Classical Ciphers - Transposition Ciphers

19CSE311 Computer Security

Jevitha KP
Department of CSE

TRANSPOSITION CIPHERS

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

- A symbol in the first position of the plaintext may appear in the tenth position of the ciphertext.

- A symbol in the eighth position in the plaintext may appear in the first position of the ciphertext.

- In other words, a transposition cipher reorders (transposes) the symbols.

Keyless Transposition Ciphers

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

- There are two methods for permutation of characters.

- In the first method, the text is written into a table column by column and then transmitted row by row.

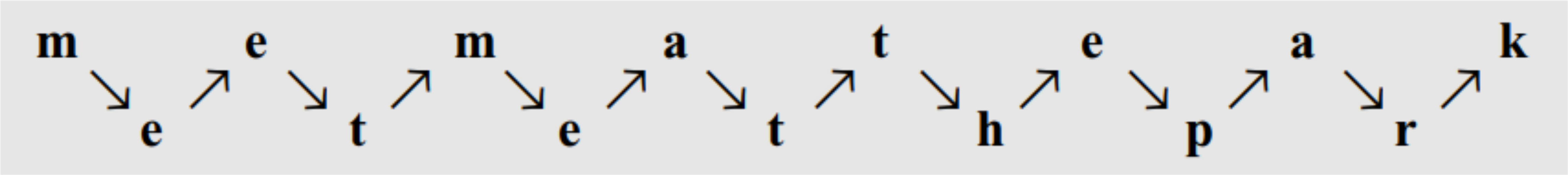
- In the second method, the text is written into the table row by row and then transmitted column by column.

Keyless Transposition Ciphers

- A good example of a keyless cipher using the first method is the **rail fence cipher.**

- In this cipher, the plaintext is arranged in two lines as a zigzag pattern (which means column by column); 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 as below. She then creates the ciphertext “MEMATEAKETETHPR” by sending the first row followed by the second row.



m e m a t e a k

e t e t h p r

Keyless Transposition Ciphers

- Bob receives the ciphertext and divides it in half (in this case the second half has one less character).

- The first half forms the first row; the second half, the second row.

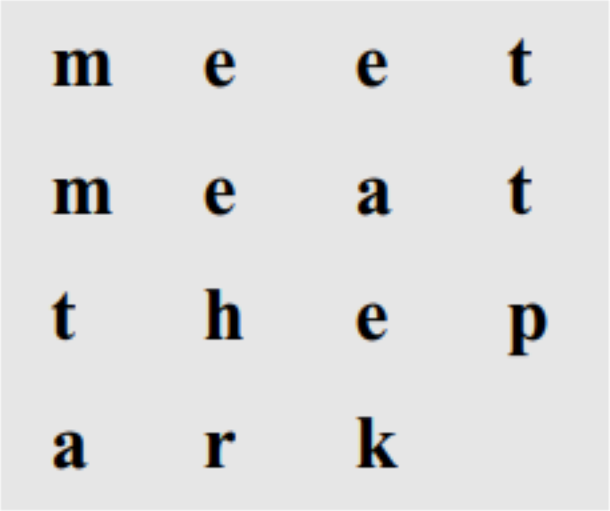
- Bob reads the result in zigzag.

- Because there is no key and the number of rows is fixed (2), the cryptanalysis of the ciphertext would be very easy for Eve.

- All she needs to know is that the rail fence cipher is used.

Keyless Transposition Ciphers

- 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.
- She then creates the ciphertext “MMTAEEHREAEKTTP” by transmitting the characters column by column.
- Bob receives the ciphertext and follows the reverse process. He writes the received message, column by column, and reads it row by row as the plaintext.
- Eve can easily decipher the message if she knows the number of columns.



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

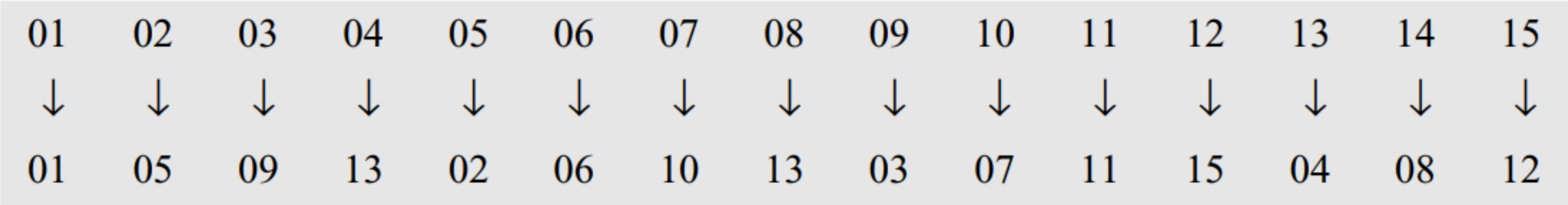
Keyless Transposition Ciphers

- The following shows the permutation of each character in the plaintext into the ciphertext based on the positions.

- 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.



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

Keyed Transposition Ciphers

- The keyless ciphers permute the characters by using writing plaintext in one way (row by row, for example) and reading it in another way (column by column, for example).

- 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.

Keyed Transposition Ciphers

- Alice needs to send the message “Enemy attacks tonight” to Bob.

- Alice and Bob have agreed to divide the text into groups of **five** characters and then **permute** the characters in each group.

- The following shows the grouping after adding a **bogus** character at the end to make the **last group the same size** as the others.

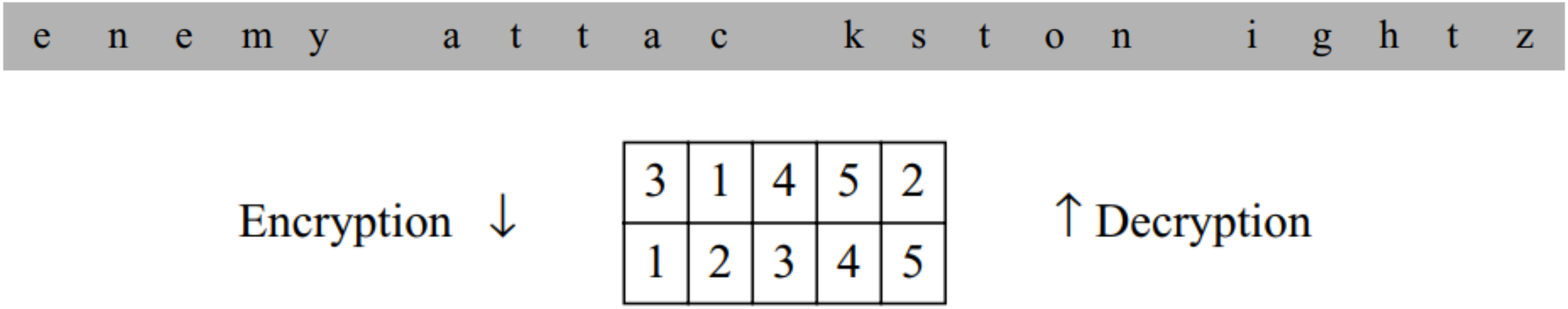
Keyed Transposition Ciphers

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

- Key : The third character in the plaintext block becomes the first character in the ciphertext block; the first character in the plaintext block becomes the second character in the ciphertext block; and so on.

- The permutation yields the ciphertext “EEMYNTAACTTKONSHITZG” to Bob.

- Bob divides the ciphertext into 5-character groups and, using the key in the reverse order, finds the plaintext.



enemy attac kston ightz

Encryption ↓

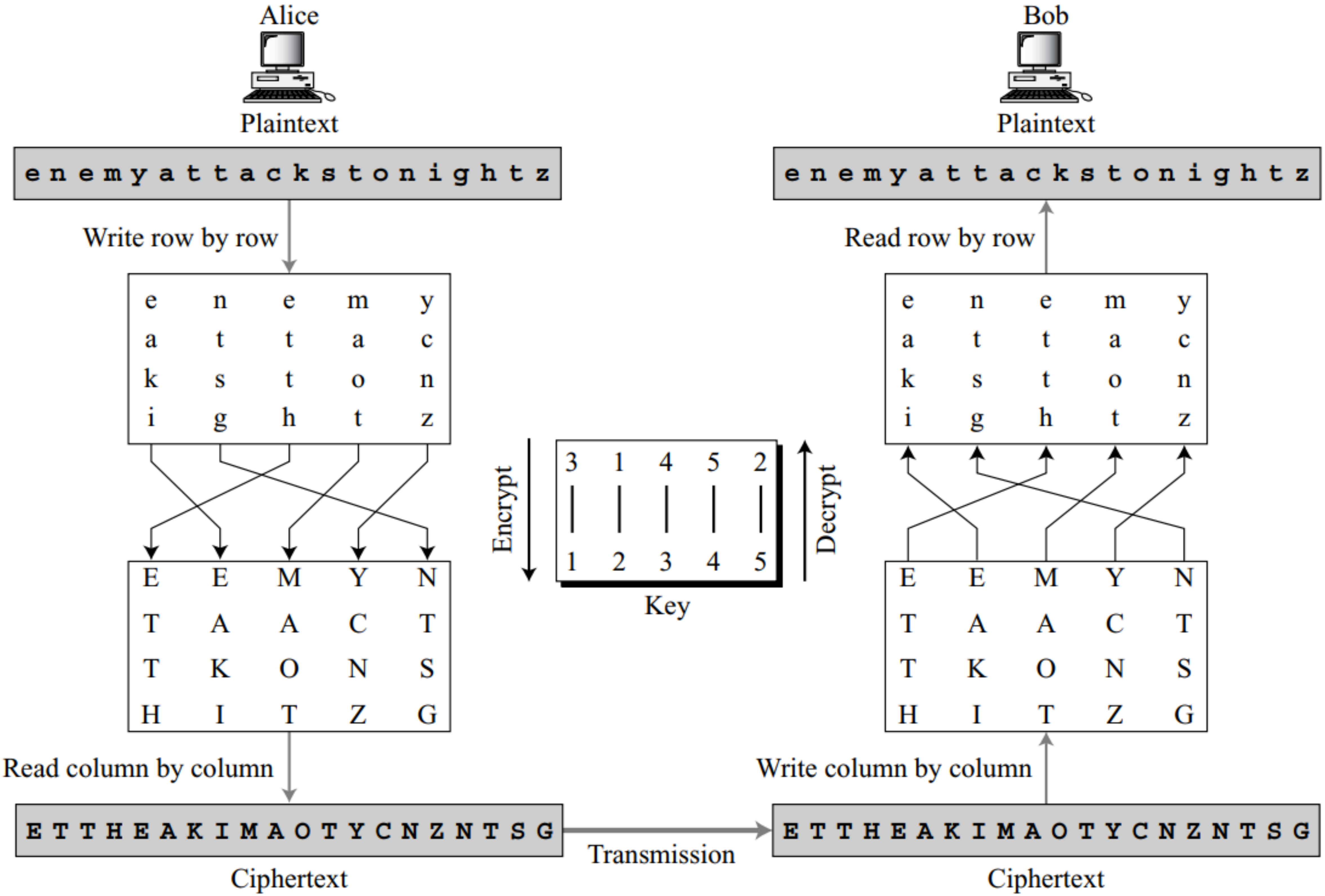
3	1	4	5	2
1	2	3	4	5

↑ Decryption

Combining Two Approaches

- More recent transposition ciphers **combine the two approaches** to achieve better scrambling.
- Encryption or decryption is done in three steps.
  - First, the text is written into a table row by row.
  - Second, the permutation is done by reordering the columns.
  - Third, the new table is read column by column.
- The first and third steps provide a keyless global reordering; the second step provides a **blockwise keyed reordering**.
- These types of ciphers are often referred to as **keyed columnar transposition ciphers** or just columnar transposition ciphers.

Combining Two Approaches



Alice

Plaintext

enemyattackstonightz

Write row by row

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

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

Read column by column

ETTHEAKIMAOTYCNZNTSG

Ciphertext

Encrypt

3	1	4	5	2
1	2	3	4	5

Key

Decrypt

Transmission

Bob

Plaintext

enemyattackstonightz

Read row by row

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

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

Write column by column

ETTHEAKIMAOTYCNZNTSG

Ciphertext

Combining two Approaches

- The first table is created by Alice writing the plaintext row by row.

- The columns are permuted using the the key.

- The ciphertext is created by reading the second table column by column.

- Bob does the same three steps in the reverse order.

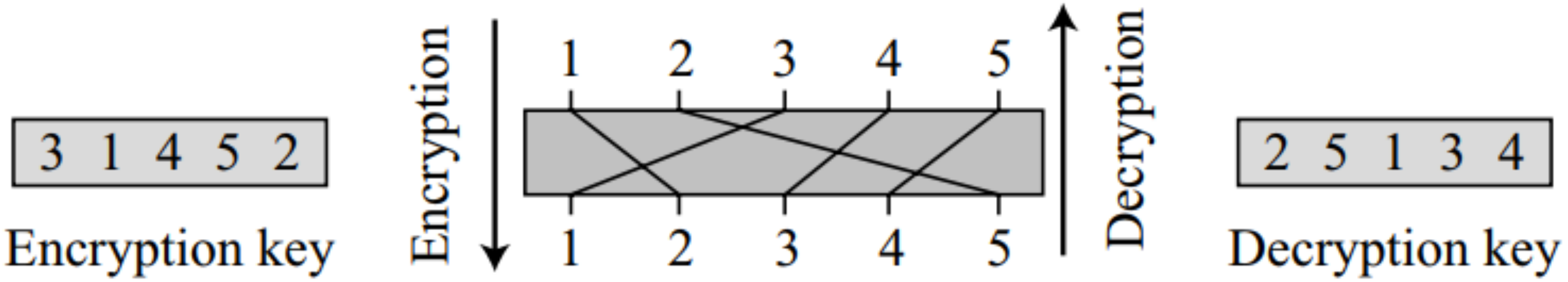
- He writes the ciphertext column by column into the first table, permutes the columns, and then reads the second table row by row.

Combining two Approaches

- **Keys**
- 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: **one for encryption and one for direction.**
  - The keys are stored in tables with one entry for each column.
  - The entry shows the source column number; the destination column number is understood from the position of the entry.

Combining two Approaches

- **Keys**
- The encryption key is (3 1 4 5 2).
- The first entry shows that column 3 (contents) in the source becomes column 1 (position or index of the entry) in the destination.
- The decryption key is (2 5 1 3 4).
- The first entry shows that column 2 in the source becomes column 1 in the destination

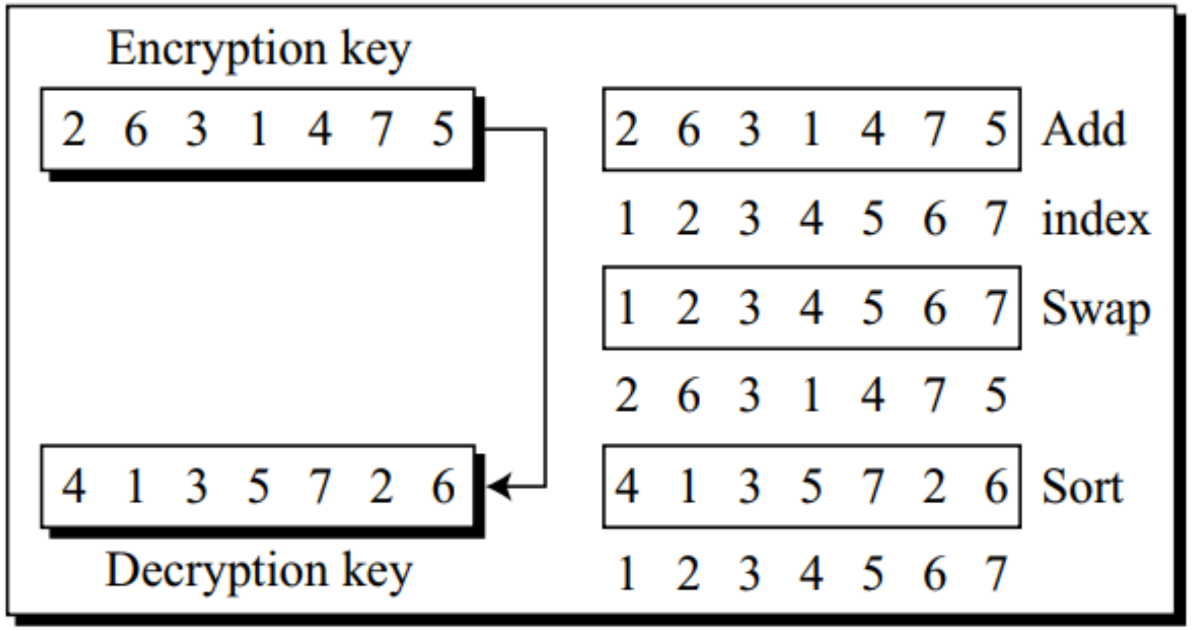


Combining two Approaches

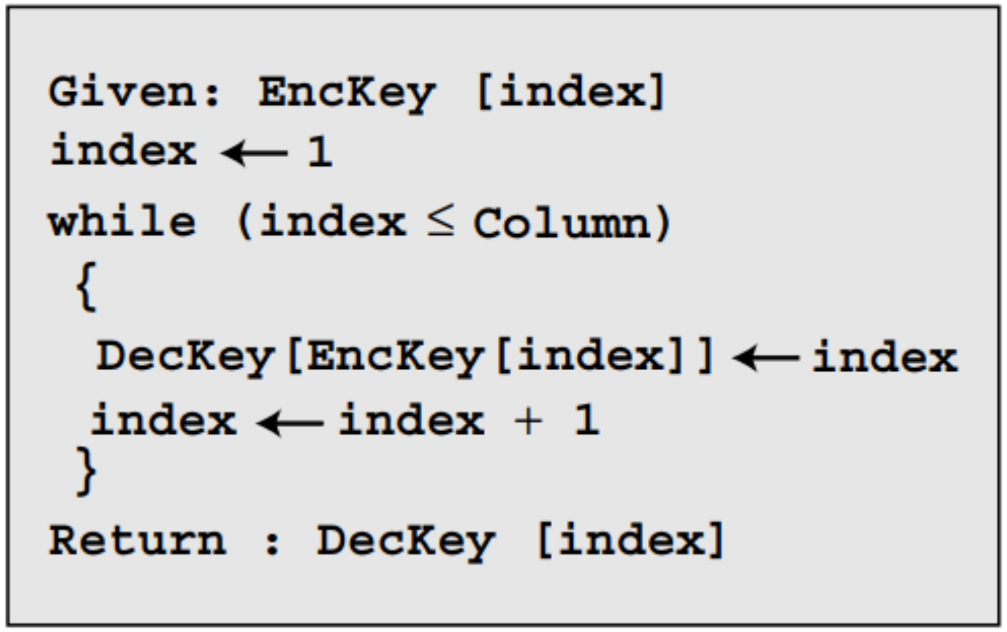
- **Keys**

- How can the decryption key be created if the encryption key is given, or vice versa?

- First add indices to the key table, then swap the contents and indices, finally sort the pairs according to the index



a. Manual process



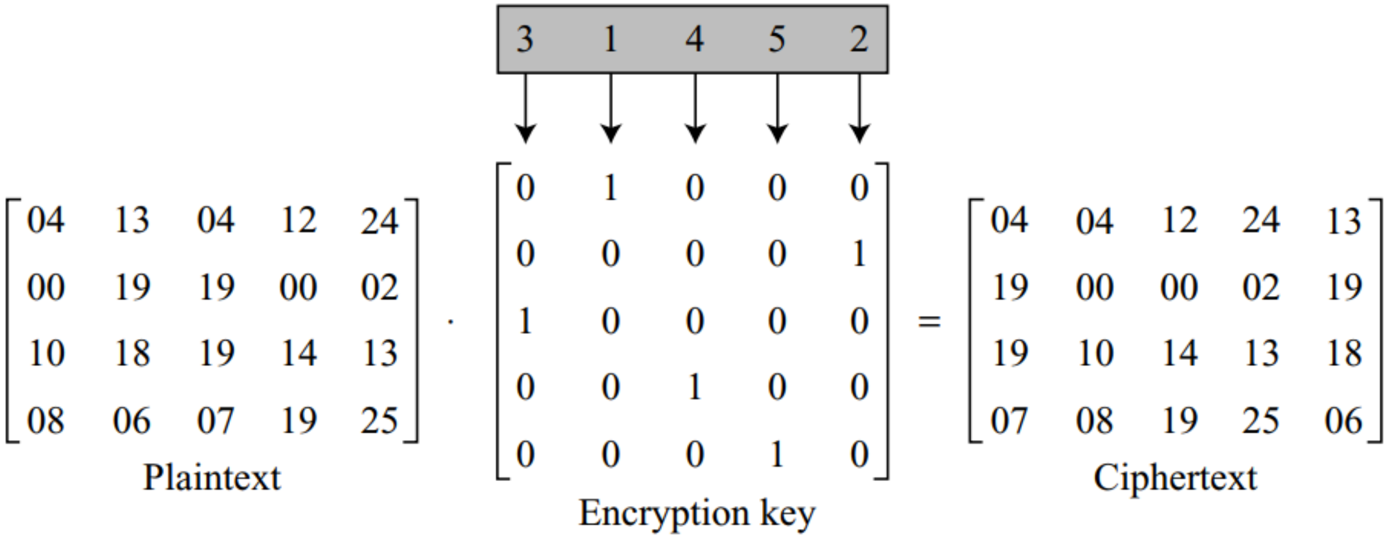
```
Given: EncKey [index]
index ← 1
while (index ≤ Column)
 {
  DecKey[EncKey[index]] ← index
  index ← index + 1
 }
Return : DecKey [index]
```

b. Algorithm

Combining two Approaches

- **Using Matrices**
- We can use matrices to show the encryption/decryption process for a **transposition cipher**.
- The plaintext and ciphertext are l × m matrices representing the **numerical values of the characters**; the keys are square matrices of size m × m.
- In a permutation matrix, every row or column has exactly one 1 and the rest of the values are 0s.
- Encryption is performed by multiplying the plaintext matrix by the **key matrix** to get the ciphertext matrix;
- decryption is performed by multiplying the ciphertext by the **inverse key matrix** to get the plaintext matrix
- There is no need to invert the matrix, the encryption key matrix can simply be transposed (swapping the rows and columns) to get the decryption key matrix.

Combining two Approaches



$$\begin{bmatrix} 04 & 13 & 04 & 12 & 24 \\ 00 & 19 & 19 & 00 & 02 \\ 10 & 18 & 19 & 14 & 13 \\ 08 & 06 & 07 & 19 & 25 \end{bmatrix} \cdot \begin{array}{ccccc} 3 & 1 & 4 & 5 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \left[\begin{matrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{matrix}\right. & \begin{matrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{matrix} & \left.\begin{matrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{matrix}\right] \end{array} = \begin{bmatrix} 04 & 04 & 12 & 24 & 13 \\ 19 & 00 & 00 & 02 & 19 \\ 19 & 10 & 14 & 13 & 18 \\ 07 & 08 & 19 & 25 & 06 \end{bmatrix}$$

Plaintext

Encryption key

Ciphertext

04	04	12	24	13
19	00	00	02	19
19	10	14	13	18
07	08	19	25	06

0	0	1	0	0
1	0	0	0	0
0	0	0	1	0
0	0	0	0	1
0	1	0	0	0

04	13	04	12	24
00	19	19	00	02
10	18	19	14	13
08	06	07	19	25

Examples

- Using Railfence encrypt “This is encryption”
- Cipher text - Tiiecytohssnrpin
- Th is is en cr yp ti on

Cryptanalysis of Transposition Ciphers

- Transposition ciphers are vulnerable to several kinds of ciphertext-only attacks
- **Statistical Attack**
- A transposition cipher **does not change the frequency of letters** in the ciphertext; it only **reorders the letters**.
- So the first attack that can be applied is **single-letter frequency analysis.**
- This method can be useful if the **length of the ciphertext is long enough**.
- However, transposition ciphers **do not preserve the frequency of digrams and trigrams.**
- In fact, **if a cipher does not preserve the frequency of digrams and trigrams, but does preserve the frequency of single letters, it is probable that the cipher is a transposition cipher.**

Brute-Force Attack

- Eve can try all possible keys to decrypt the message.
- However, the number of keys can be huge (1! + 2! + 3! + . . . + L!), where L is the length of the ciphertext.
- A better approach is to guess the number of columns.
- Eve knows that the number of columns divides L.
- For example, if the length of the cipher is 20 characters, then 20 = 1 × 2 × 2 × 5.
- This means the number of columns can be a combination of these factors (1, 2, 4, 5, 10, 20).
- However, the first (only one column) is out of the question and the last (only one row) is unlikely.

Brute-Force Attack

- **Example:**
- Suppose that Eve has intercepted the ciphertext message “EEMYNTAACTTKONSHITZG”. The message length L = 20 means the number of columns can be 1, 2, 4, 5, 10, or 20. Eve ignores the first value because it means only one column and no permutation.
- **Option a - If the number of columns is 2 :**
    - the only two permutations are (1, 2) and (2, 1).
    - (1,2) means there would be no permutation.
    - Eve tries the second one.
    - Eve divides the ciphertext into two-character units: “EE MY NT AA CT TK ON SH IT ZG”.
    - She then tries to permute each of these getting “ee ym nt aa tc kt no hs ti gz”, which does not make sense.

Brute-Force Attack

- **Option b - If the number of columns is 4**
    - there are 4! = 24 permutations.
    - The first one (1 2 3 4) means there would be no permutation.
    - Eve needs to try the rest.
    - After trying all 23 possibilities, Eve finds no plaintext that makes sense.

Brute-Force Attack

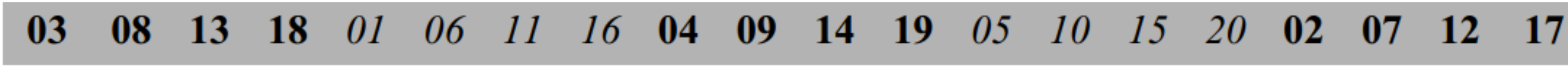
- **Option C - If the number of columns is 5**
  - there are 5! = 120 permutations.
  - The first one (1 2 3 4 5) means there would be no permutation.
  - Eve needs to try the rest.
  - The permutation (2 5 1 3 4) yields a plaintext “enemyattackstonightz” that makes sense after removing the bogus letter z and adding spaces

Pattern Attack

- Another attack on the transposition cipher can be called pattern attack.

- The ciphertext created from a keyed transposition cipher has **some repeated patterns.**

- There is a pattern in the list shown below based on prev example.



03	**08**	**13**	**18**	*01*	*06*	*11*	*16*	**04**	**09**	**14**	**19**	*05*	*10*	*15*	*20*	**02**	**07**	**12**	**17**

Pattern Attack

- We have five groups: (3, 8, 13, 18), (1, 6, 11, 16), (4, 9, 14, 19), (5, 10, 15, 20), and (2, 7, 12, 17).
- In all groups, the difference between the two adjacent numbers is 5.
- This regularity can be used by the cryptanalyst to break the cipher.
- If Eve knows or can guess the number of columns (which is 5 in this case), she can organize the ciphertext in groups of four characters.
- Permuting the groups can provide the clue to finding the plaintext.

Double Transposition Ciphers

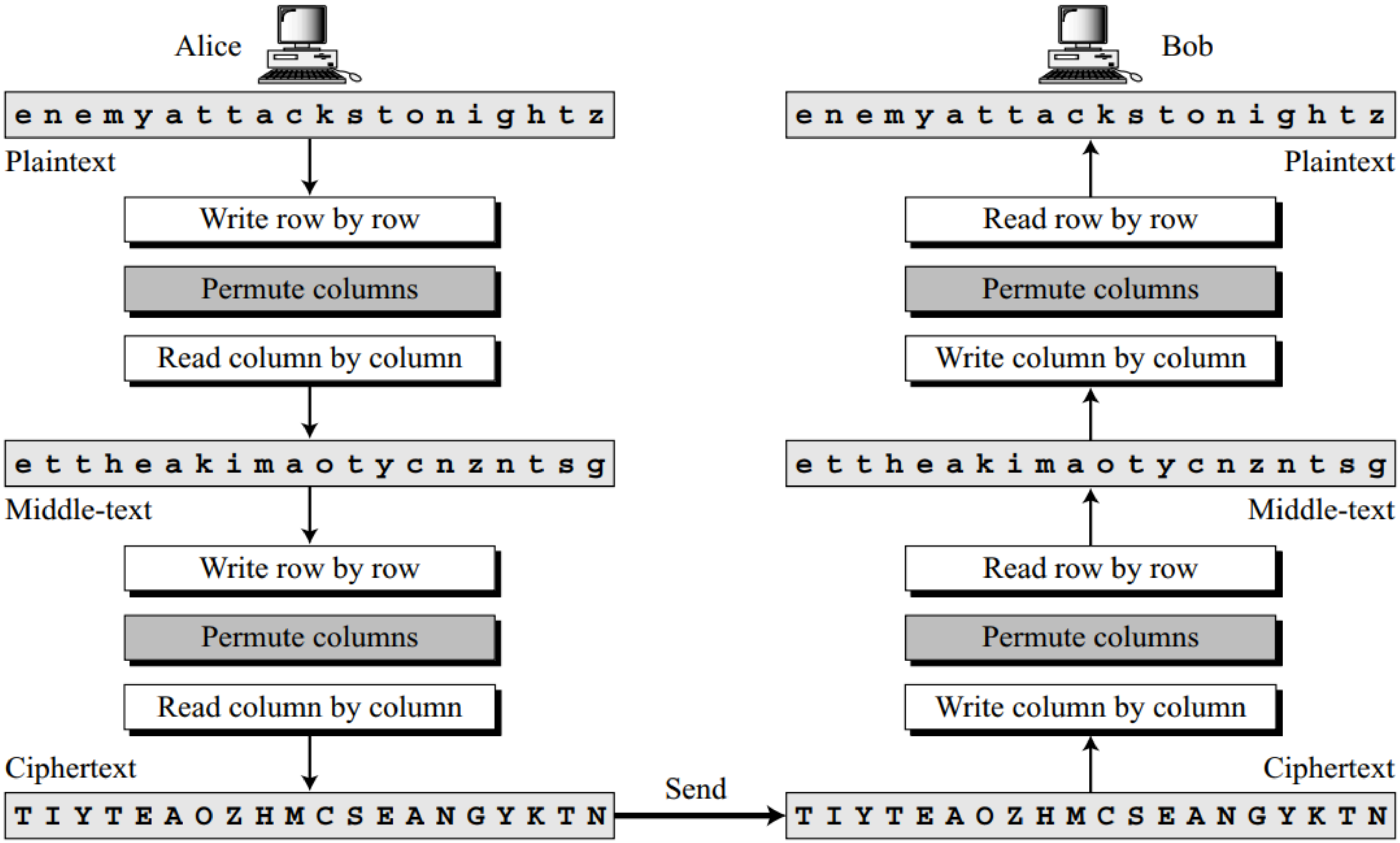
- Double transposition ciphers can make the job of the cryptanalyst difficult.

- An example of such a cipher would be the one that repeats twice the algorithm used for encryption and decryption

- A different key can be used in each step, but normally the same key is used.

- Although, the cryptanalyst can still use the single-letter frequency attack on the ciphertext, a pattern attack is now much more difficult.

Double Transposition Ciphers

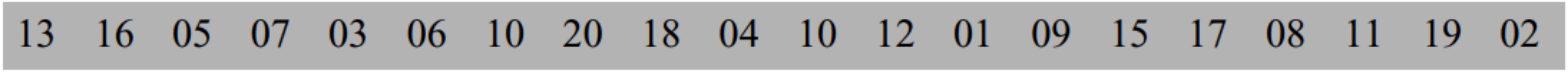


Double Transposition Ciphers

- Comparing the set shown below with the result in prev example, we see that there is no repetitive pattern.

- Double transposition removes the regularities we have seen before

- The pattern analysis of the text shows



13	16	05	07	03	06	10	20	18	04	10	12	01	09	15	17	08	11	19	02

Examples

- Encrypt the following using Transposition Cipher : “This is an encrypted message” with the key (3,1,4,5,2); block size - 5.

- PT - This is an encrypted message

- Step 1 - Group of 5 -

T h i s i

s a n e n

c r y p t

e d m e s

s a g e z

Examples

- Step 2 - Permutation with the given key - 3,1,4,5,2

T h i s i ==> i T s i h

s a n e n ==> n s e n a

c r y p t ==> y c p t r

e d m e s ==> m e e s d

s a g e z ==> g s e z a

- Step 3 - Read it column by column
- Cipher text for single transposition cipher :
- **inymg tsces sepee intsz harda**

Examples

- Step 1 & 2 for double transposition - Writing it row wise the previous cipher text. Permutation with the given key - 3,1,4,5,2

i n y m g ==> y i m g n

t s c e s ==> c t e s s

s e p e e ==> p s e e e

i n t s z ==> t i s z n

h a r d a ==> r h d a a

- Step 3 - Read it column by column
- Cipher text for **double transposition cipher** :
- **ycptr itsih meesd gseza nsena**