MODULE I INTRODUCTION TO CRYPTOGRAPHY & NUMBER THEORY

Introduction to Cryptography: Security Services And Mechanism - Conventional Encryption: Conventional Encryption Model -Classical Encryption Techniques: Substitution Techniques, Transposition Techniques– Steganography.

Introduction to Number Theory: Modular Arithmetic-Euclidean Algorithm- Fermat's and Euler's Theorem

Definition

Cryptography is the science of using mathematics to encrypt and decrypt data.

-Phil Zimmermann

Cryptography is the art and science of keeping messages secure.

-Bruce Schneier

The art and science of concealing the messages to introduce secrecy in information Security is recognized as cryptography.

Important Terminologies

Plain text: An original message is known as the **plaintext**. **Cipher text:** The coded message is called the **cipher text**.

Encryption: The process of converting from plaintext to cipher text is known as enciphering orencryption.

Decryption: The process of converting from cipher text in to plain text is known as deciphering ordecryption.

Cryptography The many schemes used for encryption constitute the area of study known as cryptography. Such a scheme is known as a cryptographic system or a cipher.

Cryptanalysis: Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. Cryptanalysis is what the layperson calls "breaking the code."

Cryptology: The areas of cryptography and cryptanalysis together are called **cryptology**.

OSI SECURITY ARCHITECTURE

The OSI security architecture focuses on security attacks, mechanisms, and services. These can bedefined briefly as follows:

- **Security attack** – Any action that compromises the security of information owned by an organization
- **Security mechanism** – A mechanism that is designed to detect, prevent or recover from a securityattack
- **Security service** – A service that enhances the security of the data processing systems and theinformation transfers of an organization.

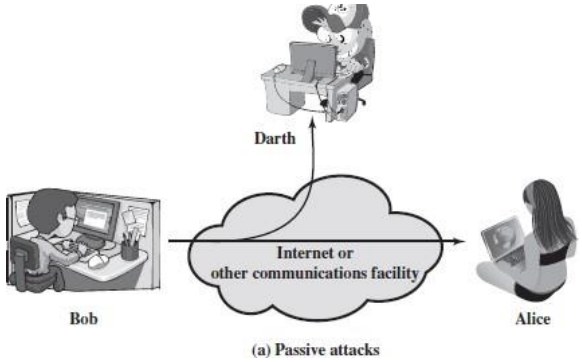
SECURITY ATTACK

There are two types of attacks

- Passive attacks
- Active attacks

Passive attack

Passive attacks attempt to learn or make use of information from the system but do not affect system resources. The goal of the opponent is to obtain information that is being transmitted.



(a) Passive attacks

Passive attacks are of two types

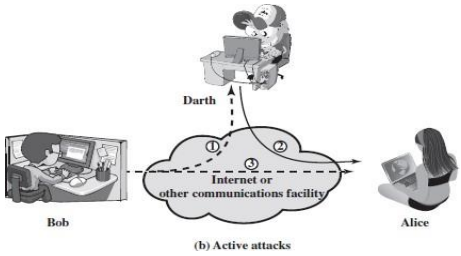
- **Release of message contents**
- **Traffic analysis**:

Release of message contents: The opponent would learn the contents of the transmission. A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents ofthese transmissions.

Traffic analysis: The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place. Passive attacks are very difficult to detect, because they do not involve any alteration of the data. However, it is feasible to prevent the success of these attacks.

Active attacks

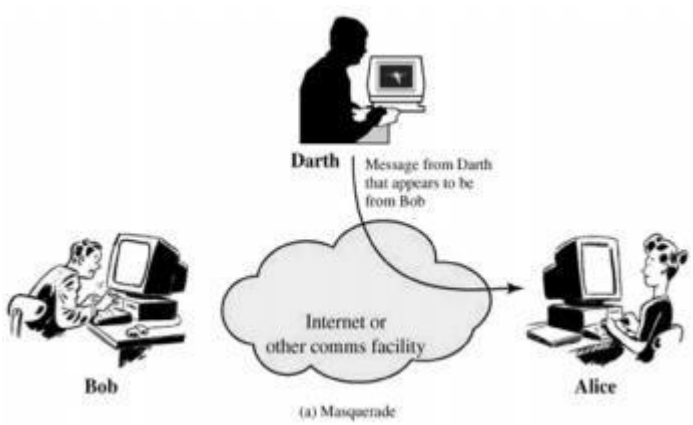
These attacks involve some modification of the data stream or the creation of a false stream.



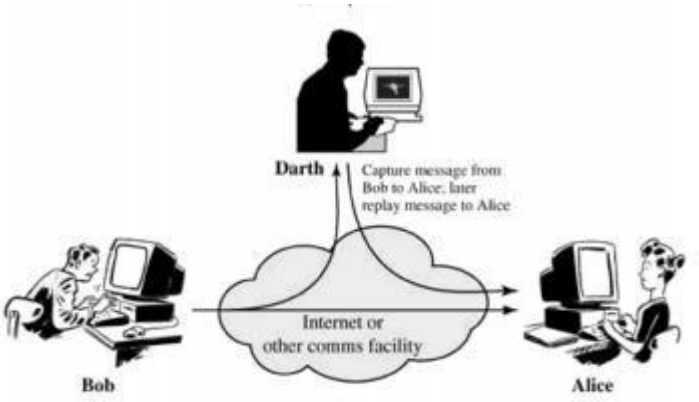
(b) Active attacks

Active attacks can be classified in to four categories:

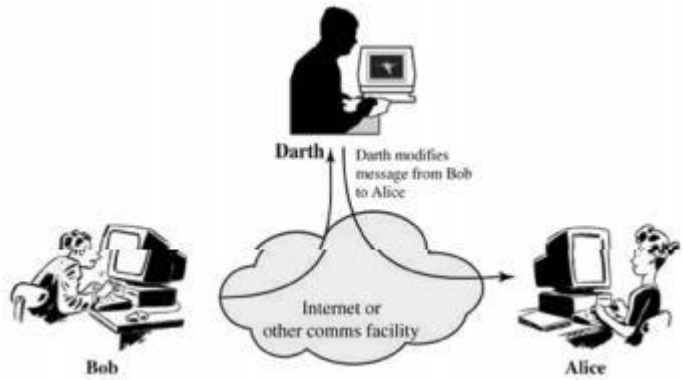
 Masquerade – One entity pretends to be a different entity. Here, the attacker capturers the authentication and impersonifies the sender.



Replay – The attacker captures the message and retransmits the message without modification toproduce unauthorized effect.



 Modification of messages – The attacker captures the message and retransmits the message with modification to produce unauthorized effect.



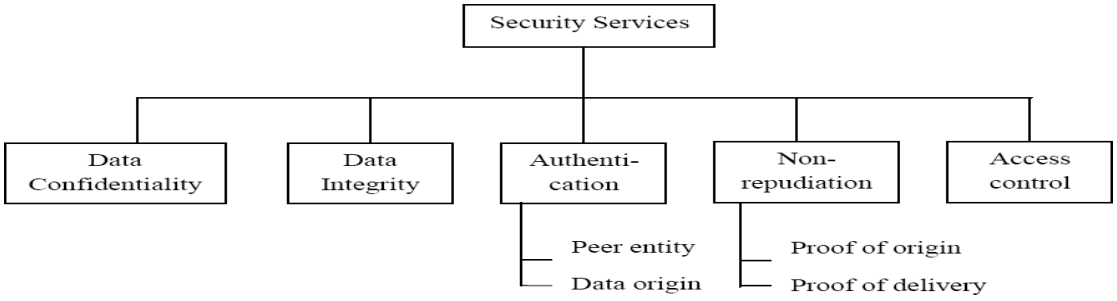
 Denial of service – The attacker may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

SECURITY SERVICES

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

The classification of security services are as follows:



(i) Authentication: The authentication service is concerned with assuring that a communication isauthentic.

Two specific authentication services are defined in X.800:

- **Peer entity authentication:** Provide confidence in the identity of entities connected.
- **Data origin authentication:** Provide assurance that the source of received data is as claimed.

(ii) Access control: Access control is the ability to limit and control the access to host systems andapplications.

(iii) Data Confidentiality: Confidentiality is the protection of transmitted data from passive attacks.

- **Connection Confidentiality**
  The protection of all user data on a connection
- **Connectionless Confidentiality**
  The protection of all user data in a single data block
- **Selective-Field Confidentiality**
  The confidentiality of selected fields within the user data on a connection or in a single datablock
- **Traffic-Flow Confidentiality**
  The protection of the information that might be derived from observation of traffic flows.

(iv)Data Integrity: The assurance that data received are exactly as sent by an authorized entity.

- **Connection Integrity with Recovery**
  Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recoveryattempted.

- **Connection Integrity without Recovery**

  As above, but provides only detection without recovery.
- **Selective-Field Connection Integrity**

  Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields havebeen modified, inserted, deleted, or replayed.
- **Connectionless Integrity**

  Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may beprovided.
- **Selective-Field Connectionless Integrity**

  Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

(v)Non repudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

- **Nonrepudiation, Origin**

  Proof that the message was sent by the specified party
- **Nonrepudiation, Destination**

  Proof that the message was received by the specified party.

SECURITY MECHANISMS

- **Encipherment:**

  It uses mathematical algorithm to transform data into a form that is not readily intelligible. It depends upon encryption algorithm and key
- **Digital signature:**

  Data appended to or a cryptographic transformation of a data unit that is to prove integrity of data unit and prevents from forgery
- **Access control**

  A variety of mechanisms that enforce access rights to resources.
- **Data integrity**

  A variety of mechanism are used to ensure integrity of data unit
- **Traffic padding**

  The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- **Notarization**

  The use of a trusted third party to assure certain properties of a data exchange.
- **Routing Control**

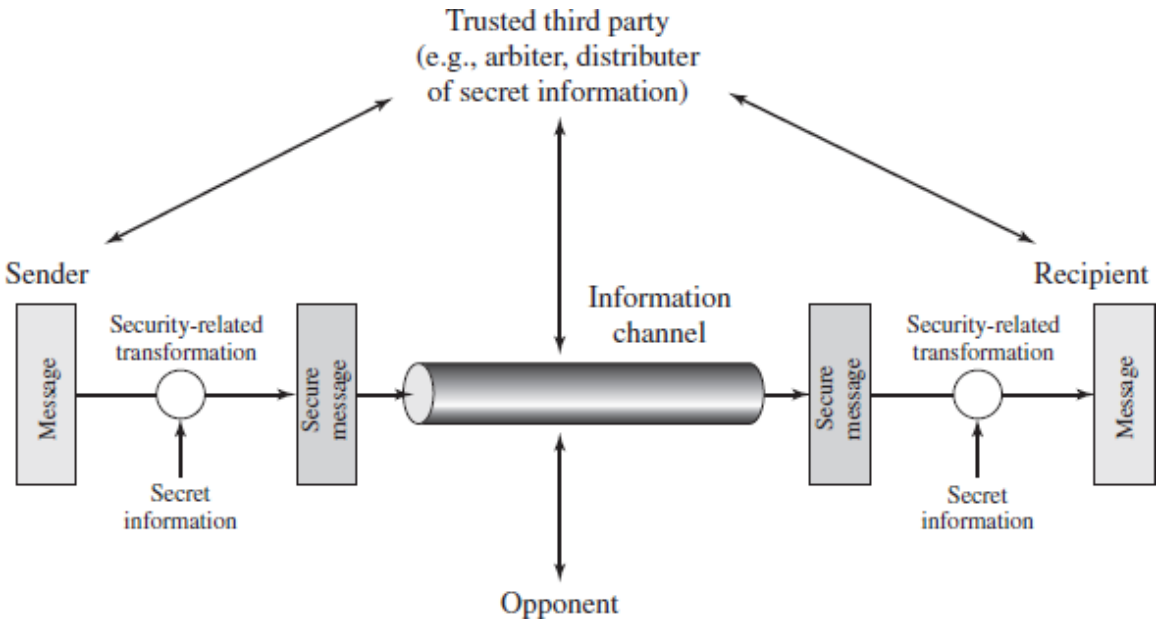
  Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

A MODEL FOR NETWORK SECURITY

Encryption/Decryption methods fall into two categories.

- Symmetric key
- Public key

- In **symmetric key algorithms,** the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it. In many cases, the encryption and decryption keys are the same.
- In **public key cryptography**, encryption key is made public, but it is computationally infeasible to find the decryption key without the information known to the receiver.



A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

All the techniques for providing security have two components:

- A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent.
- Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission

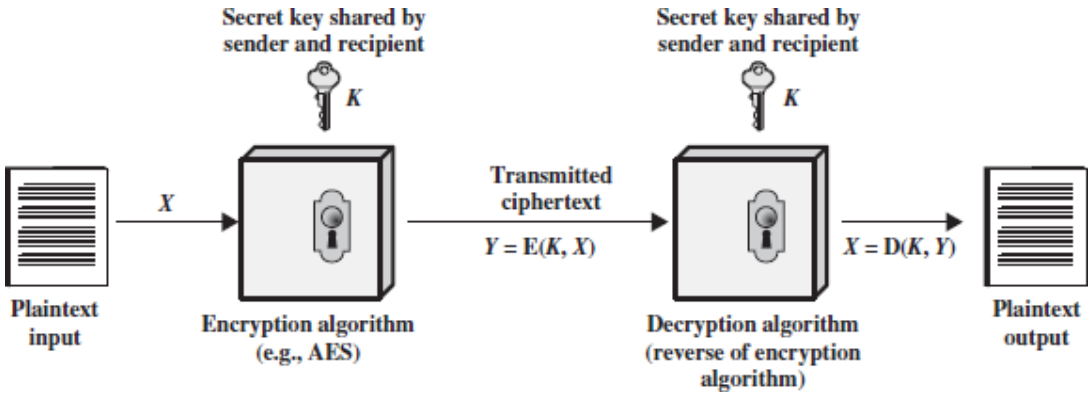
A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should besuch that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and thesecret information to achieve a particular security service.

SYMMETRIC CIPHER MODEL

Symmetric encryption also referred to as conventional encryption or single-key encryption. Here, thesender and recipient share a common key.



A symmetric encryption scheme has five components

- **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformationson the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

• **Cipher text:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

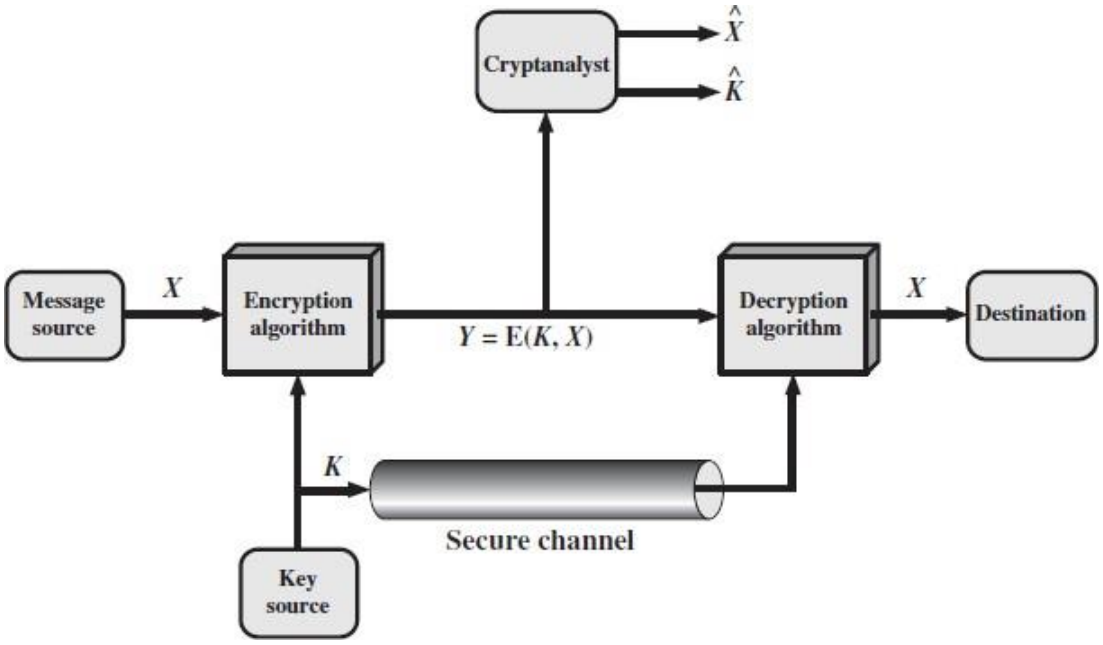
• **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

There are two requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion andmust keep the key secure.

It is impractical to decrypt a message on the basis of the cipher text *plus* knowledge of the encryption/decryption algorithm. In other words, we do not need to keep the algorithm secret; we need to keep only the key secret.



Model of symmetric cryptosystem

A source produces a message in plaintext

$X = [X1, X2,..., XM]$.

M- elements of X are letters.

For encryption, a key of the form

$K = [K1, K2, \ldots, KJ]$ is generated.

If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel. Alternatively, a third party could generate the key and securely deliverit to both source and destination.

With the message X and the encryption key K as input, the encryption algorithm forms the cipher text

$Y = [Y1, Y2,\ldots,$

Y_N]. $Y = E(K, X)$

Y- cipher text

E-Encryptionalgorithm

K- Key

X-Plain text

At the receiver side the transformation:

$X = D(K, Y)$

Y- cipher text

D-Decryption

algorithmK- Key

X-Plain text

If the opponent is interested in only this particular message only, tries to find the message estimate. But when the opponent is interested in the current and future messages, tries to find key estimate.

Cryptographic systems are generally classified along 3 independent dimensions:

- **Type of operations used for transforming plain text to cipher text**

All the encryption algorithms are based on two general principles:

- **Substitution**, in which each element in the plaintext is mapped into another element
- T**ransposition**, in which elements in the plaintext are rearranged.

- **The number of keys used**
  - If the sender and receiver uses same key then it is said to be **symmetric key (or) single key (or) conventional encryption**.
  - If the sender and receiver use different keys then it is said to be **public key encryption**.
- **The way in which the plain text is processed**
  - A **block cipher** processes the input and block of elements at a time, producing output block for each input block.
  - A **stream cipher** processes the input elements continuously, producing output element one at a time, as it goes along.

CRYPTANALYSIS AND BRUTE-FORCE ATTACK

There are two general approaches to attacking a conventional encryption scheme:

• **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm and some knowledge of thegeneral characteristics of the plaintext or even some sample plaintext–cipher text pairs.

• **Brute-force attack:** The attacker tries every possible key on a piece of cipher text until anintelligible translation into plaintext is obtained.

There are various types of cryptanalytic attacks based on the amount of information known

to thecryptanalyst.

Type of Attack	Known to Cryptanalyst
Cipher text Only	• Encryption algorithm • Cipher text
Known Plaintext	• Encryption algorithm • Cipher text • One or more plaintext–cipher text pairs formed with the secret key
Chosen Plaintex t	• Encryption algorithm • Cipher text • Plaintext message chosen by cryptanalyst, together with its correspondingCipher text generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Cipher text • Cipher text chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Cipher text • Plaintext message chosen by cryptanalyst, together with its correspondingCipher text generated with the secret key • Cipher text chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Encryption algorithms are to be

- **Unconditionally secure**
- **Computationally secure**

An encryption scheme is **unconditionally secure** if the cipher text generated by the scheme doesnot contain enough information to determine uniquely the corresponding plaintext.

An encryption scheme is said to be **computationally secure**

- If the cost of breaking the cipher exceeds the value of the encrypted information
- If the time required to break the cipher exceeds the useful lifetime of the information.

SUBSTITUTION TECHNIQUES

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- Substitution ciphers can be categorized as either

i) Monoalphabetic ciphers or ii) polyalphabetic ciphers.

- **In monoalphabetic substitution**, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.
- **In polyalphabetic substitution**, each occurrence of a character may have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is one-to-many.

Various substitution ciphers are

(i) Caesar Cipher

(ii) Mono alphabetic cipher

(iii) Playfair cipher

(iv) Hill cipher

(v) Poly alphabetic cipher

(vi) Vignere cipher

(vii) Vernam Cipher

(viii) One Time Pad

(i) CAESAR CIPHER (OR) SHIFT CIPHER

Caeser cipher was proposed by Julius Caesar. The Caesar cipher involves replacing each letter of thealphabet with the letter standing 3 places further down the alphabet.

```
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
```

```
plain:  meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB
```

Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Note that the alphabet is wrapped around, so that letter following 'z' is 'a'.

For each plaintext letter p, substitute the cipher text letter c such that

c = E(3, p) = (p+3) mod 26

Decryption is

p=D(3,c)=(c-3) mod 26

The general Caesar algorithm is

C = E(k, p) = (p + k) mod 26

where *k* takes on a value in the range 1 to 25.

The decryption algorithm is simply

p = D(k, c) = (C - k) mod 26

If it is known that a given cipher text is a Caesar cipher, then a brute-force cryptanalysis is easilyperformed: simply try all the 25 possible keys.

Cryptanalysis of Caesar Cipher

1. The encryption and decryption algorithms are known
2. There are only 25 possible keys. Hence brute force attack takes place
3. The language of the plaintext is known and easily recognizable

(ii) MONOALPHABETIC CIPHER

- Each plaintext letter maps to a different random cipher text letter
- Here, 26! Possible keys are used to eliminate brute force attack

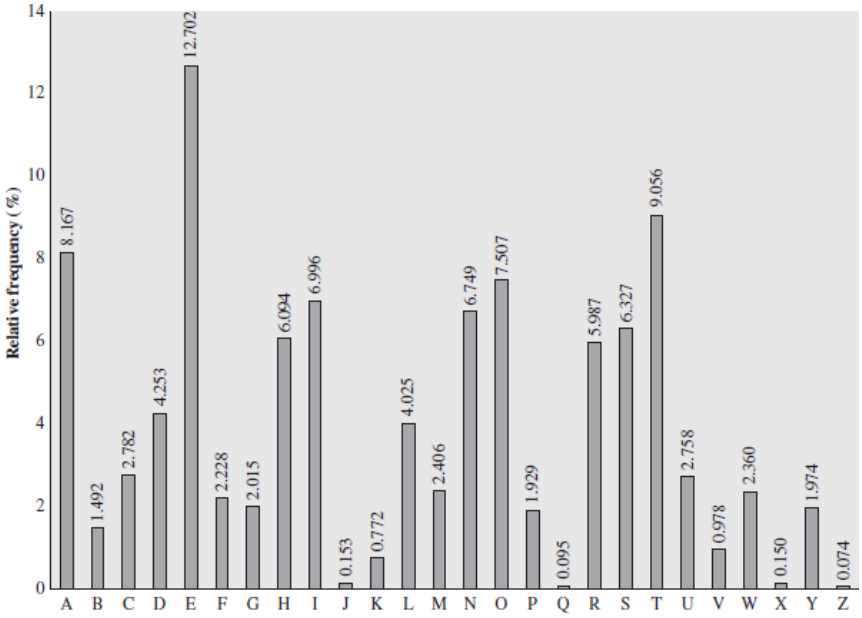
There is, however, another line of attack. If the cryptanalyst knows the nature of the plaintext (e.g., non-compressed English text), then the analyst can exploit the regularities of the language.

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

As a first step, the relative frequency of the letters can be determined and compared to a standard frequency distribution for English Only four letters have been identified, but already we have quite a bit of the message. Continued analysis of frequencies plus trial and error should easily yield a solution from this point. The complete plaintext, with spaces added between words, follows:

it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

Relative frequency of letters in English Text



P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
t a e e te a that e e a a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
e t ta t ha e ee a e th t a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
e e e tat e the t

(iii) PLAYFAIR CIPHER

The best known multiple letter encryption cipher is the playfair, which treats digrams in the plaintext as single units and translates these units into cipher text digrams. The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword.

Let the keyword be "monarchy". The matrix is constructed by

- Filling in the letters of the keyword from left to right and from top to bottom
- Duplicates are removed
- Remaining unfilled cells of the matrix is filled with remaining alphabets in alphabetical order.

The matrix is 5x5. It can accommodate 25 alphabets. To accommodate the 26th alphabet I and J are counted as one character.

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

Rules for encryption

- Repeating plaintext letters that would fall in the same pair are separated with a filler lettersuch as 'x'.
- 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. For example, ar is encrypted as RM.
- 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. For example, mu is encrypted as CM.
- 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. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

Example

Plain text: Balloon

Ba ll oo n

Ba lx lo on

Ba□I/JB

lx□SU

lo□PM

on□NA

Strength of playfair cipher

_ Playfair cipher is a great advance over simple mono alphabetic ciphers.

¯ Since there are 26 letters, 26x26 = 676 diagrams are possible, so identification of individual digramis more difficult.

□ Frequency analysis is much more difficult.

Disadvantage

Easy to break because it has the structure and the resemblance of the plain text language.

(iv)<u>HILL CIPHER</u>

It is a multi-letter cipher. It is developed by Lester Hill. The encryption algorithm takes m successive plaintext letters and substitutes for them m cipher text letters. The substitution is

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} K_{11}K_{12}K_{13} \\ K_{21}K_{22}K_{23} \\ K_{31}K_{32}K_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \bmod 26$$

determined by m linear equations in which each character is assigned numerical value (a=0,b=1…z=25). For m =3 the system can be described as follows:

C=KP mod 26

Decryption

Decryption algorithm is done as **$P=K^{-1}C \bmod 26$**

1) mathematically give each letter a number

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

2) 1st pair from plain text "me" => $\begin{pmatrix} 12 \\ 4 \end{pmatrix}$

I

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}\begin{pmatrix} 12 \\ 4 \end{pmatrix} => \begin{pmatrix} 9x12+4x4 \\ 5x12+7x4 \end{pmatrix} = \begin{pmatrix} 124 \\ 88 \end{pmatrix} => mod\ 26 => \begin{pmatrix} 20 \\ 10 \end{pmatrix} => \begin{pmatrix} u \\ k \end{pmatrix}$$

$$3)\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}\begin{pmatrix} 4 \\ 19 \end{pmatrix} => \begin{pmatrix} 9x4+4x19 \\ 5x4+7x19 \end{pmatrix} = \begin{pmatrix} 112 \\ 153 \end{pmatrix} => mod\ 26 => \begin{pmatrix} 8 \\ 23 \end{pmatrix} => \begin{pmatrix} i \\ x \end{pmatrix}$$

4) Cipher text for "meet" is "ukix"

5) To get plain text from cipher text, we need to find the inverse of K

6) |A| = (9x7 – 5x4) => 43

7) Adj (A) => $\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix}$ => $\frac{1}{43}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix}$ => $\frac{1}{17}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix}$ ($\because 43 \,\%\, 26 = 17$)

8) Find the multiplier for 17, using 17 x X = 1 mod 26 => X = 23

9) $\begin{pmatrix} 161 & -92 \\ -115 & 207 \end{pmatrix} => mod\ 26 => \begin{pmatrix} 5 & -14 \\ -11 & 25 \end{pmatrix} => \begin{pmatrix} \mathbf{5} & \mathbf{12} \\ \mathbf{15} & \mathbf{25} \end{pmatrix}$ ($\because Add\ 26\ for - ive\ values$)

10) P = CK^{-1} = > For the ciper text of "uk",

$$\begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}\begin{pmatrix} 20 \\ 10 \end{pmatrix} = \begin{pmatrix} 5x20 + 12x10 \\ 15x20 + 25x10 \end{pmatrix} => \begin{pmatrix} 220 \\ 550 \end{pmatrix} mod\ 26 => \begin{pmatrix} 12 \\ 4 \end{pmatrix} = \begin{pmatrix} m \\ e \end{pmatrix}$$

Hence the plain text is "me"

Example 2

Plain Text= 'PAY'

Key=

RRFVSVCCT

Encryption

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$$\begin{bmatrix} C1 \\ C2 \\ C3 \end{bmatrix} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}\begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} mod\ 26 = \begin{bmatrix} 375 \\ 819 \\ 486 \end{bmatrix} mod\ 26 = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} = \begin{bmatrix} l \\ n \\ s \end{bmatrix}$$

Decryption

$P=K^{-1}C \bmod 26$

$$K^{-1} = \frac{1}{Det(K)} adj(K)$$

$$\begin{bmatrix} P1 \\ P2 \\ P3 \end{bmatrix} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}^{-1}\begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} mod\ 26$$

Det(K)=17(342-42)-17(399-42)+5(42-36)= -939

$$K^T = \begin{bmatrix} 17 & 21 & 2 \\ 17 & 18 & 2 \\ 5 & 21 & 19 \end{bmatrix}$$

$$\text{adj(K)} = \begin{bmatrix} (19*18-2*21) & -(19*17-5*2) & (21*17-5*18) \\ -(19*21-2*21) & (19*17-5*2) & -(21*17-5*21) \\ (2*21-18*2) & -(2*17-2*17) & (18*17-17*21) \end{bmatrix}$$

$$= \begin{bmatrix} 300 & -313 & 276 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix}$$

$$P = \frac{1}{-939} \begin{bmatrix} 300 & -313 & 276 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix} \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} mod\ 26$$

$$= \frac{1}{939} \begin{bmatrix} -300 & 313 & -276 \\ 357 & -313 & 252 \\ -6 & 0 & 51 \end{bmatrix} \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} mod\ 26$$

$$= 939^{-1} \begin{bmatrix} -4037 \\ 4394 \\ 852 \end{bmatrix} mod\ 26$$

$939y \equiv 1 mod 26$

(939*1)%26=3(939*2)%26=6

…….. (939*9)%26=1

Therefore, y=9

Covert the negative number in to positive number

$939^{-1} mod\ 26 = 9$

$$P = 9 \begin{bmatrix} -4037 \\ 4394 \\ 852 \end{bmatrix} mod\ 26$$

$$P = \begin{bmatrix} -36333 \\ 39546 \\ 7668 \end{bmatrix} mod\ 26 = \begin{bmatrix} -11 \\ 0 \\ 24 \end{bmatrix} = \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} = \begin{bmatrix} p \\ a \\ y \end{bmatrix}$$

Example 3

Plain Text= 'ACT'

Key=

GYBNQKURP

Encryption

$$K = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

$$\begin{bmatrix} C1 \\ C2 \\ C3 \end{bmatrix} = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} mod\ 26 = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} mod\ 26 = \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} = \begin{bmatrix} p \\ o \\ h \end{bmatrix}$$

Decryption

$P=K^{-1}C \bmod 26$

$$K^{-1} = \frac{1}{Det(K)} adj(K)$$

$$\begin{bmatrix} P1 \\ P2 \\ P3 \end{bmatrix} = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} mod\ 26$$

Det(K)=6(16*15-17*10)-24(15*13-20*10)+1(17*13-20*16)= 441

$$K^T = \begin{bmatrix} 6 & 13 & 20 \\ 24 & 16 & 17 \\ 1 & 10 & 15 \end{bmatrix}$$

$$\text{adj(K)} = \begin{bmatrix} (16*15-17*10) & -(15*24-17*1) & (24*10-16*1) \\ -(15*13-20*10) & (15*6-20*1) & -(6*10-13*1) \\ (17*13-20*16) & -(17*6-24*20) & (6*16-13*24) \end{bmatrix}$$

$$= \begin{bmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{bmatrix}$$

$$P = \frac{1}{441} \begin{bmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} mod\ 26$$

$$= 441^{-1} \begin{bmatrix} 2184 \\ 726 \\ 2295 \end{bmatrix} mod\ 26$$

$441y \equiv 1 mod 26$

(441*1)%26=25

(441*2)%26=24

……..

(441*25)%26=1

Therefore, y=25

$$441^{-1} mod\ 26 = 25$$

$$P = 25 \begin{bmatrix} -2184 \\ 726 \\ 2295 \end{bmatrix} mod\ 26$$

$$P = \begin{bmatrix} -54600 \\ 18150 \\ 57375 \end{bmatrix} mod\ 26 = \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \begin{bmatrix} a \\ c \\ t \end{bmatrix}$$

Merits and Demerits

- Completely hides single letter and 2 letter frequency information.
- Easily attacked with known plain text attack

(iv) POLYALPHABETIC CIPHERS

Poly alphabetic cipher is a simple technique to improve mono-alphabetic technique.The features are

- A set of related mono-alphabetic substitution rules are used
- A key determines which particular rule is chosen for a given transformation.

(vi) Vigenere Cipher

Encryption and Decryption

Given a key letter X and plaintext letter Y, the ciphertext letter is at the intersection of the row labeled X and the column labled Y.

To encrypt a message, a key is needed that is as long as the message. Usually the key is repeating keyword. Decryption is simple. The key letter again identifies the row. The position of the ciphertext letter in that row determines the column, and the plaintext letter is the top of the column.

Example:

Key : deceptive

Plain Text : we are discovered yourself

key:deceptivedeceptivedeceptive

plaintext:wearediscoveredsaveyourself

ciphertext:

ZICVTWQNGRZGVTWAVZHCQYGLMGJ

	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
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

Strength of Vigenere cipher

o There are multiple ciphertext letters for each plaintext letter.

o Letter frequency information is obscured

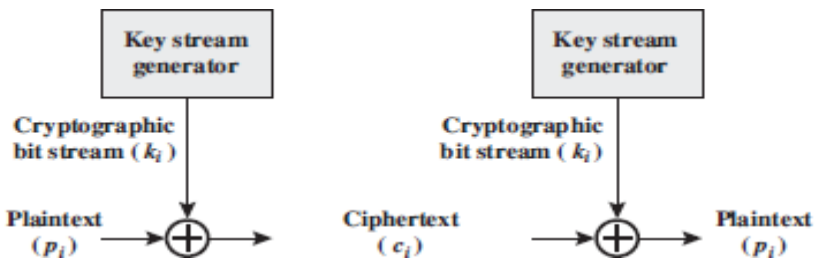
(vii)VERNAM CIPHER

The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plaintext and has no statistical relationship to it. Such a system was introduced by an AT&T engineer named Gilbert Vernam in 1918.

$$c_i = p_i \oplus k_i$$

where

p_i = ith binary digit of plaintext
k_i = ith binary digit of key
c_i = ith binary digit of ciphertext
$\oplus$ = exclusive-or (XOR) operation



(viii) ONE-TIME PAD CIPHER

- improvement to the Vernam cipher that yields the ultimate in security
- using a random key that is as long as the message, so that the key need not be repeated
- the key is to be used to encrypt and decrypt a single message, and then is discarded.
- Each new message requires a new key of the same length as the new message
- **Example**

ciphertext:ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

key:pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih

plaintext: mr mustard with thecandlestick in the hall

ciphertext:ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

key:mfugpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt

plaintext: miss scarletwith the knife in the library

Example:

Plain text: R O C K

Keyword: B O T S

Cipher Text= (Plain text+Keyword)mod 26

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

R(17)	O(14)	C(2)	K(10)
B(1)	O(14)	T(19)	S(18)
18(S)	28(C)	21(V)	28(C)

Cipher Text= SCVC

Advantages

- It is unbreakable since cipher text bears no statistical relationship to the plaintext
- Not easy to break

Drawbacks

- Practically impossible to generate a random key as to the length of the message
- The second problem is that of key distribution and key protection.

TRANSPOSITION TECHNIQUES

A very different kind of mapping is achieved by performing some sort of permutation on theplaintext letters. This technique is referred to as a transposition cipher.

1.RAIL FENCE CIPHER

It is simplest of such cipher, in which the plaintext is written down as a sequence of diagonalsand then read off as a sequence of rows.

Example1 :

to encipher the message "meet me after the toga party" with a rail fence of depth 2,

we write the following

m e m a t r h t g p r y e t e f e t e o a a t

The encrypted message is

MEMATRHTGPRYETEFETEOAAT

Example 2:

Plaintext = meet at the school house

To encipher this message with a rail fence of depth 2,We write the message as follows:

m e a t e c o l o s

e t t h s h o h u e

The encrypted message Cipher text MEATECOLOSETTHSHOHUE

2. ROW TRANSPOSITION CIPHERS/ PURE TRANSPOSITION CIPHER

A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the keyof the algorithm.

Example 1

Plaintext: attack postponed until two am

Key: 4 3 1 2 5 6 7

Plaintext: a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Example 2

plaintext = meet at the school house

Key = 4 3 1 2 5 6 7

PT = m e e t a t t

h e s c h o

ol h o u s e

CT = ESOTCUEEHMHLAHSTOETO

Demerits

- Easily recognized because the frequency is same in both plain text and cipher text.
- Can be made secure by performing more number of transpositions.

3.Double Transposition

performing more than one stage of transposition Example

- if the foregoing message is reencrypted using the same algorithm

Key: 4 3 1 2 5 6 7

Input: t t n a a p t

m t s u o a o

d w c o i x k

n l y p e t z

Output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

This is a much less structured permutation and is much more difficult to cryptanalyze

STEGANOGRAPHY

Steganography

We conclude with a discussion of a technique that is, strictly speaking, not encryption, namely,steganography

A plaintext message may be hidden in one of two ways.

- The methods of steganography conceal the existence of the message
- The methods of cryptography render the message unintelligible to outsiders by various transformations of the text

Various ways to conceal the message

Arrangement of words or letters within an apparently innocuous text spells out the real message

Character marking

Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarilynot visible unless the paper is held at an angle to bright light.

Invisible ink

A number of substances can be used for writing but leave no visible trace until heat or somechemical is applied

Pin punctures

Small pin punctures on selected letters are ordinarily not visible unless the paper is held up infront of a light.

Typewriter correction ribbon

Used between lines typed with a black ribbon, the results of typing with the correction tape arevisible only under a strong light

Hiding a message by using the least significant bits of frames on a CD

- The Kodak Photo CD format's maximum resolution is 2048 by 3072 pixels, with eachpixel containing 24 bits of RGB color information.
- The least significant bit of each 24-bit pixel can be changed without greatly affecting thequality of the image
- Thus you can hide a 2.3-megabyte message in a single digital snapshot

Advantage of steganography

- can be employed by parties who have something to lose should the fact of their secretcommunication be discovered
- Encryption flags traffic as important or secret or may identify the sender or receiver assomeone with something to hide

Drawbacks

- lot of overhead to hide a relatively few bits of information
- once the system is discovered, it becomes virtually worthless
- the insertion method depends on some sort of key

o Alternatively, a message can be first encrypted and then hidden using steganography

Modular Arithmetic

Given any positive integer *n* and any nonnegative integer *a*, if we divide *a* by *n*, we get an integerquotient *q* and an integer remainder *r* that obey the following relationship:

$$a = qn + r \qquad 0 \leq r < n; q = \lfloor a/n \rfloor$$

where $\lfloor x \rfloor$ is the largest integer less than or equal to *x*.

If *a* is an integer and *n* is a positive integer, we define *a* mod *n* to be the remainder when *a* is divided by *n*. The integer *n* is called the **modulus**. Thus, for any integer *a*, we can always write:

$$a = \lfloor a/n \rfloor \times n + (a \bmod n)$$

11 mod 7 = 4;	-11 mod 7 = 3

a = 11;	*n* = 7;	11 = 1 x 7 + 4;	*r* = 4	*q* = 1
a = -11;	*n* = 7;	-11 = (-2) x 7 + 3;	*r* = 3	*q* = -2

Two integers *a* and *b* are said to be **congruent modulo *n***, if (*a* mod *n*) = (*b* mod *n*).

This is written as $a \equiv b \pmod{n}$

$73 \equiv 4 \pmod{23}$;	$21 \equiv -9 \pmod{10}$

Properties of Congruences

Congruences have the following properties:

1. $a \equiv b \pmod{n}$ *if* $n \mid (a\ b)$.
2. $a \equiv b \pmod{n}$ *implies* $b \equiv a \pmod{n}$..
3. $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$ *imply* $a \equiv c \pmod{n}$.

To demonstrate the first point, if $n \mid (a\ b)$, then $(a\ b) = kn$ for some *k*. So we can write $a = b + kn$.
Therefore, (*a* mod *n*) = (reminder when $b + kn$ is divided by *n*) = (reminder when *b* is divided by *n*) =(*b* mod *n*)

$23 \equiv 8 \pmod{5}$	because	23 8 = 15 = 5 3
$11 \equiv 5 \pmod{8}$	because	11 5 = 16 = 8 x (2)
$81 \equiv 0 \pmod{27}$	because	81 0 = 81 = 27 x 3

Modular Arithmetic Operations

Modular arithmetic exhibits the following properties:

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$

2. $[(a \bmod n) (b \bmod n)] \bmod n = (a b) \bmod n$

3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

We demonstrate the first property. Define $(a \bmod n) = r_a$ and $(b \bmod n) = r_b$.
Then we can write $a = r_a + jn$ for some integer j and $b = r_b + kn$ for some integer k.
Then $(a + b) \bmod n = (r_a + jn + r_b + kn) \bmod n$
$= (r_a + r_b (k + j)n) \bmod n$
$= (r_a + r_b) \bmod n$
$= [(a \bmod n] + (b \bmod n)] \bmod n$

Here are examples of the three properties:

11 mod 8 = 3; 15 mod 8 = 7
[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 =2 (11 + 15) mod 8 = 26 mod 8 = 2
[(11 *mod* 8)- (15 *mod* 8)] *mod* 8 =- 4 *mod* 8 = 4 (11- 15) *mod* 8 =- 4 *mod* 8 = 4
[(11 mod 8) x (15 mod 8)] mod 8 = 21 mod 8 = 5 (11 x 15) mod 8 = 165 mod 8 = 5

Exponentiation is performed by repeated multiplication, as in ordinary arithmetic.

To find 11^7 mod 13, we can proceed as follows:
$11^2 = 121 \equiv 4 \pmod{13}$
$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$
$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$

Properties of Modular Arithmetic

Define the set Z_n as the set of nonnegative integers less than n:
$Z_n = \{0, 1,...,(n\ 1)\}$
This is referred to as the **set of residues**, or **residue classes** modulo n. To be more precise, each integer in Z_n represents a residue class. We can label the residue classes modulo n as [0], [1], [2],...,[n -1], where $[r] = \{a: a \text{ is an integer}, a \equiv r \pmod{n}\}$

The residue classes modulo 4 are	
	[0] = { ..., 16, 12, 8, 4, 0, 4, 8, 12, 16,... }
	[1] = { ..., 15, 11, 7, 3, 1, 5, 9, 13, 17,... }
	[2] = { ..., 14, 10, 6, 2, 2, 6, 10, 14, 18,... }
	[3] = { ..., 13, 9, 5, 1, 3, 7, 11, 15, 19,... }

Of all the integers in a residue class, the smallest nonnegative integer is the one usually used to represent the residue class. Finding the smallest nonnegative integer to which *k* is congruent modulo *n*is called **reducing *k* modulo *n***.

Properties of Modular Arithmetic for Integers in Z_n

Property	Expression
Commutative laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive laws	$[w + (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$ $[w + (x \times y)] \bmod n = [(w + x) \times (w + y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 + w) \bmod n = w \bmod n$
Additive inverse ($-w$)	For each w Z_n, there exists a z such that $w + z$ 0 mod n

Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses modulo 8

The Euclidean Algorithm

One of the basic techniques of number theory is the Euclidean algorithm, which is a simple procedure for determining the greatest common divisor of two positive integers.

Greatest Common Divisor

Recall that nonzero b is defined to be a divisor of a if $a = mb$ for some m, where a, b, and m are integers. We will use the notation gcd(a, b) to mean the **greatest common divisor** of a and b.

Thepositive integer c is said to be the greatest common divisor of a and b if

1. c *is a divisor of* a *and of* b;

2. *any divisor of* a *and* b *is a divisor of* c.

An equivalent definition is the following:

gcd(a, b) = max[k, such that $k|a$ and $k|b$]

In general, gcd(a, b) = gcd(|a|, |b|).

gcd(60, 24) = gcd(60, 24) = 12

Also, because all nonzero integers divide 0, we have gcd(a, 0) = |a|.

We stated that two integers a and b are relatively prime if their only common positive integer factor is 1. This is equivalent to saying that a and b are relatively prime if gcd(a, b) = 1.

8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15, so 1 is the only integer on both lists.

Finding the Greatest Common Divisor

The Euclidean algorithm is based on the following theorem: For any nonnegative integer a and anypositive integer b,

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

gcd(55, 22) = gcd(22, 55 mod 22) = gcd(22, 11) = 11

let d = gcd(a, b). Then, by the definition of gcd, $d|a$ and $d|b$. For anypositive integer b, a can be expressed in the form

$$a = kb + r \equiv r \pmod{b} \quad a \bmod b = r$$

can be used repetitively to determine the greatest common divisor.

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

gcd(18, 12) = gcd(12, 6) = gcd(6, 0) = 6

gcd(11, 10) = gcd(10, 1) = gcd(1, 0) = 1

The Euclidean algorithm determine the greatest common divisor, as follows.

The algorithm assumes $a > b > 0$. It is acceptable to restrict the algorithm to positive integers because gcd(a, b) = gcd(|a|, |b|).

EUCLID(a, b)

1. A ⟵ a; B ⟵ b
2. **if** B = 0 **return** A = gcd(a, b)
3. R = A mod B
4. A ⟵ B
5. B ⟵ R
6. *goto* **2**

The algorithm has the following progression:

Steps

$$
\begin{aligned}
a &= q_1 b + r_1 && 0 < r_1 < b \\
b &= q_2 r_1 + r_2 && 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 && 0 < r_3 < r_2 \\
&\vdots && \vdots \\
r_{n-2} &= q_n r_{n-1} + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0 \\
d &= \gcd(a, b) = r_n
\end{aligned}
$$

To find gcd(1970, 1066)		
1970	= 1 x 1066 + 904	gcd(1066, 904)
1066	= 1 x 904 + 162	gcd(904, 162)
904	= 5 x 162 + 94	gcd(162, 94)
162	= 1 x 94 + 68	gcd(94, 68)
94	= 1 x 68 + 26	gcd(68, 26)
68	= 2 x 26 + 16	gcd(26, 16)
26	= 1 x 16 + 10	gcd(16, 10)
16	= 1 x 10 + 6	gcd(10, 6)
10	= 1 x 6 + 4	gcd(6, 4)
6	= 1 x 4 + 2	gcd(4, 2)
4	= 2 x 2 + 0	gcd(2, 0)
Therefore, gcd(1970, 1066) = 2		

Euclidean Algorithm Revisited

- For any nonnegative integer a and any positive integer b,
- gcd(a, b) = gcd (b, a mod b)
  - Example: gcd(55, 22) = gcd(22, 55 mod 22) = gcd(22, 11) = 11

Recursive function.

```
Euclid(a,b)
      if (b=0) then return a;
      else return Euclid(b, a mod b);
```

The Extended Euclidean Algorithm

calculate the greatest common divisor but also two additional integers and that satisfy the following equation

$$ax + by = d = \gcd(a, b)$$

x and y will have opposite signs

(4.3), and we assume that at each step i we can find integers x_i and y_i that satisfy $r_i = ax_i + by_i$. We end up with the following sequence.

$$\begin{aligned} a &= q_1 b + r_1 & r_1 &= ax_1 + by_1 \\ b &= q_2 r_1 + r_2 & r_2 &= ax_2 + by_2 \\ r_1 &= q_3 r_2 + r_3 & r_3 &= ax_3 + by_3 \\ &\cdot & &\cdot \end{aligned} \qquad \begin{aligned} r_{n-2} &= q_n r_{n-1} + r_n & r_n &= ax_n + by_n \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

we can rearrange terms to write

$$r_i = r_{i-2} - r_{i-1} q_i$$

Also, in rows $i - 1$ and $i - 2$, we find the values

$$r_{i-2} = ax_{i-2} + by_{i-2} \quad \text{and} \quad r_{i-1} = ax_{i-1} + by_{i-1}$$

Substituting into Equation (4.8), we have

$$\begin{aligned} r_i &= (ax_{i-2} + by_{i-2}) - (ax_{i-1} + by_{i-1})q_i \\ &= a(x_{i-2} - q_i x_{i-1}) + b(y_{i-2} - q_i y_{i-1}) \end{aligned}$$

But we have already assumed that $r_i = ax_i + by_i$. Therefore,

$$x_i = x_{i-2} - q_i x_{i-1} \quad \text{and} \quad y_i = y_{i-2} - q_i y_{i-1}$$

To find d = gcd(a, b) = gcd(1160718174, 316258250)		
$a = q_1 b + r_1$	1160718174 = 3 * 316258250 + 211943424	d = gcd(316258250, 211943424)
$b = q_2 r_1 + r_2$	316258250 = 1 * 211943424 + 104314826	d = gcd(211943424, 104314826)
$r_1 = q_3 r_2 + r_3$	211943424 = 2 * 104314826 + 3313772	d = gcd(104314826, 3313772)
$r_2 = q_4 r_3 + r_4$	104314826 = 31 * 3313772 + 1587894	d = gcd(3313772, 1587894)
$r_3 = q_5 r_4 + r_5$	3313772 = 2 * 1587894 + 137984	d = gcd(1587894, 137984)
$r_4 = q_6 r_5 + r_6$	1587894 = 11 * 137984 + 70070	d = gcd(137984, 70070)
$r_5 = q_7 r_6 + r_7$	137984 = 1 * 70070 + 67914	d = gcd(70070, 67914)
$r_6 = q_8 r_7 + r_8$	70070 = 1 * 67914 + 2156	d = gcd(67914, 2156)
$r_7 = q_9 r_8 + r_9$	67914 = 31 * 2156 + 1078	d = gcd(2156, 1078)
$r8 = q10r9 + r10$	2156 = 2 * 1078 + 0	d = gcd(1078, 0) = 1078
Therefore, d = gcd(1160718174, 316258250) = 1078		