3-3 TRANSPOSITION CIPHERS

A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.

Note

A transposition cipher reorders symbols.

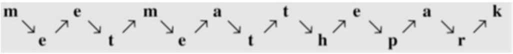
Topics discussed in this section:

3.3.1 Keyless Transposition Ciphers

Simple transposition ciphers, which were used in the past, are keyless.

Example 3.22

A good example of a keyless cipher using the first method is the rail fence cipher. The ciphertext is created reading the pattern row by row. For example, to send the message "Meet me at the park" to Bob, Alice writes



She then creates the ciphertext "MEMATEAKETETHPR".

3.3.1 Continued

Example 3.23

Alice and Bob can agree on the number of columns and use the second method. Alice writes the same plaintext, row by row, in a table of four columns.

m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

She then creates the ciphertext "MMTAEEHREAEKTTP".

3.3.1 Continued

Example 3.24

The cipher in Example 3.23 is actually a transposition cipher. The following shows the permutation of each character in the plaintext into the ciphertext based on the positions.

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
01	05	09	13	02	06	10	13	03	07	11	15	04	08	12

The second character in the plaintext has moved to the fifth position in the ciphertext; the third character has moved to the ninth position; and so on. Although the characters are permuted, there is a pattern in the permutation: (01, 05, 09, 13), (02, 06, 10, 13), (03, 07, 11, 15), and (08, 12). In each section, the difference between the two adjacent numbers is 4.

3.3.2 Keyed Transposition Ciphers

The keyless ciphers permute the characters by using writing plaintext in one way and reading it in another way The permutation is done on the whole plaintext to create the whole ciphertext. Another method is to divide the plaintext into groups of predetermined size, called blocks, and then use a key to permute the characters in each block separately.

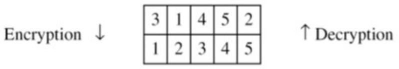
3.3.2 Continued

Example 3.25

Alice needs to send the message "Enemy attacks tonight" to Bob..

e n e m y a t t a c k s t o n i g h t z

The key used for encryption and decryption is a permutation key, which shows how the character are permuted.



The permutation yields

E E M Y N T A A C T T K O N S H I T Z G

3.3.3 Combining Two Approaches

Example 3.26

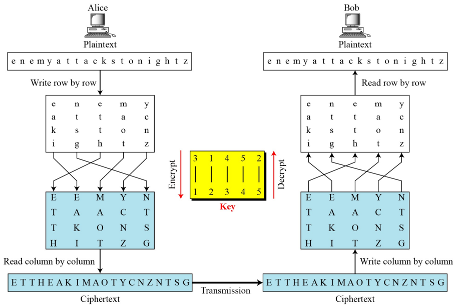


Figure 3.21

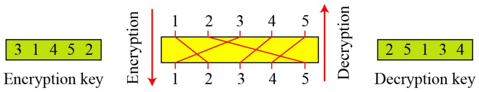
3.54

3.3.3 Continued

Keys

In Example 3.27, a single key was used in two directions for the column exchange: downward for encryption, upward for decryption. It is customary to create two keys.

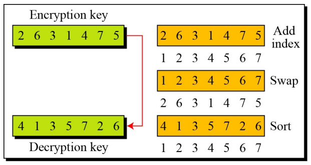
Figure 3.22 *Encryption/decryption keys in transpositional ciphers*



3.55

3.3.3 Continued

Figure 3.23 *Key inversion in a transposition cipher*



a. Manual process

```
Given: EncKey [index]
index ← 1
while (index ≤ Column)
  {
   DecKey[EncKey[index]] ← index
   index ← index + 1
  }
Return : DecKey [index]
```

b. Algorithm

3.56

3.3.3 Continued

Using Matrices

We can use matrices to show the encryption/decryption process for a transposition cipher.

Example 3.27

Figure 3.24 *Representation of the key as a matrix in the transposition cipher*

$$\underset{\text{Plaintext}}{\begin{bmatrix}04&13&04&12&24\\00&19&19&00&02\\10&18&19&14&13\\08&06&07&19&25\end{bmatrix}} \times \underset{\text{Encryption key}}{\begin{array}{c}\begin{matrix}3&1&4&5&2\\\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\end{matrix}\\\begin{bmatrix}0&1&0&0&0\\0&0&0&0&1\\1&0&0&0&0\\0&0&1&0&0\\0&0&0&1&0\end{bmatrix}\end{array}} = \underset{\text{Ciphertext}}{\begin{bmatrix}04&04&12&24&13\\19&00&00&02&19\\19&10&14&13&18\\07&08&19&25&06\end{bmatrix}}$$

3.57

3.3.3 Continued

Example 3.27

Figure 3.24 shows the encryption process. Multiplying the 4 × 5 plaintext matrix by the 5 × 5 encryption key gives the 4 × 5 ciphertext matrix.

Figure 3.24 *Representation of the key as a matrix in the transposition cipher*

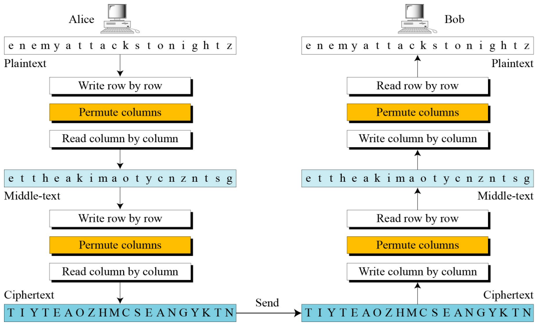
$$\underset{\text{Plaintext}}{\begin{bmatrix}04&13&04&12&24\\00&19&19&00&02\\10&18&19&14&13\\08&06&07&19&25\end{bmatrix}} \times \underset{\text{Encryption key}}{\begin{array}{c}\begin{matrix}3&1&4&5&2\\\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\end{matrix}\\\begin{bmatrix}0&1&0&0&0\\0&0&0&0&1\\1&0&0&0&0\\0&0&1&0&0\\0&0&0&1&0\end{bmatrix}\end{array}} = \underset{\text{Ciphertext}}{\begin{bmatrix}04&04&12&24&13\\19&00&00&02&19\\19&10&14&13&18\\07&08&19&25&06\end{bmatrix}}$$

3.58

3.3.3 Continued

Double Transposition Ciphers

Figure 3.25 *Double transposition cipher*



3.59