

Nama : Vernandika Stanley Hansen
NPM : 140810220031
Praktikum Kriptografi

Exercise 2

1. Exercise Shift Cipher

- Enkripsikan HASKELL dengan $K = 20$
 - Ubah ETURF menjadi Plaintext dengan $K = 12$
- Tulis setiap langkah langkahnya !

2. Exercise ROT 13

Dekripsikan cenxgvxhz xevcgbtensv dengan ROT 13

Jawab:

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

1.

- $K = 20$

HASKELL = 7 0 18 10 4 11 11

Enkripsi

$$E(7) = (7 + 20) \bmod 26 = 27 \bmod 26 = 1 \Rightarrow B$$

$$E(0) = (0 + 20) \bmod 26 = 20 \bmod 26 = 20 \Rightarrow U$$

$$E(18) = (18 + 20) \bmod 26 = 38 \bmod 26 = 12 \Rightarrow M$$

$$E(10) = (10 + 20) \bmod 26 = 30 \bmod 26 = 4 \Rightarrow E$$

$$E(4) = (4 + 20) \bmod 26 = 24 \bmod 26 = 24 \Rightarrow Y$$

$$E(11) = (11 + 20) \bmod 26 = 31 \bmod 26 = 5 \Rightarrow F$$

$$E(11) = (11 + 20) \bmod 26 = 31 \bmod 26 = 5 \Rightarrow F$$

HASKELL $\Rightarrow E(x) \Rightarrow BUMEYFF$

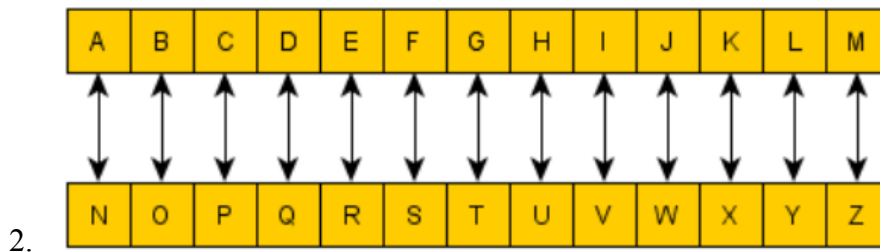
- $K = 12$

ETURF = 4 19 20 17 5

Deskripsi

$D(4) = (4 - 12 + 26) \bmod 26 = 18 \bmod 26 = 18 \Rightarrow S$
 $D(19) = (19 - 12 + 26) \bmod 26 = 33 \bmod 26 = 7 \Rightarrow H$
 $D(20) = (20 - 12 + 26) \bmod 26 = 34 \bmod 26 = 8 \Rightarrow I$
 $D(17) = (17 - 12 + 26) \bmod 26 = 31 \bmod 26 = 5 \Rightarrow F$
 $D(5) = (5 - 12 + 26) \bmod 26 = 19 \bmod 26 = 19 \Rightarrow T$

ETURF $\Rightarrow D(x) \Rightarrow$ SHIFT



$C \Rightarrow P$
 $E \Rightarrow R$
 $N \Rightarrow A$
 $X \Rightarrow K$
 $G \Rightarrow T$
 $V \Rightarrow I$
 $X \Rightarrow K$
 $H \Rightarrow U$
 $Z \Rightarrow M$

$X \Rightarrow K$
 $E \Rightarrow R$
 $V \Rightarrow I$
 $C \Rightarrow P$
 $G \Rightarrow T$
 $B \Rightarrow O$
 $T \Rightarrow G$
 $E \Rightarrow R$
 $N \Rightarrow A$
 $S \Rightarrow F$
 $V \Rightarrow I$

cenxgvxhz xevcgbtensv \Rightarrow praktikum kriptografi