جامعة الأهرام الكندية
AHRAM CANADIAN UNIVERSITY

Lecture (05)
Classical Encryption Techniques (IV)

Dr. Ahmed M. ElShafee

One time pad

- Invented by **Gilbert Vernham** in 1918, and used a long tape of random letters to encrypt the message.
- An Army Signal officer, **Joseph Mauborgne**, proposed an improvement using a random key that was truly as long as the message, with no repetitions, which thus totally obscures the original message.
- It produces random output that bears no statistical relationship to the plaintext.
- Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code, since any plaintext can be mapped to any ciphertext given some key.

- The one-time pad offers complete security but, in practice, has two fundamental difficulties:

1. There is the practical problem of making large quantities of random keys.
2. And the problem of key distribution and protection, where for every message to be sent, a key of equal length is needed by both sender and receiver.

- Because of these difficulties, the one-time pad is of limited utility, and is useful primarily for low-bandwidth channels requiring very high security.

- Encrypt the following message

"**this message is un-breakable**"

- using the following text file

"With this package installed, Power Management Driver supports power management on Lenovo computers.

If the Power Management Driver program is already installed, overwrite-installing this package will fix problems, add new functions, or expand functions as noted below.

This program is language-independent and can be used in systems of any languages."

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

t	h	i	s	m	e	s	s	a	g	e	i	s	u	n	b	r	e	a	k	a	b	l	E

w	i	t	h	t	h	i	s	p	a	c	k	a	g	e	i	n	s	t	a	l	l	e	D

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

t	h	i	s	m	e	s	s	a	g	e	i	s	u	n	b	r	e	a	k	a	b	l	E
19	7	8	18	12	4	18	18	0	6	4	8	18	20	13	1	17	4	0	10	0	1	11	4

w	i	t	h	t	h	i	s	p	a	c	k	a	g	e	i	n	s	t	a	l	l	e	D
22	8	19	7	19	7	8	18	15	0	2	10	0	6	4	8	13	18	19	0	11	11	4	3

15	15	1	25	5	11	0	10	15	6	6	18	18	0	17	9	4	22	19	10	11	12	15	7
p	p	b	z	f	l	a	k	p	g	g	s	s	a	r	j	e	w	t	k	l	m	p	H

- Decrypt the following message

"imlotdgctdceagqmyztg"

- Using the following key

"With this package installed, Power Management Driver supports power management on Lenovo computers.

If the Power Management Driver program is already installed, overwrite-installing this package will fix problems, add new functions, or expand functions as noted below.

This program is language-independent and can be used in systems of any languages."

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

i	m	l	o	t	d	g	c	t	d	c	e	a	g	q	m	y	z	t	G

w	i	t	h	t	h	i	s	p	a	c	k	a	g	e	i	n	s	t	a	l	l	e	D

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

i	m	l	o	t	d	g	c	t	d	c	e	a	g	q	m	y	z	t	G
8	12	11	14	19	3	6	2	19	3	2	4	0	6	16	12	24	25	19	6

w	i	t	h	t	h	i	s	p	a	c	k	a	g	e	i	n	s	t	a	l	l	e	D
22	8	19	7	19	7	8	18	15	0	2	10	0	6	4	8	13	18	19	0	11	11	4	3

12	4	18	7	0	22	24	10	4	3	0	20	0	0	12	4	11	7	0	6
m	e	s	h	a	w	y	k	e	d	a	u	a	a	m	e	l	h	a	g

mesh awy keda ua am elhag

Hill cipher

$C_n = (K_{n1} \times P_1 + K_{n2} \times P_2 + K_{n3} \times P_3 + \ldots\ldots + K_{nm} \times P_m) \bmod 256$

Hill2X2

For 2x2 key

- Enc — Dec
- $C = K \times P$ — $P = K^{-1} \times C$
- K^{-1}= adj(k)/det(k)
- Adjoint matrix is the transposition of original key
- Adj (k) = $\begin{pmatrix} K_{11} & -K_{01} \\ -K_{10} & K_{00} \end{pmatrix}$

- $det(K) = (K_{00} \times K_{11}) - (K_{10} \times k_{01})$
- Conditions:
- gcd(det(*k*),26)=1.

- Example
- Use Hill cipher to encrypt the following message

"**intruder detected**"

- Using the following key

"**hell**"

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

i	n	t	r	u	d	e	r	d	e	t	e	c	t	e	D
8	13	19	17	20	3	4	17	3	4	19	4	2	19	4	3

h	e	l	L
7	4	11	11

k =

7	4
11	11

det =

det_1 =

K^{-1} =

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

i	n	t	r	u	d	e	r	d	e	t	e	c	t	e	D
8	13	19	17	20	3	4	17	3	4	19	4	2	19	4	3

h	e	l	L
7	4	11	11

k =

7	4
11	11

det = 7

det_1 = 15

K^{-1} =

9	19
17	1

17	19	8	3	17	9	7	21	13	4	21	16	15	9	9	23
r	t	i	d	r	j	h	v	n	e	v	q	p	j	j	x

- Use hill cipher to decrypt the following message

"**nexvnomsqjtkautjdrdb**"

- Using the following key

"hell"

n	e	x	v	n	o	m	s	q	j	t	k	a	u	t	j	d	r	d	B
13	4	23	21	13	14	12	18	16	9	19	10	0	20	19	9	3	17	3	1

h	e	l	L
7	4	11	11

k =

7	4
11	11

det = 7

det_1 = 15

K^{-1} =

9	19
17	1

n	e	x	v	n	o	m	s	q	j	t	k	a	u	t	j	d	r	d	B
13	4	23	21	13	14	12	18	16	9	19	10	0	20	19	9	3	17	3	1

h	e	l	L
7	4	11	11

k =

7	4
11	11

det = 7

det_1 = 15

K^{-1} =

9	19
17	1

3	4	18	19	17	14	24	0	11	11	3	14	2	20	12	13	4	19	18	3
d	e	s	t	r	o	y	a	l	l	d	o	c	u	m	n	e	t	s	d

Destroy all documents

Hell3x3

For 3x3 key

- Enc
- $C = K \times P$
- K^{-1}= adj(k)/det(k)
- Adjoint matrix is the transposition of original key
- Adj (k) =

Dec

$P = K^{-1} \times C$

$$\begin{pmatrix} K_{00}\begin{pmatrix}K_{11} & K_{12}\\ K_{21} & K_{22}\end{pmatrix} & -K_{01}\begin{pmatrix}K_{10} & K_{12}\\ K_{20} & K_{22}\end{pmatrix} & K_{02}\begin{pmatrix}K_{10} & K_{11}\\ K_{20} & K_{21}\end{pmatrix} \\ -K_{10}\begin{pmatrix}K_{01} & K_{02}\\ K_{21} & K_{22}\end{pmatrix} & K_{11}\begin{pmatrix}K_{00} & K_{02}\\ K_{20} & K_{22}\end{pmatrix} & -K_{12}\begin{pmatrix}K_{00} & K_{01}\\ K_{20} & K_{21}\end{pmatrix} \\ K_{20}\begin{pmatrix}K_{01} & K_{02}\\ K_{11} & K_{12}\end{pmatrix} & -K_{21}\begin{pmatrix}K_{00} & K_{02}\\ K_{10} & K_{12}\end{pmatrix} & K_{22}\begin{pmatrix}K_{00} & K_{01}\\ K_{10} & K_{11}\end{pmatrix} \end{pmatrix}$$

- $det(K) = K_{00} \times ((K_{11} \times K_{22}) - (K_{12} \times K_{21})) -$

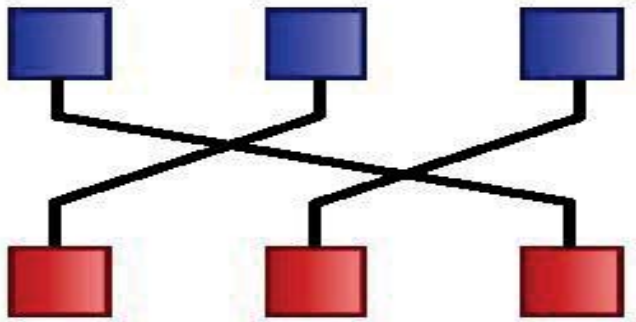
$K_{01} \times ((K_{10} \times K_{22}) - (K_{12} \times K_{20})) + K_{02} \times ((K_{10} \times K_{21}) - (K_{11} \times K_{20}))$

- Conditions:
- gcd(det(*k*),26)=1.

Transposition Ciphers

- **transposition** or **permutation** ciphers
- these hide the message by rearranging the letter order
- without altering the actual letters used
- can recognise these since have the same frequency distribution as the original text

Transposition / permutation cipher



Rail Fence cipher

- write message letters out diagonally over a number of rows
- then read off cipher row by row

Using RailFence cipher, encrypt the following message

“really easy”

r	e	a	l	l	y	e	a	s	y

r	e	a	l	l	y	e	a	s	y

r	a	l	e	s
e	l	y	a	y

r	a	l	e	s	e	l	y	a	y

Using RailFence cipher, decrypt the following message

“suiiyanlmttpdthsoiis”

s	u	i	i	y	a	n	l	m	t	t	p	d	t	h	s	o	i	i	s

s	u	i	i	y	a	n	l	m	t	t	p	d	t	h	s	o	i	i	s

s	u	i	i	y	a	n	l	m	t

t	p	d	t	h	s	o	i	i	s

s	t	u	p	i	d	i	t	y	h	a	s	n	o	l	i	m	i	t	s

Using RailFence cipher, encrypt the following message

“it is not even a real cipher”

i	t	i	s	n	o	t	e	v	e	n	a	r	e	a	l	c	i	p	h	e	r

i	t	i	s	n	o	t	e	v	e	n	a	r	e	a	l	c	i	p	h	e	r

i	i	n	t	v	n	r	a	c	p	e
t	s	o	e	e	a	e	l	i	h	r

i	i	n	t	v	n	r	a	c	p	e	t	s	o	e	e	a	e	l	i	h	r

- Using RailFence cipher, decrypt the following message

“sriijsaifsouetsutdfuin”

s	r	i	i	j	s	a	i	f	s	o	u	e	t	s	u	t	d	f	u	i	n

s	r	i	i	j	s	a	i	f	s	o	u	e	t	s	u	t	d	f	u	i	n

s	r	i	i	j	s	a	i	f	s	o
u	e	t	s	u	t	d	f	u	i	n

s	u	r	e	i	t	i	s	j	u	s	t	a	d	i	f	f	u	s	i	o	n

Row Transposition Ciphers

- a more complex transposition
- write letters of message out in rows over a specified number of columns
- then reorder the columns according to some key before reading off the rows

- A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.
- For the type of columnar transposition just shown, cryptanalysis is fairly straightforward and involves laying out the ciphertext in a matrix and playing around with column positions.
- Digram and trigram frequency tables can be useful

- Example
- Use row transposition cipher to encrypt the following message

“meet me under the bridge tomorrow at ten pm”

- Using the following permutation box

“bcedafg”

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

m	e	e	t	m	e	u	n	d	e	r	t	h	e	b	r	i	d	g	e	t	o	m	o	r	r	o	w	a	t	t	e	n	p	m

b	c	e	d	a	f	G

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

meetmeunderthebridgetomorrowattenpm

b	c	e	d	a	f	G
1	2	4	3	0	5	6

m	e	e	t	m	e	u
n	d	e	r	t	h	e
b	r	i	d	g	e	t
o	m	o	r	r	o	w
a	t	t	e	n	p	m

mtgrnmnboaedrmttrdreeeiotehepuetwm

Example

- Use row transposition cipher to decrypt the following message

“ixmeanemkptxtx”

- Using the following permutation box

“bcedafg”

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

i	x	m	e	a	n	e	m	k	p	t	x	t	x

b	c	e	d	a	f	g
1	2	4	3	0	5	6

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

i	x	m	e	a	n	e	m	k	p	t	x	t	x

b	c	e	d	a	f	g
1	2	4	3	0	5	6

m	a	k	e	i	t	t
e	n	p	m	x	x	x

m	a	k	e	i	t	t	e	n	p	m	x	x	x

Make it ten pm

Example

- Use row transposition cipher to encrypt the following message

“again it is not a cipher even it encrypt larger messages”

- Using the following permutation box

“dcabefg”

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

a	g	a	i	n	i	t	i	s	n	o	t	a	c	i	p	h	e	r	e	v
e	n	i	t	e	n	c	r	y	p	t	l	a	r	g	e	r	m	e	s	s
a	g	e	s	x	x															

d	c	a	b	e	f	g

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

a	g	a	i	n	i	t	i	s	n	o	t	a	c	i	p	h	e	r	e	v
e	n	i	t	e	n	c	r	y	p	t	l	a	r	g	e	r	m	e	s	s
a	g	e	s	x	x															

d	c	a	b	e	f	g
3	2	0	1	4	5	6

a	g	a	i	n	i	t
i	s	n	o	t	a	c
i	p	h	e	r	e	v
e	n	i	t	e	n	c
r	y	p	t	l	a	r
g	e	r	m	e	s	s
a	g	e	s	x	x	x

a	n	h	i	p	r	e	i	o	e	t	t	m	s	g	s	p	n	y	e	g
a	i	i	e	r	g	a	n	t	r	e	l	e	x	i	a	e	n	a	s	x
t	c	v	c	r	s	x														

Example

- Use row transposition cipher to decrypt the following message

“prsoeopnxfniedatcmoxttsxerix”

- Using the following permutation box

“dcabefg”

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

p r s o e o p n x f n i e d a t c m o x t t s x e r i x

d	c	a	b	e	f	g

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

p r s o e o p n x f n i e d a t c m o x t t s x e r i x

d	c	a	b	e	f	g
3	2	0	1	4	5	6

e	x	p	e	c	t	e
d	f	r	o	m	t	r
a	n	s	p	o	s	i
t	i	o	n	x	x	x

e x p e c t e d f r o m t r a n s p o s i t i o n x x x

expected from transposition

Dr. Ahmed ElShafee, ACU Spring 2014, Information Security

Thanks,..

See you next week (ISA),…