School of InfoComm Technology ict Taking IT Higher

NGEE ANN POLYTECHNIC

1

CRYPTOGRAPHY (CTG)

Diploma in Cybersecurity and Digital Forensics (Dip in CSF)

Academic Year (AY) `21/`22

WEEK 1.2

CLASSICAL CRYPTOGRAPHY –PART 2

Last Updated: 4/10/2021

Contents

Week 1 Recap

Week 1 - Summary

CTG MODULE OVERVIEW 2

----------7 Security Domains

CLASSICAL CIPHERS PART 2

SUMMARY

- **Skill**
- **Knowledge**
- **Activity**
- **Thinking**
- **Feedback**

Component	You learnt
Activity 1.1	7 Security Domains
Skill 1.1~1.3	Columnar Transposition Bifid Cipher ADFGX Cipher
Activity 1.1~1.3	Decrypting cipher texts using Columnar Transposition Bifid Cipher ADFGX Cipher
Thinking & Knowledge	7 Security Domains Columnar Transposition Bifid Cipher ADFGX Cipher
Feedback	7 Security Domains Columnar Transposition Bifid Cipher ADFGX Cipher

5

Substitution Ciphers Part 1

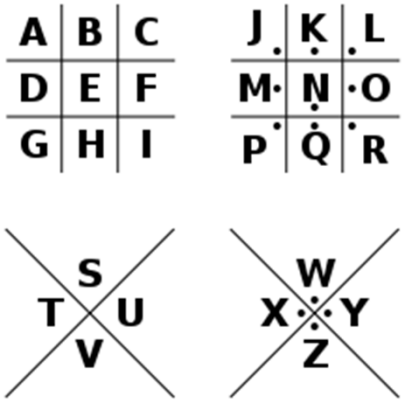
Pigpen Cipher

Shift Cipher

Shift Cipher with Modular Arithmetic

Pigpen Cipher – Skill 2.1

- Key:



- Decrypt the cipher text below:

- Plain text:

Pigpen Cipher – Activity 2.1

- Decrypt the cipher texts below:

Pigpen Cipher

- Pigpen Cipher
  - substitutes each letter for a symbol.
  - used by Freemasons in the 18th Century
    - A secret society
  - used during American Civil War by "union prisoners" in "Confederate camps" to communicate with each other.

Shift Cipher – Using the cipher disk

- Can you decode the following message?

UIF LFZ UP TUPQQJOH UIF NJTTJMF JT FMFNFOUBSZ

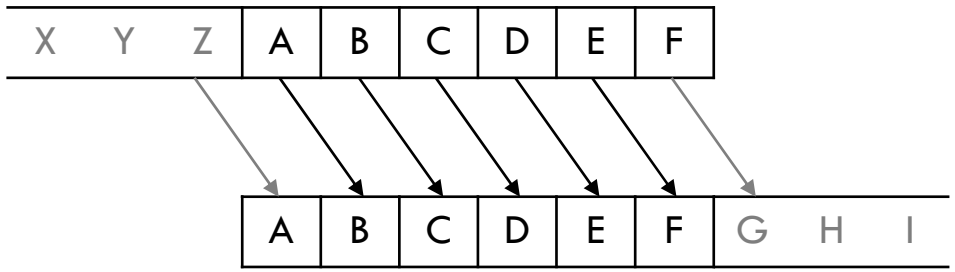
- You can use the cipher disk or use the online cipher disk:

http://inventwithpython.com/cipherwheel/

Shift Cipher – Using the cipher disk

UIF LFZ UP TUPQQJOH UIF NJTTJMF JT FMFNFOUBSZ

THE KEY TO STOPPING THE MISSILE IS ELEMENTARY

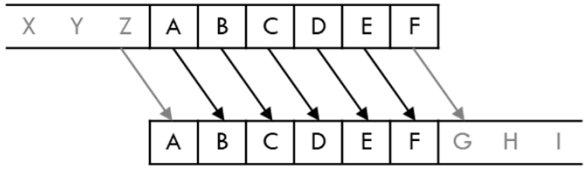


Shift + 1

This cipher has a shift of 1 characters.
The letter 'A' becomes a 'B'. The letter 'B' becomes a 'C' …

Shift Cipher – Skill 2.2

- The Caesar Shift is an example of a Substitution Cipher, where each letter is replaced with another one.
- To encrypt or decrypt a Caesar Shift we first list the alphabet, and then for a Caesar shift of one, we move every letter of the alphabet 1 place:



Shift + 1

This Caesar cipher has a shift of 1 meaning that an 'A' becomes a 'B' and a 'B' becomes a 'C' etc…

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	Plaintext
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	Ciphertext

Shift Cipher – Skill 2.2

- Either use the cipher disks provided or Caesar Cipher
- Decrypt the following cipher texts
  - KHOOR
  - FKYJWXMTHP
  - MJWPNAXDBUH
  - VA PNFU

Shift Cipher – Skill 2.2

- How many possible keys?
  - ?????
- Was it easy to break this cipher? How?
  - ?????

Modular Arithmetic – Skill 2.3

- Assume a 12-hour clock
- If it is 10 o'clock now
  - what would be the time 1 hour from now?
    - ??????
  - what was the time 2 hours ago?
    - ?????
  - what would be the time 4 hours from now?
    - Is it 14 o'clock ???
  - what was the time 15 hours ago?
    - Is it -5 o'clock ???

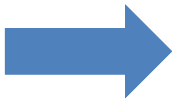
Modular Arithmetic – Skill 2.3

- This is an example of what's called "modular arithmetic". The modulus, in this case, is 12.
  - what would be the time 4 hours from now?
    - $10 + 4 = 14 \bmod 12$
      - We write $14 = 12 \times 1 + 2$
      - Therefore $14 \bmod 12 = 2$ o'clock
  - what was the time 15 hours ago?
    - $10 - 15 = -5 \bmod 12$
      - We write $-5 = 12 \times (-1) + 7$
      - Therefore $-5 \bmod 12 = 7$ o'clock

Modular Arithmetic – Activity 2.2

- 101 mod 7
  - ?????
- -101 mod 7
  - ?????
- 143 mod 16
  - ?????
- 50 mod 3
  - ??????
- 60 mod 8
  - ??????
- -121 mod 6
  - ?????

Shift Cipher using Mod Arithmetic – Encryption – Skill 2.4



A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Key (K) = 11

Plain text (P)	**w**	**e**	**w**	**i**	**l**	**l**	**m**	**e**	**e**	**t**
Convert P into integers as in the RED table above	22	4	22	8	11	11	12	4	4	19
Encryption function = (P+K) mod 26	7	15	7	19	22	22	23	15	15	4
Convert integers into to alphabets as in RED table above **= Cipher text**	H	P	H	T	W	W	X	P	P	E

Shift Cipher using Mod Arithmetic – Decryption – Skill 2.4

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Key (K) = 11

Cipher Text (C)	H	P	H	T	W	W	X	P	P	E
Convert C into integers as in the RED table above	7	15	7	19	22	22	23	15	15	4
Decryption function = (C - K) mod 26	22	4	22	8	11	11	12	4	4	19
Convert integers into to alphabets as in RED table above **= Plain text**	w	e	w	i	l	l	m	e	e	t

Shift Cipher using Mod Arithmetic – Activity 2.3

- Cipher 1
  - CT: HIPAAVVIPN
  - K: 7
- Cipher 2
  - CT: SDPLPNLXIW
  - K: 15
- Cipher 3
  - CT: HIQILHYPYL
  - K: 20

Summary

Week 2.1

Week 2.1 - Summary

SUBSTITUTION CIPHERS 1

TRANSPOSITION CIPHER EXERCISES

SUMMARY

Component	You learnt
Activity	Pigpen Cipher
Skill	Shift Cipher
Activity	Modular Arithmetic
Thinking & Knowledge	Shift Cipher with Modular Arithmetic
Feedback	