


Nama: Faiz Abyan Heryanto NIM: 064002300043	 PRAKTIKUM KEAMANAN INFORMASI	MODUL 1 Nama Dosen: Ir. Adrian Qamar, MTI
Hari/Tanggal: Selasa, 17 September 2024 2024		Nama Asisten Laboratorium : 1. Achmad Fauzy 2. Radea Aji Prasajo

POKOK BAHASAN I

Caesar Cipher

KODE POKOK BAHASAN : TIK.KI01.016.001.01

DESKRIPSI POKOK BAHASAN : Mengetahui dan memahami kriptografi Caesar Cipher.

No	Elemen Kompetensi	Indikator Kinerja	Jml Jam	Halama n
1	Caesar Cipher	Mampu menghitung dan menjelaskan teknik substitusi algoritma Caesar Cipher	3	
	Total jam		3	

1. Teori Singkat

1.1 Kriptografi



Apa yang dimaksud dengan kriptografi? Kripto = Rahasia, Grafi = Tulisan, Secara bahasa kriptografi adalah ilmu yang mempelajari teknik-teknik menulis pesan rahasia. Menurut sejarah dan tekniknya kriptografi dapat dibagi menjadi 3 kategori.

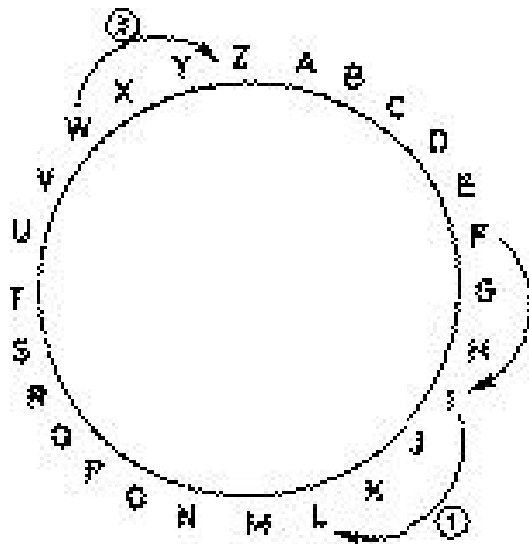
- a. Kriptografi Klasik
- b. Kriptografi Konvensional
- c. Kriptografi Kuantum

1.2 Kriptografi Klasik

Terdapat 2 teknik utama yang menjadi dasar bagi ilmu kriptografi yang digunakan sejak masa kriptografi klasik, diantaranya:

- a. Teknik Geser (Shift Cipher)

Salah satu algoritma yang paling banyak disebut untuk mewakili dari kelompok Teknik Geser adalah algoritma Caesar Cipher. Menurut sejarah Caesar cipher digunakan oleh kaisar Julius Caesar (100-44 B.C) untuk menyandikan pesan-pesan pentingnya. Secara praktis algoritma ini bekerja dengan cara menggeser pesan asli (plaintext) beberapa selang abjad dari posisi semulanya menjadi pesan tersandi (ciphertext).



$$\text{Ciphertext} = \{\text{Plaintext} + \text{Kunci}\} \bmod (N)$$



Plaintext = { Ciphert xt – kunci } mod (N) = jumlah alphabet

Misal:

Plaintext : universitas

Kunci : 3

Ciphertext : XQLYHU VLWDV

b. Teknik Anti (Substitution Cipher)

Secara prinsip algoritma Substitution Cipher bekerja dengan cara mengganti setiap sel (bit, byte, blok) pesan menjadi bentuk sel lain. Terdapat 2 jenis utama Teknik Ganti yaitu Monoalphabetic Cipher dan Poly-alphabetic Cipher. Perbedaan utama dari keduanya terletak pada kekonsistenan perubahan sel pesan dan penggunaan kunci. Mono-alphabetic Cipher.

<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>	<i>j</i>	<i>k</i>	<i>l</i>	<i>m</i>
<i>X</i>	<i>N</i>	<i>Y</i>	<i>A</i>	<i>H</i>	<i>P</i>	<i>O</i>	<i>G</i>	<i>Z</i>	<i>Q</i>	<i>W</i>	<i>B</i>	<i>T</i>

<i>n</i>	<i>o</i>	<i>p</i>	<i>q</i>	<i>r</i>	<i>s</i>	<i>t</i>	<i>u</i>	<i>v</i>	<i>w</i>	<i>x</i>	<i>y</i>	<i>z</i>
<i>S</i>	<i>F</i>	<i>L</i>	<i>R</i>	<i>C</i>	<i>V</i>	<i>M</i>	<i>U</i>	<i>E</i>	<i>K</i>	<i>J</i>	<i>D</i>	<i>I</i>

Gambar 1.1 Peta Substitusi Mono-alphabetic Cipher

Pada Mono-alphabetic Cipher setiap isi sel pesan selalu diganti dengan sel yang sama (statis), kelemahan utama dari teknik ini rentan terhadap serangan jenis “frekuensi kemunculan huruf”. Sebagai contoh dalam teks berbahasa inggris terdapat huruf yang lebih dominan muncul ketimbang huruf lainnya, ini menjadi dasar untuk menganalisis isi pesan sesungguhnya.



Tabel 1.1 Frekuensi Kemunculan Huruf Pada Teks Dokumen Berbahasa Inggris

Letter	Probability	Letter	Probability
A	.082	N	.067
B	.015	O	.075
C	.028	P	.019
D	.043	Q	.001
E	.127	R	.060
F	.022	S	.063
G	.020	T	.091
H	.061	U	.028
I	.070	V	.010
J	.002	W	.023
K	.008	X	.001
L	.040	Y	.020
M	.024	Z	.001

1.3 Poly-alphabetic Cipher



Pada Poly-alphabetic Cipher justru diharapkan untuk suatu sel yang sama dapat diganti menjadi sel –sel yang berbeda tergantung kepada isi kuncinya. Contoh utama implementasi algoritma Poly-alphabetic Cipher adalah Vigenere Cipher Pertama kali dibuat pada abad ke-16 oleh Blaise de vigenere. Vigenere cipher menjadi sangat populer pada masa perang dunia ke-2, dimana masing-masing pihak yang berperang banyak memanfaatkan mesin berbasis vigenere cipher sebagai alat penyandi pesan.

	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

Tabel 1.2. Vigenere Cipher

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

Misal

Plaintext: wearediscoveredsaveyourself

Kunci: deceptive

Ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ



ELEMEN KOMPETENSI I

- Tulislah source code dan hasil enkripsi untuk setiap plaintext yang anda buat.
- Buat isi pesan asli simpan kedalam file latihan.txt
- Compile program diatas javac Caesar.java
- Jalankan enkripsi dengan perintah java Caesar -e key < latihan.txt
- Catatan key bisa anda ganti dengan kunci bilangan: 1, 2, 3 ...
- Untuk mengembalikan pesan semula buat pesan sandi simpan pada sandi.txt
- Jalankan dekripsi dengan perintah java Caesar -d key < sandi.txt

Contoh:

No	Plaintext	Key	Chipertext
1	Attackatonce	4	exxegoexsrgi
2	Needbackup	4	riihfegoyt
3	Intwodaysgotonorth	5	nsybtifdxltytstwym

Source Code

```
class CaesarCipher
{
    // Encrypts text using a shift od s
    public static StringBuffer encrypt(String text, int s)
    {
        StringBuffer result= new StringBuffer();

        for (int i=0; i<text.length(); i++)
        {
            if (Character.isUpperCase(text.charAt(i)))
```



```
{
    char ch = (char)(((int)text.charAt(i) +
                     s - 65) % 26 + 65);
    result.append(ch);
}
else
{
    char ch = (char)(((int)text.charAt(i) +
                     s - 97) % 26 + 97);
    result.append(ch);
}
}
return result;
}

// Driver code
public static void main(String[] args)
{
    String text = "ATTACKATONCE";
    int s = 4;
    System.out.println("Text: " + text);
    System.out.println("Key: " + s);
    System.out.println("Cipher: " + encrypt(text, s));
}
}
```



Output

1. Latihan

Buat tabel hasil dan analisa hasil enkripsi program Caesar cipher untuk setiap plaintext yang anda buat (**5 plaintext**)

No	Plaintext	Key	Chipertext
1	Attackatonce	4	Cipher: EXXEGOEXSRGI
2	Needbackup	4	Cipher: Riihfegoyt
3	Intwodaysgotonorth	5	Cipher: Nsybtifdxltytstwym
4	HafidzRamadhan	6	Cipher: NglojfXgsgjngt
5	FaizAbyanHeryanto	9	Cipher: OjriJkhjwQnahjwcx

2. Tugas

Buat tabel hasil dan analisa hasil enkripsi program Caesar Cipher untuk setiap plaintext yang anda buat (**Minimal 20 plaintext**)

No	Plaintext	Key	Chipertext
----	-----------	-----	------------



1	A\$7L#9	5	Cipher: F]VQ\X
2	Z8#C!2	3	Cipher: CUZFX0
3	R1*G4X	6	Cipher: XQJMTD
4	Q#9P&5	7	Cipher: X^ZWaV
5	J3!T\$7	4	Cipher: NQYX\U
6	F5&L@2	8	Cipher: NWHTHT
7	U#2R!6	2	Cipher: WYNTWR
8	D9!H%3	1	Cipher: ETVIZN
9	K@3L\$8	7	Cipher: RaTS_Y
10	W4&X#9	6	Cipher: CT`D]Y
11	V7%Y@2	5	Cipher: AV^D_Q
12	H!1T&4	3	Cipher: KXNW]Q
13	M9\$F#5	8	Cipher: U[`N_W
14	E6!L%2	4	Cipher: T]UV[XZ
15	N#5P!8	6	Cipher: T]UV[XZ
16	T7@K\$3	1	Cipher: UR[LYN
17	B\$4J!9	8	Cipher: J`VR][
18	S2&X#5	3	Cipher: VO]AZR
19	G!9V%7	5	Cipher: LZXA^V
20	I6#Y@4	2	Cipher: KRYA\P



CEK LIST

No	Kegiatan	Checked
1	Memberikan penjelasan definisi kriptografi	✓
2	Memberikan pengetahuan tentang kategori kriptografi klasik	✓
3	Menjelaskan beberapa jenis algoritma kriptografi klasik	✓
4	Mampu menghitung dan menjelaskan teknik substitusi algoritma Caesar Cipher	✓

