Cryptography and Network Security

Chapter 2

Classical Encryption Techniques II

Prof. Mahmood Kh. Ibrahem

Playfair Cipher

- not even the large number of keys in a monoalphabetic cipher provides security
- one approach to improving security was to encrypt multiple letters
- the **Playfair Cipher** is an example invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair

Playfair Key Matrix

- a 5X5 matrix of letters based on a keyword
- fill in letters of keyword (sans duplicates)
- fill rest of matrix with other letters
- eg. using the keyword **MONARCHY**

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

Encrypting and Decrypting

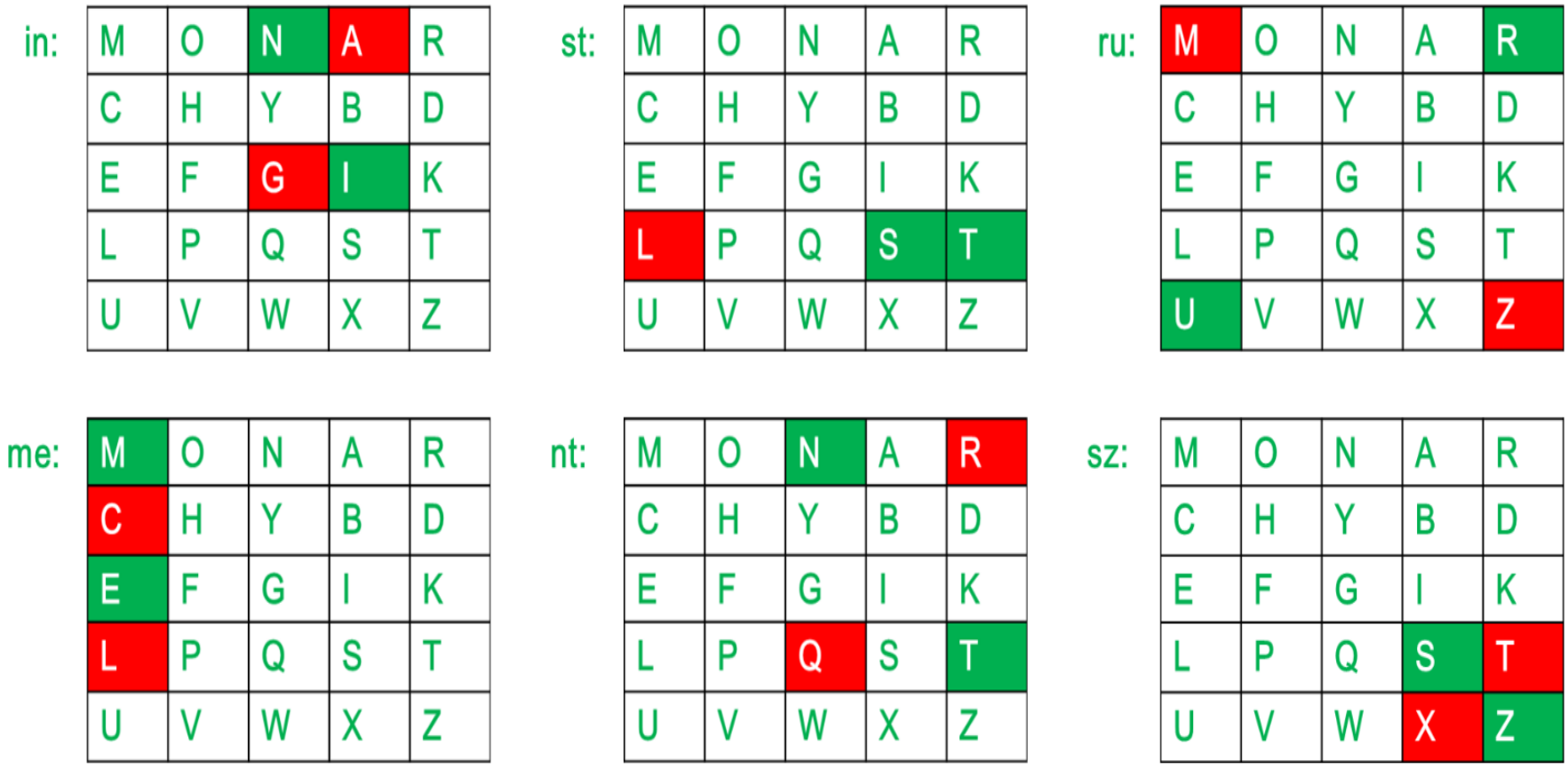
- plaintext is encrypted two letters at a time
  1. if a pair is a repeated letter, insert filler like 'X'
  2. if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
  3. if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)
  4. otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair
  5. Decrypting of course works exactly in reverse. Can see this by working the example pairs shown, backwards.

Playfair Encryption

Plain Text: "instrumentsz"
Encrypted Text: gatlmzclrqtx
Encryption:

i -> g
 n -> a
 s -> t
 t -> l
 r -> m
u -> z
m -> c
e -> l
 n -> r
t -> q
s -> t

Playfair Encryption

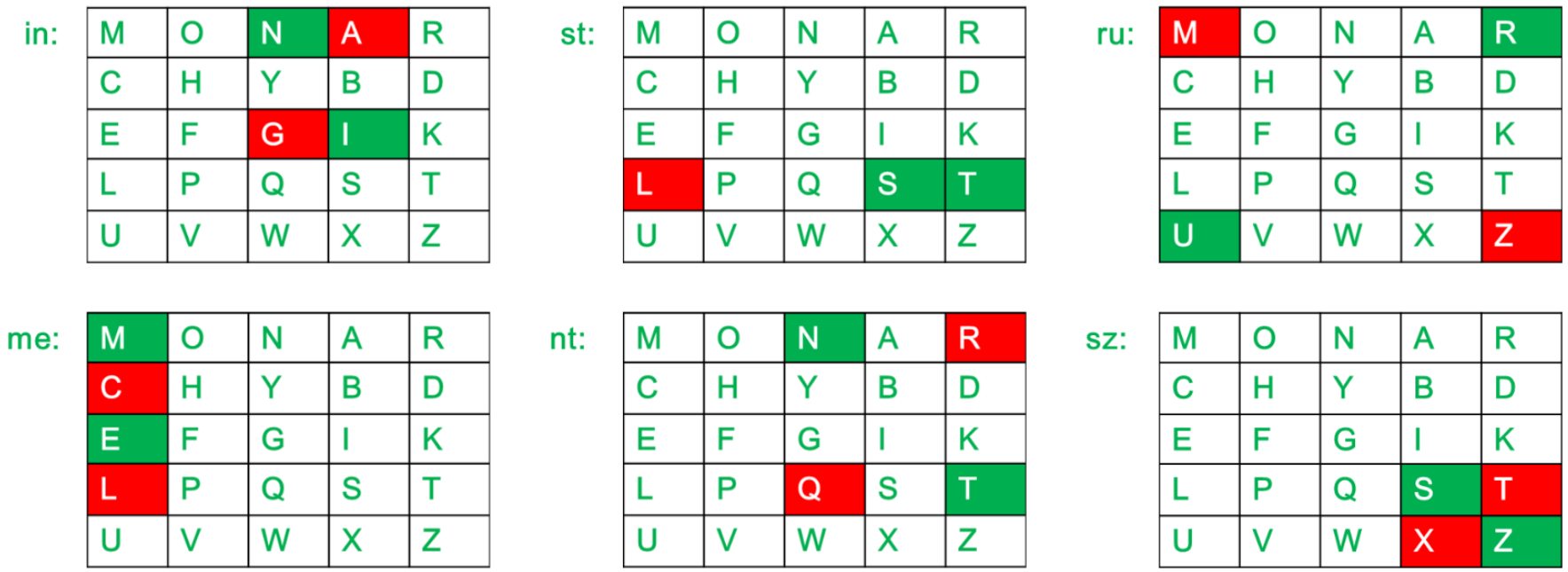


Playfair Decryption

Plain Text: "gatlmzclrqtx"
Decrypted Text: instrumentsz
Decryption: (red)-> (green)

ga -> in
tl -> st
mz -> ru
cl -> me
rq -> nt
tx -> sz

Playfair Decryption



Security of Playfair Cipher

- security much improved over monoalphabetic
- since have 26 x 26 = 676 digrams
- would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic)
- and correspondingly more ciphertext
- was widely used for many years
  - eg. by US & British military in WW1
- it **can** be broken, given a few hundred letters
- since still has much of plaintext structure

Polyalphabetic Ciphers

- **polyalphabetic substitution ciphers**
- improve security using multiple cipher alphabets
- make cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- use a key to select which alphabet is used for each letter of the message
- use each alphabet in turn
- repeat from start after end of key is reached

Polyalphabetic Ciphers

It is a substitution ciphers

improve security using multiple cipher alphabets

make cryptanalysis harder with more alphabets to guess and flatten frequency distribution

use a key to select which alphabet is used for each letter of the message

use each alphabet in turn

repeat from start after end of key is reached

$$c = E(m) = (m + k_i) \bmod n \qquad \text{for } i=1,2,\ldots,d$$

$$m = D(c) = (c - k_i) \bmod n \qquad \text{for } i=1,2,\ldots,d$$

Polyalphabetic Ciphers

write the plaintext out
write the keyword repeated above it
use each key letter as a caesar cipher key
encrypt the corresponding plaintext letter
eg using keyword deceptive

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 e

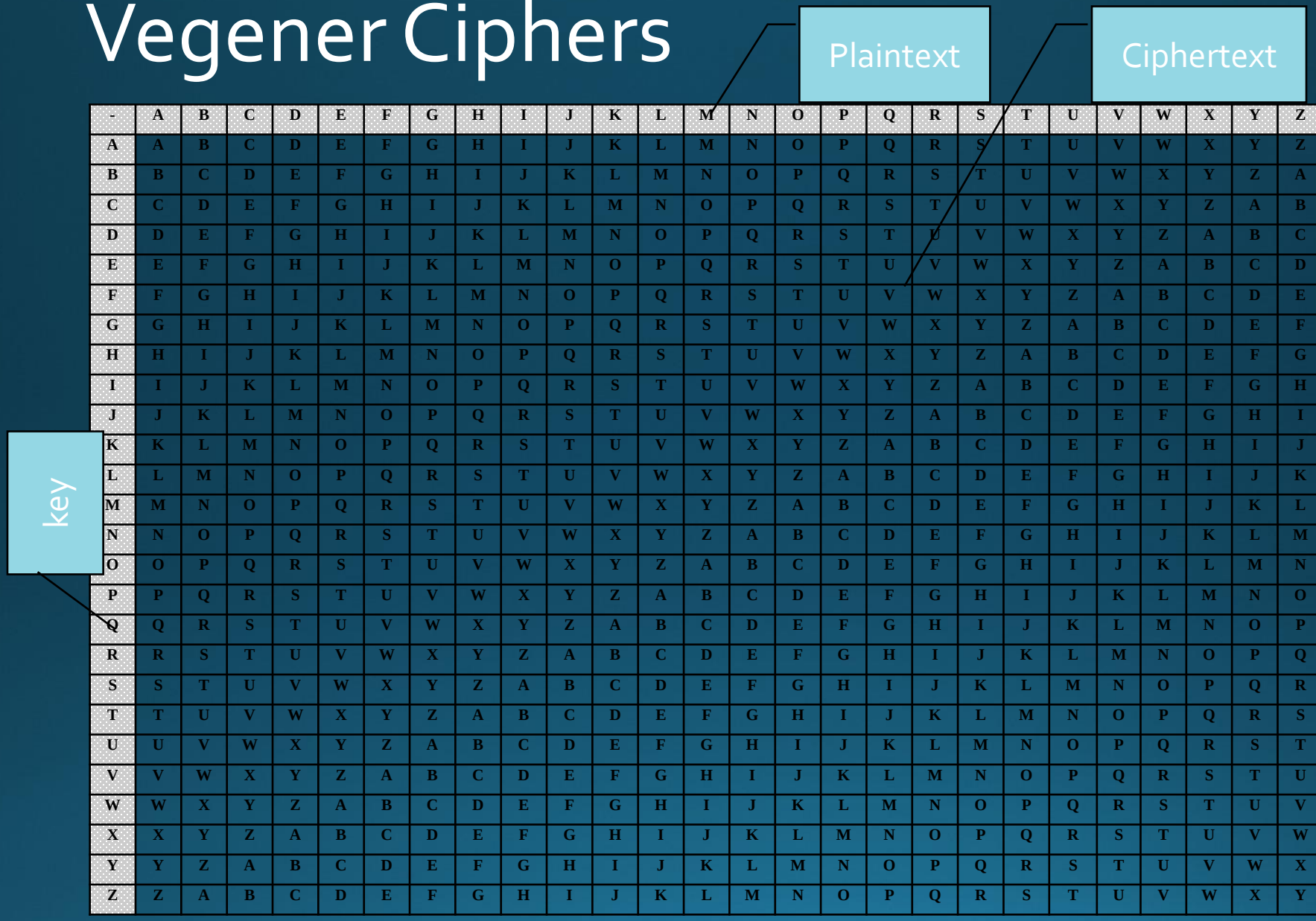
plaintext: w e a r e d i s c o v e r e d s a v e y o u r s e l f

ciphertext: Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J

Vegener Ciphers

m:	c	o	d	e	b	r	e	a	k	i	n	g		
	2	14	3	4	1	17	4	0	10	8	13	6		
k:	r	a	d	i	o	r	a	d	i	o	r	a		
	17	0	3	8	14	17	0	3	8	14	17	0		
m+k	19	14	6	12	15	8	4	3	13	22	4	6		
c:	T	O	G	M	P	I	E	D	S	W	E	G		
c-k	2	14	3	4	1	17	4	0	10	8	13	6		
m:	c	o	d	e	b	r	e	a	k	i	n	g		

Vegener Ciphers



-	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

Transposition Ciphers

- now consider classical **transposition** or **permutation** ciphers
- these hide the message by rearranging the letter order
- without altering the actual letters used
- can recognise these since have the same frequency distribution as the original text

Rail Fence cipher

- write message letters out diagonally over a number of rows
- then read off cipher row by row
- eg. write message out as:

```
m e m a t r h t g p r y
  e t e f e t e o a a t
```

- giving ciphertext

MEMATRHTGPRYETEFETEOAAT

Rail Fence cipher

- write message letters out diagonally over a number of rows
- then read off cipher row by row
- eg. write message "meet me after the toga party" as

depth 2:

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

- ciphertext: MEMATRHTGPRYETEFETEOAAT

depth 3:

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

- Ciphertext: MTAEHOPTEMFREGAYEETTTAR

Rail Fence Decryption

depth 2:
Split ciphertext into 2 halves
Select one character from each half & concatenate them together
Continue until ciphertext is finished
ciphertext: MEMATRHTGPRYETEFETEOAAT

M	E	M	A	T	R	H	T	G	P	R	Y
E	T	E	F	E	T	E	O	A	A	T	

Plaintext:
MEETMEAFTERTHETOGAPARTY

Product Ciphers

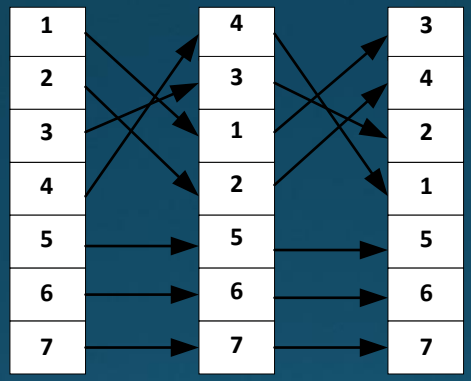
- ciphers using substitutions or transpositions are not secure because of language characteristics
- hence consider using several ciphers in succession to make harder, but:
  - two substitutions make a more complex substitution
  - two transpositions make more complex transposition
  - but a substitution followed by a transposition makes a new much harder cipher
  - C = S(m) . P(m') = P(S(m))
- this is bridge from classical to modern ciphers

Row Transposition Ciphers

a more complex transposition, write letters of message out in rows over a specified number of columns, then reorder the columns according to some key before reading off the rows.

m: attackposponeduntiltwoam

Key: f_e[4 3 1 2 5 6 7]



f_d=[3 4 2 1 5 6 7]

Key:	1	2	3	4	5	6	7		4	3	1	2	5	6	7
Plaintext:	a	t	t	a	c	k	p		a	t	a	t	c	k	p
	o	s	t	p	o	n	e		p	t	o	s	o	n	e
	d	u	n	t	i	l	t		t	n	d	u	i	l	t
	w	o	a	m	*	*	*		m	a	w	o	*	*	*

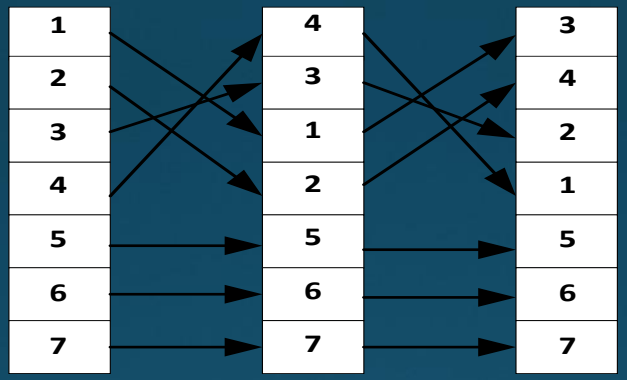
Ciphertext: ATATCKPPTOSONETNDUILTMAWO***

Row Transposition Decryption

Decryption: Generate reverse function for decryption: then reorder the columns according to decryption key before reading off the rows

Ciphertext: ATATCKPPTOSONETNDUILTMAWO***

Key: f_e[4 3 1 2 5 6 7]



f_d=[3 4 2 1 5 6 7]

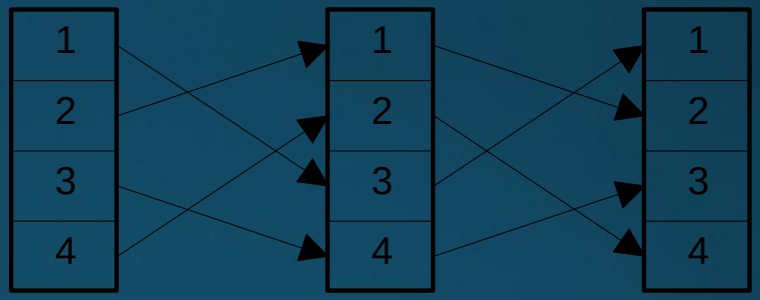
Key:	4	3	1	2	5	6	7		3	4	2	1	5	6	7
Ciphertext :	a	t	a	t	c	k	p		a	t	t	a	c	k	p
	p	t	o	s	o	n	e		o	s	t	p	o	n	e
	t	n	d	u	i	l	t		d	u	n	t	i	l	t
	m	a	w	o	*	*	*		w	o	a	m	*	*	*

plaintext: ATTACKPOSPONEDUNTILTWOAM***

Column Transposition Ciphers

1. Fill the matrix ,
2. Rearrange the matrix columns as in key (Fe)
3. Read encrypted message by columns

"RENAISSANCE" using 3x4 figure, using [2 4 1 3] scheme.



f E[2 4 1 3] f D[3 1 4 2]

1	2	3	4	2	4	1	3
R	**E**	**N**	**A**	**E**	**A**	**R**	**N**
I	S	S	A	S	A	I	S
N	**C**	**E**	*****	**C**	*****	**N**	**E**

Ciphertext: ESCAA*RINNSE.

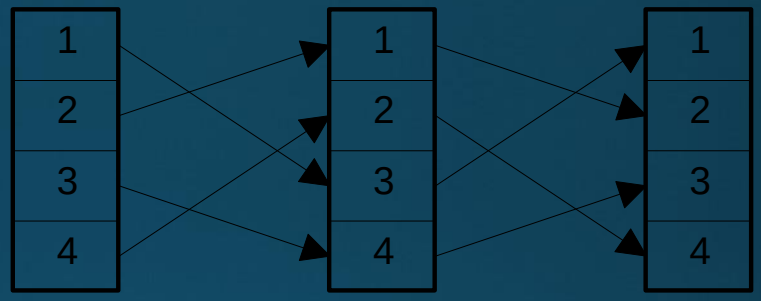
Column Transposition Decrtption

Generate reverse function for decryption:

Ciphertext: ESCAAXRINNSE

1	2	3	4
E	A	R	N
S	A	I	S
C	*	N	E

3	1	4	2
R	E	N	A
I	S	S	A
N	C	E	*



$f_E[2\,4\,1\,3]$ $f_D[3\,1\,4\,2]$

Ciphertext: RENAISSANCE*

Hill Cipher

Each letter is represented by a number modulo 26. Though this is not an essential feature of the cipher, this simple scheme is often used:

To encrypt a message, each block of *n* letters (considered as an *n*-component vector) is multiplied by an invertible *n* × *n* matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

	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
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

We have to encrypt the message 'ACT' (n=3). The key is 'GYBNQKURP', which in the form of an nxn matrix looks like below:

Hill Cipher

Message = ACT

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

Key = GYBNQKURP

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Ciphertext

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$ = POH

Plaintext

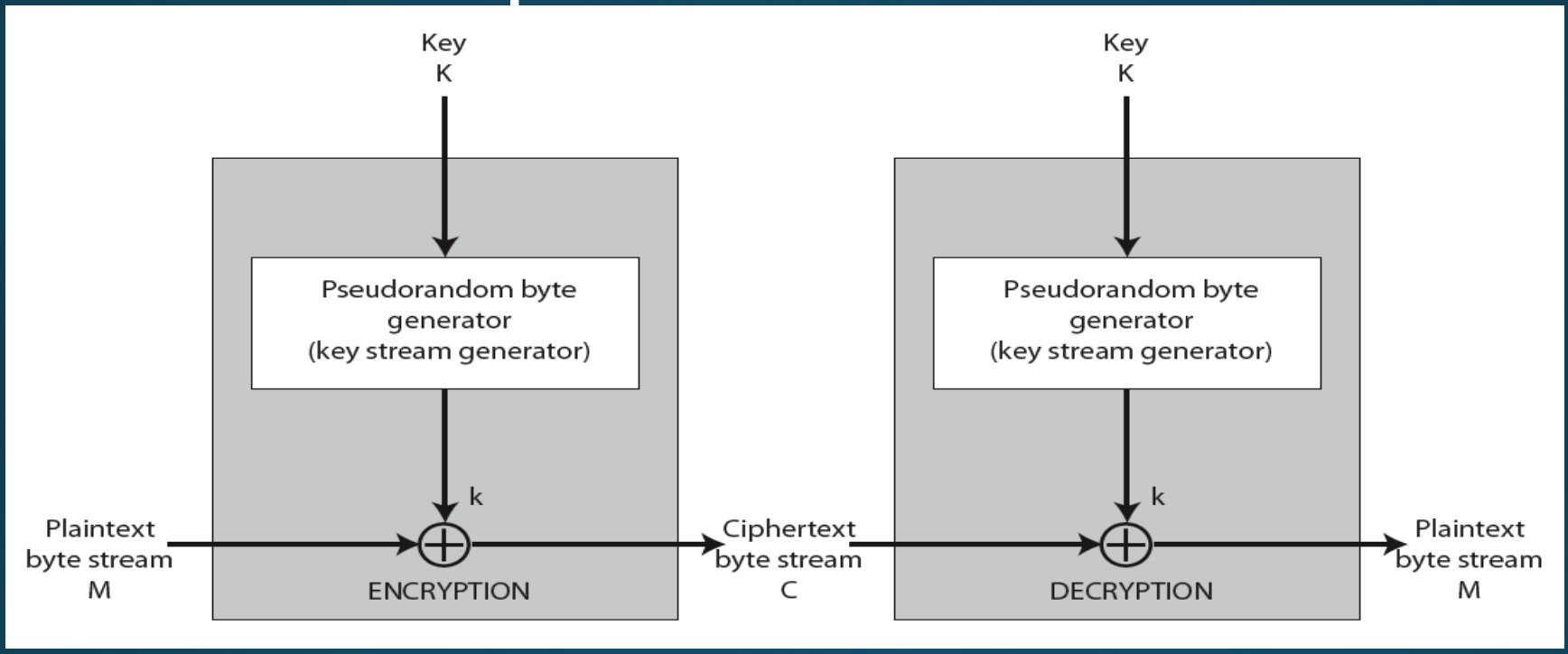
$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$ = ACT

One-Time pad

the **one-time pad** (**OTP**) is an encryption technique that cannot be cracked, but requires the use of a single-use pre-shared key that is larger than or equal to the size of the message being sent. In this technique, a plaintext is mixed with a random secret key (also referred to as *a one-time pad*). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. Must met the conditions:

1. The key must be at least as long as the plaintext.
2. The key must be random.
3. The key must never be reused in whole or in part.
4. The key must be kept completely secret by the communicating parties

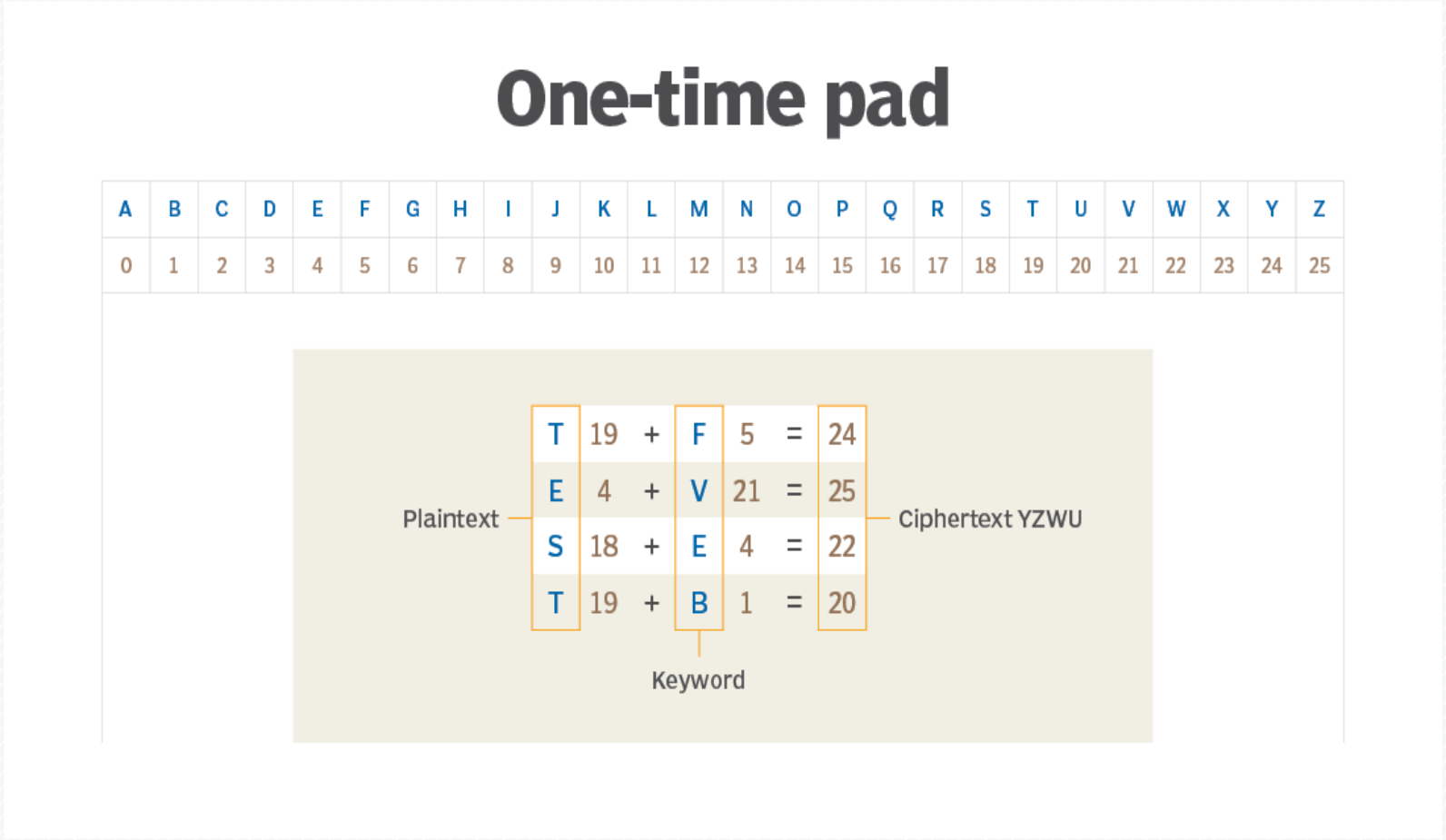
One-Time pad



Plain text: T H I S I S S E C R E T
OTP-Key : X V H E U W N O P G D Z

Ciphertext: Q C P W C O F S R X H S
In groups : QCPWC OFSRX HS

One-Time pad


One-time pad
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
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
Plaintext
T 19 + F 5 = 24
E 4 + V 21 = 25
S 18 + E 4 = 22
T 19 + B 1 = 20
Ciphertext YZWU
Keyword
SOURCE: ANDREW FROEHLICH
©2022 TECHTARGET. ALL RIGHTS RESERVED
TechTarget