

Nama : Zakiah Intan Maula

NIM : 2100015043

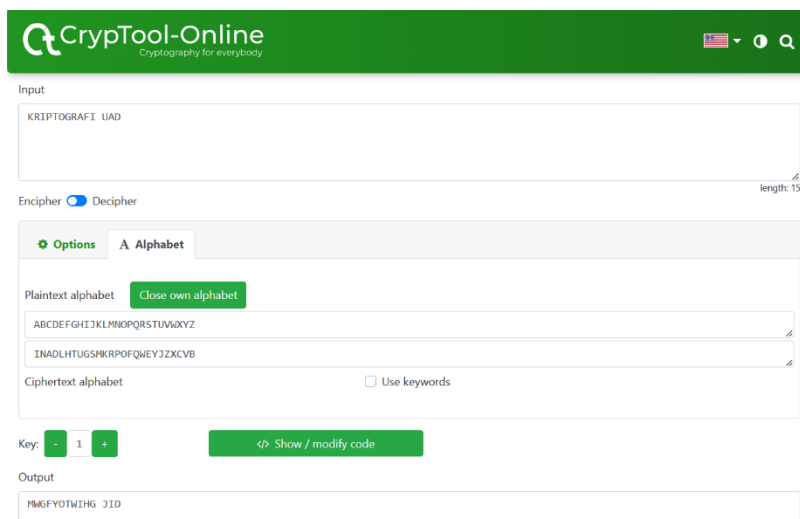
Tugas Kriptografi Pekan ke-4

Monoalphabetic Cipher

A. Deskripsi *Monoalphabetic Cipher*

Monoalphabetic Cipher adalah salah satu jenis *Classical Cipher* yang biasa digunakan dalam kriptografi. Jenis *cipher* ini merupakan salah satu bentuk *Substitution Cipher* yang mengganti satu-persatu huruf pada plainteks dengan huruf lain sesuai dengan kunci. Jumlah huruf pada kunci yang digunakan biasanya sebanyak 26, sesuai dengan banyak huruf alfabet. Tipe-tipe kunci pada *cipher* ini ada bermacam-macam, ada yang acak, berdasarkan kalimat tertentu, atau menggunakan suatu kata kunci. Namun, perlu diketahui bahwa huruf-huruf pada kolom kunci tidak boleh berulang karena akan menimbulkan kerancuan saat proses dekripsinya nanti. Dalam penerapannya, *cipher* ini sangat rentan untuk diretas karena hanya mengubah huruf sesuai kuncinya saja. Ketika ada seseorang yang berhasil menemukan kuncinya, maka akan dia akan dengan mudah meretas *ciphertext* yang sudah ada.

B. Penggunaan di *Cryptool*



The screenshot shows the Cryptool-Online web interface. At the top, there's a green header with the logo and text "Cryptool-Online Cryptography for everybody". Below the header, there's an "Input" section with a text area containing "KRIPTOGRAFI UAD" and a "length: 15" indicator. Below the input, there's a toggle for "Encipher" (checked) and "Decipher". Underneath, there's an "Options" section with a tab for "A Alphabet". In this section, there are two text areas for "Plaintext alphabet" and "Ciphertext alphabet". The "Plaintext alphabet" contains "ABCDEFGHIJKLMNOPQRSTUVWXYZ" and the "Ciphertext alphabet" contains "INADLHTUGSMKRPQFQWEYJZXCVB". There's a checkbox for "Use keywords" which is unchecked. Below the alphabets, there's a "Key" section with a value of "1" and a "Show / modify code" button. At the bottom, there's an "Output" section with a text area containing "PM6FYOTWING JID".

CrypTool-Online
Cryptography for everybody

Input
MNGFYOTWIZING JID

Encipher ☒ Decipher

Options A Alphabet

Plaintext alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

INADLHTUGSMKRPOFQWEYJZXCVB

Ciphertext alphabet ☐ Use keywords

Key:

Output
KRIPTOGRAFI UAD

C. Algoritma

1. Membaca inputan atau plainteks

Contoh :

K R I P T O G R A F I U A D

2. Mengganti huruf-huruf pada plainteks sesuai dengan kunci yang diberikan (enkripsi)

Contoh :

Kunci

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

Sehingga,

K R I P T O G R A F I U A D
M W G F Y O T W I H G J I D

3. Mengganti huruf-huruf pada cipherteks sesuai dengan kunci yang telah diinverskan (dekripsi)

Contoh :

Kunci invers

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

Sehingga,

M	W	G	F	Y	O	T	W	I	H	G		J	I	D
K	R	I	P	T	O	G	R	A	F	I		U	A	D

D. Kesimpulan

Penggunaan *monoalphabetic cipher* ini mirip dengan *substitution cipher* atau hanya menggantikan huruf pada plainteks dengan huruf pada key yang digunakan.