Unit -I

Cryptology: This is the study of techniques for ensuring the secrecy and/or authenticity of information. The two main branches of cryptology are **cryptography**, which is the study of the design of such techniques; and **cryptanalysis**, which deals with the defeating such techniques, to recover information, or forging information that will be accepted as authentic.

Network security: This area covers the use of cryptographic algorithms in networkprotocols and network applications.

Computer security: we use this term to refer to the security of computers against intruders (e.g., hackers) and malicious software (e.g., viruses). Typically, the computer to be securedis attached to a network and the bulk of the threats arise from the network.

Internet Security - measures to protect data during their transmission over a collection ofinterconnected networks

Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability

Attack
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

The OSI Security Architecture

X.800, *Security Architecture for OSI* 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 process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **Security service:** A processing or communication service that enhances

the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

I. Security Attacks

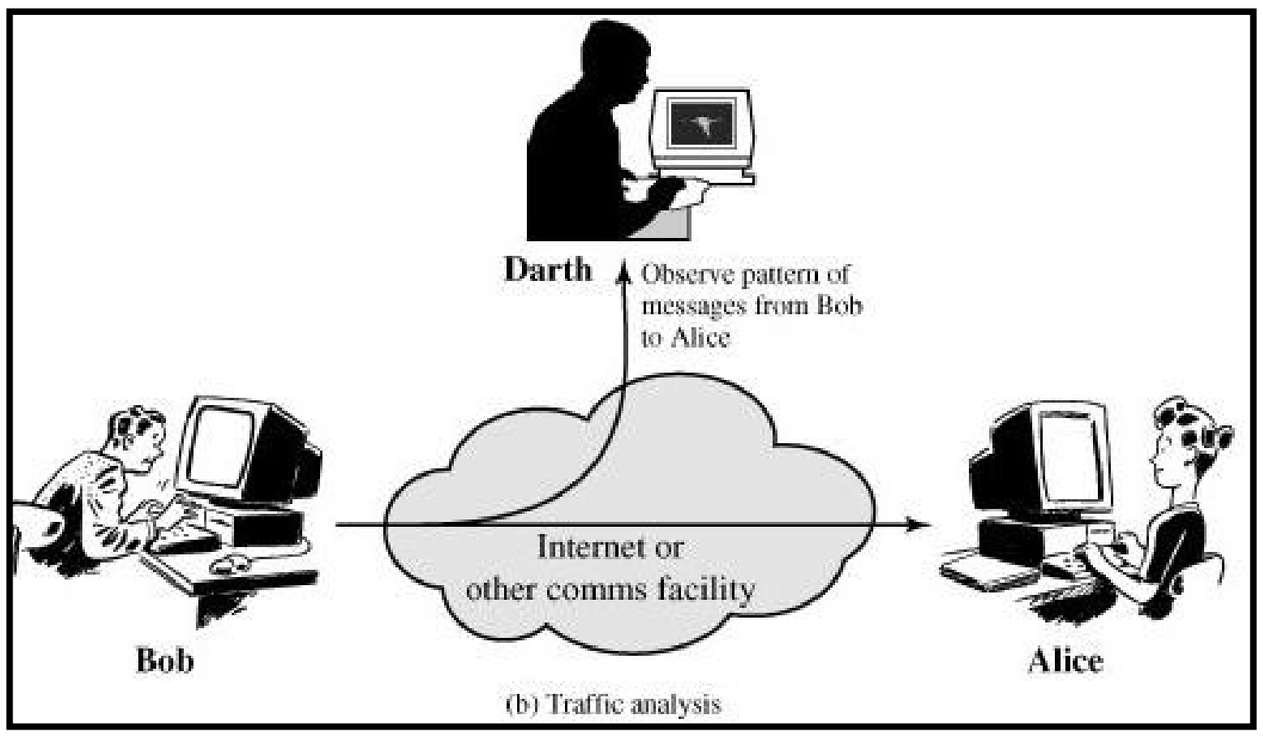
A useful means of classifying security attacks, used both in X.800 and RFC 2828, is in termsof *passive attacks* and *active attacks*.

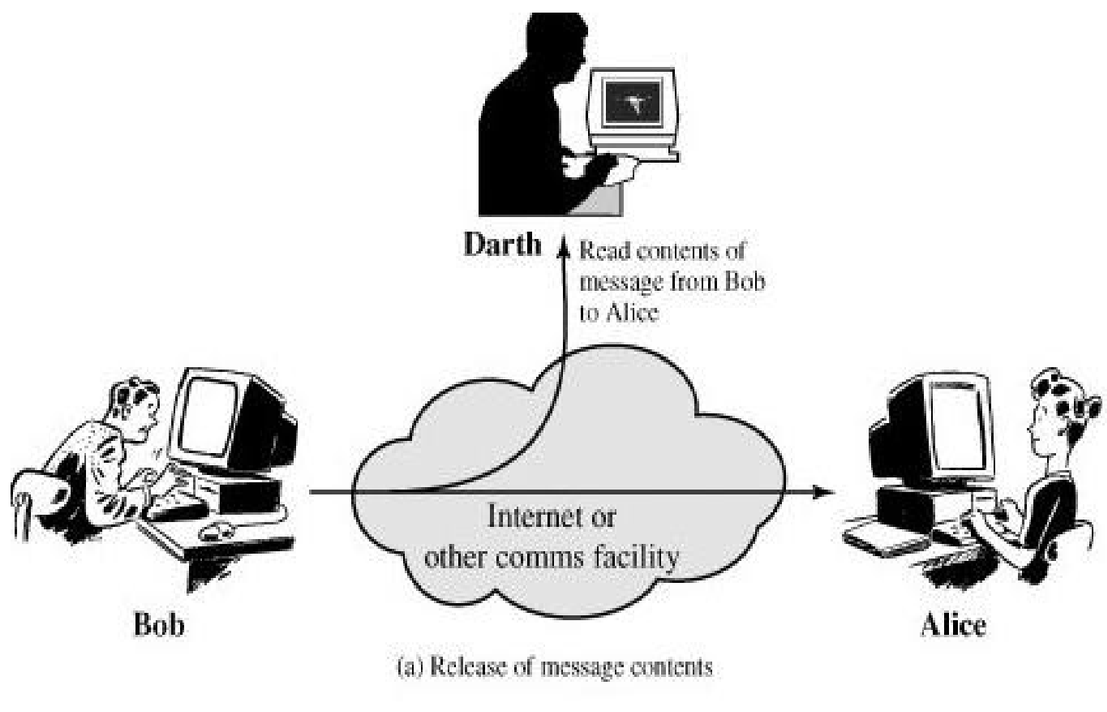
Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis.

The **release of message** contents is easily understood .A telephone conversation, an Electronic mail message and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

- A second type of passive attack, **traffic analysis**.
- Passive attacks are very difficult to detect because they do not involve any alteration ofthe data.





Active Attacks

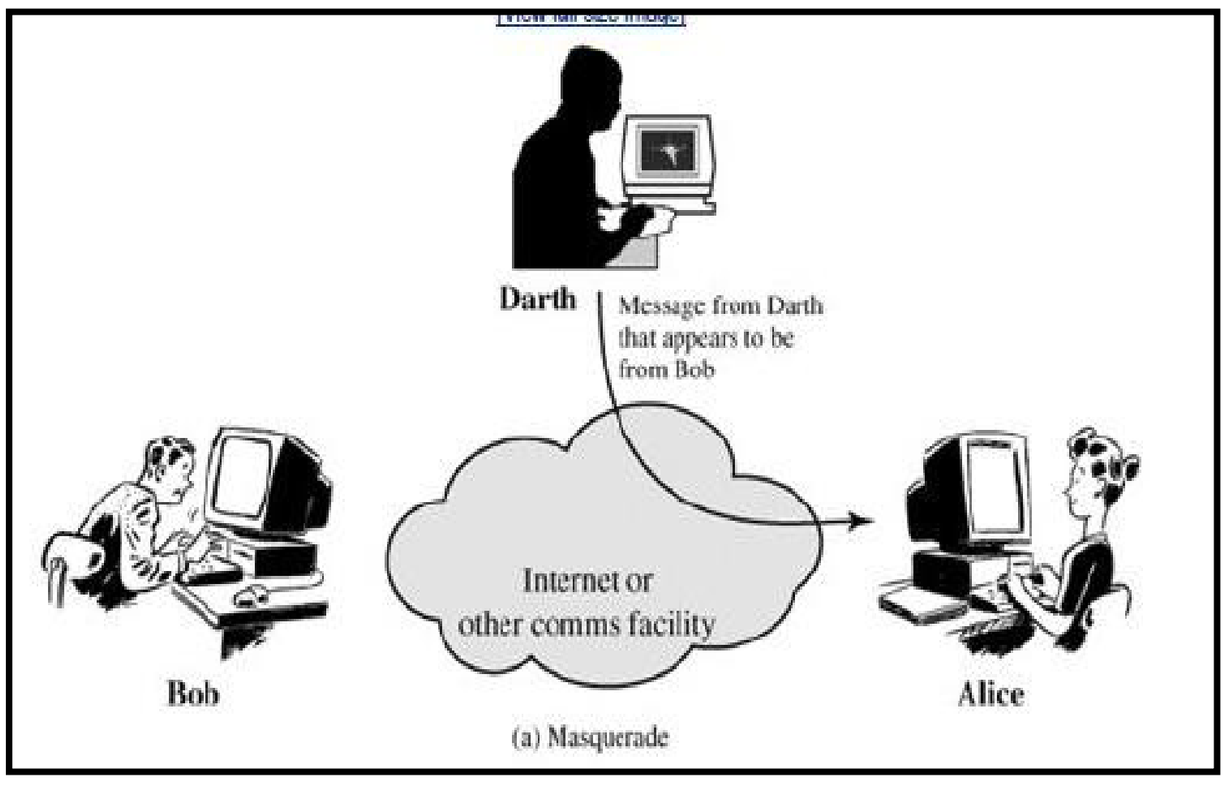
Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

- A **masquerade** takes place when one entity pretends to be a different entity . A masquerade attack usually includes one of the other forms

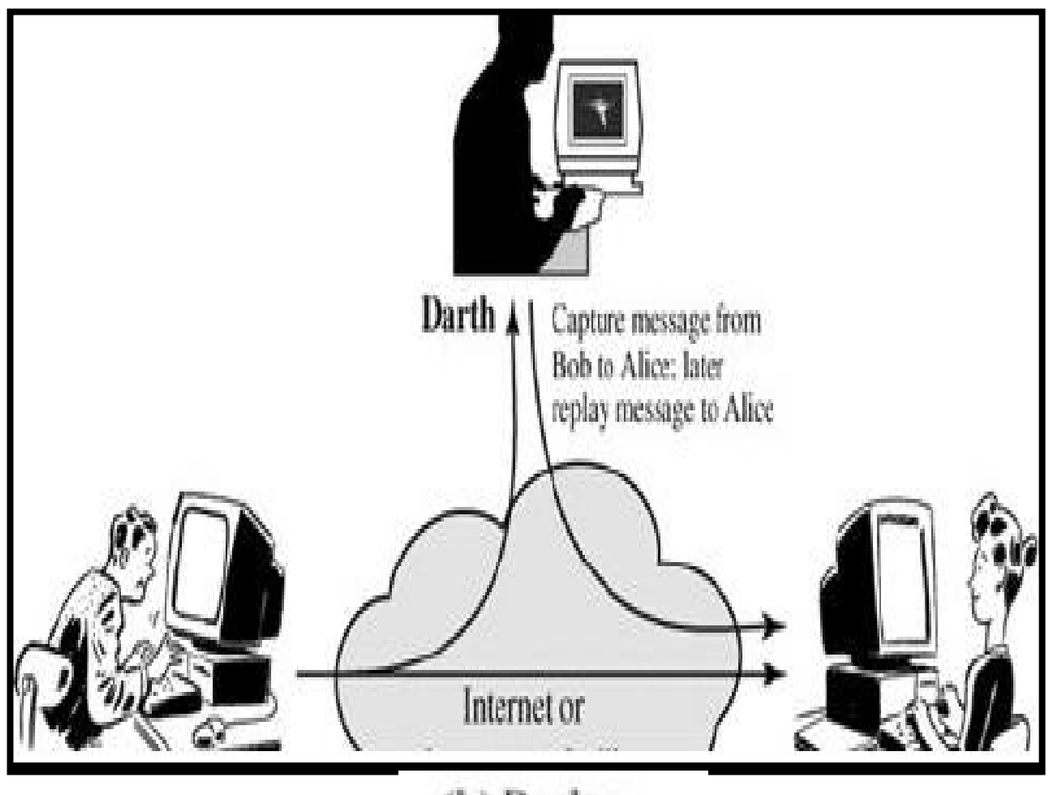
of active attack

- **Replay** involves the passive capture of a data unit and its subsequent retransmissionto produce an unauthorized effect.

- **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect



(a) Masquerade



(b) Replay

- The **denial of service** Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or 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

II. Security Services

X.800 divides these services into five categories and fourteen specific services

1. AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

- **Peer Entity Authentication**
  Used in association with a logical connection to provide confidence in the

identity of theentities connected.

Data Origin Authentication

- In a connectionless transfer, provides assurance that the source of received data is asclaimed.

2. ACCESS CONTROL

- The prevention of unauthorized use of a resource (i.e., this service controls who canhave access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

3. DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure

- **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 singledata block.
- **Traffic Flow Confidentiality**
  The protection of the information that might be derived from observation of trafficflows.

4. DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e.,contain no modification, insertion, deletion, or replay).

- **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.

5. NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication ofhaving 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.

III. Security Mechanisms

1. SPECIFIC SECURITY MECHANISMS

2. PERVASIVE SECURITY MECHANISMS

1. SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of theOSI security services

- **Encipherment**
  The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.
- **Digital Signature**
  Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and

integrity of the data unit and protect against forgery (e.g., by the recipient).

- **Access Control**
  A variety of mechanisms that enforce access rights to resources.
- **Data Integrity**
  A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- **Authentication Exchange**
  A mechanism intended to ensure the identity of an entity by means of information exchange.
- **Traffic Padding**
  The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- **Routing Control**
  Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
- **Notarization**

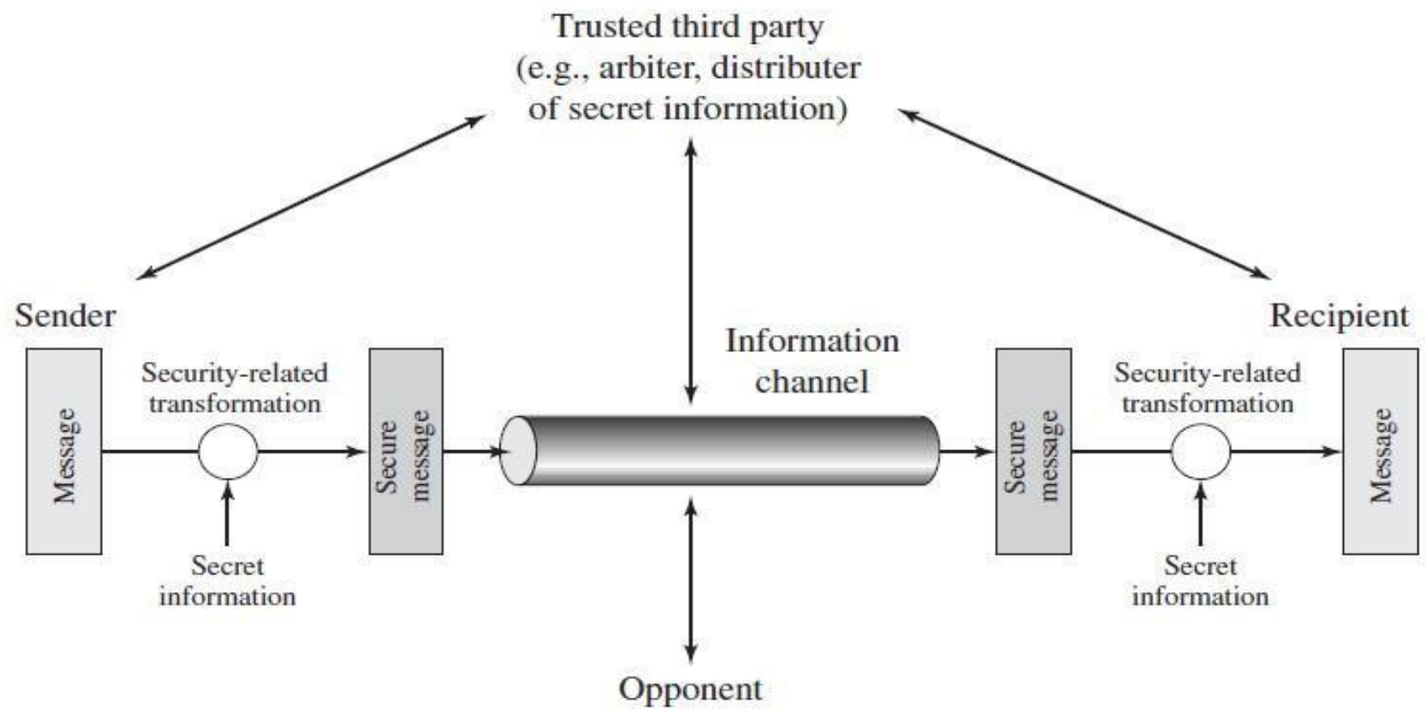
  The use of a trusted third party to assure certain properties of a data exchange.

2. **PERVASIVE SECURITY MECHANISMS**

Mechanisms that are not specific to any particular OSI security service or protocol layer.

- **Trusted Functionality**
  That which is perceived to be correct with respect to some criteria (e.g., as establishedby a security policy).
- **Security Label**
  The marking bound to a resource (which may be a data unit) that names or designatesthe security attributes of that resource.
- **Event Detection**
  Detection of security-relevant events.
- **Security Audit Trail**
  Data collected and potentially used to facilitate a security audit, which is anindependent review and examination of system records and activities.
- **Security Recovery**
  Deals with requests from mechanisms, such as event handling and managementfunctions, and takes recovery actions.

A MODEL FOR NETWORK SECURITY

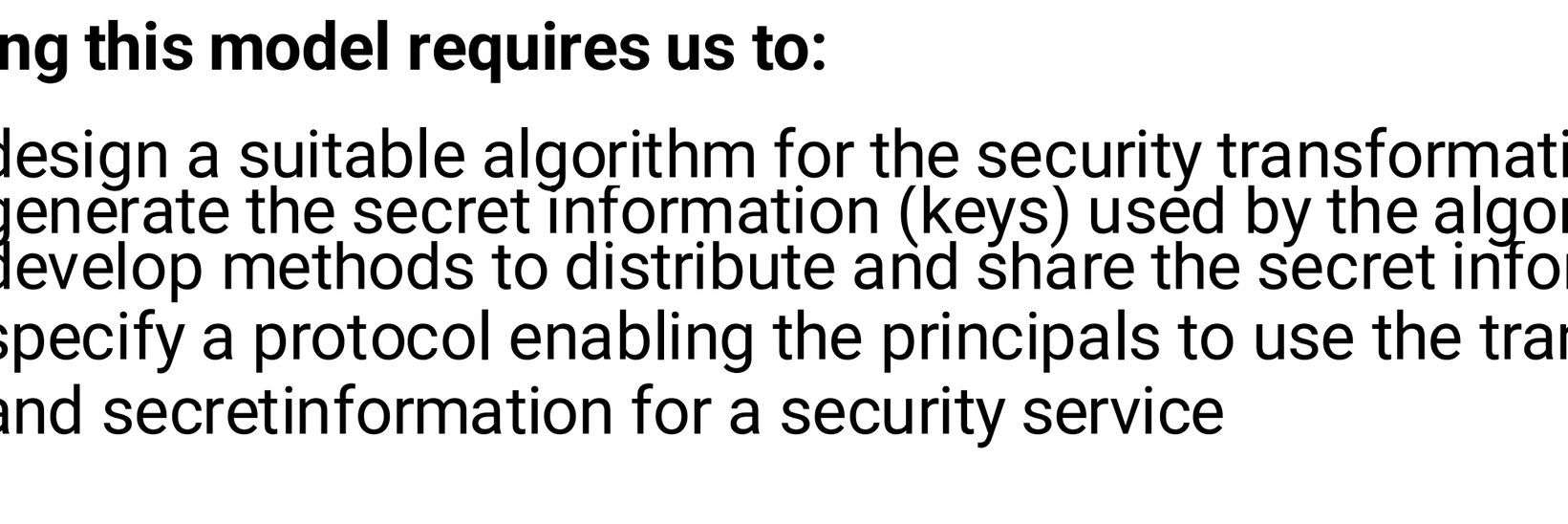


A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination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

Using this model requires us to:

- design a suitable algorithm for the security transformation
- generate the secret information (keys) used by the algorithm
- develop methods to distribute and share the secret information
- specify a protocol enabling the principals to use the transformation and secretinformation for a security service

MODEL FOR NETWORK ACCESS SECURITY



Using this model requires us to:

- select appropriate gatekeeper functions to identify users
- implement security controls to ensure only authorized users access designated information orresources
- Trusted computer systems can be used to implement this model

Key Points

*
*
*
*
*
*
*
*

Classical Encryption Techniques

- **Symmetric encryption** is a form of cryptosystem in which encryption and decryptionare performed using the same key. It is also known as conventional encryption.

- Symmetric encryption transforms plaintext into ciphertext using a secret key and anencryption algorithm. Using the same key and a decryption algorithm, the plaintext
is recovered from the ciphertext.

- The two types of attack on an encryption algorithm are cryptanalysis, based on properties of the encryption algorithm, and brute-force, which involves trying allpossible keys.
- Traditional (precomputer) symmetric ciphers use substitution and/or transposition
techniques. Substitution techniques map plaintext elements (characters, bits) intociphertext elements. Transposition techniques systematically transpose the positions of plaintext elements.

- Rotor machines are sophisticated precomputer hardware devices that usesubstitution techniques.

- Steganography is a technique for hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message.

Before beginning, we define some terms:

1. An original message is known as the **plaintext**.
2. The coded message is called the **ciphertext**.
3. The process of converting from plaintext to ciphertext is known as **enciphering** or **encryption**;
4. Restoring the plaintext from the ciphertext is **deciphering** or **decryption**.
5. 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

6. Techniques used for deciphering a message without any knowledge of the encipheringdetails fall into the area of **cryptanalysis**.

7. Cryptanalysis is what the layperson calls "breaking the code. " The areas ofcryptography
8. and cryptanalysis together are called **cryptology**.
9. **Brute-force attack:** The attacker tries every possible key on a piece of ciphertext untilan intelligible translation into plaintext is obtained. On average, half of all possible keysmust be tried to achieve success

Symmetric Cipher Model

A symmetric encryption scheme has five ingredients

- **Plaintext:** This is the original intelligible message or data that is fed into the algorithm asinput.
- **Encryption algorithm:** The encryption algorithm performs various substitutions andtransformations on the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm. The key is a value

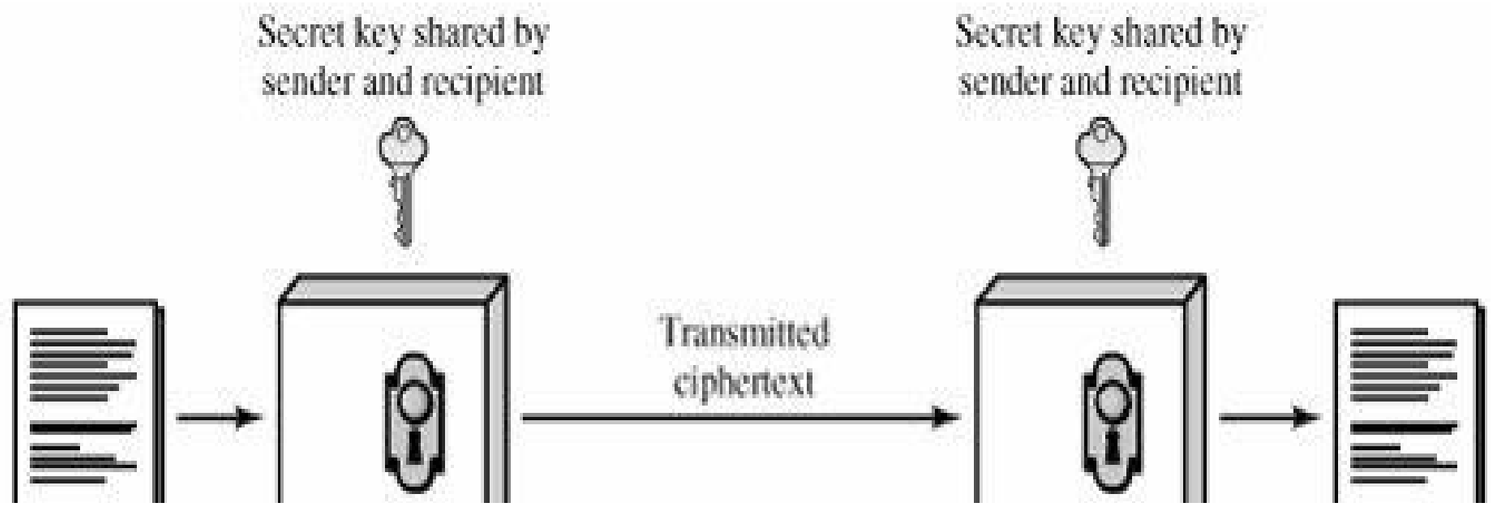
independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions andtransformations performed by the algorithm depend on the key.

- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintextand the secret key. For a given message, two different keys will produce two different ciphertexts.

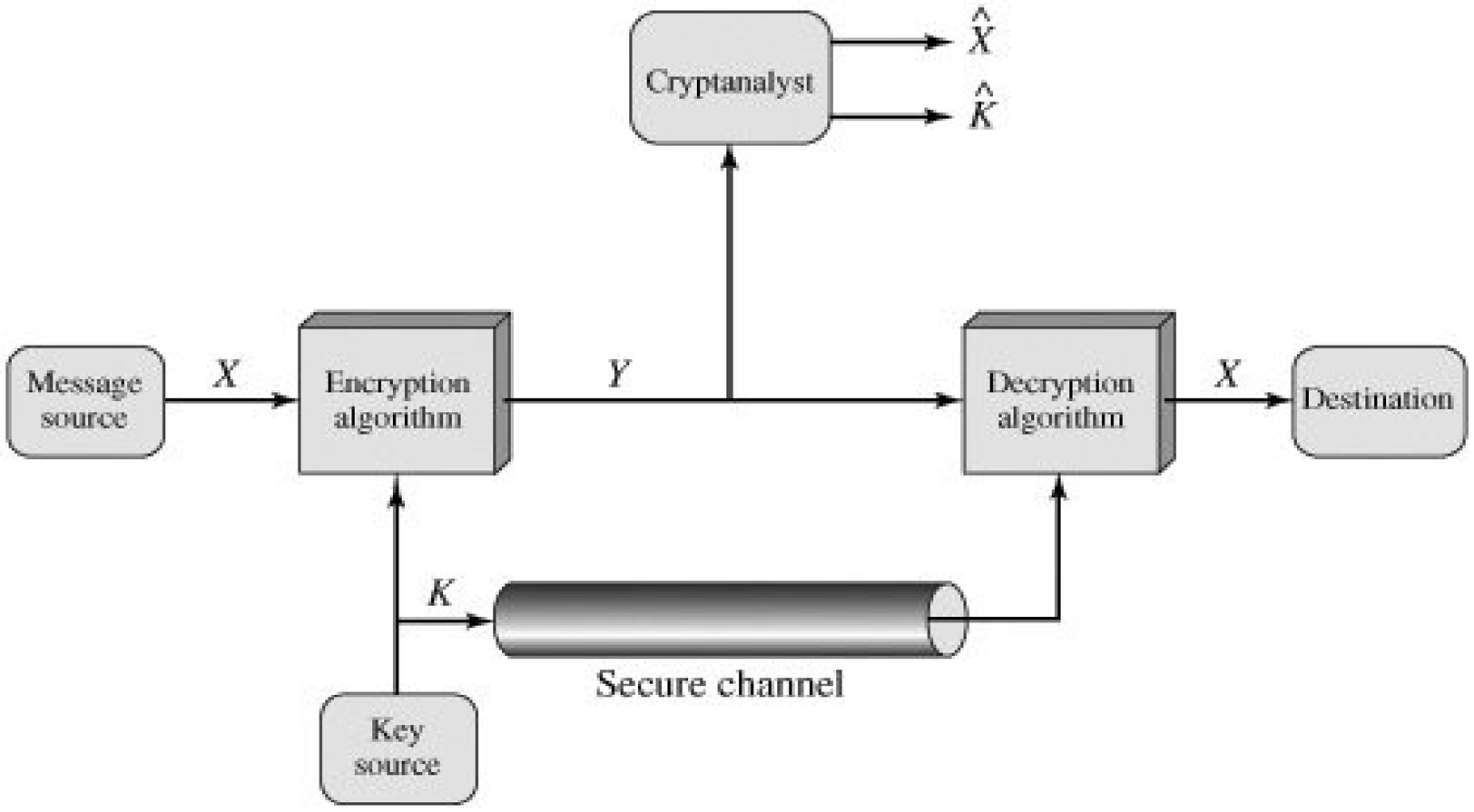
The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takesthe ciphertext and the secret key and produces the original plaintext.

Simplified Model of Conventional Encryption



Model of Conventional Cryptosystem



With the message *X* and the encryption key *K* as input, the encryption algorithm forms thecipher text *Y*
= [*Y*1, *Y*2, ..., *YN*]. We can write this as

$$Y = E(K, X)$$

The intended receiver, in possession of the key, is able to invert the transformation

$$X = D(K, Y)$$

Substitution & transposition Techniques

All encryption algorithms are based on two general principles **substitution**, **transposition**.

Substitution in which each element in the plaintext (bit, letter, group of bits or letters) ismapped into another element.

Substitution in which elements in the plaintext are rearranged. requirement is that noinformation be lost (that is, that all operations are reversible).

product systems involve multiple stages of substitutions and transpositions.

Substitution

1. Caesar Cipher

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

For example,

plain: meet me after the toga
partycipher: PHHW PH DIWHU
WKH WRJD SDUWB

Note that the alphabet is wrapped around, so that the letter following Z is A. We candefine thetransformation by listing all possibilities, as follows:

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

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

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

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

Disadvantage:

If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed: Simply try all the 25 possible keys.

2. 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 ciphertext digrams.

The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using akeyword

In this case, the keyword is ***monarchy***. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainderof the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter.

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

Plaintext is encrypted two letters at a time, according to thefollowing rules:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that **balloon** would be treated as **ba lx lo on**.

2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, **ar** is encrypted as **RM**.

3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, **mu** is encryptedas **CM**.

4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, **hs** becomes **BP** and **ea** becomes**IM** (or **JM**, as the encipherer wishes).

Advantage:

The Playfair cipher is a great advance over simple monoalphabetic ciphers. For one thing, whereas there are only 26 letters, there are 26 x 26 = 676 digrams, so that identification ofindividual digrams is more difficult.

DisAdvantage:

the Playfair cipher is relatively easy to break because it still leaves much of the structure ofthe plaintext language intact. A few hundred letters of ciphertext are generally sufficient.

3. Hill Cipher

Another interesting multiletter cipher is the Hill cipher, developed by the mathematician Lester Hill in 1929. The encryption algorithm takes *m* successive plaintext letters and substitutes for them *m* ciphertext letters. The substitution is determined by *m* linear equations in which each character is assigned a numericalvalue (a = 0, b = 1 ... z = 25). For *m* = 3, the system can be described as follows

$$c_1 = (k_{11}P1 + k_{12}P2 + k_{13}P3) \bmod 26\ c_2 = (k_{21}P1 + k_{22}P2 + k_{23}P3) \bmod 26 c_3 = (k_{31}P1 + k_{32}P2 + k_{33}P3) \bmod 26$$

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \bmod 26$$

This can be expressed in term of column vectors and matrices:

$$\mathbf{C} = E(\mathbf{K}, \mathbf{P}) = \mathbf{KP} \bmod 26$$
$$\mathbf{P} = D(\mathbf{K}, \mathbf{P}) = \mathbf{K}_1\mathbf{C} \bmod 26 = \mathbf{K}_1\mathbf{KP} = \mathbf{P}$$

where **C** and **P** are column vectors of length 3, representing the plaintext and ciphertext, and
K is a 3 x 3 matrix, representing the encryption key. Operations are

performed mod 26.For example, consider the plaintext

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

"**paymoremoney**" and use the encryption key

The first three letters of the plaintext are represented by the vector

$$\begin{pmatrix}15\\0\\24\end{pmatrix}. \text{Then } \mathbf{K}\begin{pmatrix}15\\0\\24\end{pmatrix} = \begin{pmatrix}375\\819\\486\end{pmatrix} \bmod 26 = \begin{pmatrix}11\\13\\18\end{pmatrix} = \text{LNS. Continuing in this fashion,}$$

The ciphertext for the entire plaintext is LNSHDLEWMTRW

Decryption requires using the inverse of the matrix **K**. The inverse **K**1 of a matrix **K** is defined by the equation **KK**1 = **K**1**K** = **I**, where **I** is the matrix that is all zeros except for onesalong the main diagonal from upper left to lower right. The inverse of a matrix does not always exist, but when it does, it satisfies the preceding equation. In this case, the inverse is:

$$\mathbf{K}^{-1} = \begin{pmatrix}4 & 9 & 15\\15 & 17 & 6\\24 & 0 & 17\end{pmatrix}$$

This is demonstrated as follows:

$$\begin{pmatrix}17 & 17 & 5\\21 & 18 & 21\\2 & 2 & 19\end{pmatrix}\begin{pmatrix}4 & 9 & 15\\15 & 17 & 6\\24 & 0 & 17\end{pmatrix} = \begin{pmatrix}443 & 442 & 442\\858 & 495 & 780\\494 & 52 & 365\end{pmatrix} \bmod 26 = \begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix}$$

Polyalphabetic Ciphers.

Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is polyalphabetic cipher. All the techniques have the followingfeatures in common. A set of related monoalphabetic substitution rules are used A key determines which particular rule is chosen for a given transformation.

Vigenere cipher In this scheme, the set of related monoalphabetic substitution rules consisting of 26 caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter. e.g., Caesar cipher with a shift of

3 is denoted by the key value 'd‟ (since a=0, b=1, c=2 and so on). To aid in understanding the scheme, a matrix known as vigenere tableau is Constructed 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

	PLAIN TEXT															
K		a	b	c	d	e	f	g	h	i	j	k	…	x	y	z
E	a	A	B	C	D	E	F	G	H	I	J	K	…	X	Y	Z
Y	b	B	C	D	E	F	G	H	I	J	K	L	…	Y	Z	A
	c	C	D	E	F	G	H	I	J	K	L	M	…	Z	A	B
L	d	D	E	F	G	H	I	J	K	L	M	N	…	A	B	C
E	e	E	F	G	H	I	J	K	L	M	N	O	…	B	C	D
T	f	F	G	H	I	J	K	L	M	N	O	P	…	C	D	E
T	g	G	H	I	J	K	L	M	N	O	P	Q	…	D	E	F
E R	: :	: :	: :	: :	: :	: :	: :	: :	: :	: :	: :	: :	…	: :	: :	: :
S	x	X	Y	Z	A	B	C	D	E	F	G	H	…			W
	y	Y	Z	A	B	C	D	E	F	G	H	I	…			X
	z	Z	A	B	C	D	E	F	G	H	I	J	…			Y

Encryption is simple: Given a key letter X and a plaintext letter y, the cipher text is at theintersection of the row labeled x and the column labeled y; in this case, the ciphertext is V.

To encrypt a message, a key is needed that is as long as the message. Usually, the key is arepeating keyword.
e.g.,
key = d e c e p t i v e d e c e p t i v e d e c e
p t i v ePT = w e a r e d i s c o v e r e d s av
e y o u r s e l f 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 ofthat column.

Strength of Vigenere cipher

- There are multiple cipher text letters for each plaintext letter.
- Letter frequency information is obscured.

Gilbert Vernam Cipher: 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**. His system works on

$$c_i = p_i \oplus k_i$$

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

binary data rather than letters. The systemcan be expressed succinctly as follows:

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

$$p_i = c_i \oplus k_i$$

One-Time Pad

Each new message requires a new key of the same length as the new message.Such a scheme, known as a **one-time pad**, is unbreakable.

It produces random output that bears no statistical relationship to the plaintext. Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way tobreak the code.

We now show two different decryptions using two different keys:

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key: *pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih*
plaintext: mr mustard with the candlestick in the hall

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key: *mtugpmiydgaxgouthkllmhsqddqogtewbqfgyovuhwt*
plaintext: miss scarlet with the knife in the library

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.

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

```
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
```

The transposition cipher can be made significantly more secure by performing more than one
stage of transposition. The result is a more complex permutation that is not easilyreconstructed. Thus, if the foregoing message is reencrypted using the same algorithm

** ********** *

Steganography

steganography conceal the existence of the message, whereas the methods of cryptographyrender the message unintelligible to outsiders by various transformations of the text Various other techniques have been used historically; some examples are the following

- **Character marking:** Selected letters of printed or typewritten text are overwritten inpencil. 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 visibletrace 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, theresults of typing with the correction tape are visible only under a strong light

Key Points

- A **block cipher** is an encryption/decryption scheme in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
- Many block ciphers have a Feistel structure. Such a structure consists of a number of identical rounds of processing. In each round, a substitution is performed on one half of the data being processed, followed by a permutation that interchanges the two halves. The original key is expanded so that a different key is used for each round.
- The Data Encryption Standard (DES) has been the most widely used encryption algorithm until recently. It exhibits the classic Feistel structure. DES uses a 64-bit block and a 56-bit key.
- Two important methods of cryptanalysis are differential cryptanalysis and linear cryptanalysis. DES has been shown to be highly resistant to these two types of attack.

A **stream cipher** is one that encrypts a digital data stream one bit or one byte at a time.Examples of classical stream ciphers are the autokeyed Vigenère cipher and the Vernam cipher.
A **block cipher** is one in which a block of plaintext is treated as a whole and used to producea ciphertext block of equal length. Typically, a block size of 64 or 128 bits is used

Diffusion, the statistical structure of the plaintext is dissipated into long-range statistics ofthe ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits; generally this is equivalent to having each ciphertext digit be affected
by many plaintext digits

Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover thekey.

BLOCK CIPHER PRINCIPLES

Virtually, all symmetric block encryption algorithms in current use are based on a structure referred to as Fiestel block cipher. For that reason, it is important to examine the design principles of the Fiestel cipher. We begin with a comparison of stream cipher with block cipher.

- A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. E.g, vigenere cipher.
- A block cipher is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length. Typically a block size of 64 or 128 bitsis used.

Block cipher principles

most symmetric block ciphers are based on a Feistel Cipher Structure needed since must be able to decrypt ciphertext to recover messages efficiently. block ciphers look like an extremely large substitution

- would need table of 264 entries for a 64-bit block • Instead create from smaller building blocks
- using idea of a product cipher in 1949 Claude Shannon introduced idea of substitution- permutation (S-P) networks called modern substitution-transposition product cipher these form the basis of modern block ciphers
- S-P networks are based on the two primitive cryptographic operations we have seen before:
  - *substitution* (S-box)
  - *permutation* (P-box)

- provide *confusion* and *diffusion* of message
- diffusion – dissipates statistical structure of plaintext over bulk of ciphertext
- confusion – makes relationship between ciphertext and key as complex as possible

The Feistel Cipher

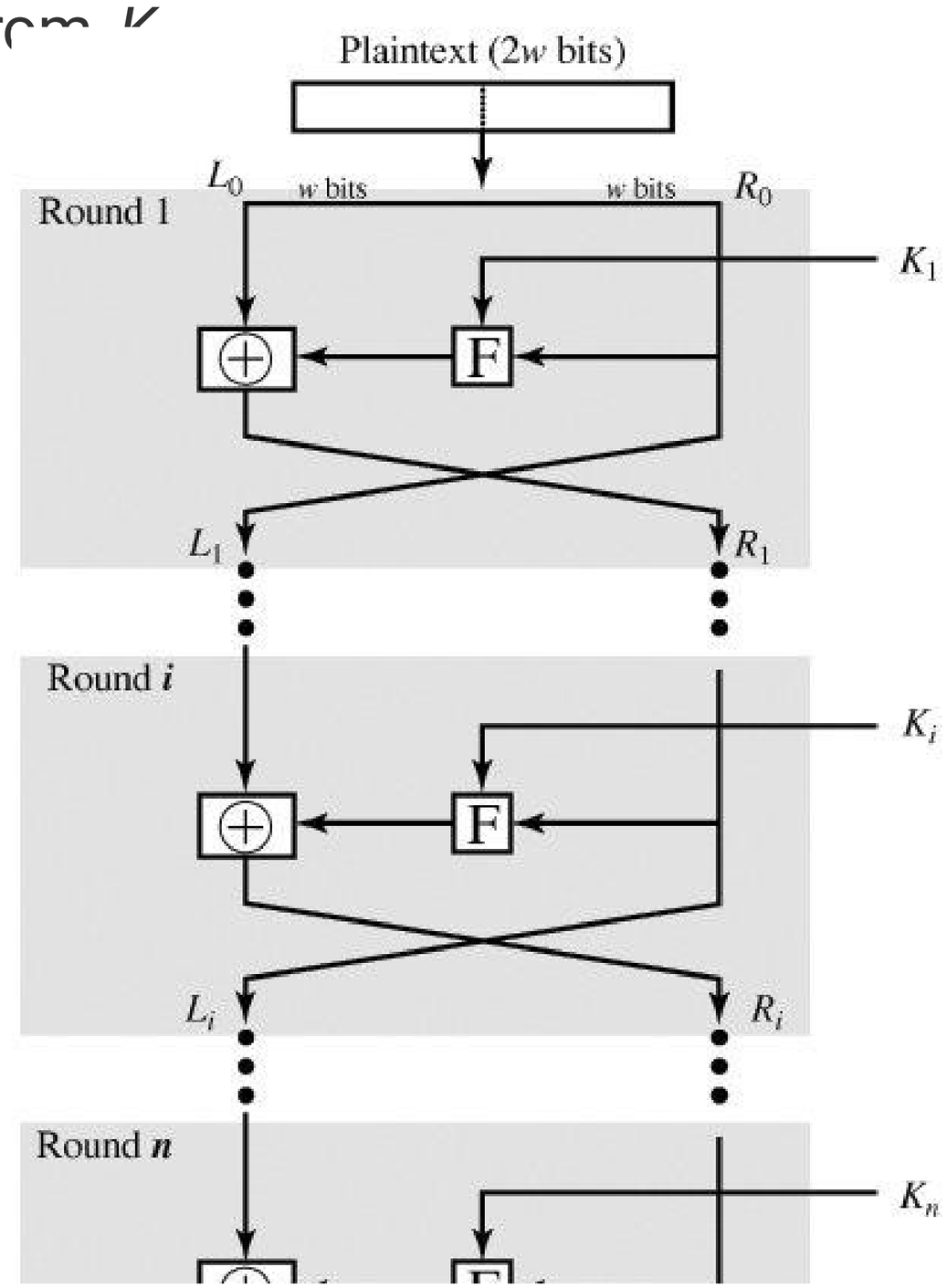
Feistel proposed [FEIS73] that we can approximate the ideal block cipher by utilizing the concept of a product cipher, which is the execution of two or more simple ciphers in sequencein such a way that the final result or product is cryptographically stronger than any of the component ciphers

Feistel Cipher Structure

- The inputs to the encryption algorithm are a plaintext block of length 2*w* bits and a key *K*.
- The plaintext block is divided into two halves, *L*0 and *R*0. T
- he two halves of the data pass through *n* rounds of processing and then combine toproduce the ciphertext block.
- Each round *i* has as inputs *Li-1* and *Ri-1*, derived from the previous round, as well as asubkey *Ki*, derived from the overall *K*.
- In general, the subkeys *Ki* are different from *K* and from each other.

<u>Description</u>:

- All rounds have the same structure.
- A **substitution** is performed on the left half ofthe data.
- This is done by applying a *round function* F to the right half of the data and then taking the exclusive-OR of the output of that function andthe left half of the data.



- The round function has the same general structure for each round but is parameterizedby the round subkey *Ki*.
- Following this substitution, a **permutation** is performed that consists of the interchange of the two halves of the data

The exact realization of a Feistel network depends on the choice of the following **parameters**
and design features:

- **Block size:** Larger block sizes mean greater security (all other things being equal) but reduced encryption/decryption speed for a given algorithm. The greater security is achievedby greater diffusion Traditionally, a block size of 64 bits has been considered a reasonable tradeoff and was nearly universal in block cipher design.

- **Key size:** Larger key size means greater security but may decrease encryption/decryptionspeed. The greater security is achieved by greater resistance to brute-force attacks and greater confusion. Key sizes of 64 bits or less are now widely considered to be inadequate, and 128 bits has become a common size.

- **Number of rounds:** The essence of the Feistel cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. A typical size is 16rounds.

The Data Encryption Standard

The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977 by the National Bureau of Standards, now the National Institute of Standardsand Technology (NIST).
The algorithm itself is referred to as the Data Encryption Algorithm (DEA).

.

DES Encryption

DES, data are encrypted in 64-bit blocks using a 56-bit key. The algorithm

transforms 64-bitinput in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption

1. Looking at the **left-hand side** of the figure, we can see that the processing of the plaintext proceeds in three phases.

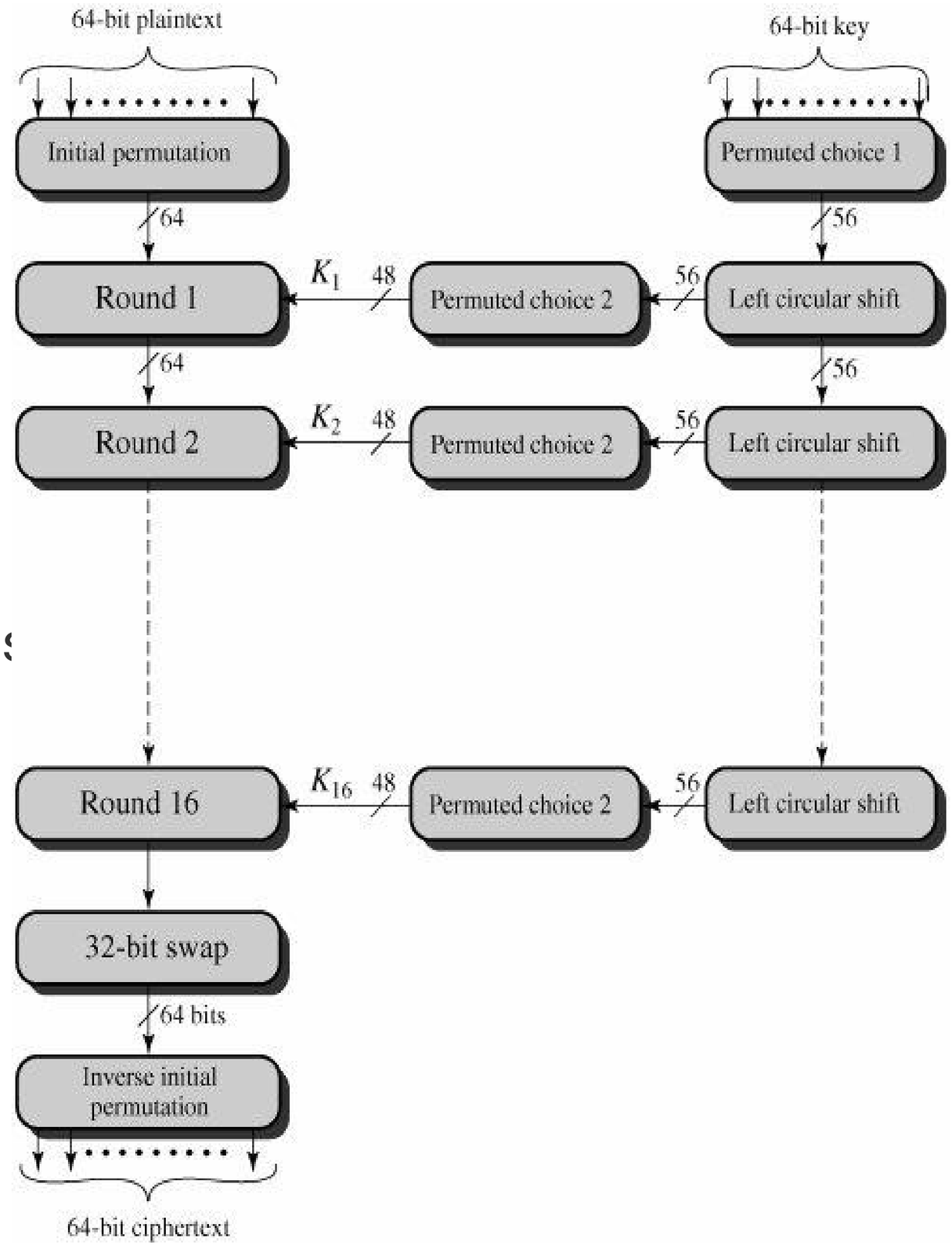
2. First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the*permuted input*.

3. This is followed by a phase consi 16 rounds of the same function, which involves both permutation and substitution functions.

4. The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key.

5. The left and right halves of the output are swapped to produce the **preoutput**.

6. Finally, the preoutput is passed through a permutation (IP-1) that is the inverse of the initial permutation function, to produce the 64-bit ciphertext.



1. **The right-hand** portion of Figure 3.4 shows the way in which the 56-bit key isused. Initially, the key is passed through a permutation function.

2. Then, for each of the 16 rounds, a *subkey* (*Ki*) is produced by
3. the combination of a left circular shift and a permutation.

4. The permutation function is the same for each round, but a different subkey isproduced because of the repeated shifts of the key bits.

Initial Permutation

permutation table contain a permutation of the numbers from 1 to 64. Each entry in the permutation table indicates the position of a numbered input bit in the output, which alsoconsists of 64 bits.
To see that these two permutation functions are indeed the inverse of each other, considerthe following 64-bit input *M*:

M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}
M_{17}	M_{18}	M_{19}	M_{20}	M_{21}	M_{22}	M_{23}	M_{24}
M_{25}	M_{26}	M_{27}	M_{28}	M_{29}	M_{30}	M_{31}	M_{32}
M_{33}	M_{34}	M_{35}	M_{36}	M_{37}	M_{38}	M_{39}	M_{40}
M_{41}	M_{42}	M_{43}	M_{44}	M_{45}	M_{46}	M_{47}	M_{48}
M_{49}	M_{50}	M_{51}	M_{52}	M_{53}	M_{54}	M_{55}	M_{56}
M_{57}	M_{58}	M_{59}	M_{60}	M_{61}	M_{62}	M_{63}	M_{64}

M_{58}	M_{50}	M_{42}	M_{34}	M_{26}	M_{18}	M_{10}	M_2
M_{60}	M_{52}	M_{44}	M_{36}	M_{28}	M_{20}	M_{12}	M_4
M_{62}	M_{54}	M_{46}	M_{38}	M_{30}	M_{22}	M_{14}	M_6
M_{64}	M_{56}	M_{48}	M_{40}	M_{32}	M_{24}	M_{16}	M_8
M_{57}	M_{49}	M_{41}	M_{33}	M_{25}	M_{17}	M_9	M_1
M_{59}	M_{51}	M_{43}	M_{35}	M_{27}	M_{19}	M_{11}	M_3
M_{61}	M_{53}	M_{45}	M_{37}	M_{29}	M_{21}	M_{13}	M_5
M_{63}	M_{55}	M_{47}	M_{39}	M_{31}	M_{23}	M_{15}	M_7

If we then take the inverse permutation ***Y* = IP-1(*X*) = IP-1(IP(*M*))**, it can be seen that theoriginal ordering of the bits is restored

Details of Single Round

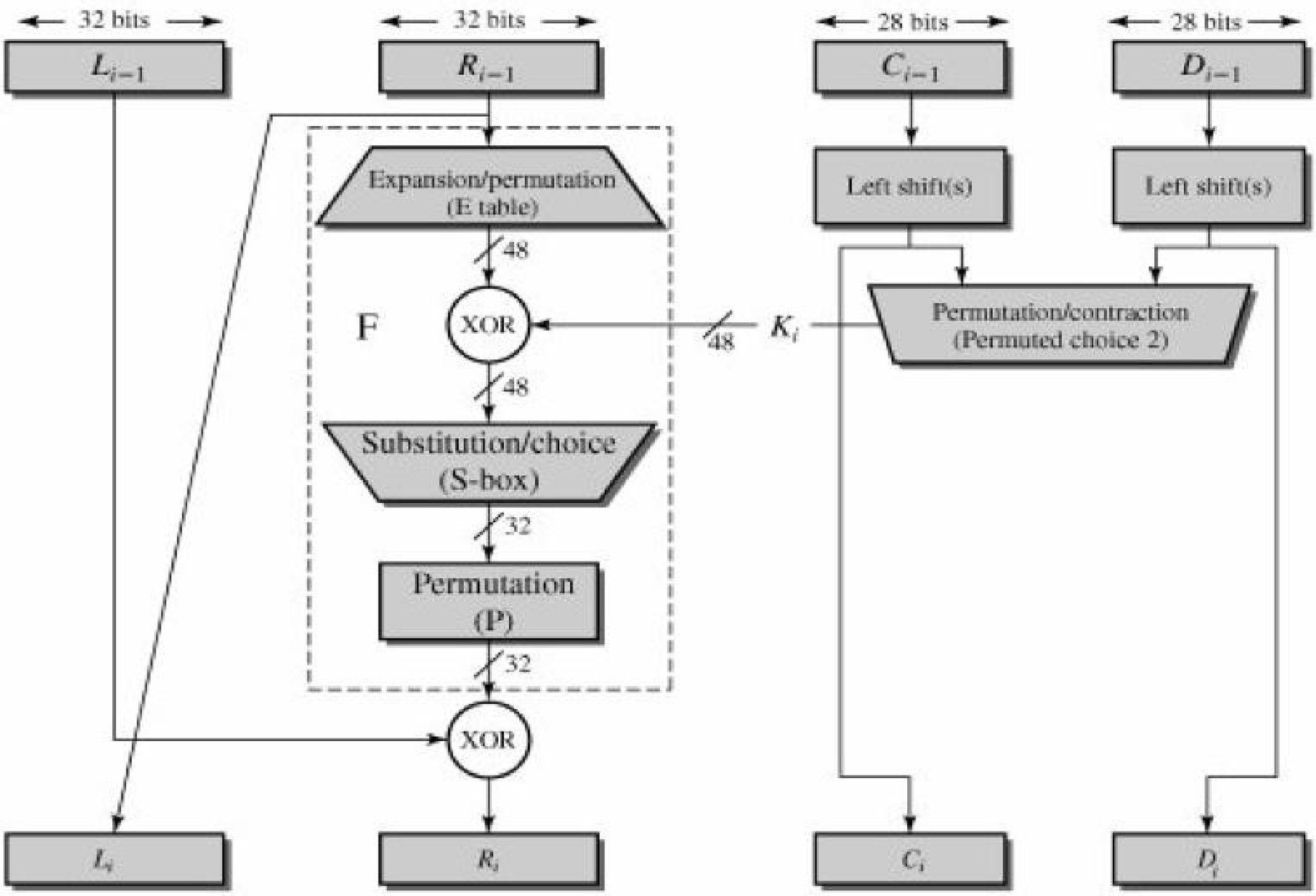
1. Figure 3.5 shows the internal structure of a single round.
2. Again, begin by focusing on the **left-hand side** of the diagram.

3. The left and right halves of each 64-bit intermediate value are treated as separate 32-bit quantities, labeled L (left) and R (right).

4. As in any classic Feistel cipher, the overall processing at each round can besummarized in the following formulas

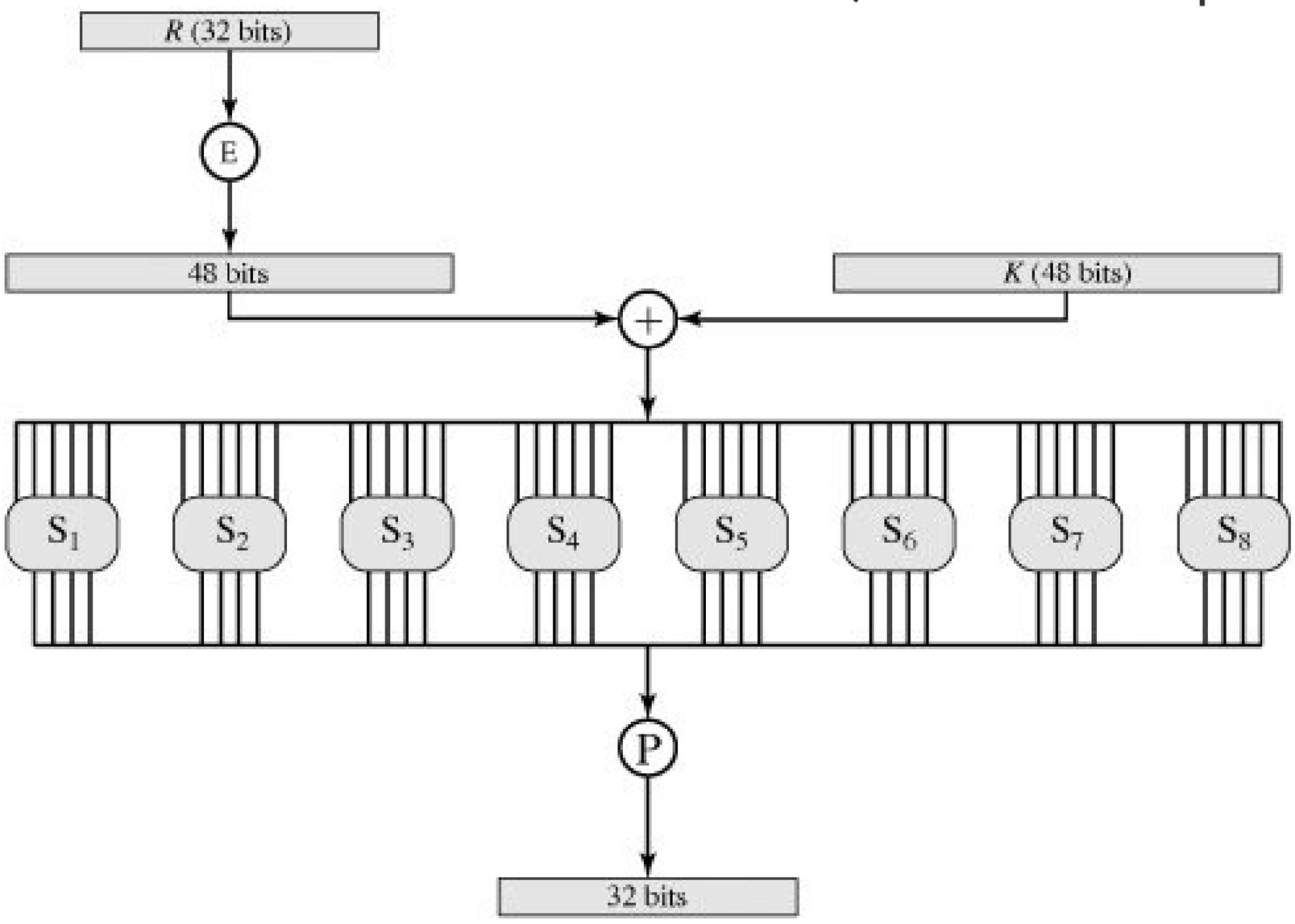
$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \times F(R_{i-1}, K_i)$$

5. The round key *Ki* is 48 bits
6. The *R* input is 32 bits.
7. This *R* input is first expanded to 48 bits by using a table that defines a permutationplus an expansion that involves duplication of 16 of the *R* bits .
8. The resulting 48 bits are XORed with *Ki*.



This 48-bit result passes through a substitution function that produces a 32-bit output.

9. The role of the S-boxes in the function F is illustrated in Figure 3.6.
10. The substitution consists of a set of eight S-boxes, each of which accepts 6 bits asinput and produces 4 bits as output. These transformations are defined, which is interpreted as follows:



1. The first and last bits of the input to box S*i* form a 2-bit binary number to select one offour substitutions defined by the four rows in the table for S*i*.
2. The middle four bits select one of the sixteen columns.
3. The decimal value in the cell selected by the row and column is then converted to its 4-bit representation to produce the output. For example, in S1 for input 011001, the row is 01 (row 1) and the column is 1100 (column 12). The value in row 1, column 12 is 9, so the output is 1001.

****

Advanced Encryption Standard (AES).

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against

exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

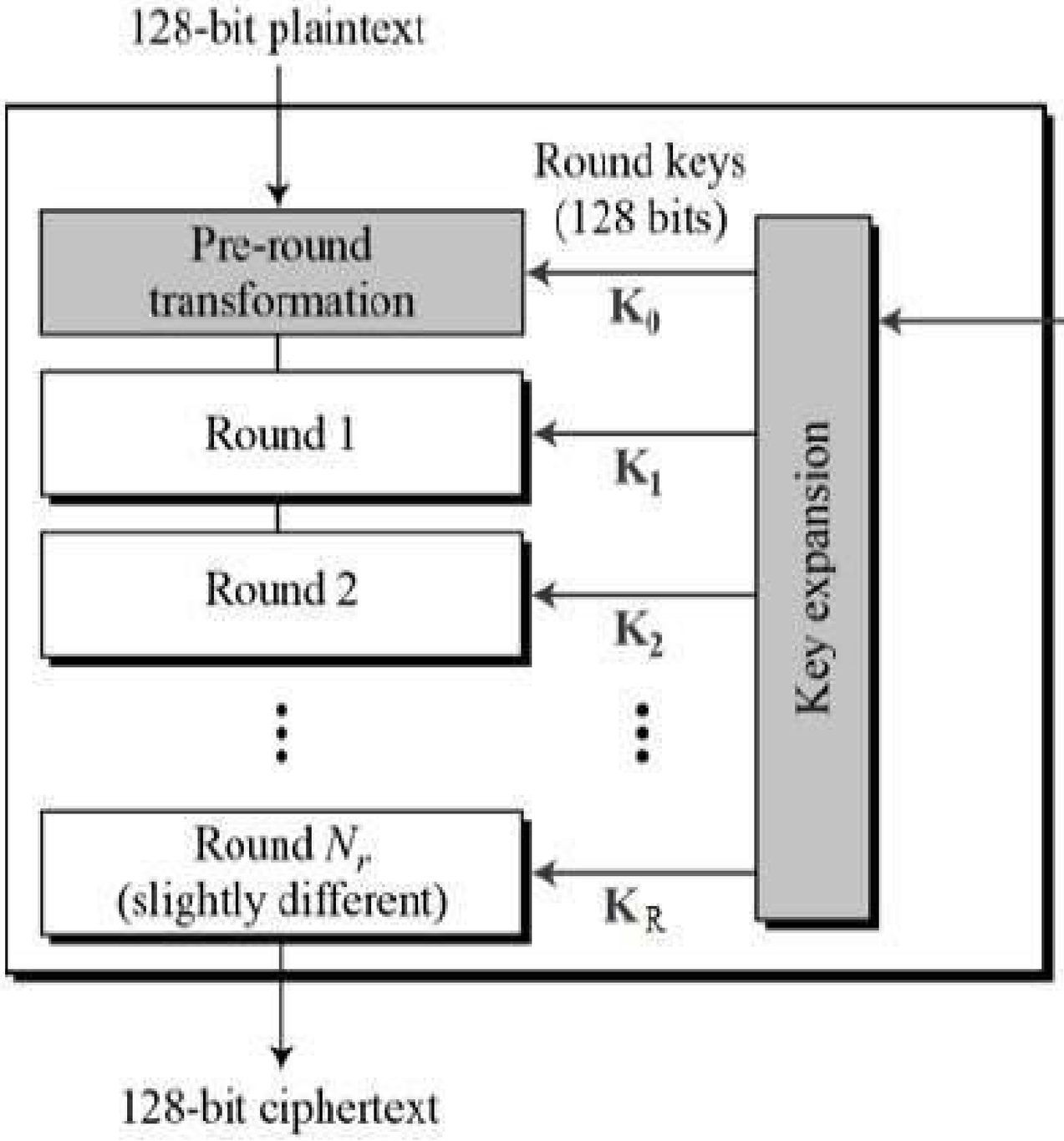
Operation of AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration −

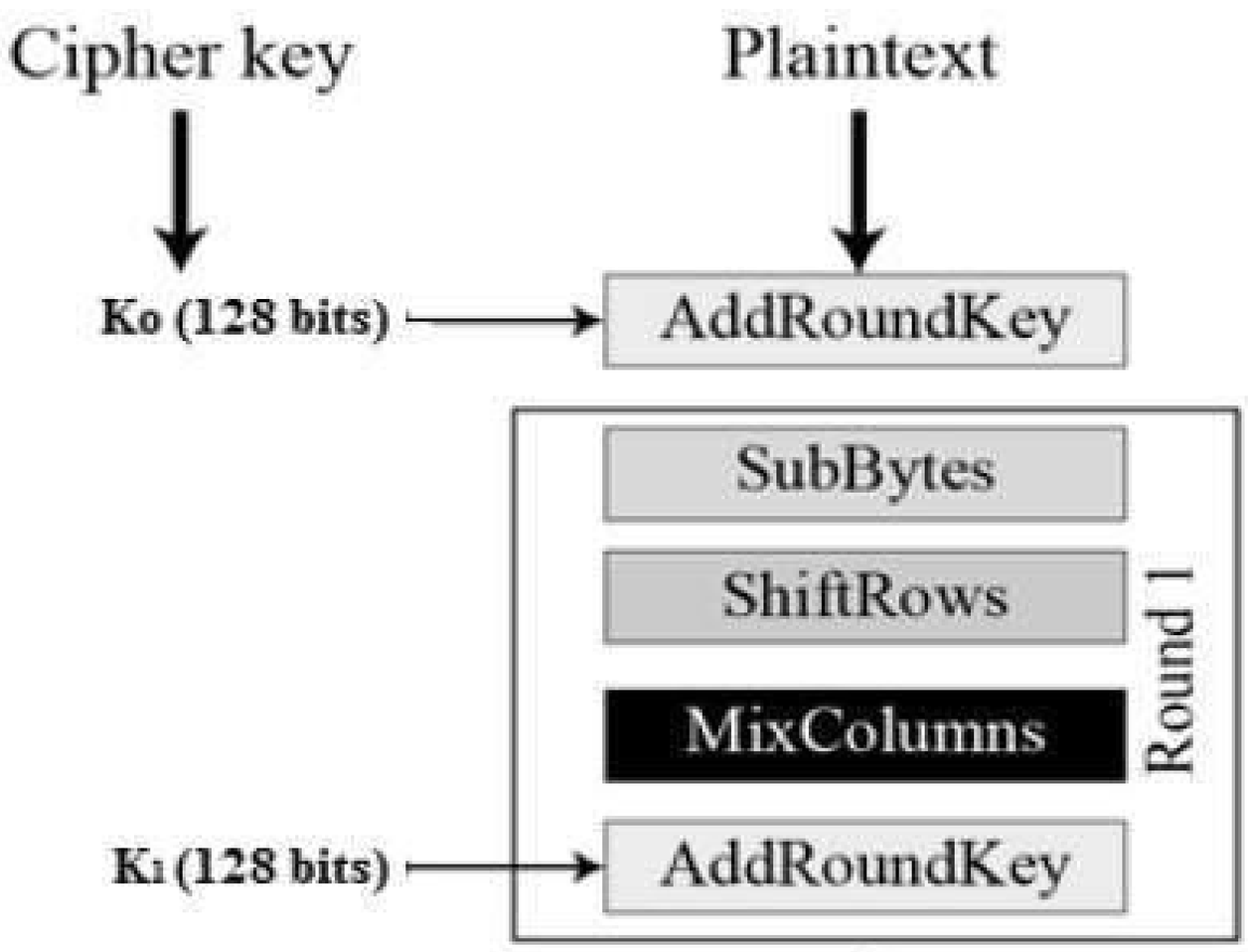


R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each



roundcomprise of four sub-processes. The first round process is depicted below

–

Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given

indesign. The result is in a matrix of four rows and four columns.

Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respectto each other.

MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented,although they are very closely related.

AES Analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of ‘future-proofing’ against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.