

**TRƯỜNG ĐẠI HỌC NGUYỄN TẤT THÀNH**  
**KHOA CÔNG NGHỆ THÔNG TIN**

**Bài giảng môn học: AN TOÀN THÔNG TIN**

**Chương 3:**  
**MÃ HÓA THÔNG TIN CỔ ĐIỂN**

**Số tín chỉ: 3**  
**Số tiết: 60 tiết**  
**(30 LT + 30 TH)**

**Biên soạn: ThS. Nguyễn Thị Phong Dung**  
**Email : [ntpdung@ntt.edu.vn](mailto:ntpdung@ntt.edu.vn)**



# Bài 3: MÃ HÓA THÔNG TIN CỔ ĐIỂN

Các khái niệm về Mã hóa thông tin

Hệ mật mã (Cryptography)

Thám mã (Cryptanalyze)

Mã hóa cổ điển: Mật mã Ceasar

Mật mã thay thế đơn ký tự

Mật mã Vigenère

# Các khái niệm về Mã hóa thông tin

## ■ Tiêu chuẩn an toàn thông tin:

- **Confidentiality** (tính bí mật): thông tin là bí mật với người không có thẩm quyền.

- **Integrity** (tính toàn vẹn): bên nhận xác minh được dữ liệu toàn vẹn.

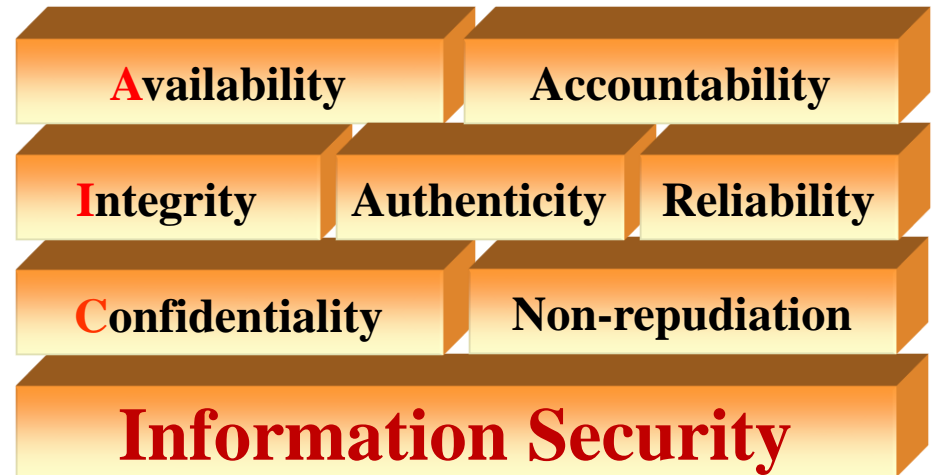
- **Authenticity** (tính xác thực): bên nhận xác minh được nguồn gốc của thông tin.

- **Non-repudiation** (tính chống thoái thác): bên tạo ra thông tin không thể phủ nhận thông tin mình đã tạo.

- **Reliability** (tính ổn định / tin cậy): độ an toàn của thuật toán cao.

### ▶ Kỳ vọng đối với hệ mã hóa:

- Đảm bảo *tính bí mật*, tính *chống thoái thác*, tính *xác thực* và *ổn định*.

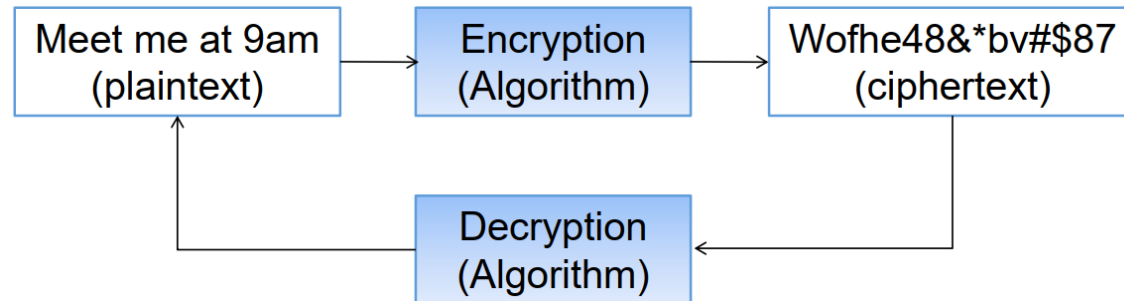


# Các khái niệm về Mã hóa thông tin

## ■ Mã hóa thông tin:

### ▶ Khái niệm:

- Mã hóa là làm biến đổi thông tin gốc => thông tin mã hóa.
- Có khả năng giải mã thông tin mã hóa => thông tin ban đầu



### ▶ Vai trò:

- Đảm bảo tính bí mật (*Confidentiality*) cho thông tin.
- Bên mã hóa có quyền lựa chọn bên giải mã (cung cấp khóa mã).
- Một số thuật toán mã hóa cung cấp thêm *tính xác thực, tính toàn vẹn, tính chống thoái thác...*

# Các khái niệm về Mã hóa thông tin

## ■ Mã hóa thông tin:

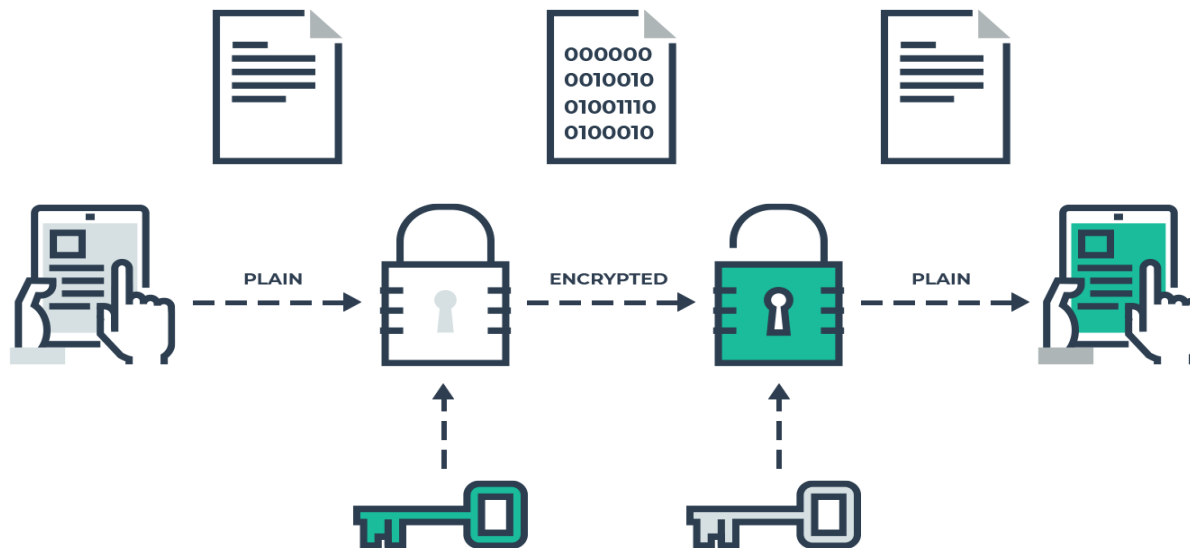
### ▶ Các thuật ngữ:

- *Plain text* (bản rõ): thông tin gốc (biểu diễn theo cách thức nào đó)
- *Encrypt* (mã hóa): hành động biến đổi cách thức biểu diễn thông tin.
- *Cipher text* (bản mã): thông tin đã được mã hóa, che giấu, giữ bí mật.
- *Decrypt* (giải mã): hành động biến đổi *Cipher text* thành *Plain text*
- *Algorithm* (thuật toán): giải thuật mã hóa / giải mã thông tin.
- *Key* (khóa): cùng 1 giải thuật, có thể có nhiều trường hợp mã hóa / giải mã khác nhau. Key = trường hợp của giải thuật.
- *Cryptography* (mật mã học): nghiên cứu các phương pháp mã hóa thông tin.
- *Cryptanalysis* (thám mã / phá mã): nghiên cứu các phương pháp để phá vỡ hệ mật mã.

# Hệ mật mã (Cryptography System)

## ■ Khái niệm Hệ mật mã:

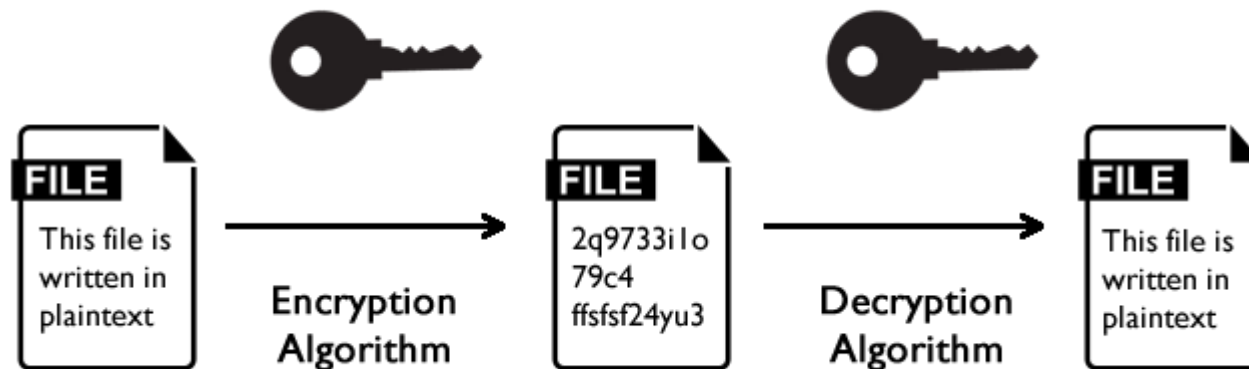
- ▶ Là hệ thống mã hóa và giải mã thông tin. Bao gồm 3 yếu tố:
  - Giải thuật (*Algorithm*) mã hóa và giải thuật giải mã.
  - Không gian khóa (*Key space*).
  - Cách thức xử lý thông tin (*Data processing*).



# Hệ mật mã (Cryptography System)

## ■ Giải thuật mật mã hóa:

- ▶ Là các thuật toán biến đổi *Plain text* => *Cipher text* => *Plain text*.
- ▶ Dựa vào 2 nguyên lý biến đổi:
  - Nguyên lý thay thế (**substitution**): mỗi thành phần trong *Plain text* (*bit, byte, ký tự, block...*) được thay thế bằng thành phần khác.
  - Nguyên lý chuyển vị (**transposition**): các thành phần trong *Plain text* được sắp xếp lại vị trí khác nhau (đảo vị trí).
- ▶ Có thể kết hợp cả 2 nguyên lý: vừa thay thế, vừa chuyển vị.





# Hệ mật mã (Cryptography System)

## ■ Giải thuật mật mã hóa:

- ▶ Minh họa cho **nguyên lý thay thế** (*substitution*) bằng giải thuật dùng “*sách*” hay “*khóa chạy*”:
- ▶ Ví dụ: bản mã là **259,19,8; 22,3,8; 375,7,4; 394,17,2** và cuốn sách được dùng là "*A Fire Up on the Deep*":
  - Trang **259**, dòng **19**, từ thứ **8** → **sack**
  - Trang **22**, dòng 3, từ thứ 8 → **island**
  - Trang **375**, dòng **7**, từ thứ **4** → **sharp**
  - Trang **394**, dòng **17**, từ thứ **2** → **path**
  - Bản rõ tương ứng của bản mã "**259,19,8; 22,3,8; 375,7,4; 394,17,2**" là "**sack island sharp path**".





# Hệ mật mã (Cryptography System)

## ■ Giải thuật mật mã hóa:

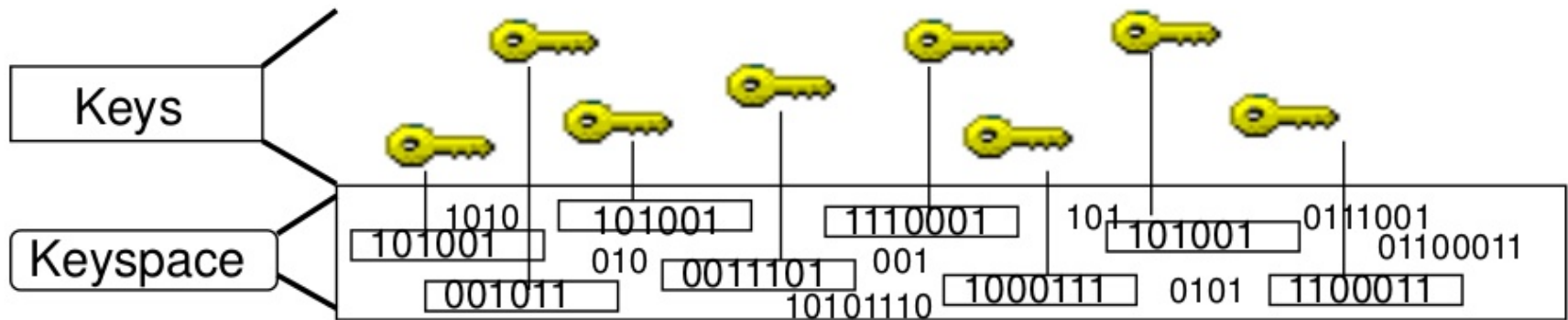
- ▶ Minh họa cho **nguyên lý chuyển vị** (*transposition*) bằng phương pháp dùng ma trận:
- ▶ Ví dụ: bản rõ **P** = “**computer security**”
  - Viết các ký tự của bản rõ vào ma trận 5 cột, **theo hàng** từ trên xuống.
  - Tạo mã chuyển vị bằng cách viết lại **theo cột**.
  - Chuỗi kết quả **C** = **CTCYOEUMRRPSIUET**

c	o	m	p	u
t	e	r	s	e
c	u	r	i	t
y				

# Hệ mật mã (Cryptography System)

## ■ Không gian khóa:

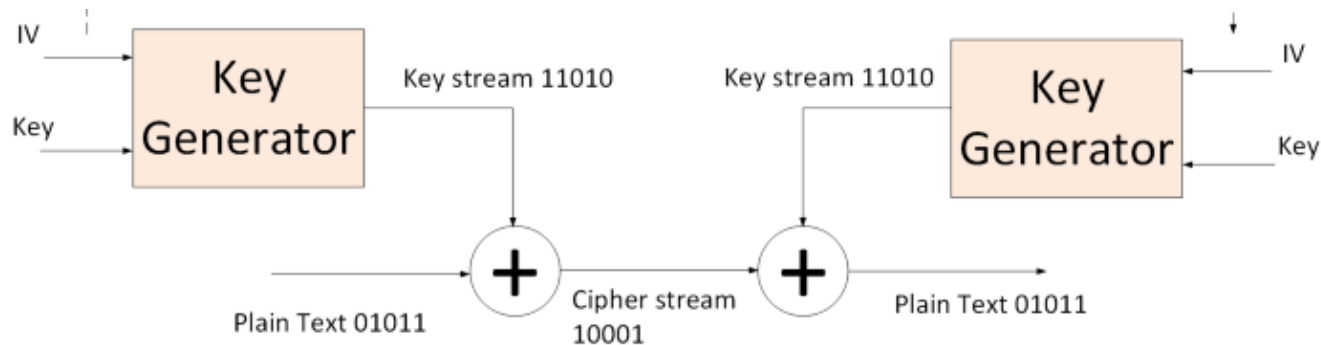
- ▶ Mỗi trường hợp biến đổi (thay thế / chuyển vị) là 1 Khóa.
- ▶ Không gian khóa: là tổng các trường hợp biến đổi của giải thuật.
- ▶ Không gian khóa càng lớn => khả năng phá mã (tìm được trường hợp biến đổi sử dụng) càng khó.



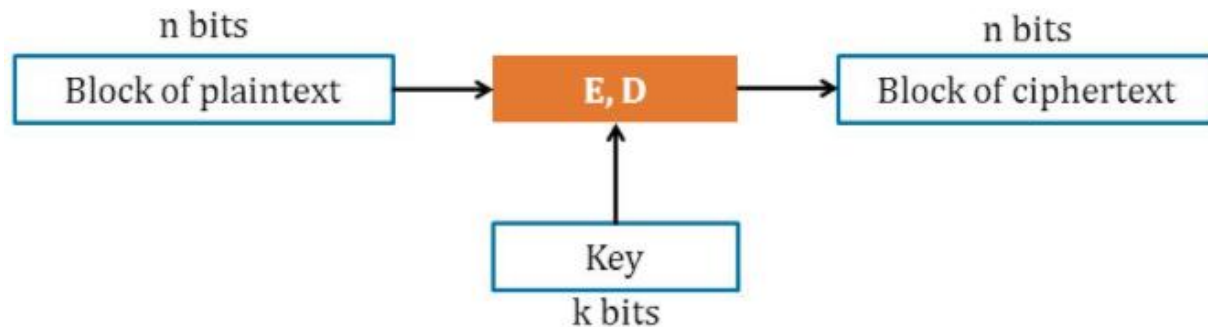
# Hệ mật mã (Cryptography System)

## ■ Cách thức xử lý thông tin:

- ▶ **Stream Cipher** (mã hóa luồng): từng phần tử của thông tin được xử lý (*mã hóa / giải mã*) liên tục, từ đầu đến cuối.



- ▶ **Block Cipher** (mã hóa khối): được chia thành nhiều khối (*block*), xử lý (*mã hóa / giải mã*) theo từng block..



# Thám mã (Cryptanalysis)

## ■ Kỹ thuật vét cạn (Brute-force):

- ▶ Thử tất cả các khả năng của khóa trên một số bản mã đến khi nhận được bản rõ minh bạch
- ▶ Về mặt lý thuyết, luôn thực hiện được
- ▶ Thời gian giải mã tỷ lệ thuận với độ phức tạp của khóa.

## ■ Kỹ thuật Phân tích mã (Cryptanalytic)

- ▶ Phân tích, suy luận để tìm ra bản rõ hoặc khóa mã dựa trên:
  - Bản chất của thuật toán mã hóa.
  - Thống kê, tìm đặc trưng của bản rõ / bản mã, ...



37 2a 08 72 d1 c4 52 24  
6a 07 03 f0 71  
ef 8f 09 81  
97 0b 07 25  
1f 6b 03 f9  
73 8d cd  
d0 6b 50 05  
c3 e8 2c  
41 e1 30 d2 cd 78 5e 2e

ork and no pl

# Thám mã (Cryptanalysis)

## ■ Nguyên lý an toàn cho hệ mật mã:

### ▶ Nguyên lý *Kerckhoff*:

- Tính an toàn của một hệ mã hoá không phụ thuộc vào việc giữ bí mật giải thuật mã hoá, mã chỉ phụ thuộc vào việc giữ bí mật khoá mã.

### ▶ Lý thuyết *Shannon*: một hệ mật mã là hoàn hảo khi:

- Độ dài của khóa tối thiểu bằng độ dài bản rõ.
- Khóa chỉ sử dụng một lần.
- => khó đạt được trên thực tế.

### ▶ 2 điều kiện an toàn cho hệ mật mã:

- Thời gian để thám mã thành công lớn hơn thời gian cần giữ bí mật thông tin.
- Chi phí để thám mã thành công lớn hơn giá trị thông tin thu được.

# Mã hóa cổ điển: Mật mã Caesar

## ■ Nguyên lý mã Caesar:

- ▶ Phát minh của **Julius Caesar**, thế kỷ 3 trước công nguyên
- ▶ Phương pháp mã: dùng nguyên lý **thay thế**.
  - Tạo **Cipher text** bằng cách: thay mỗi ký tự trong **Plain text** bằng ký tự thứ **k** tiếp theo trong bảng chữ cái.
  - Ví dụ: **k = 3**

Chữ ban đầu: 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

Chữ thay thế: 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

(sau Z sẽ vòng lại là A, do đó  $x \rightarrow A$ ,  $y \rightarrow B$  và  $z \rightarrow C$ )

Giả sử có bản tin gốc (bản rõ):                      meet me after the toga party

Như vậy bản tin mã hóa (bản mã) sẽ là:              PHHW PH DIWHU WKH WRJD SDUWB

# Mã hóa cổ điển: Mật mã Caesar

## ■ Toán học hóa mã Caesar:

- ▶ Nếu gán số thứ tự cho mỗi ký tự trong bảng chữ cái:

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

- ▶ Khi đó mã **Caesar** được định nghĩa qua phép tịnh tiến (khóa **K**):

- Mã hóa:  $C = (P + K) \bmod 26$

- Giải mã:  $P = (C - K) \bmod 26$

## ■ Độ an toàn của mã Caesar:

- ▶ Không gian khóa **K** là **25**  $\Rightarrow$  thám mã qua tối đa **25** lần thử.



# Mã hóa cổ điển: Mật mã Ceasar

## ■ Thám mã Ceasar bằng vét cạn (brute force):

- ▶ Ví dụ: nhận được *Cipher text*:

PHHW PH DIWHU WKH WRJD SDUWB

- ▶ Thử **25** key như hình bên =>
- ▶ Kết quả: ở **k = 3** giải mã được cụm từ có nghĩa.

## ■ Cải tiến mã Ceasar:

- ▶ Tăng không gian khóa.
- ▶ Nén / thay đổi nội dung bản rõ trước khi mã hóa  $\leq$  gây khó khăn khi nhận dạng

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	ydrpc	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	objv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjla
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	glzcx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc



# Mã hóa cổ điển: Mật mã Ceasar

- **Thám mã Ceasar bằng phương pháp thống kê:**
  - ▶ Thống kê tần suất sử dụng chữ cái.
    - Trong *English*: tần suất sử dụng ký tự:  $E > T > R > N > I > O > A > S$
    - Nhóm 2 ký tự:  $TH > HE > IN > ER > RE > ON > AN > EN$
    - Nhóm 3 ký tự:  $THE > AND > TIO > ATI > FOR > THA > TER > RES$
  - ▶ Dựa vào tần suất ký tự xuất hiện để dự đoán khóa
    - Ví dụ: bản mã PHHW PH DIWHU WKH WRJD SDUWB
    - Ký tự **H** xuất hiện nhiều nhất  $\Rightarrow$  **H** giải mã là **E**  $\Rightarrow K=3$

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

# Mã hóa cổ điển: Mật mã Ceasar

## ■ Bài tập mật mã Ceasar :

- ▶ 1. Áp dụng mật mã Ceasar mật mã hóa các bản rõ sau với  **$k = 4$**

**actions speak louder than words**

- ▶ 2. Bên dưới là *Cipher text* của câu *English* mã hóa bằng Ceasar:

**ST RFS HFS XJWAJ YBT RFX YJWX**

- Đoán khóa  **$k$**  của bản mã.
- Giải mã cho *Cipher text* trên.

- ▶ 3. Phá mã cho câu tiếng Anh bên dưới :

**CSYEVIXIVQMREXIH**

# Mã hóa cổ điển: Mật mã Ceasar

## ■ Cải tiến mã Ceasar:

- ▶ Tăng không gian khóa.
- ▶ Kết hợp với phương pháp chuyển vị:
  - **Chuyển vị** *Plain-text* rồi **mã hóa Ceasar**.
  - **Mã hóa Ceasar** rồi **chuyển vị** *Cipher-text*.
- ▶ Mã hóa bằng nhiều khóa khác nhau.
  - Mục đích: gây rối loạn tần suất xuất hiện của chữ cái.
  - Ví dụ: cùng chữ **E**.
    - Khi mã hóa  $k=3$  thì **E** => **H**.
    - Khi mã hóa  $k=5$  thì **E** => **J**

# Mật mã thay thế đơn ký tự

## ■ Giới thiệu:

- ▶ Tên gốc: *Mono-alphabetic substitution cipher*.
- ▶ Cải tiến từ mật mã Ceasar: tăng không gian khóa.

## ■ Nguyên lý:

- ▶ Dùng *Key* là hoán vị của **26** chữ cái.

Chữ ban đầu: 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

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

Như vậy bản rõ meet me after the toga party

được mã hóa thành: NJJU NJ ZRUJM UKJ UVSZ DZMUE

## ■ Nhận xét:

- ▶ Không gian khóa =  **$26!$**   $\approx 4.10^{26}$   $\Rightarrow$  vét cạn tốc độ  **$10^9$**  khóa/ giây thì cần **6400** thiên niên kỷ!
- ▶ Có thể phá mã bằng thống kê tần suất dùng chữ cái.

# Mật mã Vigenère

## ■ Nguyên lý: cải tiến từ mã hóa đơn ký tự

- Tạo bảng *Saint-Crypt* có 26 Key (A -> Z) để mã hóa 26 ký tự của *Plain text*.

- Chọn key trong bảng từ 1 key khác.

- Ví dụ: Key = **WORD**

- Key được chọn:
  - key 1 = **W**
  - key 2 = **O**
  - key 3 = **R**
  - key 4 = **D**

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

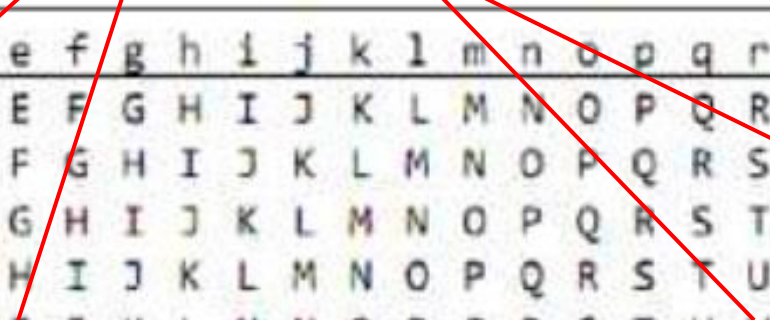


# Mật mã Vigenère

## ■ Minh họa: mã hóa Vigenère:

► Với *Key* = “**DECEPTIVE**”

plaintext:        wearediscoveredsaveyourself  
key:              DECEPTIVEDECEPTIVEDECEPTIVE  
ciphertext:       ZICVTWQNGRZGVTWAVZHCQYGLMGJ



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

## ■ Bài tập mã Vigenere:

- ▶ 1. Mã hóa Vigenere cho Plain-text “NETWORK SECURITY” với key là “ACE”
  - Plain: **NETWORKSECURITY**
  - Key: **ACE**
  - Cipher:
- ▶ 2. Tìm khóa (Key) của mã Vigenere, nếu biết:
  - Plain: **NETWORKSECURITY**
  - Cipher: **PVRLHFMJCRNFKKW**
  - Key:

# Cám ơn !

