



Bảo mật thông tin thương mại điện tử bài tập mã hóa

khoa học dữ liệu (University of Economics HCMC)



Scan to open on Studocu

BÀI TẬP:

Cho bản tin: $M=[\text{Họ tên sinh viên}]$, ví dụ $M=\text{"NguyenVanA"}$ sử dụng ký tự không dấu. Hãy sử dụng các phương pháp mã hóa cổ điển để mã hóa bản tin M . Hãy thực hiện các công việc sau:

1. Mã hóa Caesar với $K=[\text{ngày sinh}]$, nếu ngày sinh > 26 thì $k=[\text{ngày sinh}]-26$
2. Mã hóa chữ đơn với $K=\text{JZNHOCTQKLPBYDIWGEAUVXMSRF}$
3. Mã hóa Vigenère với $K=\text{baomat}$ với quá trình lặp khóa và khóa tự động
4. Mã hóa Playfair với $K=\text{baomattt}$
5. One-Time Pad (OTP) với $K=\text{antt}$ (lặp khóa cho đủ độ dài), nếu phép cộng đó > 26 thì $\text{Ketqua} = \text{Phép cộng} - 26$
6. Mã hóa hoán vị $K=[\text{tháng sinh}]$, nếu tháng sinh là tháng 1 hoặc tháng 2 thì cộng thêm $K=[\text{tháng sinh}] + 4$

Bài làm:

$M=\text{"Tran Anh Hoang"}$

Ngày sinh: 01/12/2000

1. Mã hóa Caesar với $K=[\text{ngày sinh}]$, nếu ngày sinh > 26 thì $k=[\text{ngày sinh}]-26$

Ta có:

$$k=[\text{ngày sinh}] = 1$$

CBD	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
CTT	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

=> **Mã hóa Caesar**

IP	T	R	A	N	A	N	H	H	O	A	N	G
OP	W	U	D	Q	D	Q	K	K	R	D	Q	J

2. Mã hóa chữ đơn với $K=\text{JZNHOCTQKLPBYDIWGEAUVXMSRF}$

CBD	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
-----	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

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

=> Mã hóa chữ đơn với K=JZNHOC TQKLPBYDIWGEAUVXMSRF

IP	T	R	A	N	A	N	H	H	O	A	N	G
OP	U	E	J	D	J	D	Q	Q	I	J	D	T

3. Mã hóa Vigenère với K=baomat với quá trình lập khóa và khóa tự động

CÁCH 1: Lập khóa với K = BAOMAT

M=	T	R	A	N	A	N	H	H	O	A	N	G
K=	B	A	O	M	A	T	B	A	O	M	A	T

	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

OP	U	R	O	Z	A	G	I	H	C	M	N	Z
----	---	---	---	---	---	---	---	---	---	---	---	---

CÁCH 2: KHÓA TỰ ĐỘNG

M=	T	R	A	N	A	N	H	H	O	A	N	G
K+												
M	B	A	O	M	A	T	T	R	A	N	A	N

=>

OP	U	R	O	Z	A	G	A	Y	O	N	N	T
----	---	---	---	---	---	---	---	---	---	---	---	---

4. Mã hóa Playfair với K=baomattt

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Mã trộn 5*5 Với K=baomattt

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

Ta có:

M=	T	R	A	N	A	N	H	H	O	A	N	G
----	---	---	---	---	---	---	---	---	---	---	---	---

=>

TR	AN	AN	HH	OA	NG
OU	TI	TI	NN	AB	GT

5. One-Time Pad (OTP) với K=antt (lặp khóa cho đủ độ dài), nếu phép cộng đó >26 thì

Ketqua=Phép cộng - 26

Ta có: K=antt ; M=TRANANHHOANG

a	b	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

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

M		K		m+k	OP	
T	20	A	1	21	21	U
R	18	N	14	32	32	Z
A	1	T	20	21	21	U
N	14	T	20	34	34	B
A	1	A	1	2	2	B
N	14	N	14	28	28	B
H	8	T	20	28	28	B
H	8	T	20	28	28	B
O	15	A	1	16	16	P
A	1	N	14	15	30	X
N	14	T	20	34	34	B
G	7	T	20	27	27	A

6. Mã hóa hoán vị $K=[\text{tháng sinh}]$, nếu tháng sinh là tháng 1 hoặc tháng 2 thì cộng thêm $K=[\text{tháng sinh}] + 4$

NGÀY THÁNG NĂM SINH: 01/12/2000

Ta có: $K=12$; $M=\text{TRANANH HOANG}$

1	2	3	4	5	6	7	8	9	10	11	12
T	R	A	N	A	N	H	H	O	A	N	G
X	X	X	X	X	X	X	X	X	X	X	X
X	X	X	X	X	X	X	X	X	X	X	X

$\Rightarrow \text{OP} = \text{TXX RXX AXX NXX AXX NXX HXX HXX OXX AXX NXX GXX}$

-HẾT-