Lecture 3

Elementary Cryptography

Agenda

- Some useful definition
- Why cryptography?
- Characteristics of cryptographic system
- Substitution encryption
- Transposition/permutation encryption

Terminologies

- Plaintext
- Ciphertext
- Encryption
- Decryption
- Key
- Cryptography
- cryptanalysis

What is the problem? Network threats

- Block it, by preventing its reaching R, thereby affecting the availability of the message.
- Intercept it, by reading or listening to the message, thereby affecting the confidentiality of the message.
- Modify it, by seizing the message and changing it in some way, affecting the message's integrity.
- Fabricate an authentic-looking message, arranging for it to be delivered as if it came from S, thereby also affecting the integrity of the message.

Encryption has been used for centuries to protect diplomatic and military communications, sometimes without full success. The word **cryptography** means hidden writing, and it refers to the practice of using encryption to conceal text. A **cryptanalyst** studies encryption and encrypted messages, hoping to find the hidden meanings.

What Is Cryptography?

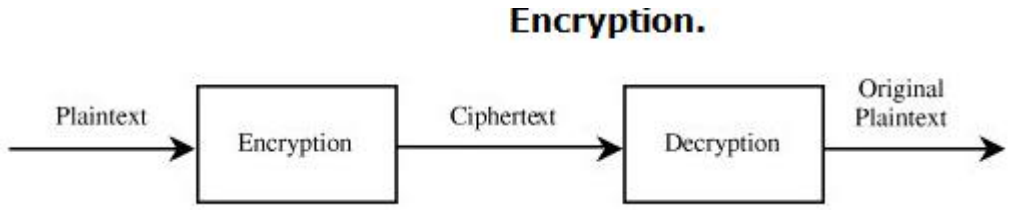
The word cryptography comes from two Greek words meaning "secret writing" and is the art and science of concealing meaning. Cryptanalysis is the breaking of codes. The basic component of cryptography is a cryptosystem.

- A cryptosystem is a 5-tuple (E, D, M, K, C), where M is the set of plaintexts, K the set of keys, C is the set of ciphertexts, E: M x K C is the set of enciphering functions, and D: C x K M is the set of deciphering functions.
- Cryptography/secret writing is the strongest tool for controlling against many kinds of security threats
- Well-disguised data cannot be read, modified, or fabricated easily.

- **Encryption** is the process of encoding a message so that its meaning is not obvious;
- **Decryption** is the reverse process, transforming an encrypted message back into its normal, original form.
- Alternatively, the terms **encode** and **decode** or **encipher** and **decipher** are used instead of encrypt and decrypt.
- That is, we say that we encode, encrypt, or encipher the original message to hide its meaning.
- Then, we decode, decrypt, or decipher it to reveal the original message.
- A system for encryption and decryption is called a **cryptosystem**.
- The original form of a message is known as **plaintext**, and the encrypted form is called **ciphertext**..
- For convenience, we denote a plaintext message P as a sequence of individual characters $P = <p_1, p_2, é , p_n>$.
- Similarly, ciphertext is written as $C = <c_1, c_2, é , c_m>$.

For instance, the plaintext message "I want cookies" can be denoted as the message string <I, ,w,a,n,t, , c,o,o,k,i,e,s>.

It can be transformed into ciphertext $<c_1, c_2, é , c_{14}>$, and the encryption algorithm tells us how the transformation is done.



Crytography

- We characterize crygraphic system by:
- Type of encryptionoperations used that is:
- Substitution/transposition/product
- Number of keys used
- Keyless; single-key or private; two-key or public
- Ways inwhch plaintext is processed Block/stream

Keys

Keyless encrytption: the encrytion algorithm itself is kept secret

Symetric encryption: both sides (sender and recipient) use the same key.

Asymmetric encryption is also known as public key

Sender and recipient use different but related keys.

Encryption Algorithms

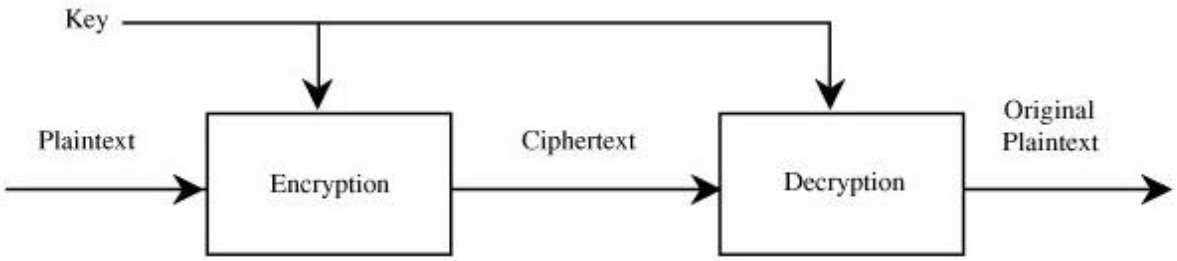
The cryptosystem involves a set of rules for how to encrypt the plaintext and how to decrypt the ciphertext. The encryption and decryption rules, called **algorithms**, often use a device called a **key**, denoted by K, so that the resulting ciphertext depends on the original plaintext message, the algorithm, and the key value

Sometimes the encryption and decryption keys are the same, so P = D(K, E(K,P)). This form is called **symmetric** encryption because D and E are mirror-image processes. At other times, encryption and decryption keys come in pairs. Then, a decryption key, K_D, inverts the encryption of key K_E so that P = D(K_D, E(K_E,P)). Encryption algorithms of this form are called **asymmetric**

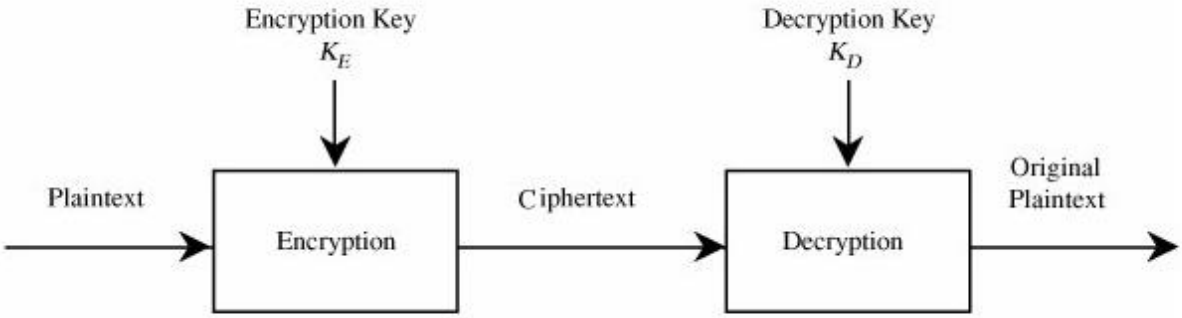
Symmetric and Asymmetric Encryption Systems

- The two basic kinds of encryptions are symmetric (also called "secret key") and asymmetric (also called "public key").
- Symmetric algorithms use one key, which works for both encryption and decryption. Usually, the decryption algorithm is closely related to the encryption one.

(For example, the Caesar cipher with a shift of 3 uses the encryption algorithm "substitute the character three letters later in the alphabet" with the decryption "substitute the character three letters earlier in the alphabet.")



(a) Symmetric Cryptosystem



(b) Asymmetric Cryptosystem

A key gives us flexibility in using an encryption scheme. We can create different encryptions of one plaintext message just by changing the key.

Moreover, using a key provides additional security. If the encryption algorithm should fall into the interceptor's hands, future messages can still be kept secret because the interceptor will not know the key value.

- An encryption scheme that does not require the use of a key is called a **keyless cipher**

Cryptanalysis

A cryptanalyst's chore is to **break** an encryption. That is, the cryptanalyst attempts to deduce the original meaning of a ciphertext message. Better yet, he or she hopes to determine which decrypting algorithm matches the encrypting algorithm so that other messages encoded in the same way can be broken.

For instance, suppose two countries are at war and the first country has intercepted encrypted messages of the second.

Cryptanalysts of the first country want to decipher a particular message so that the first country can anticipate the movements and resources of the second. But it is even better to discover the

actual decryption algorithm; then the first country can easily break the encryption of all messages sent by the second country.

Thus, a cryptanalyst can attempt to do any or all of six different things:

- break a single message
- recognize patterns in encrypted messages, to be able to break subsequent ones by applying a straightforward decryption algorithm
- infer some meaning without even breaking the encryption, such as noticing an unusual frequency of communication or determining something by whether the communication was short or long
- deduce the key, to break subsequent messages easily
- find weaknesses in the implementation or environment of use of encryption
- find general weaknesses in an encryption algorithm, without necessarily having intercepted any messages

Basic encryption (keyless)

Representing Characters/substitution

We want to study ways of encrypting any computer material, whether it is written as ASCII characters, binary data, object code, or a control stream.

However, to simplify the explanations, we begin with the encryption of messages written in the standard 26-letter English alphabet, A through Z.

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Code	0	1	2	3	4	5	6	7	8	9	10	11	12

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Code	13	14	15	16	17	18	19	20	21	22	23	24	25

- we use the convention that plaintext is written in UPPERCASE letters, and ciphertext is in lowercase letters.
- Because most encryption algorithms are based on mathematical transformations, they can be explained or studied more easily in mathematical form.
- Thus, the letter A is represented by a zero, B by a one, and so on.

This representation allows us to consider performing arithmetic on the "letters" of a message. That is, we can perform addition and subtraction on letters by adding and subtracting the corresponding code numbers.

Arithmetic operations

Expressions such as A + 3 = D; A+5= F or K+2=M; K - 1 = J and Z+1=A or X+4= B have their natural interpretation. Arithmetic is performed as if the alphabetic table were circular.

In other words, addition wraps around from one end of the table to the other so that Y + 3 = B. Thus, every result of an arithmetic operation is between 0 and 25.

This form of arithmetic is called modular arithmetic, written mod n, which means that any result

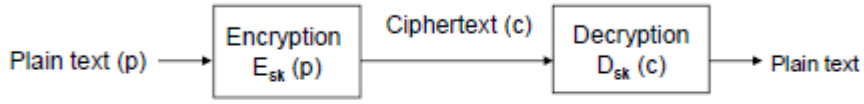
greater than n is reduced by n as many times as necessary to bring it back into the range 0 result & < n. Another way to reduce a result is to use the remainder after dividing the number by n.

For example, the value of 95 mod 26 is the remainder of 95/26, which is 17, while 95 - 26 - 26 - 26 = 17; alternatively, starting at position 0 (A) and counting ahead 95 positions (and returning to position 0 each time after passing position 25) also brings us to position 17.

There are many types of encryption. There are two simple forms of encryption:

Substitutions, in which one letter is exchanged for another, and

Symmetric Encryption (single key)



D_{ks} (E_{ks} (p)) = p, where sk is a secret key shared by sender and recipient.

EXAMPLE: The Caesar cipher is the widely known cipher in which letters are shifted. For example, if the key is 3, the letter A becomes D, B becomes E, and so forth, ending with Z becoming C. So the word "HELLO" is enciphered as "KHOOR." Informally, this cipher is a cryptosystem with:

M = { all sequences of Roman letters }

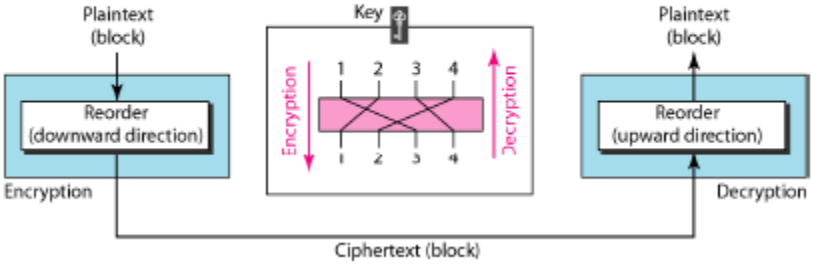
K = { i | i an integer such that 0 i 25 }

E = { E_k | k K and for all m M, E_k(m) = (m + k) mod 26 }

Representing each letter by its position in the alphabet (with A in position 0), "HELLO" is 7 4 11 11 14; if k = 3, the ciphertext is 10 7 14 14 17, or "KHOOR."

Transposition/permutation

Hide the message by rearranging letter order without altering the actual letters.



Example (Encryption)

Encrypt the message ñNETWORK SECURITYò using the above key.

Solution

- Firstly, remove the spaces in the message
- Then, divide the text into blocks of four characters
- Add a bogus character Z at the end of the third block
- The result is NETW ORKS ECUR ITYZ
- We then create a three block ciphertext

TNWE KOSR UERC YIZT

Decryption

Decrypt the message TNWEKOSRUERCYIZT

Solution

After combining the characters and removing the bogus character we get the original message ñNETWORK SECURITYò

The goals of studying these two forms are to become familiar with the concept of encryption and decryption, to learn some of the terminology and methods of cryptanalysis, and to study some of the weaknesses to which encryption is prone.