

Nama: Aliya Sania

NPM: 1408102110035

Latihan 2

Praktikum Kriptografi

Exercise Shift Cipher

- Enkripsikan HASKELL dengan $K = 20$
- Ubah ETURF menjadi Plaintext dengan $K = 12$

Jawab:

H A S K E L L
7 0 18 10 4 11 11

Enkripsi

$$E(x) = (x+K) \bmod 26$$

$E(7)$	$= (7+20) \bmod 26$	$= 27 \bmod 26$	$= 1$	$\rightarrow B$
$E(0)$	$= (0+20) \bmod 26$	$= 20 \bmod 26$	$= 20$	$\rightarrow U$
$E(18)$	$= (18+20) \bmod 26$	$= 38 \bmod 26$	$= 12$	$\rightarrow M$
$E(10)$	$= (10+20) \bmod 26$	$= 30 \bmod 26$	$= 4$	$\rightarrow E$
$E(4)$	$= (4+20) \bmod 26$	$= 24 \bmod 26$	$= 24$	$\rightarrow Y$
$E(11)$	$= (11+20) \bmod 26$	$= 31 \bmod 26$	$= 5$	$\rightarrow F$
$E(11)$	$= (11+20) \bmod 26$	$= 31 \bmod 26$	$= 5$	$\rightarrow F$

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

E T U R F
4 19 20 17 5

Dekripsi

$$D(x) = (x-K) \bmod 26$$

$E(4)$	$= (4-12) \bmod 26$	$= -8 \bmod 26$	$= 18$	$\rightarrow S$
$E(19)$	$= (19-12) \bmod 26$	$= 7 \bmod 26$	$= 7$	$\rightarrow H$
$E(20)$	$= (20-12) \bmod 26$	$= 8 \bmod 26$	$= 8$	$\rightarrow I$
$E(17)$	$= (17-12) \bmod 26$	$= 5 \bmod 26$	$= 5$	$\rightarrow F$
$E(5)$	$= (5-12) \bmod 26$	$= -7 \bmod 26$	$= 19$	$\rightarrow T$

ETURF $\rightarrow E(x) \rightarrow$ SHIFT

Exercise ROT 13

Dekripsikan **cenxgvxhz xevcgbtensv** dengan ROT 13

JAWAB:

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

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