Basic Cryptography

Al-Mustanseriya University Class: Third Year

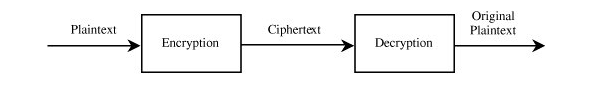
Engineering College Subject: Ciphering & Data Security

Computer and Software Engineering Dep. Lecture -3-

Terminology

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**. This relationship is shown in figure 2.1. For convenience, we denote a plaintext message P as a sequence of individual characters P = <p1, p2, …, pn>. Similarly, ciphertext is written as C = <c1, c2, …, cm>. 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 <c1, c2, …, c14>, and the encryption algorithm tells us how the transformation is done.

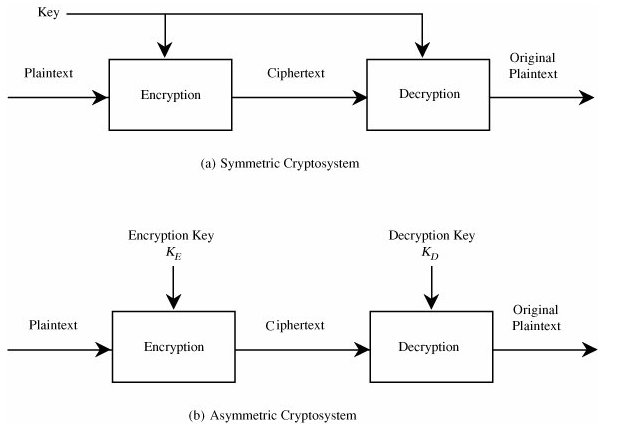


We use this formal notation to describe the transformations between plaintext and ciphertext. For example, we write C = E(P) and P = D(C), where C represents the ciphertext, E is the encryption rule, P is the plaintext, and D is the decryption rule. What we seek is a cryptosystem for which P = D(E(P)). In other words, we want to be able to convert the message to protect it from an intruder, but we also want to be able to get the original message back so that the receiver can read it properly.

##### 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. We write this dependence as C = E(K, P). Essentially, E is a set of encryption algorithms, and the key K selects one specific algorithm from the set. We see later in this chapter that a cryptosystem, such as the Caesar cipher, is keyless but that keyed encryptions are more difficult to break.

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, KD, inverts the encryption of key KE so that P = D(KD, E(KE,P)). Encryption algorithms of this form are called **asymmetric** because converting C back to P involves a series of steps and a key that are different from the steps and key of E. The difference between symmetric and asymmetric encryption is shown in figure 2.2.



There are many types of encryption. In the next two sections we look at two simple forms of encryption: **substitutions**, in which one letter is exchanged for another, and **transpositions**, in which the order of the letters is rearranged.

Concepts

A secret key cipher is composed of two algorithms

encryption algorithm E

decryption algorithm D

The same key K is used for encryption & decryption K has to be distributed beforehand

Notations

Encrypt a plaintext P using a key K & an encryption algorithm E  
 C = E(K,P)

Decrypt a ciphertext C using the same key K and the matching decryption algorithm D  
 P = D(K,C)

Note: P = D(K,C) = D(K, E(K,P))

Ciphers:

Classical Ciphers

Substitution Ciphers

Transposition Ciphers

Substitution Ciphers

Substitution Ciphers

Shift Ciphers (Caesar Cipher)

Monoalphabetic

Polyalphabetic

Ceaser Cipher

The Caesar cipher is a substitution cipher, named after Julius Caesar. Operation principle:  
each letter is translated into the letter a fixed number of positions after it in the alphabet table. The fixed number of positions is a key both for encryption and decryption.

The Caesar cipher

An example

For a key K=3,  
plaintext letter: ABCDEF...UVWXYZ  
ciphtertext letter: DEF...UVWXYZABC

Hence  
 TREATY IMPOSSIBLE  
is translated into  
 WUHDWB LPSRVVLEOH

Caesar Cipher (Another example)

Earliest known substitution cipher (shift cipher)

Replaces each letter by 3rd next letter

Transformation can be defined as:

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

d e f g h i j k l m n o p q r s t u v w x y z a b c

Caesar Cipher

If each letter is assigned a number (a=0, z=25), Encryption/Decryption defined as:

C = E(p) = (P + 3) mod (26)

P = D(c) = (C – 3) mod (26)

Example:

meet me after the toga party

phhw ph diwhu wkh wrjd sduwb

Caesar Cipher: Encryption Example

K = 7

P = Rome is the greatest empire

C = yvtl pz aol nylhalza ltwpyl

Caesar Cipher: Decryption Example

K = 7

C = yvtl dhz uva ibpsa pu h khf

P = Rome was not built in a day

Caesar Cipher: Decryption with Unknown Key

C=tfnriujuzvdrepkzdvjsvwfivkyvziuvrkyjkyvmrczrekevmvikrjkvfwuvrkyslkfetv

tfnriuj uzv drep kzdvj svwfiv kyvzi uvrkyj; kyv mrczrek evmvi krjkv fw uvrky slk fetv

P = Cowards die many times before their deaths; the valiant never taste of death but once. (K = 17)

Julius Caesar by William Shakespeare

Polyalphabetic Ciphers

Improve security using different cipher letters for different occurrences of same plaintext letter. Make cryptanalysis harder with more letters to guess and flatter frequency distribution. Use a key to select which cipher letter is used for each letter of the message. Repeat from start after end of key is reached

Vigenère Cipher

Simplest polyalphabetic substitution cipher. Effectively multiple Caesar ciphers

Key is multiple letters long K = k1 k2 ... kd

ith letter specifies ith alphabet to use

Repeat from start after d letters in message

Decryption simply works in reverse

Example of Vigenère Cipher

Write the plaintext out

Write the keyword repeated

Use each key letter as a Caesar cipher key

Encrypt the corresponding plaintext letter

Eg using keyword deceptive

plaintext: wearediscoveredsaveyourself

key: deceptivedeceptivedeceptive

ciphertext: zicvtwqngrzgvtwavzhcqyglmgj

Security of Vigenère Cipher

Much more secure than the ciphers we discussed earlier

Have multiple ciphertext letters for each plaintext letter

Hence letter frequencies are obscured

But not totally lost

Security of Vigenère Ciphers

Need to determine key size, since then can attack each Caesar cipher

Repetitions in ciphertext give clues to period

Find same plaintext an exact period apart which results in the same ciphertext

E.g, repeated “VTW” in previous example is at a distance of 9 (zicvtwqngrzgvtwavzhcqyglmgj)