UNIT I   INTRODUCTION & NUMBER THEORY

Services, Mechanisms and attacks-the OSI security architecture-Network security model-Classical Encryption techniques (Symmetric cipher model, substitution techniques, transposition techniques, steganography).FINITE FIELDS AND NUMBER THEORY: Groups, Rings, Fields-Modular arithmetic-Euclid‟s algorithm-Finite fields- Polynomial Arithmetic – Prime numbers-Fermat‟s and Euler‟s theorem-Testing for primality -The Chinese remainder theorem- Discrete logarithms.

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 or encryption.
Decryption: The process of converting from cipher text in to plain text is known as deciphering or decryption.
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 be defined 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 security attack
· **Security service** – A service that enhances the security of the data processing systems and the information transfers of an organization.

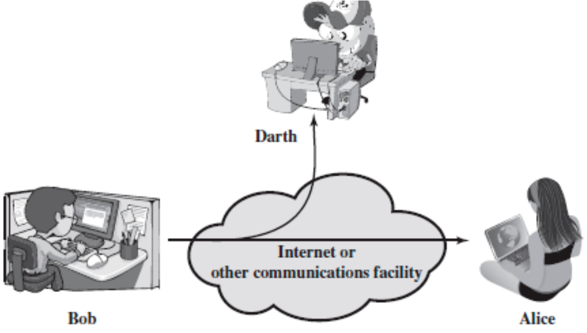
SECURITY ATTACK

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

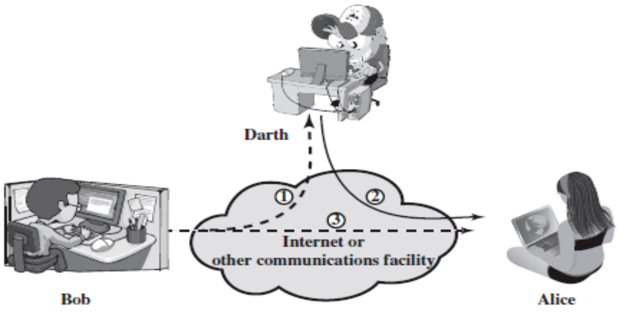
- **Release of message contents**
- **Traffic analysis**:

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 of these 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

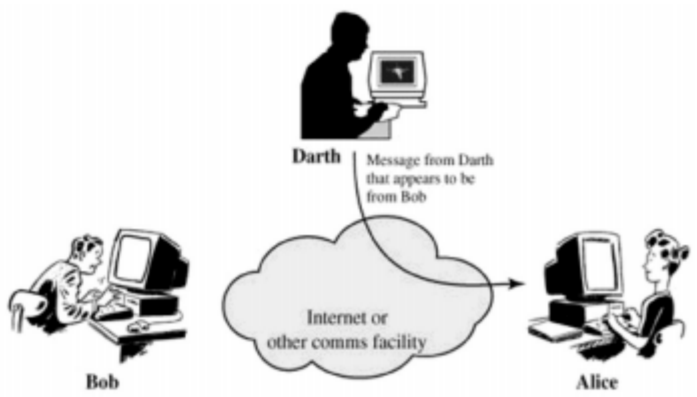
These attacks involve some modification of the data stream or the creation of a false stream.



(b) Active attacks

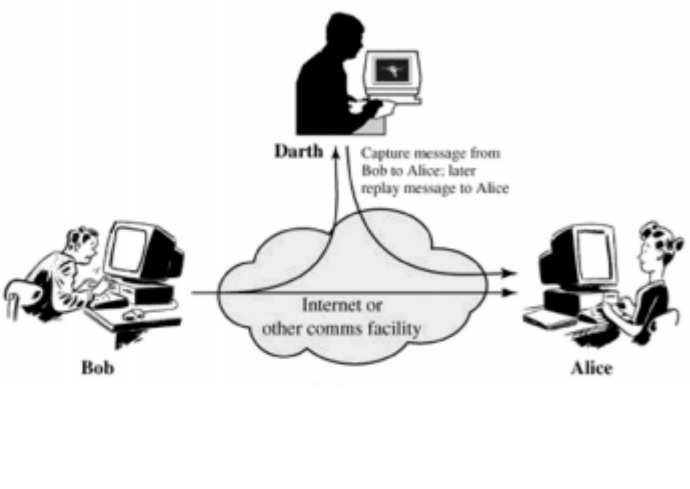
Active attacks can be classified in to four categories:

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

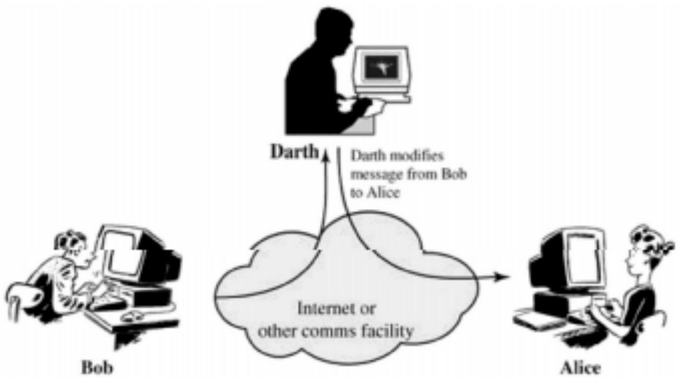


(a) Masquerade

· **Replay** – The attacker captures the message and retransmits the message without modification to produce unauthorized effect.



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

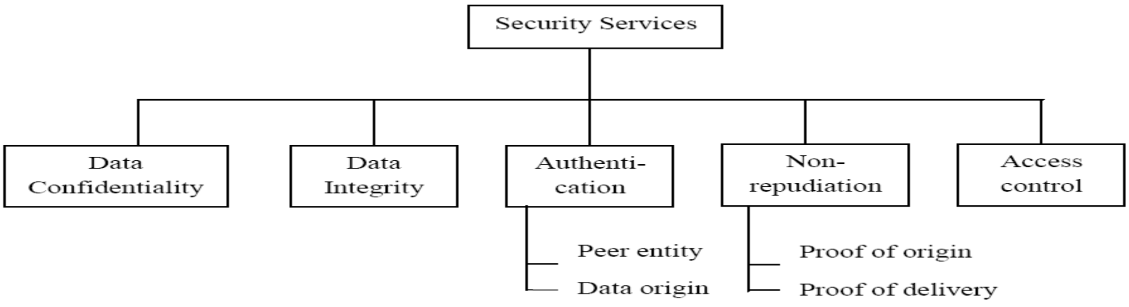

Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

· **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 is authentic.
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 and applications.

(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 data block
- **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 recovery attempted.
- **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 have been 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 be provided.
- **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

<u>SECURITY MECHANISMS</u>

- **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

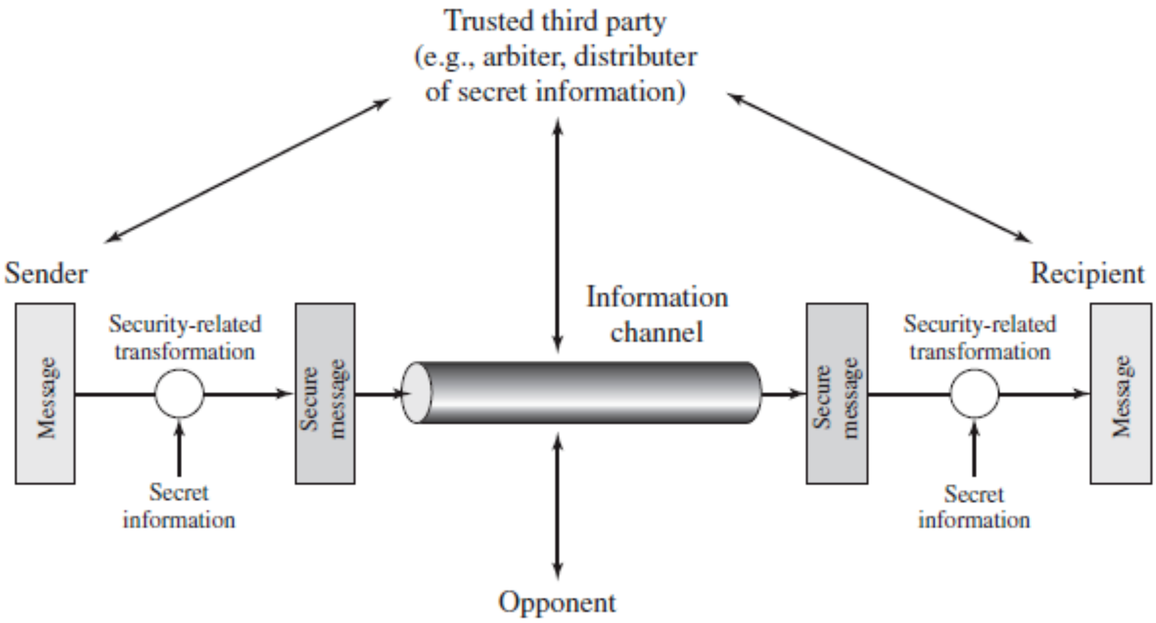
- **Traffic padding**

  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

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

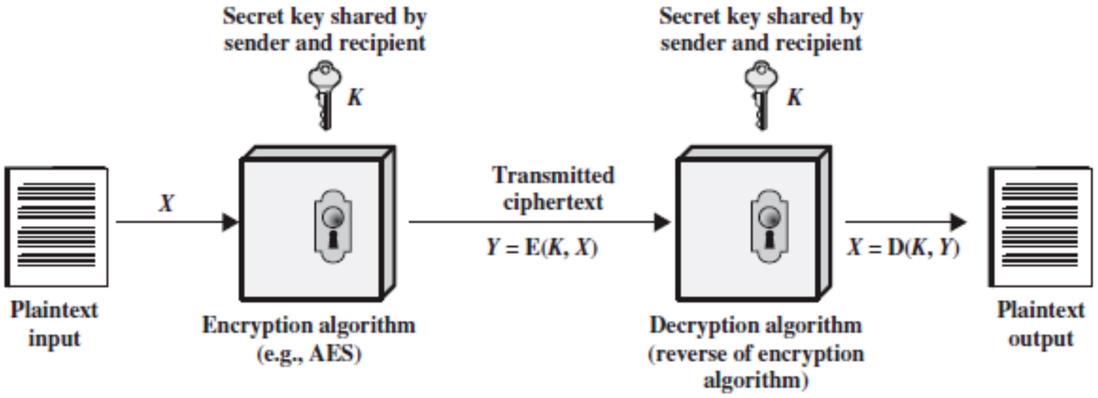
A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent.

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 be such 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 the secret information to achieve a particular security service.

SYMMRTIC CIPHER MODEL

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


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

A symmetric encryption scheme has five ingredients

• **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 transformations on 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.

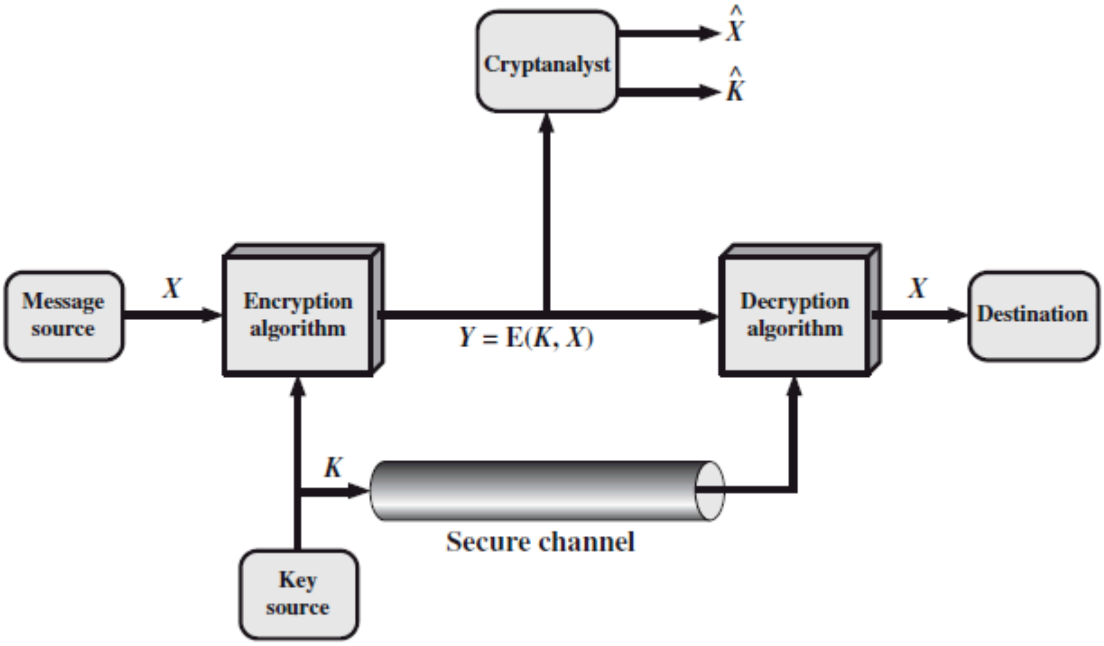
• **Cipher text:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands, is unintelligible.

• **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 and must 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

$X = [X_1, X_2,..., X_M]$.

M- elements of *X* are letters.

For encryption, a key of the form

$K = [K_1, K_2, \ldots, K_J]$ 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 deliver it to both source and destination.

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

$Y = [Y_1, Y_2,\ldots, Y_N]$.

$Y = \mathrm{E}(K, X)$

Y- cipher text
E- Encryption algorithm
K- Key
X-Plain text

At the receiver side the transformation:

$X = \mathrm{D}(K, Y)$

Y- cipher text
D-Decryption algorithm
K- Key
X-Plain text

If the opponent is interested in only this particular message only, tries to find the message estimate $\hat{X}$. But when the opponent is interested in the current and future messages, tries to find key estimate $\hat{K}$.

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 the general 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 an intelligible translation into plaintext is obtained.

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

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 Plaintext	• Encryption algorithm • Cipher text • Plaintext message chosen by cryptanalyst, together with its corresponding Cipher text generated with the secret key
Chosen Cipher text	• 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 corresponding Cipher 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 does not 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.

I .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

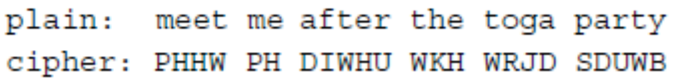
(iv) Hill cipher

(v) Poly alphabetic cipher

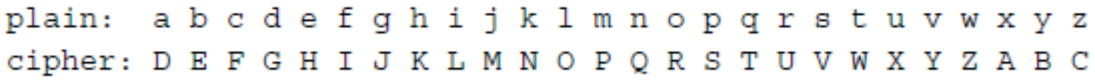
(vi) Vignere cipher

(i)**CAESAR CIPHER (OR) SHIFT CIPHER**

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

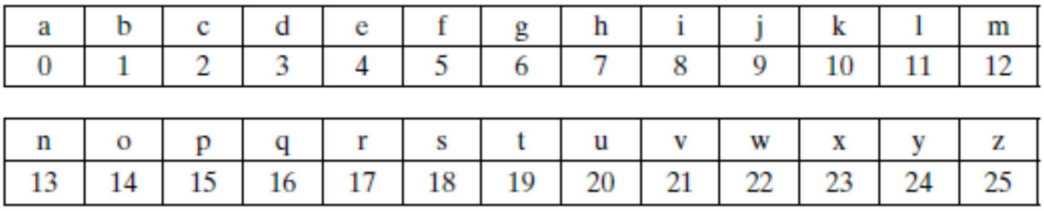


```
plain:  meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB
```



```
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
```

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

$$c = E(3, p) = (p+3) \bmod 26$$

Decryption is

$$p=D(3,c)=(c-3) \bmod 26$$

The general Caesar algorithm is

$$C = E(k, p) = (p + k) \bmod 26$$

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

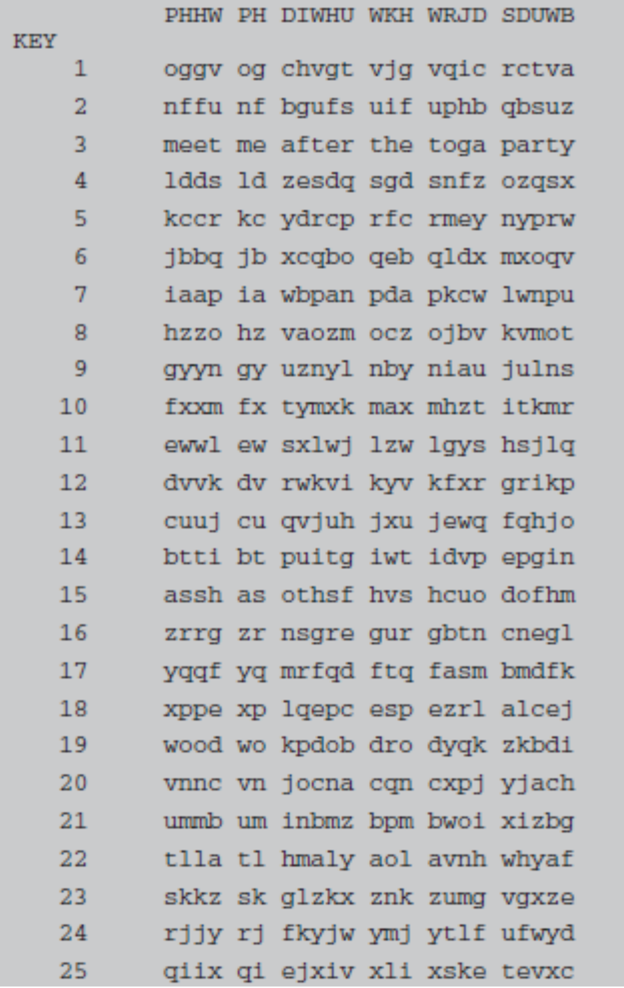
The decryption algorithm is simply

$$p = D(k, c) = (C - k) \bmod 26$$

If it is known that a given cipher text is a Caesar cipher, then a brute-force cryptanalysis is easily performed: 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



```
           PHHW PH DIWHU WKH WRJD SDUWB
KEY
    1      oggv og chvgt vjg vqic rctva
    2      nffu nf bgufs uif uphb qbsuz
    3      meet me after the toga party
    4      ldds ld zesdq sgd snfz ozqsx
    5      kccr kc ydrcp rfc rmey nyprw
    6      jbbq jb xcqbo qeb qldx mxoqv
    7      iaap ia wbpan pda pkcw lwnpu
    8      hzzo hz vaozm ocz ojbv kvmot
    9      gyyn gy uznyl nby niau julns
   10      fxxm fx tymxk max mhzt itkmr
   11      ewwl ew sxlwj lzw lgys hsjlq
   12      dvvk dv rwkvi kyv kfxr grikp
   13      cuuj cu qvjuh jxu jewq fqhjo
   14      btti bt puitg iwt idvp epgin
   15      assh as othsf hvs hcuo dofhm
   16      zrrg zr nsgre gur gbtn cnegl
   17      yqqf yq mrfqd ftq fasm bmdfk
   18      xppe xp lqepc esp ezrl alcej
   19      wood wo kpdob dro dyqk zkbdi
   20      vnnc vn jocna cqn cxpj yjach
   21      ummb um inbmz bpm bwoi xizbg
   22      tlla tl hmaly aol avnh whyaf
   23      skkz sk glzkx znk zumg vgxze
   24      rjjy rj fkyjw ymj ytlf ufwyd
   25      qiix qi ejxiv xli xske tevxc
```

Brute-Force Cryptanalysis of Caesar Cipher

(ii) MONOALPHABETIC CIPHER

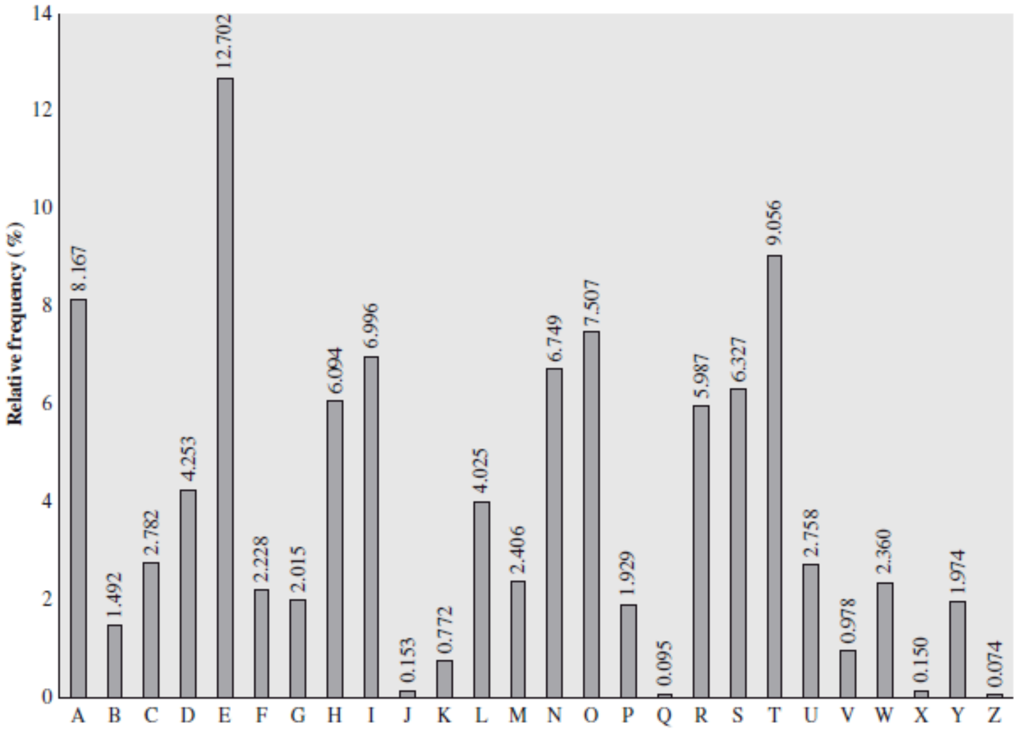
- Each plaintext letter maps to a different random cipher text letter
- Here, 26! Possible keys are used to eliminate brute force attack

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

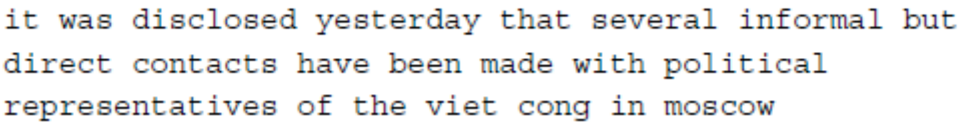
P	13.33	H	5.83	F	3.33	B	1.67	C	0.00
Z	11.67	D	5.00	W	3.33	G	1.67	K	0.00
S	8.33	E	5.00	Q	2.50	Y	1.67	L	0.00
U	8.33	V	4.17	T	2.50	I	0.83	N	0.00
O	7.50	X	4.17	A	1.67	J	0.83	R	0.00
M	6.67								



Relative frequency of letters in English text

```
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
```

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
```

(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 letter such 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 digram is 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) HILL CIPHER

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 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:

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

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

C=KP mod 26

C and P are column vectors of length 3 representing the cipher and plain text respectively.

Consider the message 'ACT', and

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

The key below (or GYBNQKURP in letters)

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

Thus the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

which corresponds to a ciphertext of 'POH’

Decryption

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

In order to decrypt, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters).

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix}$$

Cipher text of 'POH'

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \pmod{26}$$

Now gets us back the plain text 'ACT'

Merits and Demerits

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

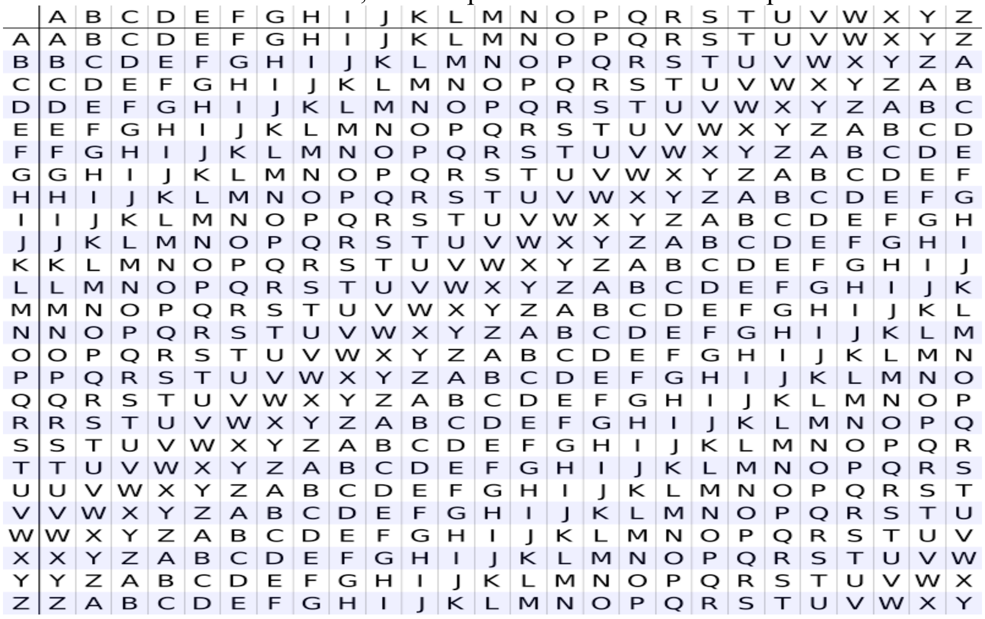
(v)POLYALPHABETIC CIPHERS

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.

Example: **Vigenere Cipher**

Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top. The process of encryption is simple: Given a key letter x and a plaintext letter y, the cipher text is at the intersection of the row labelled x and the column labelled y; in this case, the cipher text is V. To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.
Key=deceptive
Plain text= we are discovered save yourself
e.g., key = deceptivedeceptivedeceptive
PT = wearediscoveredsaveyourself
CT = ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of that column.



	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

(vi) VERNAM CIPHER or ONE-TIME PAD

It is an unbreakable cryptosystem. It represents the message as a sequence of 0s and 1s. This can be accomplished by writing all numbers in binary, for example, or by using ASCII. The key is a random sequence of 0‟s and 1‟s of same length as the message. Once a key is used, it is discarded and never used again.

The system can be expressed as follows:

$$\mathbf{C_i = P_i \oplus K_i}$$

C_i - ith binary digit of cipher text P_i - i^{th} binary digit of plaintext K_i - ith binary digit of key

$\oplus$ – exclusive OR operation

Thus the cipher text is generated by performing the bitwise XOR of the plaintext and the key. Decryption uses the same key. Because of the properties of XOR, decryption simply involves the same bitwise operation:

$$\mathbf{P_i = C_i \oplus K_i}$$

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.

Due to the above two drawbacks, one time pad is of limited use and is used for low band width channel which needs high security.

II .TRANSPOSITION TECHNIQUES

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

RAIL FENCE CIPHER

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

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

ROW TRANSPOSITION CIPHERS-

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 key of the algorithm.

e.g., 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 o
      l 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.

STEGANOGRAPHY

In Steganography, the plaintext is hidden. The existence of the message is concealed. For example, the sequence of first letters of each word of the overall message spells out the hidden message.

Various other techniques have been used historically; some examples are the following:

- **Character marking:** Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not 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 some chemical is applied to the paper.
- **Pin punctures:** Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.
- **Typewriter correction ribbon:** Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Drawback

- It requires a lot of overhead to hide a relatively few bits of information.
- Once the system is discovered, it becomes virtually worthless

GROUPS, RINGS, AND FIELDS

Groups, rings, and fields are the fundamental elements of a branch of mathematics known as abstract algebra, or modern algebra.

GROUPS

A **group** G, sometimes denoted by $\{G, \bullet\}$, is a set of elements with a binary operation denoted by • that associates to each ordered pair (a, b) of elements in G an element $(a \bullet b)$ in G, such that the following axioms are obeyed:

(A1) Closure: If a and b belong to G, then $a \bullet b$ is also in G.
(A2) Associative: $a\bullet(b\bullet c) = (a\bullet b)\bullet c$ for all a, b, c in G.
(A3) Identity element: There is an element e in G such that $a \bullet \mathrm{e} = \mathrm{e} \bullet a = a$ for all a in G.
(A4) Inverse element: For each a in G, there is an element a^{-1} in G such that $a \bullet a^{-1} = a^{-1}\bullet a = \mathrm{e}$.
If a group has a finite number of elements, it is referred to as a **finite group**, and the **order** of the group is equal to the number of elements in the group. Otherwise, the group is an **infinite group**. A group is said to be **abelian** if it satisfies the following additional condition:
(A5) Commutative: $a \bullet b = b \bullet a$ for all a, b in G.
A group G is **cyclic** if every element of G is a power a^k (k is an integer) of a fixed element $a \varepsilon G$. The element a is said to **generate** the group G or to be a **generator** of G. A cyclic group is always abelian and may be finite or infinite.

RINGS

A **ring** R, sometimes denoted by $\{R, +, *\}$, is a set of elements with two binary operations, called *addition* and *multiplication*,6 such that for all a, b, c in R the following axioms are obeyed.
(A1–A5) R is an abelian group with respect to addition; that is, R satisfies axioms A1 through A5.
(M1) Closure under multiplication: If a and b belong to R, then ab is also in R.
(M2) Associativity of multiplication: $a(bc) = (ab)c$ for all a, b, c in R.
(M3) Distributive laws: $a(b + c) = ab + ac$ for all a, b, c in R.
$(a + b)c = ac + bc$ for all a, b, c in R.
A ring is said to be **commutative** if it satisfies the following additional condition:
(M4) Commutativity of multiplication: $ab = ba$ for all a, b in R.
An **integral domain**, which is a commutative ring that obeys the following axioms.
(M5) Multiplicative identity: There is an element 1 in R such that $a1 = 1a = a$ for all a in R.
(M6) No zero divisors: If a, b in R and $ab = 0$, then either $a = 0$ or $b = 0$.

FIELDS

A **field** F, sometimes denoted by $\{F, +, *\}$, is a set of elements with two binary operations, called *addition* and *multiplication*, such that for all a, b, c in F the following axioms are obeyed.
(A1–M6) F is an integral domain; that is, F satisfies axioms A1 through A5 and M1 through M6.
(M7) Multiplicative inverse: For each a in F, except 0, there is an element a-1 in F such that $aa^{-1} = (a^{-1})a = 1$

MODULAR ARITHMETIC

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**.

$$a = qn + r \qquad 0 \leq r < n;$$

$$q = \lfloor a/n \rfloor$$

Congruent modulo

Two integers a and b are said to be congruent modulo n if
a (mod n)≡ b (mod n)
a ≡ b (mod n)
73 ≡ 4 mod 23

Properties of modulo operator

Congruences have the following properties:
1. a≡ b (mod n) if n|(a-b)
2. a≡ b (mod n) implies b≡ a(mod n)
3. a ≡ *b* (mod *n*) and *b* ≡ *c* (mod *n*) imply *a* ≡ *c* (mod *n*).

Modular Arithmetic Operations

Modular arithmetic exhibits the following properties:
1. [(*a* mod *n*) + (*b* mod *n*)] mod *n* = (*a* + *b*) mod *n*
2. [(*a* mod *n*) - (*b* mod *n*)] mod *n* = (*a* - *b*) mod *n*
3. [(*a* mod *n*) * (*b* mod *n*)] mod *n* = (*a* * *b*) mod *n*
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) * (15 mod 8)] mod 8 = 21 mod 8 = 5
(11 * 15) mod 8 = 165 mod 8 = 5

Relatively prime

Two integers are **relatively prime,** if their only common positive integer factor is 1.
8 and 15 are relatively prime because
Positive divisors of 8 are 1,2,4,8
Positive divisors of 15 are 1, 3, 5, 15
Therefore, common positive factor=1.

EUCLIDEAN ALGORITHM

Euclidean algorithm is a simple procedure for determining the greatest common divisor of two positive integers.
The positive 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)=gcd(|a|,|b|)
gcd(a,0)=|a|

```
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
```

Euclidean Algorithm Revisited

For any integers a, b, with $a \geq b \geq 0$,
gcd(a, b) = gcd(b, a mod b)

Example

gcd(55, 22) = gcd(22, 55 mod 22) = gcd(22, 11) = 11
gcd(18, 12) = gcd(12, 6) = gcd(6, 0) = 6
gcd(11, 10) = gcd(10, 1) = gcd(1, 0) = 1

POLYNOMIAL ARITHMETIC

A **polynomial** of degree n (integer $n \geq 0$) is an expression of the form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

where the a_i – *coefficients*

$$f(x) = \sum_{i=0}^{n} a_i x^i; \quad g(x) = \sum_{i=0}^{m} b_i x^i; \quad n \geq m$$

Addition is defined as

$$f(x) + g(x) = \sum_{i=0}^{m} (a_i + b_i)x^i + \sum_{i=m+1}^{n} a_i x^i$$

Multiplication is defined as

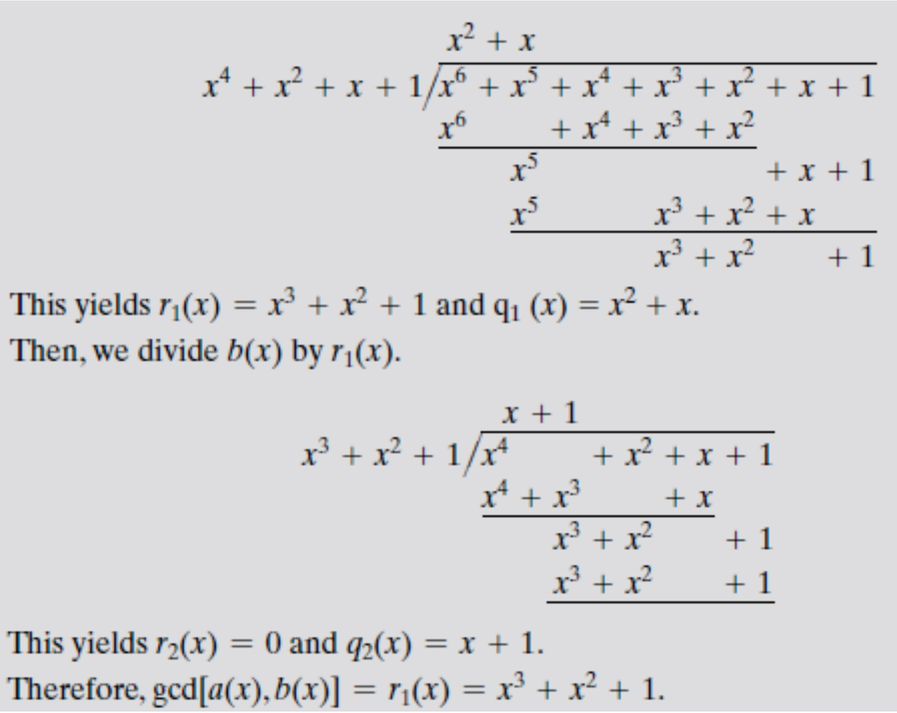
$$f(x) \times g(x) = \sum_{i=0}^{n+m} c_i x^i$$

where

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0$$

Let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$, where S is the set of integers. Then
$f(x) + g(x) = x^3 + 2x^2 - x + 3$
$f(x) - g(x) = x^3 + x + 1$
$f(x) * g(x) = x^5 + 3x^2 - 2x + 2$

Find gcd[$a(x)$, $b(x)$] for $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $b(x) = x^4 + x^2 + x + 1$.
Euclidean algorithm to compute the greatest common divisor of two polynomials
gcd[$a(x)$, $b(x)$] = gcd[$b(x)$, $a(x)$ mod $b(x)$]
=gcd(b(x),r1(x))
=gcd[r1(x),b(x) mod r1(x)]



$$\begin{array}{r}
x^2 + x \\
x^4 + x^2 + x + 1 \overline{\smash{)}\,x^6 + x^5 + x^4 + x^3 + x^2 + x + 1} \\
\underline{x^6 \qquad + x^4 + x^3 + x^2} \\
x^5 \qquad\qquad\qquad + x + 1 \\
\underline{x^5 \qquad\quad x^3 + x^2 + x} \\
x^3 + x^2 \qquad + 1
\end{array}$$

This yields $r_1(x) = x^3 + x^2 + 1$ and $q_1(x) = x^2 + x$.

Then, we divide $b(x)$ by $r_1(x)$.

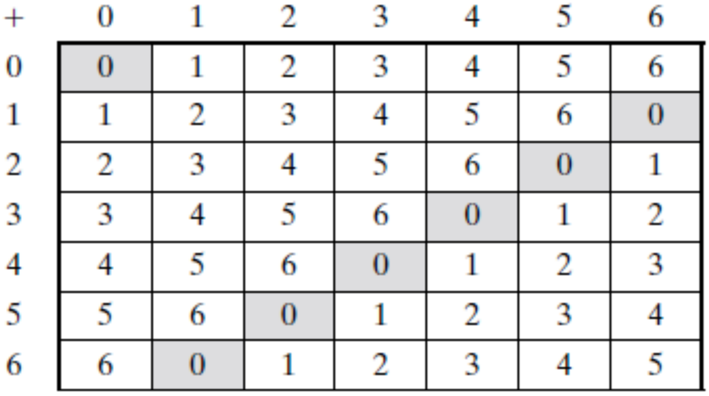
$$\begin{array}{r}
x + 1 \\
x^3 + x^2 + 1 \overline{\smash{)}\,x^4 \qquad + x^2 + x + 1} \\
\underline{x^4 + x^3 \qquad + x} \\
x^3 + x^2 \qquad + 1 \\
\underline{x^3 + x^2 \qquad + 1}
\end{array}$$

This yields $r_2(x) = 0$ and $q_2(x) = x + 1$.

Therefore, $\gcd[a(x), b(x)] = r_1(x) = x^3 + x^2 + 1$.

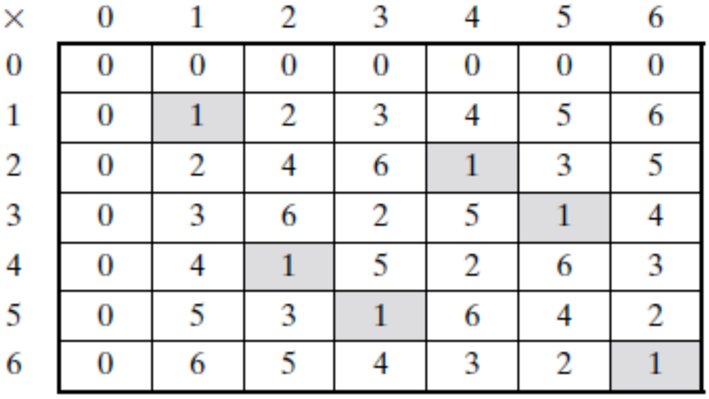
Multiplicative Inverse

It is easy to find the multiplicative inverse of an element in GF(p) for small values of p *by* constructing a multiplication table, such as shown in Table and the desired result can be read directly. However, for large values of p, this approach is not practical.



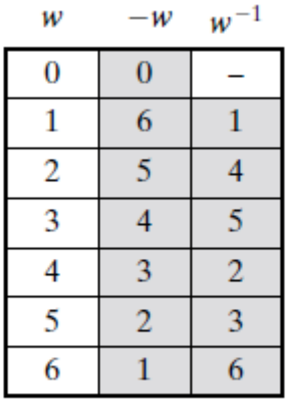
+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(a) Addition modulo 7



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

(b) Multiplication modulo 7



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

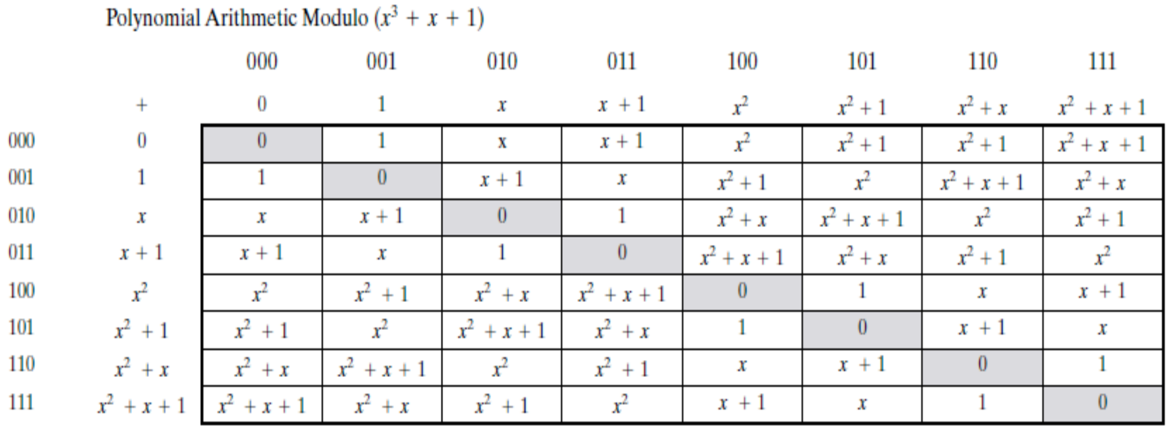
(c) Additive and multiplicative inverses modulo 7

If *a* and *b* are relatively prime, then *b* has a multiplicative inverse modulo *a*. That is, if gcd(*a*, *b*) = 1, then *b* has a multiplicative inverse modulo *a*. That is, for positive integer *b* < *a*, there exists a *b*-1 < *a* such that

$bb^{-1} = 1 \bmod a$.

If *a* is a prime number and *b* < *a*, then clearly *a* and *b* are relatively prime and have a greatest common divisor of 1. We now show that we can easily compute *b*-1 using the extended Euclidean algorithm.

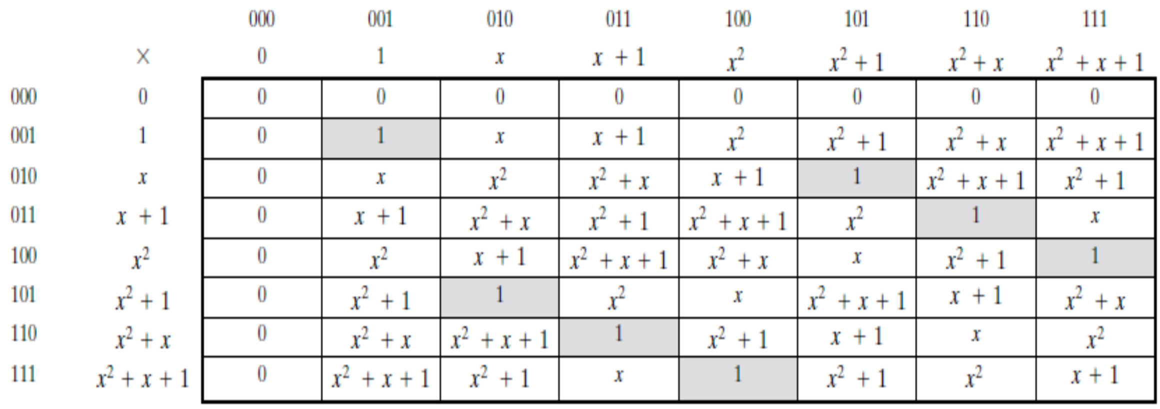
Finding the Multiplicative Inverse of a polynomial



Polynomial Arithmetic Modulo ($x^3 + x + 1$)

		000	001	010	011	100	101	110	111
	+	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+1	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(a) Addition



		000	001	010	011	100	101	110	111
	×	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+1	x^2	$x+1$

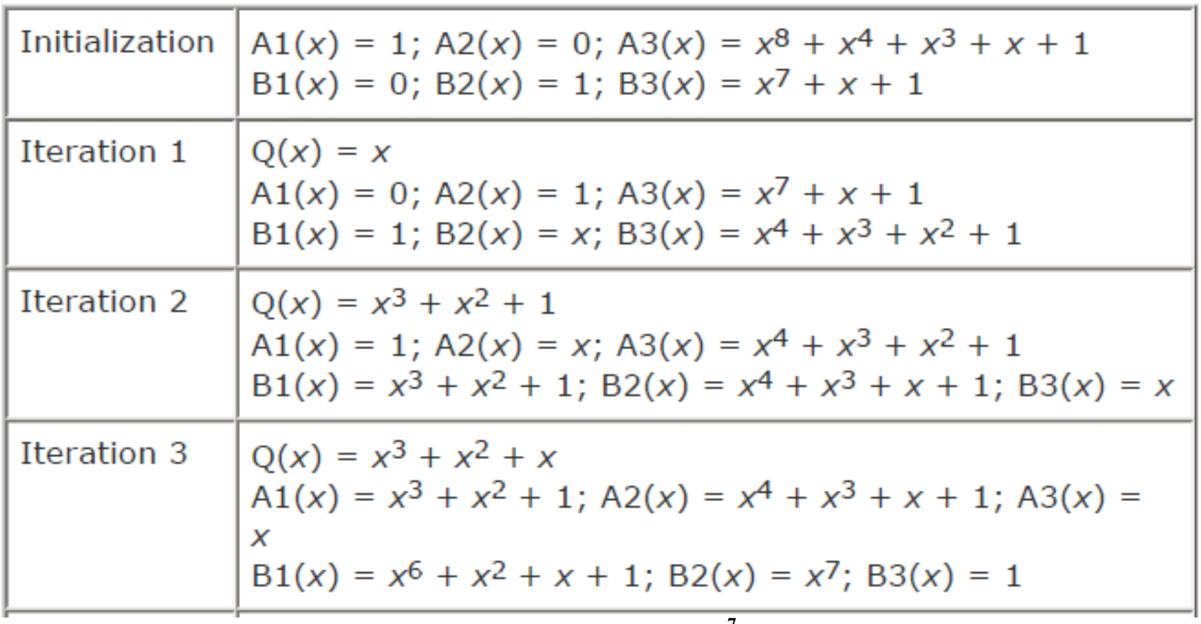
(b) Multiplication

The extended Euclidean algorithm can be adapted to find the multiplicative inverse of a polynomial. Specifically, the algorithm will find the multiplicative inverse of b(x) modulo m(x) if the degree of b(x) is less than the degree of m(x) and gcd[m(x), b(x)] = 1. If m(x) is an irreducible polynomial, then it has no factor other than itself or 1, so that gcd[m(x), b(x)] = 1. The algorithm is as follows:

```
EXTENDED EUCLID [m(x), b(x)]

1. [A1(x), A2(x), A3(x)]←[1, 0, m(x)];  [B1(x), B2(x),B3(x)] ←[0, 1, b(x)]
2. if B3(x) = 0 return A3(x) = gcd[m(x), b(x)]; no inverse
3. if B3(x) = 1 return B3(x) = gcd[m(x), b(x)]; B2(x) = b(x)1 mod m(x)
4. Q(x) = quotient of A3(x)/B3(x)
5. [T1(x), T2(x), T3(x)]← [A1(x)-Q(x)B1(x), A2(x)-Q(x)B2(x), A3(x)-QB3(x)]
6. [A1(x), A2(x), A3(x)]← [B1(x), B2(x), B3(x)]
7. [B1(x), B2(x), B3(x)]← [T1(x), T2(x), T3(x)]
8. goto 2
```

Calculate the multiplicative inverse of $(x^7 + x + 1)$ mod $(x^8 + x^4 + x^3 + x + 1)$.



Initialization	$A1(x) = 1; A2(x) = 0; A3(x) = x^8 + x^4 + x^3 + x + 1$ $B1(x) = 0; B2(x) = 1; B3(x) = x^7 + x + 1$
Iteration 1	$Q(x) = x$ $A1(x) = 0; A2(x) = 1; A3(x) = x^7 + x + 1$ $B1(x) = 1; B2(x) = x; B3(x) = x^4 + x^3 + x^2 + 1$
Iteration 2	$Q(x) = x^3 + x^2 + 1$ $A1(x) = 1; A2(x) = x; A3(x) = x^4 + x^3 + x^2 + 1$ $B1(x) = x^3 + x^2 + 1; B2(x) = x^4 + x^3 + x + 1; B3(x) = x$
Iteration 3	$Q(x) = x^3 + x^2 + x$ $A1(x) = x^3 + x^2 + 1; A2(x) = x^4 + x^3 + x + 1; A3(x) = x$ $B1(x) = x^6 + x^2 + x + 1; B2(x) = x^7; B3(x) = 1$

Since B3 = 1 B2 is the Multiplicative Inverse ie) x^7

PRIME NUMBER

An integer $p > 1$ is a prime number if and only if its only divisors are ±1 and $\pm p$.
Any integer $a > 1$ can be factored in a unique way as

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$$

where $p_1 < p_2 < \ldots < p_t$ are prime numbers and where each a_i is a positive integer.

$91 = 7 * 13$

$3600 = 2^4 * 3^2 * 5^2$

$11011 = 7 * 11^2 * 13$

If P is the set of all prime numbers, then any positive integer a can be written uniquely in the following form:

$$a = \prod_{p \in P} p^{a_p} \quad \text{where each } a_p \geq 0$$

It is easy to determine the greatest common divisor of two positive integers if we express each integer as the product of primes.

$300 = 2^2 * 3^1 * 5^2$

$18 = 2^1 * 3^2$

$\gcd(18, 300) = 2^1 * 3^1 * 5^0 = 6$

The following relationship always holds:
If $k = \gcd(a, b)$, then $k_p = \min(a_p, b_p)$ for all p.

FERMAT'S THEOREMS

Fermat's theorem states the following: if *p* is a prime and *a* is a positive integer not divisible by *p*, then

$$\mathbf{a^{p-1} \equiv 1(mod\ p)}$$

Consider the set of positive integers less than *p:*{1,2,3..p-1}
Multiply each element by *a modulo p* to get the set

X ={ a mod p,2a mod p….(p-1)mod p}.

None of the elements of X is equal to zero because *p* does not divide *a*. No two of the integers in X are equal.(p-1) elements of X are all positive integers with no two elements are equal. Multiplying the numbers in both sets and taking the result mod *p* yields.

$$a * 2a * \ldots *(p-1)a \equiv [(1*2*\ldots*(p-1)](mod\ p)$$
$$\{1 * 2 * \ldots *(p-1)\}\ a^{p-1} \equiv [(1*2*\ldots*(p-1)](mod\ p)$$
$$(p-1)!\ a^{p-1} \equiv (p-1)!(mod\ p)$$
$$\mathbf{a^{p-1} \equiv 1(mod\ p)}$$

Example

$a = 7, p = 19$

$7^2 = 49 \equiv 11\ (mod\ 19)$

$7^4 = 121 \equiv 7\ (mod\ 19)$

$7^8 \equiv 49 \equiv 11\ (mod\ 19)$

$7^{16} \equiv 121\ K\ 7\ (mod\ 19)$

$a^{p-1} = 7^{18} = 7^{16} * 7^2 \equiv 7 * 11 \equiv 1\ (mod\ 19$

An alternative form of Fermat's theorem is also useful: If *p* is prime and *a* is a positive integer, then

$$\mathbf{a^p \equiv a(mod\ p)}$$

Euler's totient function

It is represented as *ø(n).*Euler's totient function is defined as the number of positive integers less than *n* and relatively prime to *n*. *ø(1)=1*

It should be clear that for a prime number *p*

$$\boldsymbol{ø(p)=p-1}$$

Suppose that we have two prime numbers *p* and *q*, with *p* not equal to *q*. Then we can show that

n=pq.

ø(n)= ø(pq)= ø(p)* ø(q)=(p-1)*(q-1)

ø(n)=(pq-1)-[(q-1)+(p-1)]

= pq-(p+q)+1

=(p-1)*(q-1)
= ø(p)* ø(q)

To determine f(35), we list all of the positive integers less than 35 that are relatively prime to it:
1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18
19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34
There are 24 numbers on the list, so f(35) = 24.

f(21) = f(3) * f(7) = (3 - 1) * (7 - 1) = 2 * 6 = 12

EULER'S THEOREM

Euler's theorem states that for every *a* and *n* that are relatively prime:

$a^{\o(n)}=1(\text{mod } n)$

The above equation is true, if n is prime, because in that case *ø(n)=(n-1)* and Fermat's theorem holds. However it holds for any integer *n*. recall that ø(n)is the number of positive integers less than n that are relatively prime to *n*. consider the set of such integers, labeled as follows:
$R=\{x_1,x_2\ldots x_{\o(n)}\}$
That is, each element x_i of R is a unique positive integer less than *n* with gcd(x_i,n)=1.now multiply each element by *a modulo n:*
$S=\{(ax_1 \text{ mod n}), (ax_2 \text{ mod n}),\ldots (ax_{\o(n)}) \text{ mod n})\}$
The set S is a permutation of R, by the following reasons:
1.Because *a* is relatively prime to *n* and x_i is relatively prime to *n*,ax_i must also be relatively prime to *n*. thus all the members of S are integers that are less than n and that are relatively prime to n.
2. There are no duplicates in S. if ax_i mod n=ax_j mod n, then x_i=x_j

$$\prod_{i=1}^{\phi(n)}(ax_i \bmod n) = \prod_{i=1}^{\phi(n)}x_i$$

$$\prod_{i=1}^{\phi(n)}ax_i \equiv \prod_{i=1}^{\phi(n)}x_i \pmod{n}$$

$$a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)}x_i\right] \equiv \prod_{i=1}^{\phi(n)}x_i \pmod{n}$$

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

An alternative form of the theorem is also useful:

$$a^{\phi(n)+1} \equiv a \pmod{n}$$

$$a = 3; n = 10; \phi(10) = \;\; 4\, a^{\phi(n)} = 3^4 \;\; = 81 = 1 \,(\text{mod } 10) = 1 \,(\text{mod } n)$$
$$a = 2; n = 11; \phi(11) = 10\, a^{\phi(n)} = 2^{10} = 1024 = 1 \,(\text{mod } 11) = 1 \,(\text{mod } n)$$

TESTING FOR PRIMALITY

For many cryptographic algorithms, it is necessary to select one or more very large prime numbers at random. Thus, we are faced with the task of determining whether a given large number is prime. There is no simple yet efficient means of accomplishing this task.

Miller-Rabin Algorithm

The algorithm due to Miller and Rabin [MILL75, RABI80] is typically used to test a large number for primality.

TEST (*n*)

```
    1. Find integers $k$, $q$, with $k > 0$, $q$ odd, so that $(n - 1 = 2^k q)$;
    2. Select a random integer $a$, $1 < a < n - 1$;
    3. if $a^q mod\ n = 1$ then return("inconclusive");
    4. for $j = 0$ to $k - 1$ do
    5. if $a^{2jq} mod\ n = n - 1$ then return("inconclusive");
    6. return("composite");
```

Let us apply the test to the prime number $n = 29$.
$(n - 1) = 28 = 2^2(7) = 2^k q$.
First, let us try $a = 10$.
Compute 10^7 mod 29 = 17,

$(10^7)^2$ mod 29 = 28, and the test returns inconclusive.

So n is prime number.

THE CHINESE REMAINDER THEOREM

The Chinese Remainder Theorem says it is possible to reconstruct integers in certain range from their residues modulo a set of pair wise relatively prime moduli.

$x \equiv a_1 \bmod n_1$, $x \equiv a_2 \bmod n_2$, $x \equiv a_k \bmod n_k$

If $n_1,n_2,..,n_k$ are positive integers that are pairwise co-prime and $a_1,a_2,\ldots,a_k$ are any integers, then CRT is used to find the values of x that solves the following congruence simultaneously.

Value of $x=(a_1m_1y_1+a_2m_2y_2+\ldots+a_km_ky_k) \bmod M$

Where $M=n_1n_2n_3..n_k$

$m_i=M/n_i$

$m_iy_i=1 \bmod n_i$

Problem 1

$x \equiv 1 \bmod 5$
$x \equiv 2 \bmod 6$
$x \equiv 3 \bmod 7$

$a_1=1$
$a_2=2$
$a_3=3$

$n_1=5$
$n_2=6$
$n_3=7$

$M=n_1n_2n_3$
$M=5*6*7=210$

$m_i=M/n_i$

m1=210/5=42
m2=210/6=35
m3=210/7=30

$m_iy_i=1 \bmod n_i$
$42y_1=1 \bmod 5$
$y_1=3 \bmod 5$

$35y_2= 1 \bmod 6$
$y_2=5 \bmod 6$

$30y_3=1 \bmod 7$

$y_3=4 \bmod 7$

$x=(a_1m_1y_1+a_2m_2y_2+ a_3m_3y_3) \bmod M$

$=((1*42*3)+(2*35*5)+(3*30*4)) \bmod 210$

$=836 \bmod 210$

$=206$

Problem 2

A bag has contained number of pens if you take out 3 pens at a time 2 pens are left. If you take out 4 pens at a time 1 pen is left and if you take out 5 pens at a time 3 pens are left in the bag. What is the number of pens in the bag.

$x \equiv 2 \bmod 3$

$x \equiv 1 \bmod 4$

$x \equiv 3 \bmod 5$

$a_1=2$

$a_2=1$

$a_3=3$

$n_1=3$

$n_2=4$

$n_3=5$

$M=n_1n_2n_3$

$M=3*4*5=60$

$m_i=M/n_i$

m1=60/3=20

m2=60/4=15

m3=60/5=12

$m_iy_i=1 \bmod n_i$

$20y_1=1 \bmod 3$

$y_1=2 \bmod 3$

$15y_2= 1 \bmod 4$

$y_2=3 \bmod 4$

$12y_3=1 \bmod 5$

$y_3=3 \bmod 5$

$x=(a_1m_1y_1+a_2m_2y_2+ a_3m_3y_3) \bmod M$

$=((2*20*2)+(1*15*3)+(3*12*3)) \bmod 60$

$=233 \bmod 60$

$=53$

DISCRETE LOGARITHMS.

Discrete logarithms are fundamental to a number of public-key algorithms, including Diffie-Hellman key exchange and the digital signature algorithm (DSA)

A primitive root of a prime number p is one whose powers modulo p generate all the integers from 1 to p - 1. That is, if 'a' is a primitive root of the prime number p, then the numbers

$a \bmod p, a^2 \bmod p, \ldots, a^{p-1} \bmod p$

are distinct and consist of the integers from 1 through p - 1 in some permutation.

For any integer b and a primitive root a of prime number p, we can find a unique exponent i such that

$b \equiv a^i \pmod{p}$ where 0 … i … (p - 1)

The exponent i is referred to as the discrete logarithm of b for the base a, mod p.