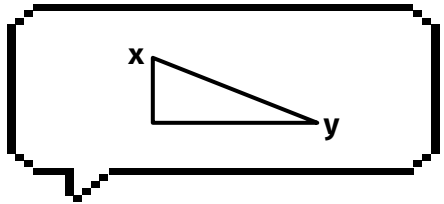
Kriptografi

Pertemuan - 02

Topik: Shift Cipher, ROT 13, Affine Cipher

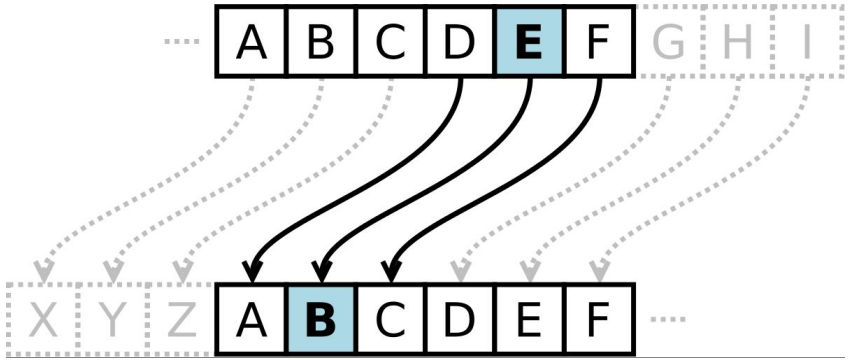


01

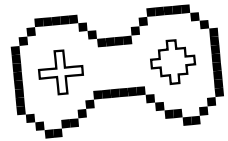
Shift Cipher

Shift Cipher

Shift Cipher atau disebut juga Caesar Cipher merupakan teknik enkripsi berbasis substitusi.



Shift 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

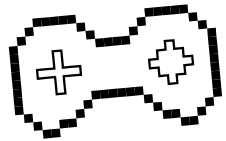
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Ket:

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

K = kunci

Shift Cipher



K = 30

WADUH = 22 0 3 20 7

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

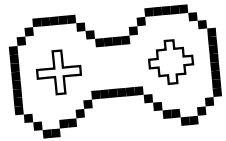
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Enkripsi

E(22) = (22 + 30) mod 26 = 52 mod 26 = 0 ⇒ **A**
E(0) = (0 + 30) mod 26 = 30 mod 26 = 4 ⇒ **E**
E(3) = (3 + 30) mod 26 = 33 mod 26 = 7 ⇒ **H**
E(20) = (20 + 30) mod 26 = 50 mod 26 = 24 ⇒ **Y**
E(7) = (7 + 30) mod 26 = 37 mod 26 = 11 ⇒ **L**

WADUH ⇒ E(x) ⇒ AEHYL

Shift 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

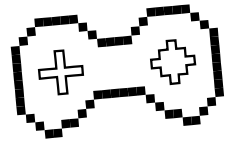
Dekripsi

AEHYL = 0 4 7 24 11

AEHYL ⇒ D(x) ⇒ **WADUH**

But how?

Exercise Shift Cipher

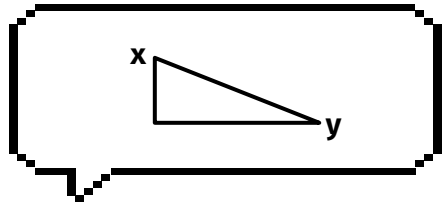


- Enkripsikan **HASKELL** dengan K = 20
- Ubah **ETURF** menjadi Plaintext dengan K = 12

  Tulis setiap langkah langkahnya !

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



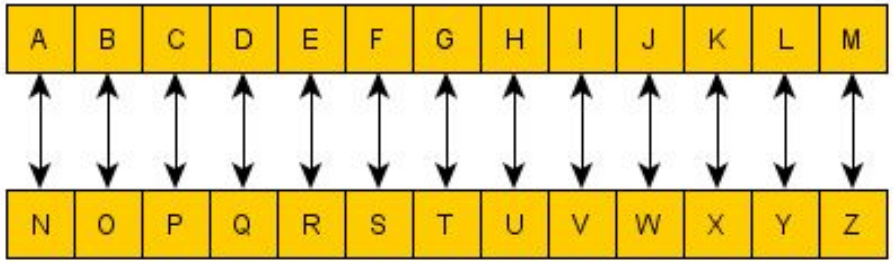
02

ROT 13

ROT 13

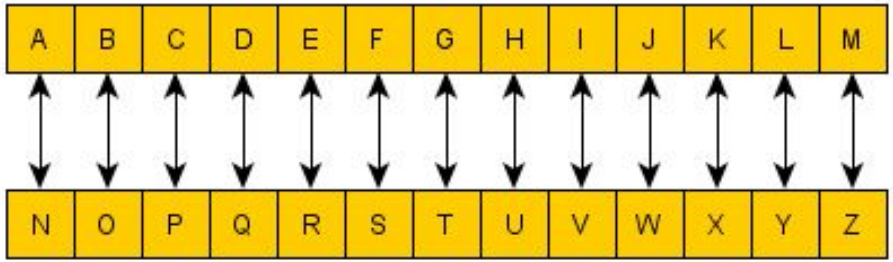
ROT 13 merupakan algoritma enkripsi sederhana yang menggunakan sandi abjad tunggal dengan pergeseran K=13.

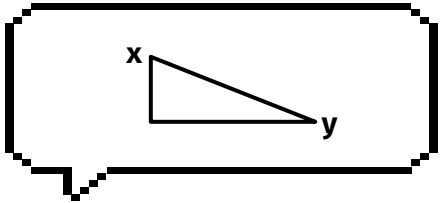
Sehingga huruf A diganti dengan N, B menjadi O.



Exercise

Dekripsikan **cenxgvxhz xevcgbtensv** dengan ROT 13

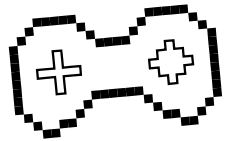




03

Affine cipher

Affine Cipher

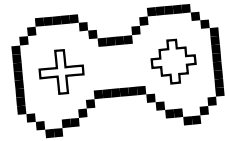


Affine Cipher merupakan perluasan dari metode Shift/Caesar Cipher. Dimana dalam Affine cipher kita akan mengalikan plainteks (P) dengan sebuah nilai a dan menambahkannya dengan nilai b.

$$E(x) = (\mathbf{a}x + \mathbf{b}) \bmod 26$$

$$D(y) = \mathbf{a}^{-1} (y - \mathbf{b}) \bmod 26$$

Affine Cipher



Enkripsikan kata PUNTEN menggunakan Affine Cipher dengan nilai a=7 b=10

PUNTEN ⇒ 15 20 13 19 4 13

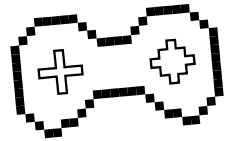
E(15) = (7(15) + 10) mod 26 = 115 mod 26 = 11 ⇒ L
E(20) = (7(20) + 10) mod 26 = 150 mod 26 = 20 ⇒ U
E(13) = (7(13) + 10) mod 26 = 101 mod 26 = 23 ⇒ X
E(19) = (7(19) + 10) mod 26 = 143 mod 26 = 13 ⇒ N
E(4) = (7(4) + 10) mod 26 = 38 mod 26 = 12 ⇒ M
E(13) = (7(13) + 10) mod 26 = 101 mod 26 = 23 ⇒ X

PUNTEN ⇒ E(x) ⇒ LUXNMX

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

Affine Cipher



Dekripsi

Mencari a-1:

GCD(a, m)

gcd (7, 26)

26 = 7 * **3** + 5

7 = 5 * **1** + 2

5 = 2 * **2** + 1

2 = **1** * 2 + 0

t0 = 0, t1 = 1

t2 = (t0 - (q1 . t1)) mod 26

= (0 - (**3** . 1)) mod 26 = -3 mod 26 = 23

t3 = (t1 - (q2 . t2)) mod 26

= (1 - (**1** . 23)) mod 26 = -22 mod 26 = 4

t4 = (t2 - (q3 . t3)) mod 26

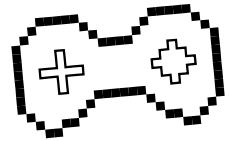
= (23 - (**2** . 4)) mod 26 = 15 mod 26 = 15

a-1 = **15**

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

Affine Cipher



D(11) = **15**(11 - 10) mod 26 = 15 mod 26 =15 ⇒ P

D(20) = **15**(20 - 10) mod 26 = 150 mod 26 = 20 ⇒ U

D(23) = **15**(23 - 10) mod 26 = 195 mod 26 = 13 ⇒ N

D(13) = **15**(13 - 10) mod 26 = 45 mod 26 = 19 ⇒ T

D(12) = **15**(12 - 10) mod 26 = 30 mod 26 = 4 ⇒ E

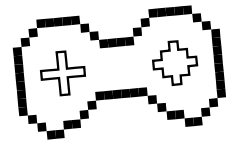
D(23) = **15**(23 - 10) mod 26 = 195 mod 26 = 13 ⇒ N

LUXNMX ⇒ D(y) ⇒ PUNTEN

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

Tugas

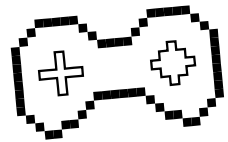


1. Kumpulkan Exercise tadi di Classroom.
2. Enkripsikan nama lengkap anda menggunakan Affine Cipher dan kembalikan menjadi plainteks, **a=9 b=[2 digit NPM akhir].**
3. Buat repositori publik Github dengan format nama

   “[2 digit terakhir NPM]-Kripto23”
4. Buatlah program Shift Cipher dengan bahasa pemrograman bebas.

* nanti setiap kode program di pertemuan selanjutnya akan disimpan di repositori tersebut

Instruksi Tugas



Tugas Perhitungan Manual :

Format: Tugas2_NPM.pdf

Exercise :

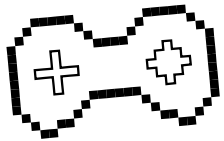
Format: Exercise2_NPM.pdf

Tugas Program :

Nama Folder: Shift-Cipher, **Format File:** shiftcipher.[ext]

* dikumpulin di classroom : 2 file PDF dan 1 attachment link ke github kalian

Deadline : H-1 Praktikum Berikutnya, 23.59



Thank You!!

Kalau misalkan ada pertanyaan,
yaudah tanya aja

Praktikum Kriptografi 2022