School of InfoComm Technology ict Taking IT Higher

NGEE ANN POLYTECHNIC

1

CRYPTOGRAPHY (CTG)

Diploma in Information Security and Forensics (Dip in ISF)

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

WEEK 2.1

CLASSICAL CRYPTOGRAPHY – PART 2

Last Updated: 14/10/2021

Contents

Week 2.1 Recap

Substitution Ciphers Part 2

Research on One-Time Pad

Summary

Week 2.1 Recap

Week 2.1 - Summary

SUBSTITUTION CIPHERS 1

TRANSPOSITION CIPHER EXERCISES

SUMMARY

Component	You learnt
Skills & Knowledge	Modular Arithmetic Shift Cipher with Modular Arithmetic
Activities	Substitution Ciphers • Pigpen Cipher • Shift Cipher with Cipher Disks • Shift Cipher with Modular Arithmetic Transposition Ciphers • Columnar Transposition Cipher • Bifid Cipher • ADFGX Cipher
Thinking	The concept of "Shift" Modular Arithmetic calculations
Feedback	Pigpen Cipher Shift Cipher Modular Arithmetic

5

Substitution Ciphers Part 2

Affine Cipher

Vigenere Cipher

One Time Pad (Vernam)

6

Affine Cipher

Affine Cipher

SUBSTITUTION CIPHERS 2
- Affine Cipher
- Vigenere Cipher

ONE-TIME PAD

SUMMARY

- The affine cipher is a type of monoalphabetic substitution cipher
- The monoalphabetic substitution takes a letter of an alphabet and substitutes it with another letter. The way of converting is fixed. A character of the plaintext will be replaced by the same ciphertext character, during the entire ciphertext.

Affine Cipher - Encryption

SUBSTITUTION CIPHERS 2
- Affine Cipher
- Vigenere Cipher

ONE-TIME PAD

SUMMARY

- Affine cipher consists of 2 Keys, we'll call them a and b
- Let:

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

- Select key "a" between 0,…,25
  - Condition for a: gcd(a,26) = 1
    - gcd: Greatest Common Divisor
  - So, a = 1,3,5,7,9,11,15,17,19,21,23,25
- Select another key "b" between 0,…,25
- $CT = ((a \times PT) + b) \bmod 26$
  - CT: Cipher Text, PT: Plain Text

Affine Cipher – Why gdc(a,26)=1?

SUBSTITUTION CIPHERS 2
- Affine Cipher
- Vigenere Cipher

ONE-TIME PAD

SUMMARY

- Let *a* = 4
  - gcd(4,26) = 2
- Let *b* = 7
- CT = ((*4* x PT) + *7*) mod 26

PT	a	b	c	d	e	f	g	h	i	j
	0	1	2	3	4	5	6	7	8	9
CT	**7**	11	15	19	23	**1**	**5**	9	13	17
	H	L	P	T	X	B	F	J	N	R

PT	k	l	m	n	o	p	q	r	s	t
	0	1	2	3	4	5	6	7	8	9
CT	21	25	3	**7**	11	15	19	23	**1**	**5**
	V	Z	D	H	L	P	T	X	B	F

Different Plain Text lead to same Cipher Text. Therefore gcd(*a*,26) must be equal to 1

Affine Cipher: Encryption - Decryption

- CT = ((*a* x PT) + *b*) mod 26
- PT = (a^{-1} x (CT – *b*)) mod 26
  - a^{-1} is called "modular multiplicative inverse" of *a*
- *Select any one of* the following values for a
  - 1,3,5,7,9,11,15,17,19,21,23,25
  - Since gcd(*a*,26) = 1
- Select "*b*" between 0,…,25
- We will learn how to calculate a^{-1} later in this module, for now just use the values provided in the table below

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

- Let *a* = 3, *b* = 7

Encryption

PT	c	a	t
	2	0	19
CT = ((*3* x PT) + *7*) mod 26	13	7	12
	N	H	M

Decryption

CT	N	H	M
	13	7	12
PT = (3^{-1} x (CT - *7*)) mod 26 PT = (*9* x (CT - *7*)) mod 26	2	0	19
	c	a	t

Affine Cipher – Possible Keys

SUBSTITUTION CIPHERS 2
- Affine Cipher
- Vigenere Cipher

ONE-TIME PAD

SUMMARY

- "*a*" can only take 12 values
  - a = 1,3,5,7,9,11,15,17,19,21,23,25
    - Since gcd(a,26) = 1
  - "*b*" can take 26 values between 0,…,25
  - Therefore the no. of possible keys
    - 12x26 = 312
- NOTE: Shift Cipher has only 26–1=25 possible keys

Affine Cipher: Exercises

SUBSTITUTION CIPHERS 2
- Affine Cipher
- Vigenere Cipher

ONE-TIME PAD

SUMMARY

- Decrypt the following
  - Ex1
    - CT: apmfmgfzcm
    - Keys: a= 3, b= 7
  - Ex2
    - CT: cxoahnetnhmzekf
    - Keys: a= 7, b= 10
  - Ex3
    - CT: mbcyjcwnczmwkmvvdozf
    - Keys: a= 15, b= 12

Vigenere Cipher

Vigenere Cipher

SUBSTITUTION CIPHERS 2
- Affine Cipher
- Vigenere Cipher

ONE-TIME PAD

SUMMARY

- The Vigenère Cipher is a polyalphabetic substitution cipher.
  - A polyalphabetic cipher uses a number of substitutions at different positions in the message, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext and vice versa
- Vigenere Cipher was actually first described by Giovan Battista Bellaso in 1553.
- However, in the 19th Century, it was misattributed to Blaise de Vigenère, who had presented a similar cipher (theAutokey Cipher) in 1586.
- The Vigenère Cipher was renowned for being a very secure cipher, and for a very long time it was believed to be unbreakable.
- It was fully broken by Friedrich Kasiski in 1863, it is still a very secure cipher in terms of paper and pen methods.

Vigenere Cipher

- The cipher is implemented using the Vigenère Square, which is made up of 26 distinct cipher alphabets

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

Vigenere Cipher

- Suppose the plaintext message was “EXAM QUESTIONS ENCLOSED” and the keyword was SINGAPORE. Hence, the following:

S	I	N	G	A	P	O	R	E	S	I	N	G	A	P	O	R	E	S	I	N
E	X	A	M	Q	U	E	S	T	I	O	N	S	E	N	C	L	O	S	E	D

- To perform the substitution:
  - Combination of keyword and message letters, SE.
  - Use the keyword letter to locate the column, the message letter to find the row, and look for the letter at their intersection.
    - For column “S” and row “E,” the ciphertext letter “W” will be found.
- - Hence, each of the letters in the message will produce the encrypted ciphertext: WFNSQJSJXAWAYECQCSKMQ.

Vigenere Cipher: Exercises

SUBSTITUTION CIPHERS 2
- Affine Cipher
- Vigenere Cipher

ONE-TIME PAD

SUMMARY

- Decrypt the following
  - Ex1
    - CT: WZVFINLSOHCWAQMERTBJAHIHVPEIEHZCS
    - Key: wonderland
  - Ex2
    - CT: I I P Q I F Y S T Q W W B T N U I U R E U F
    - Key: MEC
  - Ex3
    - CT: HHWKSWXSLGNTCG
    - Keys: PASCAL

Shift vs. Affine vs. Vigenere Ciphers

Shift

- Monoalphabetic Cipher
- Possible Keys:
  - 25
- Can be broken using Frequency Analysis
  - http://practicalcryptography.com/ciphers/classical-era/caesar/

Affine

- Monoalphabetic Cipher
- Possible Keys:
  - 312
- Can be broken
  - using Frequency Analysis
  - if the plaintext of any two ciphertext characters is known
  - http://practicalcryptography.com/ciphers/classical-era/affine/

Vigenere

- Polyalphabetic Cipher
- A key phrase/word of any length
- Cryptanalysis of the Vigenere cipher has 2 main steps: identify the period of the cipher (the length of the key), then find the specific key.
  - http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-vigenere-cipher/

19

One Time Pad

Homework Exercise:

* Read the article given in Wikipedia on one-time pad (vernam cipher)

- https://en.wikipedia.org/wiki/One-time_pad

(i) Figure out yourself how the one-time pad works

(ii) What are the possible advantages & disadvantages of this cipher algorithm?

* Other reference:

- https://genesisdatabase.wordpress.com/2010/12/13/cryptography-caesar-vigenere-vernam-columnar/

Summary

Week 2.2

Week 2.2 - Summary

SUBSTITUTION CIPHERS 2
- Affine Cipher
- Vigenere Cipher

ONE-TIME PAD

SUMMARY

Component	You learnt
Skills & Knowledge	Affine Cipher Vigenere Cipher
Activities	Affine Cipher Vigenere Cipher
Thinking	Concept of gcd(a,26) = 1 Possible number of keys for Affine Cipher Shift vs. Affine vs. Vigenere Ciphers One-Time Pad
Feedback	Affine Cipher Vigenere Cipher Shift vs. Affine vs. Vigenere Ciphers