School of InfoComm Technology ict Taking IT Higher

NGEE ANN POLYTECHNIC

CRYPTOGRAPHY (CTG)

Diploma in CyberSecurity and Digital Forensics (Dip in CSF)

Academic Year (AY) `21/`22 – Semester 2

WEEK 1.1

CLASSICAL CRYPTOGRAPHY -PART 1

Last Updated: 12/09/2021

Contents

- Recap
- CTG Module Overview -Part 2
- 7 Security Domains
- Classical Ciphers -Part 1
- Summary

CTG Module Overview

- CTG Module Synopsis
- CTG Module Topics
- Reading List
- What is Cryptography?

CTG Module - Learning Objectives (1/2)

□ On module completion, you'd be able to:

1. Explain the essential concepts, definitions, and terminology of cryptography.
2. Describe the various types of classical and modern cryptosystems.
3. Implement certain cryptosystems using Python.
4. Solve basic number theory and information theory problems related to cryptography.

CTG Module - Learning Objectives (2/2)

CTG MODULE OVERVIEW 2

- Cryptography?

- Learning Objectives

- Topics

- Reading List

----

7 SECURITY DOMAINS

CLASSICAL CIPHERS 1

SUMMARY

5. Apply cryptography to solve data security vulnerabilities and threats.
6. Explain how cryptography is applied in the real world applications;
7. Use popular cryptographic software tools.
8. Explain the 7 domains in the field of information security (cryptography belongs to the data security domain).

CTG Module Topics

CTG MODULE OVERVIEW 2
- Cryptography?
- Learning Objectives
- Topics
- Reading List
----
7 SECURITY DOMAINS

CLASSICAL CIPHERS 1

SUMMARY

- You will learn about
  - Essential concepts of cryptography
  - Classical cryptosystems
  - Symmetric key (Private-Key) cryptosystems
  - Asymmetric key (Public-Key) cryptosystems
  - Digital (Public-Key) certificate
  - Hashing
  - Digital signature
  - Public Key Infrastructure (PKI)

Reading List

CTG MODULE OVERVIEW 2
- Cryptography?
- Learning Objectives
- Topics
- **Reading List**

----

7 SECURITY DOMAINS

CLASSICAL CIPHERS 1

SUMMARY

SN	Title	Author
1	Cryptography Theory and Practice (3ed)	Douglas R. Stinson
2	An Overview of Cryptography http://www.garykessler.net/library/crypto.html	Gary C. Kessler
3	Cryptography: An Introduction (3ed)	Nigel Smart
4	An introduction to cryptography and Cryptanalysis	Edward Schaefer
5	Cryptography	Luca Trevisan
6	Crypto 101	Laurens Van Houtven
7	**Hacking Secret Ciphers with Python**	**Al Sweigart**
8	Handbook of Applied Cryptography	Alfred J. Menezes, et. al.
9	Elementary Number Theory: Primes, Congruences, and Secrets	William Stein
10	A Computational Introduction to Number Theory and Algebra (Ver. 2)	Victor Shoup

For Assignment

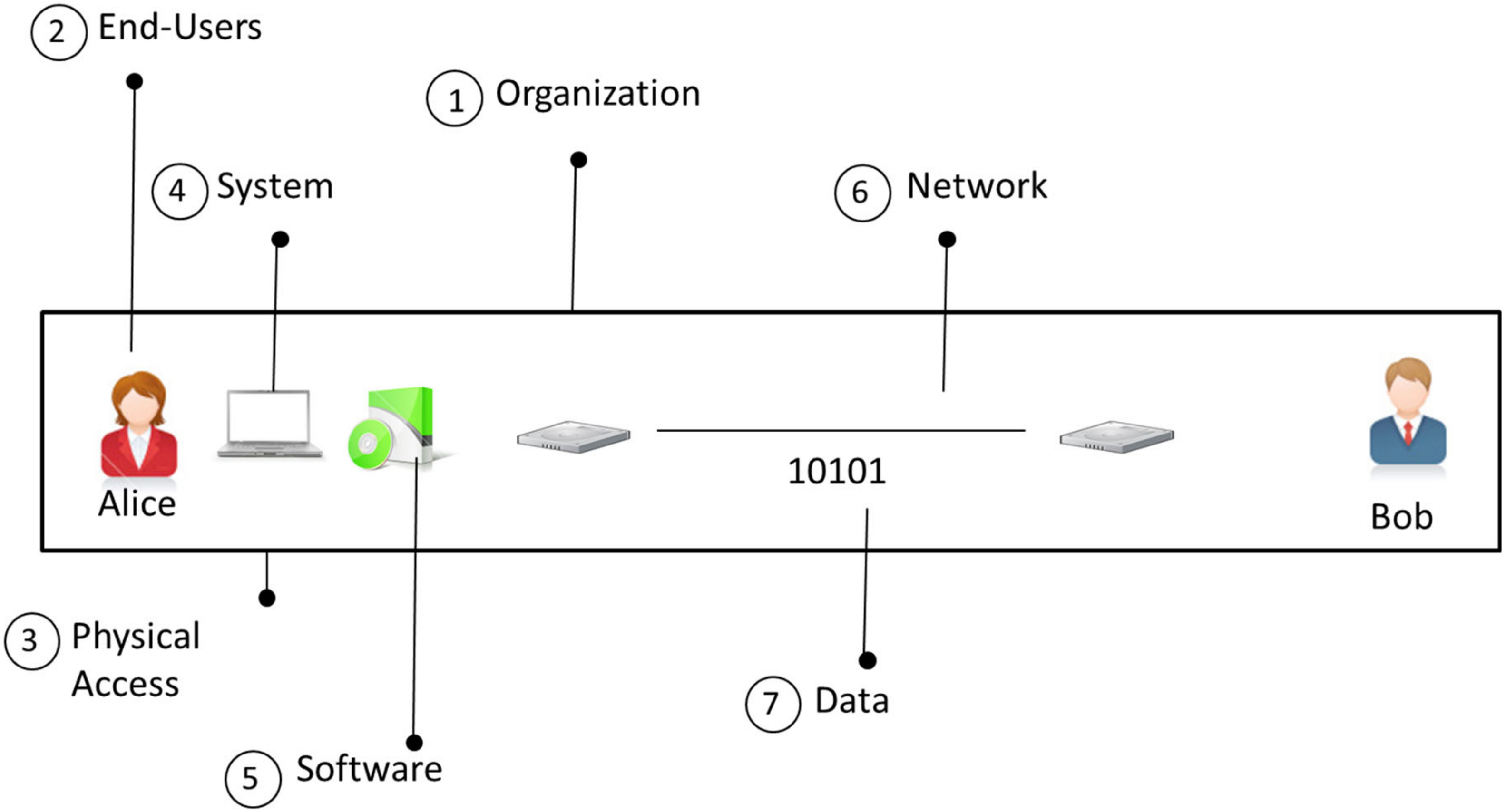
Thanks to the authors (2~10) for making their materials available for free online. You can download them from MeL → Module Information.

7 Security Domains

- Organization
- Physical
- End-user
- System
- Software
- Network
- Data

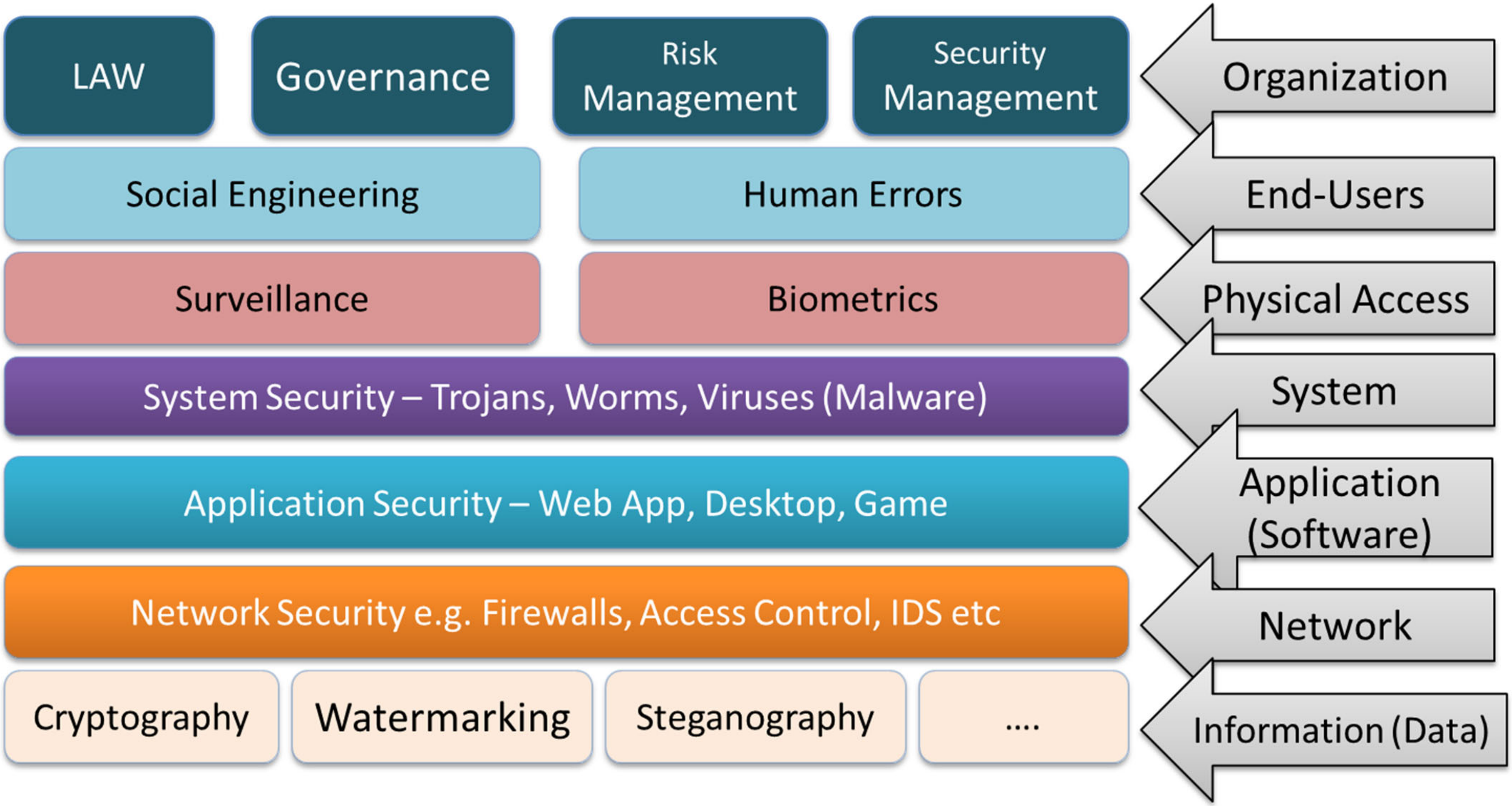
Feedback Component

7 Security Domains



Feedback Component

7 Security Domains



Recap

- Recalling terminologies from the previous semester (CSF module)

What is Cryptography?

CTG MODULE OVERVIEW
----
7 SECURITY DOMAINS

- Learning Objectives
- Topics
- Reading List

- Cryptography?

CLASSICAL CIPHERS 1

SUMMARY

- Duration: 2 mins
- Type in your own words (<= 50 words) on What is Cryptography?
  - ………..

Feedback Component

Crypto Vocabulary

CTG MODULE OVERVIEW

----

7 SECURITY DOMAINS

- Learning Objectives
- Topics
- Reading List

- Cryptography?

CLASSICAL CIPHERS 1

SUMMARY

Source: An introduction to cryptography and cryptanalysis - Edward Schaefer

- Define in your own words
  - Plain text
  - Cipher text
  - Cipher or Cryptosystem
  - Transposition cipher
  - Encryption

Feedback Component

Crypto Vocabulary

CTG MODULE OVERVIEW

----

7 SECURITY DOMAINS

- Learning Objectives
- Topics
- Reading List

- Cryptography?

CLASSICAL CIPHERS 1

SUMMARY

Source: An introduction to cryptography and cryptanalysis - Edward Schaefer

- Define in your own words
  - Decryption
    -
  - Cryptanalysis
    -
  - Key
    -
  - Brute force
    -

Feedback Component

Crypto Vocabulary

CTG MODULE OVERVIEW
----
7 SECURITY DOMAINS

- Learning Objectives
- Topics
- Reading List

- Cryptography?

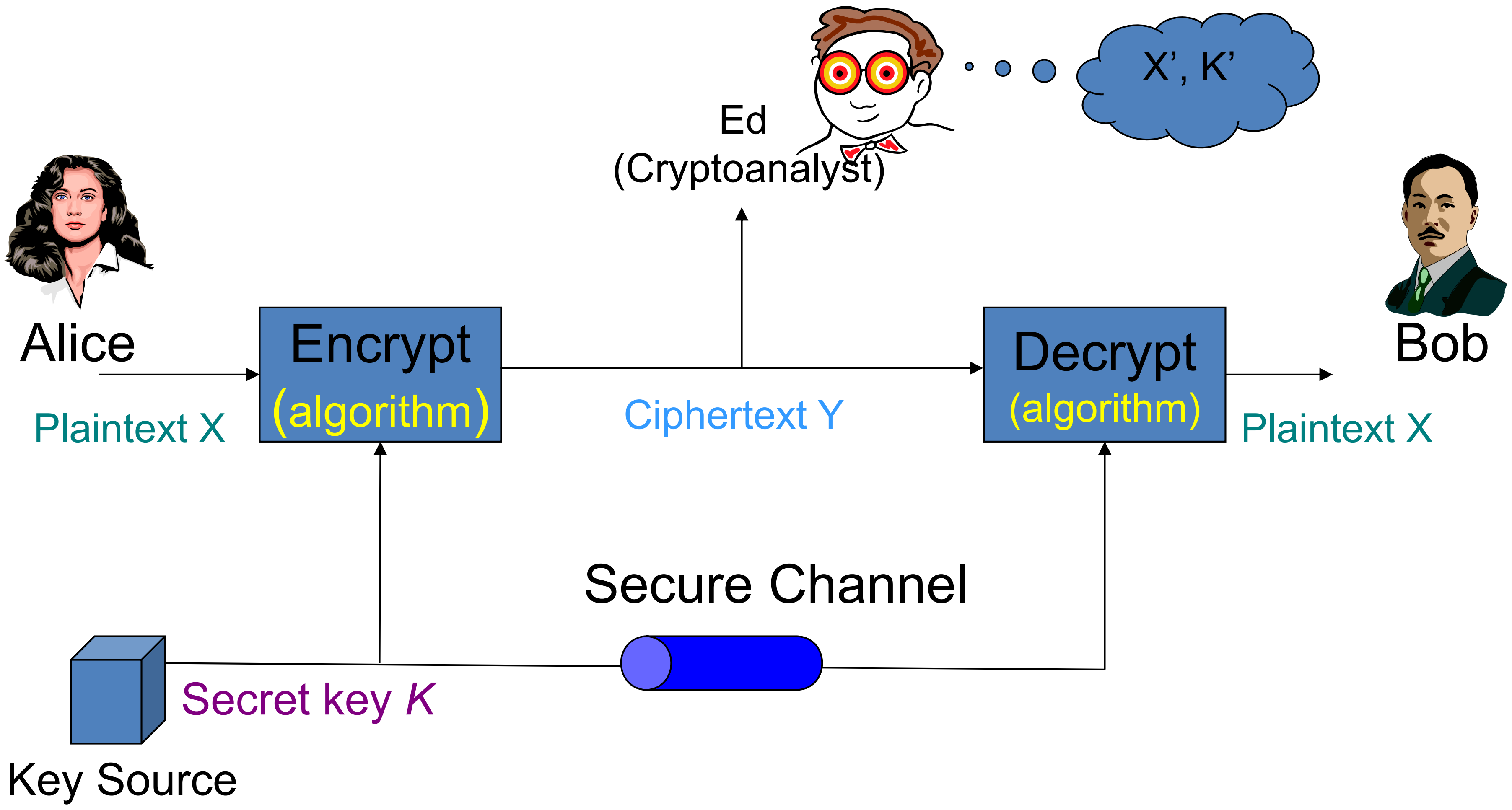
CLASSICAL CIPHERS 1

SUMMARY

Source: An introduction to cryptography and cryptanalysis - Edward Schaefer

- Define in your own words
  - Key
    -
  - Key Length
    -
  - Symmetric Cryptosystem
    -
  - Asymmetric Cryptosystem
    -

Classical Cryptography



Classical Cryptography

- Sender, receiver share common key
  - Keys may be the same, or trivial to derive from one another
  - Sometimes called *symmetric cryptography*
- Two basic types
  - **Transposition ciphers**
  - **Substitution ciphers**
- Product ciphers
  - Combinations of the two basic types

Transposition Cipher

- Rearrange letters in plaintext to produce ciphertext
- Example
  - Plaintext is “`HELLO WORLD`”
  - Rearrange as (with an algorithm)

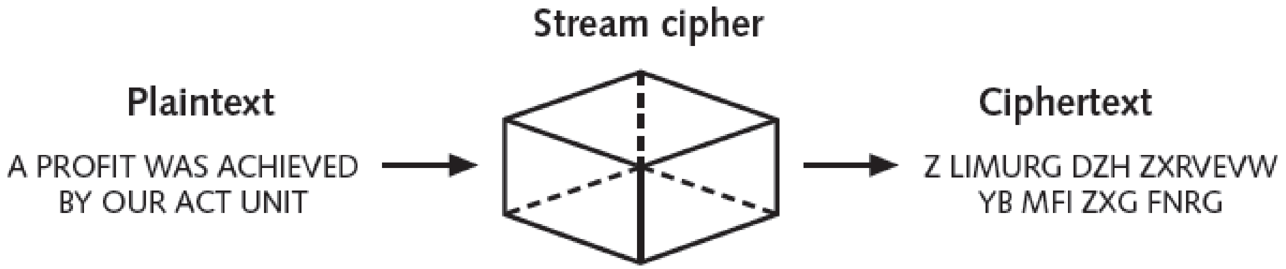
```
HLOOL
ELWRD
```

  - Ciphertext is `HLOOL ELWRD`

Substitution Ciphers

- □ Change characters in plaintext to produce ciphertext
- □ Example

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



Classical Cipher Part 1

More Transposition Ciphers

- Columnar Transposition
- Bifid Cipher
- ADFGX Cipher

Columnar Transposition – Skill 1.1

CTG MODULE OVERVIEW 2

----

7 SECURITY DOMAINS

CLASSICAL CIPHERS 1

- Columnar Transposition

- Bifid Cipher

- ADFGX Cipher

SUMMARY

- Encryption
- Plain Text: A ROTTEN APPLE SPOILS THE BARREL
- Key: ABANDONED

A	B	A	N	D	O	N	E	D	1. Key
1	3	2	7	4	9	8	6	5	2. Assign number value.
A	R	O	T	T	E	N	A	P	3. Record plain text by row
P	L	E	S	P	O	I	L	S	
T	H	E	B	A	R	R	E	L	
									4. Extract by column

- Cipher text: APT OEE RLH TPA PSL ALE TSB NIR EOR

Columnar Transposition – Skill 1.1

CTG MODULE OVERVIEW 2

----

7 SECURITY DOMAINS

CLASSICAL CIPHERS 1

- Columnar Transposition

- Bifid Cipher

- ADFGX Cipher

SUMMARY

- □ Decryption
- □ Cipher Text: APTOEERLHTPAPSLALETSBNIREOR
- □ Key: ABANDONED

A	B	A	N	D	O	N	E	D	**1. Determine key**
1	3	2	7	4	9	8	6	5	2. Assign number value
A	R	O	T	T	E	N	A	P	3a. No. of rows = cipher text size / key size = 27/9 = 3 3b. Record cipher text by column
P	L	E	S	P	O	I	L	S	
T	H	E	B	A	R	R	E	L	
									4. Extract by column

- □ Plain text: AROTTENAPPLESPOILSTHE BARREL

Columnar Transposition – Activity 1.1

CTG MODULE OVERVIEW 2

----

7 SECURITY DOMAINS

CLASSICAL CIPHERS 1

- Columnar Transposition

- Bifid Cipher

- ADFGX Cipher

SUMMARY

- Decrypt the following cipher texts using columnar transposition
  - Exercise1
    - Cipher Text: ararafiamolttvmnetoetipc
    - Key: ABACUS
  - Exercise 2
    - Cipher Text: aindtdrhbkmawadijrnae
    - Key: ABETTER
  - Exercise 3
    - Cipher Text: Lfgxaeexnznxborxiaey
    - Key: ZEBRA

Thinking & Activity Component | **Doing, Exploring: LCL**

Columnar Transposition – Activity 1.1

CTG MODULE OVERVIEW 2

----

7 SECURITY DOMAINS

CLASSICAL CIPHERS 1

- Columnar Transposition

- Bifid Cipher

- ADFGX Cipher

SUMMARY

- Decrypt the following cipher texts using columnar transposition
  - Exercise 4
    - Cipher Text: EARAORNSIEBDOAEESHNREMMSGAUSSNNOCL
    - Key: PILGRIM
  - Exercise 5
    - Cipher Text: VNYOEOMCTEUAOPHHMRTSVOKROLR
    - Key: SQUANTO
  - Exercise 6
    - Cipher Text: UPILAIAPCHAKACUPDWEINACNEMNPREMETS
    - Key: MAYFLOWER

Bifid Cipher – Skill 1.2

Developed in 1901 by the Frenchman Felix Delastelle

- □ Encryption: Plain text: FLEEATONCE
- □ 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

- □ Step A:

	F	L	E	E	A	T	O	N	C	E
Row	4	4	3	3	3	5	3	2	4	3
Col.	1	3	5	5	3	1	2	3	2	5

- □ Step B: 4 4 3 3 3 5 3 2 4 3 1 3 5 5 3 1 2 3 2 5
- □ Step C:

44	33	35	32	43	13	55	31	23	25	
U	A	E	O	L	W	R	J	N	S	CIPHER TEXT

Thinking & Activity Component | Doing, Exploring: LCL

Bifid Cipher – Activity 1.2

CTG MODULE OVERVIEW 2

----

7 SECURITY DOMAINS

CLASSICAL CIPHERS 1

- Columnar Transposition

- Bifid Cipher

- ADFGX Cipher

SUMMARY

- Decrypt the following cipher texts using Bifid cipher
  - Exercise1
    - Cipher Text: NIANICOPFQ
    - Key: As in the previous slide
  - Exercise 2
    - Cipher Text: WORECPNGRL
    - Key: As in the previous slide

Thinking & Activity Component | Doing, Exploring: LCL

Bifid Cipher – Activity 1.2.1

CTG MODULE OVERVIEW 2

----

7 SECURITY DOMAINS

CLASSICAL CIPHERS 1

- Columnar Transposition

- Bifid Cipher

- ADFGX Cipher

SUMMARY

□ Decrypt the following cipher texts using Bifid cipher

Key:

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

- Exercise 3
  - Cipher Text: fudsnnv spnt ilhb eoisqwvr usip
- Exercise 4
  - Cipher Text: wmt oe fo gih t os dqgro
- Exercise 5
  - Cipher Text: chfuo mqmwrstshiyr fx tlx

ADFGX Cipher – Skill 1.3

CTG MODULE OVERVIEW 2

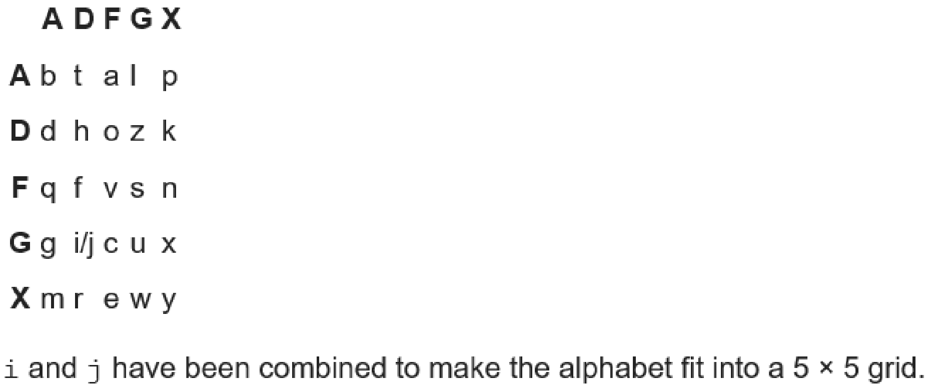
----

7 SECURITY DOMAINS

CLASSICAL CIPHERS 1
- Columnar Transposition
- Bifid Cipher
- **ADFGX Cipher**

SUMMARY

- Refer to the reference and please figure it out yourself.
- Similar to Bifid Cipher
- Reference:
  - http://en.wikipedia.org/wiki/ADFGVX_cipher



	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

i and j have been combined to make the alphabet fit into a 5 × 5 grid.

Thinking & Activity Component | **Doing, Exploring: LCL**

ADFGX Cipher – Activity 1.3

CTG MODULE OVERVIEW 2

----

7 SECURITY DOMAINS

CLASSICAL CIPHERS 1

- Columnar Transposition

- Bifid Cipher

- ADFGX Cipher

SUMMARY

- Decrypt the following cipher texts using ADFGX cipher
  - Exercise1
    - Cipher Text: AFDDAFAFADAFFFDXXFDGADGD
    - Key: ABETS
  - Exercise 2
    - Cipher Text: XXFGADDXDXFGADDFDDGGXFDF
    - Key: ZOUKS
- Succeeded in understanding ADFGX Cipher?
  - Try ADFGVX Cipher.

Summary

Week 1.1

Week 1.1 - Summary

CTG MODULE OVERVIEW 2

----

7 SECURITY DOMAINS

CLASSICAL CIPHERS PART 2

SUMMARY

- Skill
- Knowledge
- Activity
- Thinking
- Feedback

Component	You learnt
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