جامعة الأهرام الكندية
AHRAM CANADIAN UNIVERSITY

Lecture (04)
Classical Encryption Techniques (III)

Dr. Ahmed M. ElShafee

Playfair Cipher

one approach to improve security was to encrypt multiple letters the **Playfair Cipher** is an example

- invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair
- Treats digrams in the plaintext as single units and translates these units into ciphertext digrams
- The Playfair algorithm is based on the use of a 5x5 matrix of letters constructed using a keyword

- The rules for filling in this 5x5 matrix are:
  - L to R, top to bottom,
  - first with keyword after duplicate letters have been removed,
  - and then with the remain letters,
  - with I/J used as a single letter.

- using the keyword MONARCHY

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

- Plaintext is encrypted two letters at a time, according to the rules as shown.
- Note how you wrap from right side back to left, or from bottom back to top.

1. if a pair is a repeated letter, insert a filler like 'X', eg. "balloon“ encrypts as "ba lx lo on"
2. if both letters fall in the same row, replace each with letter to right (wrapping back to start from end), eg. “ar" encrypts as "RM"
3. if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom), eg. “mu" encrypts to "CM"
4. otherwise each letter is replaced by the one in its row in the column of the other letter of the pair, eg.

   “hs" encrypts to "BP", and

   “ea" to "IM" or "JM" (as desired)

- Decrypting of course works exactly in reverse.

Security of Playfair Cipher

- Number of available diagreams are 26^2!= 1.88 E1621
- Total trials to break playfair = 26^m → m=key length
- so that identification of individual digrams is more difficult.
- Also,the relative frequencies of individual letters exhibit a much greater range than that of digrams, making frequency analysis much more difficult.
- The Playfair cipher was for a long time considered unbreakable.
- It was used as the standard field system by the British Army in World War I and still enjoyed considerable use by the U.S.Army and other Allied forces during World War I

- Example
- Use playfair cipher to encrypt the following message

"we need new agent in field"

- Using the following key

"hollow man"

w	e	n	e	e	d	n	e	w	a	g	e	n	t	i	n	f	i	e	l	d

h	o	l	l	o	w	m	a	n

w	e	n	e	e	d	n	e	w	a	g	e	n	t	i	n	f	i	e	l	d

h	o	l	l	o	w	m	a	n

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

w	e	n	e	e	d	n	e	w	a	g	e	n	t	i	n	f	i	e	l	d

h	o	l	l	o	w	m	a	n

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

h	i	a	f	k	a	a	f	h	c	f	k	d	q	f	c	e	g	g	h	b	z

Example

Decrypt the following reply

“hkkpfckrhnxlpbbffggstpnqeusgbl”

h	k	k	p	f	c	k	r	h	n	x	l	p	b	b	f	k	e	g	s	r	s	n	q	e	u	s	g	b	l

h	o	l	l	o	w	m	a	n

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

h	k	k	p	f	c	k	r	h	n	x	l	p	b	b	f	k	e	g	s	r	s	n	q	e	u	s	g	b	l

h	o	l	l	o	w	m	a	n

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

m	e	e	t	i	n	g	t	o	a	r	x	r	a	n	g	e	f	i	r	s	t	o	f	a	p	r	i	l	x

Polyalphabetic Ciphers

polyalphabetic substitution ciphers

- improve security using multiple cipher alphabets
- make cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- use a key to select which alphabet is used for each letter of the message
- use each alphabet in turn
- repeat from start after end of key is reached

Vigenère Cipher

- simplest polyalphabetic substitution cipher
- effectively multiple caesar ciphers
- key is multiple letters long $K = k_1\ k_2\ ...\ k_d$
- i^{th} letter specifies i^{th} alphabet to use
- use each alphabet in turn
- repeat from start after end letters in message
- decryption simply works in reverse

$$E_K(x_1, x_2, \ldots, x_m) = (x_1+k_1, x_2+k_2, \ldots, x_m+k_m)$$
$$D_K(y_1, y_2, \ldots, y_m) = (y_1-k_1, y_2-k_2, \ldots, y_m-k_m)$$

- Example
- keyword *deceptive*

```
key:        deceptivedeceptivedeceptive
plaintext:  weare discovered save yourself
ciphertext:ZICVT WQNGRZGVTW AVZH CQYGLMGJ
```

- Example
- Encrypt the following message

"leave now it is going to blow in ten"

- Using key

"boom"

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

l	e	a	v	e	n	o	w	i	t	i	s	g	o	i	n	g	t	o	b	l	o	w	i	n	t	e	N
11	4	0	21	4	13	14	22	8	19	8	18	6	14	8	13	6	19	14	1	11	14	22	8	13	19	4	13

b	o	o	M
1	14	14	12

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

l	e	a	v	e	n	o	wi	t	i	s	g	o	i	n	g	t	o	b	l	o	wi	n	t	e	N
11	4	0	21	4	13	14	22	8	19	8	18	6	14	8	13	6	19	14	1	11	14	22	8	13	19	4	13

b	o	o	M
1	14	14	12

12	18	14	7	5	1	2	8	9	7	22	4	7	2	22	25	7	7	2	13	12	2	10	20	14	7	18	25
ms	o	h	f	b	c	i	j	h	we	h	c	wz	h	h	c	n	mc	k	u	o	h	s	Z				

- Decrypt the following message

"cshdbmsdcshifsbgt"

- Using the following key

"boom"

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

c	s	h	d	b	m	s	d	c	s	h	i	f	s	b	g	T
2	18	7	3	1	12	18	3	2	18	7	8	5	18	1	6	19

b	o	o	M
1	14	14	12

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

c	s	h	d	b	m	s	d	c	s	h	i	f	s	b	g	T
2	18	7	3	1	12	18	3	2	18	7	8	5	18	1	6	19

b	o	o	M
1	14	14	12

1	4	19	17	0	24	4	17	1	4	19	22	4	4	13	20	18
b	e	t	r	a	y	e	r	b	e	t	w	e	e	n	u	s

betrayer between us

Security of Vigenère Ciphers

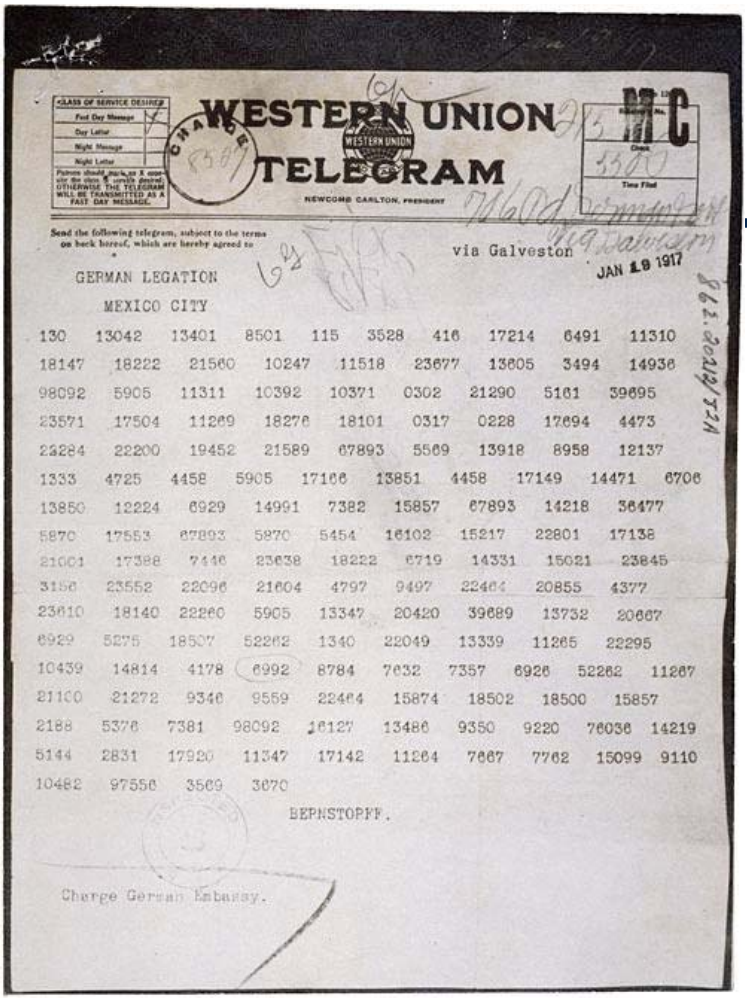
- As Vigenère is polyalphabetic cipher, it perfectly hide the language redundancy of single character and diagrams.
- Security is based on keyword length

Key length	Total number of keys
3	$26^3 = 17576 = 1.76\ E4$
4	$26^4 = 456976 = 4.75\ E5$
5	$26^5 = 11881376 = 1.19\ E7$
6	$26^6 = 308915776 = 3.1\ E8$
7	$26^7 = 8031810176 = 8\ E9$
8	$26^8 = 208827064576 = 2.1\ E11$

Kasiski Method to break polyalphabetic cipher

- For some centuries the Vigenère cipher was unbreakable cipher).
- As a result of a challenge, it was broken by **Charles Babbage** (the inventor of the computer) in 1854 but kept secret (possibly because of the **Crimean War** - not the first time governments have kept advances to themselves!).
- The method was independently reinvented by a **Prussian**, **Friedrich Kasiski**, who published the attack now named after him in 1863.
- One very famous incident was the breaking of the Zimmermann telegram in WW1 which resulted in the USA entering the war.

•



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston JAN 19 1917

GERMAN LEGATION

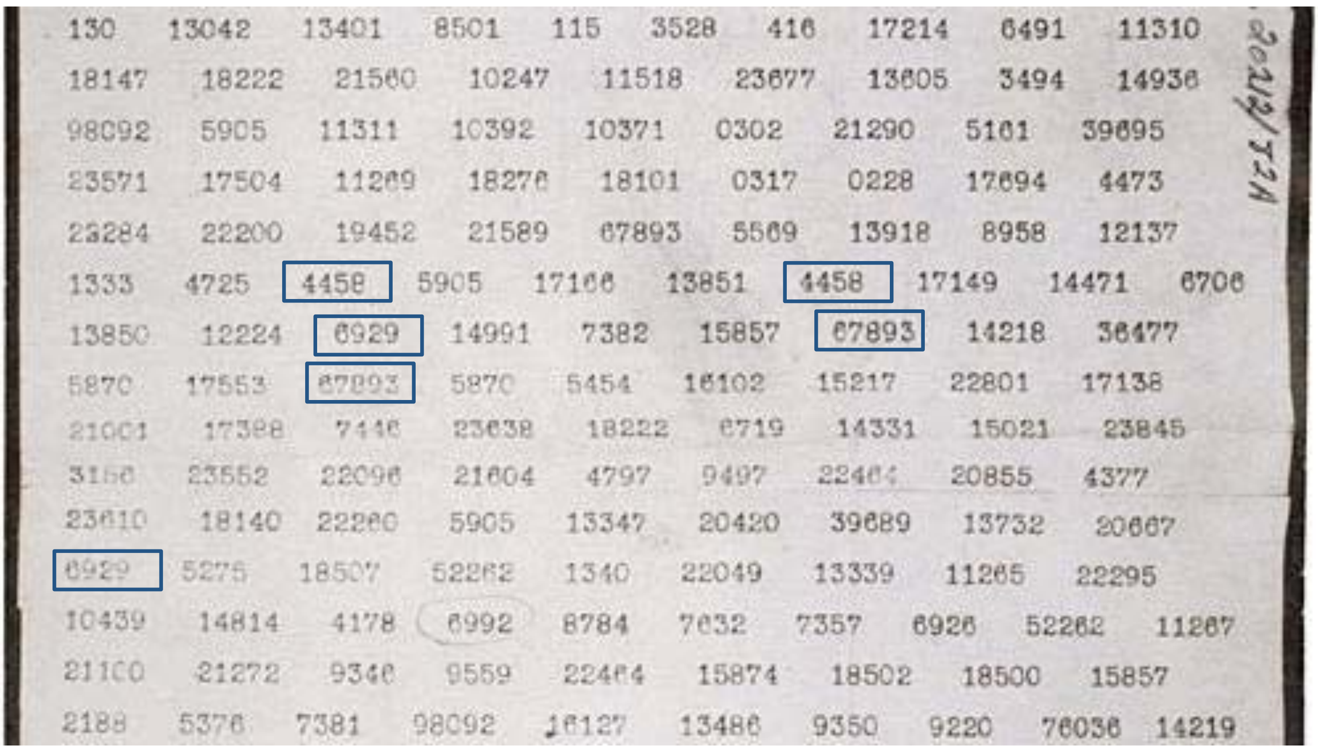
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

``



130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219

- In general the approach is to find a number of duplicated sequences, collect all their distances apart, look for common factors, remembering that some will be random flukes and need to be discarded.
- Now have a series of monoalphabetic ciphers, each with original language letter frequency characteristics.
- Can attack these in turn to break the cipher.

Autokey Cipher

- ideally want a key as long as the message
- Vigenère proposed the **autokey** cipher
- Firstly use user key to encrypt first part of plaintext, then use plaintext itself to enctypt the rest of message.
- Example
- given key *deceptive*

```
key:        de cep tive weared isco veredsav
plaintext: we are disc overed save yourself
ciphertext:ZI CVT WQNG KZEIIG ASXS TSLVVWLA
```

- Encrypt the following message

“bring money in ninth pm at the bridge”

- Using the following key

“dirty deal”

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

b	r	i	n	g	m	o	n	e	y	i	n	n	i	n	t	h	p	m	a	t	t	h	e	b	r	i	d	g	E
1	17	8	13	6	12	14	13	4	24	8	13	13	8	13	19	7	15	12	0	19	19	7	4	1	17	8	3	6	4

d	i	r	t	y	d	e	a	L
3	8	17	19	24	3	4	0	11

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

b	r	i	n	g	m	o	n	e	y	i	n	n	i	n	t	h	p	m	a	t	t	h	e	b	r	i	d	g	E
1	17	8	13	6	12	14	13	4	24	8	13	13	8	13	19	7	15	12	0	19	19	7	4	1	17	8	3	6	4

d	i	r	t	y	d	e	a	L
3	8	17	19	24	3	4	0	11

4	25	25	6	4	15	18	13	15	25	25	21	0	14	25	7	20	19	10	8	6	6	15	17	20	24	23	15	6	23
e	z	z	g	e	p	s	n	p	z	z	v	a	o	z	h	u	t	k	i	g	g	p	r	u	y	x	p	g	X

- Decrypt the following message using

"ezzgewlehiftrymbjbasyoy"

- Using the following key

"dirty deal"

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

e	z	z	g	e	w	l	e	h	i	f	t	r	y	m	b	j	b	a	s	y	o	Y
4	25	25	6	4	22	11	4	7	8	5	19	17	24	12	1	9	1	0	18	24	14	24

d	i	r	t	y	d	e	a	L
3	8	17	19	24	3	4	0	11

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

e	z	z	g	e	w	l	e	h	i	f	t	r	y	m	b	j	b	a	s	y	o	Y
4	25	25	6	4	22	11	4	7	8	5	19	17	24	12	1	9	1	0	18	24	14	24

d	i	r	t	y	d	e	a	L
3	8	17	19	24	3	4	0	11

1	17	8	13	6	19	7	4	22	7	14	11	4	18	19	20	5	5	19	4	13	10	6
b	r	i	n	g	t	h	e	w	h	o	l	e	s	t	u	f	f	t	e	n	k	g

bring the whole staff ten KG

Thanks,..

See you next week (ISA),…