

# **Modular Arithmetic and Cryptography<sup>1</sup>**

**Math 435 Spring 2008**

**University of North Dakota**

## **Section 1 Introduction**

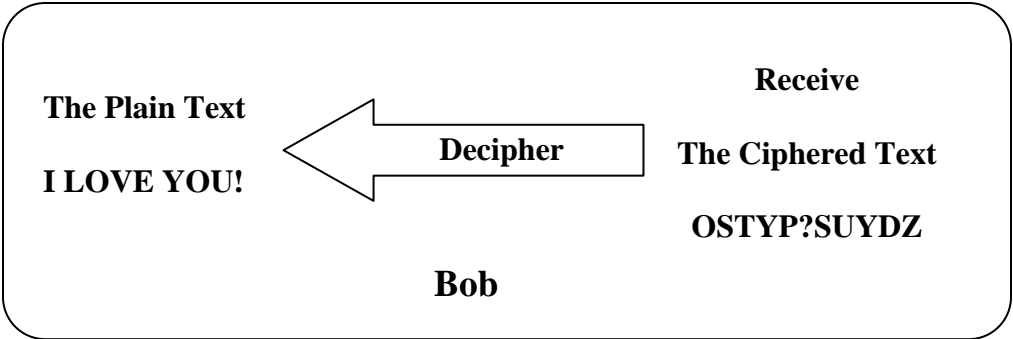
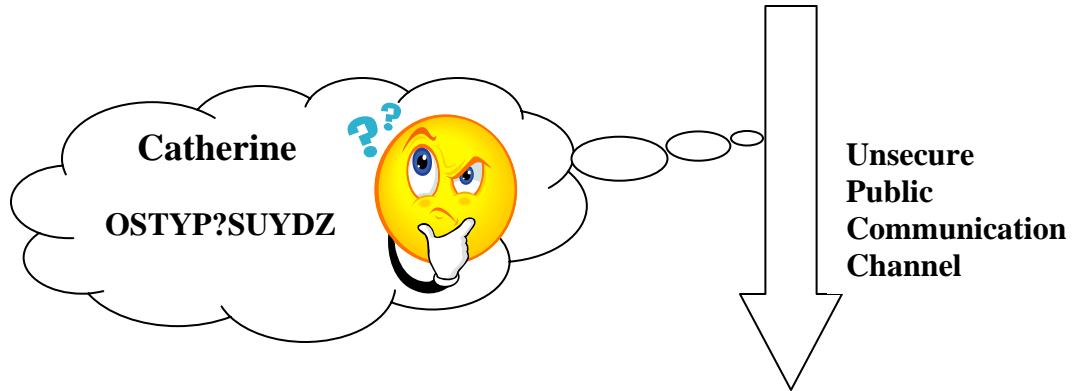
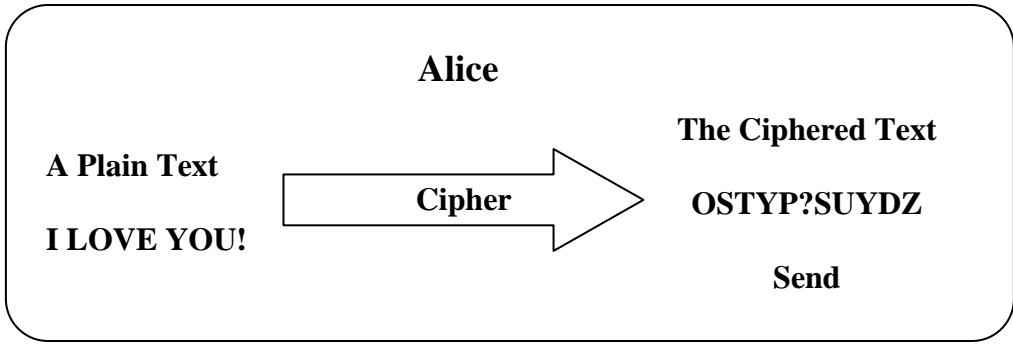
In this short note, we will study the use of modular arithmetic in cryptography.

Alice wants to send a secret message to Bob through an unsecure communication channel without revealing the message to the eavesdropper Catherine. Since the communication channel is not secure, Catherine can obtain any information that is sent by Alice to Bob. Hence, Alice must cipher (disguise) the message before sending it and Bob must decipher the ciphered message which he receives. Thus, Alice and Bob must share some information required for ciphering and deciphering. Moreover, this information cannot be shared with Catherine.

How can we use modular arithmetic to develop a cryptosystem which enables Alice and Bob to exchange secret messages without revealing them to Catherine?

---

<sup>1</sup> Comments should be addressed to [shuzo.takahashi@und.nodak.edu](mailto:shuzo.takahashi@und.nodak.edu).



<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>	<b>F</b>	<b>G</b>	<b>H</b>	<b>I</b>	<b>J</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>
<b>K</b>	<b>L</b>	<b>M</b>	<b>N</b>	<b>O</b>	<b>P</b>	<b>Q</b>	<b>R</b>	<b>S</b>	<b>T</b>
<b>11</b>	<b>12</b>	<b>13</b>	<b>14</b>	<b>15</b>	<b>16</b>	<b>17</b>	<b>18</b>	<b>19</b>	<b>20</b>
<b>U</b>	<b>V</b>	<b>W</b>	<b>X</b>	<b>Y</b>	<b>Z</b>	<b>.</b>	<b>!</b>	<b>?</b>	
<b>21</b>	<b>22</b>	<b>23</b>	<b>24</b>	<b>25</b>	<b>26</b>	<b>27</b>	<b>28</b>	<b>29</b>	<b>30</b>

## Section 2 A Linear Cryptosystem

In this section, we will study a simple linear cryptosystem based on modular arithmetic. Consider a reduced residue system mod 31,  $R_{31} = \{1, 2, \dots, 29, 30\}$ . A sentence is translated into a sequence of numbers in  $R_{31}$ , using the above table. (Note that a blank space is translated into the number 30.) Each number in the sequence is ciphered and deciphered by using the following functions.

**Definition** (Linear Ciphering and Deciphering Transformations)

Let  $k$  be a number in  $R_{31}$ . This number is called a key.

A linear ciphering transformation is a function  $C_k : R_{31} \rightarrow R_{31}$  defined by

$$C_k(x) \equiv kx \pmod{31}.$$

Let  $\ell$  be the number in  $R_{31}$  such that  $\ell k \equiv 1 \pmod{31}$ .

A linear deciphering transformation is a function  $D_\ell : R_{31} \rightarrow R_{31}$  defined by

$$D_\ell(x) \equiv \ell x \pmod{31}.$$

**Example** Suppose that Alice and Bob want to communicate using a common key  $k = 12$  (and so  $\ell = 13$  because  $13 \cdot 12 \equiv 1 \pmod{31}$ ), but Catherine does not know their common key. Alice wants to send a plain text WHAT? to Bob.

**Alice does the following:**

- (1) She translates the text WHAT? into a sequence of numbers using the above table. She obtains 23,8,1,20,29.
- (2) She ciphers the sequence 23,8,1,20,29, using the linear ciphering transformation. For example,  $C_{12}(23) \equiv 12 \cdot 23 \equiv 28 \pmod{31}$ . She obtains 28,3,12,23,7.
- (3) She sends 28,3,12,23,7 to Bob.

**Bob does the following:**

- (1) He receives 28,3,12,23,7 from Alice.
- (2) He decipheres the sequence 28,3,12,23,7, using the linear deciphering transformation. For example,  $D_{13}(28) \equiv 13 \cdot 28 \equiv 23 \pmod{31}$ . He obtains 23,8,1,20,29.
- (3) He translates 23,8,1,20,29 into an alphabetic sequence using the above table. He obtains WHAT?

**Catherine can do the following:**

- (1) She can intercept 28,3,12,23,7. But, since she does not know the key 12, she cannot recover the original message that was sent by Alice.
- (2) If she uses the table to translate 28,3,12,23,7 into an alphabetic sequence, she will obtain !CLWG ☹

**Exercise** Suppose that Alice and Bob are communicating by using the key  $k = 8$ . Bob received 24,27,27,3,7 from Alice. What was her message?

## Section 3 A Major Question

In the cryptosystem described in the previous section, it is important that Alice and Bob must share a common key and Catherine does not know it.

How can Alice and Bob share (exchange) a common key without revealing it to Catherine?

We need to establish a method that enables the following to occur:

- Alice sends some information about a key to Bob and Bob sends some information about a key to Alice through an unsecure communication channel.
- They can figure out a common key using the information exchanged.
- Catherine can intercept the same information, but she cannot figure out what the key is.

A solution to this question is the Diffie-Hellman Public Key Exchange (1976), which will be discussed in Section 5. An important concept for the Public Key Exchange is the concept of one-way functions.

## Section 4 One-way Functions

**Definition** (One-way Functions) Let  $X$  and  $Y$  be sets. A one-one function  $f : X \rightarrow Y$  is said to be one-way if

- (1) it is relatively easy to compute  $f(x)$  for any  $x \in X$ , and
- (2) it is very hard to compute  $f^{-1}(y)$  for most randomly selected  $y \in \text{Range}(f)$ .

**Remark** The concept of one-way functions is not a precise mathematical concept. It depends on algorithms currently available to compute  $f$  and  $f^{-1}$ , and also depends on current computational power. Also, see the remarks below.

**Example 1** Let  $X$  be the set of the pairs of prime numbers and  $Y$  be the set of positive integers. Consider a function  $f : X \rightarrow Y$  defined by  $f((p, q)) = pq$  (the multiplication of two prime numbers). Given two prime numbers  $p$  and  $q$ , it is easy to compute  $pq$ . But, given a number, it is not easy to determine whether the number is a product of two prime numbers, and if so, to find the two prime factors. Think about the following two problems:

- (1) Multiply two prime numbers 907 and 1009.
- (2) Determine whether or not 783451 is a product of two prime numbers. If so, find the two prime factors.

**Example 2** Let  $p$  be a prime number. Consider a reduced residue system mod  $p$ ,  $R_p = \{1, 2, \dots, p-1\}$ . Let  $g$  be a primitive root of  $p$ . Let  $\exp_g : R_p \rightarrow R_p$  be a function defined by  $\exp_g t \equiv g^t \pmod{p}$ . Then, its inverse is the index function  $\text{ind}_g : R_p \rightarrow R_p$ . Given an integer  $t$  in  $R_p$ , it is relatively easy to compute  $\exp_g t$ . However, given an integer  $a$  in  $R_p$ , it is generally difficult to compute  $\text{ind}_g a$ . Just to illustrate the idea, let  $p = 31$  and  $g = 3$ . Think about the following two problems:

- (1) Compute  $3^{19} \pmod{31}$ .
- (2) Compute  $\text{ind}_3 11$ .

**A Solution of (1)** (The Repeated Squaring Method)

If you compute  $3^{19} = 3 \cdot 3 \cdots 3 \cdot 3$  literally, it takes 18 multiplication operations. But, rewrite  $3^{19}$  as  $3^{19} = (3^9)^2 \cdot 3^1 = \left( (3^4)^2 \cdot 3^1 \right)^2 \cdot 3^1 = \left( \left( (3^2)^2 \right)^2 \cdot 3^1 \right)^2 \cdot 3^1$ . To compute the last expression, it takes only 6 multiplication operations.

**Exercise** Rewrite  $3^{20}$  using the repeated squaring method. How many multiplication operations are needed?

**A Solution of (2)**

By definition,  $t = \text{ind}_3 11 \Leftrightarrow 3^t \equiv 11 \pmod{31}$ . Thus, to find the value of  $\text{ind}_3 11$ , we must solve the equation  $3^t \equiv 11 \pmod{31}$  for  $t$ . The only method that we know in this class is to compute  $3^t \pmod{31}$  for all  $t \in \{1, 2, \dots, 30\}$  and to find  $t \in \{1, 2, \dots, 30\}$  such that  $3^t \equiv 11 \pmod{31}$ . This is very time consuming.

**Important Remarks**

- (1) In practice, to use  $\exp_g : R_p \rightarrow R_p$  as a one-way function, we must use a huge prime number for  $p$  so that it is practically impossible for us to compute  $\text{ind}_g a$  for a randomly chosen  $a$ , using computational power available at this moment.
- (2) If computational power is improved in the future, we will have to choose an even larger prime number for  $p$ .
- (3) Also, if someone discovers an efficient algorithm for computing  $\text{ind}_g a$ , then we cannot use  $\exp_g : R_p \rightarrow R_p$  as a one-way function.

## Section 5 Diffie-Hellman Public Key Exchange

The Public Key Exchange is a method that enables the following to occur:

- Alice sends some information about a key to Bob and Bob sends some information about a key to Alice through an unsecure communication channel.
- They can figure out a common key using the information exchanged.
- Catherine can intercept the same information, but she cannot figure out what the key is.

To understand the Public Key Exchange, it is very important to distinguish public knowledge and private knowledge.

### Public Knowledge

This is the knowledge that everybody (Alice, Bob, or Catherine) has.

- We are using the linear cryptosystem described in Section 2 to communicate with each other.
- We are using  $p = 31$  and  $R_{31} = \{1, 2, \dots, 29, 30\}$ .
- We are using  $g = 3$  as a primitive root of 31.

### Private Knowledge

This is the knowledge that only one individual knows.

- Alice randomly chooses a number  $t_A$  in  $R_{31} = \{1, 2, \dots, 29, 30\}$  and keeps it secretly. She does not share this number with anybody including Bob.
- Bob randomly chooses a number  $t_B$  in  $R_{31} = \{1, 2, \dots, 29, 30\}$  and keeps it secretly. He does not share this number with anybody including Alice.

### What do Alice and Bob have to do to exchange a key common to both of them?

- Alice computes  $a \equiv 3^{t_A} \pmod{31}$  and sends  $a$  to Bob through an unsecure communication channel.
- Bob computes  $b \equiv 3^{t_B} \pmod{31}$  and sends  $b$  to Alice through an unsecure communication channel.
- Alice receives  $b$  from Bob. Then, she computes  $b^{t_A} \pmod{31}$ .
- Bob receives  $a$  from Alice. Then, he computes  $a^{t_B} \pmod{31}$ .
- Since  $b^{t_A} \equiv (3^{t_B})^{t_A} \equiv 3^{t_A t_B} \pmod{31}$  and  $a^{t_B} \equiv (3^{t_A})^{t_B} \equiv 3^{t_A t_B} \pmod{31}$ , we have  $b^{t_A} \equiv a^{t_B} \pmod{31}$ . Alice and Bob can communicate, using this common number as a key in the linear cryptosystem described in Section 2.

### What can Catherine do?

- She can intercept both  $a$  and  $b$ .
- What can she do with them? She needs to compute  $\text{ind}_3 a$  or  $\text{ind}_3 b$  so that she obtains  $b^{\text{ind}_3 a} \equiv (3^{t_B})^{t_A} \equiv 3^{t_A t_B} \pmod{31}$  or  $a^{\text{ind}_3 b} \equiv (3^{t_A})^{t_B} \equiv 3^{t_A t_B} \pmod{31}$ . But, this is not an easy task.

### Important Remark

Here, we are using  $p = 31$  to illustrate the idea. But, in practice, we use a huge prime number for  $p$  so that it is practically impossible for Catherine to compute  $\text{ind}_3 a$  or  $\text{ind}_3 b$ , using computational power available at this moment. Thus, she cannot obtain the key that Alice and Bob share.

### Example

- Suppose that Alice randomly chooses  $t_A = 19$ .  
She computes  $a \equiv 3^{t_A} = 3^{19} \equiv 12 \pmod{31}$ .  
She sends 12 to Bob.
- Suppose that Bob randomly chooses  $t_B = 23$ .  
He computes  $b \equiv 3^{t_B} = 3^{23} \equiv 11 \pmod{31}$ .  
He sends 11 to Alice.
- Alice receives 11 from Bob.  
She computes  $11^{t_A} = 11^{19} \equiv 22 \pmod{31}$ .
- Bob receives 12 from Alice.  
He computes  $12^{t_B} = 12^{23} \equiv 22 \pmod{31}$ .
- Alice and Bob end up with the same number 22. They use  $k = 22$  as a key in the linear cryptosystem. ☺