MẬT MÃ HỌC

NỘI DUNG MÔN HỌC

Chương 1: Giới thiệu - Mã hoá cổ điển
Chương 2: Mã hoá đối xứng
Chương 3: Mã hoá khoá công khai và quản lý khoá
Chương 4: Chứng thực thông điệp
Chương 5: Chữ ký số
Chương 6: Các giao thức và ứng dụng

CHƯƠNG 1

GIỚI THIỆU MÃ HOÁ CỔ ĐIỂN

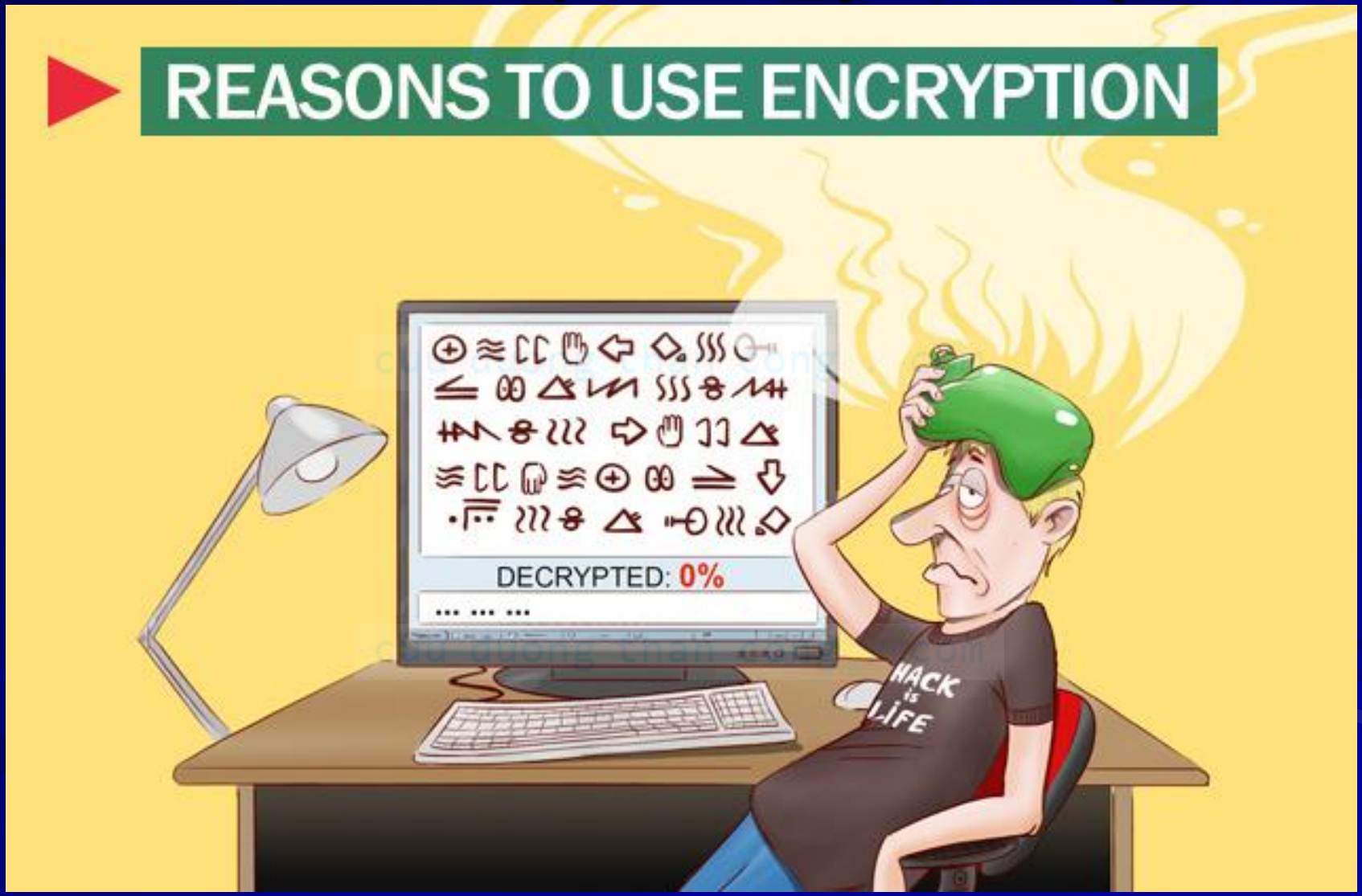
Giới thiệu – Mã hoá cổ điển

1. Giới thiệu về mật mã học
2. Lịch sử của mật mã
3. Các giải thuật mã hoá cổ điển
4. Bẻ gãy một hệ thống mật mã
5. Bài tập

1. Giới thiệu về mật mã học

- **Giới thiệu**
  - Mật mã được sử dụng kể từ cổ đại cho đến tận ngày nay.
  - Hiện nay, các giao dịch tài chính, chuyển khoản, mua sắm hàng hoá, thư từ, tài liệu… được thực hiện nhiều qua môi trường mạng đòi hỏi dữ liệu phải được bảo mật tốt => phải được mã hoá.

1. Giới thiệu về mật mã học



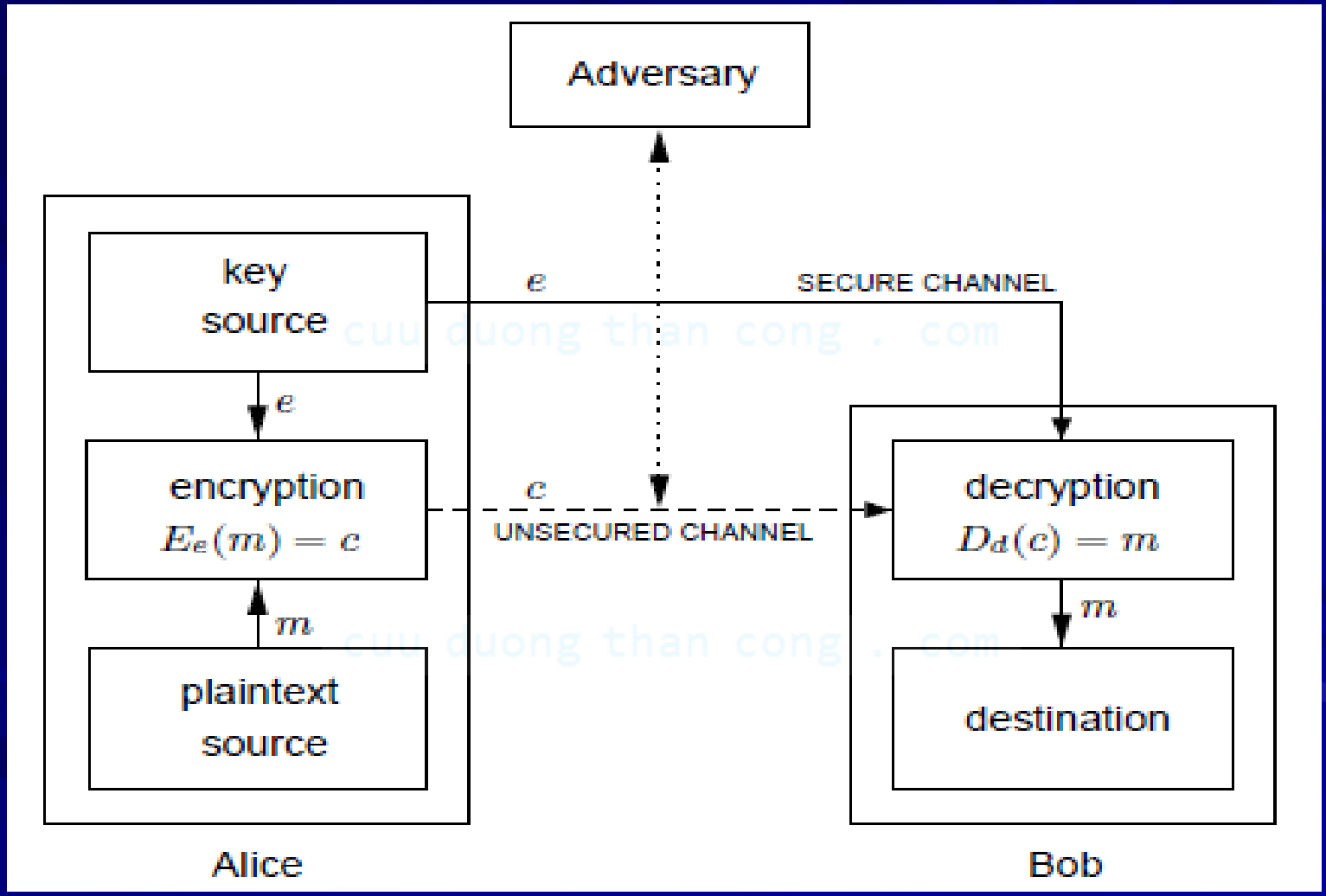
1. Giới thiệu về mật mã học

- **Một số khái niệm**
  - Thông báo, văn bản: là một chuỗi hữu hạn các ký hiệu lấy từ một bảng chữ cái Z nào đó và được ký hiệu là m.
  - Mật mã hoá: là việc biến đổi một thông báo sao cho nó không thể hiểu nổi đối với bất kỳ người khác ngoài người nhận được mong muốn.
  - Phép mật mã hoá thường được ký hiệu là e(m), với m là thông báo cần mã hoá.

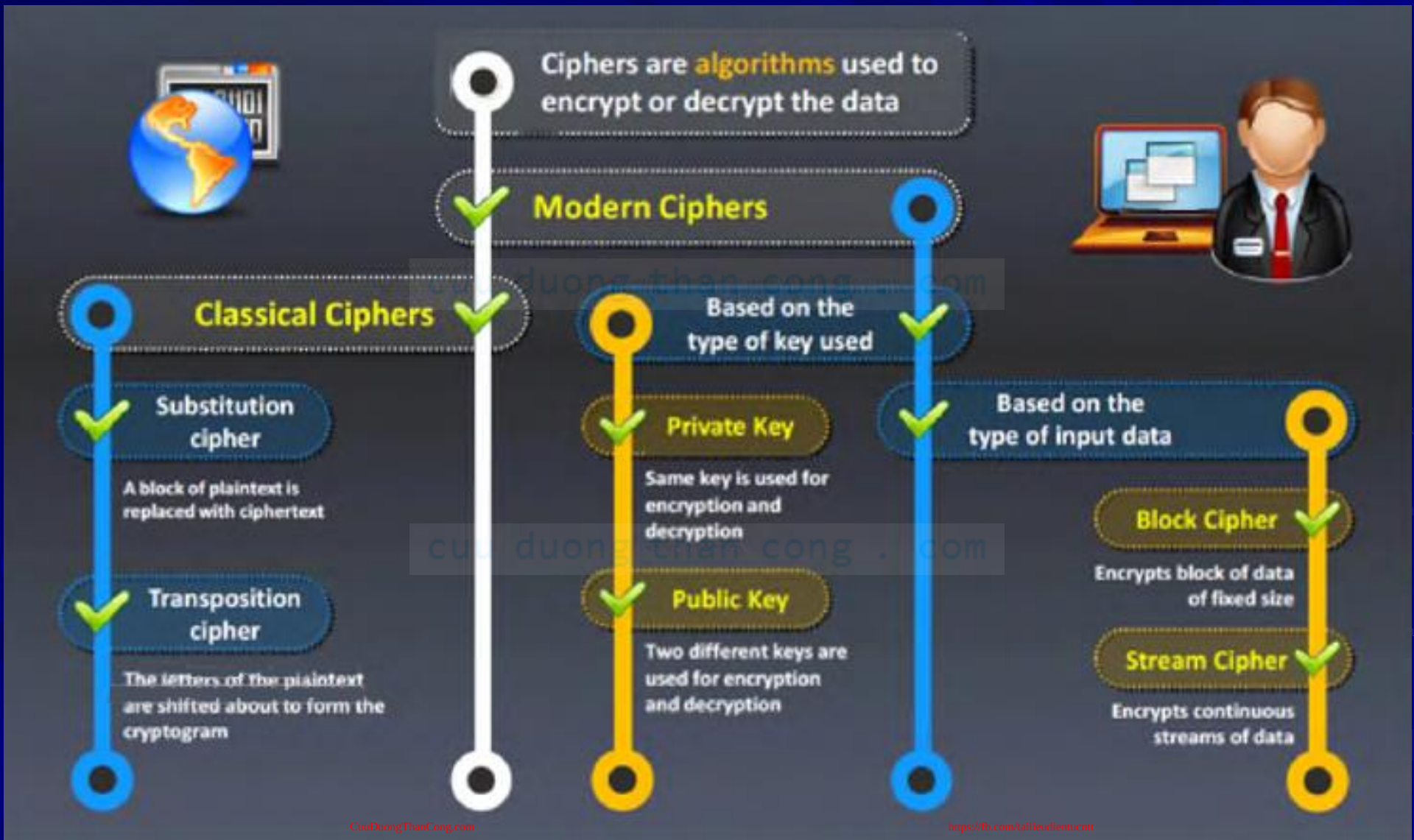
1. Giới thiệu về mật mã học

- **Một số khái niệm**
  - Khoá: là một thông số đầu vào của phép mã hoá hoặc giải mã. Khoá dùng để mã hoá ký hiệu là k_e, khoá dùng để giải mã ký hiệu là k_d.
  - Chuỗi mật mã: là chuỗi nguỵ trang, tức là chuỗi thông báo qua phép mật mã hoá và thường được ký hiệu là c: $c=e(m,k_e)$.
  - Phép giải mã $d(c,k_d)$ là quá trình xác định thông báo gốc (m) từ chuỗi mật mã c và khoá giải mã kd, và thường được ký hiệu là $d(c,k_d)$: $d(c,k_d)=m$.

1. Giới thiệu về mật mã học



1. Giới thiệu về mật mã học



2. Lịch sử của mật mã

- Mật mã học là ngành có lịch sử hàng ngàn năm.
- Mật mã học cổ điển với bút và giấy.
- Mật mã học hiện đại với điện cơ, điện tử, máy tính.
- Sự phát triển của mật mã học đi liền với sự phát triển của phá mã (thám mã):
  - Phát hiện ra bức điện Zimmermann khiến Hoa Kỳ tham gia Thế chiến I
  - Việc phá mã thành công hệ thống mật mã của Đức Quốc xã góp phần đẩy nhanh thời điểm kết thúc thế chiến II.
- Hai sự kiện khiến cho mật mã học trở nên đại chúng:
  - Sự xuất hiện của tiêu chuẩn mật mã hóa DES.
  - Sự ra đời của các kỹ thuật mật mã hóa khóa công khai.

2. Lịch sử của mật mã

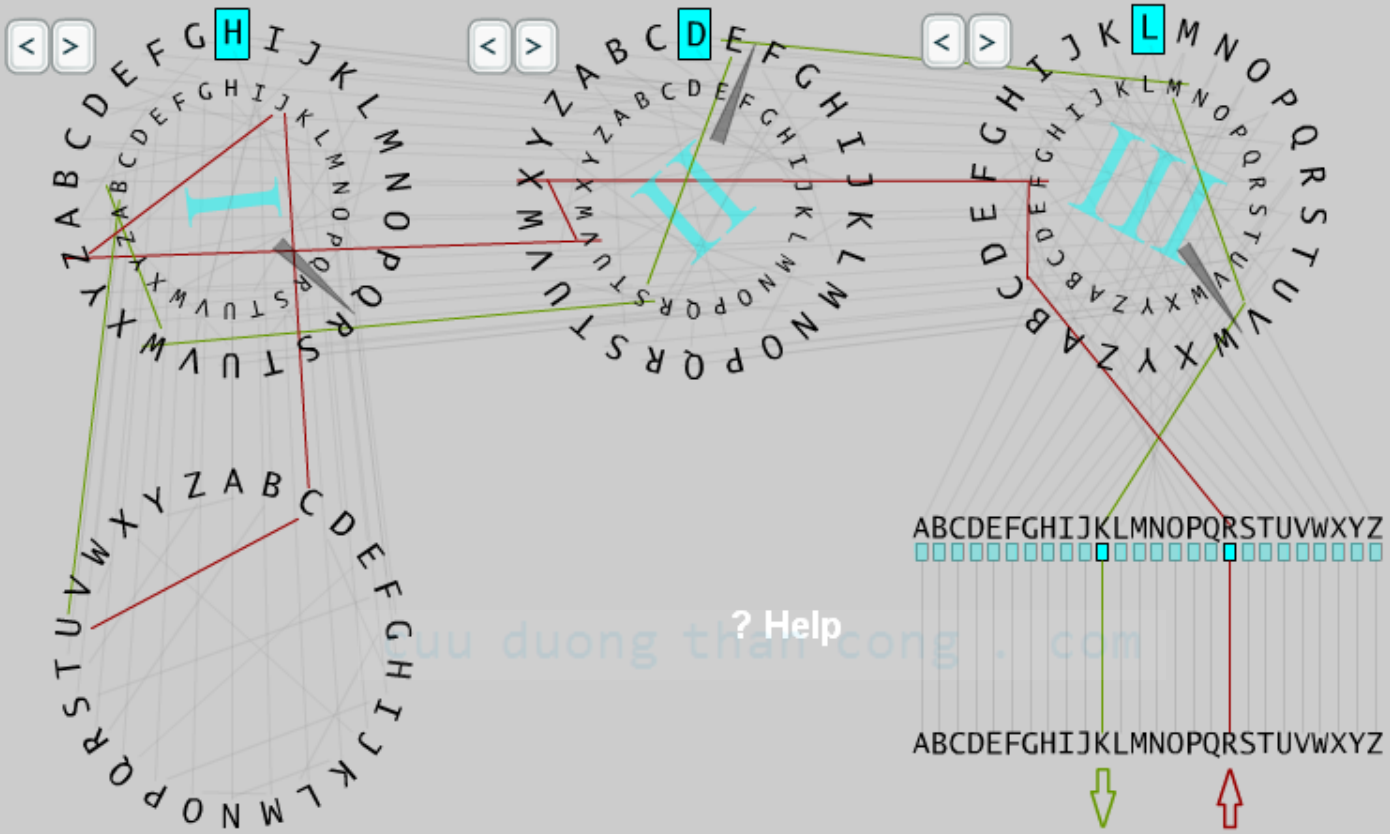
- **Mật mã học cổ điển**
  - Các chữ tượng hình không tiêu chuẩn tìm thấy trên các bức tượng Ai Cập cổ đại (cách đây khoảng 4500 năm tr.CN).
  - Mã hóa thay thế bảng chữ cái đơn giản như mật mã hóa Atbash (khoảng năm 500-600 tr.CN).
  - Người La Mã xây dựng mật mã Caesar.

2. Lịch sử của mật mã

- **Mật mã học trong thế chiến thứ 2**
  - Người Đức sử dụng rộng rãi một hệ thống máy rôto cơ điện tử có tên gọi là máy Enigma.
  - Phe Đồng minh sử dụng máy TypeX của Anh và máy SIGABA của Mỹ, đều là những thiết kế cơ điện dùng rôto tương tự như máy Enigma, song với nhiều nâng cấp hơn.

2. Lịch sử của mật mã

Máy Enigma



Input:

COMPUTER

Output:

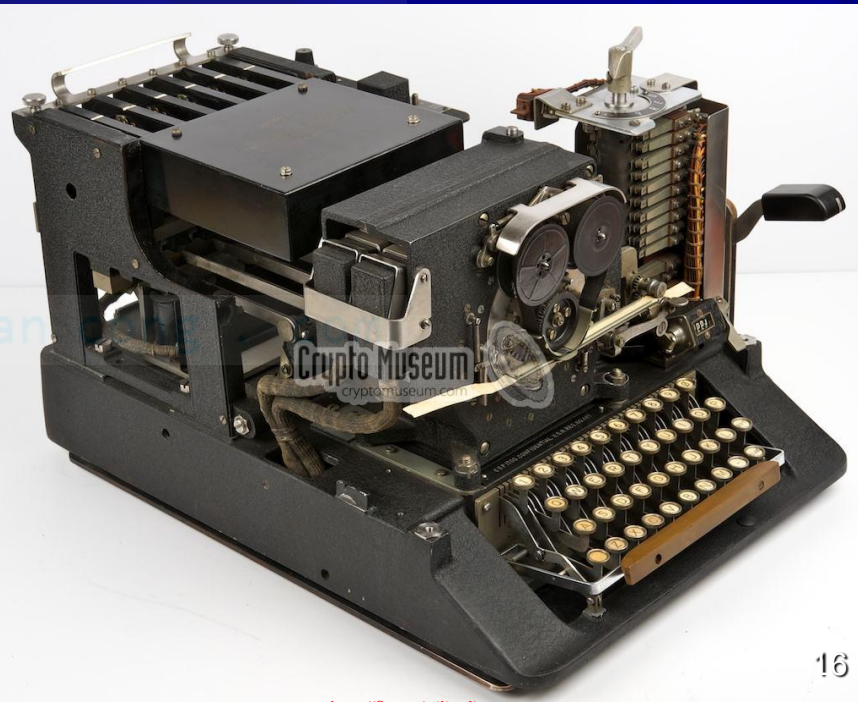
HEYGBZSK

Status Highlighted wires show encryption steps.

Máy Enigma

2. Lịch sử của mật mã

Máy Sigaba



Máy TypeX

2. Lịch sử của mật mã

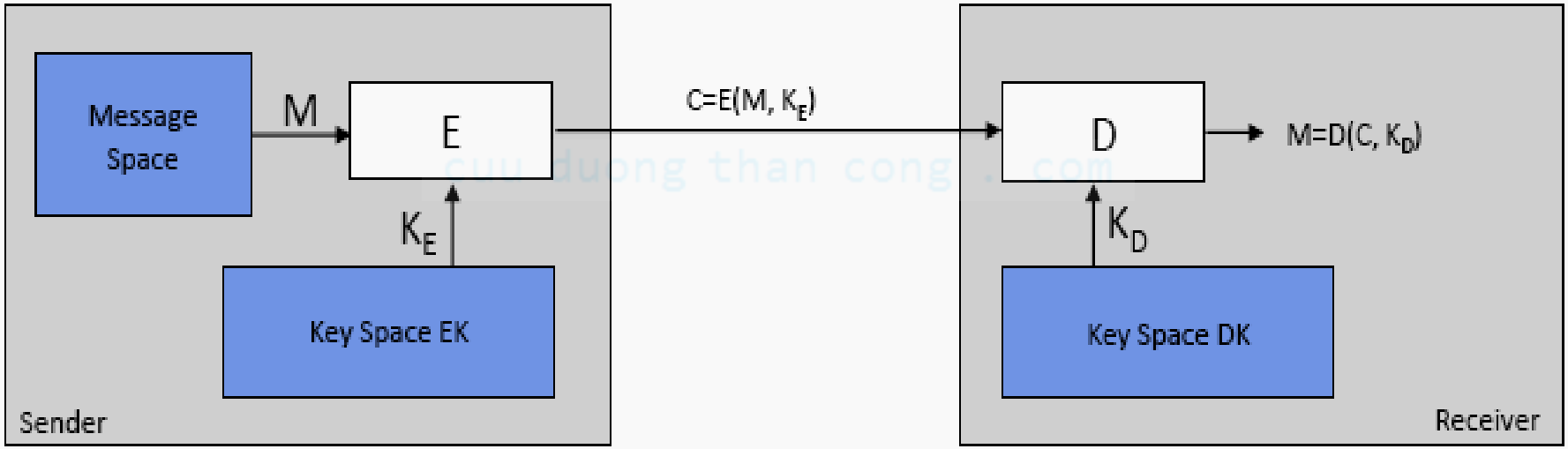
- **Mật mã học hiện đại**
  - Cha đẻ của mật mã học hiện đại là Claude Shannon.
  - Tiêu chuẩn mật mã hóa dữ liệu (**D**ata **E**ncryption **S**tandard) là một phương thức mã hoá được công bố tại Mỹ vào ngày 17.03.1975.
  - Với chiều dài khoá chỉ là 56-bit, DES đã được chứng minh là không đủ sức chống lại những tấn công kiểu vét cạn (*brute force attack - tấn công dùng bạo lực*).

2. Lịch sử của mật mã

- **Mật mã học hiện đại**
  - Năm 2001, DES đã chính thức được thay thế bởi AES (*Advanced Encryption Standard - Tiêu chuẩn mã hóa tiên tiến*).
  - Trước thời kỳ này, hầu hết các thuật toán mật mã hóa hiện đại đều là những thuật toán khóa đối xứng (*symmetric key algorithms*), trong đó cả người gửi và người nhận phải dùng chung một khóa, và cả hai người đều phải giữ bí mật về khóa này.
  - Đối với mật mã hóa dùng khóa bất đối xứng, người ta phải có một cặp khóa có quan hệ toán học để dùng trong thuật toán, một dùng để mã hóa và một dùng để giải mã. Phổ biến nhất là mã hoá RSA.

2. Lịch sử của mật mã

- **Mật mã học hiện đại**



a) Symmetric Encryption: $K_E = K_D$ (e.g. AES)

b) Asymmetric Encryption: $K_E \neq K_D$ (e.g. RSA)

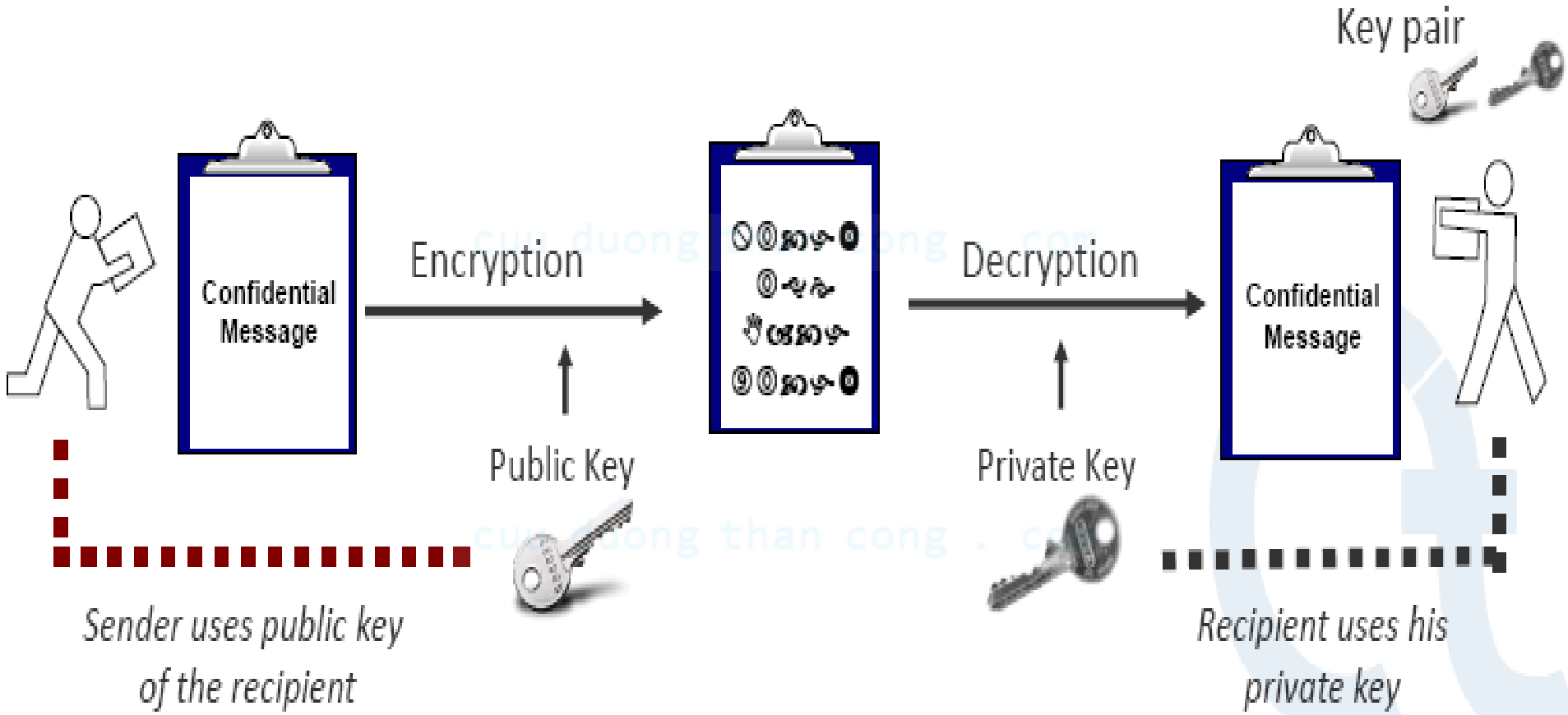
secret

public

private/secret

2. Lịch sử của mật mã

- **Mật mã học hiện đại**



Mã hoá RSA

3. Các giải thuật mã hoá cổ điển

- Các yêu cầu cơ bản đối với giải thuật mật mã hoá là:
  - Có tính bảo mật cao
  - Công khai, dễ hiểu. Khả năng bảo mật được chốt vào khoá chứ không vào bản thân giải thuật.
  - Có thể triển khai trên các thiết bị điện tử.

3. Các giải thuật mã hoá cổ điển

1. **Mã thay thế đơn giản (**Substitution Cipher**)**
   - Trong phép này, khoá là một hoán vị h của bảng chữ cái Z và mỗi ký hiệu của thông báo được thay thế bằng ảnh của nó qua hoán vị h.
   - Khoá thường được biểu diễn bằng một chuỗi 26 ký tự. Có 26! ($\approx 4.10^{26}$) hoán vị (khoá)
   - Ví dụ: khoá là chuỗi UXEOS…, ký hiệu A trong thông báo sẽ được thay bằng U, ký hiệu B sẽ được thay bằng X…
   - ⇨ Phá mã?

3. Các giải thuật mã hoá cổ điển

1. Mã thay thế đơn giản (Substitution Cipher)

- Chọn một hoán vị p: $Z_{26} \rightarrow Z_{26}$ làm khoá.
- VD:
  - Mã hoá

$e_p(a)=X$

a	b	c	d	e	f	g	h	i	j	k	l	m
X	N	Y	A	H	P	O	G	Z	Q	W	B	T

n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

  - Giải mã

$d_p(A)=d$

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	t

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	g	f	j	q	n	m	u	s	k	a	c	i

3. Các giải thuật mã hoá cổ điển

2. Mã thay thế n-gram

- Thay vì thay thế các ký tự, người ta có thể thay thế cho từng cụm 2 ký tự (diagram), 3 ký tự (trigram) hoặc tổng quát cho từng cụm n ký tự (n-gram).
- Với bảng chữ cái gồm 26 ký tự tiếng Anh thì phép thay thế n-gram sẽ có khoá là một hoán vị của 26^n n-gram khác nhau.
- ⇨ Phá mã?

3. Các giải thuật mã hoá cổ điển

2. Mã thay thế n-gram

Trong trường hợp diagram thì hoán vị gồm 26^2 diagram và có thể biểu diễn bằng một dãy 2 chiều 26x26 trong đó các hàng biểu diễn ký hiệu đầu tiên, các cột biểu diễn ký hiệu thứ hai, nội dung của các ô biểu diễn chuỗi thay thế.

	A	B	…
A	EG	RS	
B	BO	SC	
…			

3. Các giải thuật mã hoá cổ điển

3. Mã hoán vị bậc d (Permutation Cypher)

- Đối với một số nguyên dương d bất kỳ, chia thông báo m thành từng khối có chiều dài d. Rồi lấy một hoán vị h của 1, 2, …, d và áp dụng h vào mỗi khối.
- Ví dụ: nếu d=5 và h=(4 1 3 2 5), hoán vị (1 2 3 4 5) sẽ được thay thế bằng hoán vị mới (4 1 3 2 5).

3. Các giải thuật mã hoá cổ điển

3. Mã hoán vị bậc d

- Ví dụ: ta có thông báo

  m = JOHN IS A GOOD ACTOR

  Qua phép mã hoá này m sẽ trở thành chuỗi mật mã c sau:

  c = NJHO AI S DGOO OATCR

- ⇨ Phá mã?

3. Các giải thuật mã hoá cổ điển

4. **Mã dịch chuyển (Shift Cypher)**

   Vigenère và Caesar

- Trong phương pháp Vigenère, khoá bao gồm một chuỗi có d ký tự. Chúng được viết lặp lại bên dưới thông báo và được cộng modulo 26. Các ký tự trắng được giữ nguyên không cộng.
- Nếu d=1 thì khoá chỉ là một ký tự đơn và được gọi là phương pháp Caesar (được đưa ra sử dụng đầu tiên bởi Julius Caesar).
- ⇨ Phá mã?

	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

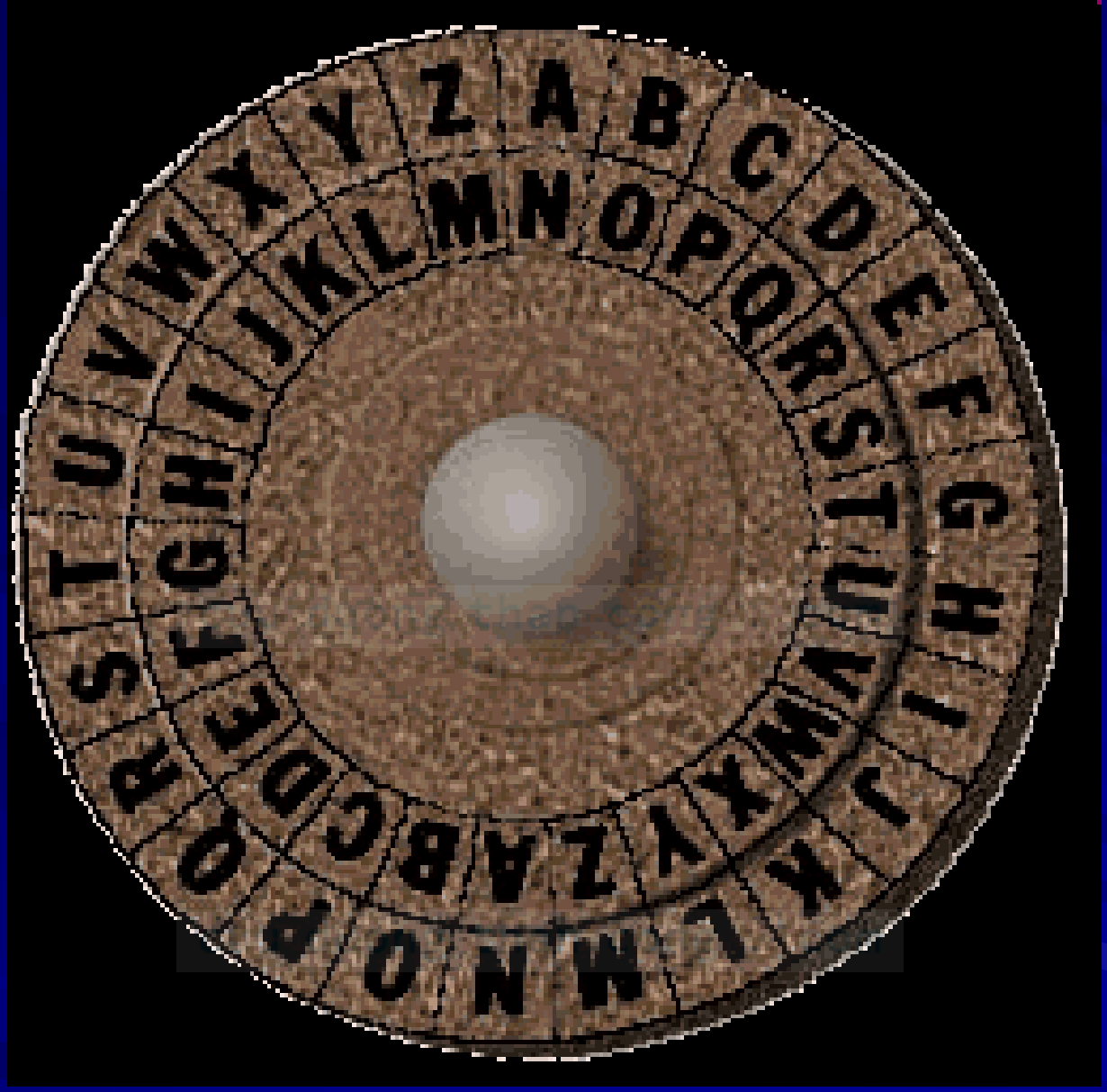
The classic Caesar Shift chart

Ví dụ:

Plaintext: CRYPTOGRAPHY

Ciphertext: HWDUYTLWFUMD (Shift of 5)

C=(p+5) mod 26



Mã dịch chuyển – Shift Cypher

Vigenère Encryption – Block Cypher (1523 – 1596)

Ví dụ:

Từ khoá: CHIFFRE

Mã hoá: VIGENERE

Kết quả: XPOJSVVG

	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

3. Các giải thuật mã hoá cổ điển

5. One - time Pad:

e=000 h=001 l=010 d=011 p=100 n=101 a=110

Encryption: Plaintext ⊕ Key = Ciphertext

Plaintext:	h	e	l	p	n	e	e	d	e	d
	001	000	010	100	101	000	000	011	000	011
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	110	101	100	001	010	100	000	110	110	011
	a	n	p	h	l	p	e	a	a	d

3. Các giải thuật mã hoá cổ điển

6. Mã tuyến tính (Affine Cipher)

Mã tuyến tính là mã thay thế có dạng:

$e(x) = ax + b \pmod{26}$, với $a, b \in \mathbf{Z}_{26}$.

Nếu a = 1 ta có mã dịch chuyển.

Giải mã: Tìm x?

$y = ax + b \pmod{26}$

$ax = y - b \pmod{26}$

$x = a^{-1}(y - b) \pmod{26}$.

3. Các giải thuật mã hoá cổ điển

7. Mã Playfair

Mật mã đa ký tự (mỗi lần mã hoá 2 ký tự liên tiếp nhau)

Giải thuật dựa trên một ma trận các chữ cái n×n (n=5 hoặc n=6) được xây dựng từ một khóa (chuỗi các ký tự).

Xây dựng ma trận khóa:

- Lần lượt thêm từng ký tự của khóa vào ma trận.
- Nếu ma trận chưa đầy, thêm các ký tự còn lại trong bảng chữ cái vào ma trận theo thứ tự A – Z.
- I và J xem như 1 ký tự.
- Các ký tự trong ma trận khoá không được trùng nhau.

3. Các giải thuật mã hoá cổ điển

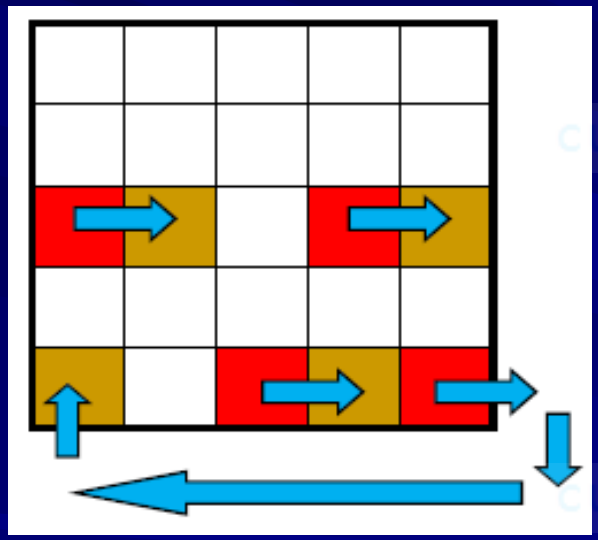
7. Mã Playfair

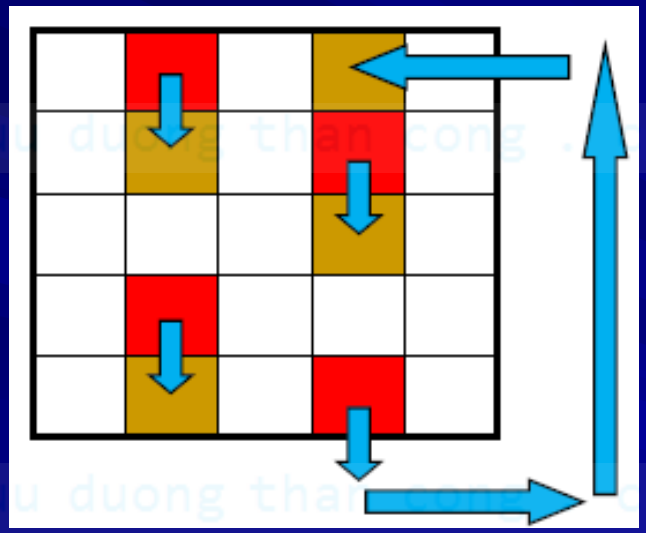
Giải thuật mã hóa:

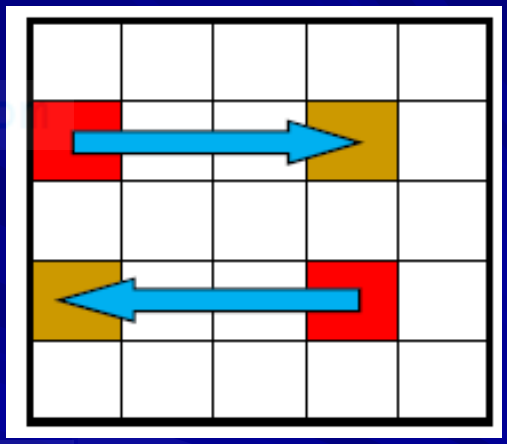
- Mã hóa từng cặp 2 ký tự liên tiếp nhau.
- Nếu dư 1 ký tự, thêm ký tự “x” vào cuối.
- Nếu 2 ký tự nằm cùng dòng, thay thế bằng 2 ký tự tương ứng bên phải. Ký tự ở cột cuối cùng được thay bằng ký tự ở cột đầu tiên.
- Nếu 2 ký tự nằm cùng cột được thay thế bằng 2 ký tự bên
- dưới. Ký tự ở hàng cuối cùng được thay thế bằng ký tự ở hàng trên cùng
- Nếu 2 ký tự lập thành hình chữ nhật được thay thế bằng 2 ký tự tương ứng trên cùng dòng ở hai góc còn lại.

3. Các giải thuật mã hoá cổ điển

7. Mã Playfair

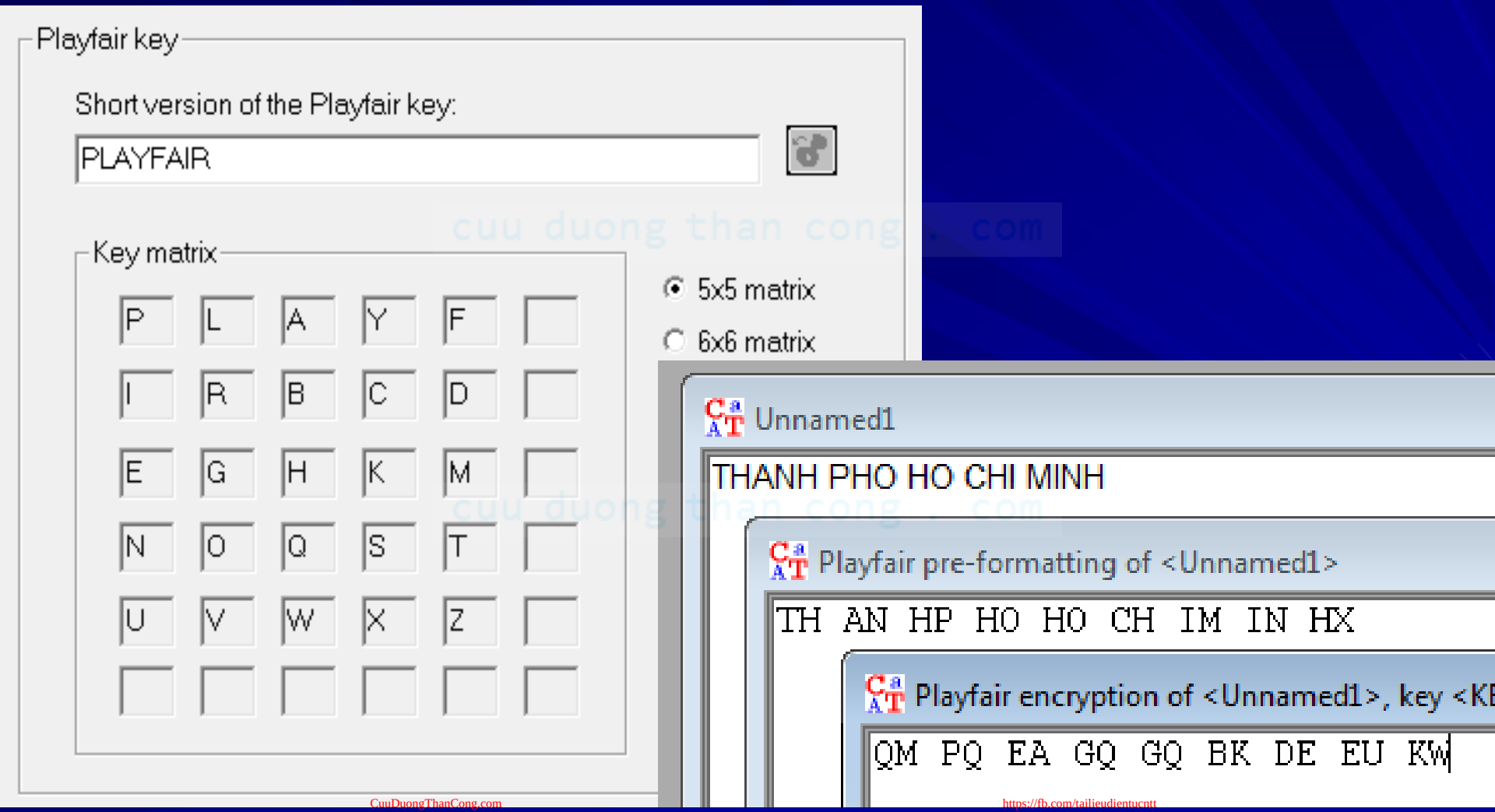






3. Các giải thuật mã hoá cổ điển

7. Mã Playfair



3. Các giải thuật mã hoá cổ điển

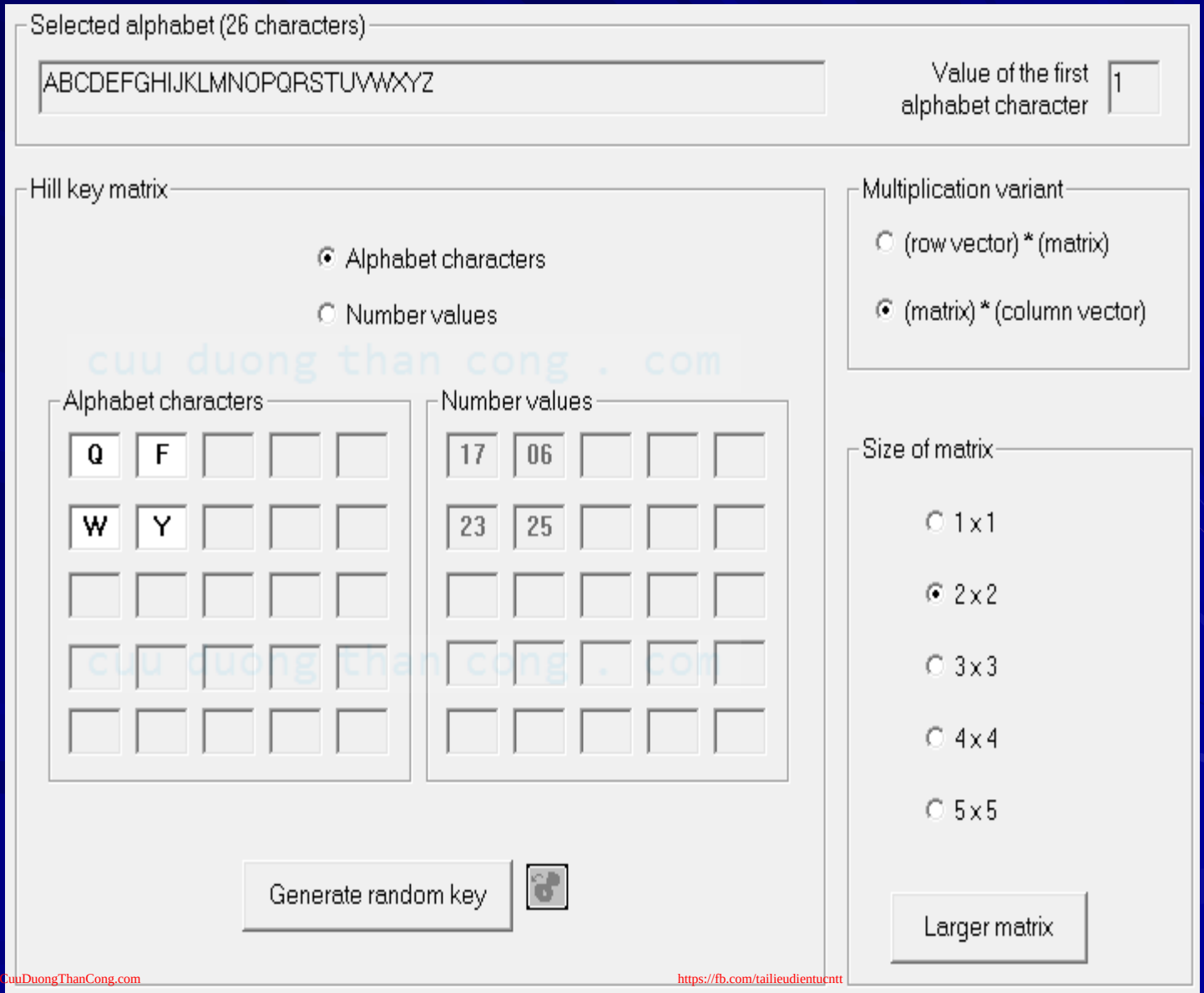
8. Mã Hill

Giải thuật mã hóa:

- Sử dụng m ký tự liên tiếp của plaintext và thay thế bằng m ký tự trong ciphertext với một phương trình tuyến tính trên các ký tự được gán giá trị lần lượt là A=01, B=02, …, Z=26.
- Chọn ma trận vuông Hill (ma trận H) làm khoá.
- Mã hoá từng chuỗi n ký tự trên plaintext (vector P) với n là kích thước ma trận vuông Hill.
- $C = HP \bmod 26$
- $P = H^{-1}C \bmod 26$

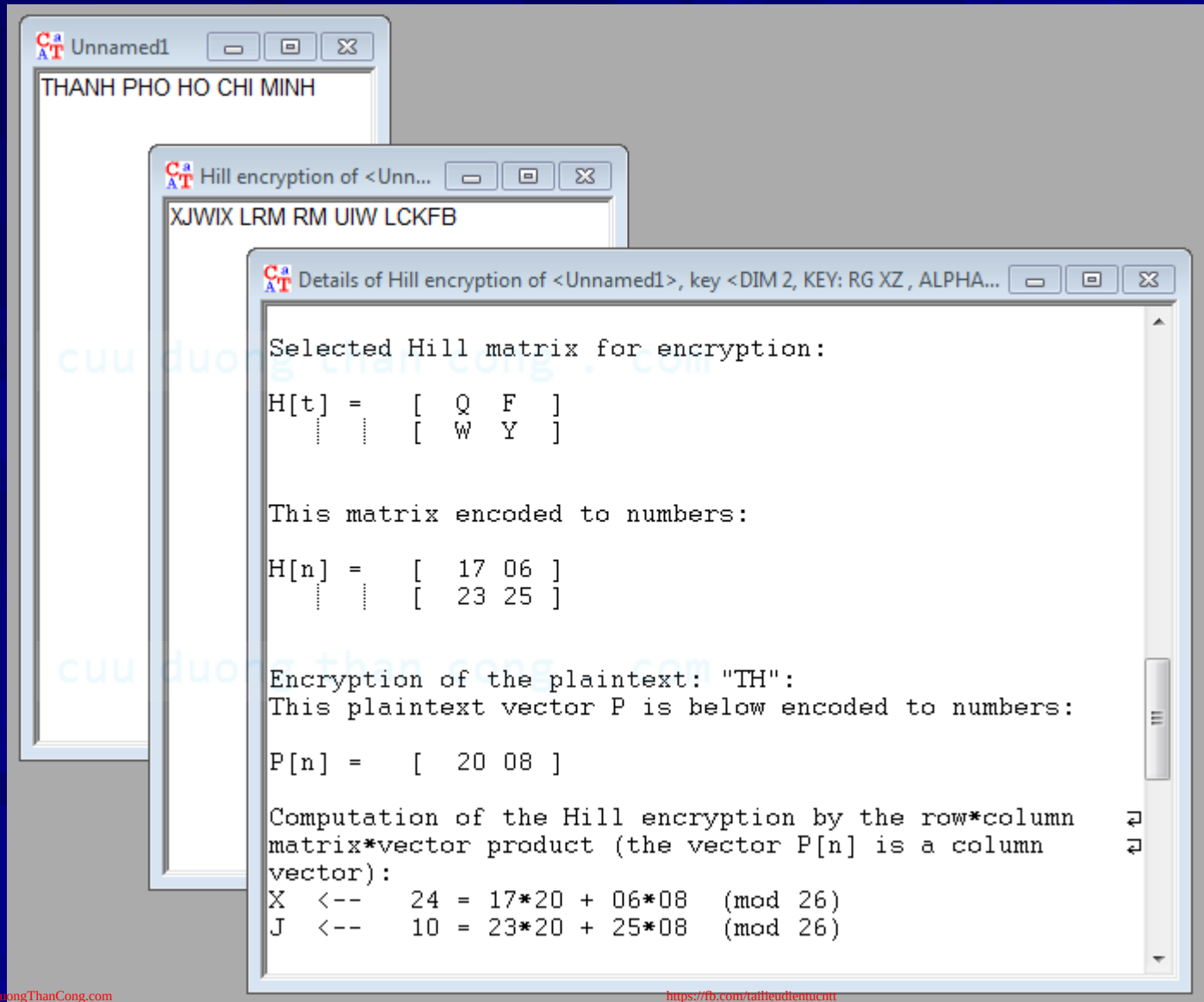
3. Các giải thuật mã hoá cổ điển

8. Mã Hill



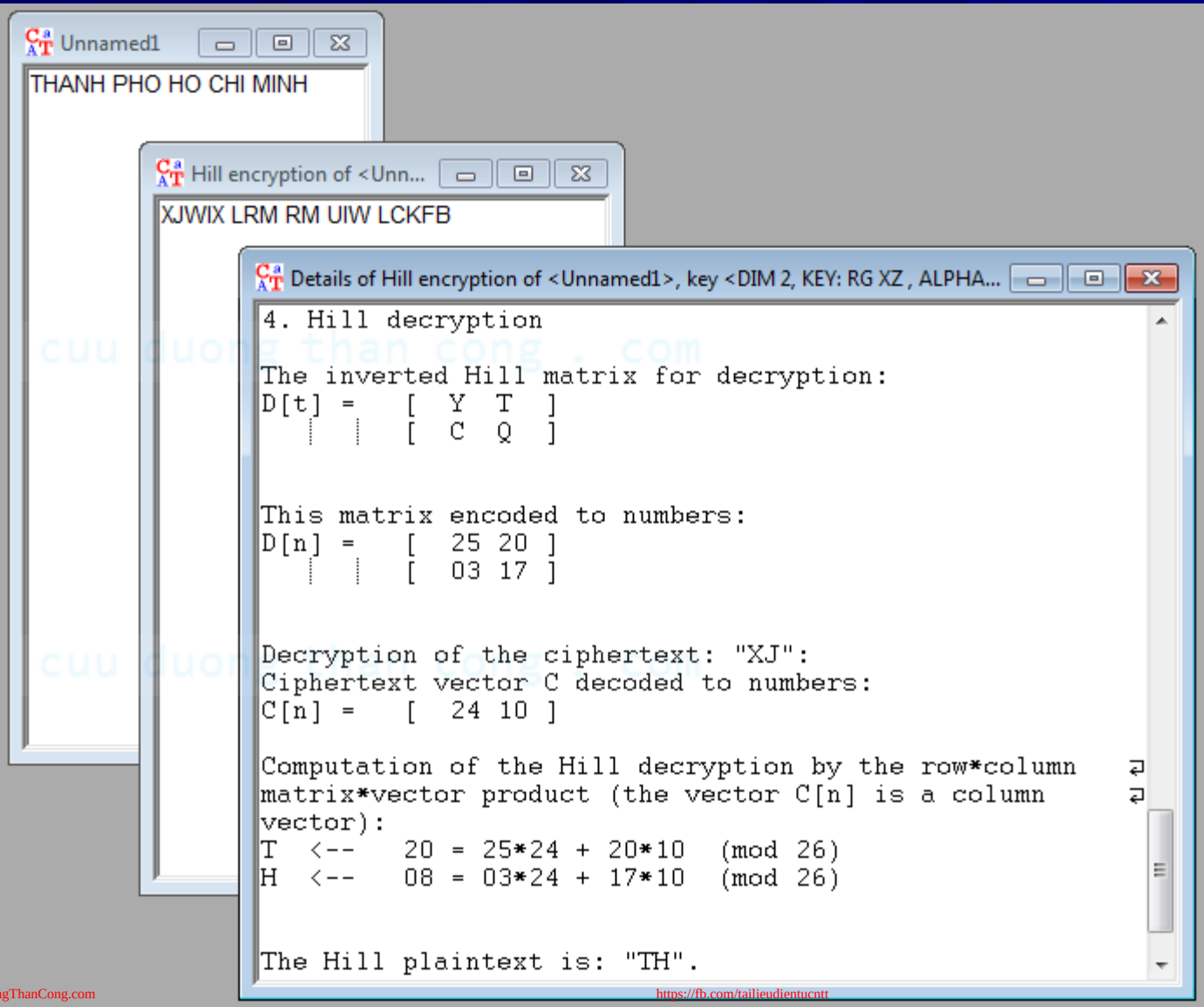
3. Các giải thuật mã hoá cổ điển

8. Mã Hill



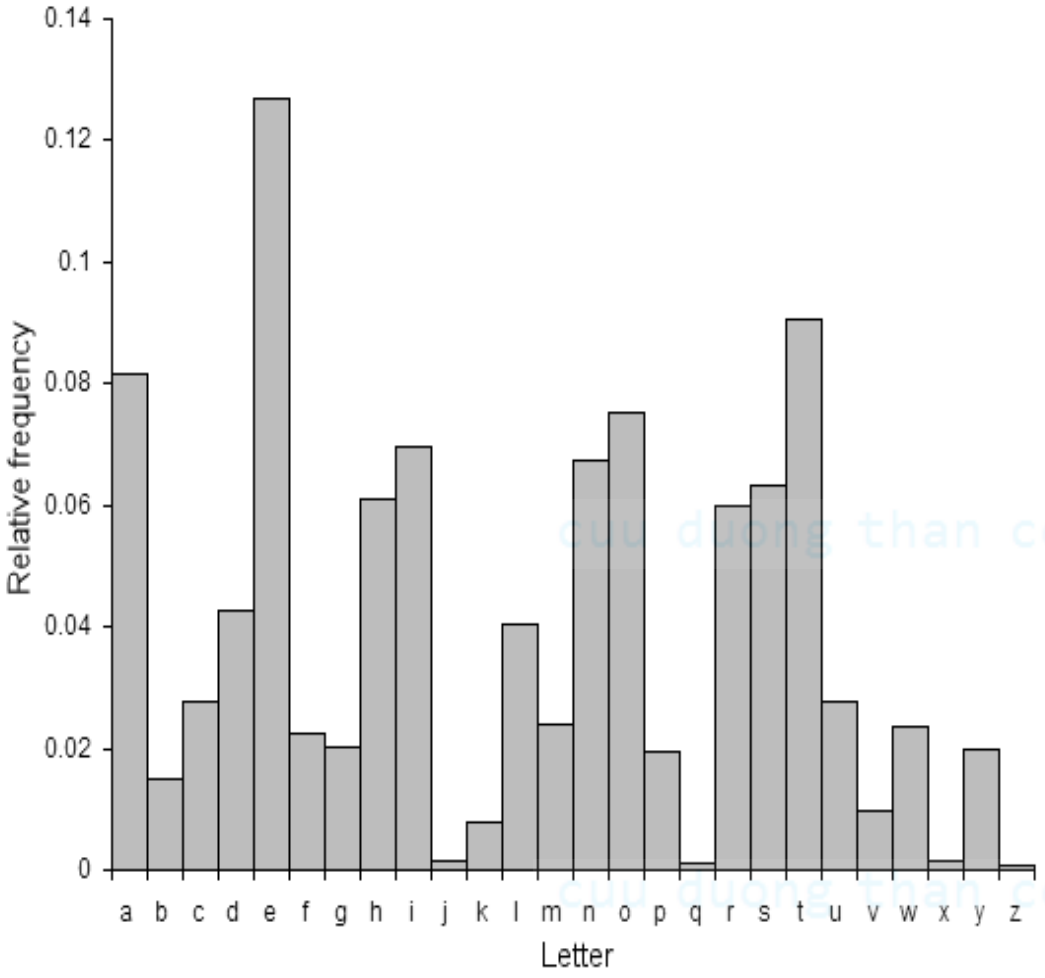
3. Các giải thuật mã hoá cổ điển

8. Mã Hill



3. Các giải thuật mã hoá cổ điển

9. **Phương pháp phá mã cổ điển:**
   - Dựa vào đặc điểm ngôn ngữ.
   - Dựa vào tần suất xuất hiện của các chữ cái trong bảng chữ cái thông qua thống kê từ nhiều nguồn văn bản khác nhau, dựa vào số lượng các ký tự trong bảng mã để xác định thông báo đầu vào.



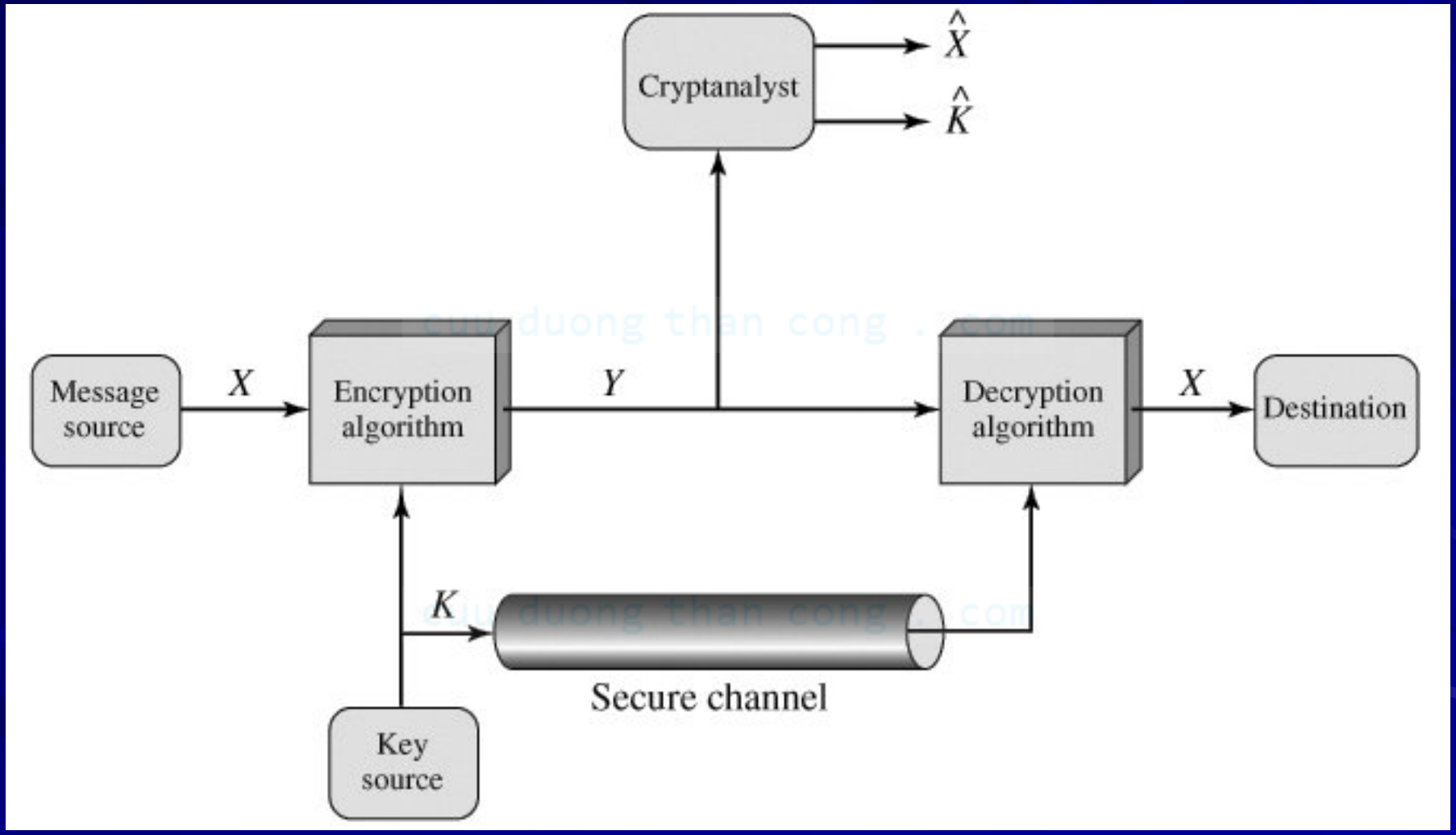
letter	probability	letter	probability
A	.082	*N*	.067
B	.015	*O*	.075
C	.028	*P*	.019
D	.043	*Q*	.001
E	.127	*R*	.060
F	.022	*S*	.063
G	.020	*T*	.091
H	.061	*U*	.028
I	.070	*V*	.010
J	.002	*W*	.023
K	.008	*X*	.001
L	.040	*Y*	.020
M	.024	*Z*	.001

Tần suất của các ký tự trong ngôn ngữ tiếng Anh

4. Bẻ gãy một hệ thống mật mã

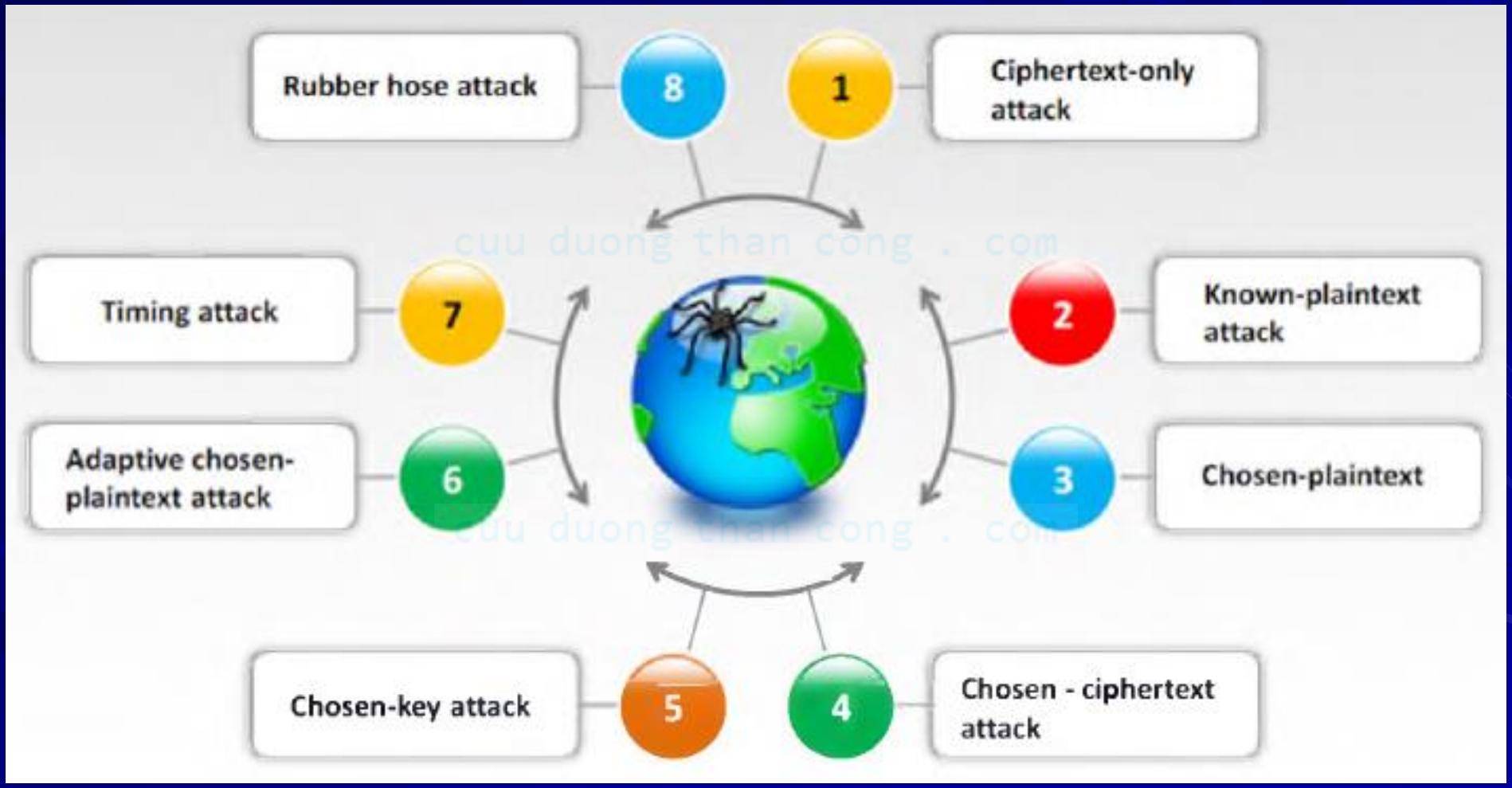
- Những chuyên gia mật mã hay những kẻ tấn công thường được giả thiết biết đầy đủ thông tin về hàm mã hoá e và hàm giải mã d.
- Các chuyên gia này cũng có thể có thêm nhiều thông tin hỗ trợ như các thống kê về ngôn ngữ, kiến thức về ngữ cảnh...
- Với một chuỗi mật mã nào đó, họ thiếu khoá k để có thể sử dụng d để giải mã c một cách chính xác.

4. Bẻ gãy một hệ thống mật mã



4. Bẻ gãy một hệ thống mật mã

Các khả năng tấn công trên hệ thống:



4. Bẻ gãy một hệ thống mật mã

Các khả năng tấn công trên hệ thống:

- Tấn công chỉ dựa trên chuỗi mật mã (crytogram-only attack): đối phương chỉ biết một vài mẫu chuỗi mật mã c.
- Tấn công dựa trên văn bản đã biết (known-plaintext attack): Trong trường hợp này những người tấn công được giả thiết là đã biết một độ dài đáng kể của văn bản thông báo và chuỗi mật mã tương ứng, và từ đó cố gắng tìm ra khoá.
- Tấn công dựa trên văn bản được chọn (chosen-plaintext attack): những người tấn công có thể đã có được một số lượng tuỳ ý của các cặp thông báo và chuỗi mật mã tương ứng (m, c).

4. Bẻ gãy một hệ thống mật mã

Các khả năng tấn công trên hệ thống:

Kiểu tấn công	Đối phương nắm được
ciphertext only attack	Chỉ văn bản mã c
known plaintext attack	Cả văn bản nguồn p và văn bản mã c
chosen plaintext attack	Đột nhập được vào **máy mã hoá**. Tự chọn văn bản p và mã hoá lấy được văn bản mã c tương ứng.
chosen ciphertext attack	Đột nhập được vào **máy giải mã**. Tự chọn văn bản mã c và giải mã lấy được văn bản p tương ứng.

4. Bẻ gãy một hệ thống mật mã

Thời gian trung bình để tìm khoá theo kiểu vét cạn

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 = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

4. Bẻ gãy một hệ thống mật mã

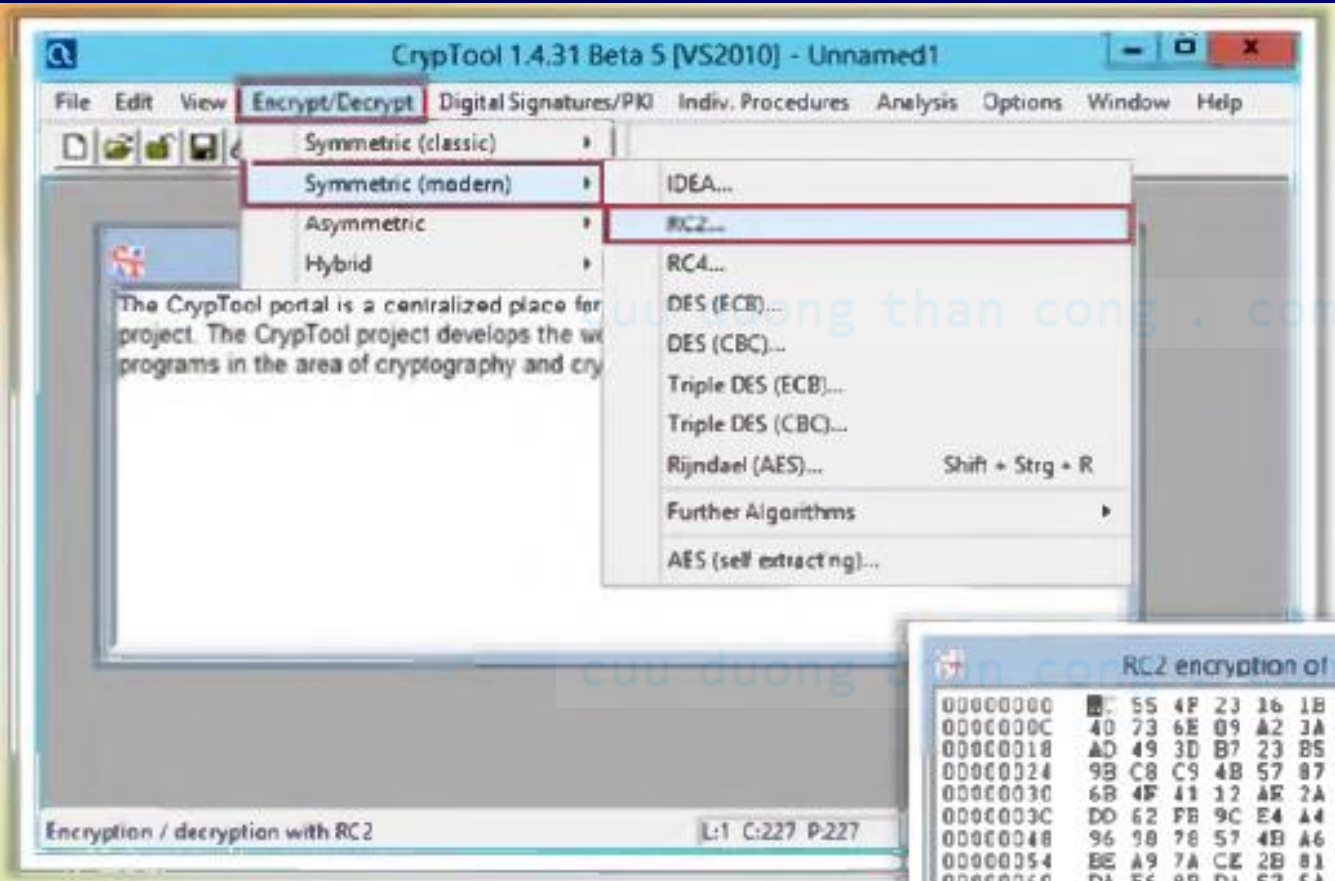
Thời gian trung bình để tìm khoá theo kiểu vét cạn

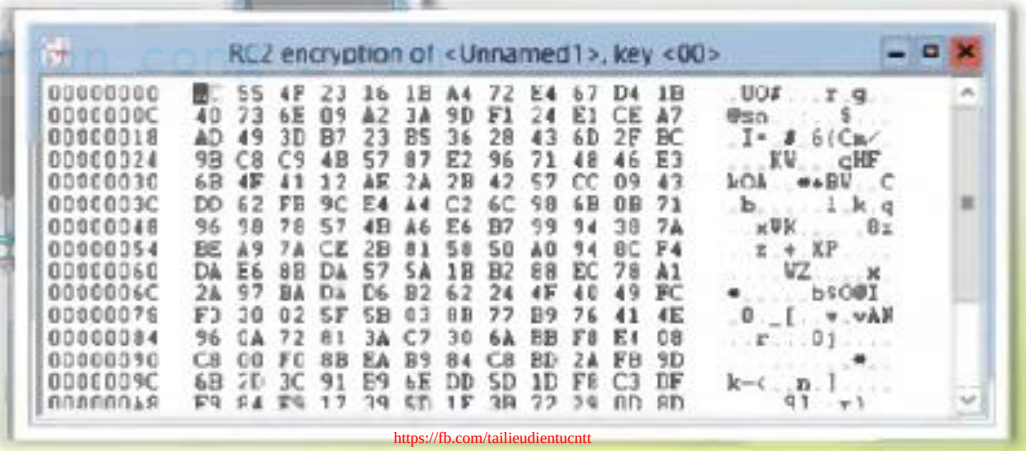
Power/Cost	40 bits (5 char)	56 bit (7 char)	64 bit (8 char)	128 bit (16 char)
$ 2K (1 PC. Can be achieved by an individual)	1.4 min	73 days	50 years	10^20 years
$ 100K (this can be achieved by a company)	2 sec	35 hours	1 year	10^19 years
$ 1M (Achieved by a huge organization or a state)	0.2 sec	3.5 hours	37 days	10^18 years

Estimate Time for Successful Bruteforce Attack

4. Bẻ gãy một hệ thống mật mã

Công cụ phân tích Cryptool

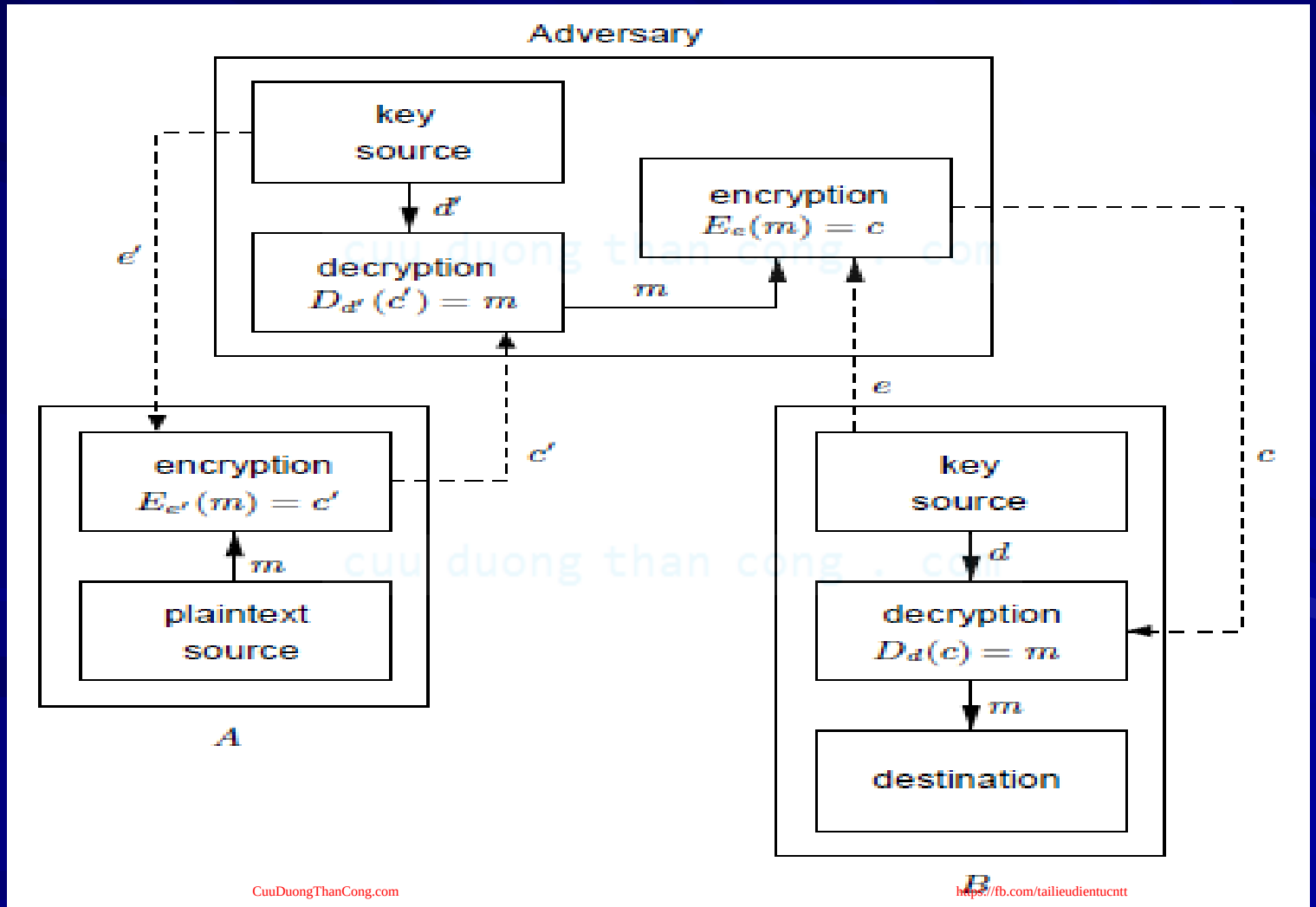




- CrypTool is a free e-learning program in the area of cryptography and cryptoanalysis
- Subprojects of CrypTool:
  - CrypTool 1 (CT1)
  - CrypTool 2 (CT2)
  - JCrypTool (JCT)
  - CrypTool-Online (CTO)

5. Bài tập

1. Giải thích cơ chế của việc bẻ gãy mật mã của hệ thống sau:



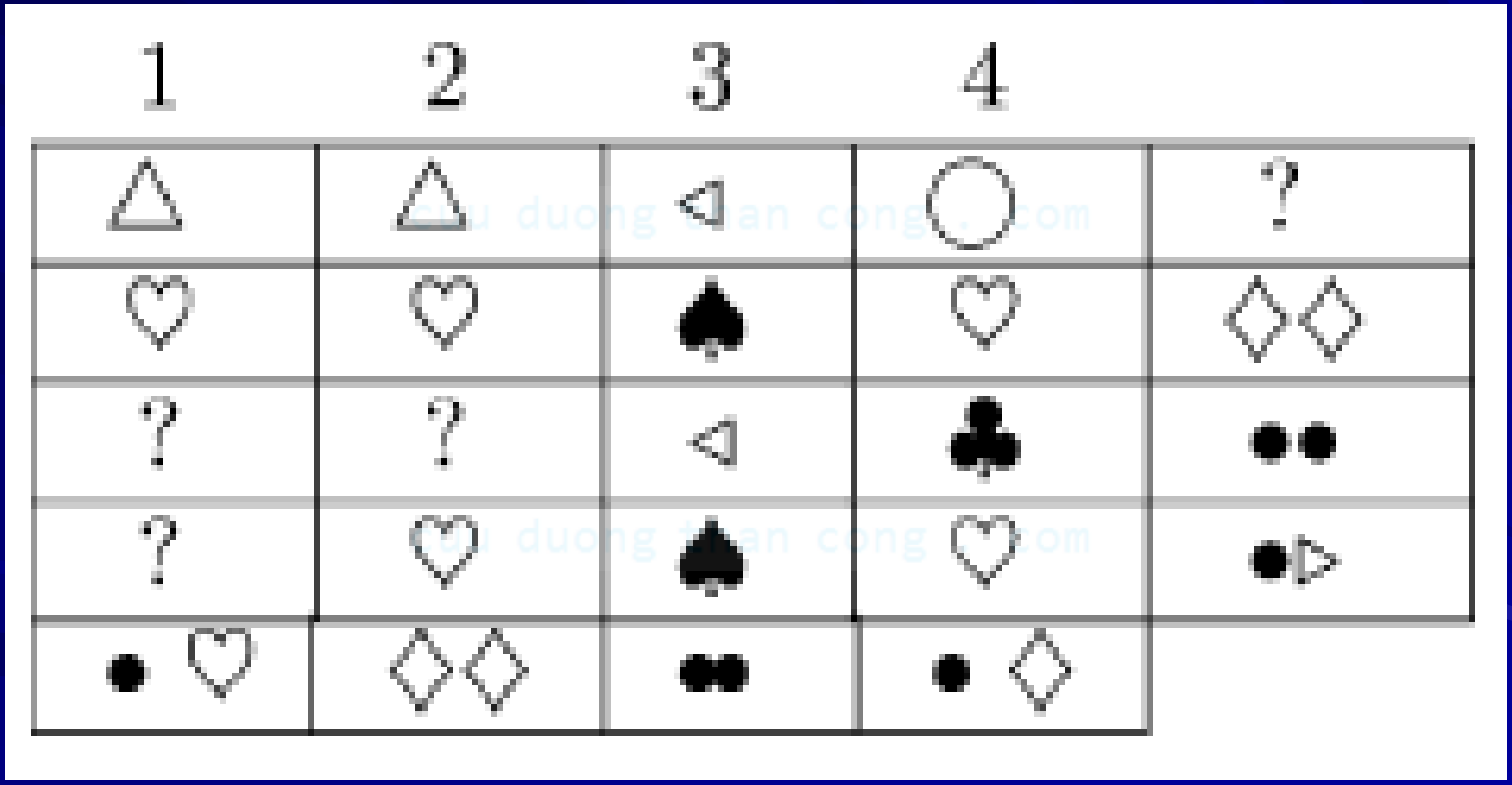
5. Bài tập

2. Tìm mã hoá của các ký số 1-9:

- Mỗi biểu tượng trong số chín biểu tượng xuất hiện trong mảng dưới đây (△◁▷○♥♠◊♣•) mã hóa duy nhất một trong các chữ số 1 đến 9.
- Cột ngoài cùng bên phải là các tổng số ở mỗi hàng
- Hàng dưới cùng cho các tổng số ở mỗi cột.
- Một dấu hỏi có thể đại diện cho bất kỳ một hoặc hai chữ số và không nhất thiết phải cùng một số trong mỗi trường hợp.

6. Bài tập

2. Tìm mã hoá của các ký số 1-9:



5. Bài tập

3. Sử dụng công cụ Cryptool

- Cryptool là một ứng dụng miễn phí chạy trên Windows, thường được sử dụng để phân tích các giải thuật mã hoá. Phiên bản hiện nay là 1.4.31.
- Địa chỉ download Cryptool:

http://www.cryptool.org/

5. Bài tập

4. Nêu cơ chế hoạt động và viết ứng dụng cho phép mã hoá và giải mã với những giải thuật mã hoá sau:
   - Vigenère
   - Hill.
   - Affine
   - Playfair
   - Solitaire