PRAKTIKUM KRIPTOGRAFI

TUGAS 4

Nama : Novem Romadhofi Kika

NPM : 140810220083

Kelas : A

UNIVERSITAS PADJAJARAN

Fakultas Matematika Dan Ilmu Pengetahuan Alam

Program Studi S-1 Teknik Informatika

2024

2. Buat satu kalimat sederhana (min 3 kata & total min 15 huruf), enkripsikan dengan Vigenere dan Autokey Cipher dan kembalikan menjadi plainteks.

Plainteks = HIDUP ADALAH PERJUANGAN
Key = Novem
A. Vigenere
Enkripsi

H	I	D	U	P	A	D	A	L	A	H	P	E	R	J	U	A	N	G	A	N
7	8	3	20	15	0	3	0	11	0	7	15	4	17	9	20	0	13	6	0	13

N	O	V	E	M
13	14	21	4	12

E(7) = (7 + 13) mod 26 = 20 => U
E(8) = (8 + 14) mod 26 = 22 => W
E(3) = (3 + 21) mod 26 = 0 => A
E(20) = (20 + 4) mod 26 = 24 => Y
E(15) = (15 + 12) mod 26 = 1 => B
E(0) = (0 + 13) mod 26 = 13 => N
E(3) = (3 + 14) mod 26 = 17 => R
E(0) = (0 + 21) mod 26 = 21 => V
E(11) = (11 + 4) mod 26 = 15 => P
E(0) = (0 + 12) mod 26 = 12 => M
E(7) = (7 + 13) mod 26 = 20 => U
E(15) = (15 + 14) mod 26 = 3 => D
E(4) = (4 + 21) mod 26 = 25 => Z
E(17) = (17 + 4) mod 26 = 21 => V
E(9) = (9 + 12) mod 26 = 21 => V
E(20) = (20 + 13) mod 26 = 7 => H
E(0) = (0 + 14) mod 26 = 14 => O
E(13) = (13 + 21) mod 26 = 8 => I
E(6) = (6 + 4) mod 26 = 10 => K
E(0) = (0 + 12) mod 26 = 12 => M
E(13) = (13 + 13) mod 26 = 26 => D
Hasil enkripsi : UWAYBNRVPUM DZVVHOKMD

Deskripsi
Cipherteks: UWAYBNRVPUMDZVVHOKMD
Kunci: NOVEM

U	W	A	Y	B	N	R	V	P	U	M	D	Z	V	V	H	O	K	M	D
20	22	0	24	1	13	17	21	15	12	20	3	25	21	21	7	0	13	6	0

N	O	V	E	M
13	14	21	4	12

D(0) = (20 - 13) mod 26 = 7 => H
D(1) = (22 - 14) mod 26 = 8 => I
D(2) = (0 - 21) mod 26 = 3 => D
D(3) = (24 - 4) mod 26 = 20 => U
D(4) = (1 - 12) mod 26 = 15 => P
D(5) = (13 - 13) mod 26 = 0 => A
D(6) = (17 - 14) mod 26 = 3 => D
D(7) = (21 - 21) mod 26 = 0 => A
D(8) = (15 - 4) mod 26 = 11 => L
D(9) = (12 - 12) mod 26 = 0 => A
D(10) = (20 - 13) mod 26 = 7 => H
D(11) = (3 - 14) mod 26 = 15 => P
D(12) = (25 - 21) mod 26 = 4 => E
D(13) = (21 - 4) mod 26 = 17 => R
D(14) = (21 - 12) mod 26 = 9 => J
D(15) = (7 - 13) mod 26 = 20 => U
D(16) = (0 - 14) mod 26 = 0 => N
D(17) = (13 - 21) mod 26 = 6 => G
D(18) = (6 - 4) mod 26 = 6 => G
D(19) = (0 - 12) mod 26 = 0 => A
D(16) = (0 - 14) mod 26 = 0 => N
Hasil Deskripsi : HIDUPADALAHPERJUANGAN

B. Autokey Cipher
Enkripsi

H	I	D	U	P	A	D	A	L	A	H	P	E	R	J	U	A	N	G	A	N
7	8	3	20	15	0	3	0	11	0	7	15	4	17	9	20	0	13	6	0	13

N	O	V	E	M
13	14	21	4	12

E(7) = (7 + 13) mod 26 = 20 => U
E(8) = (8 + 14) mod 26 = 22 => W
E(3) = (3 + 21) mod 26 = 0 => A

E(20) = (20 + 4) mod 26 = 24 => Y
E(15) = (15 + 12) mod 26 = 1 => B
E(0) = (0 + 7) mod 26 = 7 => H
E(3) = (3 + 8) mod 26 = 11 => L
E(0) = (0 + 3) mod 26 = 3 => D
E(11) = (11 + 20) mod 26 = 5 => F
E(0) = (0 + 15) mod 26 = 15 => P
E(7) = (7 + 0) mod 26 = 7 => H
E(15) = (15 + 3) mod 26 = 18 => S
E(4) = (4 + 0) mod 26 = 4 => E
E(17) = (17 + 11) mod 26 = 2 => C
E(9) = (9 + 0) mod 26 = 9 => J
E(20) = (20 + 7) mod 26 = 3 => D
E(0) = (0 + 15) mod 26 = 15 => P
E(13) = (13 + 4) mod 26 = 17 => R
E(6) = (6 + 17) mod 26 = 23 => X
E(0) = (0 + 9) mod 26 = 9 => J
Hasil Enkripsi : UWAYBHLDPHSECJPRXJ

Deskripsi
Cipherteks: UWAYBHLDPHSECJPRXJ
Kunci: NOVEM

U	W	A	Y	B	H	L	D	P	H	S	E	C	R	P	R	X	J
20	22	0	24	1	3	5	18	4	2	9	3	15	17	23	9	0	13

N	O	V	E	M
13	14	21	4	12

D(0) = (20 - 13) mod 26 = 7 => H
D(1) = (22 - 14) mod 26 = 8 => I
D(2) = (0 - 21) mod 26 = 3 => D
D(3) = (24 - 4) mod 26 = 20 => U
D(4) = (1 - 12) mod 26 = 15 => P
D(5) = (7 - 7) mod 26 = 0 => A
D(6) = (11 - 8) mod 26 = 3 => D
D(7) = (3 - 3) mod 26 = 0 => A
D(8) = (5 - 20) mod 26 = 11 => L
D(9) = (15 - 15) mod 26 = 0 => A
D(10) = (7 - 0) mod 26 = 7 => H
D(11) = (18 - 3) mod 26 = 15 => P
D(12) = (4 - 0) mod 26 = 4 => E

D(13) = (2 - 11) mod 26 = 17 => R
D(14) = (9 - 0) mod 26 = 9 => J
D(15) = (3 - 7) mod 26 = 20 => U
D(16) = (0 - 0) mod 26 = 0 => A
D(17) = (17 - 11) mod 26 = 0 => N
D(18) = (23 - 0) mod 26 = 6 => G
D(19) = (9 - 15) mod 26 = 0 => A
Hasil Deskripsi : HIDUPADALAHPERJUANGAN

4. Buatlah program Vigenere Cipher (bahasa pemrograman bebas)

Program :

```
"""
Nama  : Novem Romadhofi Kika
Npm   : 140810220083
Kelas : A
Deskrpsi : Vegenere Cipher
"""

def generate_key(text, key):
    key = list(key)
    if len(text) == len(key):
        return key
    else:
        for i in range(len(text) - len(key)):
            key.append(key[i % len(key)])
    return "".join(key)

def encrypt_vigenere(plaintext, key):
    ciphertext = []
    for i in range(len(plaintext)):
        char = (ord(plaintext[i]) + ord(key[i])) % 26
        char += ord('A')
        ciphertext.append(chr(char))
    return "".join(ciphertext)

def decrypt_vigenere(ciphertext, key):
    plaintext = []
    for i in range(len(ciphertext)):
        char = (ord(ciphertext[i]) - ord(key[i]) + 26) % 26
```

```
            char += ord('A')
            plaintext.append(chr(char))
    return "".join(plaintext)

if __name__ == "__main__":
    plaintext = input("Masukkan plaintext: ").upper().replace(" ", "")
    key = input("Masukkan kunci: ").upper().replace(" ", "")

    generated_key = generate_key(plaintext, key)
    print(f"Kunci yang digunakan: {generated_key}")

    ciphertext = encrypt_vigenere(plaintext, generated_key)
    print(f"Ciphertext: {ciphertext}")

    decrypted_text = decrypt_vigenere(ciphertext, generated_key)
    print(f"Hasil dekripsi: {decrypted_text}")
```

Hasil running program :

```
PS C:\Semester 5> & C:/pyhton/python.exe "c:/Semester 5/Praktikum Kriptografi/Vigenere-Cipher/vigenerecipher.py"
Masukkan plaintext: HIDUPADALAHPERJUANGAN
Masukkan kunci: NOVEM
Kunci yang digunakan: NOVEMNOVEMNOVEMNOVEMN
Ciphertext: UWYYBNRVPMUDZVVHOIKMA
Hasil dekripsi: HIDUPADALAHPERJUANGAN
```