Modular Arithmetic and Cryptography

There are many situations where information must be kept secure or secret. Secret codes have been a part of political intrigue for as long as there have been competing groups of people. Information security is also important in business, industry, government, and in private life, particularly in online settings. The mathematics used to keep information secure in all these situations is called *cryptography*.

Cryptography is the study of mathematical techniques used to provide information security. A fundamental aspect of cryptography is *confidentiality*. Confidentiality is important, for example, when you send a credit card number over the Internet, or when your government sends a secret message to an embassy abroad. Confidential information is transmitted and received as illustrated in the diagram below.

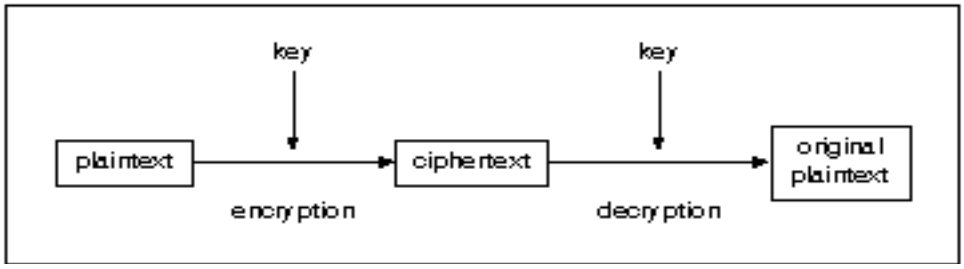


Figure 1:
A cryptosystem uses keys to convert plaintext to ciphertext and then back to the original plaintext

The original plaintext message is encrypted. The resulting ciphertext message is decrypted upon receipt. A key is used to encrypt and decrypt the information. A **cryptosystem** is the overall method of encrypting and decrypting using keys.

There are two basic types of cryptosystems. In a **symmetric-key cryptosystem**, the same key is used to encrypt and decrypt. (The exact same key may not be used, but at least it is easy to calculate the encryption key from the decryption key, and vice versa.) Thus, the security of a symmetric-key cryptosystem depends on the secrecy of the key. In contrast, in a **public-key cryptosystem**, different keys are used for encryption and decryption. One key is made public, and the other is kept secret. Since symmetric-key systems are faster, while public-key systems are more secure, *hybrid cryptosystems* are often used, in which the same key is used to encrypt and decrypt but the key is transmitted from sender to receiver using a public-key system.

You often see cryptosystems in action when you use the Internet. For example, you might see a warning message such as on the left in Figure 2 when you are entering personal information on a website. When shopping online, you know that cryptography is being used to keep your transaction secure when you see that the website address begins with "https" instead of "http," as on the right in Figure 2. This indicates that the Secure Sockets Layer (SSL) protocol is being used to securely transfer information. According to the Apple OS X Help guide, "Web browsers and many websites use the SSL protocol to transfer confidential user information, such as credit card numbers. SSL uses a public and private key encryption system" (OS X 10.5.6 Help, "About Secure Sockets Layer").

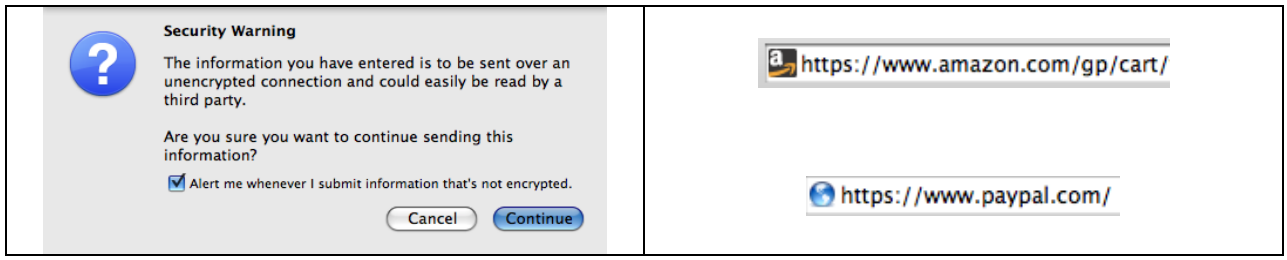


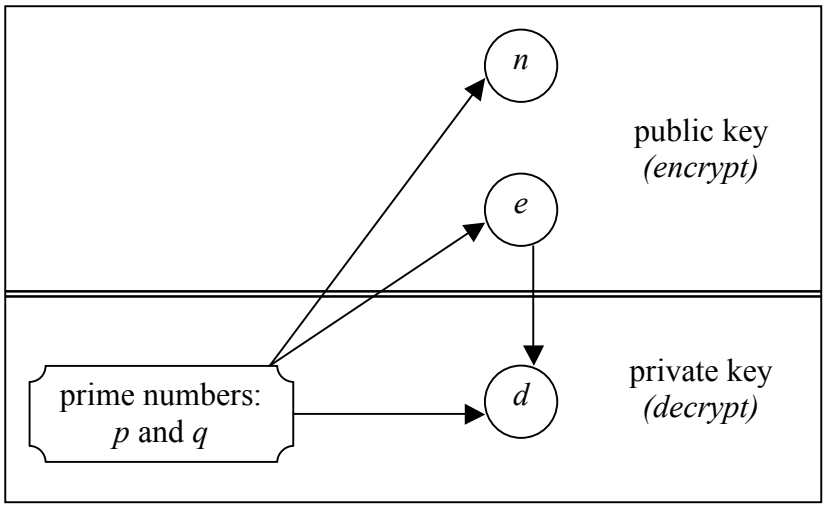
Figure 2: Examples of cryptography in action on the Internet

Public-key cryptography was developed in the mid-1970s by Whitfield Diffie and Martin Hellman at Stanford University and Ronald L. Rivest, Adi Shamir, and Leonard Adleman at the Massachusetts Institute of Technology. (It appears that James Ellis, Clifford Cocks, and Malcolm Williamson developed the idea earlier as part of secret work for a British intelligence service, but this was not made public until the 1990s.) Public-key cryptography is one of the most significant developments in the history of cryptography, and it is still widely used today.

Consider the RSA public-key cryptosystem (with initials in honor of the MIT developers). This system is based on the fact that it is relatively easy to multiply two large numbers, but difficult to factor a large composite number. Messages are first converted to numbers (e.g., A becomes 1, B becomes 2, etc.) and then the numbers are transformed using modular arithmetic. The steps of this procedure are described on the next page.

The keys for the RSA public-key cryptosystem are numbers constructed by the receiver. The numbers are constructed using prime numbers and modular arithmetic. The general strategy is shown in the diagram below. The numbers n and e are used for encrypting. They comprise the **public key**, known to everyone. The numbers p, q, and d are used for decrypting. They comprise the **private key**, known only to the receiver. The arrows in the diagram show which numbers are used to construct which. The procedure below the diagram explains how to encrypt and decrypt messages.

RSA Cryptosystem



The Receiver Constructs the Keys:

- Choose two prime numbers, p and q.
- Compute $n = pq$.
- Compute $r = (p - 1)(q - 1)$.
- Choose a number e (for encrypt) such that e has a multiplicative inverse in Z_r.
- d (for decrypt) is the multiplicative inverse of e in Z_r.
- The receiver publishes e and n in a public directory. This is the receiver's public encryption key.
- The receiver keeps d secret, along with p and q. This is the private decryption key.

Encrypting:

- Convert the plaintext message to numbers, each of which is less than n.
- Raise each number to the power e. Reduce *mod n*.

Decrypting:

- Raise each ciphertext number to the power d. Reduce *mod n*.
- Convert from numbers to letters.

Before investigating this method further, we need to understand some of the mathematical ideas involved in the above description. In particular, we must figure out what the notation Z_r and *mod n* mean. These are part of an area of mathematics called *modular arithmetic*.

Modular Arithmetic

In the following problems you will investigate modular arithmetic. Your goal, by the end of the lesson, is to answer this question:

What is modular arithmetic, how does it work,
and how does it compare to standard arithmetic with real numbers?

1. Suppose that as part of a secret code you will substitute numbers for letters. You will also need a number to represent a space. Use the following translation scheme:

$0 \rightarrow$ space
$1 \rightarrow$ A
$2 \rightarrow$ B
$3 \rightarrow$ C
:
$26 \rightarrow$ Z

So you have 27 characters, numbered from 0 to 26.

Think about how you could convert numbers larger than 26 into letters, by starting to count over after you reach 26. For example, the number 28 translates to "A".

(a) Translate the numbers 29, 52, and 119 into letters. Compare your translation with those of some other students. Resolve any differences.

(b) Verify that 31 and 58 both translate to the letter D. Find two other numbers that translate to D. Describe any pattern you notice for all numbers that translate to D.

(c) Translate –2 into a character. Translate –10. Describe how you do the translation. Compare your translation with those of some other students. Resolve any differences.

2. To translate numbers into characters in Problem 1, you first need to convert any given integer into an integer between 0 and 26. This is an example of what is called *modular arithmetic*. In particular, you are using a *mod 27* system, since you are limited to the 27 integers between 0 and 26: 0, 1, 2, 3, ..., 26. It is possible to do arithmetic in this system. For example, $2 + 3 = 5$ in *mod 27*, just as in regular arithmetic.

(a) Perform the following computations in *mod 27*.

- Explain why $25 + 9 = 7$ in *mod 27*.

- $18 + 14 =$ ___ in *mod 27*

- $3 \times 25 =$ ___ in *mod 27*

- $7^2 =$ ___ in *mod 27*

- $-5 =$ ___ in *mod 27*

(b) Compare your results and explanations with those of some other classmates. Make sure everyone is getting the same answers. Resolve any differences.

3. Now consider some other modular systems.

(a) Consider a *mod 31* system. Do the same computations as in Part (a) of Problem 2, using *mod 31*. Record your answers next to the *mod 27* answers in Problem 2.

(b) Consider *mod 15*. Would you say that 23 and 38 are "equivalent *mod 15*"? Why?

4. The definition of "equivalent *mod n*" is as follows.

Integers a and b are ***equivalent mod n***
if and only if a and b have the same remainder upon division by n.

A "three-line equal sign" is used to denote equivalence *mod n*. Thus,
$a \equiv b \text{ mod } n$ is read as, "*a* is equivalent to *b mod n*."

(a) Use the definition above to show that $23 \equiv 8 \text{ mod } 5$.

(b) Use the definition above to show that $76 \equiv 4 \text{ mod } 9$.

(c) Use the definition above to show that $-3 \equiv 24 \text{ mod } 27$.

(d) Find four integers that are equivalent to 2 *mod 7*.

(e) Can you think of an equivalent yet different definition of "equivalent *mod n*"? Perhaps using subtraction?

5. To **reduce an integer *mod n*** means to replace the integer by its remainder upon division by *n*. For example, if you reduce 58 *mod 7* you get 2, since dividing 58 by 7 leaves a remainder of 2.

(a) Reduce each of the integers below, using the indicated modular system.

- 48 *mod 5*

- 397 *mod 10*

- –24 *mod 7*

(b) What are all the possible results when you reduce integers *mod 5*? How about when you reduce *mod 12*? How about *mod 348*? How about *mod n*? Explain.

(c) Suppose two integers reduce *mod n* to the same number. Are these two integers equivalent *mod n*? Prove your answer.

Integers mod n: Z_n

You found in Part (b) of Problem 5 above that every integer can be reduced *mod 5* to 0, 1, 2, 3, or 4, since these are the possible remainders when you divide an integer by 5. You also found that, in general, every integer can be reduced *mod n* to an integer between 0 and $(n - 1)$, inclusive. Because of this, we can define a new set of numbers, called **integers *mod n***:

$$\boldsymbol{Z_n = \{0, 1, 2, ..., n - 1\}}.$$

Each "number" in Z_n really represents all the integers that reduce to it *mod n*. Even so, you can think of the elements of Z_n as the numbers $0, 1, 2, ..., n - 1$. Arithmetic in Z_n is the same arithmetic *mod n* that you have been using above.

Properties of Z_n The modular arithmetic in Z_n has many interesting properties. Some properties are similar to properties of regular arithmetic with real numbers, while other properties are different.

6. Think about additive inverses.

(a) Every real number x has an **additive inverse**, which when added to x yields 0. Find the additive inverse of these real numbers: 5, $\frac{3}{4}$, and -1.5.

(b). Check to see if the additive inverse property is true in Z_n.

- What is the additive inverse of 6 in Z_{10}?
- What is the additive inverse of 3 in Z_8?
- What is the additive inverse of m in Z_n?
- Do you think every number in Z_n has an additive inverse? Explain.

7. Think about multiplicative inverses.

(a) Every nonzero real number x has a **multiplicative inverse**, which when multiplied by x yields 1. Find the multiplicative inverse of 5, $\frac{3}{4}$, and –1.5.

(b) Check to see if the multiplicative inverse property is true in Z_n.
Consider Z_7.

- Find a number in Z_7 that you can multiply by 3 to get 1 *mod 7*. Such a number is the multiplicative inverse of 3 in Z_7.

- For each nonzero number in Z_7, try to find its multiplicative inverse.

(c) Consider Z_6.

- For each number in Z_6, try to find its multiplicative inverse. (Remember that you multiply in Z_6 using *mod 6* modular arithmetic.)

- State any patterns you notice concerning which numbers in Z_6 have a multiplicative inverse and which do not.

(d) Consider Z_9.

- For each number in Z_9, try to find its multiplicative inverse. (Remember that you multiply in Z_9 using *mod 9* modular arithmetic.)

- State any patterns you notice concerning which numbers in Z_9 have a multiplicative inverse and which do not.

(e) Does every number in Z_n have a multiplicative inverse, for every n? Explain.

8. You discovered in Problem 7 that not all numbers in a given modular system have a multiplicative inverse. Think about when multiplicative inverses exist in Z_n.

(a) Make some conjectures about which numbers have multiplicative inverses in Z_n, either for a general n or for particular values of n. For each conjecture, try to prove it or disprove it. (You can disprove it by finding a counterexample.)

After trying some of your own conjectures, complete and prove the following three statements.

(b) When n is _____, then every nonzero integer in Z_n has a multiplicative inverse.

(c) If n and m have a particular relationship to each other, then m does <u>not</u> have a multiplicative inverse in Z_n. What is that relationship?

(d) m has a multiplicative inverse in Z_n if and only if _____.

9. Summarize Review and practice what you have learned about the number system Z_n and the associated operations of addition and multiplication *mod n*, as you work through the following problems.

(a) 8 and 5 can be considered elements in many different modular systems. Think about the arithmetic of the various modular systems as you complete the following:

- $8 + 5 =$ __, in Z_9
- $8 + 5 =$ __, in Z_{27}
- $8 \times 5 =$ __, in Z_9
- $8 \times 5 =$ __, in Z_{27}
- $8^5 =$ __, in Z_9
- Find the additive inverse of 8 in Z_{12}.
- Find the multiplicative inverse of 5 in Z_{11}.

(b) Consider a *mod 8* system.

- Describe how to determine if two integers are equivalent *mod 8*.
- Find three integers that are equivalent to –6 *mod 8*.
- Reduce 346 *mod 8*.

(c) Give a general explanation or description of the following.

- Two integers are equivalent mod *n*.
- Reduce an integer mod n.
- Z_n, and the properties of addition and multiplication in Z_n

(d) Go back and examine the description of the RSA cryptosystem on page 3. Identify the places where modular arithmetic is used.