BK
TP.HCM

Cryptography and Network Security

2. Symmetric Ciphers

Lectured by
Nguyễn Đức Thái

Outline

- Symmetric Encryption
- Substitution Techniques
- Transposition Techniques
- Steganography

Symmetric Encryption

- There are two requirements for secure use of conventional encryption:
  - We need a strong encryption algorithm.
  - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

Symmetric Cipher Model

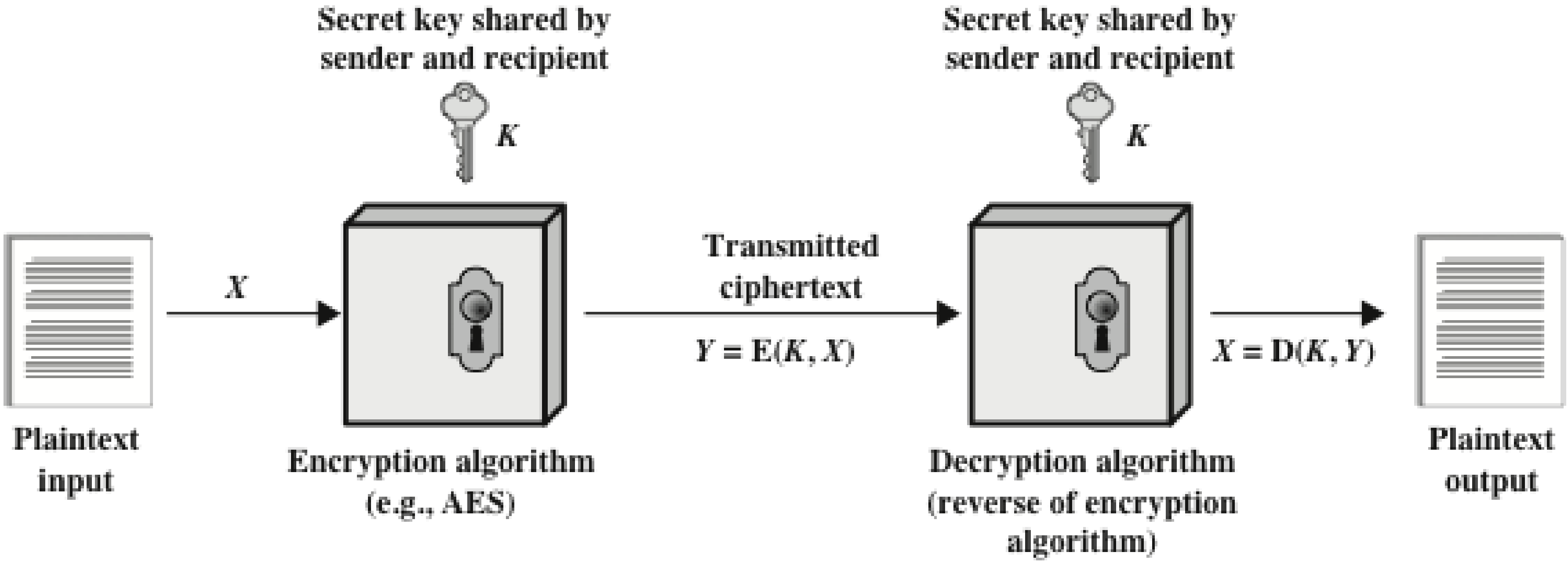

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2.1 Simplified Model of Symmetric Encryption

Symmetric Encryption: Requirements

- **Two requirements for secure use of symmetric encryption:**
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- **Mathematically have:**

  $Y = E(K, X) = E_K(X) = \{X\}_K$

  $X = D(K, Y) = D_K(Y)$
- **Assume encryption algorithm is known**
  - Kerckhoff’s Principle: security in secrecy of key alone, not in obscurity of the encryption algorithm
- **Implies a secure channel to distribute key**
  - Central problem in symmetric cryptography

Cryptography

- **Cryptographic systems are characterized by:**
  - type of encryption operations used
    - substitution
    - transposition
    - product: involve multiple stages of substitutions and transpositions.
  - number of keys used
    - single-key or private
    - two-key or public
  - way in which plaintext is processed
    - block
    - stream

Model of Symmetric Cryptosystem

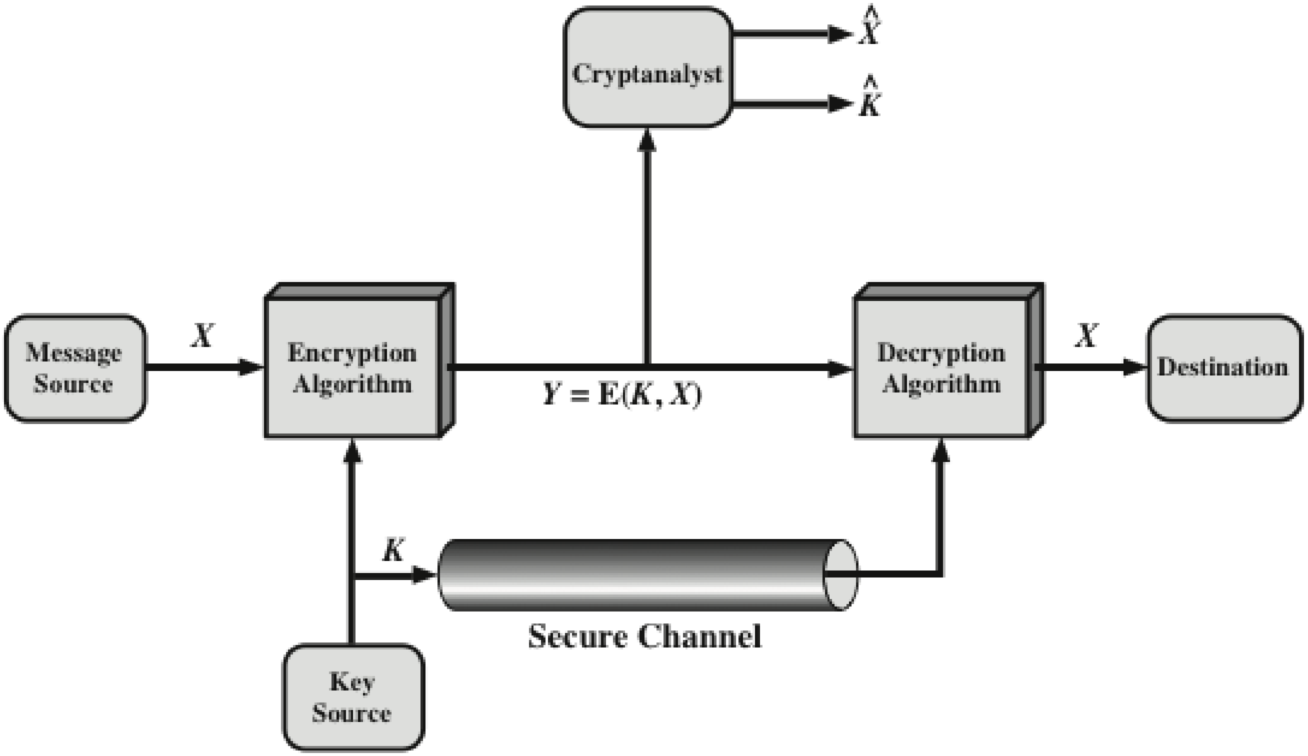
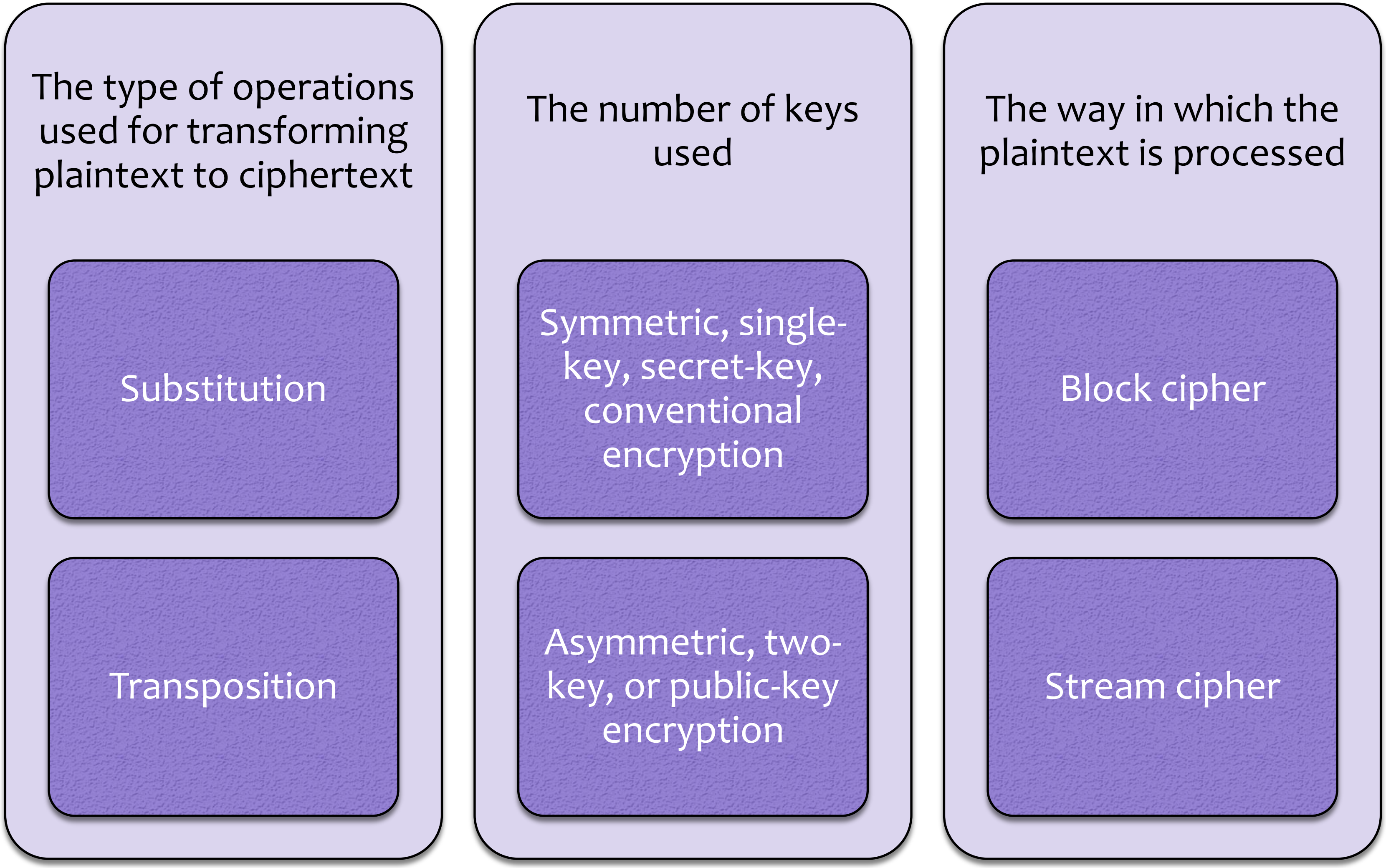


Figure 2.2 Model of Symmetric Cryptosystem

Cryptographic Systems



The type of operations used for transforming plaintext to ciphertext

Substitution

Transposition

The number of keys used

Symmetric, single-key, secret-key, conventional encryption

Asymmetric, two-key, or public-key encryption

The way in which the plaintext is processed

Block cipher

Stream cipher

Cryptanalysis and Brute-Force Attacks

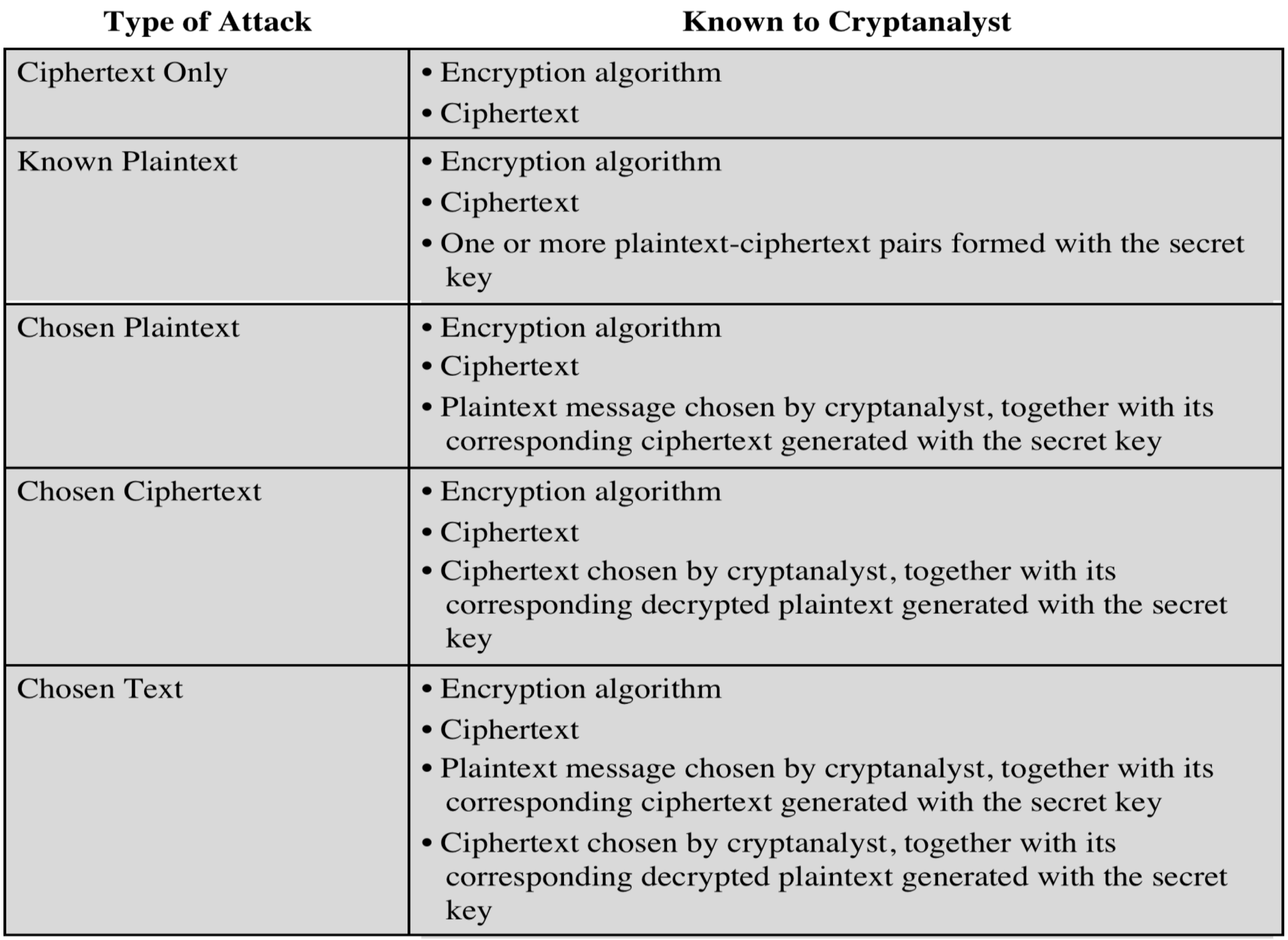
Cryptanalysis

- Attack relies on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext
- Attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used

Brute-force attack

- Attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained
- On average, half of all possible keys must be tried to achieve success

Cryptanalysis Attacks

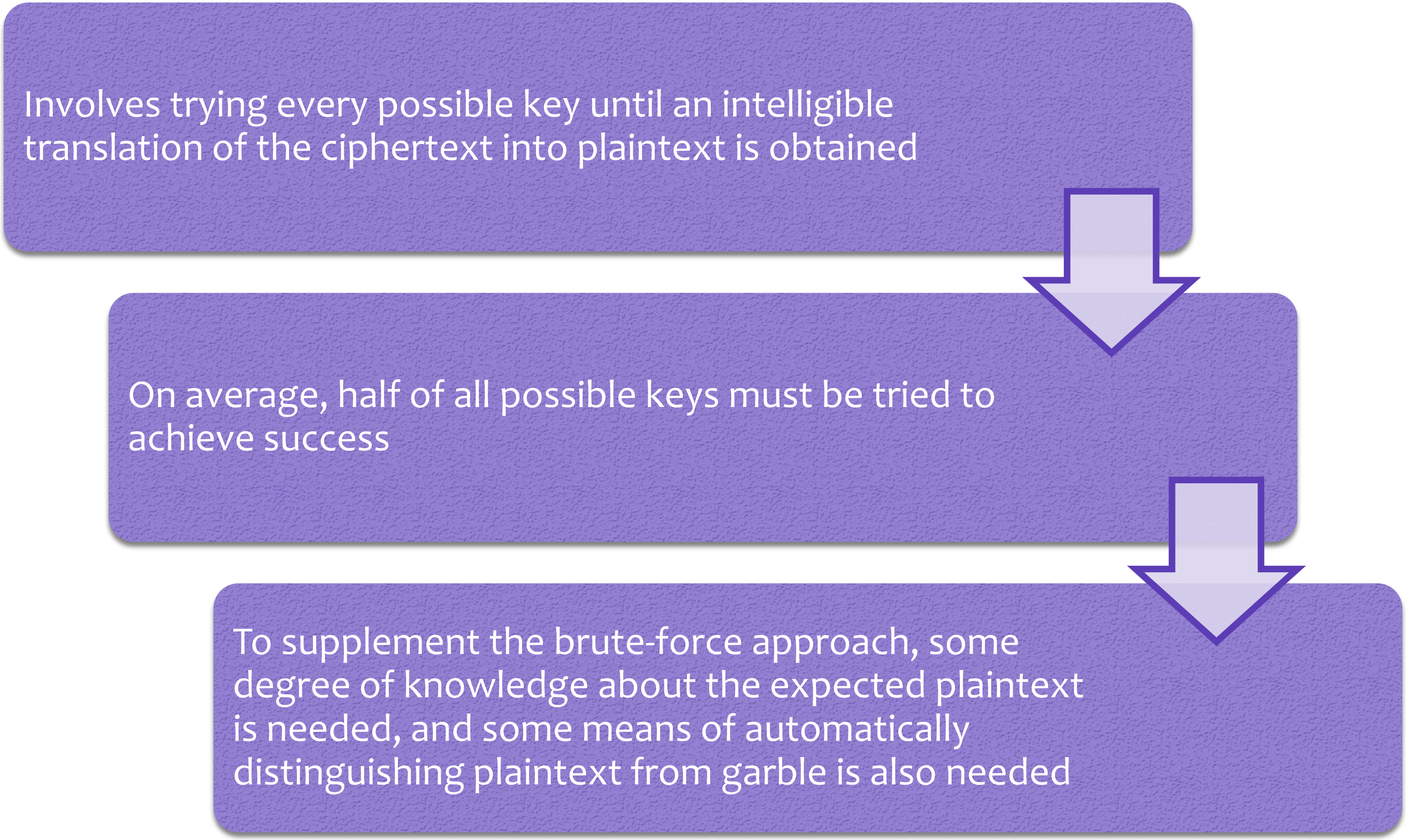


Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst,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

Cipher Strength

- **Unconditionally secure**
  - no matter how much computer power or time is available, the cipher **cannot be broken** since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext
- **Computationally secure**
  - given limited computing resources (e.g. time needed for calculations is greater than age of universe), the cipher cannot be broken

Brute-Force Attacks



Involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained

On average, half of all possible keys must be tried to achieve success

To supplement the brute-force approach, some degree of knowledge about the expected plaintext is needed, and some means of automatically distinguishing plaintext from garble is also needed

Substitution Technique

- Is one in which the letters of plaintext are replaced by other letters or by numbers or symbols
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Transposition Techniques

- All the techniques examined so far involve the substitution of a *ciphertext symbol* for a *plaintext symbol*.
- A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters.
- This technique is referred to as a transposition cipher.

Transposition Techniques – Rail Fence

- The simplest such cipher is the 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

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:

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

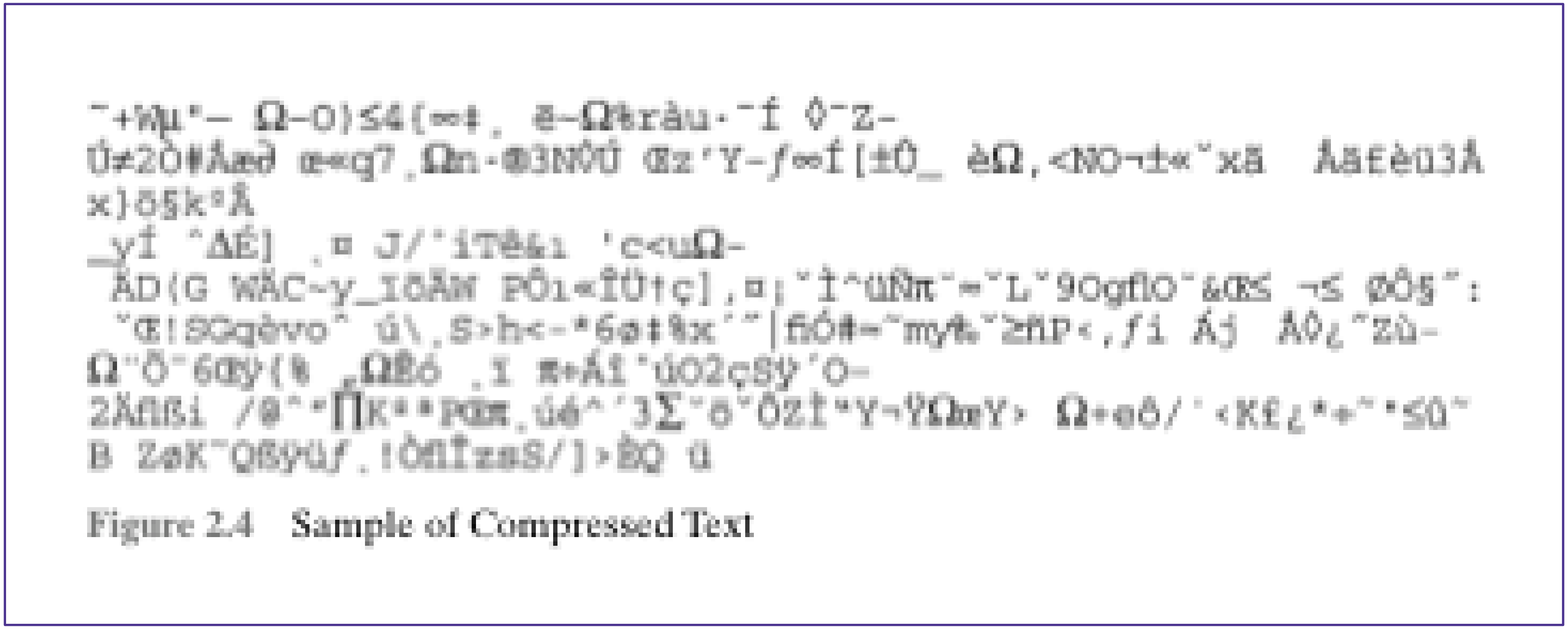
- A shift may be of any amount, so that the general Caesar algorithm is:

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

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

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

Sample of Compressed Text



```
¯+¼µ°– Ω–0)≤4(∞‡, ä–Ω‰ràu·¯ƒ ◊¯z-
Ù≠2Ò#Åæ∂ œ«g7,Ωn·®3NØÛ Œz'Y–ƒ∞ƒ[±Ô_ èΩ,<NO¬±«˘xß  Åaƒèü3Å
x}ö§k°Å
_yƒ ˆΔÉ] ,¤ J/ˆiTê‰ı 'c<uΩ-
 ÅD(G WÄC~y_IöÅW PÔı«îÜ†ç],¤¦˘Î^üÑπ˘=˘L˘9Ogﬂ0˘&ŒS ¬≤ øÔ§˘:
 ˇŒ!SQgèvo˘ ú\,S›h<–*6ø‡%x´˝|ﬁÓ#=˝my‰˘≥ñP‹,ƒi Áj ÀÔ¿˝zù-
Ω¨Õ¯6œy(% „Ωßó ,1 π•Áî'úO2çßÿ'O–
2ÄñßÍ /@ˆ˝*∏K**Pœπ,úé^'3∑˘ö˘ÖzÌ*Y-¥£ΩwY› Ω•øô/''‹K£¿*+˝*≤0˝
B Zøk¯QßÿU/.!ÒñÎzøS/]›ÈQ ü
```

Figure 2.4 Sample of Compressed Text

Monoalphabetic Ciphers

- Permutation
  - Of a finite set of elements S is an ordered sequence of all the elements of S, with each element appearing exactly once

- If the “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! possible keys
  - This is 10 orders of magnitude greater than the key space for DES
  - Approach is referred to as a *monoalphabetic substitution cipher* because a single cipher alphabet is used per message

Relative Freq of Letters in English Text

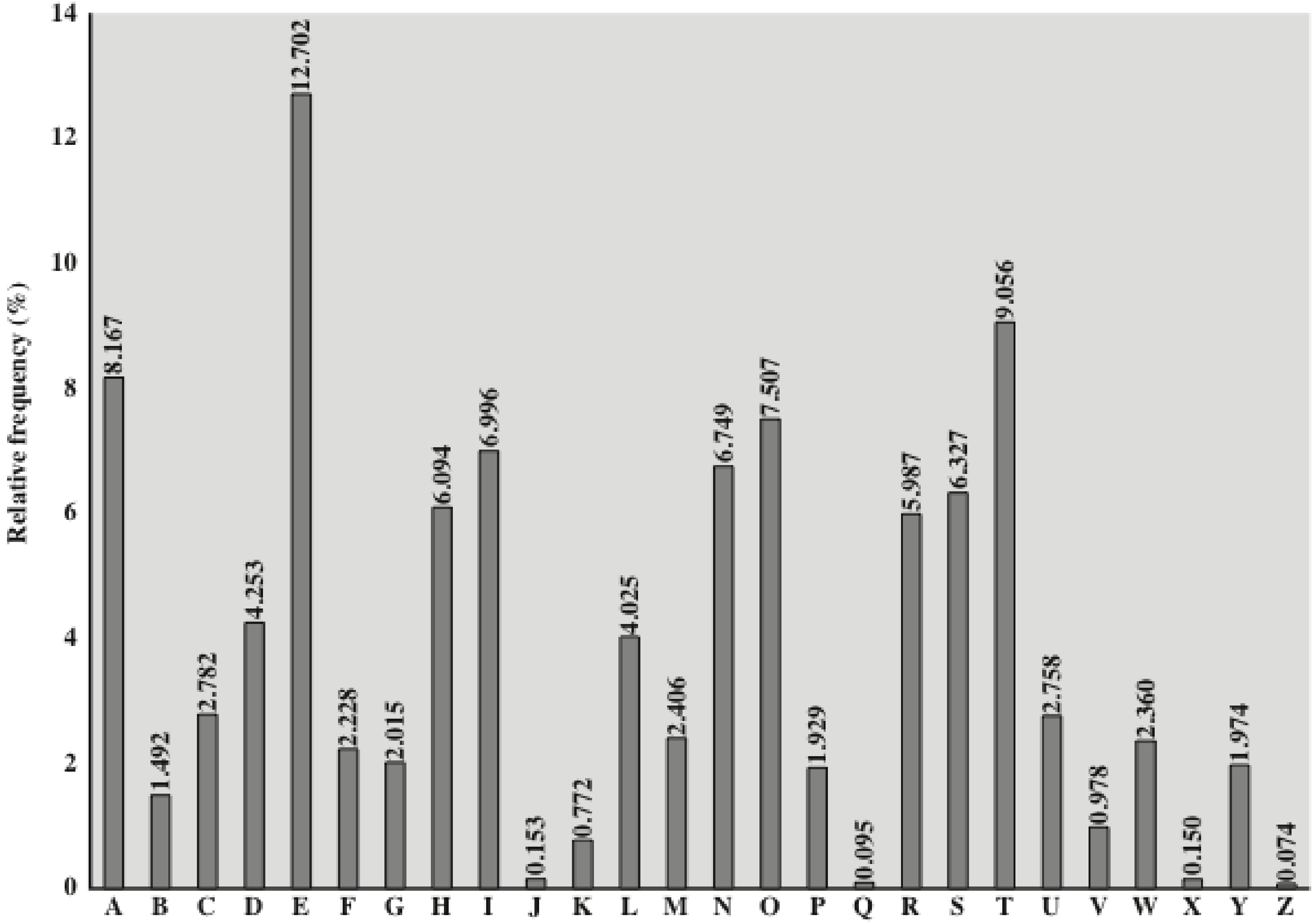
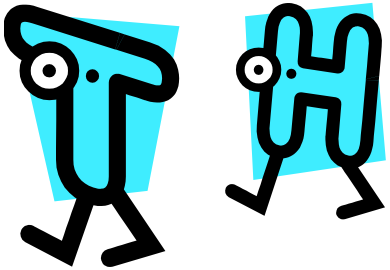
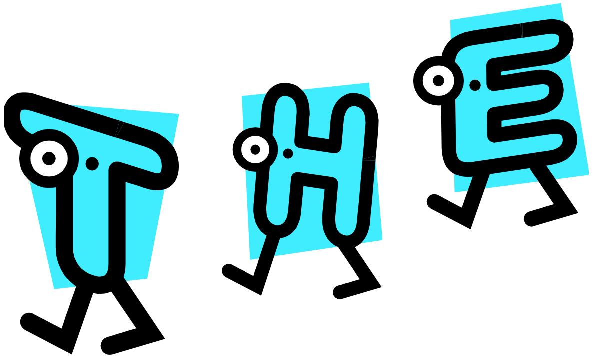


Figure 2.5 Relative Frequency of Letters in English Text

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 Ciphers

- 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

- Using the keyword MONARCHY
- Fill in letters of keyword *from left to right* and *from top to bottom*, then fill in the remainder of the matrix with the remaining letters in alphabetic order

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
- If a pair is a repeated letter, insert filler like 'X’
- If both letters fall in the *same row*, replace each with letter to right (wrapping back to start from end)
- If both letters fall in the *same column*, replace each with the letter below it (wrapping to top from bottom)
- *Otherwise* each letter is replaced by the letter in the same row and in the column of the other letter of the pair

Playfair Example

- Message = Move forward
- Plaintext = mo ve fo rw ar dx
- message is *padded* and *segmented*

x is just a filler

Cipher	Positions	Ciphertext
mo	same rows	mo → ON
ve	diffent rows and columns	ve → UF
fo	same column	fo → PH
rw	diffent rows and columns	rw → NZ
ar	same row	ar → RM
dx	diffent rows and columns	dx → BZ

- Ciphertext = ON UF PH NZ RM BZ

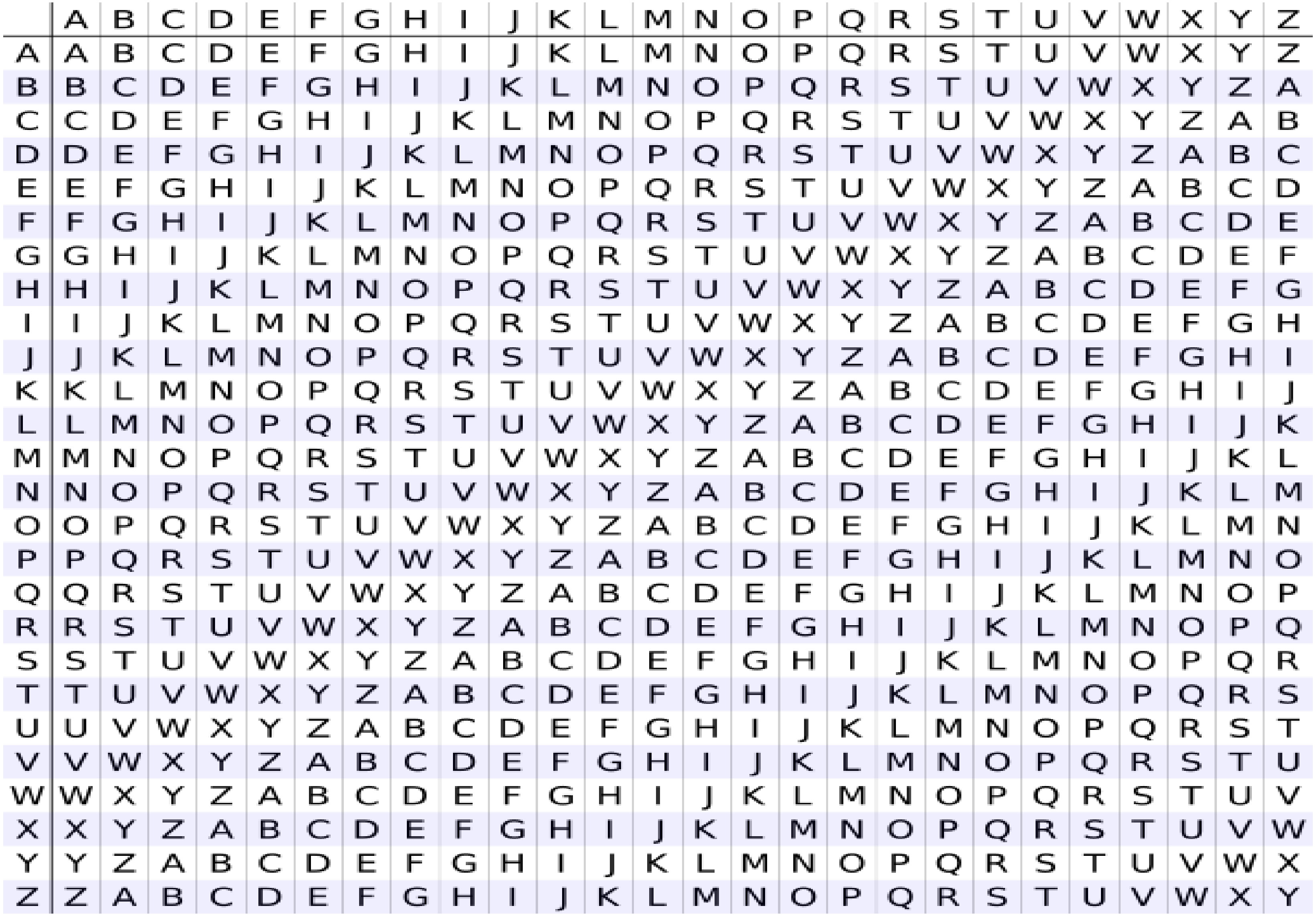
Security of Playfair Ciphers

- Security *much* ***improved*** over monoalphabetic
- Since have 26 x 26 = 676 digrams
- Would need a 676 entry frequency table to analyze (versus 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

Vigenère Cipher

- Best known and one of the simplest polyalphabetic substitution ciphers
- In this scheme the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25
- Each cipher is denoted by a *key letter* which is the ciphertext letter that substitutes for the plaintext letter a

Vigenère Table



	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 of Vigenère Cipher

- To encrypt a message, a key is needed that is as long as the message
- Usually, the key is a *repeating keyword*
- For example, if the keyword is ***deceptive***, the message “we are discovered save yourself” is encrypted as:
- key: deceptivedeceptivedeceptive
- plaintext: wearediscoveredsaveyourself
- ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ
- It works as follows: (look into Vigenère table)
    - Row d + column w → Z
    - Row e + column e → I

Steganography

- An alternative to encryption
- Hides existence of message
  - using only a subset of letters/words in a longer message marked in some way
  - using invisible ink
  - hiding in LSB in graphic image or sound file
  - hide in “noise”
- Has drawbacks
  - high overhead to hide relatively few info bits
- Advantage is can obscure encryption use

Summary (1/2)

- Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key.
- Symmetric encryption transforms **plaintext into ciphertext** using a secret key and an encryption algorithm.
- Using the same key and a decryption algorithm, the plaintext is recovered from the ciphertext.
- The two types of attack on an encryption algorithm are cryptanalysis, based on properties of the encryption algorithm, and brute-force, which involves trying all possible keys.

Summary (2/2)

- Traditional (precomputer) symmetric ciphers use substitution and/or transposition techniques.
  - Substitution techniques map plaintext elements (characters, bits) into ciphertext elements.
  - Transposition techniques systematically transpose the positions of plaintext elements.
- Steganography is a technique for hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message.

References

- *Cryptography and Network Security*, Principles and Practice, William Stallings, Prentice Hall, Sixth Edition, 2013