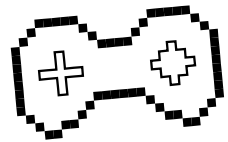
Praktikum Kriptografi

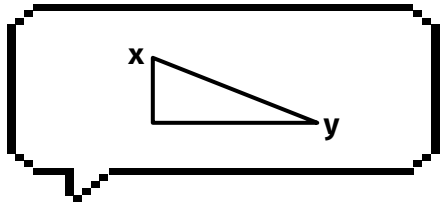
Pertemuan - 05

Topik: Vigenere, Autokey, Permutasi

Review



Materi yang sudah dipelajari dari Pertemuan 1 hingga Quiz



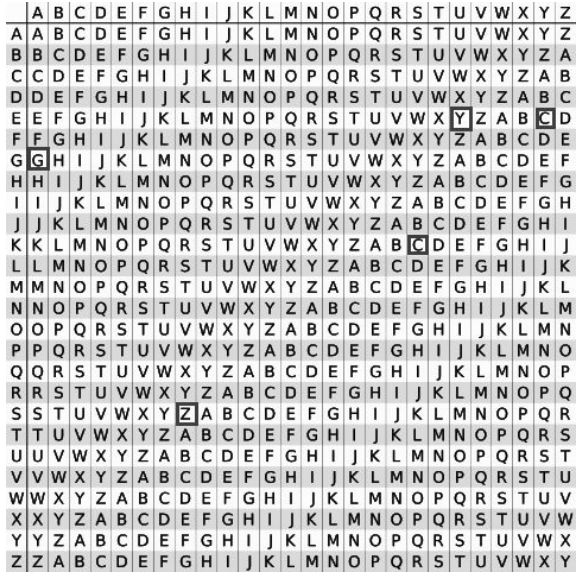
01

Vigenere Cipher

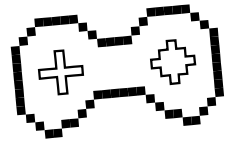
Vigenere Cipher

Vigenere Cipher merupakan sebuah bentuk polyalphabetic cipher, dimana akan **dilakukan beberapa substitusi alfabet**. Proses enkripsi manual umumnya memanfaatkan **Vigenere Table/Square.**

Proses enkripsi menggunakan **Plain Text** & **Key.** (Key pada kasus ini merupakan text lain, bukan angka)



Vigenere Cipher



Enkripsi

E(x) = (x+K) mod 26

Dekripsi

D(x) = (x-K) mod 26

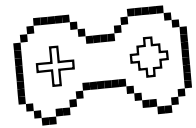
A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Ket:

x = alfabet dalam angka (A-Z = 0-25)

K = kunci dalam angka (A-Z = 0-25)

Enkripsi Vigenere Cipher

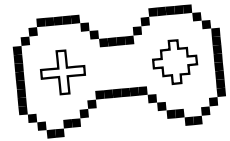


1. Tentukan **Plaintext** (Pt), dan **konversi** ke dalam bentuk angka
2. Tentukan **Key** (K), dan **konversi** ke dalam bentuk angka
3. Pasangkan setiap huruf pada **Pt** dengan **K**, key dapat di-extend sesuai jumlah karakter **Pt,** jika **Pt** lebih panjang dari **K**
4. Operasikan **Pt** dan **K**, sesuai rumus enkripsi

Dekripsi Vigenere Cipher

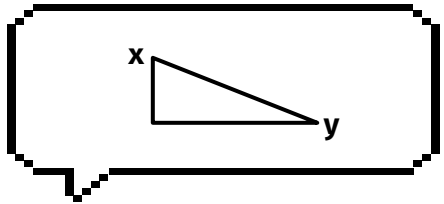
1. Ambil **Ciphertext** (Ct), dan **konversi** ke dalam bentuk angka
2. Ambil **Key** (K), dan **konversi** ke dalam bentuk angka
3. Pasangkan setiap huruf pada **Ct** dengan **K**, key dapat di-extend sesuai jumlah karakter **Ct,** jika **Ct** lebih panjang dari **K**
4. Operasikan **Ct** dan **K**, sesuai rumus dekripsi

Contoh Vigenere Cipher



Pt : OMEGA
Key : LUL

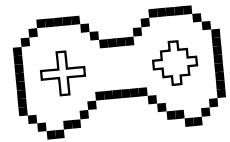
PT	O	M	E	G	A
n(PT)	14	12	4	6	0
n(K)	11	20	11	11	20
(n(PT) + n(K)) mod 26	25	6	15	17	20
CT	Z	G	P	R	U
n(CT)	25	6	15	17	20
n(K)	11	20	11	11	20
(n(CT) - n(K)) mod 26	14	12	4	6	0
PT	O	M	E	G	A



02

Autokey Cipher

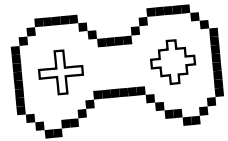
Autokey Cipher



Autokey Cipher merupakan pengembangan dari Shift dan Vigenere Cipher. **Pt** atau **Ct** dioperasikan menggunakan **Key** berupa text. Perbedaan terletak pada **cara extend Key**.

Contoh:
Pt : KRIPTO
Key : EZ
Hasil Extend Key menjadi, **EZKRIP**

Autokey Cipher



Enkripsi

E(x) = (x+K) mod 26

Dekripsi

D(x) = (x-K) mod 26

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

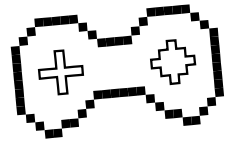
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Ket:

x = alfabet dalam angka (A-Z = 0-25)

K = kunci dalam angka (A-Z = 0-25)

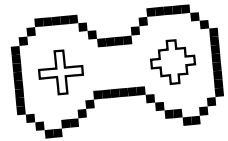
Contoh Autokey Cipher



Pt : ODADINGMANGOLEH, **Key :** IRONMAN

PT	O	D	A	D	I	N	G	M	A	N	G	O	L	E	H
n(PT)	14	3	0	3	8	13	6	12	0	13	6	14	11	4	7
K	I	R	O	N	M	A	N	O	D	A	D	I	N	G	M
n(K)	8	17	14	13	12	0	13	14	3	0	3	8	13	6	12
(n(PT) + n(K)) mod 26	22	20	14	16	20	13	19	0	3	13	9	22	24	10	19
CT	W	U	O	Q	U	N	T	A	D	N	J	W	Y	K	T
n(CT)	22	20	14	16	20	13	19	0	3	13	9	22	24	10	19
n(K)	8	17	14	13	12	0	13	14	3	0	3	8	13	6	12
(n(CT) - n(K)) mod 26	14	3	0	3	8	13	6	12	0	13	6	14	11	4	7
PT	O	D	A	D	I	N	G	M	A	N	G	O	L	E	H

Exercise

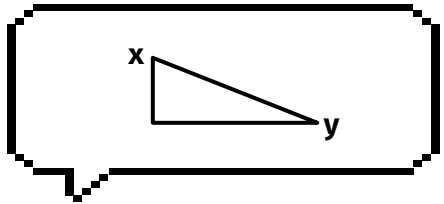


- Enkripsikan Plaintext **TAHUSUMEDANG**
- Gunakan Key **MAKANAJA**

Gunakan **Vigenere** dan **Autokey Cipher**!!

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

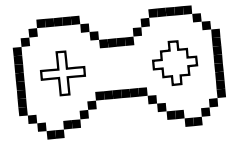
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25



03

Permutation / Transposition Cipher

Permutation/Transposition Cipher

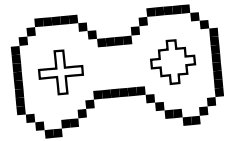


Permutation/Transposition Cipher merupakan sebuah teknik kriptografi klasik dimana dilakukan pengacakan karakter teks, dengan mengikuti suatu pola permutasi atau transposisi tertentu.

Beberapa Model Algoritma :

- **Columnar Transposition**
- **Triangle**
- **Route Cipher**
- **Diagonal**
- **Zig-Zag / Rail Fence Cipher**

Columnar Transposition Cipher



Enkripsi Columnar Transposition melibatkan penulisan **Plaintext (Pt)** berurutan dalam baris, dan kemudian membaca **Ciphertext (Ct)** dari setiap kolom sesuai dengan urutan derajat alfabetik kunci.

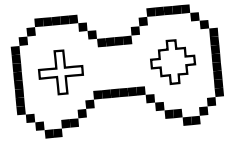
Enkripsi :
PT : ikan hiu makan tomat
K : ernec

Maka,
CT : _m_tihatn_naauamkiko

E	R	N	E	C
2	*5*	*4*	*3*	*1*
i	k	a	n	_
h	i	u	_	m
a	k	a	n	_
t	o	m	a	t

Alphabetic Order

Columnar Transposition Cipher



Dekripsi Columnar Transposition dilakukan dengan memasukkan **Ciphertext (Ct)** ke setiap kolom tabel dengan urutan alfabetik kunci & mencari **Plaintext (Pt)** dengan membaca baris dari atas ke bawah tabel.

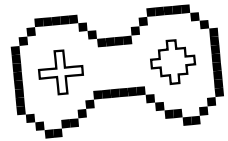
Dekripsi :
CT : _m_tihatn_naauamkiko
K : ernec

Maka,
PT : ikan hiu makan tomat

E	R	N	E	C
2	*5*	*4*	*3*	*1*
i	k	a	n	_
h	i	u	_	m
a	k	a	n	_
t	o	m	a	t

Alphabetic Order

Triangle Cipher



Enkripsi Triangle Cipher dilakukan dengan memasukkan **Plaintext (Pt)** ke baris (atas ke bawah) yang sudah ditentukan sedemikian rupa, hingga teks membentuk segitiga. **Ciphertext (Ct)** dibaca dengan urutan kolom, dari kiri ke kanan.

Enkripsi :
PT : ikan hiu makan tomat

Maka,
CT : tkxhaxkinxiautxnmoxamxaxx

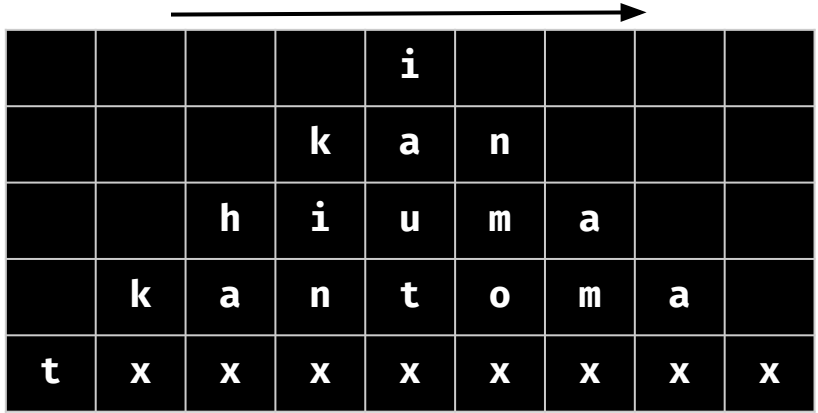
				i				
			k	a	n			
		h	i	u	m	a		
	k	a	n	t	o	m	a	
t	x	x	x	x	x	x	x	x

Triangle Cipher

Dekripsi Triangle Cipher dilakukan dengan memasukkan **Ciphertext (Ct)** ke kolom (kiri ke kanan) yang sudah ditentukan sedemikian rupa, hingga teks membentuk segitiga. **Plaintext (Pt)** dibaca dengan urutan baris, dari atas ke bawah.

Dekripsi :
CT : tkxhaxkinxiautxnmoxamxaxx

Maka,
PT : ikan hiu makan tomat

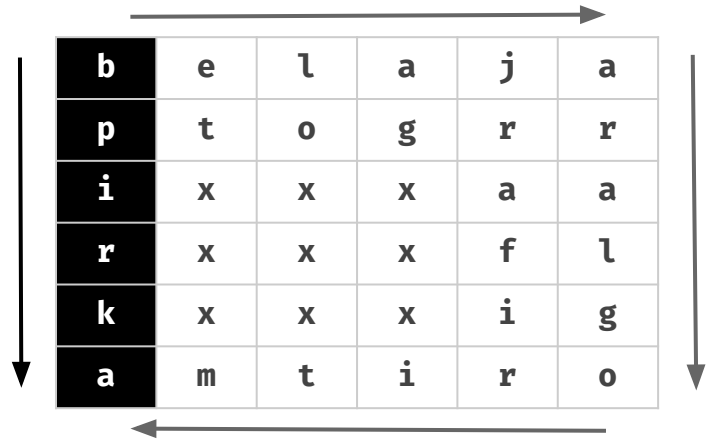


Route Cipher

Enkripsi Route Cipher dilakukan dengan memasukkan **Plaintext (Pt)** ke tabel dengan mengikuti pola yang ditentukan. **Ciphertext (Ct)** dibaca dengan acuan kolom dari kiri ke kanan.

Enkripsi :
PT : belajaralgoritmakriptografi
Pola : Spiral

Maka,
CT :
bpirkaetxxxmloxxxtagxxxijrafiraralgo



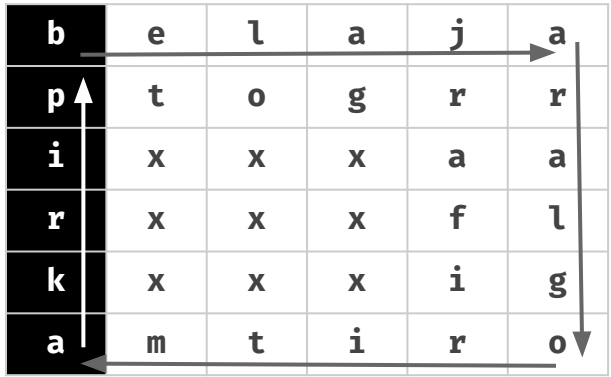
b	e	l	a	j	a
p	t	o	g	r	r
i	x	x	x	a	a
r	x	x	x	f	l
k	x	x	x	i	g
a	m	t	i	r	o

Route Cipher

Dekripsi Route Cipher dilakukan dengan memasukkan **Ciphertext (Ct)** ke tabel dengan acuan kolom dari kiri ke kanan. **Plaintext (Pt)** dibaca dengan mengikuti pola yang ditentukan.

Enkripsi :
**CT : **
bpirkaetxxxmloxxxtagxxxijrafiraralgo
Pola : Spiral

Maka,
**PT : **belajaralgoritmakriptografi

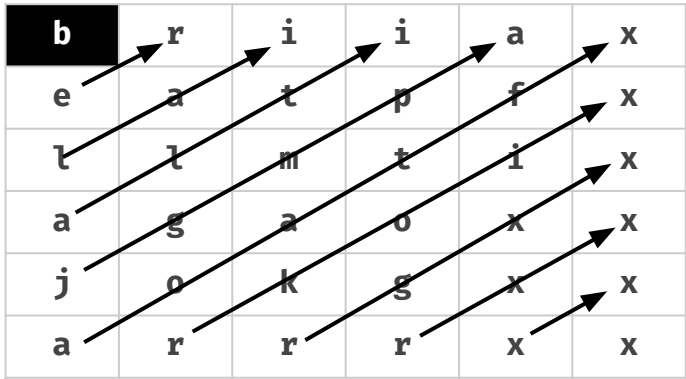


Diagonal Cipher

Enkripsi Diagonal Cipher dilakukan dengan memasukkan **Plaintext (Pt)** ke tabel dengan acuan kolom dari kiri ke kanan. **Ciphertext (Ct)** dibaca secara diagonal dari pojok tabel (kiri atau kanan sesuai dari model yang ditentukan).

Enkripsi :
PT : belajaralgoritmakriptografi
K : 6

Maka,
CT : berlaialtijgmpaaoatfxrkoixrxxxxx

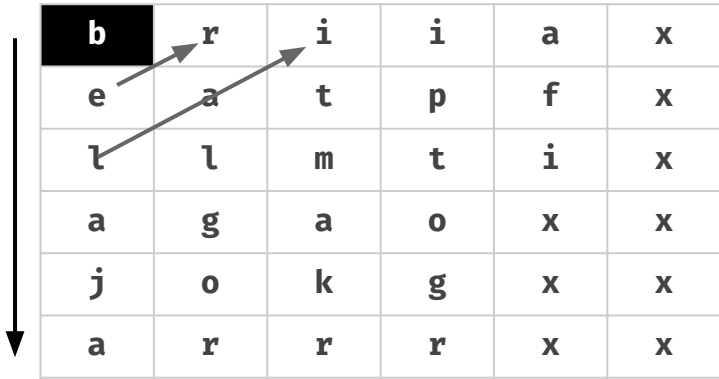


Diagonal Cipher

Dekripsi Diagonal Cipher dilakukan dengan memasukkan **Ciphertext (Ct)** ke tabel dengan mengikuti pola diagonal. **Plaintext (Pt)** dibaca secara mengikuti kolom atau baris sesuai pola yang ditentukan.

Dekripsi :
CT : berlaialtijgmpaaoatfxrkoixrxxxxx
K : 6

Maka,
PT : belajaralgoritmakriptografi



b	r	i	i	a	x
e	a	t	p	f	x
l	l	m	t	i	x
a	g	a	o	x	x
j	o	k	g	x	x
a	r	r	r	x	x

Rail Fence Cipher

Enkripsi Rail Fence Cipher dilakukan dengan memasukkan **Plaintext (Pt)** ke tabel secara zigzag, hingga membentuk pola pagar rel (rail fence). Bentuk selalu simetris, bergantung pada nilai offset. **Ciphertext (Ct)** dibaca dengan acuan baris dari atas ke bawah.

Enkripsi :

PT : belajaralgoritmakriptografi
K : 4 → Jumlah Baris
Offset : 3

Maka,
CT : agaoxljlomktgixeaartrprfxbriiax

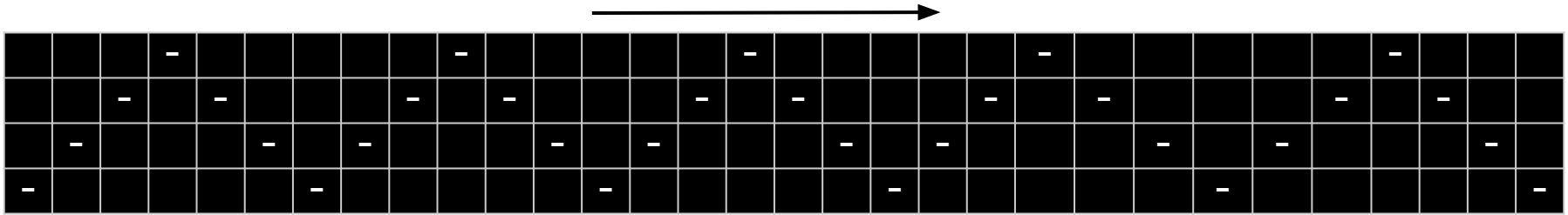
			a						g						a						o						x			
		l		j				l		o				m		k				t		g				i		x		
	e				a		a				r		t				r		p				r		f				x	
b						r						i						i						a						x

Rail Fence Cipher

Dekripsi Rail Fence Cipher dilakukan dengan membuat kerangka tabel, jumlah baris sebesar **K**. Lalu, isi **dash** pada tabel dimulai dari tempat **offset**. Ganti dash dengan karakter pada **Ciphertext (Ct)** dengan acuan kolom (dari atas ke bawah), **Plaintext (Pt)** dibaca dengan pola zigzag, dimulai dari offset.

Dekripsi :

CT : agaoxljlomktgixeaartrprfxbriiax
K : 4 → Jumlah Baris
Offset : 3



Rail Fence Cipher

Dekripsi :

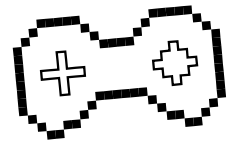
CT : agaoxljlomktgixeaartrprfxbriiax
K : 4 → Jumlah Baris
Offset : 3

Maka,
PT : belajaralgoritmakriptografi

			a						g						a						o						x			
		l		j				l		o				-		-				-		-				-		-		
	-				-		-				-		-				-		-				-		-				-	
-						-						-						-						-						-

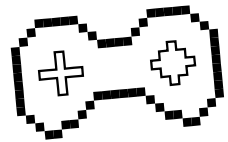
			a						g						a						o						x			
		l		j				l		o				m		k				t		g				i		x		
	e				a		a				r		t				r		p				r		f				x	
b						r						i						i						a						x

Tugas



1. Kumpulkan Exercise tadi di Classroom
2. Buat satu kalimat sederhana (min 3 kata & total min 15 huruf), enkripsikan dengan Vigenere dan Autokey Cipher dan kembalikan menjadi plainteks.
3. Untuk nomor 2, Gunakan **NAMA PANGGILAN KALIAN** sebagai **KEY.**
4. Buatlah program Vigenere Cipher (bahasa pemrograman bebas)
5. Exercise dan Soal Nomor 2 Format PDF
6. Buat 1 Repo GitHub, dengan nama **NPM-Kripto23** (untuk seluruh tugas program)
7. Source Code Program di push ke github masing-masing dan sertakan Screenshot pada (Folder)
8. **Note:** Untuk link repo GitHub jangan lupa attach di assignment Classroom!

Instruksi Tugas



Tugas Perhitungan Manual :

Format: Tugas5_NPM.pdf

Exercise :

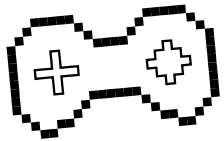
Format: Exercise5_NPM.pdf

Tugas Program :

Format Repo GitHub: NPM-Kripto23

Format Folder: Vigenere-Cipher, **Format File:** vigenerecipher.<ext>

Deadline Tugas: H-1 Praktikum Berikutnya, 23.59



Thank You!!

Kalau misalkan ada pertanyaan,
yaudah tanya aja

Praktikum Kriptografi 2022