Encryption Algorithms & Protocols

More Classical Ciphers

Dr. Omar Abusada
E-mail: abossada1@gmail.com

Playfair Cipher

- Not even the large number of keys in a monoalphabetic cipher provides security.
- Multiple letters encryption cipher.
- In playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.
- The Playfair Cipher is invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair.

Playfair Encryption Technique

- For the encryption process let us consider the following example:
- **Key: monarchy, Plaintext: instruments**
- A 5X5 matrix of letters based on a keyword
- The Playfair Cipher Encryption Algorithm consists of 2 steps:
- Fill in letters of keyword (No duplicated letters is allowed)
- Fill rest of matrix with other letters, eg. 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**

Rules for Encryption Using Playfair

- Diagrams.
- Repeating letters – Filler letter
- Same column | ↓ | warp around.
- Same row | → | warp around.
- rectangle | ⇆ | swap.

- Examples:
  - Plaintext (attack) → digrams: at ta ck
  - Plaintext (rules) → digrams: ru le sx
  - Plaintext (balloon) → digrams: ba ll oo n

    digrams: ba lx lo on

Understanding the rules

- Examples:Plaintext (attack) → digrams: at ta ck
  - **at:** rule number 5 (rectangle) Ciphertext (sr)
  - **ta:** rule number 5 (rectangle) Ciphertext (rs)
  - **ck:** rule number 5 (rectangle) Ciphertext (de)
  - Plaintext (attack) → ciphertext (rssrde)

at	ta	ck
rs	sr	de

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

- Examples:Plaintext (mosque) → digrams: mo sq ue
  - **at:** rule number 4 (same raw) Ciphertext (sr)
  - **ta:** rule number 5 (rectangle) Ciphertext (rs)
  - **ck:** rule number 5 (rectangle) Ciphertext (de)
  - Plaintext (mosque) → ciphertext (ontslm)

mo	sq	ue
on	ts	ml

Example

Encrypt the message “hide the gold under the carpet” using playfair technique with keyword “Neso Academy”

Plaintext: hide the gold under the carpet

Key: Neso Academy

Ciphertext: IKGDQKDPNRCVECOPQKNDOTVDRZ

hi	de	th	eg	ol	du	nd	er	th	ec	ar	pe	tx
IK	GD	QK	DP	NR	CV	EC	OP	QK	ND	OT	VD	RZ

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

Note: Single VS Multiple (Look at E in plaintext and what is corresponding ciphertext)

H.W

Decrypt the ciphertext “ODZFQSEZSONTSW” using playfair technique. Key “NESO APP”

Vigenère Cipher

- Simplest polyalphabetic substitution cipher.
- Effectively multiple Caesar Ciphers.
- Key is multiple letters long K = k1 k2 ... Km.
- I^{th} letter specifies the I^{th} alphabet to use.
- Repeat from start after m letters in message.
- Decryption simply works in reverse.

Rules of Vigenère Cipher

- Write the plaintext out P = p0,p1,……,pn-1
- Write the keyword repeated above it.
- Key = k0,k1,……,km-1 such that m<n
- Encrypt the corresponding plaintext letter
- Ciphertext = (pi + ki mod m) mod 26
- Plaintext= (pi - ki mod m) mod 26

Rules of Vigenère Cipher

- Encrypt the message "**wearediscoveredsaveyourself**" with keyword **deceptive**
  - **Encryption process**: +
  - **Decryption process**:
  - **0 to 25 = A to Z**

Key	**d**	**e**	**c**	**e**	**p**	**t**	**i**	**v**	**e**	**d**	**e**	**c**	**e**	**p**	**t**	**i**	**v**	**e**	**d**	**e**	**c**	**e**	**p**	**t**	**i**	**v**	**e**
plaintext	w	e	a	r	e	d	i	s	c	o	v	e	r	e	d	s	a	v	e	y	o	u	r	s	e	l	f

Key	**3**	**4**	**2**	**4**	**15**	**19**	**8**	**21**	**4**	**3**	**4**	**2**	**4**	**15**	**19**	**8**	**21**	**4**	**3**	**4**	**2**	**4**	**15**	**19**	**8**	**21**	**4**
P.T	**22**	**4**	**0**	**17**	**4**	**3**	**8**	**18**	**2**	**14**	**21**	**4**	**17**	**4**	**3**	**18**	**0**	**21**	**4**	**24**	**14**	**20**	**17**	**18**	**4**	**11**	**5**
C.T	**25**	**8**	**2**	**21**	**19**	**22**	**16**	**13**	**6**	**17**	**25**	**6**	**21**	**19**	**22**	**0**	**21**	**25**	**7**	**2**	**16**	**24**	**6**	**11**	**12**	**6**	**9**

Ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Autokey system in Vigenère Cipher

- For better security, repeating the keyword is not recommended.
- Instead of repeating the keyword, we combine the keyword with the plaintext.
- Based on autokey system, keyword for the previous example (deceptive) can be formed as:

- Key: deceptivewearediscoveredsav
- Plaintext: wearediscoveredsaveyourself

- Then Ciphertext is written as:
- Ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA

More videos about classical encryption technique

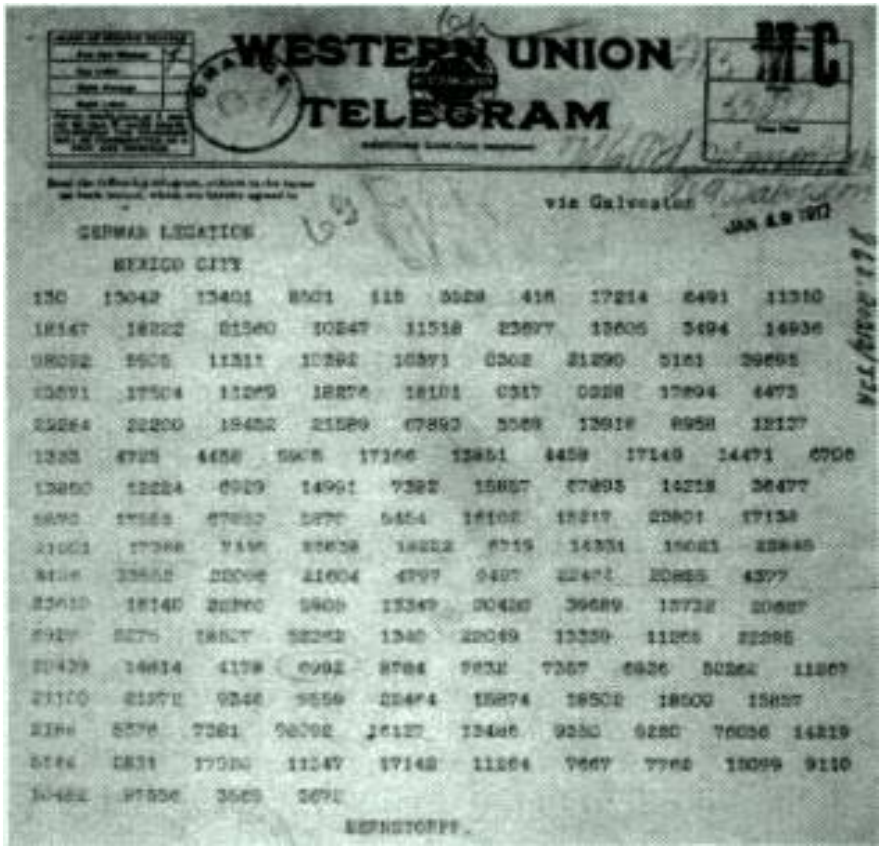
- https://www.youtube.com/watch?v=JtbKh_12ctg
- https://www.youtube.com/watch?v=na5rapg1XsI
- https://www.youtube.com/watch?v=6iYqHn3q8sY
- https://www.youtube.com/watch?v=JK3ur6W4rvw
- https://www.youtube.com/watch?v=Ic4BzVggNY8

Codebook Cipher

- A classic codebook cipher is, literally, a dictionary-like book containing (plaintext)
- words and their corresponding (ciphertext) codewords. To encrypt a given word, the cipher clerk would simply look up the word in the codebook and replace it with the corresponding codeword.
- Decryption, using the inverse codebook.
- The following table contains an excerpt from a famous codebook used by **Germany** during **World War I**.

Codebook Cipher

Zimmerman Telegram encrypted via Codebook	
Plaintext	Ciphertext
Februar	13605
fest	13732
finanzielle	13850
folgender	13918
Frieden	17142
Friedenschluss	17149
.	.
.	.
.	.
.	.



Zimmerman Telegram

Codebook Cipher

- For example, to use the codebook in previous table to encrypt the German word **Februar**, the entire word would be replaced with the 5-digit codeword **13605**. This codebook was used for encryption, while the corresponding inverse codebook, arranged with the 5-digit codewords in numerical order, was used for decryption. A codebook is a form of a substitution cipher, but the substitutions are far from simple, since substitutions are for entire words, or in some cases, entire phrases.
- The codebook illustrated in previous table was used to encrypt the famous Zimmermann telegram. At the height of **World War I in 1917**, the **German Foreign Minister**, **Arthur Zimmermann**, sent an encrypted telegram to the **German ambassador in Mexico City**.

Codebook Cipher

- The ciphertext message, which appears in previous picture, was intercepted by the **British**. At the time, the **British** and **French** were at war with **Germany**, but the **U.S. was neutral**.
- The **Russians** had recovered a damaged version of the **German** codebook, and the partial codebook had been passed on to the **British**. Through A carful analyses, the British were able to fill in the gaps in the codebook so that by the time they obtained the **Zimmermann telegram**, they could decrypt it.
- The telegram stated that the German government was planning to begin unrestricted submarine warfare and had concluded that this would likely lead to war with the **United States**.

Codebook Cipher

- As a result, **Zimmermann** told his ambassador that **Germany** should try to employ **Mexico** as an partner to fight against the **United States**. The encouragement for **Mexico** was that it would "reconquer the lost territory in **Texas**, **New Mexico** and **Arizona**."
- When the **Zimmermann telegram** was released in the **U.S**., public opinion turned against **Germany** and, after the sinking of the Lusitania, the **U.S. declared war**.

… Thank you …