CHAPTER 2

Codes and Encipherment Techniques

2.1 INTRODUCTION

There are two groups of people, one type strongly feels that everything should be secure and must be in the encrypted format. Mostly these are business personnel who use it for commercial purpose. The other groups of the society feel that it is an unnecessary and burden to the network and there should be no sanctuary for the message communication. This group of people feels that in addition to using encipherment techniques there should be more stringent rules for the information exploiters. But my submission is that there should be more stringent rules for the information exploiters as well as better encipherment techniques.

Codes and encipherment techniques are used to write the message in such a way that without the knowledge of key it is impossible to guess the original message. Cryptography means secret writing. Cryptography can restructure and renovate the data, making it safer to communicate between the various computers in the network. The technology is based on the essentials of secret codes, using a cipher key that is either public or private or it may be symmetric or asymmetric in nature that protects the data in powerful ways. The output of the encrypted message is called cipher text or code text whereas the output of the decrypted message is called the decode text and this process is called encipherment.

2.2 ENCIPHERMENT METHODS

The methods of encryption and decryption are easy to understand. Unlike the lock of the door, it is protected by a lock with the key. When one set of keys is required to lock the door and the same set is required to unlock the door then it is referred as symmetric key. Otherwise, if one set of the keys is required to lock the door and the some other set of keys is required to unlock the door then it is referred as asymmetric key. There are two types of crptography.

1. Symmetric key cryptography
2. Asymmetric key cryptography

Plain Text (*PT*) Encryption Key (*K*) Cipher Text (*CT*) i.e., $PT + E(K) = CT$

Cipher Text (*CT*) Decryption Key (*K*) Plain Text (*PT*) i.e., $CT + D(K) = PT$

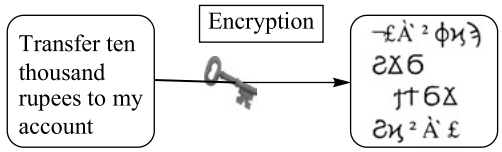


Fig. 2.1 Symmetric key encryption.

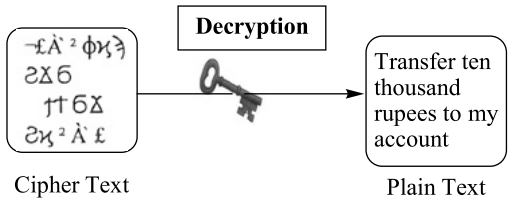


Fig. 2.2 Symmetric key decryption.

Some of the examples of symmetrical key cryptography are substitution cipher, Transposition cipher, Playfair cipher, Hill cipher and DES, etc.

2.6 ASYMMETRICAL KEY CRYPTOGRAPHY

When one set of keys is required to encrypt the message/plain text and some other set of keys is required to decrypt the message/plain text then it is called asymmetrical key cryptography.

Plain Text (PT) Encryption Key (K_1) Cipher Text (*CT*) i.e., PT + $E(K_1)$ = CT

Cipher Text (*CT*) Decryption Key (K_2) Plain Text (*PT*) i.e., CT + $D(K_2)$ = PT

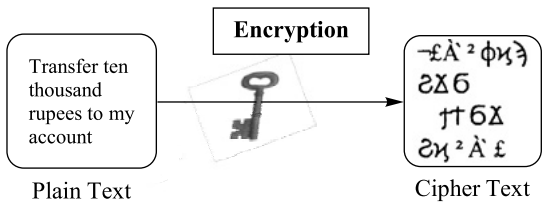


Fig. 2.3 Asymmetric key encryption.

Some examples of asymmetrical key cryptography are Rivest Shamir

Adleman (RSA), Digital Signature Algorithm (DSA), Diffie Hellman, Elliptical curve cryptography, etc.

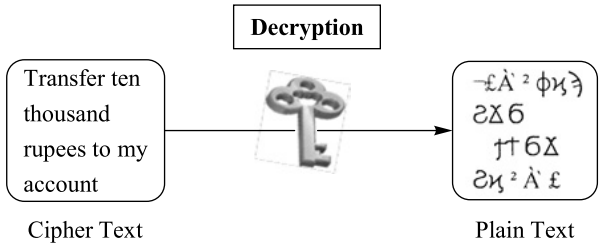


Fig. 2.4 Asymmetric key decryption.

2.6.1 Substitution Cipher

Substitution cipher is a technique in which the cipher text will be generated by using the replacement of the plain text by some defined pattern. The replacement may be the letters from sequence of the letters or it may be replaced by the some sequence of numbers also.

Caesar cipher: Caesar cipher is the earliest known example of substitution technique. The idea was given by the Julius Caesar. It is easily breakable by the Brute force attack.

Features: only 26 key combinations are used using only the alphabets from a to *z*.

- Encryption and decryption method is well defined.
- Plain text could be easily identified.

For example, if the Julius Caesar used a shift of 5, so the plain text is enciphered as cipher text letter CT_i as with the key 5.

Table 2.1 Substitution cipher

$$CT_i = (E\ (PT_i), 5) = (PT_i + 5) \bmod 26$$

PT	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*
CT	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*
PT	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
CT	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*

At the receiver end the above cipher text is decrypted as

$$PT_i = (D\ (CT_i), 5) = (CT_i - 5) \bmod 26$$

The message "computerengineering" is encrypted using as follows:

Table 2.2 Example of substitution cipher

PT	*c*	*o*	*m*	*p*	*u*	*t*	*e*	*r*	*e*	*n*	*g*	*i*	*n*
CT	*H*	*T*	*R*	*U*	*Z*	*S*	*J*	*W*	*J*	*S*	*L*	*V*	*S*
PT	*e*	*e*	*r*	*i*	*n*	*g*							
CT	*J*	*J*	*W*	*N*	*S*	*L*							

in English alphabet system the frequency of occurrence of *I* and *J* is approximately same. It is called polyalphabetic ciphering technique. It means that more than one character is decrypted at one time. This technique was used in the World War I by the British army.

2.6.3.1 Matrix structure

For example, COMPUTE is the key, then it is written in the first 7 blocks of the box and rest of the boxes will be filled by the remaining alphabets from *A* to *Z*.

C	*O*	*M*	*P*	*U*
T	*E*	*A*	*B*	*D*
F	*G*	*H*	*I/J*	*K*
L	*N*	*Q*	*R*	*S*
V	*W*	*X*	*Y*	*Z*

Fig. 2.5 Matrix for play fair cipher

2.6.3.2 Encryption method

To make the cipher the following rules are to be followed:

(a) If the two letters in the pair are in the same row, then the corresponding character for each letter is replaced by the letter to the right, with the first element of the row circularly follows the right.

(b) If the two letters in the pair are in the same column, then the corresponding character for each letter is replaced by the letter below with the top element of the column circularly follows the last.

(c) If the two plain text letters neither exist in the same row nor in the same column, then the corresponding character for each letter is a letter that is its own row but in the same column as the other letter.

(d) If the plain text does not make the exact pair, then it is to create pair by using any extra letter — that extra letter is called filler letter or if there is repetition of the same letter in a pair then it is also separated by a filler letter.

For example, for the above play fair matrix following are the four rules:

(a) The pu is encrypted as UC, and ab is encrypted as BD, etc., since they exist in the same row.

(b) The oe is encrypted as EG, and mx is encrypted as AM, etc., since they exist in the same column.

(c) The ez is encrypted as DW and ts is encrypted as DL, etc., since they neither exist in the same row nor in the same column.

(d) If the message is spoof then the pair is to be made by extra filler letter like *x*. So it will become sp ox of, now it will be encrypted using the rules.

The plain text "where are you" is encrypted by using the play fair cipher.

Cipher Text: XGBNABNBWPMZ

2.6.3.3 Decryption method

Since it is symmetrical key cryptography, the decryption process is the inverse of the encryption method. The cipher text pair will be created as

XG BN AB NB WP MZ

Write down the alphabet matrix with the key as

C	*O*	*M*	*P*	*U*
T	*E*	*A*	*B*	*D*
F	*G*	*H*	*I/J*	*K*
L	*N*	*Q*	*R*	*S*
V	*W*	*X*	*Y*	*Z*

Now according to the method XG will become wh, BN will become er, AB will ea, and so on. In this way the whole cipher text will be decrypted as "where are you".

Features:

- The size of key domain is 25!. It is hard to break.
- Brute force attack is not applicable.
- Cipher text only attack is able to break the message since the structure of plain text is intact.

2.6.4 Hill Cipher

Hill cipher was developed by Lester Hill in 1929. This is again a poly-alphabetic cryptographic method. The size of the plain text encrypted depends upon the size of the key matrix. For example, if the size of the key matrix is 3 × 3, we can encrypt three characters at a time, or if the size of the matrix is 4 × 4 then we can encrypt four characters at a time.

2.6.4.1 Encryption method

- Each letter is assigned a digit in base 26, for example, $A = 0$, $B = 1$, $C = 2$, etc.
- m successive plain text letters are encrypted by m successive cipher text letters.
- Operations are performed using mod 26 method.
- Decryption requires the inverse of the key matrx.

For example, encryption key consists of 3 × 3 matrix as

$$k = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix}$$

= 24, p = 15, t = 19, o = 14, g = 6, r = 17, p = 15, h = 7, y = 24.

So the matrix for

$$P = \begin{pmatrix} 2 \\ 17 \\ 24 \end{pmatrix}$$

Thus, the encipher vector is

$$\begin{pmatrix} 17 & 7 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \times \begin{pmatrix} 2 \\ 17 \\ 24 \end{pmatrix} \bmod 26 = \begin{pmatrix} 273 \\ 852 \\ 494 \end{pmatrix} \bmod 26 = \begin{pmatrix} 13 \\ 20 \\ 0 \end{pmatrix} = \text{N U A}$$

So the cry will become NUA, similarly, we can now encrypt the next three letters like pto in the same manner and make the cipher text.

2.6.4.3 Decryption

In order to decrypt the cipher text the inverse matrix of key is used.

$$k^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \text{and } C = \begin{pmatrix} 13 \\ 20 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \times \begin{pmatrix} 13 \\ 20 \\ 0 \end{pmatrix} \bmod 26 = \begin{pmatrix} 2 \\ 17 \\ 24 \end{pmatrix} = \text{cry}$$

One of the difficulties that could be overlooked that the inverse of the matrix doesn't always exist. If the determinant is 0 or the common factor with the modulus, i.e., factor of 2 or 13 in the case of mod 26 is not used.

Features:

- This technique hides the single letter frequencies unlike the play fair cipher.
- This is secure against cipher text attack only, since the size of the key chosen form a large number of options of matrix formation.
- It can be easily broken with the known plain text attack, since the inverse of the plain text could be found easily.

Suppose that the plain text "friday" is encrypted as using 2 × 2 Hill cipher to return PQCFKU, then k = (15, 16); k = (2, 5); and k = (10, 20). Using the first two plain text cipher text pair we have

$$\begin{pmatrix} 15 & 2 \\ 16 & 5 \end{pmatrix} = K \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} \bmod 26$$

Here the first matrix is the cipher text and the second matrix is plain

text matrix.

The inverse of plain text matrix can be computed:

$$k = \begin{pmatrix} 15 & 2 \\ 16 & 5 \end{pmatrix} \times \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix} = \begin{pmatrix} 137 & 60 \\ 149 & 107 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}$$

This proves that it is easily broken with known plain text attack. In the above example knowing the pair of plain text- cipher text we can easily find the encryption key matrix.

2.7 POLYALPHABETIC CIPHER

In this method more than one letter is to be encrypted at one time. The size of the key is equal to the size of the message. The substitution occurs according to the cryptographic keys. The strength of the technique is that even a single letter may be encrypted by many letters. So it doesn't give any clue to the attackers about the same times occurrence of the same letter. One example of polyalpahabetic cipher is Vigenere cipher. In this cipher the set of 26 letters from a to *z* are shifted from 1 to 25 to make the Vigenere Table 2.5 this means that every twenty-fifth letter is encrypted with the same key.

Each row of the table is a shifting of one character to the right. This means the first row is a shift of 0, second row is a shift of 1, and the last row is shift of 25.

For example, we desire to encrypt the following message:

"welcome to world of cryptography"

Suppose the key used is "security". We start to write the key repeatedly so that the size of the key will become the size of the message.

Plain text	:	welcomet	o world of	cryptogr	aphy
key	:	security	security	security	security

Cipher text : OINWFUXR GAQLCLHD UVAJKWZP STJS

To make the cipher text, take the plain text character from the column and the letter of key from the row and then see the cross point of plain text and key. For the above message the plain text letter is *w*, and the key letter is *s*, see the meeting point of *w* from the column and *s* from the row, it is *O*. Similarly, we can find out the cipher text for the rest of the letters.

The decryption process is inverse of the encryption method, since it is the symmetrical key cryptography.

key	:	security	security	security	security
Cipher text	:	OINWFUXR	GAQLCLHD	UVAJKWZP	STJS
Plain text	:	welcomet	o world of	cryptogr	aphy

x	*y*	*z*
X	*Y*	*Z*
Y	*Z*	*A*
Z	*A*	*B*
A	*B*	*C*
B	*C*	*D*
C	*D*	*E*
D	*E*	*F*
E	*F*	*G*
F	*G*	*H*
G	*H*	*I*
H	*I*	*J*
I	*J*	*K*
J	*K*	*L*
K	*L*	*M*
L	*M*	*N*
M	*N*	*O*
N	*O*	*P*
O	*P*	*Q*
P	*Q*	*R*
Q	*R*	*S*
R	*S*	*T*
S	*T*	*U*
T	*U*	*V*
U	*V*	*W*
V	*W*	*X*
W	*X*	*Y*

ey, wherever
n text letter.
is found see
etters of the

in a defined

by using the

nd fourth to

Cipher text : AWHKSGW

Features:

- It is easy to implement
- Not prone to the Brute force attack.
- Repetition of the key is the weakness of this method.
- It is susceptible to the chosen plain text attack.

2.7.1 One-time Pad

As the name suggests that in one time pad cryptography, the key is used only once. Once the key is used it may never be used for the other pattern of the plain text. Plain text is to be generated by using the key and cipher text. When one set of keys is used to find the plain text then one steam of message is generated. But when the some other key pattern is used then the new plain text is recovered. So, it will confuse the attacker that which of the key is correct and similarly, which of the message is correct. As many keys are used so that many plain text are displayed. We can make table of 30 × 30 which includes four more extra special characters to make the table like Vigenere cipher.

For example, if we consider the following cipher text with a set of keys:

Key : w x c t u r s a y o n m x
Cipher text : PEKLCJLHCHREQ
Plain text : t h i s i s t h e t e s t

But by using the same key and different cipher text some other meaningful message is displayed, which confused the attacker about the right message.

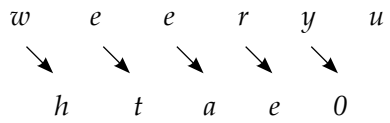
Features:

- Very difficult for attackers to guess the original message.
- Not susceptible to plain text known attack.
- Random key generation is difficult to manage.
- Practically it is difficult to generate the random set of keys which is used only once.

2.7.2 Transposition Cipher

Transposition means the change of position not only in the context of plain text but the change of position of keys also. The simplest form of the transposition cipher is rail fence technique. In this method the plain texts are written as sequence of diagonals and read as sequence of rows.

For example, the plain text " where are you " is written as



The cipher text will become "WEERYUHRAEO". This type of rail fence is of depth 2. We may write the text of any of the depth depending upon the size of the message, but the way of writing and reading of the plain text and cipher text will always follow this pattern.

The other type of the transposition cipher is the columnar cipher. We make the columns of the keys and then the keys are sorted in the alphabetic order. For example:

Key : hack

Plain text : send me your account details.

Then the key is written as

3	1	2	4
H	*A*	*C*	*K*
s	*e*	*n*	*d*
m	*e*	*y*	*o*
u	*r*	*a*	*c*
c	*o*	*u*	*n*
t	*d*	*e*	*t*
a	*i*	*l*	*$*

Now the keys are sorted according to their alphabetic order. *A* comes first so it is numbered as 1, then is the *C* as 2, *H* as 3 and *K* as 4.

The keys are mapped into a substitution box as follows:

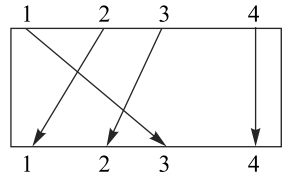


Fig. 2.6 Mapping box for keys.

The cipher text for the above message will become:

EERODINYAUELSMUCTADOCNT$

A precaution will be taken for choosing a key. The key shouldn't have any repeated alphabet. If there is repetition of the same alphabet then we can't give the numbering of the same character. When employing the transposition cipher, one has to add dummy letters like here $ to make it the full length of column.

To decrypt the cipher text we use the inverse method of encryption since it is a symmetrical key cryptography. For the purpose of decryption

- Some sort of decimal/binary number or the alphabets that will be used with the plain text will be chosen as key. The size of the key depends on the type of the encryption method used.
- Output of the plain text when encrypted by the encryption method using a set of keys is called cipher text.
- Cryptanalysis is the process of analyzing the cipher text without any prior knowledge of the key used.
- Substitution cipher is a technique in which the cipher text will be generated by using the replacement of the plain text by some defined pattern.
- The monoalphabetic cipher uses a key, which is a defined rearrangement of the letters of the alphabet.
- Play fair cipher uses the 5 × 5 matrix to accommodate all the alphabets. The letter *I* and *J* are written in the single box.
- Hill cipher is a polyalphabetic cryptographic method. The size of the plain text encrypted depends upon the size of the key matrix.
- If more than one letter is to be encrypted at one time, then it is known as polyalpahabetic cipher.
- In the method of one-time pad cryptography, the key is used only once. Once the key is used it may never be used for the other pattern of the plain text.
- In the transposition cipher the change of position not only in the context of plain text but the change of position of keys also happens.

Key Terms

Encipherment
Public key
Plain text
Decryption algorithm
Substitution cipher
Symmetric key cryptography
Playfair cipher
DES (Data Encryption Standard)
Brute force attack
Elliptical curve cryptography
Hacker
Cracker
Secret writing
Private key
Encryption key
Transposition cipher
Asymmetric key cryptography
Hill cipher
RSA (Rivest Shamir Adleman)
Diffie Hellman
Julius Caesar cipher
KPA (Known Plain text) attack
CPA (Chosen Plain text) attack
CCA (Chosen Cipher text) attack
One-time pad

Multiple-Choice Questions

1. In cryptography, what is cipher?
   (a) Algorithm for performing encryption and decryption
   (b) Encrypted message
   (c) Both (a) and (b).
   (d) None of the above
2. Which one of the following algorithm is not used in asymmetric-key cryptography?
   (a) RSA algorithm
   (b) Diffie-Hellman algorithm
   (c) Electronic code book algorithm
   (d) Elliptical curve cryptography
3. Which of the following is a polyalphabetic cipher?
   (a) Hill cipher
   (b) Caesar cipher
   (c) Linear cipher
   (d) Keyword cipher
4. By using substitution cipher with the key value 5, "computer engineering" will be encrypted as:
   (a) HTRJJWUZSJWJSLVSNSL
   (b) HTRUZSJWJJJWSLVSNSL
   (c) HTRJJWJWJSLUZSVSNSL
   (d) HTRUZSJWJSLVSJJWNSL
5. By using play fair cipher with the key compute, "where are you" will be encrypted as
   (a) XGBBWNABNPMZ
   (b) XGBNABNBWPMZ
   (c) XGBNABNPBWMZ
   (d) XGPBWBNABNMZ
6. In cryptography, _____ the order of the letters in a message is rearranged by
   (a) Transposition cipher
   (b) Substitution cipher
   (c) Hill cipher
   (d) Play fair cipher
7. Transient
   (a) Locates itself in memory so that it can remain active even after its attached program ends
   (b) A class of malicious code that detonates when a specified condition occurs
   (c) Runs when its attached program executes and terminates when its attached program ends

key $\begin{pmatrix} 5 & 1 \\ 2 & 7 \end{pmatrix}$.

9. If the key is defined as key = (16, 5, 2, 20), encrypt the plain text " seek " using a suitable encryption technique.
10. Encrypt and decrypt the message "cryptography and network security" with the key "HACK" using transposition cipher.