جامعة الأهرام الكندية
AHRAM CANADIAN UNIVERSITY
Faculty of Computer Science & IT

Course name: Information Security
Course Code: CNE308
Lecturer: Dr. Ahmed ElShafee

Exam number: Midterm, model answer
Exam Date: 28/04/2014
Time Allowed: 60 minutes

Name:

ID:

1	2	3	4	5	6.1	6.2	6.3	7.1	7.2	7.3	Total
4	2	4	4	4	1	1	5	1	1	3	30

Standard English plaintext characters space decimal cods

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
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. Encrypt the following message using affine cipher "**enemy at the gate**." Using the following key pairs (**r, k**). Assume that the 26 plain English characters is the used characters space.

Answer

plain

e	n	e	m	y	a	t	t	h	e	g	a	t	e
4	13	4	12	24	0	19	19	7	4	6	0	19	4

Keys pair

r	k
17	10

Cipher

0	23	0	6	2	10	21	21	25	0	8	10	21	0
a	x	a	g	c	k	v	v	z	a	i	k	v	a

Ciphertext

. . . . . .

. . . . . .

. . . . . .

2. find the multiplicative inverse of key "r" modulus 26.

answer

r == 17

17^{-1} mode 26 = 23

23 == x

3. Using Affine cipher and the same key pair of (1) to decrypt the following message "**uaknavnkffajkxjomvoremffpqae**", Assume that the 26 plain English characters is used characters space.

answer

plain

u	a	k	n	a	v	n	k	f	f	a	j	k	x	j	o	m	v	o	r	e	m	f	f	p	q	a	e
20	0	10	13	0	21	13	10	5	5	0	9	10	23	9	14	12	21	14	17	4	12	5	5	15	16	0	4

Keys pair

k	$r^{-1} = X$
10	23

Cipher

22	4	0	17	4	19	17	0	15	15	4	3	0	13	3	14	20	19	14	5	18	20	15	15	11	8	4	18
w	e	a	r	e	t	r	a	p	p	e	d	a	n	d	o	u	t	o	f	s	u	p	p	l	i	e	s

Ciphertext

. . . . . .

. . . . . .

. . . . . .

4. Using playfair cipher, encrypt the following message "**burn stuff they discovered you**", using the following key "**password**". Assuming that the used characters space is the 26 plain English characters.

answer

Playfair box

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

Plain/Cipher

b	u	r	n	s	t	u	f	f	t	h	e	y	d	i	s	c	o	v	e	r	e	d	y	o	u
r	x	b	l	o	n	p	l	k	l	k	b	v	c	h	w	e	w	z	d	e	c	c	v	p	z

Ciphertext

. . . . . .

. . . . . .

5. Using playfair cipher, encrypt the following message "**zeptomkzkbxcecoghqpmecdgxv**", using the following key "**password**". Assuming that the used characters space is the 26 plain English characters.

answer

Playfair box

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

Cipher/Plain

z	e	p	t	o	m	k	z	k	b	x	c	e	c	o	g	h	q	p	m	e	c	d	g	x	v
t	o	o	l	a	t	e	t	h	e	y	b	r	e	a	k	i	n	a	l	r	e	a	d	y	

plaintext

. . . . . .

. . . . . .

6. a rotor of three wheels and reflector used to decrypt the following message "**hak**". Find

6.1 rotor period.

6.2 total number of trials to find the plaintext (brute force attack)

6.3 find the plaintext.

Rotor:

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

answer

6.1 period = $26^3 = 17576$

6.2 brute force attack = $(26!)^3 = 6.56 \times 10^{79}$

1st character

h
07

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
v	h	r	z	c	i	o	g	x	l	n	b	k	f	e	p	w	u	s	t	a	j	q	y	d	m
21	7	17	25	2	8	14	6	23	11	13	1	10	5	4	15	22	20	18	19	0	9	16	24	3	12
q	e	k	w	m	y	j	a	p	b	n	l	r	i	x	h	f	v	g	s	d	c	z	u	t	o
16	4	10	22	12	24	9	0	15	1	13	11	17	8	23	7	5	21	6	18	3	2	25	20	19	14
e	p	b	u	s	a	i	g	q	y	w	f	j	x	d	t	v	r	z	k	h	m	l	n	c	o
4	15	1	20	18	0	8	6	16	24	22	5	9	23	3	19	21	17	25	10	7	12	11	13	2	14

2
c

2nd character

a
0

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
m	v	h	r	z	c	i	o	g	x	l	n	b	k	f	e	p	w	u	s	t	a	j	q	y	d
12	21	7	17	25	2	8	14	6	23	11	13	1	10	5	4	15	22	20	18	19	0	9	16	24	3
q	e	k	w	m	y	j	a	p	b	n	l	r	i	x	h	f	v	g	s	d	c	z	u	t	o
16	4	10	22	12	24	9	0	15	1	13	11	17	8	23	7	5	21	6	18	3	2	25	20	19	14
e	p	b	u	s	a	i	g	q	y	w	f	j	x	d	t	v	r	z	k	h	m	l	n	c	o
4	15	1	20	18	0	8	6	16	24	22	5	9	23	3	19	21	17	25	10	7	12	11	13	2	14

0
a

3rd character

k
10

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
d	m	v	h	r	z	c	i	o	g	x	l	n	b	k	f	e	p	w	u	s	t	a	j	q	y
3	12	21	7	17	25	2	8	14	6	23	11	13	1	10	5	4	15	22	20	18	19	0	9	16	24
q	e	k	w	m	y	j	a	p	b	n	l	r	i	x	h	f	v	g	s	d	c	z	u	t	o
16	4	10	22	12	24	9	0	15	1	13	11	17	8	23	7	5	21	6	18	3	2	25	20	19	14
e	p	b	u	s	a	i	g	q	y	w	f	j	x	d	t	v	r	z	k	h	m	l	n	c	o
4	15	1	20	18	0	8	6	16	24	22	5	9	23	3	19	21	17	25	10	7	12	11	13	2	14

10
n

Plaintext

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

7. the following permutation box "**gjahfbcdei**" is used as standard permutation cipher

7.1 find the total number of trials to break produced ciphertext

7.2 find cipher period

7.3 decrypt the following message "**hksitoyoungntoeoyarisigtstopahhesauoryovraapenothl**"

7.1 brute force attack = 10! =3628800

7.2 period = 10

cipher

h	k	s	i	t	o	y	o	u	n	g	n	t	o	e	o	y	a	r	i	s	i	g	t	s
t	o	p	a	h	h	e	s	a	u	o	r	y	o	v	r	a	a	p	e	n	o	t	h	l

Pbox

g	j	a	h	f	b	c	d	e	l
6	9	0	7	5	1	2	3	4	8

Plain

s	o	y	o	u	t	h	i	n	k	t	o	y	a	r	e	g	o	i	n	g	t	o	p	a
s	s	t	h	i	s	o	r	y	o	u	h	a	v	e	a	n	o	t	h	e	r	p	l	a

Plaintext

. . . . . .

. . . . . .

. . . . . .

. . . . . .