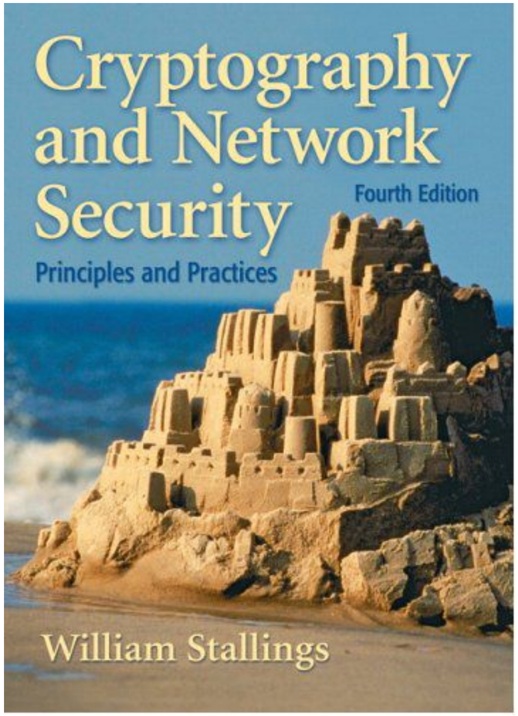


Data Security

Section 1

Chapter 1: Introduction
Chapter 2: Classical Encryption Techniques

Introduction

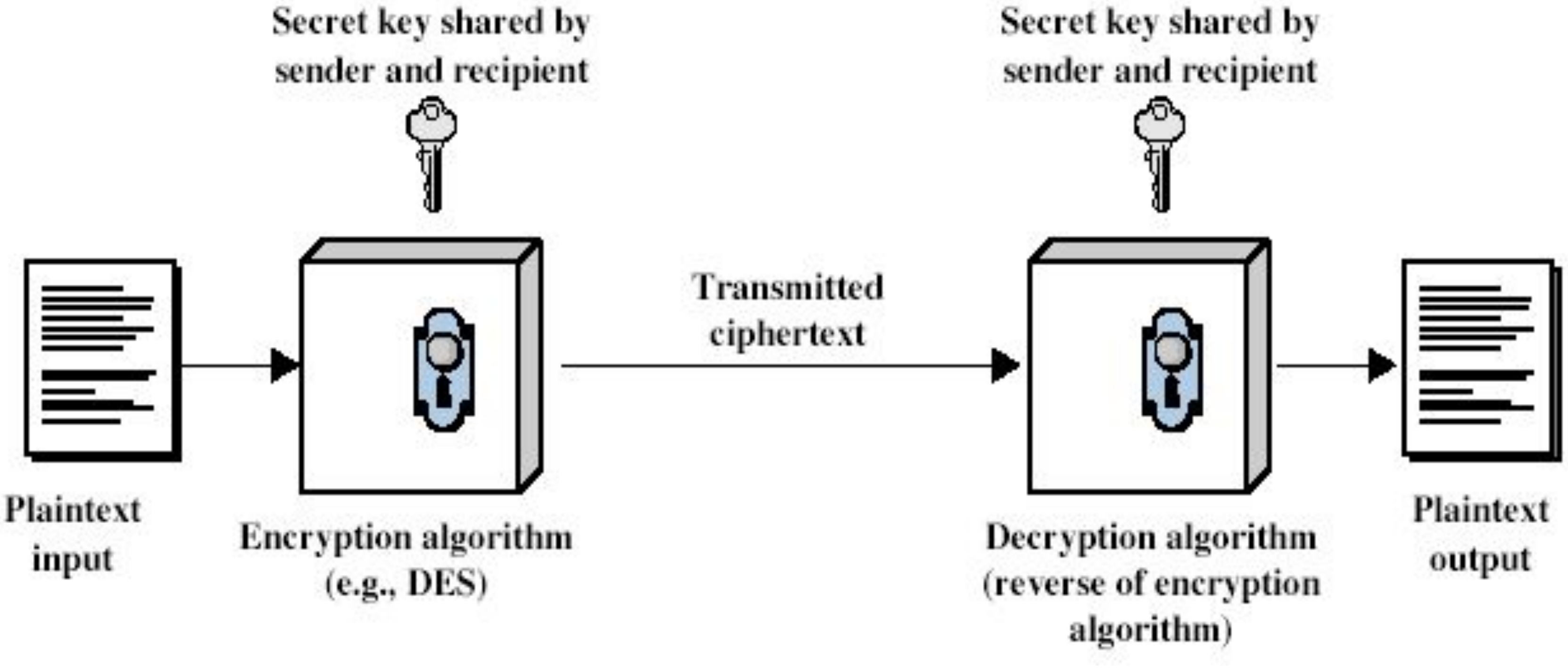
- **Cryptology**:
  - This is the study of techniques for ensuring the **secrecy** and/or **authenticity** of information. The two main branches of cryptology are:
  - **Cryptography:** which is the study of the design of such techniques;
  - **Cryptanalysis:** which deals with the defeating such techniques, to recover information

Introduction

- **Computer security**: Refers to the security of computers against **intruders** (e.g., hackers) and **malicious software** (e.g., viruses).
- Typically, the computer to be secured is attached to a network and the bulk of the threats arise from the network.

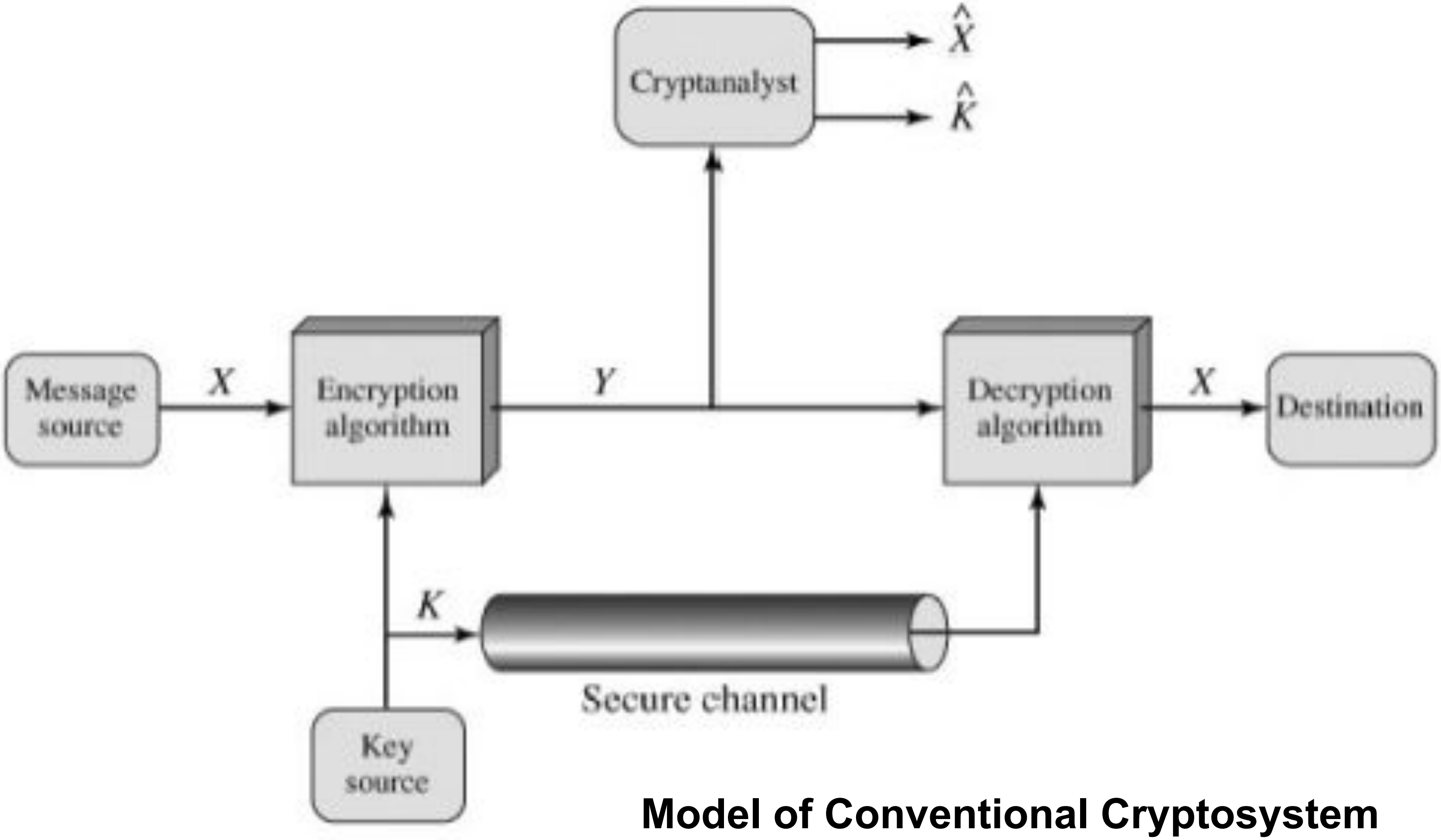
- **Network security**: This area covers the use of cryptographic algorithms in network protocols and network applications.

Classical Encryption Techniques


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Simplified Model of Conventional Encryption

Classical Encryption Techniques



Model of Conventional Cryptosystem

Classical Encryption Techniques

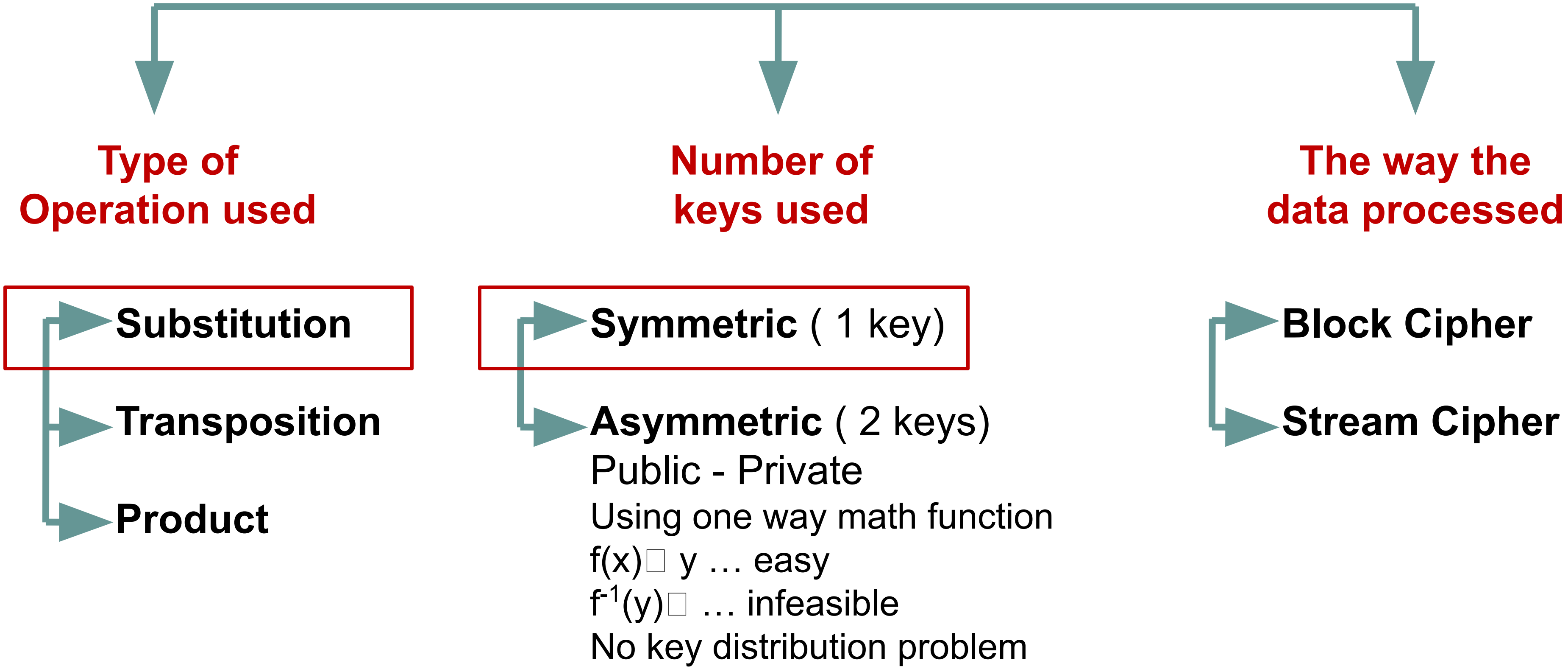
- **Unconditionally Secure**:
  - C.T have no enough information to determine only one corresponding P.T

- **Computationally Secure:**
  - Cost to break the cipher exceeds the value of the information

  - Time required to break the cipher exceeds the information life time

Classical Encryption Techniques

Encryption techniques can be classified according to:



Type of Operation used

- **Substitution**
- **Transposition**
- **Product**

Number of keys used

- **Symmetric** (1 key)
- **Asymmetric** (2 keys)

Public - Private

Using one way math function

f(x)□ y … easy

$f^{-1}(y)$□ … infeasible

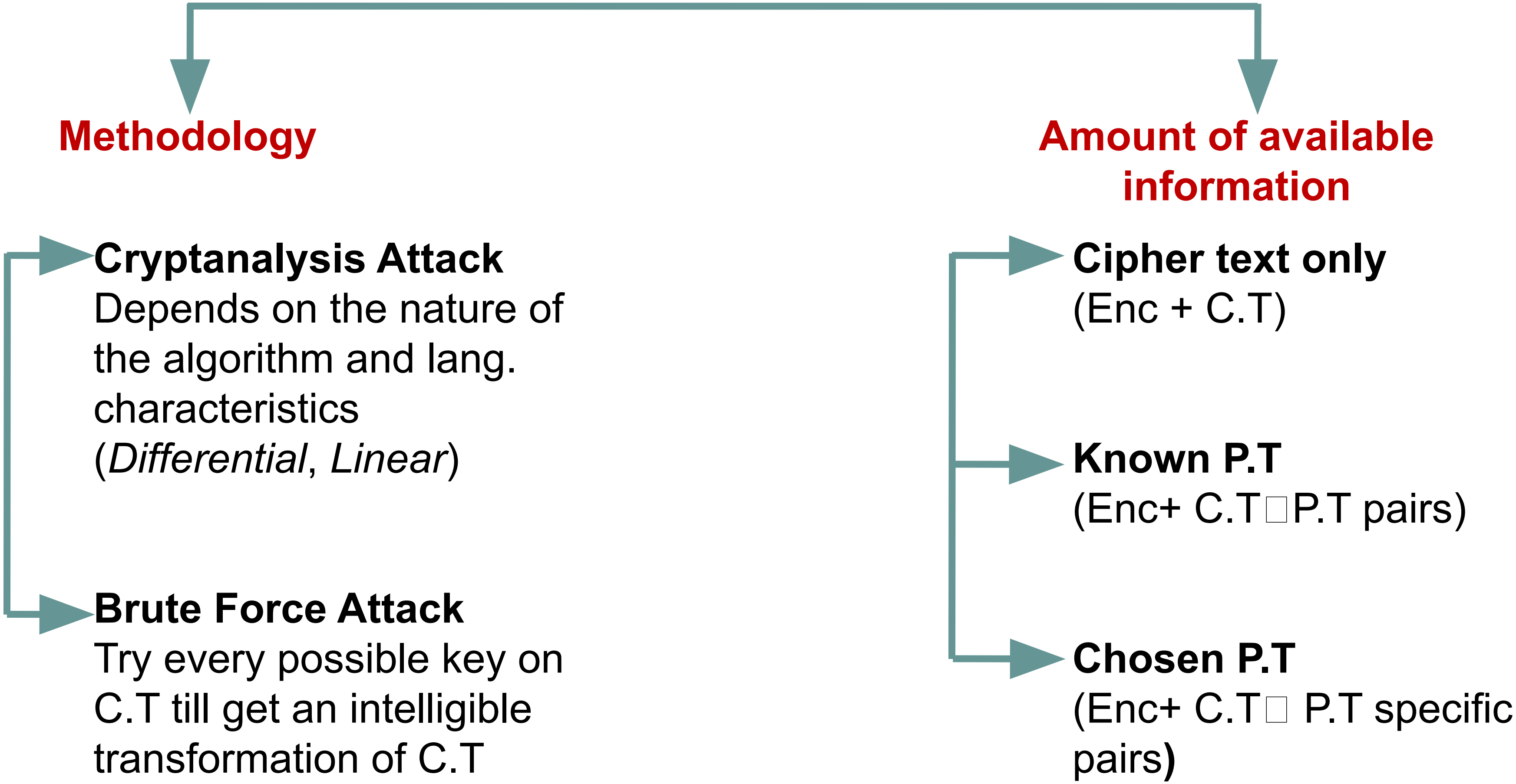
No key distribution problem

The way the data processed

- **Block Cipher**
- **Stream Cipher**

Classical Encryption Techniques

Cryptanalysis techniques can be classified according to:



Methodology

Cryptanalysis Attack
Depends on the nature of the algorithm and lang. characteristics
(*Differential*, *Linear*)

Brute Force Attack
Try every possible key on C.T till get an intelligible transformation of C.T

Amount of available information

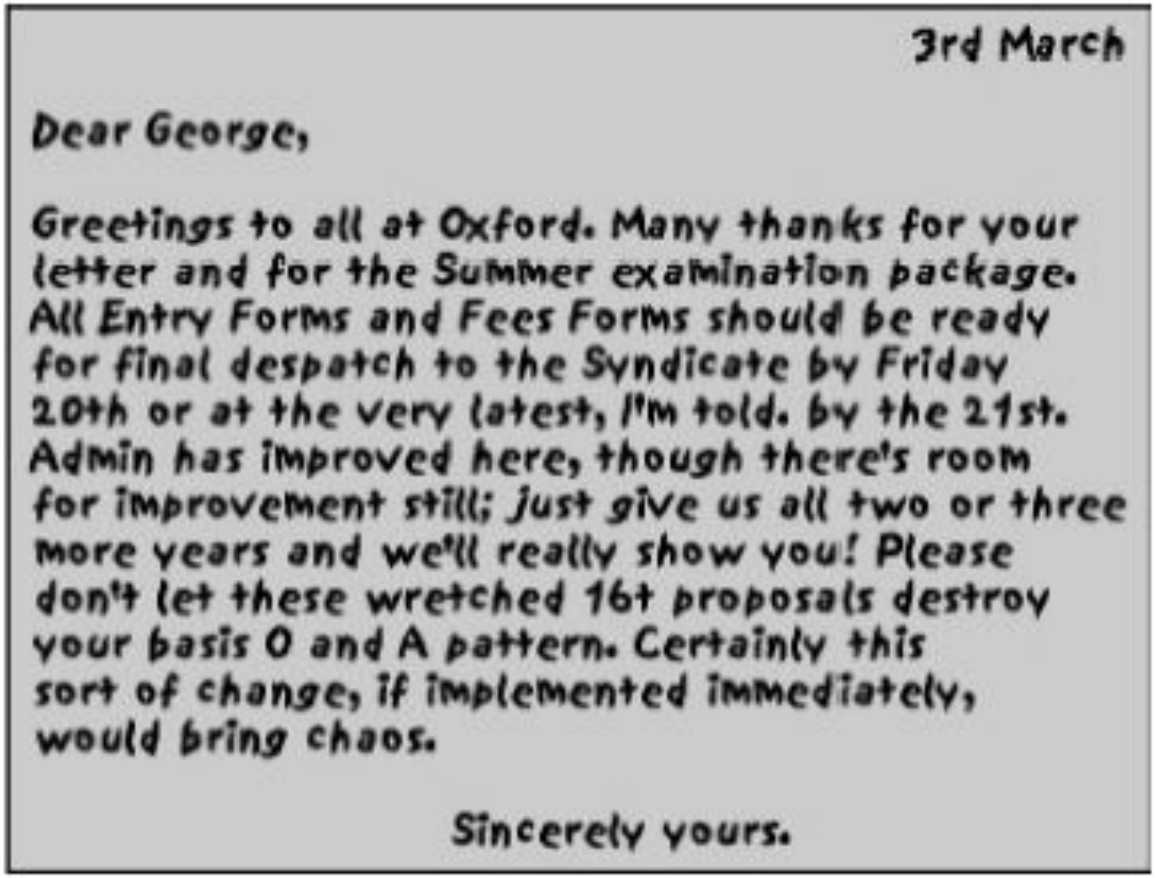
Cipher text only
(Enc + C.T)

Known P.T
(Enc+ C.T□P.T pairs)

Chosen P.T
(Enc+ C.T□ P.T specific pairs**)**

Steganography

- Methods of **hiding** the existence of a message or other data. This is different than cryptography, which hides the meaning of a message but does not hide the message itself.



3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your
letter and for the Summer examination package.
All Entry Forms and Fees Forms should be ready
for final despatch to the Syndicate by Friday
20th or at the very latest, I'm told. by the 21st.
Admin has improved here, though there's room
for improvement still; just give us all two or three
more years and we'll really show you! Please
don't let these wretched 16+ proposals destroy
your basis O and A pattern. Certainly this
sort of change, if implemented immediately,
would bring chaos.

Sincerely yours.

Substitution Techniques

- Ceaser
- Monoalphabetic
- Polyalphabetic
- Playfair
- Hill Cipher

Substitution Techniques

- Ceaser
- Monoalphabetic
- Polyalphabetic
- Playfair
- Hill Cipher

Ceaser Cipher

1. Assign numeric equivalent for each letter
2. For each P.T letter P substitute with C.T letter C

   where index of **C = (index of P + key) mod 26**

Example: P.T = Computer, Key = 8

P.T	c	o	m	p	u	t	e	r
P.T Index	2	14	12	15	20	19	4	17
C.T Index	10	22	20	23	2	1	12	25
C.T	K	W	U	X	C	B	M	Z

A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
[illegible]	15
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	18
[illegible]	19
U	20
V	21
W	22
X	23
Y	24
Z	25

Decryption?
# of keys ?
Cryptanalysis
?

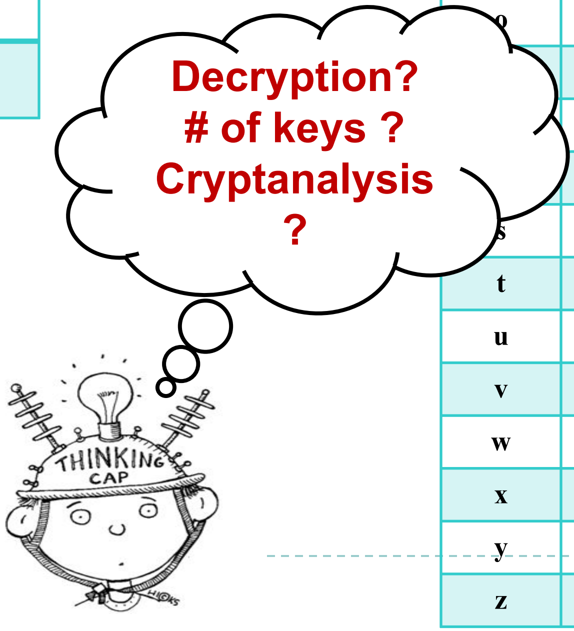
Monoalphabetic Cipher

1. Use any permutation of alphabetic to substitute each letter in the P.T with its corresponding (**Mapping**)

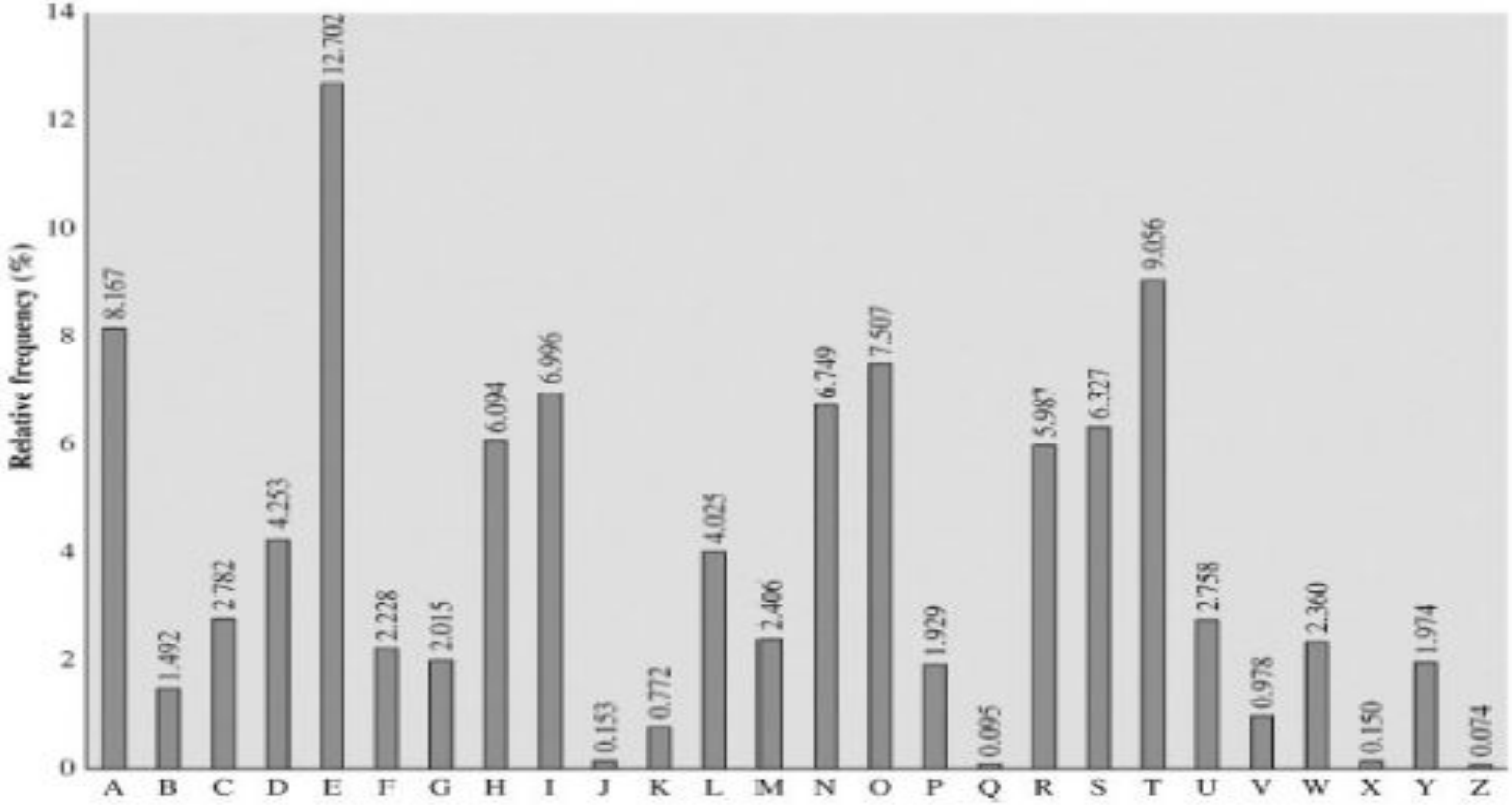
a	D
b	Q
c	E
d	P
e	R
f	S
g	F
h	T
i	A
j	W
k	X
l	U
m	G
n	O
o	B
	V
	H
	N
s	C
t	M
u	I
v	Z
w	L
x	Y
y	J
z	K

Example: P.T = Computer, Key = this permutation

P.T	c	o	m	p	u	t	e	r
C.T	E	B	G	V	I	M	R	N



Monoalphabetic Cipher



Monoalphabetic Cipher

? To increase the immunity of monoalphabetic cipher

1. **Using homophones**

a	D,-,?
b	Q,2,T
c	E,7,&
. . .	. . .

2. **Polyalphabetic**

a	D	O
b	Q	L
c	E	V
. . .	. . .	. . .

3. **Higher order substitution**

Block cipher

aa	DS
ab	CG
ac	HH
. . .	. . .

Playfair Cipher

- It is a **multiple letter** substitution cipher.

- It treats **diagrams** (block of two letters) in plaintext as single units and translates these units into ciphertext diagrams.

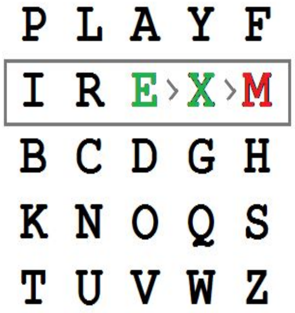
- The playfair algorithm is based on the use of **5x5 matrix** of letters constructed using a keyword

Playfair Cipher

1. The matrix is constructed using the keyword, Example, keyword = “**playfairexample**”

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

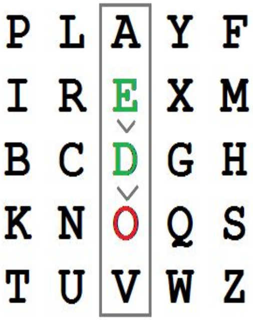
2. Plaintext is encrypted as two letters as a time, according to the following rules:



EX

Shape: Row
Rule: Pick Items to Right of Each Letter, Wrap to Left if Needed

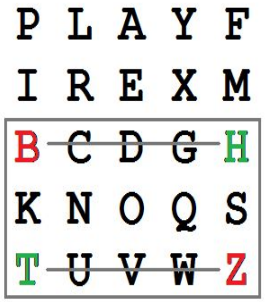
XM



DE

Shape: Column
Rule: Pick Items Below Each Letter, Wrap to Top if Needed

OD



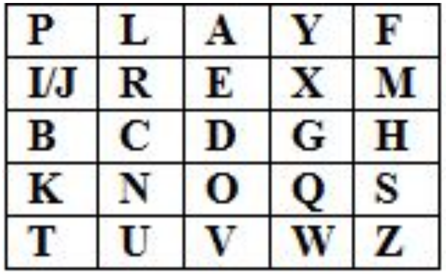
TH

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

ZB

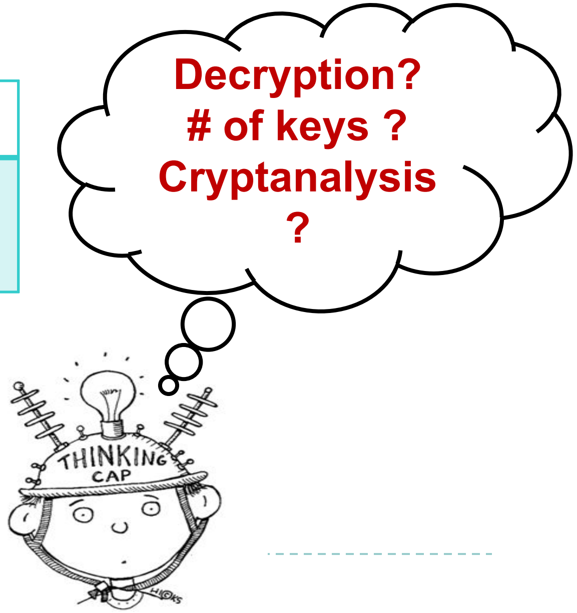
Playfair Cipher

Example: P.T = communication, Keyword = “**playfairexample**”



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

P.T	co	mx	mu	ni	ca	ti	on
C.T	DN	IM/ JM	RZ	KR	DL	PB	QO



Decryption?
# of keys ?
Cryptanalysis
?

Your Turn … ☺

- Encrypt the following P.T = “ Computer Systems” using playfair cipher with keyword = “balloon”

Thank You!