CYB 241 Digital Cryptography Techniques

Classical Encryption Techniques

Definitions

Plaintext

- An original message

Ciphertext

- The coded message

Enciphering/encryption

- The process of converting from plaintext to ciphertext

Deciphering/decryption

- Restoring the plaintext from the ciphertext

Secret Key

- used to set some or all of the various parameters used by the encryption algorithm.

Cryptography

- The area of study of the many schemes used for encryption

Cryptographic system/cipher

- A scheme for encryption and decryption

Cryptanalysis

- Techniques used for deciphering a message without any knowledge of the enciphering details

Cryptology

- The areas of cryptography and cryptanalysis

Symmetric Encryption

- Symmetric
  - uses same key for encryption, decryption
- Other names
  - classical , conventional , single-key encryption
- Was the only type of encryption in use prior to the development of public-key encryption in the 1970s
- Remains most widely used

Simplified Model

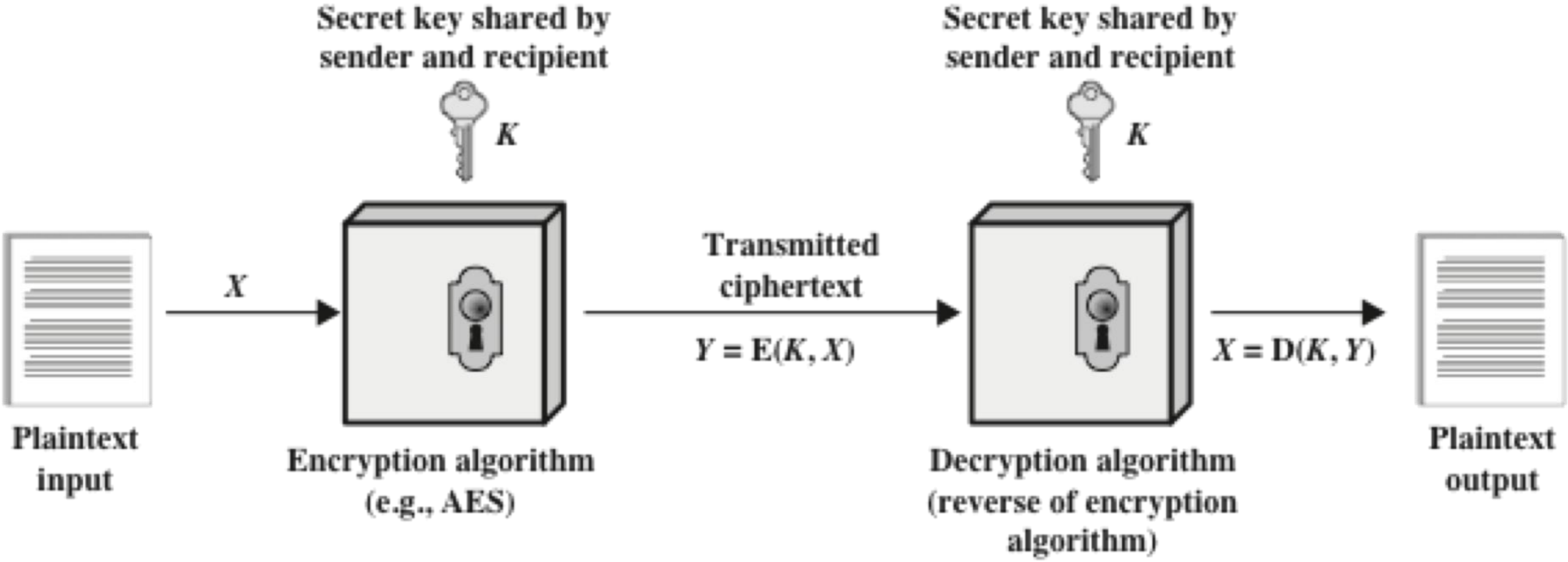

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
$Y = E(K, X)$
$X = D(K, Y)$
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 3.1 Simplified Model of Symmetric Encryption

Symmetric Cipher Model

- There are two requirements for secure use of conventional encryption:
  - A strong encryption algorithm
    - Impractical to decrypt by only knowing ciphertext and algorithm
    - Algorithm need not to be kept secret
      - allows widespread use
      - low-cost manufacturing
  - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure

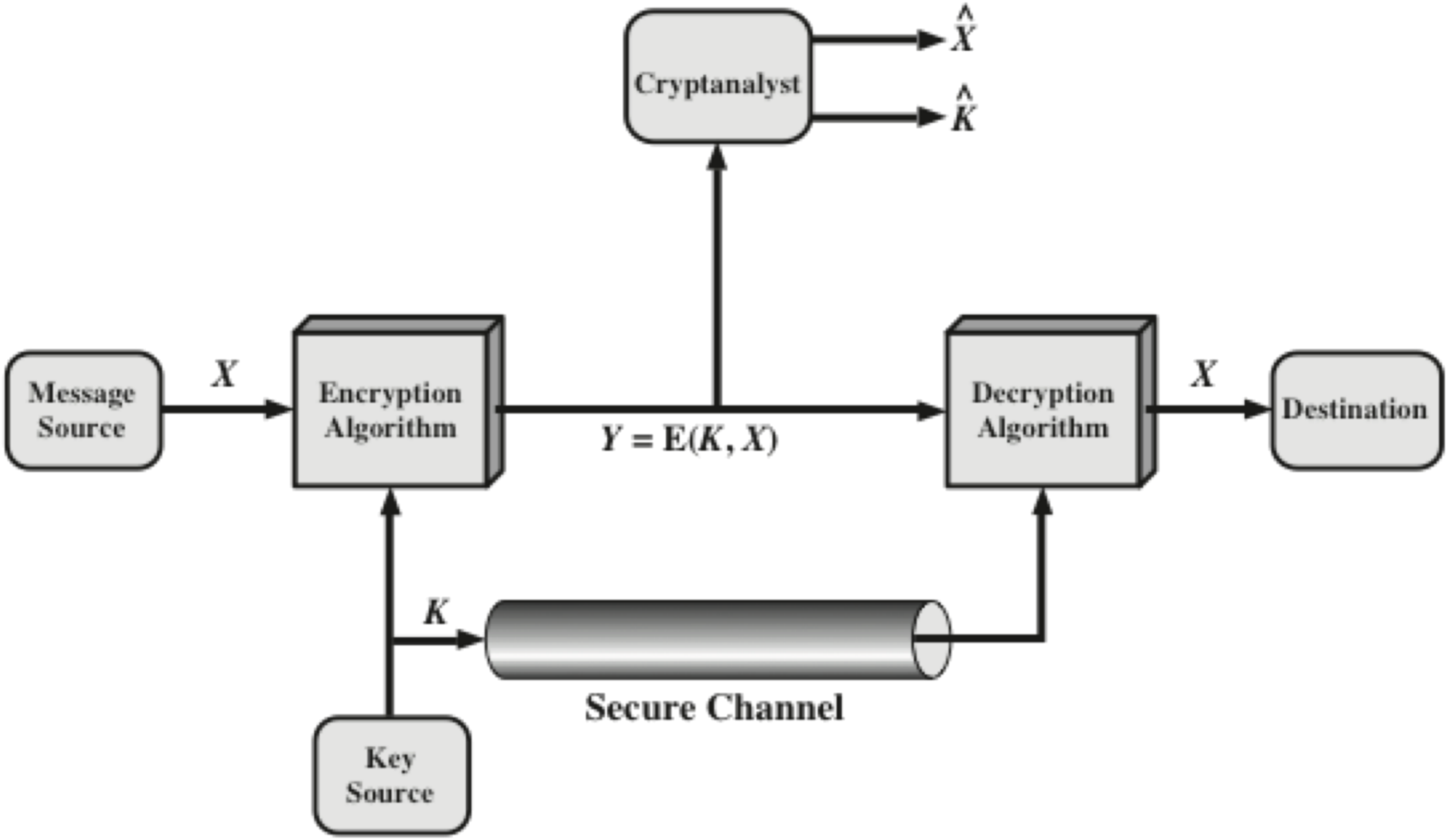


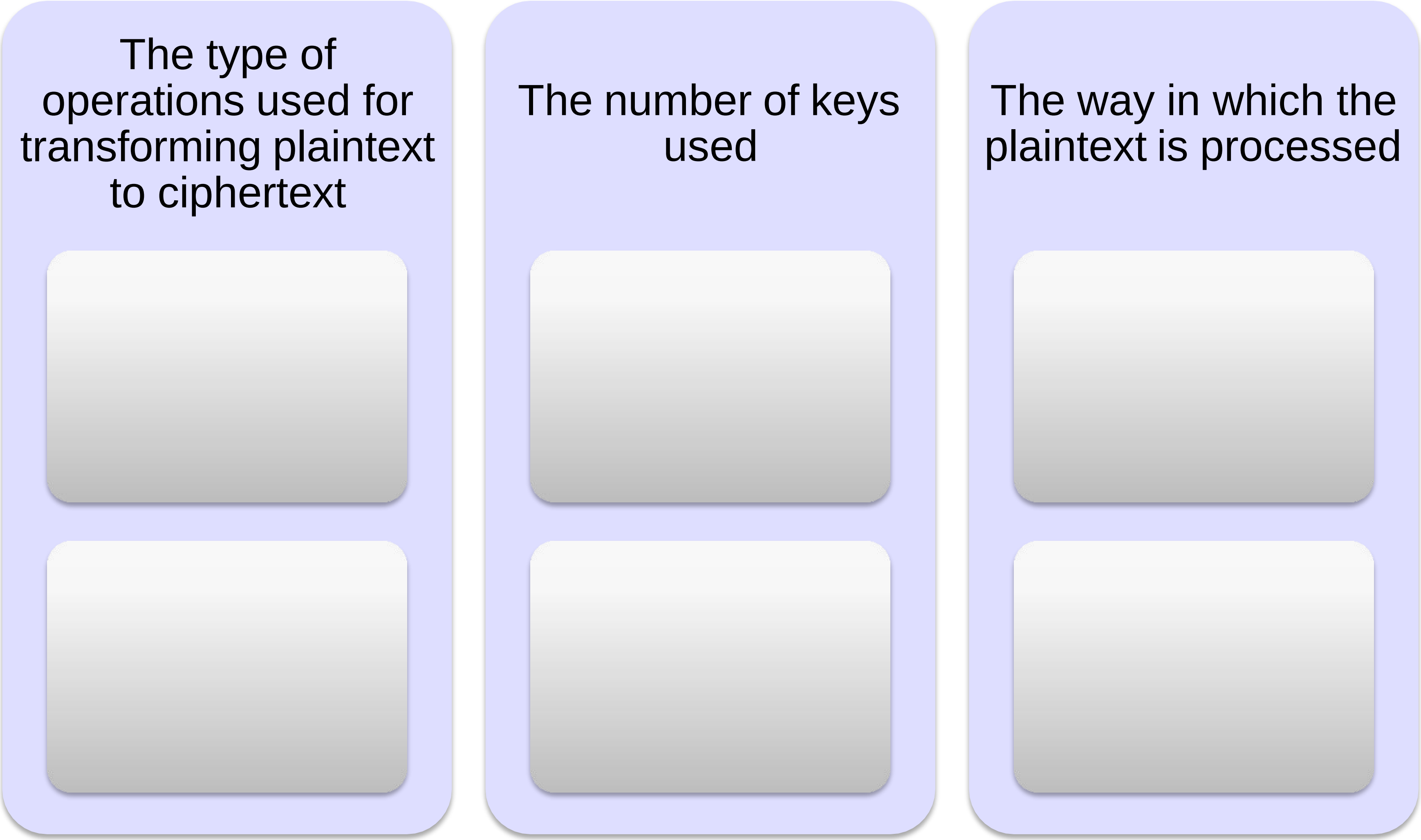
Figure 3.2 Model of Symmetric Cryptosystem

Notation

- $Y = E(K, X)$ or $Y = E_K(X)$
- $X = D(K, Y)$ or $X = D_K(Y)$
- $\hat{X}$:estimate of plaintext
- $\widehat{K}$: estimate of key
- Which is higher risk?
  - □ Attacker infers the plaintext.
  - □ Attacker infers the secret key.

Cryptographic Systems

- Characterized along three independent dimensions:



The type of operations used for transforming plaintext to ciphertext

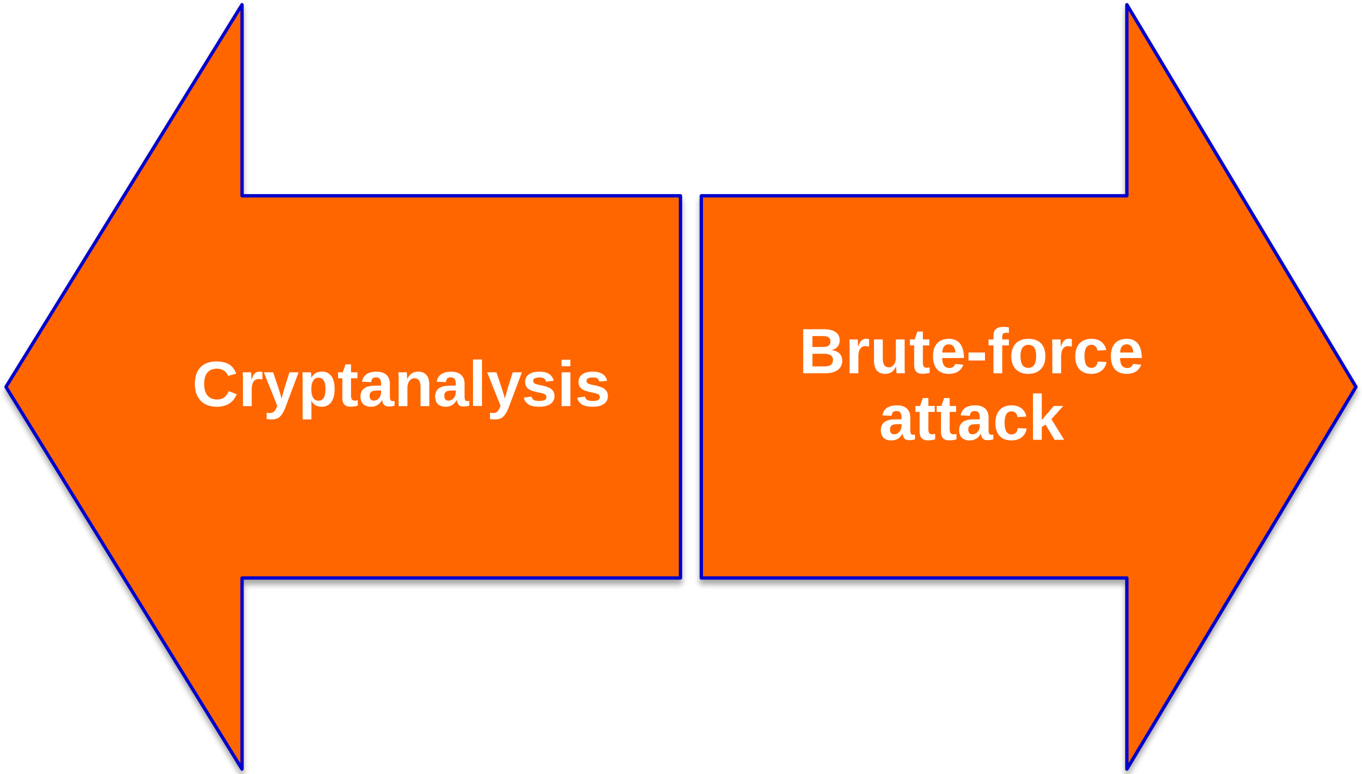
The number of keys used

The way in which the plaintext is processed

Characterization

- Type of operation
  - Substitution: each element of plaintext (bit, character) mapped to another element
  - Transposition: plaintext elements rearranged
- Number of keys used
  - symmetric: same key for sender, receiver
  - asymmetric/public-key: different keys
- Processing method
  - Stream cipher: element by element (bit, byte)
  - Block cipher: block transformed as a whole

Encryption Attacks



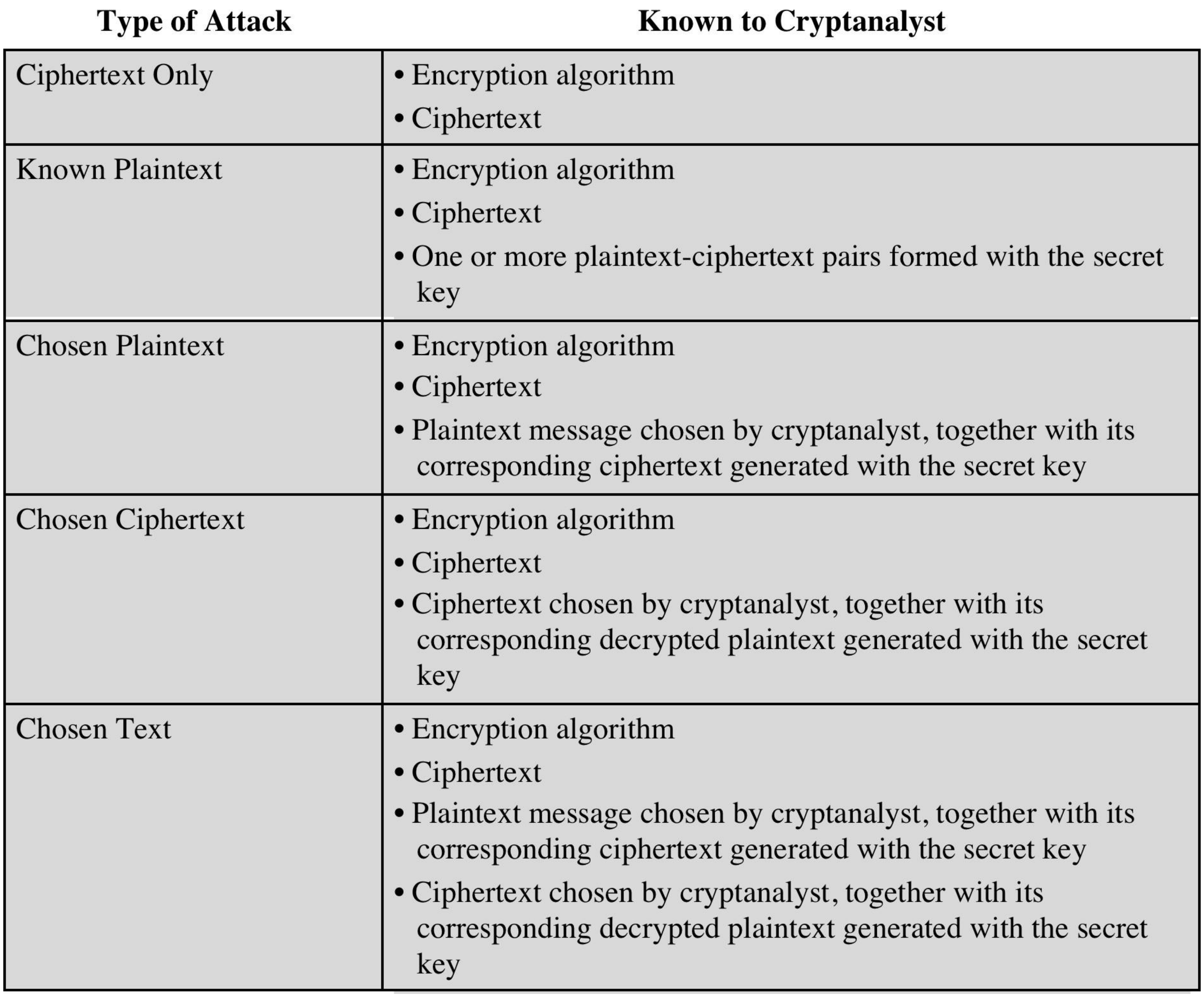
Cryptanalysis

Brute-force attack

Cryptanalysis Attacks

- Attempt to deduce specific plaintext or key
- Rely on
  - nature of algorithm
  - some knowledge of plaintext characteristics
  - may use sample plaintext-ciphertext pairs
- Examples
  - some file types have common header
  - exploit statistics of human language
  - power consumed by encryption algorithm

Cryptanalysis Attacks



Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

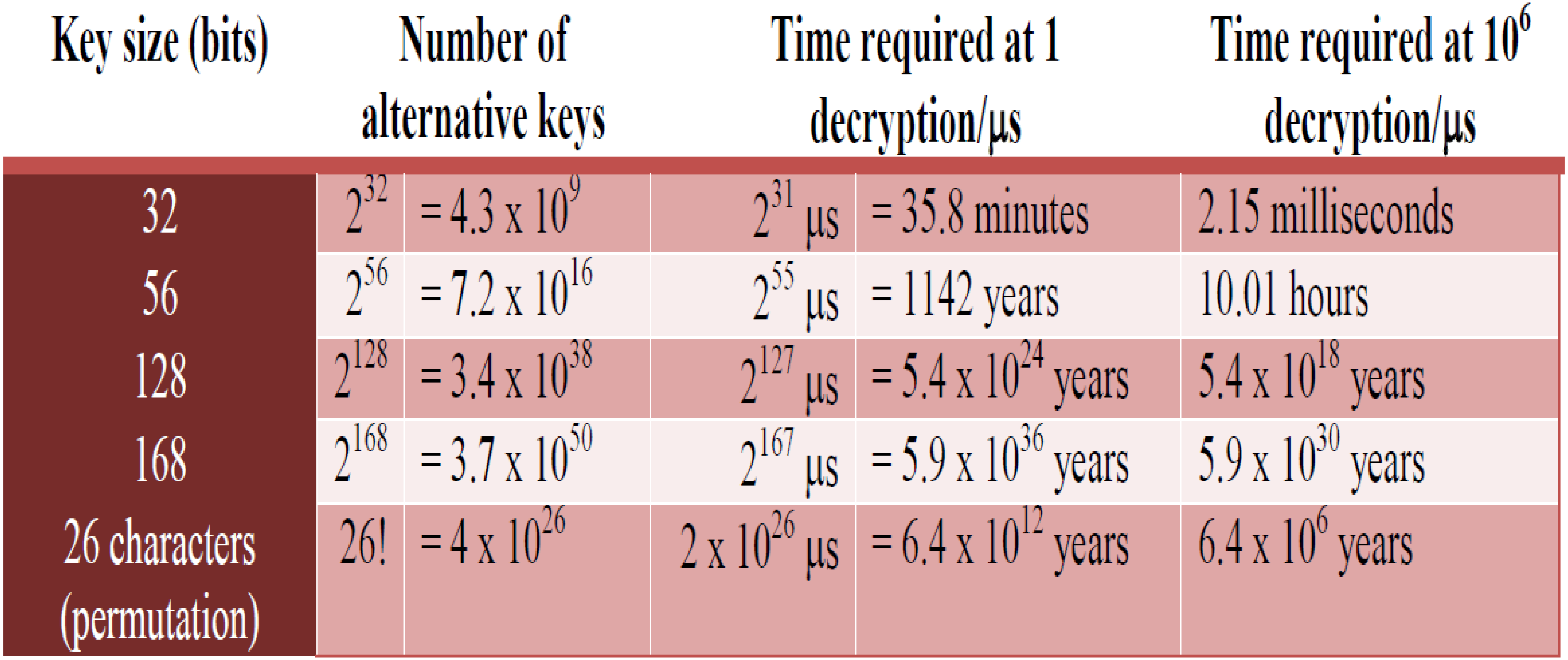
Encryption Scheme Security

- Unconditionally secure
  - unbreakable cipher
  - no matter how much time is available
  - only one algorithm: one-time pad
- Computationally secure
  - time required to break cipher exceeds the time data is useful
  - cost of breaking cipher exceeds value of data

Brute-Force Attacks

- Try all possible keys
- On average, half of keys are attempted
- Some degree of knowledge about the expected plaintext is needed
- Must be able to recognize plaintext
  - Human language
  - header of known file type
  - file format, checksum, …

Brute Force Attacks



Key size (bits)	Number of alternative keys		Time required at 1 decryption/µs		Time required at 10^6 decryption/µs
32	2^{32}	$= 4.3 \times 10^{9}$	2^{31} µs	= 35.8 minutes	2.15 milliseconds
56	2^{56}	$= 7.2 \times 10^{16}$	2^{55} µs	= 1142 years	10.01 hours
128	2^{128}	$= 3.4 \times 10^{38}$	2^{127} µs	$= 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	2^{168}	$= 3.7 \times 10^{50}$	2^{167} µs	$= 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	26!	$= 4 \times 10^{26}$	2×10^{26} µs	$= 6.4 \times 10^{12}$ years	6.4×10^{6} years

Questions

- What is the easier cryptanalysis attack
  - □ Ciphertext only
  - □ Chosen Plaintext

Substitution Techniques

- Letters in plaintext is replaced by
  - other letters
  - numbers
  - symbols
- Plaintext bit-sequence is replaced by a ciphertext sequence

Substitution Techniques

- Caesar cipher
- Monoalphabetic ciphers
- Playfair cipher
- Polyalphabetic ciphers

Caesar Cipher

- Simplest and earliest known use of a substitution cipher
- Used by Julius Caesar
- Involves replacing each letter of the alphabet with the letter standing three places further down the alphabet
- Alphabet is wrapped around so that the letter following Z is A

plain: `MEET ME AFTER THE TOGA PARTY`

cipher: `PHHW PH DIWHU WKH WRJD SDUWB`

Caesar Cipher Algorithm

- Can define transformation as:

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
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

- Mathematically give each letter a number

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

- Algorithm can be expressed as:

$$c = \mathrm{E}(3, p) = (p + 3) \bmod (26)$$

- A shift may be of any amount, so that the general Caesar algorithm is:

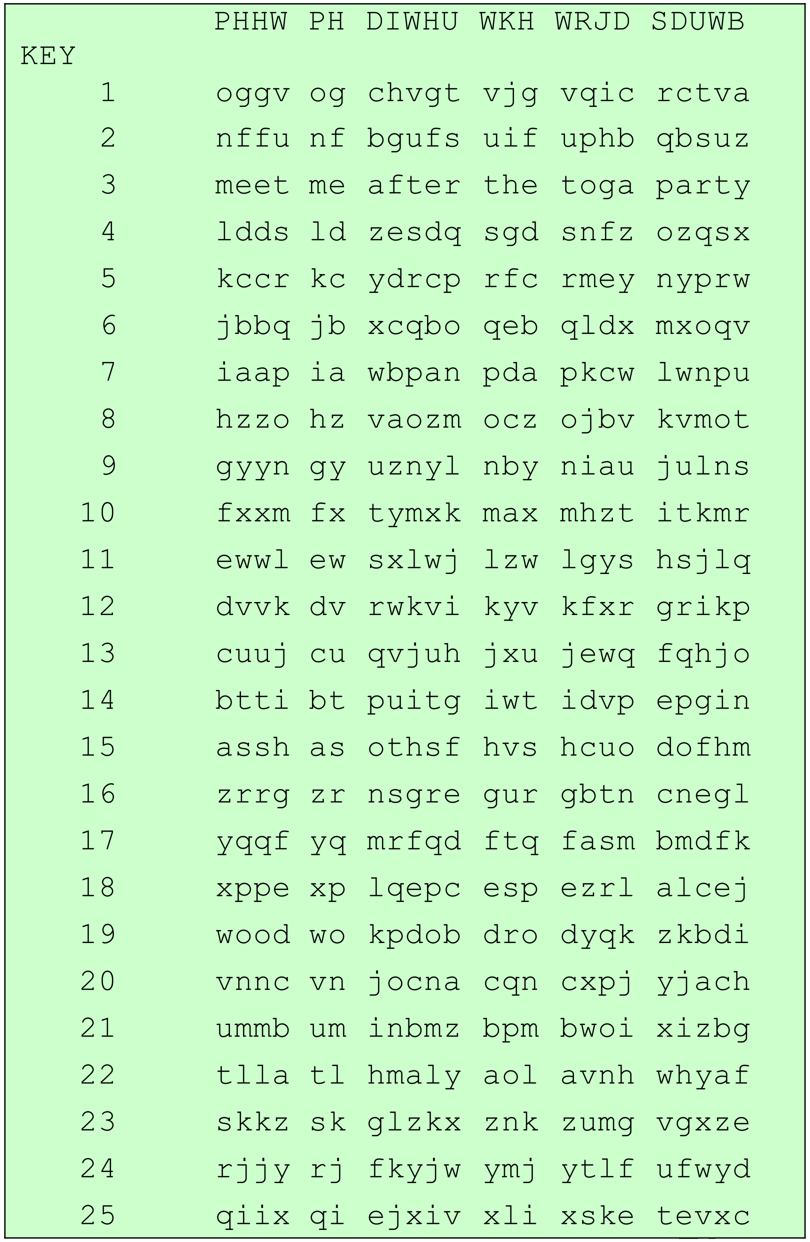
$$C = E(k, p) = (p + k) \bmod 26$$

- Where k takes on a value in the range 1 to 25; the decryption algorithm is simply:

$$p = D(k, C) = (C - k) \bmod 26$$

Brute Force Attack

- Why it is easy to use brute force attack?
  - □ Encryption and decryption algorithms are known
  - □ Only 25 keys to try
  - □ Plaintext language is known



KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrcp	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

Monoalphabetic Cipher

- Use arbitrary substitution of letters where cipher can be any *permutation* of the 26 alphabetic characters
- Permutation
  - Of a finite set of elements *S* is an ordered sequence of all the elements of *S* , with each element appearing exactly once
- Then there are 26! or greater than 4 x 10^{26} possible keys
- Regularities in the language can be exploited

Monoalphabetic – Example

Ciphertext:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

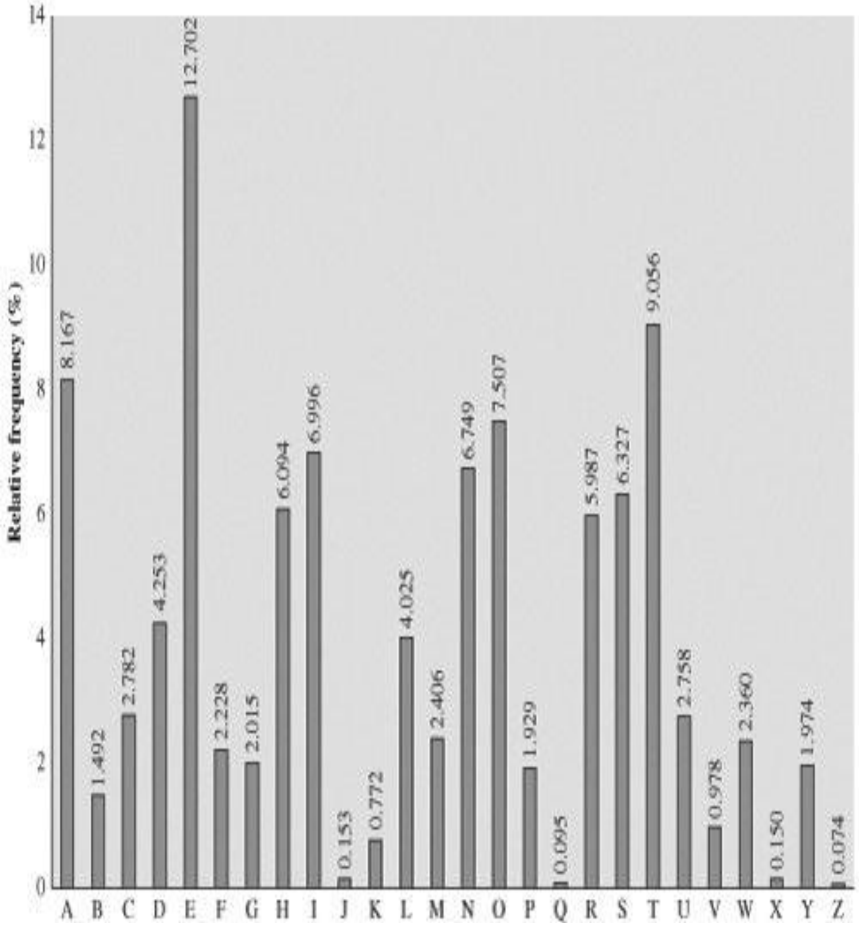
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

Relative frequency of letters in Ciphtertext

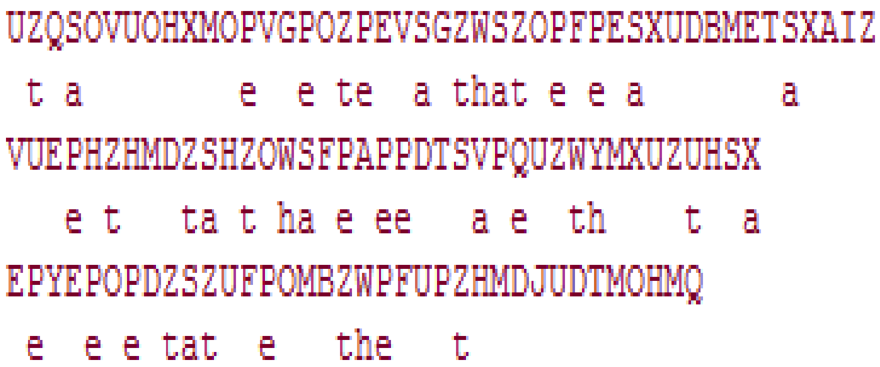
P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

Relative frequency of letters in English text

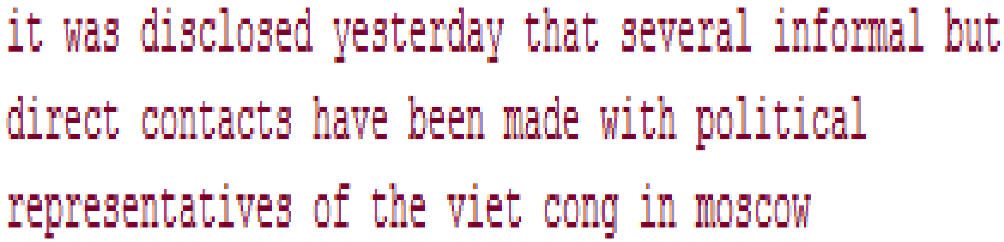


Monoalphabetic – Example

- Frequency of letters
  - □ P → e, Z → t
- Frequency of two-letter combinations
  - □ ZW → th

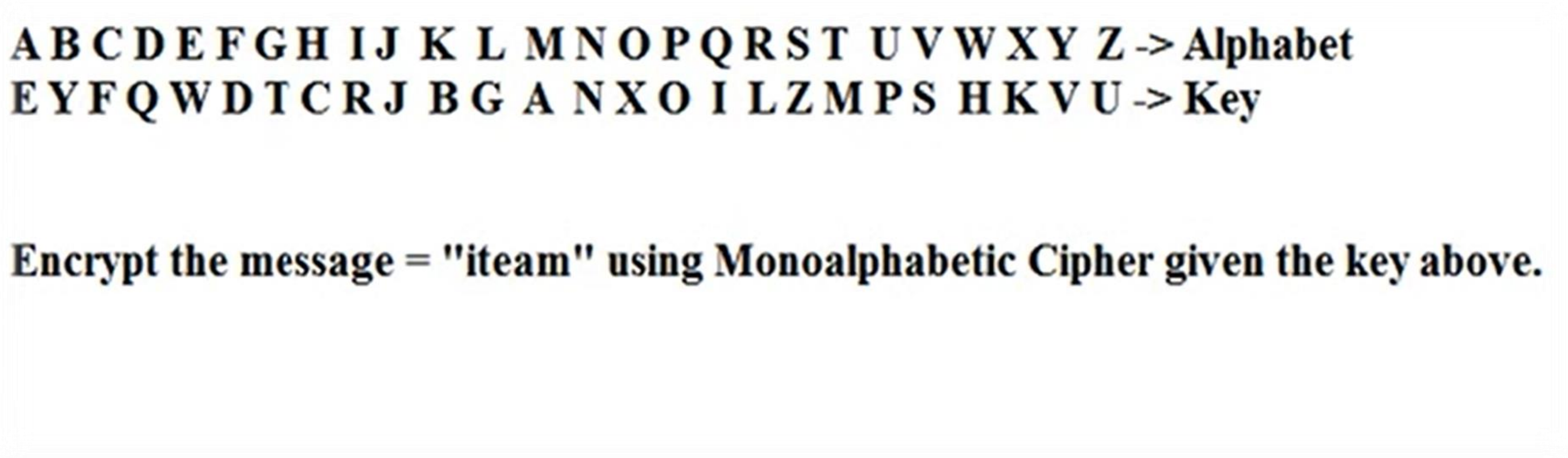


```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a        e  e te  a that e e a       a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t   ta t ha e ee  a e  th    t  a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the   t
```



it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow

Example 2 :

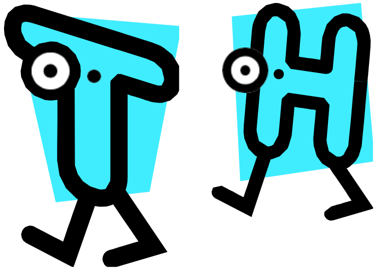


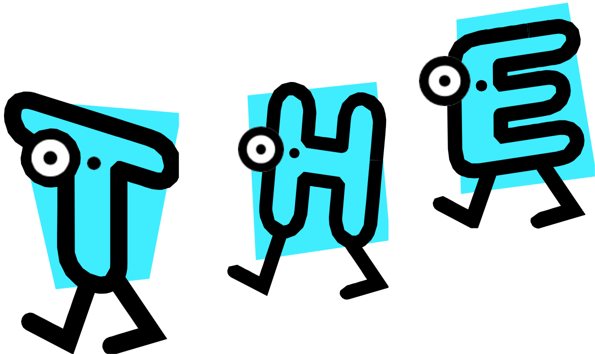
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z -> Alphabet
E Y F Q W D T C R J B G A N X O I L Z M P S H K V U -> Key

Encrypt the message = "iteam" using Monoalphabetic Cipher given the key above.

Monoalphabetic Ciphers

- Easy to break because they reflect the frequency data of the original alphabet
  - □ Countermeasure is to provide multiple substitutes (homophones) for a single letter
- Digram
  - □ Two-letter combination
  - □ Most common is *th*
- Trigram
  - □ Three-letter combination
  - □ Most frequent is *the*





Playfair Cipher

- Best-known multiple-letter encryption cipher
- Treats digrams in the plaintext as single units and translates these units into ciphertext digrams
- Based on the use of a 5 x 5 matrix of letters constructed using a keyword
- Invented by British scientist Sir Charles Wheatstone in 1854
- Used as the standard field system by the British Army in World War I and the U.S. Army and other Allied forces during World War II

Playfair Key Matrix

- Fill in letters of keyword (minus duplicates) from left to right and from top to bottom, then fill in the remainder of the matrix with the remaining letters in alphabetic order
- 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

Playfair Rules

- Divide the plaintext into a group of 2 of plaintext characters.
- For any given pair of plaintext characters, you use the following three rules
  1. Two plaintext letters that fall in the same row of the matrix are replaced by letters to the right, with the first element of the row circularly following the last.
  2. Two plaintext letters that fall in the same column are replaced by the letters just below them in the column, with the top element of the column circularly following the last.
  3. Otherwise, for each plaintext letter in a pair, replace it with the letter that is in the same row but in the column of the other letter.
- If any pair of plaintext has consecutive identical letters, insert X in between
  - □ example: WILL → WILXL
- If the plaintext length is odd, insert X at the end.
  - □ example: THE → THEX

Playfair Example

LXLO

HELLO

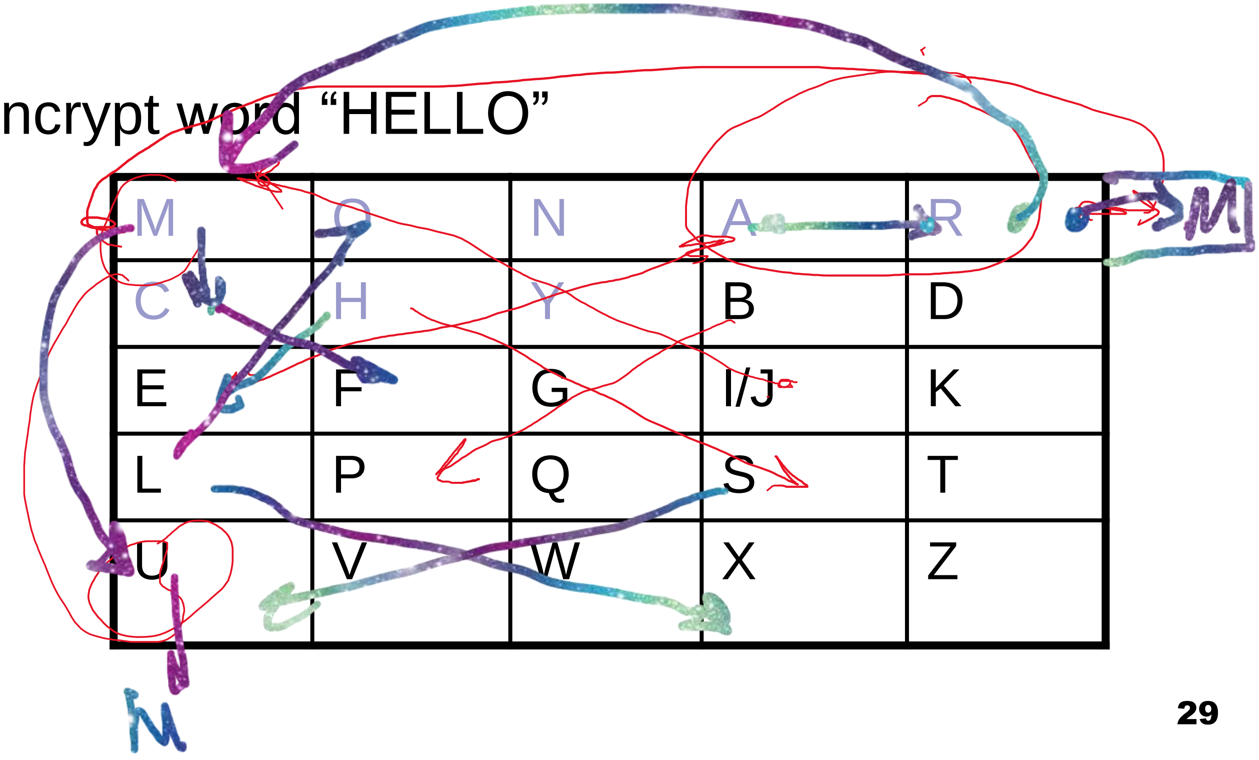
CFSU

HE LXLO

CF SU PM

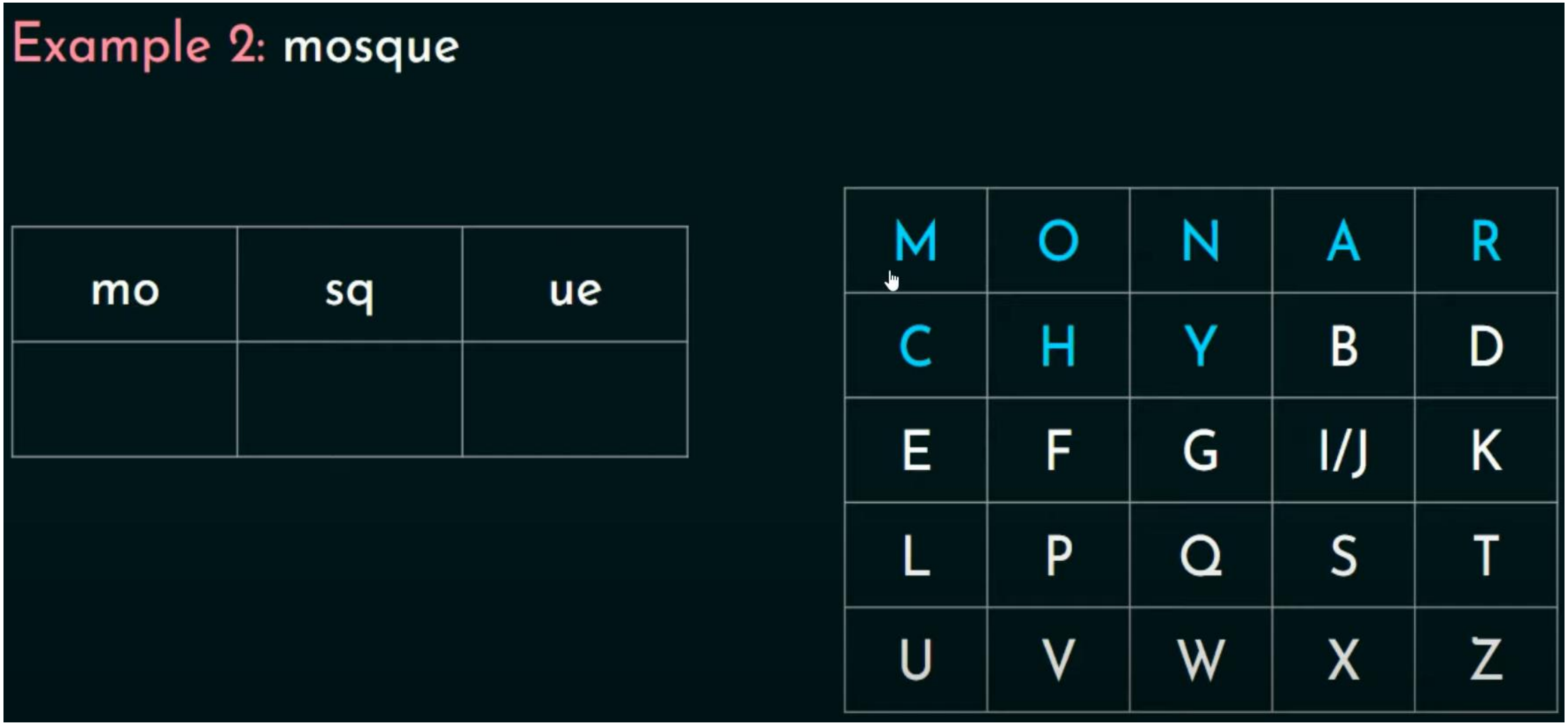
- Example:
  - □ AR is encrypted as RM. *(rule 1)*
  - □ MU is encrypted as CM. *(rule 2)*
  - □ HS becomes BP and EA becomes IM (or JM). *(rule 3)*

- Let’s try the encrypt word “HELLO”



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

Playfair Example 2



Example 2: mosque

mo	sq	ue

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

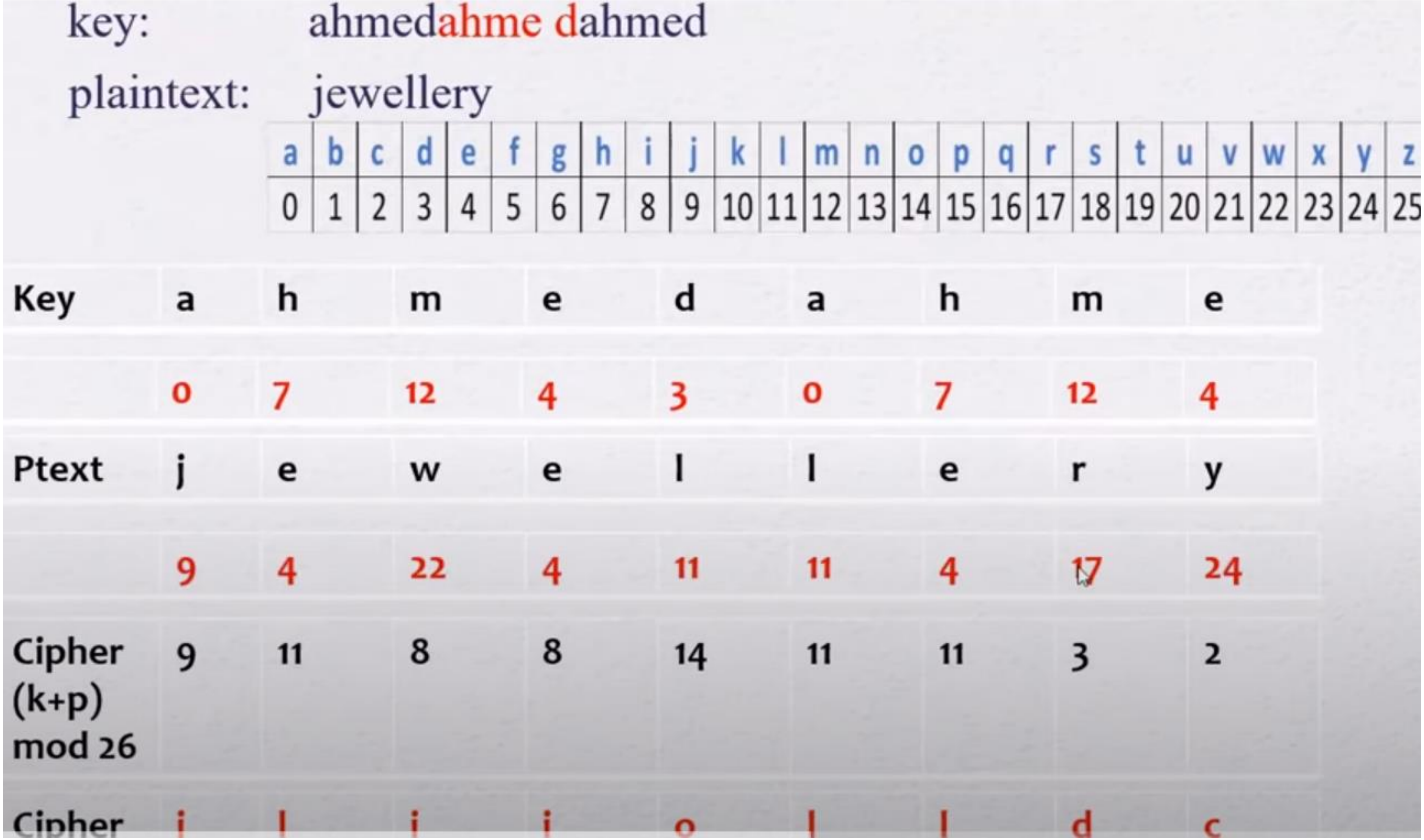
Polyalphabetic Ciphers

- Different monoalphabetic substitutions for different parts of plaintext
- Set of monoalphabetic substitution rules
- Key determines rule used for each part
- Flatter letter frequency, harder cryptanalysis
- Best known example: Vigenère cipher

Vigenère Cipher

- 26 Caesar ciphers
- Using keys 0 to 25
- Each denoted by key letter (0=a, 1=b, …)
- Arranged in a matrix (Vigenère tableau)
- Key constructed from keyword
- Repeated to match length of plaintext
- Ciphertext letter = intersection of:
  - row of plaintext letter
  - column of key letter

Example :



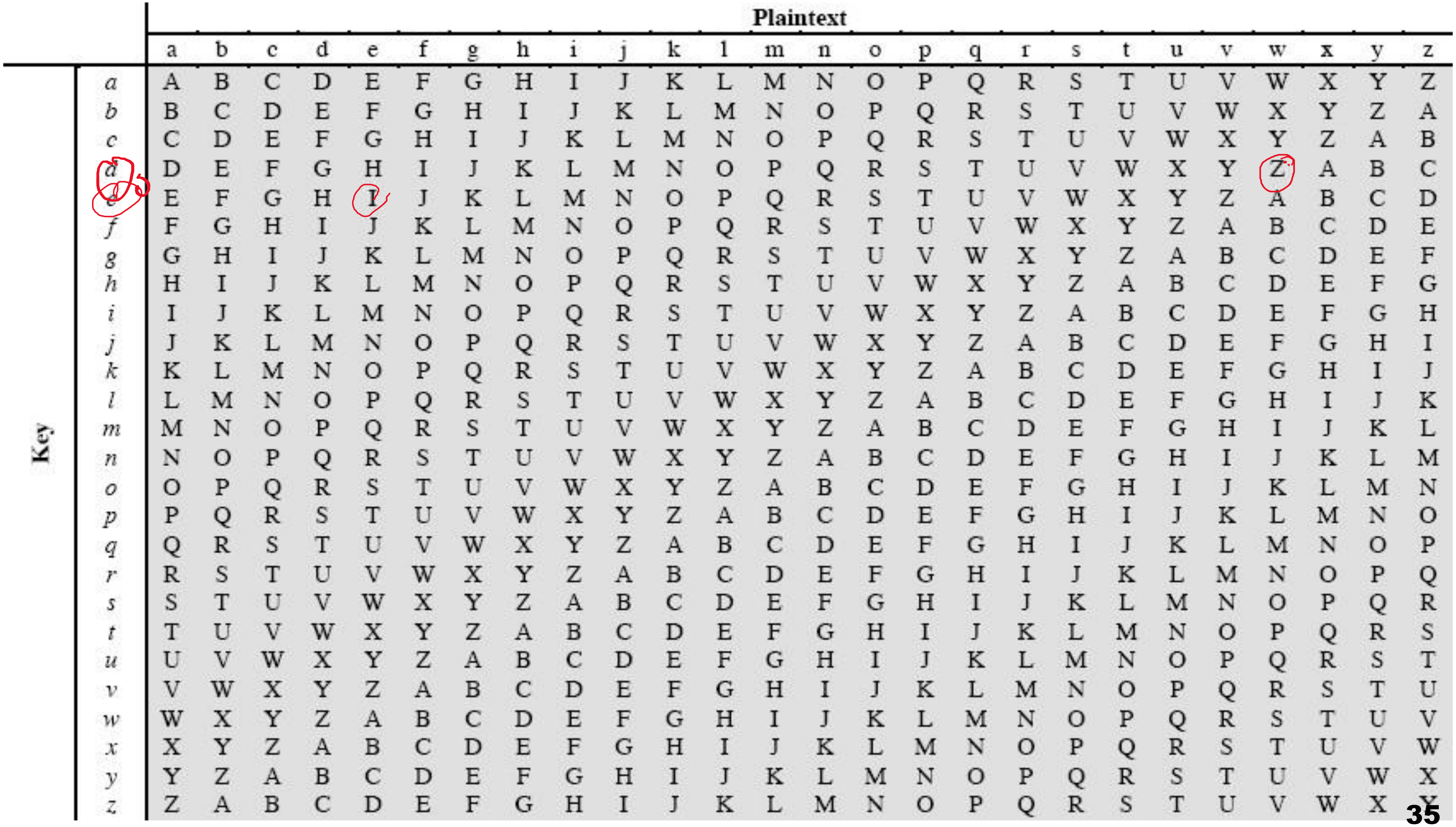
key: ahmedahme dahmed

plaintext: jewellery

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

Key	a	h	m	e	d	a	h	m	e
	0	7	12	4	3	0	7	12	4
Ptext	j	e	w	e	l	l	e	r	y
	9	4	22	4	11	11	4	17	24
Cipher (k+p) mod 26	9	11	8	8	14	11	11	3	2
Cipher	j	l	i	i	o	l	l	d	c

Vigenère Tableau



	Plaintext																									
Key	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

Example

- Keyword: deceptive
- Plaintext: we are discovered save yourself

Keyword	deceptive
Key	deceptivedeceptivedeceptive
Plaintext	wearediscoveredsaveyourself
Ciphertext	ZICVTWQNGRZGVTWAVZHCQYGLMGJ

One-time Pad

- Invented by Vernam in the 1920s
- Fix the vulnerability of the Vigenere cipher by using very long keys
- Key is a random string that is at least as long as the plaintext
- Operation:
  - □ Using Vigenere **key size = plaintext size**

One-time Pad

- There are many different versions and ways of describing the perfectly secure cipher system most often described as the **one-time pad**. However these all have the same three essential properties:
  - The number of possible keys is equal to the number of possible plaintexts.
  - The key is selected at random from the choice of all possible keys.
  - Any key should only be used once.

One-time Pad

offers complete security but, in practice, has two fundamental difficulties:

- ❑ There is the practical problem of making large quantities of random keys.
- ❑ The problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver.

so ,it has limited utility and is useful primarily for low-bandwidth channels requiring very high security. **The one-time pad is the only cryptosystem that exhibits what is referred to as**

perfect secrecy

The Binary One-Time Pad

- Plaintext space = Ciphtertext space
- Key is chosen randomly
- Using XOR for encryption and decryption
- For example:
  - □ Plaintext is 11011011
  - □ Key is 01101001
  - □ Then ciphertext is 10110010

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

Transposition Techniques

- Perform some permutations on plaintext letters
  - Rail fence
  - Transposition Matrix

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:

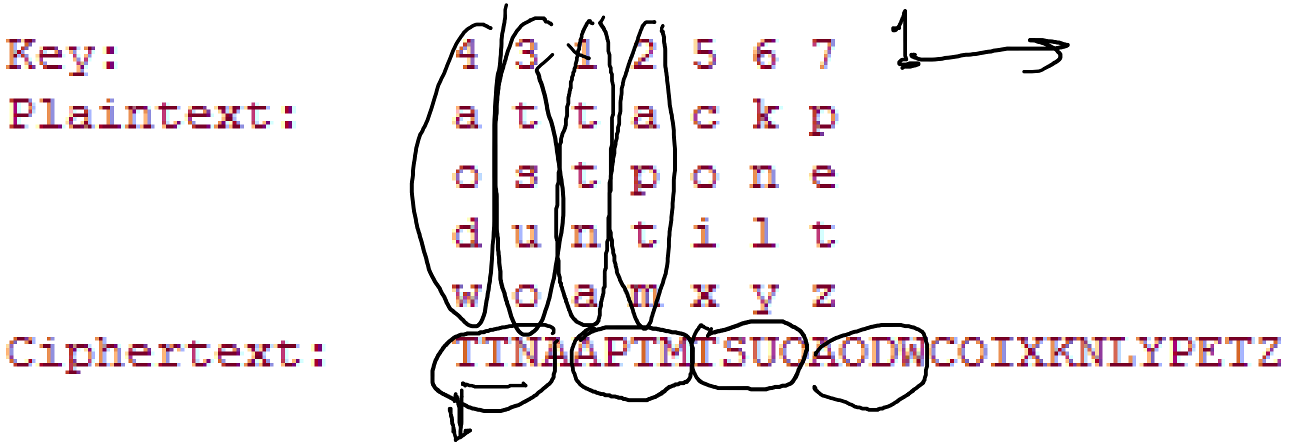
```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

The encrypted message is

```
MEMATRHTGPRYETEFETEOAAT
```

Transposition Matrix

- Write message in rectangle, row by row
- Permute order of columns
- Order of columns is the key
- Read message off, column by column



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

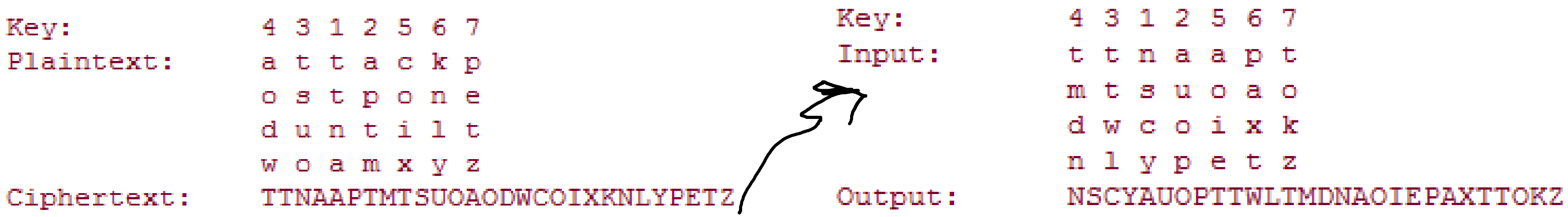
Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Transposition Matrix

- Original order of letters
  - 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 transposition
  - 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
- Somewhat regular structure

Transposition Matrix

- More than one stage of transposition



```
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
```

```
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
```

  - After second transposition
  - 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
  - Much less structured

Reading Assignment

- Textbook
  - chapter 3
    - 3.1
    - 3.2
      - Caesar Cipher
      - Monoalphabetic Ciphers
      - Playfair Cipher
      - Polyalphabetic Ciphers
    - 3.3
      - Transposition matrix