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 2.2

CLASSICAL CRYPTOGRAPHY –PART 3

Last Updated: 4/10/2021

Contents

Week 1&2 Recap

Week 1&2 - 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	Columnar Transposition Bifid Cipher ADFGX Cipher	Affine Cipher Vigenere Cipher Vernam Cipher
Activity	Decrypting cipher texts using Columnar Transposition Bifid Cipher ADFGX Cipher	 Affine Cipher Vigenere Cipher
Thinking & Knowledge	7 Security Domains Columnar Transposition Bifid Cipher ADFGX Cipher	 Affine Cipher Vigenere Cipher Vernam Cipher
Feedback	7 Security Domains Columnar Transposition Bifid Cipher ADFGX Cipher	 Affine Cipher Vigenere Cipher Vernam Cipher

Practice Transposition Ciphers

- Columnar Transposition Cipher
- Bifid Cipher
- ADFGX Cipher

Columnar Transposition – Activity 2.4

- Decrypt the following cipher texts using columnar transposition
  - Exercise1
    - CT: bdesgootorap
    - Key: ACTION
  - Exercise 2
    - CT: orsigntiinheneuhbstts
    - Key: TAKEOUT
  - Exercise 3
    - CT: atbhaeafyidodfacte
    - Key: ACCORDERS

Bifid Cipher – Activity 2.5

- Decrypt the following cipher texts using Bifid cipher
  - Exercise1
    - CT: SEAAWHEYGM
  - Exercise 2
    - CT: LFROIINCQWAT
  - Exercise 3
    - CT: LUIMLOEGANYEXR

Key:

	1	2	3	4	5
1	B	G	W	K	Z
2	Q	P	N	D	S
3	I/J	O	A	X	E
4	F	C	L	U	M
5	T	H	Y	V	R

ADFGX Cipher – Activity 2.6

- Decrypt the following cipher texts using ADFGX cipher
  - Exercise1
    - CT: DAFAFDDADDDXFDXXGDFF
    - Key 2: CARGO
  - Exercise 2
    - CT: GXDDAAADFGXFAA
    - Key 2: AIRPLAY

Key 1:

	A	D	F	G	X
A	b	t	a	l	p
D	d	h	o	z	k
F	q	f	v	s	n
G	g	i/j	c	u	x
X	m	r	e	w	y

Practice Substitution Ciphers

- Affine Cipher
- Venegere Cipher
- Vernam Cipher (One-Time Pad)

Affine Cipher – Activity

- Decrypt the following cipher texts using affine cipher
  - Exercise1
    - CT: nfzzrnnbnhkdfeurp
    - Key: a= 9 b= 7
  - Exercise 2
    - CT: qxgdyfzghqdghxq
    - Key: a= 7 b = 3
  - Exercise 3
    - CT: Urqdcrwjudmlqjzqoell erncrjzqnedirqgghcrnjzqo
    - Key: a = 3 b = 4

Venegere Cipher – Activity

- Decrypt the following cipher texts
  - Exercise 1
    - CT: LBCDUIQVHNJOHYOYGNCVHVG
    - Keyword: Puck
  - Exercise 2
    - CT: JAMVBOVGEVFMYMSCMIPZSMAZJSYMZP
    - Keyword: BOXENTRIQ
- Encrypt the following
  - Exercise 3
    - PT: polyalphabeticity
    - Keyword : magic

Vernam Cipher – Activity

- Encrypt the following
  - Exercise 1
    - PT : clothes do not make the man.
    - Key: Apple
- Decrypt the following cipher texts
  - Exercise2
    - CT: WHPEWHBHRWGZGXEXHRQI
    - Key: ENCRYPT
  - Exercise 3
    - CT: VMRSRNAPKMWBYVFY
    - Key: NGEEANN