University of Salahaddin - Erbil
College of Engineering
Department of Software Engineering

Data Security

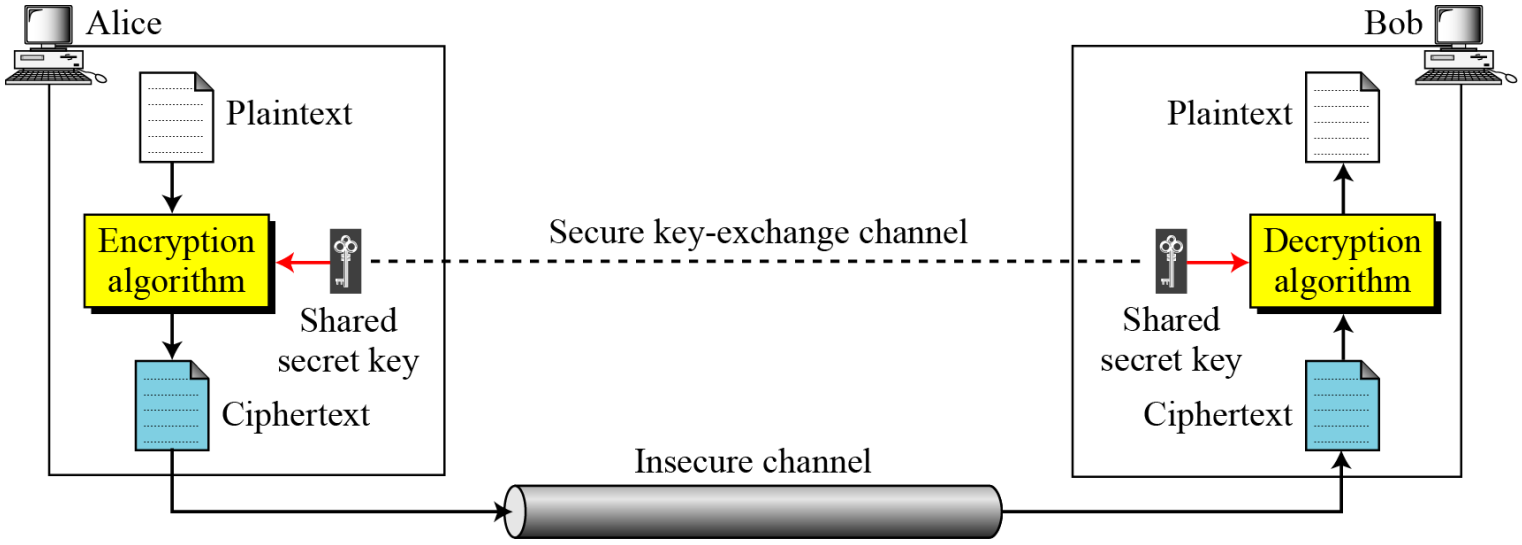
Academic year 2021-2022
4th Year Material
Chapter Two

Classical Encryption Techniques
substitution ciphers and transpositions ciphers

Prepared By: Mr. **Zana Farhad Doghramachi, M.Tech(CSE)**
Zana.softeng@gmail.com

Symmetric Key Cipher

- The general idea behind a symmetric-key cipher is shown in this figure. The original message from Alice to Bob is called plaintext; the message that is sent through the channel is called the ciphertext. To create the ciphertext from the plaintext, Alice uses an encryption algorithm and a shared secret key. To create the plaintext from ciphertext, Bob uses a decryption algorithm and the same secret key.



Substitution Ciphers

- A substitution cipher replaces one symbol with another. If the symbol in the plaintext are alphabetic characters, we replace one character with another character. If the symbols are digits (0 to 9), we replace one digit with another digit.

- Substitution cipher can be categorized as:

a) monoalphabetic ciphers.

b) polyalphabetic ciphers.

Monoalphabetic

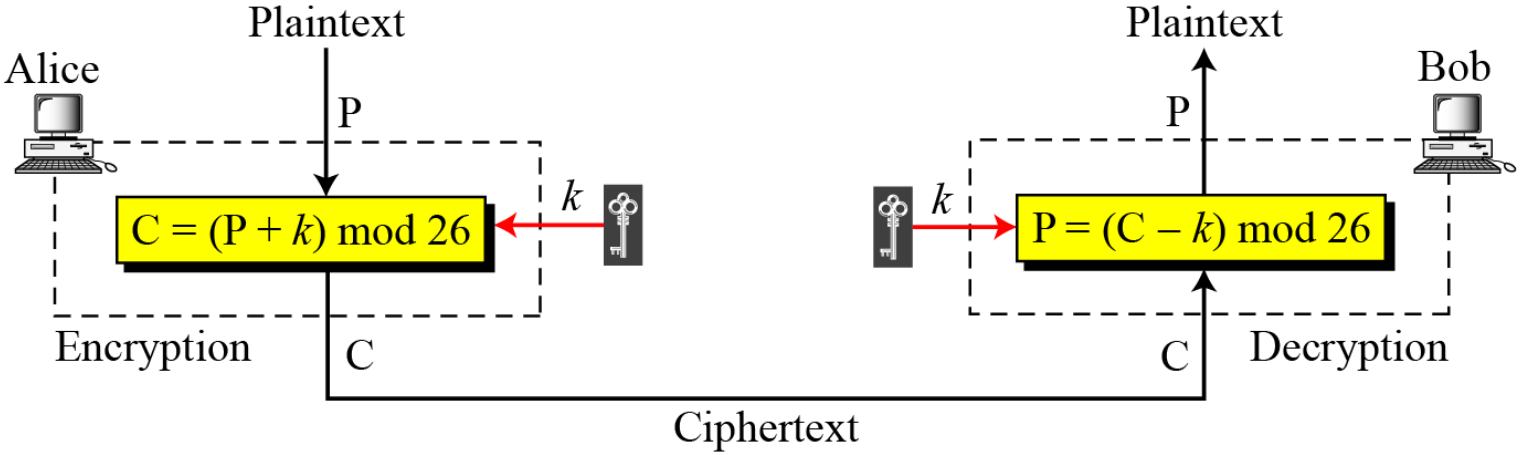
- In monoalphabetic substitution, a character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of it's position in the text.
- For example, if the algorithm says that letter A in the plaintext is changed to letter D, every latter A is changed to letter D. In other words, the relationship between letters in the plaintext and the ciphertext is one-to-one.
- The following shows a plaintext and it's corresponding cipherterxt1 and ciphertext2. The first cipher is probably monoalphabetic because both l's are encrypted as a O's, and the second cipher is not monoalphabetic because each l's are encrypted by different character.

plaintext: hello

ciphertext1: khoor ciphertext2 abnzf

Additive Cipher I

- It's simplest monoalphabetic cipher. This cipher is sometimes called a ***shift cipher*** and sometimes a ***Caeser cipher*** .
- Each character is assigned an integer in $Z_{26.}$ The secret key between Alice and Bob is also an interger in $Z_{26.}$
- The encryption algorithm adds the key to the plaintext character.



Additive Cipher II

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

Q1: use the additive cipher with key=15 to encrypt the message ”hello”.

Q2: use the additive cipher with key=3 to decrypt the message ”phhw ph diwhu wkh sduwb”

Q3: Eve has intercepted the ciphertext “uvaclyfzlbyl”. Show how she can use a brute-force attack to break the cipher.

Shift Cipher

- Historically, additive cipher are called shift ciphers. The reason is that the encryption algorithm can be interpreted as “shift key characters down” and the decryption algorithm can be interpreted as “shift key character up”.

- For example, if the key=15, the encryption algorithm shifts 15 characters down (toward the end of the alphabet). The decryption algorithm shifts 15 character up (toward the beginning of the alphabet). Of course, when we reach the end or the beginning of the alphabet, we wrap around.

Caeser Cipher

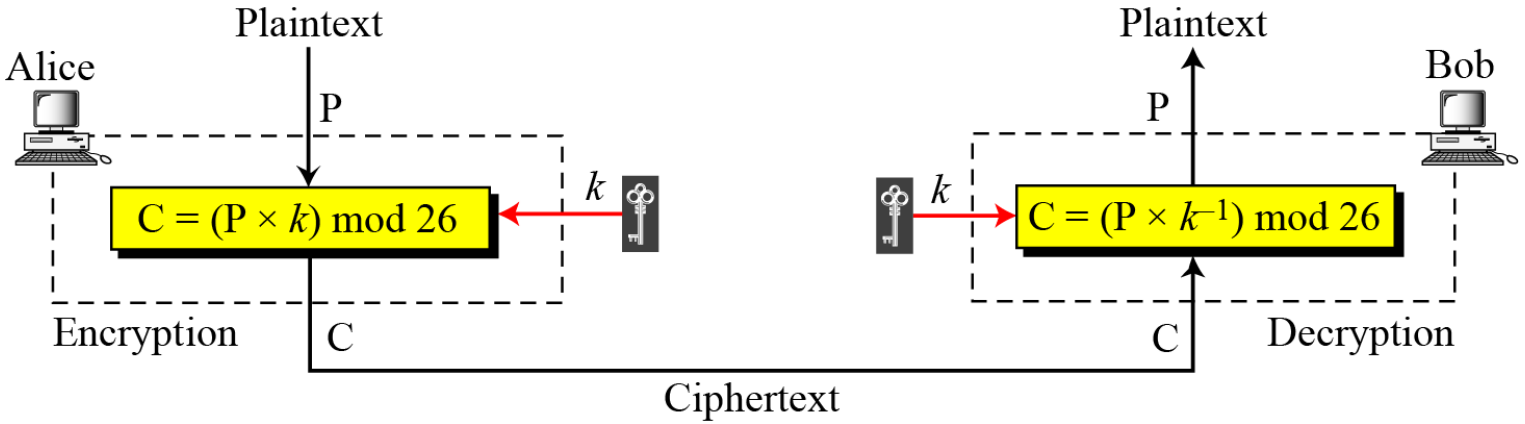
- Julius Caeser used an additive cipher to communicate with his officers. For this reason, the additive ciphers are sometimes referred to as the Caeser cipher.

- Caeser used a key of 3 for his communications.

Multiplicative Ciphers

- In multiplicative ciphers, the encryption algorithm specifies multiplication of the plaintext by the key and the decryption algorithm specifies division of the ciphertext.

- Note that the key needs to belong to the set Z_{26} to guarantee that the encryption and decryption are inverse of each other.



Home work

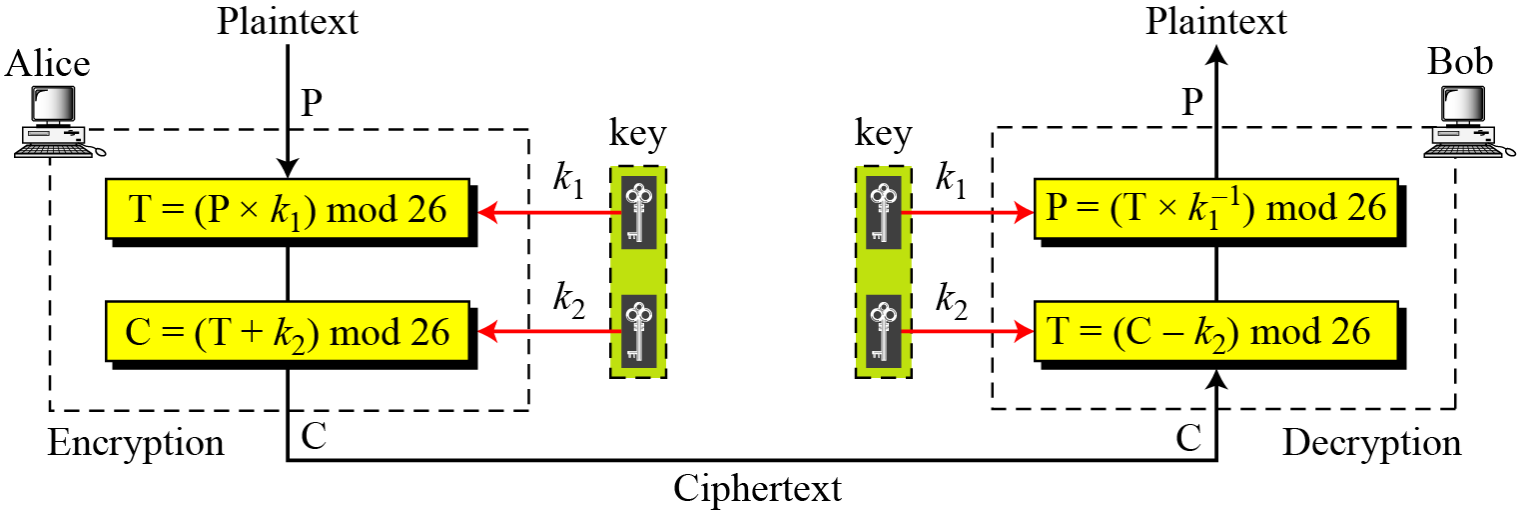
Q1: use the multiplicative cipher with a key of 5 to encrypt the message ”please”.

Q2: What is the key domain for any multiplicative cipher?

Affine Cipher

- We can combine additive and multiplicative ciphers to get what is called the affine cipher, a combination of both ciphers with a pair of keys.

- The first key is used with the multiplicative cipher; the second key is used with the additive cipher.



Home work

Q1: use the affine cipher to encrypt the message ”meet” with the key pair (5,3).

Q2: use the affine cipher to decrypt the message ”zebbw” with the key pair (7,2).

Polyalphabetic I

- In polyalphabetic substitution, each occurrence of a character may have a different substitution. The relationship between a character in the plaintext to character in chiphertext is one-to-many.
- For example, “a” could be enciphered as “d” in the beginning of the text, but “n” in the middle.
- To create a polyalphabetic cipher, we need to make each ciphertext character dependent on both the corresponding plaintext character and the position of the plaintext character in the message. This implies that our key should be a stream of subkeys, in which each subkey depends somehow on the position of the plaintext character that uses that subkey for decipherment.

Polyalphabetic II

- In other words, we need to have a key stream k=(k1 ,k2 ,k3…) in which k_i is used to encipher the $_i$th character in the plaintext to create the $_i$th character in the ciphertext.

Playfair Cipher I

- Is a polyalphabetic cipher, used by the British army during World War I. The secret key in this cipher is made of 25 alphabet letters arranged in a 5x5 matrix (letters I and J considered the same when encrypting).

- Different arrangements of the letters in the matrix can create many different secret keys.

- Before encryption, if the two letters in a pair are the same, a bogus letter is inserted to separate them. After inserting bogus letters, if the number of characters in the plaintext is odd, one extra bogus character is added at the end to make the number of characters even.

Playfair Cipher II

- The cipher uses three rules for encryption:

a) If the two letters in a pair are located in the same row of the secret key, the corresponding encrypted character for each letter is the next letter to the right in the same row.

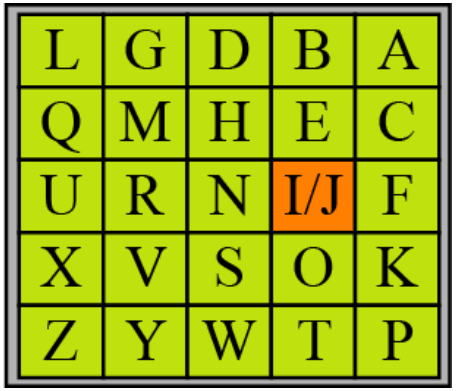
b) If the two letters in a pair are located in the same column of the secret key, the corresponding encrypted character for each letter is the letter beneath it in the same column.

c) If the two letters in a pair are not located in the same row or column of the secret, the corresponding encrypted character for each letter is a letter that is in it's own row but in the same column as the other letter.

Playfair Cipher III

a) Example of the key secret:-

Secret Key =



L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

b) Q1: Use the above secret key to encrypt the plaintext “hello”.

Vigenere Cipher I

- Was designed by Blaise de Vigenere, a sixteenth century French mathematician.

- A Vigenère cipher uses a different strategy to create the key stream. The key stream is a repetition of an initial secret key stream of length m, where we have 1=< m=<26. The cipher can be described as follows where (k1,k2,….,km) is the initial secret key agree to by Alice and Bob.

$p=p_1p_2p_3 \ldots \quad ,c=c_1c_2c_3\ldots , \quad k=[(k_1,k_2,..,k_m)(k_1,k_2,..,k_m) \ldots]$

Encryption: $c_i = p_i + k_i \mod 26$

Decryption: $p_i = c_i - k_i \mod 26$

Vigenere Cipher II

Q1: Encrypt the message “she is listening” using 6- character keyword “PASCAL”.

Q2: When additive cipher is a special case of Vigenere cipher?

Vigenere Table

Key	Plaintext																								
	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

Hill Cipher I

- Invented by Laster S. Hill. In this cipher the plaintext is divided into equal size blocks. The blocks are encrypted one at a time in such a way that each character in the block contributes to the encryption of other characters in the block. For this reason, the Hill cipher belongs to a category of ciphers called block ciphers.

- In a Hill cipher, the key is a square matrix of size $m_x m$ in which m is the size of the block. If we call the key matrix K, each element of the matrix is $k_{i,j}$ as shown

$$K = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix}$$

Hill Cipher II

- Let us show how one block of the ciphertext is encrypted. If we call the m characters in the plaintext block $p_1, p_2, \ldots, p_m$ corresponding characters in the ciphertext block are $C_1, C_2, \ldots, C_m$, then we have

$$
\begin{aligned}
C_1 &= P_1 k_{11} + P_2 k_{21} + \cdots + P_m k_{m1} \\
C_2 &= P_1 k_{12} + P_2 k_{22} + \cdots + P_m k_{m2} \\
&\cdots \\
C_m &= P_1 k_{1m} + P_2 k_{2m} + \cdots + P_m k_{mm}
\end{aligned}
$$

Q1: Use Hill cipher to encrypt the plaintext "code is ready" by using 3_x4 matrix, if

$$
K = \begin{matrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \end{matrix}
$$

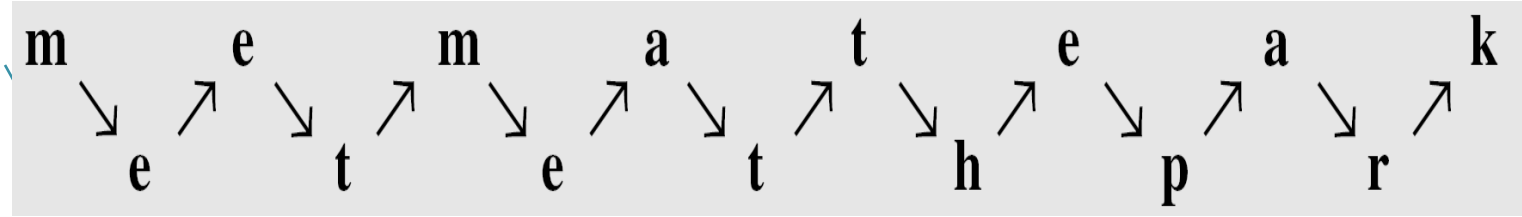
Transposition Ciphers I

- A **transposition cipher** it changes the location of the symbols and does not substitute one symbol for another. A symbol in the first position of the plaintext may appear in the tenth position in the ciphertext. In other words, a transposition cipher reorders the symbols.

- 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.

- **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

Transposition Ciphers II



- She then creates the ciphertext “memateaketethpr” by sending the first row followed by the second row.
- 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 form the second tow. 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 rail fence cipher is used.

Transposition Ciphers III

- 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 creates the ciphertext “mmtaeehreaekttp” by transmitting the characters column by column, and reads it row by row as the plaintext.

- Eva can easily dechiper the message if she knows the number of columns

Transposition Ciphers IV

- 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.

Key:	4	3	1	2
Plaintext:	m	e	e	t
	m	e	a	t
	t	h	e	p
	a	r	k	x

Ciphertext: eaekttpxeehrmmta