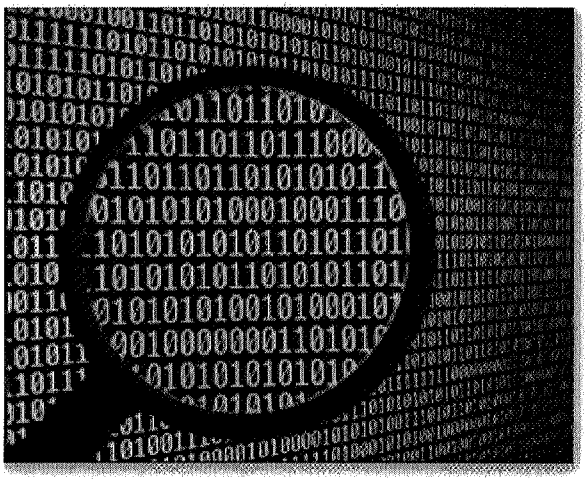
Introduction to Cryptography

Suppose you want to tell your friend a secret, something that you don't want anyone else to hear. If you are together, you can whisper the message close to your friend's ear. But suppose that speaking to your friend in privacy is not an option. How can you communicate your message to your friend and prevent others from sharing it?

For thousands of years, people have been finding ways to hide communications from anyone other than the intended recipient. **Cryptography** is the design and use of methods to conceal messages. These methods can rely on very simple techniques like scrambling the letters in the message, or use highly theoretical algorithms based on advanced mathematics.



Cryptography has long been used by militaries and governments to facilitate secret communications, but is now also commonly used within many civilian systems to protect data. For example, most digital communications today travels across the public networks (the Internet). It is virtually impossible to guarantee that an eavesdropper cannot physically access the information traveling over the Internet. However, for many computer applications that use the Internet, such as e-commerce, maintaining the privacy of their information is critical. In e-commerce (buying products and services over the Internet), a buyer's credit card information must be protected while it is in transit from the buyer to the seller. Cryptography is used to protect information transmitted over the Internet, including emails and Internet telephony. It is also used to protect entire communications infrastructures, such as wireless networks; stored data, from single files to entire hard disks; and computer code, such as computer operating systems.

Let's consider a basic communication scenario. Imagine that Alice wants to communicate secretly with her friend Bob. Alice must somehow transform her message, called **plaintext**, in order to keep the message private. This process is called **encryption**.

Alice uses an encryption algorithm, or **cipher**, to transform her plaintext message into **ciphertext**. Ciphertext is an unreadable form of the original message that hopefully

prevents others from eavesdropping. The cipher uses the plaintext together with a **key** that determines exactly how to transform the plaintext into ciphertext. Bob uses the same cipher used by Alice and a key, possibly different from the key used by Alice to **decrypt** the ciphertext and recover Alice's message.

The key is very important – even if others know the cipher that Alice and Bob use to communicate, they can't read Alice's and Bob's messages without the key.

Below we discuss three types of ciphers: **substitution**, **transposition**, and **public/private key**.

Substitution Cipher

In a substitution cipher, letters in the plaintext are replaced by other letters.

The simplest example is the **Caesar cipher,** so called because Caesar used this technique to communicate secretly with his generals. To encrypt a message using the Caesar cipher, each letter in the plaintext is shifted by the same number of letters in the alphabet. The number of letters to shift is based on the value of the key.

For example, if Alice's plaintext message is "hello" and the key is 3, then the Caesar cipher will generate "hello"+3 = "khoor". Notice, that each letter in the encrypted message, "khoor" is exactly three letters away from each letter in the plaintext message; "k" is three after "h", "h" is three letters from "e" and so on. Bob can retrieve the original message from the encrypted message by simply taking the text he receives and **subtracting** the value of the key from each letter.

What happens when a plaintext letter appears near the end of the alphabet and "falls off" the end when its value is added to the key? The solution is to "wrap around" to the beginning of the alphabet whenever this occurs. For example, the letter "x" becomes an "a" with a key of 3.

Like the Caesar code, the **Vigenère cipher** also shifts letters in the plaintext. However, instead of using the same shift for every letter, it applies different shifts defined by a **keyword**. For example, if the keyword is "dog," consisting of the 4th, 15th, and 7th letters of the alphabet, then the first letter of the message is shifted by 4, the second letter is shifted by 15, the third by 7, the fourth by 4 (here we return to the beginning of the keyword), the fifth by 15, and so on. Using this cipher and the keyword "dog", Alice's "hello" message becomes "ltspd". Decryption involves sequentially subtracting the keyword shift values.

Transposition Cipher

In a **transposition cipher** the letters of the plaintext message are rearranged in a different and usually quite complex way, but the letters themselves are left unchanged.

In **a simple transposition cipher**, the message is rearranged in a way determined by a keyword known by both the sender and receiver. To encrypt the plaintext, the sender writes the message in a box composed of several rows of a fixed length, ignoring spaces between words and punctuation. Then the message is read out again column by column; however, the columns are chosen in a scrambled order. Both the width of the rows and the order of the columns are defined by the keyword: the number of rows is the length of the keyword, and the column permutation is determined by the alphabetical order of the letters in the keyword. For example, suppose the keyword is "zebras". Since the keyword is 6 letters long, then the rows are of length 6; the column order is: 6 3 2 4 1 5, the alphabetical order of the letters in the word "zebras".

It is possible that there will not be enough letters in the plaintext to fill the last row. Then the message is padded at the end with enough dummy letters to fill this row.

Let's consider this longer message from Alice: "Hello, how is the weather there?" Let's use the keyword "early" to encrypt this message using a simple transposition cipher. First, we write the message out in a box with rows of length 5:

e	a	r	l	y
h	e	l	l	o
h	o	w	i	s
t	h	e	w	e
a	t	h	e	r
t	h	e	r	e

Next, we read the columns in the order indicated by the keyword: 2 1 4 3 5. The ciphertext is "eohthhhtatliwerlweheosere".

Can you figure out how Bob would decipher this message from Alice? Remember that he knows that Alice used the simple transposition cipher with the keyword "early".

Public Key Crytography

There are two types of cryptography, **symmetric** and **asymmetric**. So far, the ciphers we have discussed have been symmetric, meaning that the encryption and decryption keys are identical. Modern cryptographic systems rely on more sophisticated asymmetric techniques that require two separate keys, one to encrypt the plaintext and one to decrypt the ciphertext. Neither key alone will do both functions. This cryptography system eliminates the need for key exchange, enhancing the security and privacy of the messages.

An asymmetric system commonly in use today is the **public/private key** system. In this system, one of these keys is published (public) and the other is kept private. Public/private key cryptography was invented in the mid 1970's. Examples include the Diffie-Hellman key exchange protocol and the RSA encryption algorithm.

The public/private key system relies on concepts from algebra, such as modular arithmetic. Specifically using the modulo operator, which computes the remainder of the division of two integers. For example, given two integers a and b, where $a = 5$ and $b = 3$, a mod b would be 2, since a divided by b is equal 1 with a remainder of 2.

In this system, messages must be in the form of positive integers. Here is a simple example of a public/private key cipher. In order to send a message, Bob chooses any two integers a_1 and b_1, and sets $Z = a_1b_1 - 1$. He then chooses two more integers $a_2$andb_2, and sets

$$e = a_2 Z + a_1, \quad d = b_2 Z + b_1, \quad n = (de - 1)/Z = a_2 b_2 Z + a_1 b_2 + a_2 b_1 + 1.$$

Note that since $de - nZ = 1$, then $de = 1 \pmod{n}$.

Bob's public key is (n,e), and his private key is (n, d). Anyone, including Alice, can know Bob's public key, but only Bob knows his private key.

To send Bob a plaintext m, Alice computes $c = em \pmod{n}$, to perform encrypt the message using Bob's public key (n,e). Bob uses his private key to decipher the ciphertext by computing $dc \pmod{n}$. Note that the decryption operation recovers the plaintext, because $dc \pmod{n} = dem \pmod{n} = m \pmod{n}$.

As an example, suppose Bob chooses $a_1 = 3$, $b_1 = 5$, $a_2 = 2$, and $b_2 = 7$. Then $Z = 14$, $e = 31$, $d = 103$, and $n = 228$. Bob's public key is (228, 31). Now suppose that Alice wants to send Bob the numeric message $m = 13$. This could represent anything that Alice and Bob both understand. For example, this could mean the letters "ac". Alternatively, this could be a message that Alice and Bob have previously agreed on to mean "meet me at the mall." Note: the value of Alice's message should be less than n.

To encrypt the message, Alice computes

$$c = em \pmod{n} = 31 \cdot 13 \pmod{228} = 175,$$

and sends this ciphertext to Bob. After receiving this message, Bob computes

$$m = dc \pmod{n} = 103 \cdot 175 \pmod{228} = 13.$$

Challenge: Suppose you are an eavesdropper, and you detect Alice's ciphertext $c = 175$ sent to Bob. You also know Bob's public key (228, 31). How would you go about trying to determine Alice's original plaintext m?

Sources:

http://williamstallings.com/Crypt-Tut/Crypto%20Tutorial%20-%20JERIC.html
http://www.math.washington.edu/~koblitz/crlogia.html
http://en.wikipedia.org/wiki/Transposition_cipher
http://library.thinkquest.org/04oct/00451/trancipher.htm

http://www.parliament.uk/documents/post/postpn270.pdf
http://en.wikipedia.org/wiki/Modulo_operation

Cryptography Worksheet

This document presents the same example cryptography challenges that are presented in the virtual robot environment. The

Legend:

* = Easy

** = Medium

*** = Difficult

Encode the following messages:

***1. Caesar cipher with a shift key of 4**

Plaintext: I LOVE MESA

***2. Caesar cipher with a shift key of 21**

Plaintext: PROGRAMMING

****3. Vigenere cipher with a keyword of MESA**

Plaintext: RAVENS

****4. Simple Transposition Cipher with keyword: cat**

Plaintext: OCEAN CITY

***5. Caesar cipher with a shift key of 7**

Plaintext: MARYLAND BLUE CRABS

*** 6. Caesar cipher with a shift key of 2**

Plaintext: INNER HARBOR IN BALTIMORE CITY

Decode the following messages:

****1. Use the Caesar cipher with a shift key of __2___**

Ciphertext: EQORWVGTUEKGPEG

***2. Use the Caesar cipher with a shift key of __2___**

Ciphertext: OCTANCPFJCUVJGDGUVETCDECMGU

****3. Use the Caesar cipher with a shift key of __-3___**

Ciphertext: QEBZFMEBOEXPYBBKYOLHBK

*****4. Use the Vigenere cipher with the keyword: bad**

Ciphertext: XJVWT

****5. Use the Vigenere cipher with the keyword: __team___**

Ciphertext: WMFFUUFNEJCNS

*****6. Use the Vigenere cipher with the keyword: __byte___**

Ciphertext: INNJTOM

*****7. Use Simple Transpostion cipher with the keyword: lions**

Ciphertext: HPSSRTIIABSETTAIHNYECREOK

*****8. Use the Simple Transposition cipher with the keyword: cyber**

Ciphertext: EGPNIMANXETRRTTUAIHYETDIC

Public/Private Key:

****1. Decrypt ciphertext message 15 with a private key of (44,19) and the public key of (44,7)**

*****2 . Encrypt plaintext 89 which represents the word HI using the following integer values:**

$a_1 = 1$, $b_1 = 2$, $a_2=3$, and $b_2 =5$

Cryptography Worksheet Solutions

Encode the following messages:

1. Caesar cipher with a shift key of 4

   Ciphertext: MPSZIQIWE

2. Caesar cipher with a shift key of 21

   Ciphertext: KMJBMVHHDIB

3. Vigenere cipher with a key word of MESA

   Ciphertext: EFOFAX

4. Simple Transposition with the keyword: cat

   Ciphertext: CNTOAIECY

5. Caesar cipher with a shift key of 7

   Ciphertext: THYFSHUKISBLJYHIZ

6. Caesar cipher with a shift key of 2

   Ciphertext: KPPGTJCTDQTKPDCNVKOTGEKVA

Decode the following messages:

1. Caesar cipher with a shift key of __2__

   Plaintext : COMPUTER SCIENCE

2. Caesar cipher with a shift key of __2__

   Plaintext :MARYLAND HAS THE BEST CRAB CAKES

3. Vigenere cipher with key word of team

   Plaintext : CHEASAPEAKE BAY

4. Vigenere cipher with key word of byte

   Plaintext : GO TERPS

5. Simple Transposition cipher with the keyword: lions

Plaintext : THIS CIPHER ISNT EASY TO BREAK

6. Simple Transposition cipher with the keyword: cyber

   Plaintext : MEET U AT GRAND PRIX IN THE CITY

Public/Private Key:

1. **Decrypt ciphertext message 15 with a private key of (44,19) and the public key of (44,7)**

   Plaintext : 21

2. **Encrypt plaintext 89 which represents the word HI using the following integer values:**

   $a_1 = 1$, $b_1 = 2$, $a_2=3$, and $b_2 =5$

   Ciphertext: 5

Names_____

Cryptology 101 Worksheet

Question Sheet

Cipher Type	Encode	Key	Decode	Key
Substitution (Caesar)				
Substitution (Vigenere)				
Transposition (Simple)				
Public Key				

Names_____

Cryptology 101 Worksheet

Answer Sheet

Cipher Type	Encode	Key	Decode	Key
Substitution (Caesar)				
Substitution (Vigenere)				
Transposition (Simple)				
Public Key				