Kriptografi Terapan

Demonstrasi Program Sederhana Menggunakan Algoritma Viginere Cipher

Oleh : PBL RKS-301

Kode Pemrograman

>>>

```python
from string import ascii_uppercase as up

class Enkripsivigenere:
    def padding(self, plain, key):
        panjangPlain = len(plain)
        keyPadding = key * panjangPlain
        return keyPadding[:panjangPlain]

    def encrypt(self, plain, key, table):
        padding = self.padding(plain, key)
        plainToIndex = [table[0].find(z) for z in plain.upper()]
        keyToIndex = [up.find(i) for i in padding.upper()]

        cipherText = ""
        indexNumber = 0
        for i in keyToIndex:
            for p in range(i, i + 1):
                cipherText += table[int(p)][plainToIndex[indexNumber]]
            indexNumber += 1
        return cipherText
```

Kode Pemrograman

>>>

```python
from string import ascii_uppercase as up

class Decryptvigenere:
    def padding(self, text, key):
        panjang_text = len(text)
        keyPadding = key * panjang_text
        return keyPadding[:panjang_text]

    def decrypt(self, cipher, key, table):
        padding = self.padding(cipher, key)
        cipherToIndex = [up.find(z) for z in cipher.upper()]
        keyToIndex = [up.find(i) for i in padding.upper()]

        plainText = ""
        for i, c_index in enumerate(cipherToIndex):
            row = table[keyToIndex[i]]
            plainText += up[row.find(up[c_index])]

        return plainText
```

Kode Pemrograman

>>>

```python
from encrypt import Enkripsivigenere
from decrypt import Decryptvigenere
from string import ascii_uppercase as up

class VigenereTable:
    def __init__(self) -> None:
        self.table = []
        for i in range(len(up)):
            self.table.append(up[i:] + up[:i])

    def generateTable(self):
        return self.table

# Buat objek untuk enkripsi, dekripsi, dan tabel
vigenere_table = VigenereTable()
vigenere_encrypt = Enkripsivigenere()
vigenere_decrypt = Decryptvigenere()

# Tampilkan tabel Vigenere
print("Tabel Vigenere:")
for row in vigenere_table.generateTable():
    print(" ".join(row))

# Input dari pengguna
plain_text = input("\nMasukkan plaintext: ")
key = input("Masukkan key: ")
```

Kode Pemrograman

>>>

```
28    # Enkripsi
29    cipher_text = vigenere_encrypt.encrypt(plain_text, key, vigenere_table.generateTable())
30    print("\nHasil enkripsi: ", cipher_text)
31
32    # Dekripsi
33    decrypted_text = vigenere_decrypt.decrypt(cipher_text, key, vigenere_table.generateTable())
34    print("Hasil dekripsi: ", decrypted_text)
```

Pertanyaan

1. Apakah Viginere Cipher termasuk Kriptografi Klasik atau Modern? jelaskan!

2. Jelaskan algoritma Viginere Cipher

1

Blaise de Vigenere
1586

Vigenère Cipher termasuk kriptogafi klasik karena menggunakan teknik yang disebut **substitusi polialfabetik**, di mana setiap huruf dalam pesan diganti dengan huruf lain berdasarkan kata kunci yang digunakan.

Ini berbeda dengan teknik modern, yang menggunakan rumus matematika yang sangat rumit dan biasanya memerlukan komputer untuk melakukan enkripsi.

2

Menggunakan Tabel Subtitusi

Tabel subtitusi digunakan untuk mengganti atau menginisiasikan huruf abjad A-Z kedalam angka 0-25.

>>>

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P

16	17	18	19	20	21	22	23	24	25
Q	R	S	T	U	V	W	X	Y	Z

Contoh Encrypt :

plaintext : saya suka rks
key : vigenere
rumus encrypt : Ci (Pi + Ki) mod 26

Plaintext	**S**	**A**	**Y**	**A**	**S**	**U**	**K**	**A**	**R**	**K**	**S**
Konversi	18	0	24	0	18	20	10	0	17	10	18

Key	**V**	**I**	**G**	**E**	**N**	**E**	**R**	**E**	**V**	**I**	**G**
Konversi	21	8	6	4	13	4	17	4	21	8	6

Contoh Encrypt :

plaintext : saya suka rks
key : vigenere
rumus encrypt : Ci (Pi + Ki) mod 26

Hasil perhitungan Konversi	**39**	**8**	**30**	**4**	**31**	**24**	**27**	**4**	**38**	**18**	**24**

mod 26	**13**	**8**	**4**	**4**	**5**	**24**	**1**	**4**	**12**	**18**	**24**
Ciphertext	**N**	**I**	**E**	**E**	**F**	**Y**	**B**	**E**	**M**	**S**	**Y**

Contoh Decrypt :

Ciphertext : NIEEFYBEMSY
key : vigenere
rumus decrypt : Pi (Ci - Ki) mod 26

Ciphertext	**N**	**I**	**E**	**E**	**F**	**Y**	**B**	**E**	**M**	**S**	**Y**
Konversi	13	8	4	4	5	24	1	4	12	18	24

Key	**V**	**I**	**G**	**E**	**N**	**E**	**R**	**E**	**V**	**I**	**G**
Konversi	21	8	6	4	13	4	17	4	21	8	6

Contoh Decrypt :

Ciphertext : NIEEFYBEMSY
key : vigenere
rumus decrypt : Pi (Ci - Ki) mod 26

Hasil pengurangan Konversi	**-8**	**0**	**-2**	**0**	**-8**	**20**	**-16**	**0**	**-9**	**10**	**18**

mod 26	**18**	**0**	**24**	**0**	**18**	**20**	**10**	**0**	**17**	**10**	**18**
Plaintext	**S**	**A**	**Y**	**A**	**S**	**U**	**K**	**A**	**R**	**K**	**S**

Menggunakan Tabel Tabula Recta

>>>

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

Plaintext : HALO
Key : AYAM
Ciphertext : HYLA

Terima Kasih