**COMPUTER SECURITY**

**MODULE I**

**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. The simplest such cipher is the **rail fence** technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

For example, to encipher the message

“meet me after the toga party” with a rail fence of depth 2, we write the following:

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

e t e f e t e o a a t

The encrypted message is

MEMATRHTGPRYETEFETEOAAT

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 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

Pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. 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 easily reconstructed. Thus, if the foregoing message is reencrypted using the same algorithm,

Key: 4 3 1 2 5 6 7

Input: t t n a a p t

m t s u o a o

d w c o i x k

n l y p e t z

Output:NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

To visualize the result of this double transposition, designate the letters in the original plaintext message by the numbers designating their position. Thus, with 28 letters in the message, the original sequence of letters is

01 02 03 04 05 06 07 08 09 10 11 12 13 14

15 16 17 18 19 20 21 22 23 24 25 26 27 28

After the first transposition, we have

03 10 17 24 04 11 18 25 02 09 16 23 01 08

15 22 05 12 19 26 06 13 20 27 07 14 21 28

which has a somewhat regular structure. But after the second transposition, we have

17 09 05 27 24 16 12 07 10 02 22 20 03 25

15 13 04 23 19 14 11 01 26 21 18 08 06 28

**ROTOR MACHINES**

The most important application of the principle of multiple stages of encryption was a class of systems known as rotor machines.The basic principle of the rotor machine is illustrated in Figure 1.7.



Fig.1.7

The machine consists of a set of independently rotating cylinders through which electrical pulses can flow. Each cylinder has 26 input pins and 26 output pins, with internal wiring that connects each input pin to a unique output pin. For simplicity, only three of the internal connections in each cylinder are shown.

If we associate each input and output pin with a letter of the alphabet, then a single cylinder defines a monoalphabetic substitution. For example, in Figure 1.7, if an operator depresses the key for the letter A, an electric signal is applied to the first pin of the first cylinder and flows through the internal connection to the twenty-fifth output pin.

The power of the rotor machine is in the use of multiple cylinders, in which the output pins of one cylinder are connected to the input pins of the next. The left half of the figure shows a position in which the input from the operator to the first pin (plaintext letter a) is routed through the three cylinders to appear at the output of the second pin (ciphertext letter B).

With multiple cylinders, the one closest to the operator input rotates one pin position with each keystroke.The right half of Figure 2.8 shows the system’s configuration after a single keystroke. For every complete rotation of the inner cylinder, the middle cylinder rotates one pin position. Finally, for every complete rotation of the middle cylinder, the outer cylinder rotates one pin position.

**STEGANOGRAPHY**

A plaintext message may be hidden in one of two ways. The methods of **steganography** conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.A simple form of steganography, but one that is time-consuming to construct,is one in which an arrangement of words or letters within an apparently innocuous text spells out the real 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.

Steganography has a number of drawbacks when compared to encryption. It requires a lot of overhead to hide a relatively few bits of information. The advantage of steganography is that it can be employed by parties who have something to lose should the fact of their secret communication (not necessarily the content) be discovered.

**BLOCK CIPHERS AND THE DATA ENCRYPTION STANDARD**

**Stream Ciphers and Block Ciphers**

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 produce a ciphertext block of equal length. Typically, a block size of 64 or 128 bits is used. As with a stream cipher, the two users share a symmetric encryption key. Many current ciphers are block ciphers.

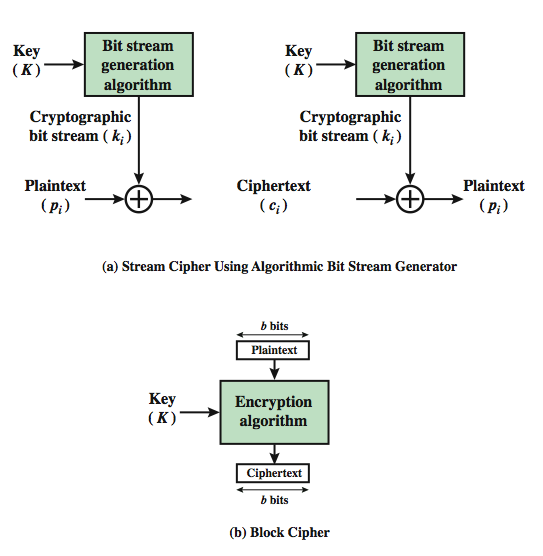


Fig 1.8

**BLOCK CIPHER PRINCIPLES**

Many symmetric block encryption algorithms in current use are based on a structure referred to as a Feistel block cipher.A block cipher operates on a plaintext block of n bits to produce a ciphertext block of n bits **.** There are2n possible different plaintext blocks and, for the encryption to be reversible (i.e., for decryption to be possible), each must produce a unique ciphertext block. Such a transformation is called reversible, or nonsingular.The following examples illustrate nonsingular and singular transformations for *n* = 2.

**Reversible Mapping Irreversible Mapping**

**Plaintext Ciphertext Plaintext Ciphertext**

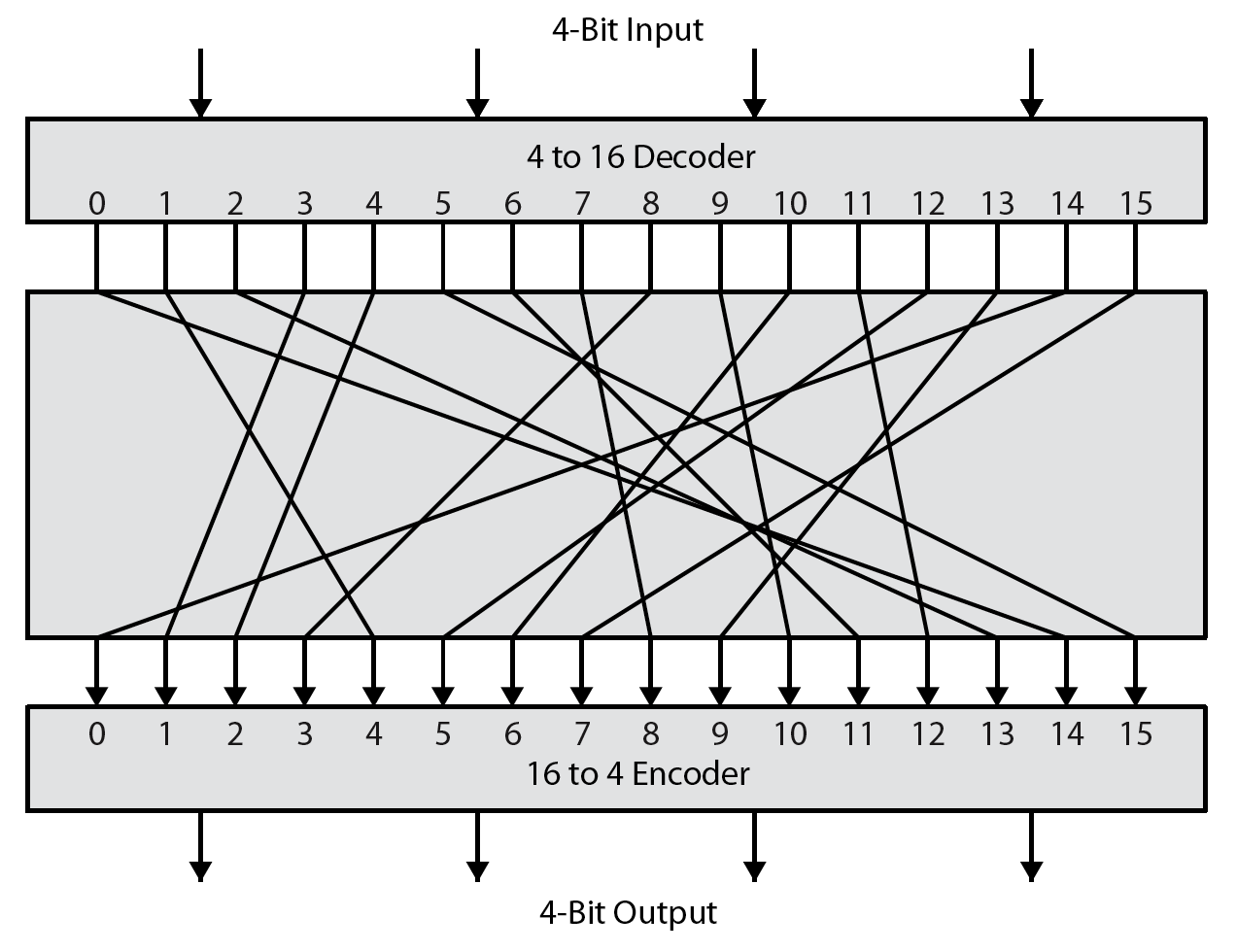
00 11 00 11

01 10 01 10

10 00 10 01

11 01 11 01

In the latter case, a ciphertext of 01 could have been produced by one of two plaintext blocks. So if we limit ourselves to reversible mappings, the number of different transformations is 2n!.



**Fig 1.9**

Figure 1.9 illustrates the logic of a general substitution cipher for n=4 .A 4-bit input produces one of 16 possible input states, which is mapped by the substitution cipher into a unique one of 16 possible output states, each of which is represented by 4 ciphertext bits This is the most general form of block cipher and can be used to define any reversible mapping between plaintext and ciphertext.Feistel refers to this as the *ideal block cipher*, because it allows for the maximum number of possible encryption mappings from the plaintext block.

Feistel proposed the use of a cipher that alternates substitutions and permutations, where these terms are defined as follows:

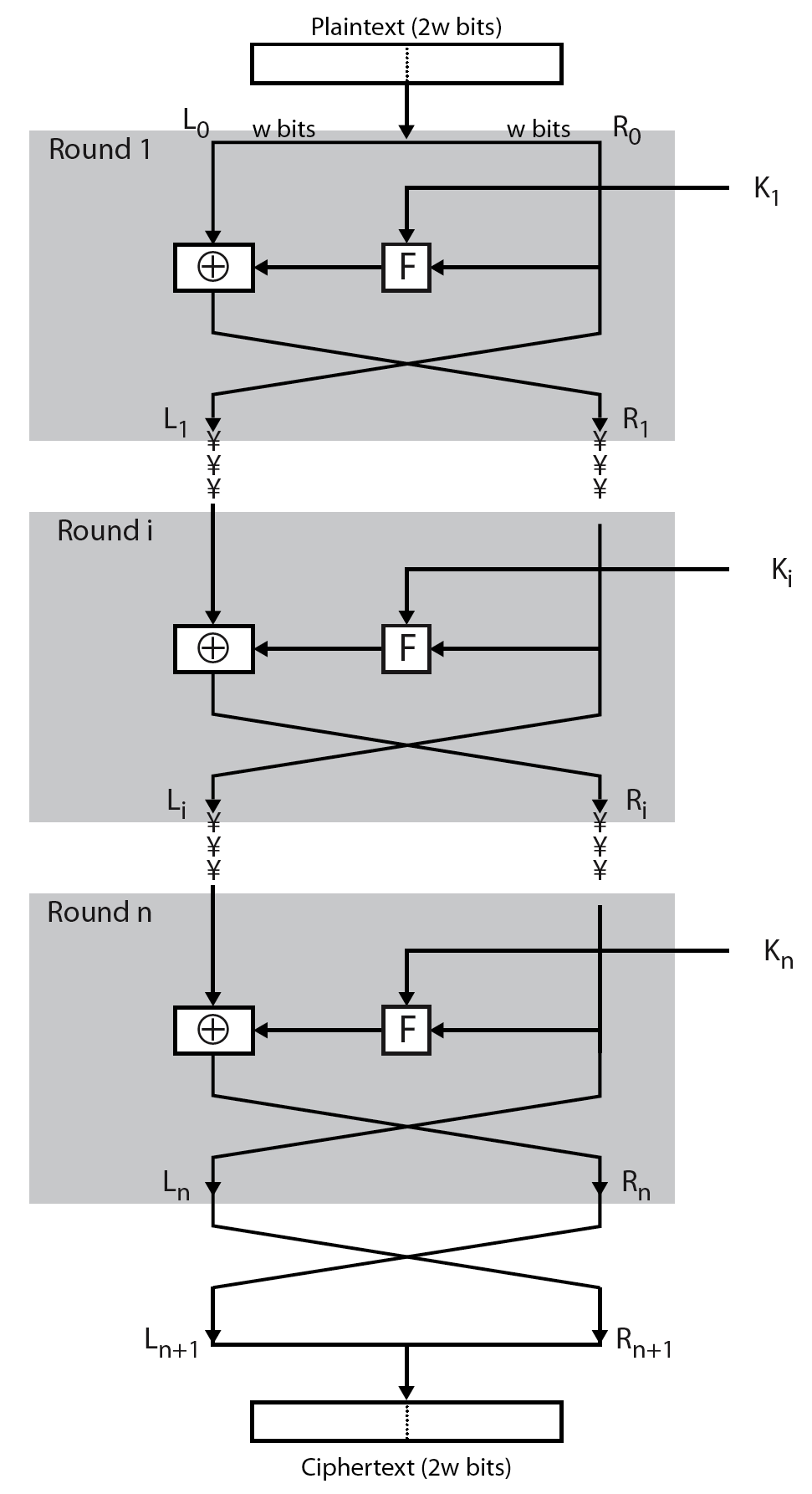
• **Substitution:** Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.

• **Permutation:** A sequence of plaintext elements is replaced by a permutation of that sequence. That is, no elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.

**Claude Shannon and Substitution-Permutation Ciphers**

* Claude Shannon introduced idea of substitution-permutation (S-P) networks in 1949
* form basis of modern block ciphers
* S-P nets are based on the two primitive cryptographic operations seen before:
  + substitution (S-box)
  + permutation (P-box)
* provide confusion & diffusion of message & key

**Fiestal cipher structure**

****

**Confusion and diffusion**

* + diffusion

dissipates statistical structure of plaintext over bulk of ciphertext i.e. each plaintext digits affects value of many ciphertext digits.It make the statistical relationship between the plaintext and ciphertext as complex as possible.

* confusion

make relation between statistics of ciphertext and the value of the encryption key as complex as possible