Các kỹ thuật mã hóa cổ điển

WWW.UIT.EDU.VN

TS. Nguyễn Tấn Cầm

Nội dung

WWW.UIT.EDU.VN

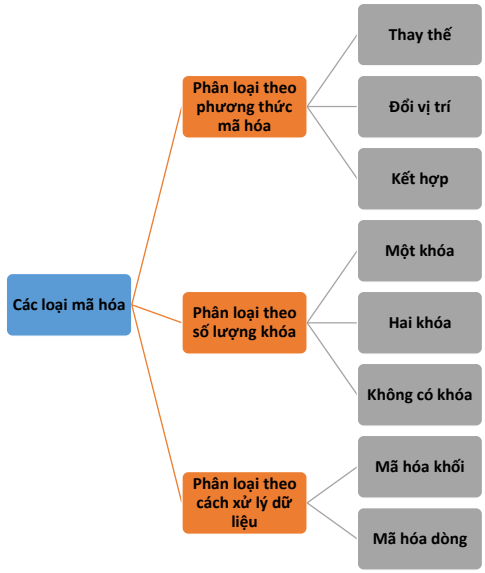
- Một số khái niệm liên quan đến kỹ thuật mã hóa
- Mã hóa đối xứng
- Caesar Cipher
- Playfair Cipher
- Vigenère Cipher
- Câu hỏi ôn tập

Một số khái niệm liên quan đến kỹ thuật mã hóa

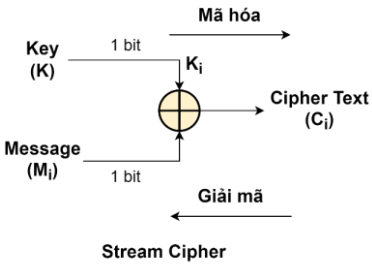
Một số khái niệm liên quan đến kỹ thuật mã hóa

- Plaintext:
  - là dữ liệu ban đầu trước khi được mã hóa. Trong sách này, chúng được ký hiệu là *P*.
- Ciphertext:
  - là dữ liệu đã được mã hóa. Trong sách này, chúng được ký hiệu là *C*.
- Encryption hoặc Enciphering:
  - là quá trình chuyển dữ liệu ban đầu sang dữ liệu đã được mã hóa. Trong sách này, chúng được ký hiệu là *E*.
- Cryptography:
  - là lĩnh vực nghiên cứu thiết kế các kỹ thuật mã hóa. Chúng ta có thể gom nhóm các kỹ thuật mã hóa dựa vào phương thức chuyển dữ liệu từ Plaintext sang Ciphertext, dựa vào số lượng khóa được sử dụng, và dựa vào cách xử lý plaintext.

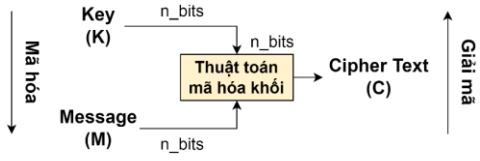
Một số khái niệm liên quan đến kỹ thuật mã hóa



Một số khái niệm liên quan đến kỹ thuật mã hóa



Stream Cipher



Block Cipher

Một số khái niệm liên quan đến kỹ thuật mã hóa

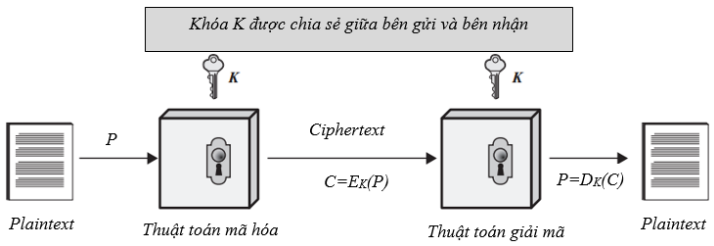
- Cryptanalysis:
  - là quá trình dịch ngược các dữ liệu đã mã hóa thành các chuỗi ban đầu mà không cần các kiến thức về quá trình mã hóa.
  - Có hai loại cryptanalysis là cryptanalytic attack và brute-force attack. Cryptanalytic sử dụng cách phân tích các đặc điểm của plaintext, thậm chí là cặp plaintext-cipher text để tìm khóa.
  - Trong khi đó, brute-force attack là kỹ thuật mà kẻ tấn công thử hết tất cả các khóa có thể có để tìm plaintext của một ciphertext nào đó.
- Cryptology:
  - là bao gồm cả hai lĩnh vực Cryptography và Cryptanalysis

Mã hóa đối xứng

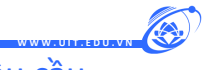
Mã hóa đối xứng

- Mã hóa đối xứng là mã hóa mà quá trình mã hóa và quá trình giải mã dùng chung khóa.
- Trong mã hóa đối xứng có các thành phần sau: dữ liệu dạng rõ (Plaintext), thuật toán mã hóa (Encryption algorithm), khóa bí mật (Secret key), dữ liệu đã được mã hóa (Ciphertext) và thuật toán giải mã (Decryption algorithm).
- Trong đó khóa bí mật (Secret key): là giá trị được dùng để mã hóa và giải mã. Trong mã hóa đối xứng, khóa bí mật này chỉ được biết bởi người gửi và người nhận

Mã hóa đối xứng



Mã hóa đối xứng

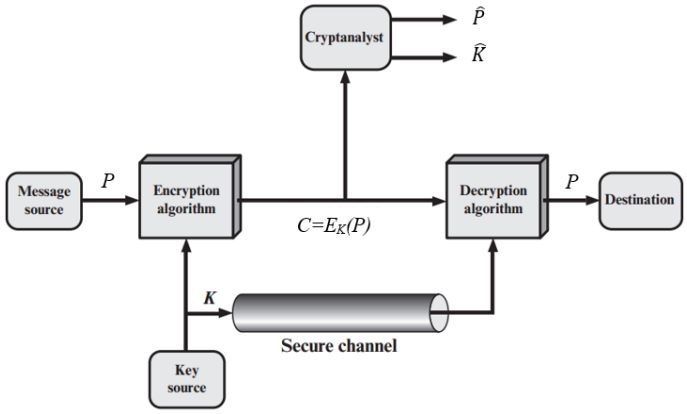


- Để đảm bảo tính bảo mật cho mã hóa đối xứng, chúng có hai yêu cầu chính sau:
  - Thuật toán mã hóa phải mạnh. Kẻ tấn công khó tìm ra dữ liệu gốc hoặc khóa bí mật từ dữ liệu đã được mã hóa. Ví dụ: thay vì mã hóa một lần, chúng ta có thể mã hóa nhiều lần trước khi gửi cho người nhận.
  - Khóa bí mật chỉ được biết bởi người gửi và người nhận. Do đó, cần phải có một kênh trao đổi khóa an toàn.

Mã hóa đối xứng

- Giả định rằng thuật toán mã hóa không cần được giữ bí mật.
- Do đó, một hệ thống mã hóa có thể bị vô hiệu hóa khi thuật toán mã hóa không đủ mạnh và kênh trao đổi khóa không an toàn.
- Hình sau trình bày mối liên hệ giữa Cryptography và Cryptanalysis. Trong đó, khóa bí mật *K* được chia sẻ giữa bên gửi và bên nhận thông qua kênh trao đổi khóa an toàn (Secure channel).
- Trong mô hình này, kẻ tấn công thực hiện việc tấn công hệ thống mã hóa (Cryptanalysis) bằng cách phân tích dữ liệu đã được mã hóa (*C)* để kỳ vọng có được dữ liệu trước khi mã hóa, và khóa bí mật.

Mã hóa đối xứng



13

Caesar Cipher

14

Caesar Cipher

- Mã hóa Caesar Cipher được biết đến là mã hóa thay thế (substitution) sớm nhất được đề xuất bởi Julius Caesar.
- Theo thuật toán Caesar Cipher, mỗi ký tự trong plaintext được thay thế bằng một ký tự cách nó *K* vị trí trong bảng chữ cái Alphabet.

Bảng 2.1. Ví dụ mã hóa bằng Caesar Cipher

Plaintext	INFORMATION TECHNOLOGY
Ciphertext	LQIRUPDWLRQ WHFKQRORJB

Bảng 2.2. Ví dụ cách thay thế ký tự

Plaintext	A B CDE FG H I J K L M N O P Q R S T U V W X Y Z
Ciphertext	D E FG H I J K L M N O P Q R S T U V W X Y Z A B C

15

Caesar Cipher

- Quá trình mã hóa của thuật toán Caesar Cipher được biểu diễn như sau:

$$C = E_K(P) = (P + K)\ mod\ 26$$

- Quá trình giải mã của thuật toán Caesar Cipher được biểu diễn như sau:

$$P = D_K(C) = (C - K)\ mod\ 26$$

- Ví dụ 1

$$Với\ K = 3, Plaintext\ là\ I, ta\ có$$

$$C = E_K(I) = (8 + 3)\ mod\ 26 = 11 \rightarrow L$$

- Như vậy, với thuật toán Caesar Cipher, khi khóa *K* là 3, ký tự *I* được mã hóa thành ký tự *L*.

16

Caesar Cipher

```
def encrypt(text,s):
    result = ""
    # transverse the plain text
    for i in range(len(text)):
        char = text[i]
        # Encrypt uppercase characters in plain text

        if (char.isupper()):
            result += chr((ord(char) + s-65) % 26 + 65)
        # Encrypt lowercase characters in plain text
        else:
            result += chr((ord(char) + s - 97) % 26 + 97)
    return result
#check the above function
text = "CEASER CIPHER DEMO"
s = 4

print ("Plain Text : " + text)
print ("Shift pattern : " + str(s))
print ("Cipher: " + encrypt(text,s))
```

Minh họa cách hiện thực thuật toán Caesar Cipher

Caesar Cipher

- Bởi vì thuật toán Caesar Cipher dùng khóa K có giá trị từ 1 đến 25. Điều này có nghĩa là chỉ có 25 giá trị cho khóa K.
- Đây được xem là điểm yếu của thuật toán này.
- Nó có thể dễ dàng bị tấn công bằng kỹ thuật vét cạn (Brute-force).
- Theo đó, kẻ tấn công có thể thử tất cả các trường hợp có thể có của khóa để tìm Plaintext.
- Hình sau trình bày một trường hợp tấn công bằng kỹ thuật Brute-force. Khóa cần tìm trong trường hợp này là 3.

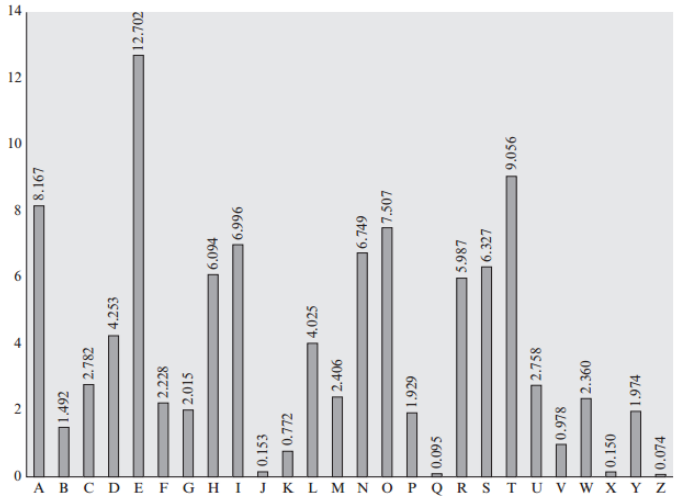
Caesar Cipher

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nfu 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

Caesar Cipher

- Một kỹ thuật tấn công khác là kỹ thuật phân tích thống kê.
- Vì mỗi ký tự trong Plaintext được mã hóa bằng cùng một khóa.
- Điều này có nghĩa là ánh xạ một ký tự trong Plaintext sang một ký tự trong Ciphertext.
- Như vậy, về mặt lý thuyết thì một ký tự trong Plaintext và ký tự được mã hóa thành của nó trong Ciphertext có xác suất giống nhau. Hình sau cho thấy trong ngôn ngữ tiếng Anh, tần số xuất hiện của ký tự E cao nhất.
- Như vậy, giả định rằng chúng ta có kích thước của chuỗi Ciphertext đủ lớn.
- Lúc đó, chúng ta thống kê tần số xuất hiện của các ký tự trong chuỗi Ciphertext.
- Ký tự nào có tần số xuất hiện nhiều nhất sẽ là ký tự được mã hóa của ký tự E trong Plaintext.
- Dựa vào cặp ký tự này, chúng ta có thể tính được khóa

Caesar Cipher



Minh họa thống kê tần số xuất hiện của mỗi ký tự

Playfair Cipher

Playfair Cipher

- Một trong những hạn chế của thuật toán Caesar Cipher là dễ bị tấn công theo kỹ thuật Brute-force và kỹ thuật phân tích thống kê.
- Do đó cần thiết phải có một thuật toán cho phép ánh xạ ký tự trong Plaintext và ký tự trong Ciphertext theo cơ chế ánh xạ "một - nhiều" (mỗi lần mã hóa, một ký tự có thể được mã hóa thành nhiều ký tự khác nhau) thay vì ánh xạ "một – một" (1-1) của thuật toán Caesar Cipher.
- Thuật toán Playfair Cipher là một thuật toán theo cơ chế ánh xạ "một - nhiều".

Playfair Cipher

- Thuật toán Playfair Cipher dựa vào ma trận 5x5.
- Ma trận này được xây dựng từ một từ khóa.
- Ví dụ, với từ khóa UNIVERSITY, ta có ma trận 5x5 như sau:

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

Hình 2.9. Ma trận khóa

Playfair Cipher

- Theo thuật toán Playfair Cipher, ma trận 5x5 được tạo thành bằng cách điền các ký tự trong từ khóa sao cho không trùng lắp, từ trái qua phải và từ trên xuống dưới.
- Các ô còn lại của ma trận sẽ được điền bởi các ký tự còn lại theo thứ tự Alphabe.
- Vì chúng ta chỉ có 25 ô trong ma trận, do đó chúng ta chỉ điền được 25 ký tự.
- Theo thuật toán Playfair Cipher, ký tự I và J được xem như là một ký tự I.

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

Hình 2.9. Ma trận khóa

25

Playfair Cipher

- Plaintext được mã hóa hai ký tự một lần.
- Quá trình mã hóa được thực hiện như sau:
  - Lặp lại quá trình gom nhóm hai ký tự liền nhau.
    - Nếu hai ký tự trong cùng một nhóm giống nhau, chúng ta chèn thêm ký tự phân cách vào (Thuật toán này đề xuất ký tự X).
    - Nếu thiếu một ký tự thì chúng ta thêm ký tự phân cách vào cho đủ cặp. Ví dụ, "MYBALLOONS" được gom thành các nhóm như sau: MY BA LX LO ON SX.

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

Hình 2.9. Ma trận khóa

26

Playfair Cipher

- Plaintext được mã hóa hai ký tự một lần.
- Quá trình mã hóa được thực hiện như sau:
  - Lặp lại quá trình gom nhóm hai ký tự liền nhau.
    - Nếu hai ký tự trong cùng một nhóm giống nhau, chúng ta chèn thêm ký tự phân cách vào (Thuật toán này đề xuất ký tự X).
    - Nếu thiếu một ký tự thì chúng ta thêm ký tự phân cách vào cho đủ cặp. Ví dụ, "MYBALLOONS" được gom thành các nhóm như sau: MY BA LX LO ON SX.
  - Mã hóa từng cặp ký tự này bằng cách tìm trong ma trận khóa:
    - Nếu hai ký tự này nằm trên cùng một cột, thì ký tự mã hóa là ký tự nằm dòng liền dưới, cùng cột. Nếu ký tự ở hàng cuối cùng thì được mã hóa bằng ký tự ở dòng đầu tiên cùng cột. Ví dụ: MY được mã hóa thành XF.

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

Hai ký tự nằm trên cùng một cột

Playfair Cipher

- Plaintext được mã hóa hai ký tự một lần.
- Quá trình mã hóa được thực hiện như sau:
  - Lặp lại quá trình gom nhóm hai ký tự liền nhau.
    - Nếu hai ký tự trong cùng một nhóm giống nhau, chúng ta chèn thêm ký tự phân cách vào (Thuật toán này đề xuất ký tự X).
    - Nếu thiếu một ký tự thì chúng ta thêm ký tự phân cách vào cho đủ cặp. Ví dụ, "MYBALLOONS" được gom thành các nhóm như sau: MY BA LX LO ON SX.
  - Mã hóa từng cặp ký tự này bằng cách tìm trong ma trận khóa:
    - Nếu hai ký tự này nằm trên cùng một dòng, thì ký tự mã hóa là ký tự nằm ở cột liền bên phải, cùng dòng. Nếu ký tự ở cột cuối cùng thì được mã hóa thành ký tự ở cột đầu tiên cùng dòng. Ví dụ: LO được mã hóa thành MH.

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

Hai ký tự nằm trên cùng một dòng

Playfair Cipher

- Plaintext được mã hóa hai ký tự một lần.
- Quá trình mã hóa được thực hiện như sau:
  - Lặp lại quá trình gom nhóm hai ký tự liền nhau.
    - Nếu hai ký tự trong cùng một nhóm giống nhau, chúng ta chèn thêm ký tự phân cách vào (Thuật toán này đề xuất ký tự X).
    - Nếu thiếu một ký tự thì chúng ta thêm ký tự phân cách vào cho đủ cặp. Ví dụ, "MYBALLOONS" được gom thành các nhóm như sau: MY BA LX LO ON SX.
  - Mã hóa từng cặp ký tự này bằng cách tìm trong ma trận khóa:
    - Trong các trường hợp còn lại, nếu hai ký tự tạo thành hình chữ nhật, thì ký tự mã hóa là ký tự nằm trên cùng dòng nhưng ở góc đối diện. Ví dụ: BA được mã hóa thành GR.

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

Hai ký tự tạo thành một hình chữ nhật

Vigenère Cipher

Vigenère Cipher

- Thuật toán Playfair Cipher dùng ma trận khóa có kích thước 5x5. Để tăng khả năng mã hóa một ký tự thành nhiều các ký tự khác, thuật toán Vigenère Cipher dùng ma trận 26x26. Ma trận này gọi là Vigenère Table.
- Hàng đầu tiên của bảng này có 26 chữ cái tiếng Anh. Bắt đầu với hàng thứ hai, mỗi hàng có các chữ cái dịch chuyển sang trái một vị trí theo cách tuần hoàn. Ví dụ, khi chữ B được chuyển đến vị trí đầu tiên trên hàng thứ hai, chữ A sẽ di chuyển về cuối cùng.
- Tuy nhiên, ma trận 26x26 là ma trận tham chiếu, không phải ma trận khóa như Playfair Cipher. Do đó, ma trận này không cần được giữ bí mật. Hình sau biểu diễn ma trận tham chiếu 26x26.

Vigenère Cipher

	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

Ma trận tham chiếu

Vigenère Cipher

Plaintext: **MICHIGAN TECHNOLOGICAL UNIVERSITY**
Keyword: **HOUGHTON**

```
MICHIGAN TECHNOLOGICAL UNIVERSITY
HOUGHTON HOUGHTONHOUGH TONHOUGNTO
```

```
MICHI GANTE CHNOL OGICA LUNIV ERSIT Y
HOUGH TONHO UGHTO NHOUG HTONH OUGHT O
```

```
MICHI GANTE CHNOL OGICA LUNIV ERSIT Y
HOUGH TONHO UGHTO NHOUG HTONH OUGHT O
TWWNP ZOAAS WNUHZ BNWWG SNBVC SLYPM M
```

	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

https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html

Vigenère Cipher

- Ngoài Plaintext, mật mã Vigenère cũng yêu cầu một từ khóa (keyword), được lặp lại sao cho tổng độ dài bằng với độ dài của bản rõ.
- Ví dụ, giả sử bản rõ là INFORMATION TECHNOLOGY và từ khóa là UNIVERSITY. Sau đó, từ khóa phải được lặp lại như sau:

Bảng 2.5. Minh họa cách tạo khóa từ từ khóa

I	N	F	O	R	M	A	T	I	O	N		T	E	C	H	N	O	L	O	G	Y
U	N	I	V	E	R	S	I	T	Y	U		N	I	V	E	R	S	I	T	Y	U

Vigenère Cipher

- Qui tắc mã hóa của thuật toán Vigenère Cipher như sau:
  - Đọc từng ký tự *t* trong plaintext và một ký tự *k* trong từ khóa.
  - *t* được mã hóa bằng thuật toán Caesar Cipher với khóa là *k*.
  - Ký tự kế tiếp trong Plaintext được mã hóa bằng khóa là ký tự kế tiếp trong từ khóa.
  - Khi từ qua khỏi ký tự cuối cùng trong từ khóa, thì ký tự kế tiếp trong Plaintext sẽ được mã hóa ký tự bắt đầu của từ khóa.
  - Lúc này $C_i = (P_i + K_{i \bmod m}) \bmod 26$, với *m* là chiều dài của từ khóa.

Câu hỏi ôn tập

Câu hỏi ôn tập

- **Câu 1:** Mô tả các yêu cầu chính đối với việc sử dụng an toàn mã hóa đối xứng.
- **Câu 2:** Trình bày sự khác biệt giữa mã hóa khối và mã hóa dòng. Vẽ hình minh họa.
- **Câu 3:** Trình bày hai hướng tiếp cận cơ bản để tấn công một thuật toán mã hóa.
- **Câu 4:** Tại sao thuật toán mã hóa Caesar Cipher có khả năng bị tấn công vét cạn (Brute-force attack)?
- **Câu 5:** Trình bày mối liên hệ giữa thuật toán Caesar Cipher và thuật toán Vigenère Cipher.

Câu hỏi trắc nghiệm

Câu hỏi trắc nghiệm

- Câu 2.1:
  - Phát biểu nào sau đây đúng:
  - Phát biểu A: Encryption hoặc Enciphering là lĩnh vực nghiên cứu thiết kế các kỹ thuật mã hóa
  - Phát biểu B: Cryptography là quá trình chuyển dữ liệu ban đầu sang dữ liệu đã được mã hóa.
    - A. Phát biểu A đúng, Phát biểu B sai
    - B. Phát biểu A sai, Phát biểu B đúng
    - C. Phát biểu A và B đúng
    - D. Phát biểu A và B sai.

Câu hỏi trắc nghiệm

- Câu 2.2:
  - Phát biểu nào sau đây đúng:
  - Phát biểu A: Mã hóa đối xứng là mã hóa mà quá trình mã hóa và quá trình giải mã dùng chung khóa.
  - Phát biểu B: Mã hóa đối xứng là mã hóa mà quá trình mã hóa và quá trình giải mã dùng hai khóa khác nhau.
    - A. Phát biểu A đúng, Phát biểu B sai
    - B. Phát biểu A sai, Phát biểu B đúng
    - C. Phát biểu A và B đúng
    - D. Phát biểu A và B sai.

Câu hỏi trắc nghiệm

- Câu 2.3:
  - Thuật toán nào sau đây mỗi ký tự trong plaintext được thay thế bằng một ký tự cách nó *K* vị trí trong bảng chữ cái Alphabet.
    - A. Playfair Cipher
    - B. DES
    - C. Vigenere Cipher
    - D. Caesar Cipher

Câu hỏi trắc nghiệm

- Câu 2.4:
  - Quá trình mã hóa của thuật toán Caesar Cipher được biểu diễn như thế nào?
    - A. $C = E_K(P) = (P - K)\ mod\ 26$
    - B. $C = E_K(P) = (P + K)\ mod\ 26$
    - C. $C = E_K(P) = (K - P)\ mod\ 24$
    - D. $C = E_K(P) = (P + K)\ mod\ 24$

Câu hỏi trắc nghiệm

- Câu 2.5:
  - Trong thuật toán Playfair Cipher, phát biểu nào sau đây đúng?
  - Phát biểu A: Nếu hai ký tự này nằm trên cùng một cột, thì ký tự mã hóa là ký tự nằm dòng liền dưới, cùng cột.
  - Phát biểu B: Nếu hai ký tự này nằm trên cùng một dòng, thì ký tự mã hóa là ký tự nằm ở cột liền bên phải, cùng dòng.
    - A. Phát biểu A đúng, Phát biểu B sai
    - B. Phát biểu A sai, Phát biểu B đúng
    - C. Phát biểu A và B đúng
    - D. Phát biểu A và B sai.