زانکۆی سەلاحەدین - هەولێر
Salahaddin University-Erbil

Coding Theory and Cryptography

Lecture Six

Classical Cryptography- Part 2

Instructor: Newroz N. Abdulrazaq

Science College- Department of Computer Science & I.T.

newroz.abudlrazaq@su.edu.krd

Text Book: William Stalling, Cryptography And Network Security Principles And Practice.+ Educational Websites.

Overview:

- Vigenere Cipher.
  - Encryption Process.
  - Decryption Process.
- Affine Cipher.
  - Encryption Process.
  - Decryption Process.

Vigenere Cipher

- is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword.
- It employs a form of polyalphabetic substitution.
- The key for the encryption is a vector. Often the key corresponds to a word that is easily remembered. In our case, the word is vector. The security of the system depends on the fact that neither the keyword nor its length is known.

Vigenere Encryption & Decryption Process

1. Choose a keyword (or key phrase). Then Find the index for each letter within keyword.
2. Find the index for each letter within Plaintext.
3. Repeat this keyword over and over until it is the same length as the plaintext.
4. **For encryption**: i=0, 2, …, length(plaintext)

$$c[i] = p[i]+key[i \bmod length(key)] \bmod 26$$

For decryption:

$$p[i] = c[i]-key[i \bmod length(key)] \bmod 26$$

Example: Encrypt (Thanks Peshmarga) using Vigenere cipher with key= hawler?

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

Step2: Convert the key from alphabetic to it is index:

h	a	w	l	e	r
7	0	22	11	4	17

Step3: Convert the plaintext from alphabetic to it is index:

t	h	a	n	k	s	p	e	s	h	m	a	r	g	a
19	7	0	13	10	18	15	4	18	7	12	0	17	6	0

Step3&4:Repeat this keyword over and over until it is the same length as the plaintext and use c=(index+key)mod26.

Plain Text	t	h	a	n	k	s	p	e	s	h	m	a	r	g	a
Plain Index	19	7	0	13	10	18	15	4	18	7	12	0	17	6	0
Key Index															
Index + key	26	7	22	24	14	35	22	4	40	18	16	17	24	6	22
Mod 26	0	7	22	24	14	9	22	4	14	18	16	17	24	6	22
Cipher Text	A	H	W	Y	O	J	W	E	O	S	Q	R	Y	G	W

∴ **Cipher Text = AHWYOJWEOSQRYGW**

Example: Decrypt (XMNVCPO) using Vigenere cipher with key= kirkuk?

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

Step2: Convert the key from alphabetic to it is index:

k	i	r	k	u	k
10	8	17	10	20	10

Step3: Convert the ciphertext from alphabetic to it is index:

X	M	N	V	C	P	O
23	12	13	21	2	15	14

Step3&4:Repeat this keyword over and over until it is the same length as the cipher text and use c=(index-key)mod26.

Cipher Text	X	M	N	V	C	P	O
Cipher Index	23	12	13	21	2	15	14
Key Index							
Index - key	13	4	-4	11	-18	5	4
Mod 26	13	4	22	11	8	5	4
Plain Text	n	e	W	l	i	f	e

∴ Plain Text = new life

Example: Find the key of Vigenere cipher, if you know that the plaintext is (new life) while cipher text is (JIJHQSA)?

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

Step2: Convert the plaintext from alphabetic to it is index:

n	**e**	**w**	**l**	**i**	**f**	**e**
13	4	22	11	8	5	4

Step3: Convert the ciphertext from alphabetic to it is index:

J	**I**	**J**	**H**	**Q**	**S**	**A**
9	8	9	7	16	18	0

Step3: key=(cipher_index-plain_index)mod26.

Cipher index	9	8	9	7	16	18	0
Plain Index	13	0	22	11	8	5	4
Cindex - Pindex	-4	8	-13	-4	8	13	-4
Mod 26	22	8	13	22	8	13	22
Key word	w	i	n	w	i	n	W

∴ key word = Win

Vigenere Cipher- Table Representation

	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

p	e	s	h	m	a	r	g	a
h	a	w	l	e	r	h	a	W
W	E	O	S	Q	R	Y	G	W

Affine Cipher

- The affine cipher is a type of monoalphabetic substitution cipher.
- The 'key' for the Affine cipher consists of 2 numbers, we'll call them $\alpha \; and \; \beta$.
- α should be chosen to be relatively prime to m (the length of the alphabet used) i.e. GCD(α ,m)=1
- The Caesar cipher is an Affine cipher with α = 1.

Affine Encryption & Decryption Process

1. Choose α *and* β, such that GCD(α, 26)=1.

2. Find the index for each letter within Plaintext.

3. For each index within Plaintext do the following:

For Encryption: c= (α×index + β) mod 26.

For Decryption: p= α^{-1}×(index - β) mod 26.

Example: Encrypt (Computer) using Affine cipher with keys α=5 *and* β=8?

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

For Encryption we should use $c = (\alpha \times index + \beta) \bmod 26$

$= (5 \times index + 8) \bmod 26$

Plain Text: Cipher Text:

$c \equiv 2 \Rightarrow c = 5 \times 2 + 8 = 18 \bmod 26 = 18 \Rightarrow$ S

$o \equiv 14 \Rightarrow c = 5 \times 14 + 8 = 78 \bmod 26 = 0 \Rightarrow$ A

$m \equiv 12 \Rightarrow c = 5 \times 12 + 8 = 68 \bmod 26 = 16 \Rightarrow$ Q

Cont.

Plain Text: Cipher Text:

$p \equiv 15 \Rightarrow c = 5 \times 15 + 8 = 83 \bmod 26 = 5 \Rightarrow F$

$u \equiv 20 \Rightarrow c = 5 \times 20 + 8 = 108 \bmod 26 = 4 \Rightarrow E$

$t \equiv 19 \Rightarrow c = 5 \times 19 + 8 = 103 \bmod 26 = 25 \Rightarrow Z$

$e \equiv 4 \Rightarrow c = 5 \times 4 + 8 = 28 \bmod 26 = 2 \Rightarrow C$

$r \equiv 17 \Rightarrow c = 5 \times 17 + 8 = 93 \bmod 26 = 15 \Rightarrow P$

∴ Cipher Text = PAQFEZCP

Example: Decrypt (SAQFEZCP) using Affine cipher with keys α=5 *and* β=8?

Find inverse of α=5 mod 26 = 21 → **H.W.**

For Decryption we should use $P = \alpha^{-1} \times (\text{index} - \beta) \bmod 26$

$= 21 \times (\text{index} - 8) \bmod 26$

Cipher Text:		Plain Text:
S ≡ 18	$c = 21 \times (18 - 8) = 210 \bmod 26 = 2$	c
A≡ 0	$c = 21 \times (0 - 8) = -168 \bmod 26 = 14$	o
Q ≡ 16	$c = 21 \times (16 - 8) = 168 \bmod 26 = 12$	m

Cont….

Cipher Text: Plain Text:

F ≡ 5 ⇒ c = 21 × (5- 8) = -63 mod 26 = 15 ⇒ p

E ≡ 4 ⇒ c = 21 × (4 - 8) = -84 mod 26 = 20 ⇒ u

Z ≡ 25 ⇒ c = 21 × (25 - 8) = 357 mod 26 = 19 ⇒ t

C ≡ 2 ⇒ c = 21 × (2 - 8) = -126 mod 26 = 4 ⇒ e

P ≡ 15 ⇒ c = 21 × (15 - 8) = 147 mod 26 = 17 ⇒ r

∴ Plain Text = computer

Homework6:

Q1: Use Affine cipher to Decrypt the message (XIIXFL) α=17 *and* β=23?

Q2: Use Vigenere cipher to Encrypt the message (Attack starts tomorrow) with key =lemmon?

Q3: Use Affine cipher to Decrypt the message (opqz) if you know that the last two letters from plaintext are (fe)?