. Suppose you have to transmit a secret message under a threat of it being intercepted by a third party. To avoid leaking the secret, the message needs to be disguised, or *enciphered*. A message to be transmitted is called a *plaintext* (the spaces and punctuation in the original message are usually omitted), a disguised message a *ciphertext*, the process of disguising *enciphering*, and the reverse process *deciphering*. A *cryptosystem* consists of a *key* to turn a plaintext message into a ciphertext, and an *inverse key* to turn a ciphertext into a plaintext message. The goal of a cryptosystem is to transfer a message in a way that only the designated destination party can read it. The goal of the *code-breakers* is the opposite: to decipher the message without knowing the key.

Cryptosystems are compared for their relative strength, or security - the ability to withstand code-breaker attacks. Known ciphers range from simple encodings, some of which we will discuss below, to very complicated and virtually unbreakable ones. Earlier in the course we have encountered a formidable example of a (hopefully) enciphered text, the Voynich Manuscript, written in an unknown language using an unknown alphabet that remains as yet undeciphered. Another famous manuscript dating from the eighteenth century, the Copiale Cipher, has been recently deciphered using methods of modern cryptography (see the *New York Times* article I uploaded). More recent historical examples include the cracking by the Allied code-breakers of the Enigma cipher, used by the Nazis during the World War II. In everyday experience, anyone shopping online relies on the strength of the Advanced Encryption Standard cryptosystem used in the Internet to transfer their credit card information.

The simplest example of a cipher is the *translation* cipher, where each letter of a plaintext is replaced by the letter standing n position further in the alphabet. If we are at the end of the alphabet, it is assumed that the letter following Z is A again, and so on, listing the alphabet in a *cyclic order*. For example, the *Caesar cipher* is a translation cipher with $n = 3$:

$$\begin{array}{cccccccc} A & B & C & D & \dots & X & Y & Z \\ \downarrow & \downarrow & \downarrow & \downarrow & \dots & \downarrow & \downarrow & \downarrow \\ D & E & F & G & \dots & A & B & C \end{array}$$

The key of this cipher is "shift by three to the right in the cyclic alphabetical order", and the inverse key "shift by three to the left in the cyclic alphabetical order". Both keys are represented by the scheme of mapping of the letters shown above.

Example 1. Decipher the message $PDWKLVDODQJXDJH$ written in the Caesar cipher. *Hint:* if your answer makes sense, it is correct!

Example 2. How many different translation ciphers can be made using the English alphabet? *Answer:* 25.

A generalization of a translation cipher is a *permutation cipher*, where each letter in the alphabet is assigned a "partner" letter with which it is replaced when enciphering a message. Each letter in the alphabet can be assigned one and only one partner. (For example, one cannot have $A \to X$ and $B \to X$.) The easiest way to describe a permutation cipher is by giving a permutation (a new order) of the letters in the alphabet. Then A corresponds to the first letter in the new sequence, B to the second and so on. The key of the cipher is given by the list of all 26 correspondences, or by a permutation of 26 letters. The inverse key is the same correspondence read in the opposite way. For example, the key

$$\begin{array}{cccccccccccccccccccccccccc} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ Q & W & E & R & T & Y & U & I & O & P & L & K & J & H & G & F & D & S & A & Z & X & C & V & B & N & M \end{array}$$

is used to encipher the plaintext message $CLOUDYSKY$ into $EKGXRNALN$. Note that all translation ciphers are special cases of the permutation ciphers, when the permutation is a cyclic shift of the alphabet.

Example 3. How many different permutation ciphers can be made using the English alphabet?

Solution: The number of different permutation ciphers equals to the number of different permutations of 26 letters, or ${}_{26}P_{26} = 26!$.

The number 26! is very large, but the security of a cryptosystem based on a permutation cipher is low. Any permutation cipher can be easily broken by a frequency analysis: matching ciphertext letters with plaintext letters according to their relative frequency of appearance in an English text.

To avoid this weakness, *polyalphabetic substitution ciphers* are used. Suppose that you have several lists of 26 symbols of any nature (a slavic alphabet, pairs of English letters, etc) and you use any of the lists randomly when replacing each letter of the plaintext message. Then any given English letter corresponds to several symbols and the frequency analysis is much harder to perform. For example, if $M \to TU$, $A \to LV$, $T \to KS$, $H \to LQ$ are some of the correspondancies in the first list and $M \to IS$, $A \to VS$, $T \to PA$, $H \to VN$ in the second list, then $MATH$ can be enciphered as any of the following strings:

$$TULVKSLQ, \quad TUVSKSVN, \quad ISLVPAVN, ...,$$

totally $2^4 = 16$ different strings of ciphertext. Provided the necessary keys, each ciphertext above can be deciphered unambiguously back to obtain the plaintext message $MATH$. In this case, the key consists of several ordered lists of 26 symbols and can become quite long.

Before we can go on, we need to introduce a new mathematical tool.

Modular arithmetics. This branch of mathematics deals only with integer numbers and studies their divisibility properties. For two integers a and n, a is *divisible* by n (or a is a multiple of n) if $a = nk$ for some integer k. For example, 14 is divisible by 2 and by 7 and it is not divisible by 3 or by 4.

Here is the definition that gives modular arithmetic its name: Let a, x be integers and n be a positive integer. We say that a is *congruent* to x *modulo* n if $(a - x)$ is divisible by n. The notation is

$$a \equiv x \mod n$$

In other words, $a \equiv x \mod n$ if a and x differ by a multiple of n. For instance, $25 - 4 = 21$ is a multiple of 7, so $25 \equiv 4 \mod 7$. Also, $30 - (-5) = 35$ is a multiple of 7, so $30 \equiv -5 \mod 7$. At the same time, $30 - 2 = 28$ is a multiple of 7 as well, therefore $30 \equiv 2 \mod 7$.

Modular arithmetic is widely used in everyday life without our ever knowing it. For example, what time is it, sixteen hours after 10 AM? We compute: $10 + 16 = 26$ but the time is measured in a 24 hour cycle, so to find the time of the day we can subtract any multiple of 24: $26 - 24 = 2$ AM. In other words,

$$(10 + 16) \equiv 2 \mod 24.$$

Example 4. What time is it a hundred hours from noon?
Solution: We see that $100 = 4 \cdot 24 + 4$, in other words $100 \equiv 4 \mod 24$. Disregarding the four complete days, we just say: 4 hours after noon, or 4 PM.

Example 5. Find the number $0 \leq x \leq 15$ such that $78 \equiv x \mod 15$.
Solution: $15 \cdot 5 = 75$ is the closest multiple of 15 to 78 which is less than 78. We have $78 - 75 = 3$, therefore $78 \equiv 3 \mod 15$, and $x = 3$.

The following properties of modular congruences are the "same" as those of the usual equalities. They come very useful in solving problems. Suppose

$$a \equiv x \mod n \quad \text{and} \quad b \equiv y \mod n$$

Attention: n is the same in both formulas! Then

$$(a + b) \equiv (x + y) \mod n, \quad (a - b) \equiv (x - y) \mod n, \quad ab \equiv xy \mod n.$$

Let us for example prove the last property. By definition of the congruences, we have $a = nk + x$ and $b = nm + y$, where m and k are some integers. Then $ab = (nk + x)(nm + y) = n^2km + nmx + nky + xy = n(nkm + mx + ky) + xy$. Therefore,

the products ab and xy differ by a multiple of n, which by definition implies $ab \equiv xy \mod n$.

The last property means that we can multiply congruences modulo the same number. In particular, we can consider powers of a congruence: if s is any positive integer, and $a \equiv x \mod n$, then the following holds as well:

$$a^s \equiv x^s \mod n.$$

Attention: in general, you cannot divide congruences. We have $24 \equiv 3 \mod 7$ and $12 \equiv 5 \mod 7$, but $\frac{24}{12} = 2 \equiv 2 \mod 7$. In particular, $\frac{3}{5} \neq 2$ is not an integer.

Example 6. For example, what time is it, 10,000 hours from noon? We saw above that $100 \equiv 4 \mod 24$, so $10,000 \equiv 100^2 \equiv 4^2 \equiv 16 \mod 24$. (Though 4^2 actually *equals* 16, we write $4^2 \equiv 16$ since we are working modulo 24.) So the answer is: 16 hours past noon, or, 4 AM.

Example 7. What is 10^{17} modulo 9?
Solution: $10 \equiv 1 \mod 9$, therefore $10^{17} \equiv 1^{17} \equiv 1 \mod 9$.

Example 8. Find $-785 \mod 14$.
Solution: Divide -785 by 14 to get $\simeq -56.07$. Therefore, the closest multiple of 14 to 785 is $14 \cdot (-56) = -784$. We have $-785 \equiv -784 - 1 \equiv -1 \mod 14$. Equivalently, we can write $-785 \equiv 13 \mod 14$. (This only works with integers small enough to be handled with exact precision by a calculator).

Example 9. Find $3^{514} \mod 26$.
Solution: Here we cannot compute the result of the division of 3^{514} by 26 with any adequate precision. Instead let us calculate some powers of 3:

$$3^2 \equiv 9 \mod 26, \quad 3^3 \equiv 27 \equiv 1 \mod 26$$

This last equation is very useful because we see that any power of 27 is congruent to 1 modulo 26. Now, $514 = 3 \cdot 171 + 1$, therefore

$$3^{514} = 27^{171} \cdot 3 \equiv 1^{171} \cdot 3 \equiv 3 \mod 26.$$

Example 10. What is the last digit of 12^{50}?
Solution: The last digit of an integer k is $k \mod 10$ (Because the number k minus its last digit is a multiple of 10). So we need to compute $12^{50} \mod 10$. We have $12 \equiv 2 \mod 10$, therefore $12^{50} \equiv 2^{50} \mod 10$. Now, for 2^{50} we note that $2^4 = 16 \equiv 6 \mod 10$. This is useful because the last digit of any power of 6 is 6. Then $2^{48} \equiv (2^4)^{12} \equiv 6^{12} \equiv 6 \mod 10$. We have $2^{50} = 2^{48} \cdot 2^2 \equiv 6 \cdot 4 \equiv 24 \equiv 4 \mod 10$. Finally, $12^{50} \equiv 2^{50} \equiv 4 \mod 10$. Answer: the last digit is 4.

Modular mathematics in cryptography. Now going back to cryptography, let us reconsider the translation cipher. It is easy to see that it can be represented easily using modular arithmetic. Enumerate the letters of the alphabet by integers from 0 to 25. Then the Caesar cipher replaces a letter with number n in the alphabet by the

letter with number $(n+3) \mod 26$. We have to add " $\mod 26$" to account for the cyclic order that we are using: then for example the letter number 24, which is Y, is mapped to the letter number $(24+3) \equiv 27 \equiv 1 \mod 26$, and we obtain the letter B. The key of the Caesar cipher is given by "$+3 \mod 26$", and the inverse key by "$-3 \mod 26$".

In many polyalphabetic ciphers with multiple keys, the choice of the key is not random, but determined by the position of the character within the plaintext message. If each of, say, m keys is applied periodically to each mth letter of the plaintext, it is called a *periodic substitution cipher* of period m. A simple example of a periodic substitution cipher is the *Vigenère cipher*: in this case each of the keys is a translation by a fixed number of positions in the cyclic alphabetic order. Consider for example the Vigenère cipher with period 5 and keys $(+15, +1, +2, +3, +4) \mod 26$. This means that the enciphering replaces the first letter in the plaintext by the one 15 positions to the right in the alphabet, the second by the one following it in the alphabet, the third by the letter 2 positions to the right, the fourth by 3, and the fifth by 4. Then again, the sixth letter is replaced by the one 15 positions to the right, the seventh by the letter following it in the alphabet, the eighth by the letter shifted by 2 positions and so on.

Example 11. Using the Vigenère cipher with the key $(+15, +1, +2, +3, +4) \mod 26$, encipher the plaintext

$$DESTROYANDFORGET$$

First we encode the plaintext as a string of numbers from 0 to 25 according to the alphabetical order and space them in groups of 5 (since the period of the key is 5):

$$3, 4, 18, 19, 17, \quad 14, 24, 0, 13, 3, \quad 5, 14, 17, 6, 4, \quad 19$$

Now write the periodic key under the string of numbers and perform addition **modulo** 26:

3	4	18	19	17	14	24	0	13	3	5	14	17	6	4	19
+15	+1	+2	+3	+4	+15	+1	+2	+3	+4	+15	+1	+2	+3	+4	+15
18	5	20	22	21	3	25	2	16	7	20	15	19	9	8	8

Converting the obtained string back into letters, we get:

$$SFUWVDZCQHUPTJII$$

Note that the first E in the plaintext is enciphered as F, and the second as I. Moreover, I stands for both E and T in the ciphertext. This shows that although the enciphering and deciphering (if you know the key) with the Vigenère cipher is easy to perform, it provides a good protection from a direct frequency analysis attack. It also has an advantage of being easily converted into a machine algorithm. In fact, the Enigma cipher, though more complicated than the Vigenère cipher, was also an example of an automatized polyalphabetic cipher.

Public key exchange. As another example of application of modular arithmetic in cryptography, let us consider the *Diffie-Hellman key exchange*. For two parties to exchange secret messages, it is necessary to agree on a cryptosystem and have a common key. But how to secretly exchange a key? Say, Thing1 and Thing2 want to exchange secret messages using a cipher whose key can be represented as a single number (virtually anything can be represented as a single number, think why ☺). They don't want anyone else to know what that number is. The Diffie-Hellman algorithm goes as follows:

(1) Thing1 and Thing2 openly exchange two numbers, say g and p.
(2) Thing1 secretly chooses number x_1. Thing2 secretly chooses number x_2.
(3) Thing1 computes $y_1 = g^{x_1} \mod p$. Thing2 computes $y_2 = g^{x_2} \mod p$. They openly exchange the results: now Thing1 knows y_2 and Thing2 knows y_1.
(4) Thing1 computes $y_2^{x_1} \mod p$ and Thing2 computes $y_1^{x_2} \mod p$. These numbers are equal and it is an integer between 0 and $p-1$. This number is their **common secret key** K.

First, let us see why the numbers $y_2^{x_1} \mod p$ and $y_1^{x_2} \mod p$ are equal. We have

$$y_2^{x_1} \equiv (g^{x_2})^{x_1} \equiv g^{x_1 \cdot x_2} \equiv g^{x_2 \cdot x_1} \equiv (g^{x_1})^{x_2} \equiv y_1^{x_2} \mod p$$

Therefore, $K \equiv y_2^{x_1} \equiv y_1^{x_2} \mod p$ is indeed a common key.

Now, why is this secure? The third party could have seen the following information: g, p, y_1, y_2. This information does not allow to compute the common key $g^{x_1 \cdot x_2} \mod p$. If Thing1 and Thing2 openly exchanged g^{x_1} and g^{x_2}, then knowing g, it would be easy to find x_1 and x_2. But they only made public y_1 (and y_2) which equals g^{x_1} (and g^{x_2}) up to an unknown multiple of p. As of today, there are no efficient algorithms to find x_1, x_2, or the common key K, based on this information. To make the exchange secure, a large prime number should be taken for p, and sufficiently large powers x_1 and x_2 chosen.

Example 12. Suppose $p = 13$, $g = 4$, $x_1 = 80$, $x_2 = 29$. Compute y_1, y_2 and the common key K according to the Diffie-Hellman algorithm.
Solution: First we try to find a power of g that is close enough (ideally differ by 1) to a multiple of p. We have $4^2 = 16 \equiv 3 \mod 13$, $4^3 \equiv 3 \cdot 4 \equiv 12 \equiv (-1) \mod 13$. Then $4^6 \equiv (-1)^2 \equiv 1 \mod 13$. So any number of the form 4^{6k} is congruent to 1 modulo 13. Then to find $y_1 = g^{x_1} \mod p$ and $y_2 = g^{x_2} \mod p$, we write

$$4^{80} = 4^{78} \cdot 4^2 = 4^{6 \cdot 13} \cdot 16 \equiv 1 \cdot 16 \equiv 3 \mod 13.$$

$$4^{29} = 4^{24} \cdot 4^5 = 4^{6 \cdot 4} \cdot 4^5 \equiv 1 \cdot 4^5 \equiv 4^3 \cdot 4^2 \equiv (-1) \cdot 3 \equiv -3 \equiv 10 \mod 13.$$

Therefore, $y_1 = 3$, $y_2 = 10$.
Now for the common key $K = y_1^{x_2} \mod p$ we have

$$K \equiv 3^{29} \mod 13.$$

We have $3^3 \equiv 27 \equiv 1 \mod 13$, therefore

$$3^{29} \equiv 3^{27} \cdot 3^2 \equiv (3^3)^3 \cdot 9 \equiv 1 \cdot 9 \equiv 9 \mod 13.$$

Therefore, $K = 9$.