Ministry of Higher Education and Scientific Research

Al-Mustansiriyah University

College of Education

Department of Computer Science

4th Class

Computer Security

By

Ass.Lecturer.Mohammed H. AL-Bawi

2016 - 2017

1

Chapter One

Introduction

Is there a security problem in computing?

Is there a security problem in computing?

Comparative between security in computing systems and security in banks

Characteristic	Bank	Computing systems
Size and portability	Sites storing money are Large, not at a portable and Buildings require guards.	Items storing valuable assets are very small and portable
Ability to avoid physical contact	Difficult	Simple
Value of assets	Very high	Variable, from very high to very low

Characteristics of Computer Intrusion

- Any part of computing system which includes a collection of hardware, software, storage media, data, and people that an organization uses to perform computing tasks can be the target of **a crime**.
- **Principle of Easiest Penetration**: An intruder must be expected to use any available means of penetration. This principle implies that computer security specialists must consider all possible means of penetration. The penetration analysis must be done repeatedly, and especially whenever the system change.

Kinds of security breaches(penetration)

- **Vulnerability** is a weakness in the security system, for example, in procedures, design, or implementation that might be exploited to cause loss or harm.
- **A threat** to a computing system is a set of circumstances that has the potential to cause loss or harm
- A human who exploits a vulnerability perpetrates an **attack** on the system. An attack can also be launched by another system.

Kinds of threats

1) **Interception:** means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit

copying of program or data files, or wiretapping to obtain data in a network.

2) **Interruption**: an asset of the system becomes lost, unavailable, or unusable. An example is malicious destruction of a hardware device, erasure of a program or data file or malfunction of an operating system file manager so that it cannot find a particular disk file.
3) **Modification** means an unauthorized party not only accesses but tampers with an asset,. For example, someone might change the values in a database, alter a program so that it performs an additional computation, or modify data being transmitted electronically.
4) **Fabrication**: an unauthorized party might create a fabrication of counterfeit objects on a computing system. The intruder may insert spurious transactions to a network communication system or add records to an existing database.

Security Goals (service)

1) **Confidentiality** ensures that computer-related assets are accessed only by authorized parties. Its means not only reading but also viewing, printing, or simply knowing that a particular asset exists. Confidentiality is sometimes called secrecy or privacy.
2) **Integrity** means that assets can be modified only by authorized parties or only in authorized ways. In this context, modification includes writing, changing, changing status, deleting and creating.
3) **Availability** means that assets are accessible to authorized parties at appropriate times. In other words, if some person or system has legitimate access to a particular set of objects, that access should

not be prevented. For this reason, availability is sometimes known by its opposite, denial of service.

4) **Authentication** is the process by which the information system assures that you are who you say you are; how you prove your identity is authentic.
5) **Accountability (Non-Repudiation):** is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Vulnerabilities of Computing Systems

1) **Hardware Vulnerabilities**: Hardware is more visible than software, largely because it is composed of physical objects. Its simple to attack by adding devices, changing them, removing them.This type of attack might be considered as involuntary or voluntary machine slaughter:

   - **Involuntary machine slaughter**: accidental acts not intended to do serious damage to the hardware such that:electrocuted with power surges drenched with water and People have spilled soft drinks.
   - **Voluntary machine slaughter**: more serious attack usually involves someone who actually wishes to harm the computer hardware such as Machines have been shot with guns and stabbed with knives.

2) **Software Vulnerabilities**: Software can be replaced, changed, or destroyed maliciously, or it can be modified, deleted, or misplaced accidentally.

- **Software Deletion**: Software is surprisingly easy to delete.Access to software is usually carefully controlled through a process called **configuration management** so that software cannot be deleted, destroyed, or replaced accidentally.
- **Software Modification**: S/W easy to modify. Changing a bit or two can convert a working program into a failing one .Depending on which bit was changed, the program may crash when it begins or it may execute for some time before it falters.The program called **logic bomb** when this program maliciously modified to fail when certain conditions are met or when a certain date or time is reached.

Other categories of software modification include

1) **Trojan horse**: a program that overtly does one thing while covertly doing another
2) **Virus**: a specific type of Trojan horse that can be used to spread its "infection" from one computer to another.
3) **Trapdoor**: a program that has a secret entry point.
4) **Information leaks in a program**: code that makes information accessible to unauthorized people or programs.

- **Software theft**: This attack includes unauthorized copying of software. Software authors and distributors are entitled to fair compensation for use of their product, as are musicians and book authors.

3) **Data Vulnerabilities:** data attack is a more widespread and serious problem than either a hardware or software attack because data can be readily interpreted by the general public.

How the three goals of security apply to data

- **Data Confidentiality (secrecy):** the confidentiality of data is a major concern in computer security , since it's available in a form people can read.
- **Data Integrity:** Data are especially vulnerable to modification, Small and skillfully done modifications may not be detected in ordinary ways. Example **salami attack.**
- **Salami attack** is a series of unimportant **attacks** that together result in a larger **attack.**

Principle of Adequate Protection (Timeliness): Computer items must be protected only until they lose their value.

Other Exposed Assets

1) **Networks:** Networks are specialized collections of hardware, software, and data. Each network node is itself a computing system, networks can easily multiply the problems of computer security . The challenges are rooted in a network's lack of physical proximity, use of insecure shared media, and the inability of a network to identify remote users positively.
2) **Access:** Access to computing equipment leads to three types of vulnerabilities, In the first, an intruder may steal computer time to do general purpose computing that does not attack the integrity of the system itself. A second vulnerability involves malicious access to a computing system, whereby an intruding

person or system actually destroys software or data, Finally, unauthorized access may deny service to a legitimate user.

3) **Key People** : People can be crucial weak points in security. If only one person knows how to use or maintain a particular program, trouble can arise if that person is ill, suffers an accident, or leaves the organization. For this reason trusted individuals are usually selected carefully.

Kinds of people who commit computer crimes

1) **Amateurs**: the amateur may start using the computer at work to write letters, maintain soccer league team standings, or do accounting.
2) **Crackers or Malicious Hackers** : system hackers are usually high school or university students attempt to access computing facilities for which they have not been authorized.
3) **Career Criminals:** the career computer criminal understands the targets of computer crime. Criminals begin as computer professionals who engage in computer crime.
4) **Terrorists :** terrorists using computers in three ways: targets of attack, propaganda vehicles and methods of attack.

Methods of Defense

1) **Encryption**
2) **Software Controls**
3) **Hardware Controls**
4) **Policies and Procedures**
5) **Physical Controls**

1) **Encryption**: is the formal name for the scrambling process. We take data in their normal,unscrambled state, called cleartext, and transform them so that they are unintelligible to the outside observer; the transformed data are called enciphered text or ciphertext. Encryption deals with secrecy and integrity.
2) **Software Controls:** Programs must be secure enough to prevent outside attack. Program(S/W) controls include the following**:**

    a. **Internal program controls**: parts of the program that enforce security restrictions, such as access limitations in a database management program.
    b. **Operating system and network system controls**: limitations enforced by the operating system or network to protect each user from all other users.
    c. **Independent control programs**: application programs, such as password checkers, intrusion detection utilities, or virus scanners, that protect against certain types of vulnerabilities.
    d. **Development controls**: quality standards under which a program is designed, coded, tested, and maintained to prevent software faults from becoming exploitable vulnerabilities.

3) **Hardware Controls**: Numerous hardware devices have been created to assist in providing computer security. Some of these device are :

    a. hardware or smart card implementations of encryption.
    b. locks or cables limiting access or deterring theft.
    c. devices to verify users' identities.
    d. firewalls.
    e. intrusion detection systems.

f. circuit boards that control access to storage media.

4) **Policies and Procedures**: A policy is a statement of intent, and is implemented as a procedure or protocol. An example of this type of control is frequent changes of passwords.
5) **Physical Controls:** include locks on doors, guards at entry points, backup copies of important software and data, and physical site planning that reduces the risk of natural disasters.

- **Principle of Effectiveness**: Controls must be used and used properly to be effective. They must be efficient, easy to use, and appropriate. Computer security controls must be efficient enough, in terms of time, memory space, human activity, or other resources used.
- **Overlapping Controls**: several different controls may apply to address a single vulnerability.
- **Periodic control**: it has temporary effective.
- **Principle of Weakest Link**: Security can be no stronger than its weakest link. Failure of any control can lead to a security failure.

2

Chapter Two

Elementary Of Cryptography

Cryptography, Cryptanalysis and Cryptology

- **Cryptography** refer to the way of Protection information by prevent unauthorized people to access this information. Also it means hidden writing.
- Cryptography deals with methods to encrypt and decrypt information.
- **Cryptanalysis** is an attempt to convert ciphertext to plaintext.
- Cryptanalysis deals with analyzing and breaking encryption information.
- Cryptology consists of two subfields, **Cryptography and Cryptanalysis.**

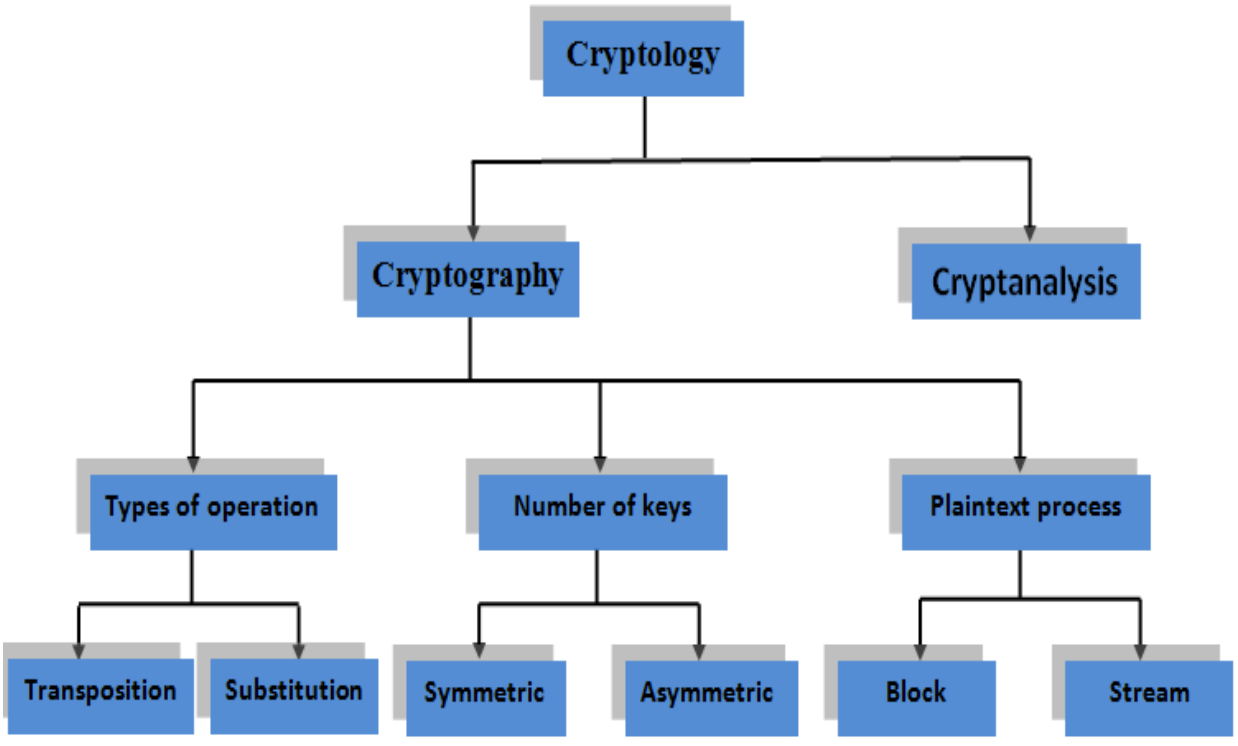
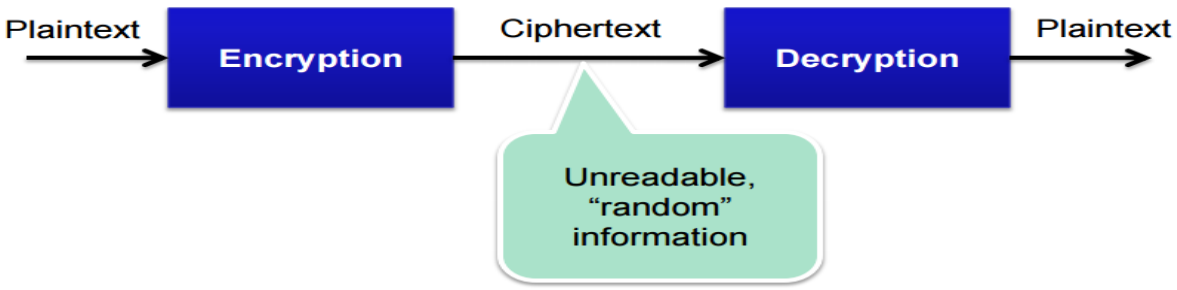


Figure (1): Schematic Representation of Cryptology types

Terminology

- Encryption is the process of encoding a message so that its meaning is not obvious. Other name for Encryption are (encoding, encipher).
- Decryption is transforming an encrypted message back into its normal. .(other name for Decryption are (decoding, decipher).
- System for encryption and decryption is called a cryptosystem.
- 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.
- Plaintext: original form of a message. Plaintext is the message to be transmitted or stored.
- Ciphertext: the encrypted form.



Figure(2) :Encryption and Decryption system

- **Encode** is the process of convert the message into a representation in a standard alphabet.
- **Decode** is the process of convert the encoded message back to its original alphabet and original form.

- P or M: plaintext message ----------C: ciphertext message
- E :Encryption ----------D: Decryption
- C = E(P) and P = D(C) P= D(E(P))(without key)
- C = E(K,P) and P = D(K,E(K,P)) (with same key) (symmetric)
- C = E(KE,P) and P = D(KD, E(KE,P)). (with different key) (Asymmetric).

Breakable Encryption

- An encryption algorithm is called breakable when, given enough time and data, an analyst can determine the algorithm.

Cryptanalysis

- Cryptanalysis refers to the study of **ciphertext** , or cryptosystems with a view to finding **weaknesses** in them that will allow retrieval of the plaintext from the ciphertext , without necessarily knowing the key or the algorithm.

Cryptanalyst can attempt to do any or all of six different things:

1) Break a single message.

2) Recognize patterns in encrypted messages, to be able to break subsequent ones by applying a straightforward decryption algorithm.

3) Find general weaknesses in an encryption algorithm without necessarily having intercepted any messages.

Types of cryptanalytic attack

1) **Ciphertext-only attack** : Only know algorithm and ciphertext.

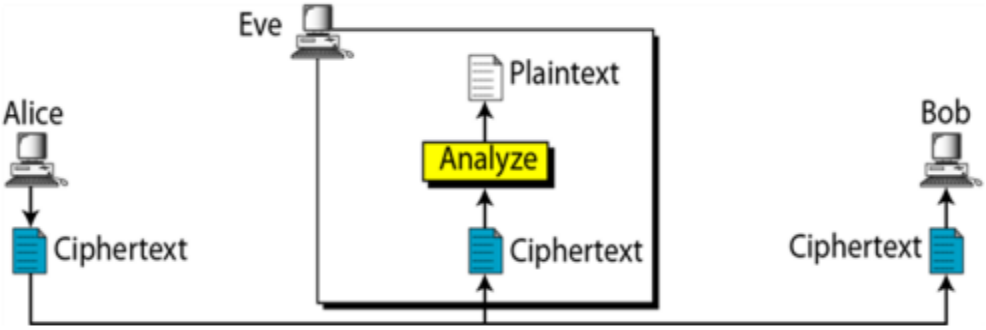


Figure (3): Ciphertext-only attack

2) **Known-plaintext attack** :know algorithm , ciphertext and plaintext for some parts of the ciphertext.

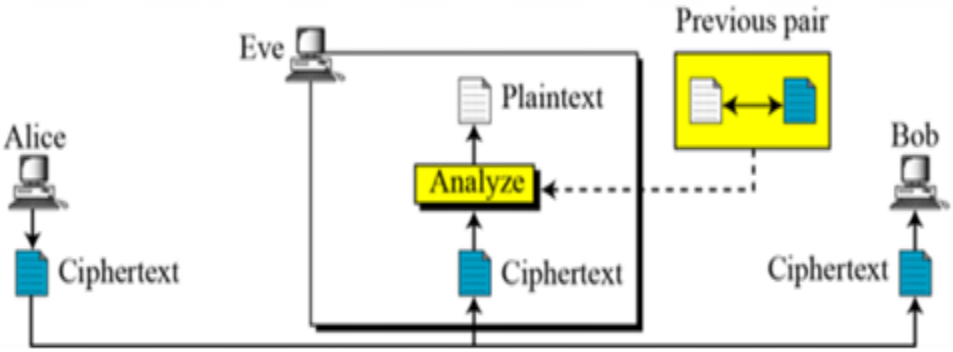


Figure (4): Known-plaintext attack

3) **Chosen-plaintext attack :** know algorithm , ciphertext and various cipher text corresponding to an arbitrary set of plaintext.

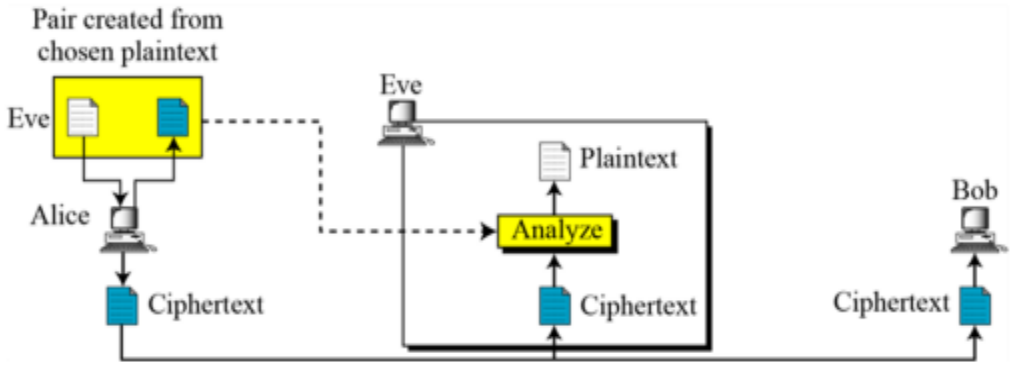


Figure (5): Chosen-plaintext attack

4) **Chosen Cipher text:** know algorithm , ciphertext and various plaintext corresponding to an arbitrary set of ciphertext.

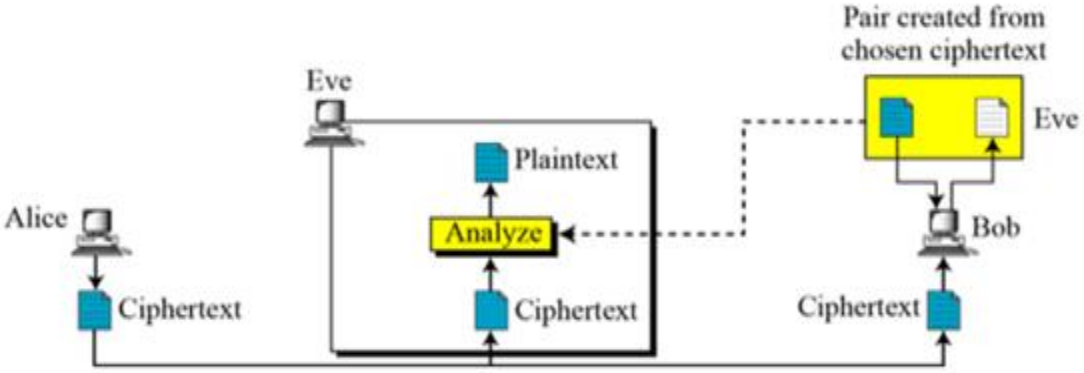


Figure (6): Chosen- Cipher text

Chapter Three

Clssical Cipher Systems

Substitution Ciphers

Substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

There are two types of substitution cipher which are **monoalphabetic** cipher and **polyalphabetic .**

monoalphabetic cipher or simple substitution

- **Caesar Cipher**

- The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar.The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet, it means shift of 3.

plain: 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

cipher: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

- **C = E(3, p) = (p + 3) mod 26**

Example/ Encrypt the following message using caesar cipher?

"TREATY IMPOSSIBLE"

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

plain: t r e a t y i m p o s s i b l e

cipher: W U H D W B L P S R V V L E O H

TREATY IMPOSSIBLE ⟶ WUHDWB LPSRVVLEOH

Another methods to solve previous example

C = (p + 3) mod 26

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext: "**treaty impossible**"

C(t) = 19+3 mod26 = 22 ⟶ W

C(r) = 17+3 mod26 = 20 ⟶ U

C(e) = 4+3 mod26 = 7 ⟶ H

C(a) = 0+3 mod26 = 3 ⟶ D

C(t) =19+3 mod26=22 ⟶ W

C(y) =24+3 mod26=1 ⟶ B

…….etc

Until obtain the ciphertext " **WUHDWB LPSRVVLEOH** "

Advantages of the Caesar Cipher

- Easy to use.

Disadvantages of the Caesar Cipher

- Very simple.
- Easy to recover the plaintext.

➢ Playfair cipher

Playfair: is multiple-letter encryption cipher based on the use of a 5 × 5 matrix of letters.

Steps of Encryption

1) Repeating plaintext letters that are in the same pair are separated with a filler Letter.
2) Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
3) Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.
4) Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

Example/ encrypt the following message using playfair cipher? Key is "**PROBLEMS**"?

Plaintext: "**SHE WENT TO THE STORE**"

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

Plaintext : SH EW EN TX TO TH ES TO RE

Ciphertext: AG MV MK QY QB YT MA QB PM

For **decryption**, if two ciphertext letters are on the same row or column, replace them with the two letters to the left or above, respectively. Otherwise, for each letter choose the letter on the same row and the other letter's column for decryption.

Example/ Deccrypt the following message encrypt with playfair cipher? Key is "**PROBLEMS**"?

Ciphertext: "**AGMVMKQYQBYTMAQBPM**"

Answer/

Ciphertext: AG MV MK QY QB YT MA QB PM

Plaintext : SH EW EN TX TO TH ES TO RE

plaintext message is "**SHE WENT TO THE STORE**"

Characteristics (security) of playfair

- Security much improved over monoalphabetic because it have 26*26 letters.
- Widely used for many years.
- It can broken.

Polyalphabetic cipher

Hill cipher

Hill cipher uses matrix multiplication to encrypt a message. The encryption key is an nxn matrix with an inverse mod 26.

Example/ encrypt the following message using hill cipher with

$$K = \begin{bmatrix} 03 & 07 \\ 05 & 12 \end{bmatrix}$$

"**Herbert Yardley wrote The American Black Chamber"?**

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
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

He rb er ty ar dl ey wr ot et he am er ic an bl ac kc ha mb er

- Now convert letters into number-pair

8 5 18 2 5 18 20 25 1 18 4 12 5 25 23 18 15 20 5 20 8 5 1 13 5 18 9 3 1 14 2 12 1 3 11 3 8 1 13 2 5 18

Make the first pair a column vector (**h (8) e (5)**),and multiply that matrix by the key.

$$\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}\begin{bmatrix} 8 \\ 5 \end{bmatrix}=\begin{bmatrix} 59 \\ 100 \end{bmatrix}$$

we need our result to be mod 26

$$\begin{bmatrix} 59 \\ 100 \end{bmatrix}\equiv\begin{bmatrix} 7 \\ 22 \end{bmatrix}\bmod 26$$

The ciphertext is **G** (7) **V** (22).

For the next pair **r** (18) **b** (2),

For the next pair **p** (16) **j** (10),

Do this for every pair and obtain

"GVPJKGAJYMRHHMMSCCYEGVPEKGVCWQLXXOBMEZAKKG"

Example/ encrypt the following message “code is ready”?

$$\text{Key}=\begin{bmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{bmatrix}$$

Plaintext:	c	o	d	e	I	s	r	e	a	d	y	+z
	2	14	3	4	8	18	17	4	0	3	24	25

add character “z” to the last block to make 3*4 matrix

- Represent the plaintext in to matrix 3*4

$$\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}$$

$$C_1 = P_1 k_{11} + P_2 k_{21} + \cdots + P_m k_{m1}$$
$$C_2 = P_1 k_{12} + P_2 k_{22} + \cdots + P_m k_{m2}$$
$$\cdots$$
$$C_m = P_1 k_{1m} + P_2 k_{2m} + \cdots + P_m k_{mm}$$

$$K = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}$$

$$\underset{C}{\begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}} = \underset{P}{\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}} \underset{K}{\begin{bmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{bmatrix}}$$

Encryption

$$\underset{P}{\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}} = \underset{C}{\begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}} \underset{K^{-1}}{\begin{bmatrix} 02 & 15 & 22 & 03 \\ 15 & 00 & 19 & 03 \\ 09 & 09 & 03 & 11 \\ 17 & 00 & 04 & 07 \end{bmatrix}}$$

Decryption

Multiplicative Inverse

Example/ Find the multiplicative inverse of 11 inZ_{26}.

26=11*2+4

11=4*2+3

4=3*1+1

3=3*1+0

•We are now in reverse compensation starting from one as shown

1=4-(3*1)

1=4-(11-(4*2))

1=4-11+4*2

1=3*4-11

1=3*(26-11*2)-11

1=3*26-6*11-11= 3*26-7*11 so the multiplicative inverse of 11 is -7

Example / Find the multiplicative inverse of 23 inZ_{100}.

100=23*4+8

23=8*2+7

8=7*1+1

7=1*7+0

- Now in reverse way

1=8-(7*1)

1=8-(23-8*2)

1=8-23+8*2

1=3*8-23

1=3*(100-23*4)-23=3*100-12*23-23=3*100-13*23 So the multiplicative inverse of 23 in Z_{100} is -13 or 87(-13 mod 100).

Hill Cipher Decryption

Example/ decrypt the following message "SAK NOXAOJX"

Encryption Key= $\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$?

1) Group the ciphertext into pairs

S A K N O X A O J X

2) Replace each letter by the number corresponding to its position in the alphabet.

S A K N O X A O J X

19 1 11 14 15 24 1 15 10 24

3) Convert each pair of letters into ciphertext vectors.

$$S \rightarrow \begin{bmatrix} 19 \\ 1 \end{bmatrix} \quad K \rightarrow \begin{bmatrix} 11 \\ 14 \end{bmatrix} \quad O \rightarrow \begin{bmatrix} 15 \\ 24 \end{bmatrix} \quad A \rightarrow \begin{bmatrix} 1 \\ 15 \end{bmatrix} \quad J \rightarrow \begin{bmatrix} 10 \\ 24 \end{bmatrix}$$

4) **Find the inverse of the enciphering matrix.**

a) Find the determinant of the enciphering matrix:

$$\det\begin{bmatrix}4 & 1\\ 3 & 2\end{bmatrix} = (4\times 2)-(1\times 3) = 5$$

b) Find the determinant's reciprocal modulo 26.

$$5^{-1}(\text{mod } 26) = 21$$

c) Multiply the reciprocal modulo 26 by the enciphering matrix.

$$21\begin{bmatrix}4 & 1\\ 3 & 2\end{bmatrix} = \begin{bmatrix}42 & -21\\ -63 & 84\end{bmatrix}$$

d) Find the residue modulo 26 of the new matrix.

$$21\begin{bmatrix}4 & 1\\ 3 & 2\end{bmatrix} = \begin{bmatrix}42 & -21\\ -63 & 84\end{bmatrix} = \begin{bmatrix}16 & 5\\ 15 & 6\end{bmatrix}(\text{mod } 26)$$

5) Multiply the deciphering matrix by each ciphertext vector.

$$\begin{matrix}S\to\\ A\to\end{matrix}\begin{bmatrix}16 & 5\\ 15 & 6\end{bmatrix}\begin{bmatrix}19\\ 1\end{bmatrix} = \begin{bmatrix}309\\ 291\end{bmatrix} = \begin{bmatrix}23\\ 5\end{bmatrix}(\text{mod } 26)\begin{matrix}\to W\\ \to E\end{matrix}$$

$$\begin{matrix}K\to\\ N\to\end{matrix}\begin{bmatrix}16 & 5\\ 15 & 6\end{bmatrix}\begin{bmatrix}11\\ 14\end{bmatrix} = \begin{bmatrix}246\\ 249\end{bmatrix} = \begin{bmatrix}12\\ 15\end{bmatrix}(\text{mod } 26)\begin{matrix}\to L\\ \to O\end{matrix}$$

$$\begin{matrix}O\to\\ X\to\end{matrix}\begin{bmatrix}16 & 5\\ 15 & 6\end{bmatrix}\begin{bmatrix}15\\ 24\end{bmatrix} = \begin{bmatrix}360\\ 369\end{bmatrix} = \begin{bmatrix}22\\ 5\end{bmatrix}(\text{mod } 26)\begin{matrix}\to V\\ \to E\end{matrix}$$

$$\begin{matrix}A\to\\ O\to\end{matrix}\begin{bmatrix}16 & 5\\ 15 & 6\end{bmatrix}\begin{bmatrix}1\\ 15\end{bmatrix} = \begin{bmatrix}91\\ 105\end{bmatrix} = \begin{bmatrix}13\\ 1\end{bmatrix}(\text{mod } 26)\begin{matrix}\to M\\ \to A\end{matrix}$$

$$\begin{matrix}J\to\\ X\to\end{matrix}\begin{bmatrix}16 & 5\\ 15 & 6\end{bmatrix}\begin{bmatrix}10\\ 24\end{bmatrix} = \begin{bmatrix}280\\ 294\end{bmatrix} = \begin{bmatrix}20\\ 9\end{bmatrix}(\text{mod } 26)\begin{matrix}\to T\\ \to H\end{matrix}$$

SAKNOXAOJX ⟹ *WE LOVE MATH*

Multiplicative Ciphers

The plaintext and ciphertext are integers in Z_{26}; the key is an integer in Z_{26}.

Ciphertext= (plaintext* key) mod26

Plaintext = (ciphertext* inverse key)mod26

The key needs to be in Z_{26}. This set has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.

Example/ Encrypt the message "**hello**" with a key of **7** We using multiplicative cipher .

Plaintext: h → 07	Encryption: (07 × 07) mod 26	ciphertext: 23 → X
Plaintext: e → 04	Encryption: (04 × 07) mod 26	ciphertext: 02 → C
Plaintext: l → 11	Encryption: (11 × 07) mod 26	ciphertext: 25 → Z
Plaintext: l → 11	Encryption: (11 × 07) mod 26	ciphertext: 25 → Z
Plaintext: o → 14	Encryption: (14 × 07) mod 26	ciphertext: 20 → U

Hello ⟹ XCZZU

Example / Decrypt the following message encrypted using multiplication cipher with **encryption key** =7?

"**XCZZU**"

- First we must find the multiplication inverse of key 7 which equal to 15.

Ciphertext X → 23 /Decryption: (23 * 15) mod 26 plaintext= 7→h

Ciphertext C → 2 /Decryption: (2 * 15) mod 26 plaintext= 4→e

Ciphertext Z → 25/Decryption: (25 * 15) mod 26 plaintext=11→l

Ciphertext Z →/25 Decryption:(25 * 15) mod 26 plaintext=11→l

Ciphertext U →/20 Decryption:(20 * 15) mod 26 plaintext=14→o

➢ Vigenere cipher

The Vigenère cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. It is a simple form of polyalphabetic substitution.

Encryption:

Ek(p1, p2… pm) = (p1+k1, p2+k2…pm+km) (mod 26) **Decryption:**

Dk(c1, c2… cm) = (c1-k1, c2-k2 … cm- km) (mod 26)

Example/ encrypt the following message using vigenere cipher "**C R Y P T O G R A P H Y**"? Key= "**L U C K L U C K L U C K**"?

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext: C R Y P T O G R A P H Y

2 17 24 15 19 14 6 17 0 15 7 24

Key : L U C K L U C K L U C K

11 20 2 10 11 20 2 10 11 20 2 10

Ciphertext = (plaintext + key) mod26

Ciphertext= 13 11 0 25 4 8 8 1 11 9 9 8

Ciphertext= N L A Z E I I B L J J I

Example/ Decrypt the following message encrypted by vigenere cipher "**NLAZEIIBLJJI**"?

Key= "**L U C K** "

Plaintext = (ciphertext – key)mod26

Ciphertext=	N	L	A	Z	E	I	I	B	L	J	J	I
	13	11	0	25	4	8	8	1	11	9	9	8
Key=	L	U	C	K	L	U	C	K	L	U	C	K
	11	20	2	10	11	20	2	10	11	20	2	10
Plaintext=	2	17	24	15	19	14	6	17	0	15	7	24
	C	R	Y	P	T	O	G	R	A	P	H	Y

Vigenere cipher can be seen as combinations of m additive ciphers. As shown in a Vigenere Tableau which can be used to find ciphertext which the intersection of a row and column.

Question/ Distinguish between a **monoalphabetic** cipher and a **polyalphabetic** cipher?

Answer/

In **monoalphabetic** cipher single cipher alphabet is used per message.

In **polyalphabetic** cipher there are multiple ciphertext letters for each plaintext letter, one for each unique letter of keyword.

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

Security of Vigenere Cipher

Any message encrypted by a Vigenere cipher is a collection of as many shift ciphers as there are letters in the key. Makes the use of frequency analysis more difficult.

One Time Pad : is an encryption technique that cannot be cracked (unbreakable) , but requires each plaintext symbol encrypted with a key randomly chosen from a key domain. Which means the key length is equal to the plaintext length. Also called **Vernam-cipher** or **the perfect cipher.**

- **Vernam Cipher** : type of substitution cipher used for data encryption. The Vernam cipher was devised in 1918 by Gilbert S. Vernam.

Example/ Encrypt the following plaintext using Vernam cipher system:

" VERNAMCIPHER"? **Key= 76 48 16 82 44 3 58 11 60 5 48 88**

V E R N A M C I P H E R

Plaintext 21 4 17 13 0 12 2 8 15 7 4 17

+

Key 76 48 16 82 44 3 58 11 60 5 48 88

Ciphertext (97 52 33 95 44 15 60 19 75 12 52 105) mod 26

19 0 7 17 18 15 8 19 23 12 0 1

Ciphertext= **"t a h r s p i t x m a b"**

Decryption

Ciphertext= " **t a h r s p i t x m a b**"

19 0 7 17 18 15 8 19 23 12 0 1

Key = **76 48 16 82 44 3 58 11 60 5 48 88**

plaintext **(-57 -48 -9 -65 -26 12 -50 8 -37 7 -48 -87**)mod 26

21 4 17 13 0 12 2 8 15 7 4 17 ⟶ **V E R N A M C I P H E R**

Cryptanalysis of substitution cipher

1) **Cryptanalysis of Monoalphabetic(Caesar cipher)**: The Caesar cipher can be easily broken even in a ciphertext-only scenario. Two situations can be considered:
    - **a.** an attacker knows (or guesses) that some sort of simple substitution cipher has been used, but not specifically that it is a Caesar scheme(**Frequency Analysis)**
    - b. an attacker knows that a Caesar cipher is in use, but does not know the shift value (**Brute Force Attack)**

Frequency Analysis: If there is a sufficiently large ciphertext, it can be decrypted by comparing the frequency of letters in the cipher text against the frequency of letters in standard English. If the frequency of the letter in the cipher text is almost the same as the frequency of letters in Standard English, we can find out which letter is substituted as there exist a one to one relationship between each letter.

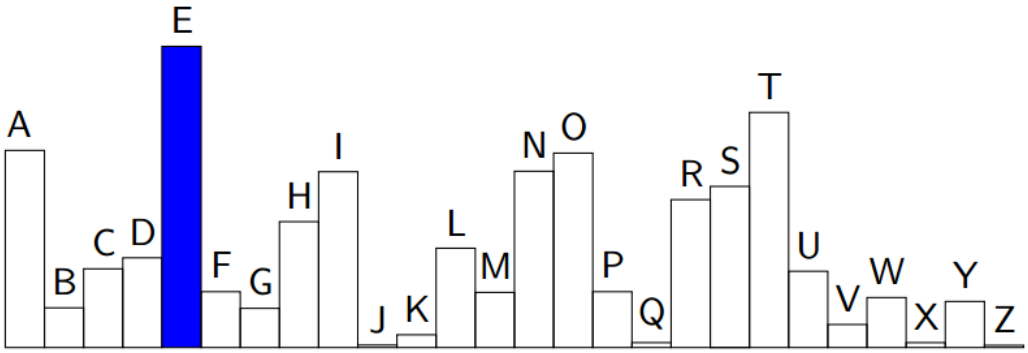


Figure (7): frequency of letters in Standard English

Brute Force Attack: It involves systematically checking all possible keys until the correct key is found. longer keys more difficult to crack than shorter ones.

Example/ Decrypt the following cuphertext:

" **wklv phvvdjh lv qrw wrr kdug wr euhdn** "

As a start, assume that the coder was lazy, and has allowed the blank space to be translated to itself. Hence, the message has actually been enciphered with a 27-symbol alphabet: A through Z and a blank-space separating the words. – If this assumption is true, knowing where the spaces helps to find out what are the small words. – The English language has very few short words like am, is, to, be, he, she, we, and, you, are, and so on.

• There is a strong clue in the repeated r of the word wrr. Two very common three-letter words having the pattern xyy are see and too; other less common possibilities are add, odd and off. Try the more common word first.

Also, the combination **wr** appears in the ciphertext too, so you can determine whether the first two letters of the three-letter word form a separate word by themselves.

– wklv phvvdjh lv qrw wrr kdug wr euhdn

– T--- ------- -- -------OT TOO ------- TO -----

– The –OT could be cot, dot, got, hot, lot, not, pot, rot or tot. A likely choice is not. So q = N

– The word **lv** is also the end of the word **wklv**.

• **lv** cannot be SO, because then **wklv** is T-SO. There is no such word

• **lv** cannot be **IN**, because we have q = N

• **lv** has to be **IS**, so **wklv** is **THIS**

– wklv phvvdjh lv qrw wrr kdug wr euhdn

– THIS ----SS--- -IS NOT TOO H--- -TO -----

By now, we should be able to figure out that the shift has been by three characters for each character in the plaintext. So, the plaintext for the given ciphertext is:

Wklv phvvdjh lv qrw wrr kdug wr euhdn

THIS MESSAGE IS NOT TOO HARD TO BREAK

Some clues to break the code more quickly

- The frequency with which certain letters are used can help us to break the code more quickly:
  - The letters E, T, O, A occur more often the letters J, Q, X, Z.

Frequency distributions of Plaintext :
- E
- T
- A, O, R, N , I
- H , C , D , L, M
- .
- .
- X , J ,Z , Q

- Letters appear to each other with predictable frequency:
  - In usual English, EN, RE, ER,…, and ENT, ION, AND,… are most frequently-occurring coincident pairs (digrams) and triples (trigrams) of letters
- Digrams and trigram frequencies are well-known for all written languages .

- Frequency distribution may not give complete decryption, due to peculiarities of plaintext, but considerably narrows down choices.

Short messages give a cryptanalyst little to work with as the latter works by finding patterns (possible to obtain more with long messages). So, shorter messages are fairly more secure with simple encryption algorithms.

Homework

1)Decrypt the following message using **brute force attack:**

"**UVACLYFZLJBYL**"?

2) Decrypt the following message:

hqfubswlrq lv d phdqv ri dwwdlqlqj vhfxuh frpsxwdxlrq ryhu lqvhfxuh fkdqqhov eb xvlqj hqfubswlrq zh glvjxlvh wkh phvvdjh vr wkdw hyhq li wkh wudqvplvvlrq lv glyhuwhg whk phvvdjh zloo qrw eh uhyhdohg

A=0,B=2,C=0,D=9,E=2,F=6,G=2,H=24,I=2,J=5,K=4,L=12,M=0,N=0,O=4,P=5,Q=16,R=9,S=3,T=0,U=6,V=17,W=9,X=6,Y=4,Z=2.

3)Decrypt the following message:

"Pmmfi zsfwf bzepc ppheo ldvme pvzoj nbyfs"

A=0,B=2,C=1,D=1,E=3,F=4,G=0,H=1,I=1.J=1,K=0,L=1,M=3,N=1,O=2,P=5,Q=0,R=0,S=2,T=0,U=0,V=2,W=1,X=0,Y=1Z=3.

2) Cryptanalysis of polyalphabetic substitution

A) Kasiski method: is a method of attacking polyalphabetic substitution ciphers, such as the Vigenère cipher.

- Repetitions occur when characters of the key appear over the same characters in the ciphertext.
- The number of characters between repetitions must be a multiple of the length of the key.
- find the candidates of the key length
- rely on the regularity of English:
  - high frequency
  - ending: th, ing, ed, ion, tion, ation, etc.
  - beginning: im, in, un, re, etc.
  - pattern: eek-, oot-, -our-, etc.
  - word: of, and, to, the, with, are, is, that, etc.

Steps of Kasiski method

1) Identify repeated patterns of three or more characters.
2) For each pattern write down the position at which each instance of the pattern begins.
3) Compute the difference between the starting points of successive instances.
4) Determine all factors of each difference.
5) If a polyalphabetic substitution cipher was used, the key length will be one of the factors that appear often in step 4.

Example/ xugghr trtei mngt**h ggf**kl rtra**h ggf**ui fbdnc kmlp**h ggf**ty nbvcf?

- **15 ⟶ 25-15=10 2,5,10**
- **25 ⟶ 40-25=15 3,5,15**
- **40 ⟶ 40-15=25 5,25**

Key length= 5

Example/**vhvs**sp**quce**mrvbvbbb**vhvs**urqgibdugrnicj**quce**rvuaxss r?

1 ⟶ 19-1=18 2,3,6,9,18

7 ⟶ 37-7=30 2,3,5,6,10,15,30

Key length= 3 or 6

B) Index of Coincidence(IC): a measure of the variation between frequencies in a distribution.

$$\frac{\sum(f_i * (f_i-1))}{N(N-1)}$$

- f_i is the count of letter **i** (where **i = A,B,...,Z**) in the ciphertext,
- **N** is the total number of letters in the ciphertext.

Example/ The IC of the text **"THE INDEX OF COINCIDENCE"** would be given by:

c(3*2)+ d(2*1)+ e(4*3)+ f(1*0)+ h(1*0)+ i(3*2)+ n(3*2)+ o(2*1)+ t(1*0)+ x(1*0) = 34

divided by N*(N-1) = 21*20 = 420

which gives us an IC of 34/420 = 0.0809

Example/The IC of the text **BMQVSZFPJTCSSWGWVJLIO** would be given by:

b(1*0)+ c(1*0)+ f(1*0)+ g(1*0)+ i(1*0)+ j(2*1)+ l(1*0)+ m(1*0)+ o(1*0) + p(1*0)+ q(1*0)+ s(3*2)+ t(1*0)+ v(2*1)+ w(2*1)+ z(1*0) = 12

divided by **N*(N-1) = 21*20 = 420**

which gives us an **IC** of **12/420 = 0.0286**

Homework

EX/Find the **IC** for the following message:

"WKHUH DUHWZ RZDBV RIFRQ VWUXF WLQJD VRIWZ DUHGHVLJQRQHZDBLVWRPDNHLWVRVLPSOHWKDWWKHUHDUHRE YLRXVOBQRGHILFLHQFLHVDQGWKHRWKHUZDBLVWRPDNHLWVRF RPSOLFDWHGWKDWWKHUHDUHQRREYLRXVGHILFLHQFLHVWKHIL UVWPHWKRGLVIDUPRUHGLIILFXOW"

The frequency count is shown below:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	4	0	15	2	9	7	27	8	2	9	20	0
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	4	5	10	19	2	0	12	15	22	4	2	5

$$\textbf{Length of Key (L)} = \frac{0.027n}{(n-1)IC - 0.038n + 0.065}$$

Uses of IC

- IC can be used to test if text is plain text or cipher text.
- Text encrypted with a substitution cipher would have an IC closer to 0.0385, since the frequencies would be closer to random.
- English plaintext would have an IC closer to 0.0667.
- This measure allows computers to score possible decryptions effectively.

Transposition Cipher

- In transposition systems, the (plaintext) cleartext is left unchanged but rearrange the characters order. Transpositions cipher also known as a permutation cipher. The letters of the plaintext are just rearranged in some fashion.

Simple Types of Transposition Ciphers

1) Keyless Transposition Ciphers: - A good example of a keyless cipher is the **rail fence cipher**. The ciphertext is created reading the pattern row by row.

Example/ encrypt the following message" **CHUCK NORRIS IS A TOUGH GUY**"

C U K O R S S T U H U

H C N R I I A O G G Y

Ciphertext= "**CUKORSSTUHUHCNRIIAOGGY**"

2) Simple Columnar Transpositions: Write the message in rows of a fixed length, and then read out again column by column.

- The columns are chosen in some scrambled order.
- Both the length of the rows and the permutation of the columns are usually defined by a key.

Example/ Let the plaintext is "**WE ARE DISCOVERED FLEE AT ONCE**" and the encryption key "**ZEBRA**".

Z	E	B	R	A
W	E	A	R	E
D	I	S	C	O
V	E	R	E	D
F	L	E	E	A
T	O	N	C	E

Ciphertext= "**EODAEASRENEIELORCEECWDVFT**"

Example/ encrypt the following message "**WE ARE DISCOVERED FLEE AT ONCE**"? Encryption key=632415?

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	Q	K	J	E	U

Ciphertext= "**EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE**"

Cryptanalysis of transposition cipher system

Since transposition does not affect the frequency of individual symbols, simple transposition can be easily detected by the cryptanalyst by doing a frequency count. If the ciphertext exhibits a frequency distribution very similar to plaintext, it is most likely a transposition. This can then often be attacked by sliding pieces of ciphertext around, then looking for sections that look like anagrams of English words, and solving the anagrams. Once such anagrams have been found, they reveal information about the transposition pattern, and can consequently be extended.

Most common bigrams and trigrams:

Bigrams

TI	TH	ON	HE	AT	RE	ER	EN	ES	IO	AN	OF	NT	AL	ND

Trigrams

THE	ION	TIO	ENT	AND	ING	EVO	PRO	HER	GEN	LUT

Product Cipher : An encryption system that uses multiple ciphers in which the cipher text of one cipher is used as the clear text of the next cipher. Usually, substitution ciphers and transposition ciphers are used alternatively to construct a **product cipher**.

4

Chapter Four

Modern Symmetric Ciphers (Stream&Block)

Modern Symmetric Ciphers

(Stream Cipher and Block Cipher)

1) **Stream cipher:** is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). This is achieved by adding a bit from a key stream to a plaintext bit. Basic Idea of stream cipher comes from One-Time-Pad cipher. The main advantage of one time pad is unbreakable system cipher but the main drawback (disadvantage) of One-Time-Pad cipher are Key distribution & Management difficult. Stream ciphers overcome the drawback of one time pad by generated keystream in pseudorandom fashion from relatively short secret key. **Pseudorandomness** is sequences appears random to a computationally bounded adversary.

Encryption : $c_i = m_i \oplus k_i \qquad i = 1,2,3,\ldots$

m_i : plain-text bits.

k_i : key (key-stream) bits

c_i : cipher-text bits.

Decryption : $m_i = c_i \oplus k_i \qquad i = 1,2,3,\ldots$

Types of stream cipher

A) Synchronous Stream Ciphers: Key-stream is independent of plaintext and ciphertext and both sender &receiver must be synchronized.

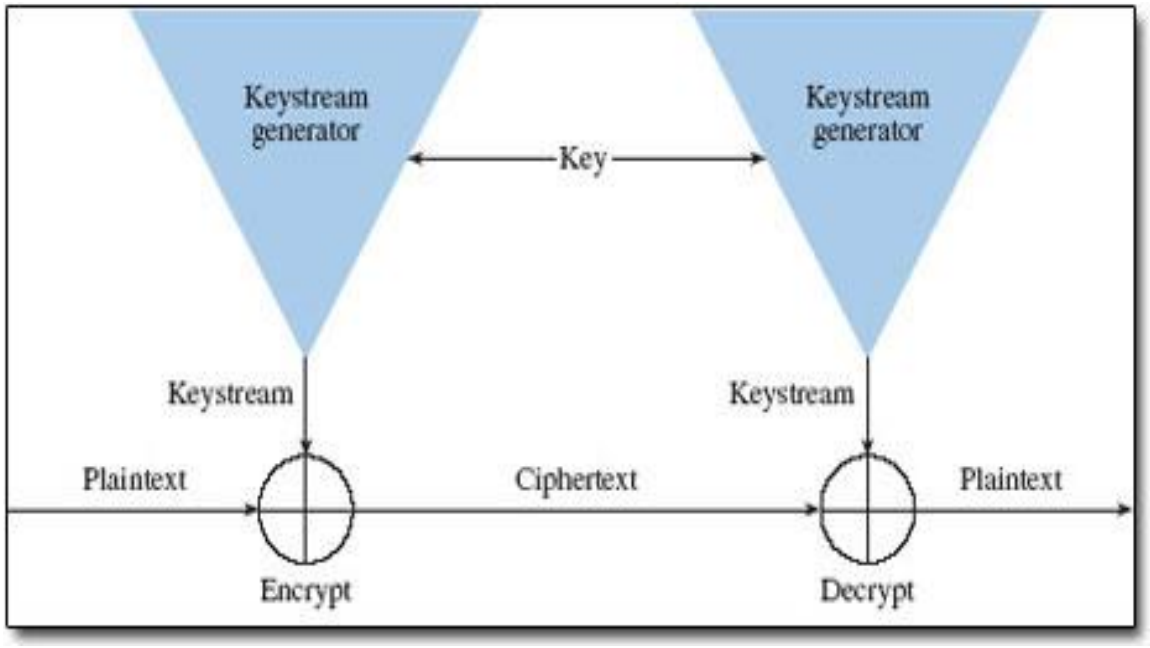


Figure (8): Synchronous Stream Ciphers

B) Self-Synchronizing Stream Ciphers: Key-stream is a function of fixed number of ciphertext bits.

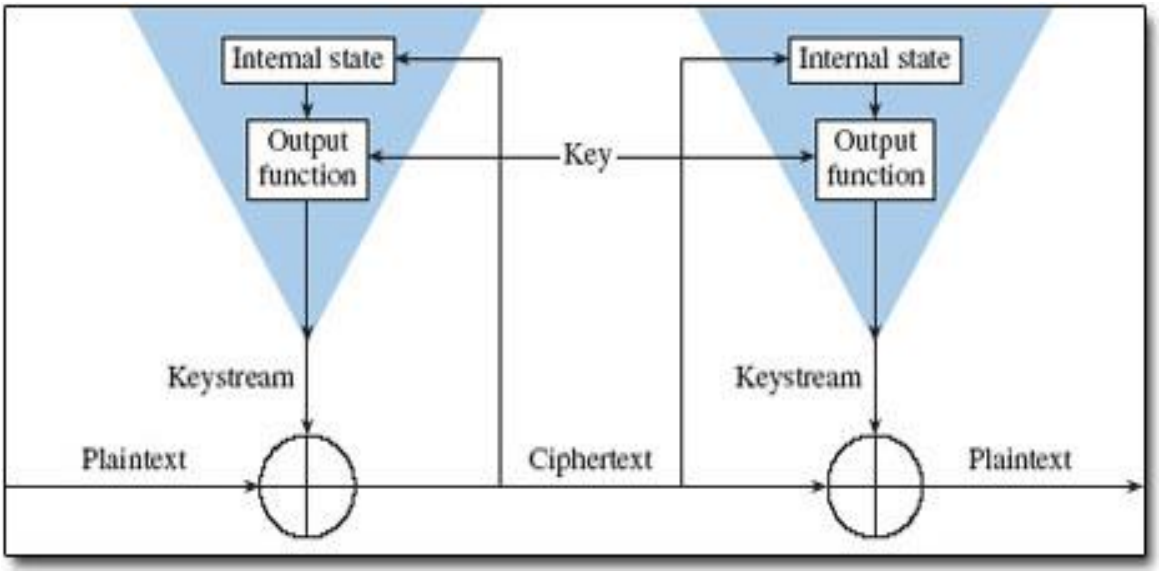


Figure (9): Self-Synchronizing Stream Ciphers

Comparative between Synchronous and Self-Synchronizing Stream

Synchronous stream cipher	Self-Synchronizing Stream
Key-stream is independent of plaintext and ciphertext	Key-stream is not independent of plaintext and ciphertext
not propagating errors	Limited error propagation
Active attacks can easily be detected	Active attacks cannot be detected
Example/ RC4	Example/ CFB

2) Block cipher: Plaintext is divided into blocks of fixed length and every block is encrypted one at a time. Columnar transposition is an example of this type.

Comparative between stream and block ciphers

Stream cipher	Block cipher
Encrypt one bit or byte at a time	Encrypt one block at a time
High speed and low error propagation	Slower and high error propagation
Low diffusion	High diffusion
Example/ RC4 and FISH	Example/DES and IDEA
Susceptibility to attacks on integrity	Immunity to insertions

Block cipher operation modes

1) Electronic Code Book(ECB).
2) Cipher-Block Chaining (CBC).
3) Cipher FeedBack (CFB).
4) Output Feedback Mode (OFM).

1) <u>Electronic Code Book(ECB)</u> : The message is divided into blocks, and each block is encrypted separately.

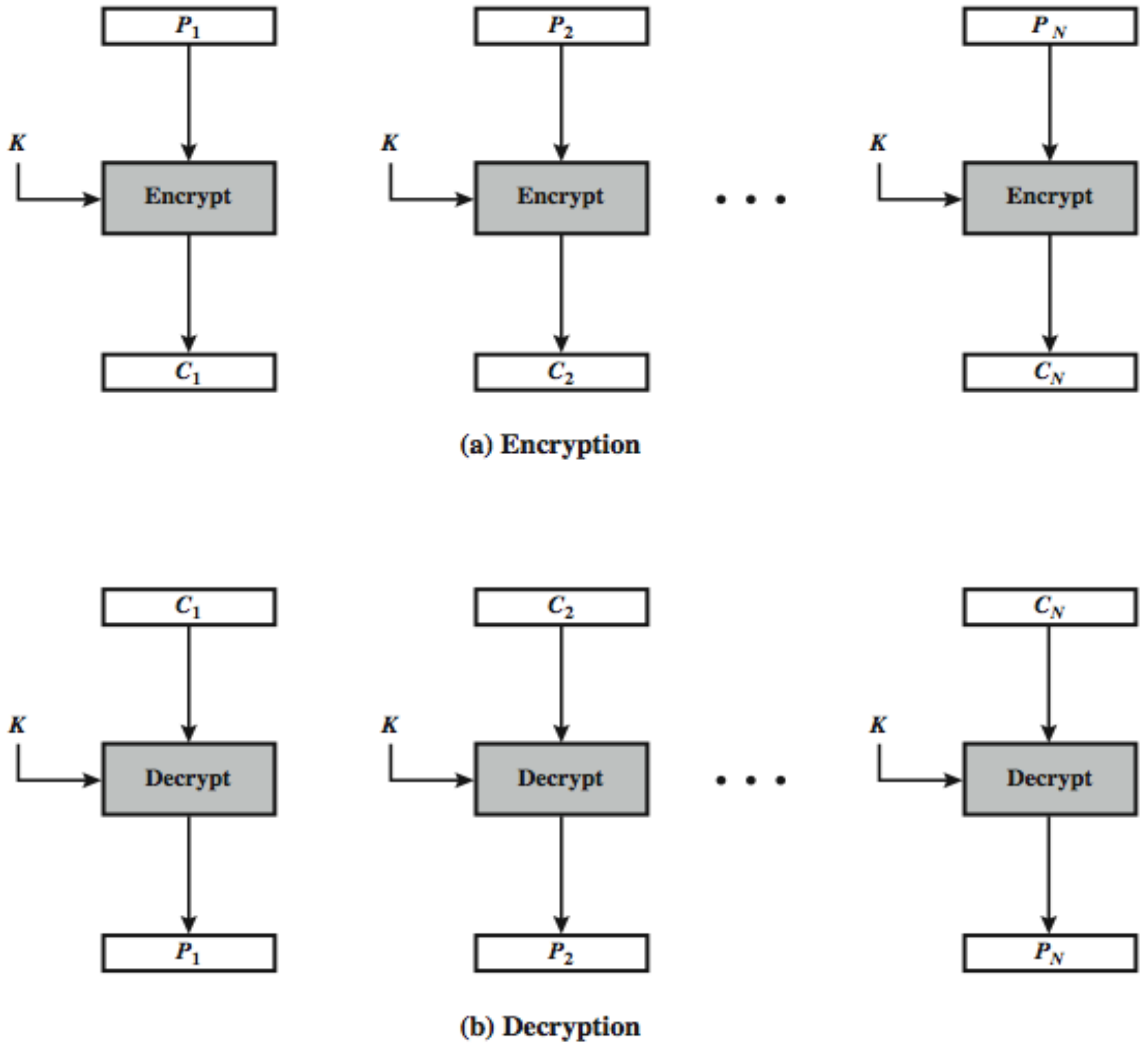


Figure (10): Encryption and Decryption(ECB).

The main advantage of ECB is that it's simple and the main disadvantage is that the identical plaintext blocks are encrypted into identical ciphertext blocks. ECB used in the secure transmission of short pieces of information.

2) <u>Cipher-Block Chaining (CBC)</u> : each block of plaintext is XORed with the previous ciphertext block before being encrypted.

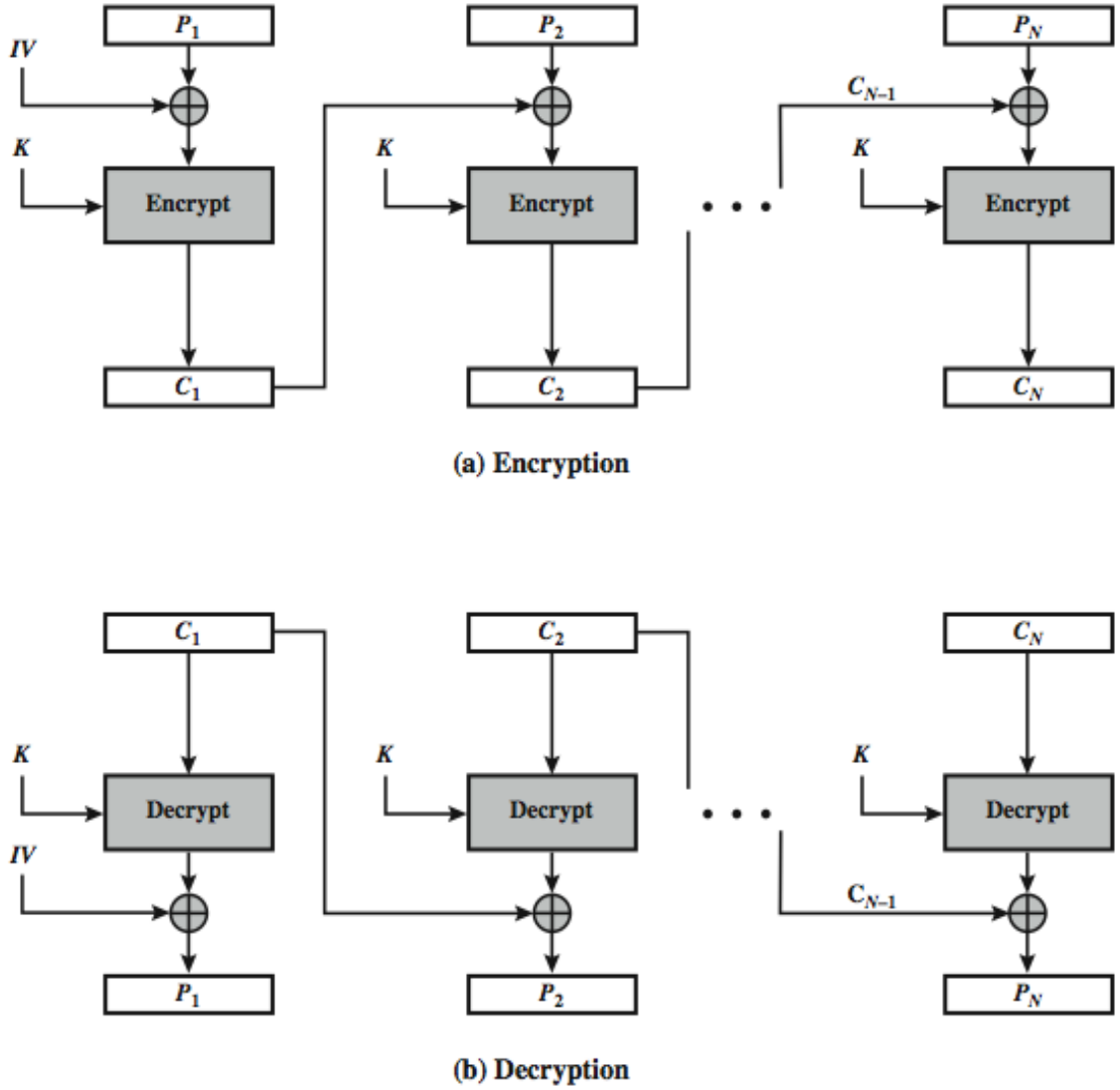
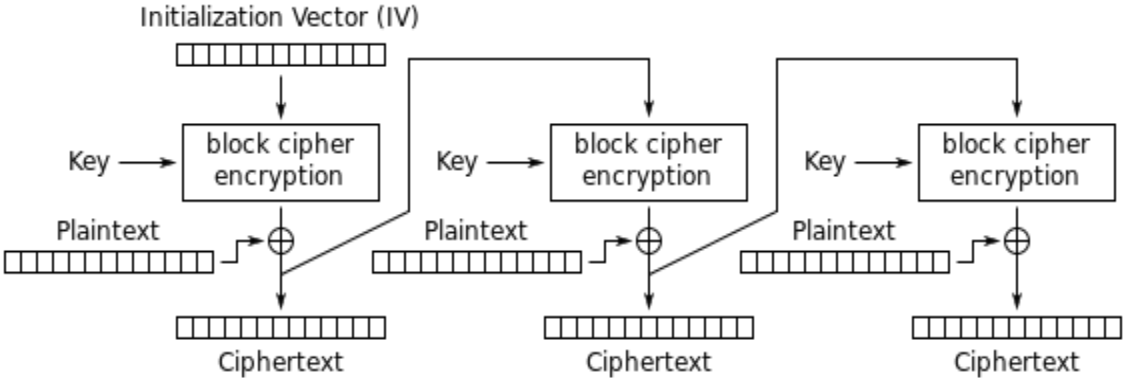


Figure (11): Encryption and Decryption(CBC)

The main advantage of CBC is that the repeated same plaintext block result different ciphertext block.

3) <u>Cipher FeedBack (CFB)</u> : plaintext is treated as a stream of bits. it Uses for stream data encryption, authentication.



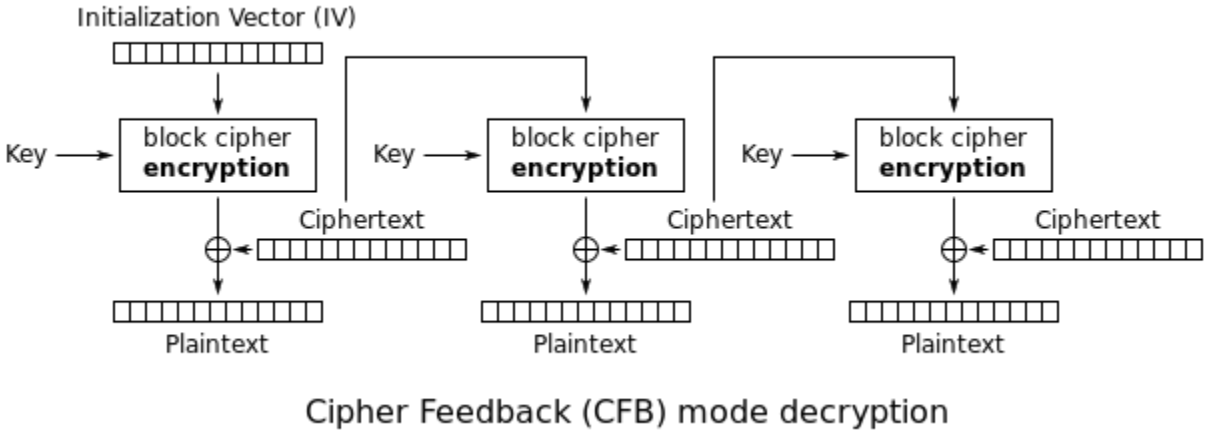


Figure (12): Encryption and Decryption(CFB)

4) **<u>Output Feedback Mode (OFM)</u> :**The block cipher is used as a stream cipher. Very similar to CFB But output of the encryption function is feedback, instead of ciphertext.

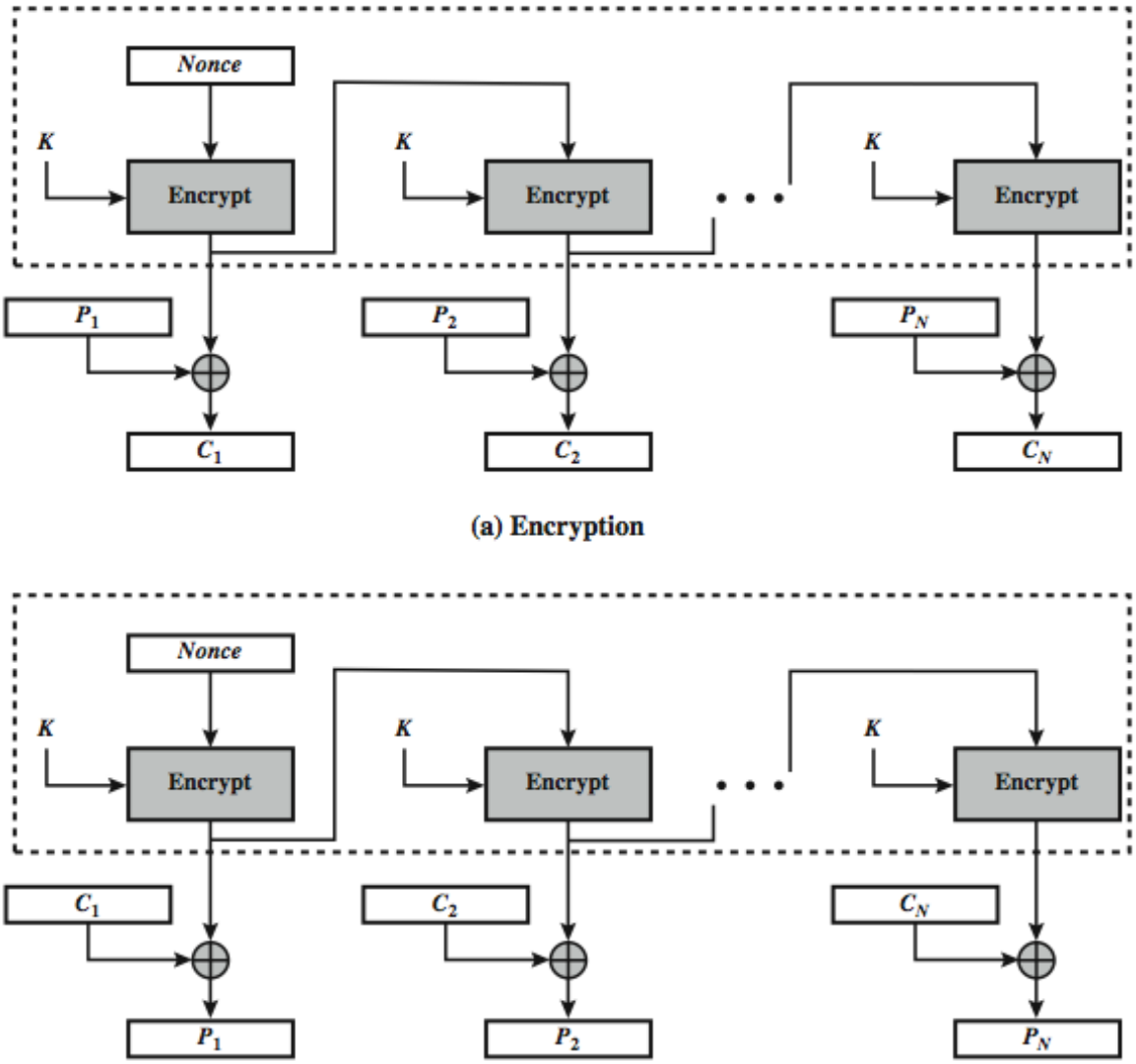


Figure (13): Encryption and Decryption(OFM)

Shannon Characteristics For Good Cipher

1) The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption.
2) The set of keys and the enciphering algorithm should be free from complexity.
3) The implementation of the process should be as simple as possible.
4) Errors in ciphering should not propagate and cause corruption of further information in the message.
5) The size of the enciphered text should be no larger than the text of the original message.

Feistel Cipher Structure

Feistel Cipher: is an iterative block cipher that Process through multiple rounds .

Steps of Feistel cipher

1) Partitions input block into two halves.
2) Perform a substitution on left plaintext half.
3) Based on round function of right half & sub key.
4) Swapping halves.

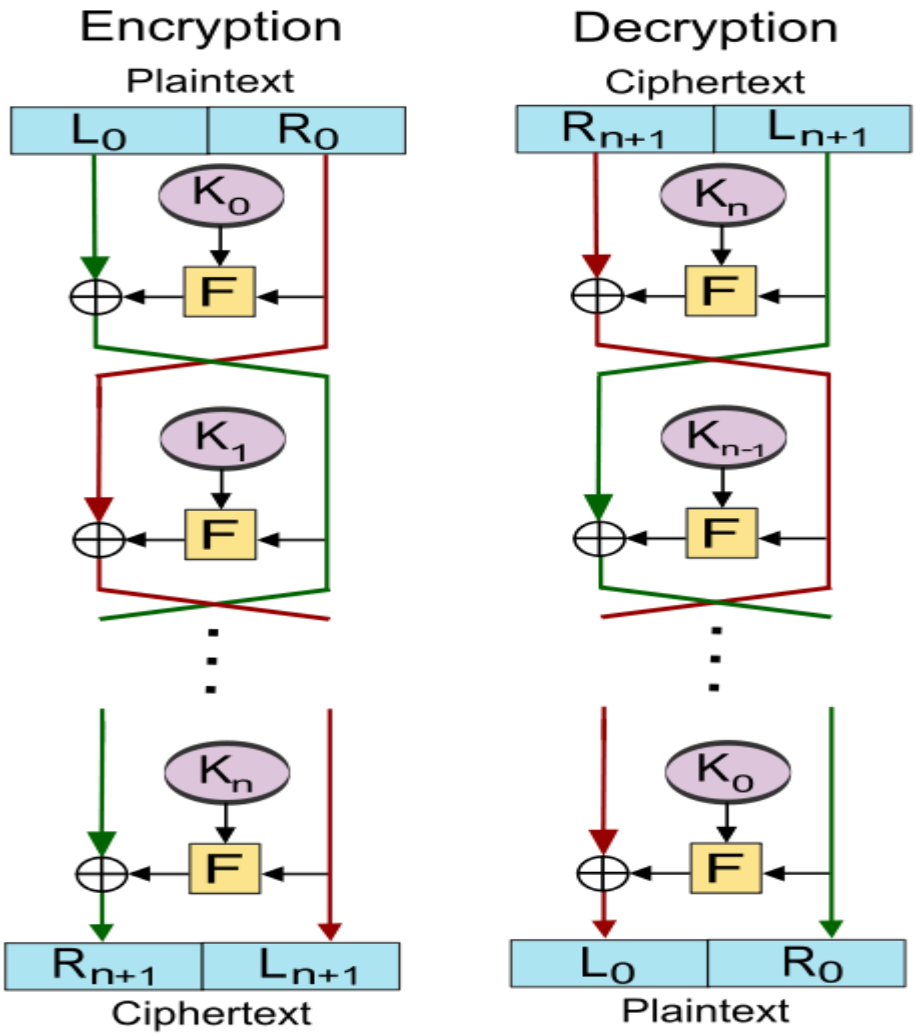


Figure (14): Feistel cipher

Data Encryption Standard (DES)

DES is the most widely used block cipher in the world adopted by National Bureau of Standards (NBS) in 1977. For DES, plaintexts are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption.

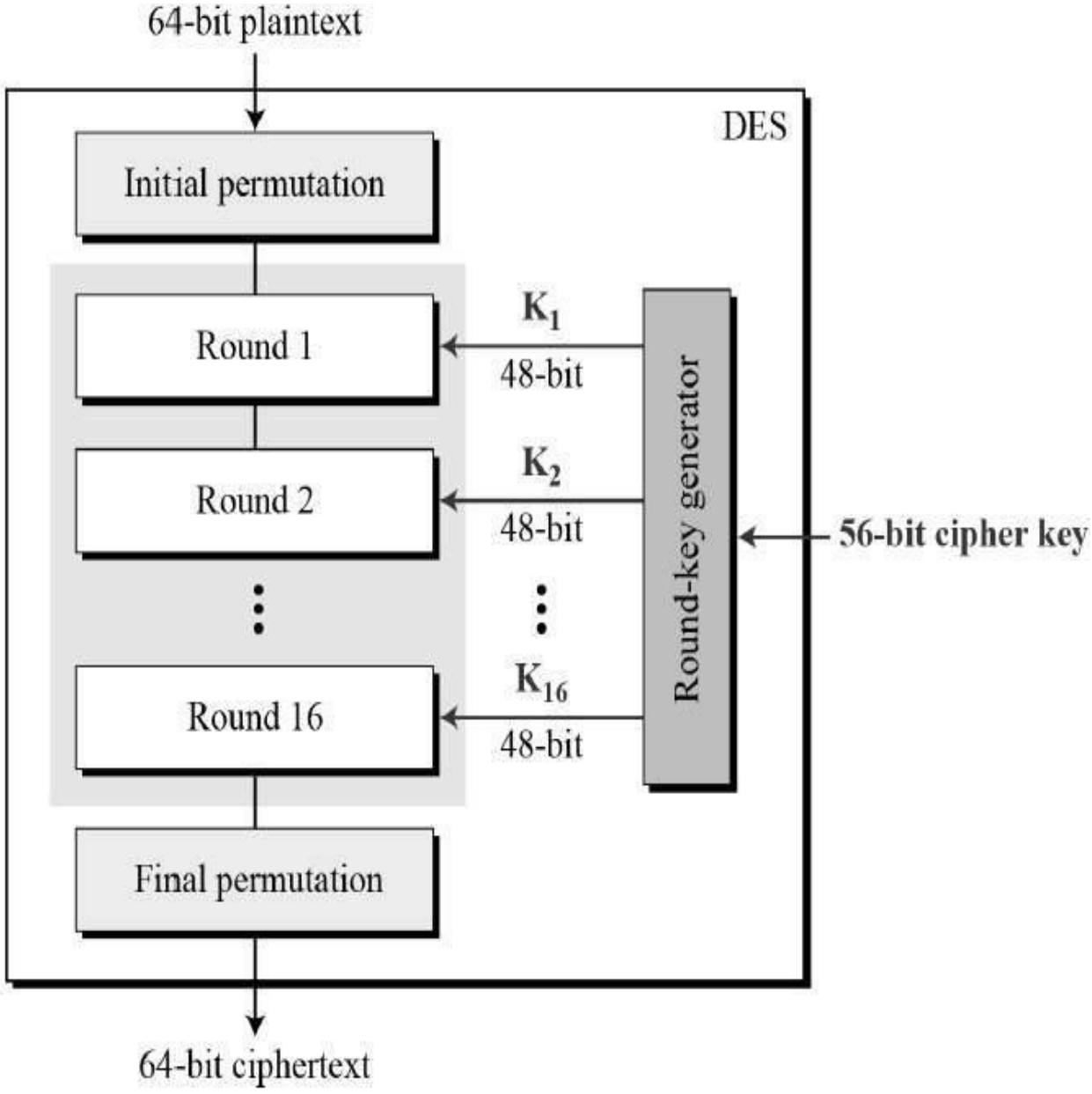


Figure (15): DES Algorithm Structure

Steps of DES algorithm

1) Input 64-bit plaintext
2) Initial permutation(IP)
3) 16- Rounds(R)
4) Final permutation

Initial permutation (IP)

The initial permutation occurs before round 1, it transposes the input block as described in this table:

Table(1): Initial permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

The initial permutation and the corresponding final permutation do not improve DES's security, just make DES more complex should be read left to right, top to bottom.

For example, the initial permutation moves bit 58 of the plaintext to bit position 1, bit 50 to bit position 2, bit 42 to bit position 3, and so forth.

DES Round structure

In each round : -

1) The 64 bits key are shifted to 56 bits, and 48 bits are selecting from the 56 bits of the key.
2) The right half of the plaintext (32 bit) are expanding to 48 bits through an expansion permutation and combined with 48 bits of key through an XOR.
3) Sent through 8 S-boxes to producing 32 new bits.
4) Permuted the 32 bit(output of S-boxes).
5) These four operations make up Function (F).
6) The output of Function is combining with left half through XOR.
7) The result of these operations becomes the new right half; the old right half becomes the new left half.

   $L_i = R_{i-1}$, $R_i = L_{i-1}$ XOR $F(R_{i-1}, K_i)$

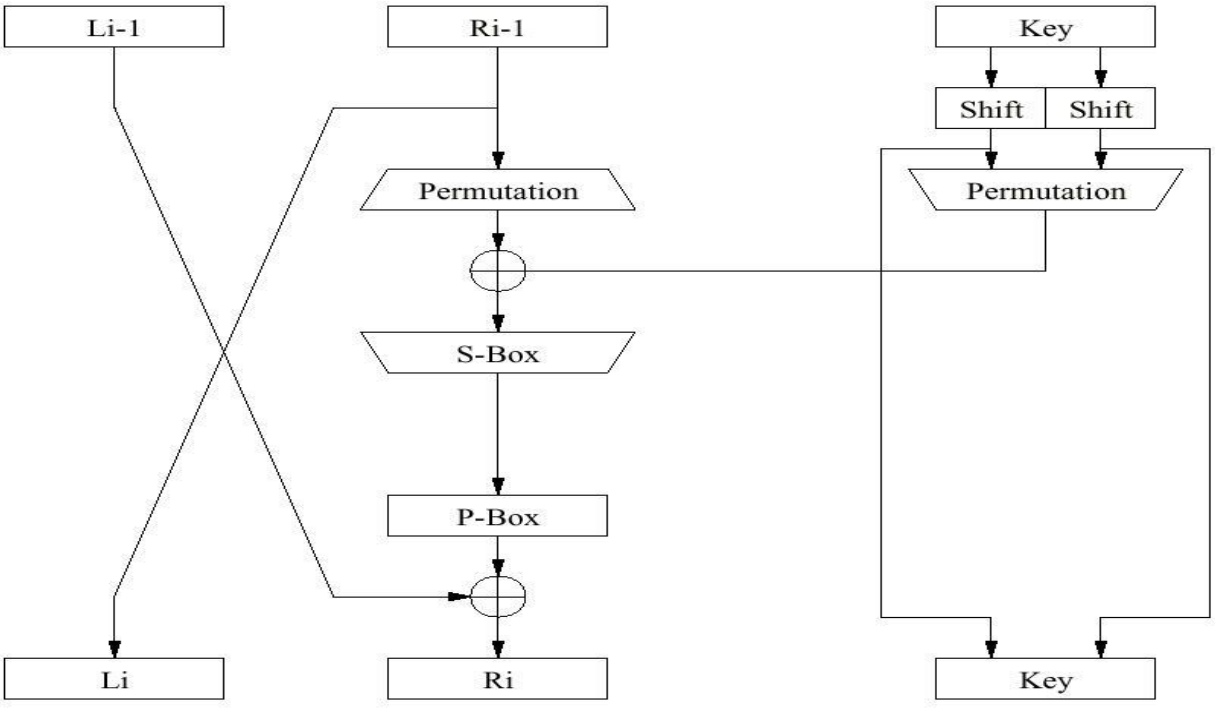


Figure (16): DES Round structure

Key Transformation

1) Initially, the 64-bit DES key is reduced to a 56-bit key by ignoring every eighth bit using permutation choice one.

Table(2): permutation choice one

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

2) Splits the 56-bits key bits into 2 halves (C_i and D_i), each of them 28-bits.
3) The halves C_i and D_i are circularly shifted left by either one or two bits, depending on the round.

Number of Key Bits Shifted per Round															
Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Number	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

4) After being shifted, The 56-bits key is reduced to a 48-bits subkey using permutation choice two.

Table (3): permutation choice two

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

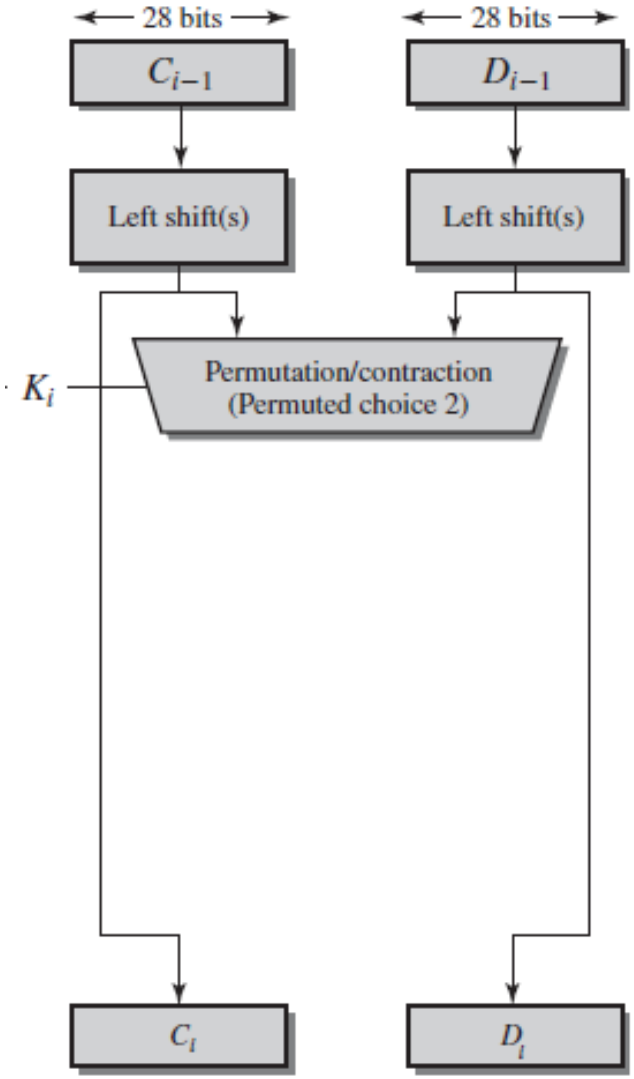


Figure (17): Key Transformation

The Expansion Permutation

This operation expands the right half of the plaintext(R_i) from 32 bits to 48 bits. This operation has two purposes:

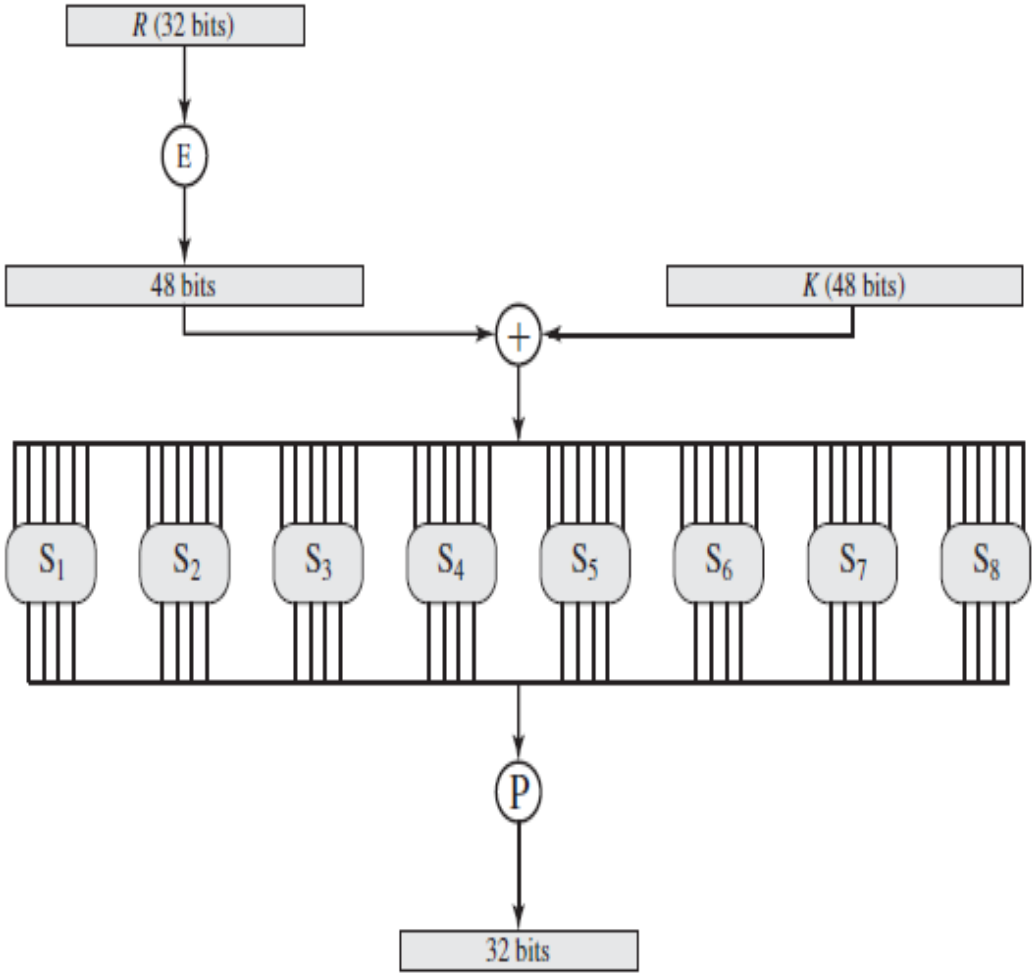
1) It makes the right half the same size as the key for the XOR operation
2) It provides a longer result that can be compressed during the substitution operation.

Table (4): Expansion Permutation

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

The S-Box Substitution

1) The 48-bit moves to 8 S-Boxes.
2) Each S-box has a 6-bit input and a 4-bit output.
3) The 48 bits are divided into eight 6-bit sub-blocks.
4) Each 6-bit block is operated on by one S-box:
    a. Outer bits 1 and 6 (row bits)
    b. Inner bits 2 – 5 (column bits)



Figure(18): S-BOX

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Example

48-bit Input

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	1	1	1	0	1	0	1	0	0	1	0	1	1	0	1	0	1	0	1	1	0	1	1

25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
0	0	1	1	1	0	1	1	0	1	0	0	1	1	0	1	0	0	1	1	1	0	0	0

Substitution with Permutation

	6-bit input	Row value	Column value	S-box result	4-bit output
S-box S1	011101	1 (01)	14 (1110)	3	0011
S-box S2	010010	0 (00)	9 (1001)	7	0111
S-box S3	110101	3 (11)	10 (1010)	14	1110
S-box S4	011011	1 (01)	13 (1101)	10	1010
S-box S5	001110	0 (00)	7 (0111)	6	0110
S-box S6	110100	2 (10)	10 (1010)	4	0100
S-box S7	110100	2 (10)	10 (1010)	6	0110
S-box S8	111000	2 (10)	12 (1100)	15	1111

The P-Box Permutation

The 32-bit output of the S-box substitution is permuted according to a P-box. This permutation maps each input bit to an output position; no bits are used twice and no bits are ignored.

Table (5): P-Box Permutation

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Finally, the result of the P-box permutation is XOR with the left half of the initial 64-bit block. Then the left and right halves are switched and another round begins.

The Final Permutation

The final permutation is the inverse of the initial permutation.

(a) Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b) Inverse Initial Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Table (6): inverse and initial permutation

Note that the left and right halves are not exchanged after the last round of DES; instead the concatenated block R16L16 is used as the input to the final permutation.

Decrypting DES

- The same algorithm used for encryption and decryption.
- Reversed the order of key (Key_{16}, Key_{15}, … Key_1).

For example:

1. IP undoes IP^{-1} step of encryption.
2. First round with K_{16} undoes , second round with K_{15} and soon.
3. Final permutation undoes initial permutation.
4. The algorithm that generates the key used for each round is circular as well.
5. The key shift is a right shift and the number of positions shifted is 0, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 1.

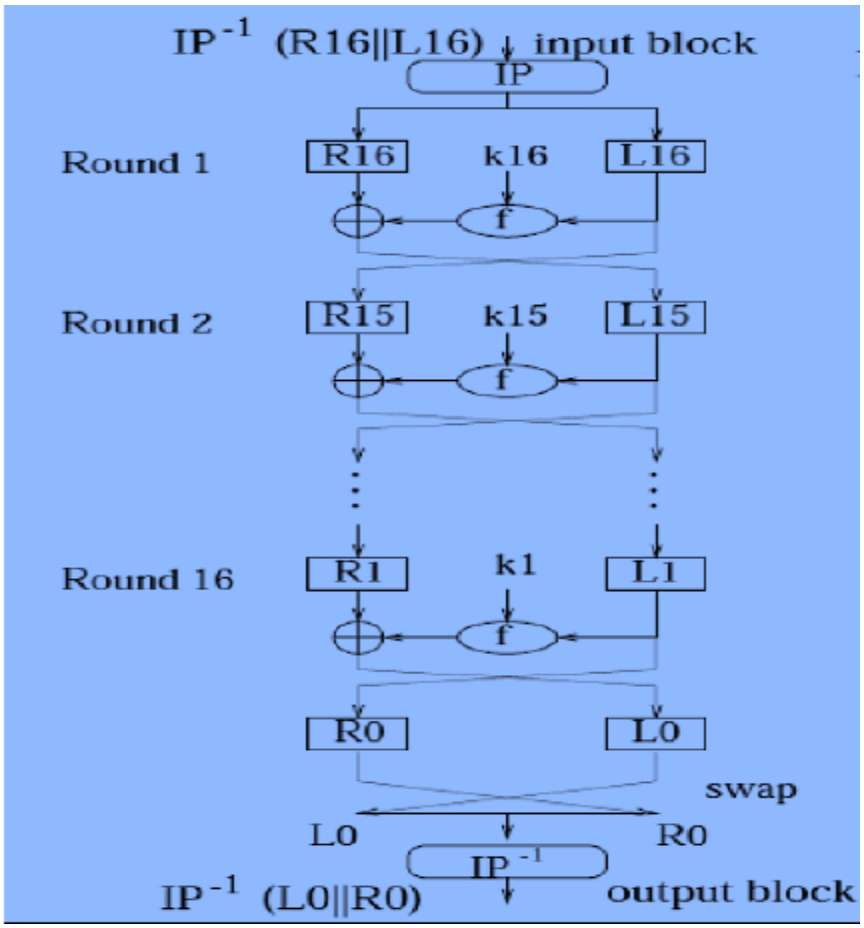


Figure (19): DES Decryption

Characteristics Of DES Algorithm

1) Most widely used block cipher in the world.
2) Encrypt plaintext with length 64-bits using key length 56-bit.
3) Brute force attack looks hard.
4) Generally the statistical attacks are :
    a. Differential cryptanalysis.
    b. Linear cryptanalysis.
    c. Related key attack.

Confusion and Diffusion

Confusion: Makes relationship between ciphertext and key as complex as possible (each character of the ciphertext should depend on several parts of the key).Example (substitution).

Diffusion: Spreading the effect of change in the plaintext to many parts of the ciphertext (if we change a character of the plaintext then several characters of the ciphertext change).Example (transposition).

5

Chapter Five

Public Key Cryptography (Asymmetric)

Public Key Cryptography(Asymmetric)

- public-key is an Asymmetric Cryptography involves the use of two keys:
    - **Public-key**, which may be known by anybody, and can be used to encrypt messages, and verify signatures.
    - **Private-key**, known only to the receiver, used to decrypt messages, and create signatures.

Public-Key Cryptography Characteristics

1) It is computationally infeasible to find decryption key knowing only algorithm & encryption key.
2) It is computationally easy to encrypt and decrypt messages when the public and private keys are known.
3) Either of the public and private keys can be used for encryption and other used for decryption.

Public-Key Applications

1) Encryption/decryption (provide secrecy).
2) Digital signatures (provide authentication).
3) Key exchange (Session keys).

Security of Public Key Schemes

- like private key schemes brute force exhaustive search attack is always theoretically possible.
- But keys used are too large (>512bits).

Comparative between conventional encryption(Symmetric) and public key encryption(Asymmetric)

Conventional encryption	public key encryption
The same algorithm with the same key is used for encryption and decryption.	The same algorithm with a pair of keys, one for encryption and one for decryption
The sender and receiver must share the algorithm and the key.	The sender and receiver must share the algorithm and one of the matched pair of keys.
The key must be kept secret	One of the two keys must be kept secret.
Knowledge of the algorithm and samples of ciphertext must be insufficient to determine the key.	Knowledge of the algorithm and one of the keys and samples of ciphertext must be insufficient to determine other key.
Example/ DES,AES	Example/ Diffie-Hellman/ RSA

Diffie-Hellman Algorithm

- First public-key type scheme proposed by Diffie & Hellman in 1976 along with the exposition of public key concepts.
- Based on the difficulty of computing discrete logarithms of large numbers.
- The purpose of the algorithm is to enable two users to securely exchange keys .

Steps of Diffie Hellman Algorithm

1) Alice and Bob agree **p** and **g**.
   P---------Prime number.
   g---------g< P , g is primitive root of P.
2) Alice chooses a secret number **a**, and calculation **A**, **A= g^a mod p** Sent to Bob (**a< P).**
3) Bob chooses a secret number **b**, and calculation **B, B= g^b mod p** Sent to Alice (**b< P).**
4) Alice computes **B^a mod p** .
5) Bob computes **A^b mod p** .

Example/ Alice and Bob agree on **p = 23** and **g = 5**?

1) Alice chooses **a= 6**, **A= g^a mod p ------ $A=5^6$ mod23=8**
2) Bob chooses **b = 15**, **B= g^b mod p ------ $B=5^{15}$ mod23=19**
3) Alice computes **B^a mod p -----19^6 mod 23 = 2.**
4) Bob computes **A^b mod p------8^{15} mod 23 = 2.**

Homework

Ex/ Alice and Bob agree on P=9967, g=3, Alice secretly chooses 34(a), and Bob secretly chooses 37(b)?

RSA Algorithm

- Proposed by Rivest, Shamir, and Adleman in 1977.
- Best known & widely used public-key scheme
- Based on exponentiation in a finite (Galois) field over integers modulo a prime.
- Security due to cost of factoring large numbers.

Steps of RSA Algorithm

1) Each user generates a public/private key pair by :
    - Selecting two large primes at random - p, q.
    - Computing their system modulus N=p.q.
    - ø(N) = (p-1) (q-1).
2) Selecting at random the encryption key (e):
    - $1 < e < ø(N)$, gcd (e,ø(N)) = 1 .
3) Find decryption key (d):
    - $e \cdot d = 1 \bmod ø(N)$ and $0 \leq d \leq N$.
4) Publish their public encryption key: KU = {e ,N }.
5) keep secret private decryption key: KR = { d, p, q }.
6) To encrypt a message M the sender:
    - Obtains public key of recipient KU={e,N}
    - Computes: $C=M^e \bmod N$, where $0 \leq M < N$
7) To decrypt the ciphertext C the owner:
    - Uses their private key KR={d,p,q}
    - Computes: $M=C^d \bmod N$

RSA Example

1) Select primes: p=17 & q=11.
2) Compute n = pq =17×11=187.
3) Compute ø(n)=(p–1)(q-1)=16×10=160.
4) Select e : gcd(e,160)=1; choose e=7.
5) Determine d: d.e=1 mod 160 and d < 160 Value is d=23 .
6) Publish public key KU={7,187}.
7) Keep secret private key KR={23,17,11}.
8) given message M = 88 (88<187)
9) encryption: $C=M^e \bmod N$:

$C = 88^7 \bmod 187 = 11$

10) Decryption: $M=C^d \bmod N$.

$M = 11^{23} \bmod 187 = 88$

Homework

Ex/ p=3,q=11,e=7,m=2 encrypt and decrypt using RSA Algorithm?

GOOD LUCK