جامـــــعة المـــــستـقبـل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قســـم الانظمة الطبية الذكية

Lecture: (5)

Information Security in Healthcare

Subject: Traditional methods mixed cipher
Level: Fourth
Lecturer: Prof. Dr. Mehdi Ebady Manaa

1. Mixed Alphabet

If we permit the cipher alphabet to be any rearrangement of the plain alphabet, then we can generate an enormous number of distinct modes of encryption. There are 26! such rearrangements, which is greater than 4 * 10^{26} which gives rise to an equivalent number of distinct cipher alphabets. Each cipher alphabet is known as a key. If our message is intercepted by the enemy, who correctly assumes that we have used a monoalphabetic substitution cipher, they are still faced with the impossible challenge of checking all possible keys. If an enemy agent could check one of these possible keys every second, it would take roughly one billion

times the lifetime of the universe to check all of them and find the correct one. The disadvantage of this method is that the arrangement is difficult to be remembered. It would involve both sender and recipient to remember a random string of 26 letters. In the table below is one such random ciphertext alphabet.

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

A Mixed Ciphertext alphabet, where the order of the ciphertext letters has been selected randomly.

Example_01:

Plaintext message: **bad**

Plaintext	Ciphertext
a	K
b	D
c	G
d	F

Ciphertext:

DKF

2. Keyword Mixed or Alphabet Mixing via a Keyword

A keyword or key phrase can be used to mix the letters to generate the cipher alphabet. In this method we need a **keyword** like **MATHEMATICS**, and a **keyletter** like **S**, then:

- Remove the repeated letters from the keyword, and you will get MATHEICS.
- Put the first letter of the modified keyword

under the keyletter followed by the remaining letters of the keyword.

- Complete the ciphertext alphabet by the remaining letters without repetitions.

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

Example_02

Plaintext message: **data**

Using the substitution table:

- **d → G**
- **a → B**
- **t → A**
- **a → B**

Ciphertext

GBAB

Example_03

Encrypt the message "**medical records are sensitive data**", using a keyword Mixed cipher for a given keyword (**MATH**) and key latter a.

Encrypt the message:
“medical record are sensitive data”

Using a **Keyword Mixed Cipher** with:

- **Keyword:** MATH
- **Key letter:** a

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

Letter-by-Letter Substitution

Plaintext	m	e	d	i	c	a	l	r	e	c	o	r	d	s	a	r	e	s	e	n	s	i	t	i	v	e	d	a	t	a
Ciphertext	K	B	H	F	T	M	J	Q	B	T	N	Q	H	R	M	Q	B	R	B	I	R	F	S	F	V	B	H	M	S	M

Final Ciphertext

KBHFTMJ QBTNQHR MQB RBLRFSFVB HMSM

Example_04: Decrypt the message **"ANA, F WMR WQNLD. KY TNVBQ FR CFLB.** MJFTB", using a keyword Mixed cipher for a given keyword (**MATH**) and key letter a.

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

The Plaintext: "bob, i was wrong. my cover is fine. alice".

3. Transposition Techniques

A transposition is not a permutation of alphabet characters, but a permutation of places. Transposition or Permutation cipher works by breaking a message into fixed size blocks, and then permuting the characters within each block according to a fixed permutation, say P. The key to the transposition cipher is simply the permutation P. So, the transposition cipher has the property that the encrypted message i.e. the cipher text contains all the characters that were in the plain text message. In the other word, the unigram statistics for the message are unchanged by the encryption process.

In this method, the message is written in a rectangle, **(arrange row by row. Reading the message off, row by row, but permuting the order of the columns)**.

The order of the columns then becomes the key to the algorithm.

For example_05: The plaintext is: breaking transposition cipher.

Key: K = {4 1 3 5 7 6 2}

In this case, the message is broken into block of seven characters, and after encryption the fourth character in the block will be moved to position

1, the first is moved to position 2, the third remains in position 3, the fifth to position 4, the seventh to position five, the sixth remains in position 6, the two is moved to position 7. The following Figure (A) shows the key and Fig. (B) Shows the encryption process of the previously described transposition cipher. It can be noticed that the random string "X" was appended to the end of message to enforce a massage length, which is a multiple of the block size.

1	2	3	4	5	6	7
b	r	e	a	k	i	n
g	t	r	a	n	s	p
o	s	i	t	i	o	n
c	i	p	h	e	r	x

(A)

Encryption

4	1	3	5	7	6	2
a	b	e	k	n	i	r
a	g	r	n	p	s	t
t	o	i	i	n	o	s
h	c	p	e	x	r	i

(B)

4	1	3	5	7	6	2
a	b	e	k	n	i	r
a	g	r	n	p	s	t
t	o	i	i	n	o	s
h	c	p	e	x	r	i

Decryption

1	2	3	4	5	6	7
b	r	e	a	k	i	n
g	t	r	a	n	s	p
o	s	i	t	i	o	n
c	i	p	h	e	r	x

The ciphertext is:

ABEKNIRAGRNPSTTOIINOSHCPEXRI

4. Transposed Keyword Mixed or Alphabet Mixing via a Columnar Transposition

In this method we need a **keyword** like **MATHEMATICS**. After removing the repeated letters, we put it in a matrix with number of columns equal to the number of the letters in the ***modified keyword***. The letters of the keyword form the headings of the columns and the remaining letters of the alphabet fill in order in the rows below. Then, Mixing is achieved by *transcribing columns and taking the matrix letters column by column and we will get*:

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

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

Example_06: Encrypt the message "**far above cayuga's waters**", using Transposed Keyword Mixed for a given keyword (**CORNELL**)

H.W. Apply the decipher for the example above

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

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

Ciphertext: "OCV CANWY ICQPBC'E LCGYVE".