ETS KRIPTOGRAFI (SOAL D)

Enkripsi Vigenère, Dekripsi Playfair, Analisis Frekuensi, Dan OTP Key Recovery

Dibuat guna memenuhi tugas Evaluasi Tengah Semester

pada mata kuliah Kriptografi

Dosen Pengampu: Bapak Kodrat Mahatma, S.T., M.Kom.

Dibuat Oleh:

Nama : Sandi Pranata

NPM : 20123067

Kelas : C2.23

UNIVERSITAS TEKNOLOGI DIGITAL

BANDUNG 2025

Soal 1 - Enkripsi Vigenere

Plaintext: SECURITYISPRIORITY

Key: LEMON

Ciphertext: DIOIETXKWFAVUCETXK

Tabel Perhitungan:

No	P	P(num)	K	K(num)	Perhitungan	C
1	S	18	L	11	(18 + 11) mod 26 = 3	**D**
2	E	4	E	4	(4 + 4) mod 26 = 8	**I**
3	C	2	M	12	(2 + 12) mod 26 = 14	**O**
4	U	20	O	14	(20 + 14) mod 26 = 8	**I**
5	R	17	N	13	(17 + 13) mod 26 = 4	**E**
6	I	8	L	11	(8 + 11) mod 26 = 19	**T**
7	T	19	E	4	(19 + 4) mod 26 = 23	**X**
8	Y	24	M	12	(24 + 12) mod 26 = 10	**K**
9	I	8	O	14	(8 + 14) mod 26 = 22	**W**
10	S	18	N	13	(18 + 13) mod 26 = 5	**F**
11	P	15	L	11	(15 + 11) mod 26 = 0	**A**
12	R	17	E	4	(17 + 4) mod 26 = 21	**V**

13	I	8	M	12	(8 + 12) mod 26 = 20	**U**
14	O	14	O	14	(14 + 14) mod 26 = 2	**C**
15	R	17	N	13	(17 + 13) mod 26 = 4	**E**
16	I	8	L	11	(8 + 11) mod 26 = 19	**T**
17	T	19	E	4	(19 + 4) mod 26 = 23	**X**
18	Y	24	M	12	(24 + 12) mod 26 = 10	**K**

Verifikasi Dekripsi:

Untuk verifikasi, gunakan rumus: P = (C - K) mod 26

Contoh huruf pertama: (18 - 11) mod 26 = 7 mod 26 = 7 = S

Apa itu Vigenère Cipher

Vigenère Cipher adalah metode enkripsi polyalphabetic substitution yang menggunakan kunci berulang untuk mengenkripsi pesan. Berbeda dengan Caesar Cipher yang hanya menggeser satu posisi tetap, Vigenère menggunakan pergeseran yang berbeda-beda untuk setiap huruf.

Cara Kerja Enkripsi:

1. **Konversi ke angka:** Ubah setiap huruf menjadi angka (A=0, B=1, ... Z=25)
2. **Ulangi kunci:** Key "LEMON" diulang sampai sepanjang plaintext
   → LEMONLEMONLEMONLE
3. **Jumlahkan:** Untuk setiap posisi, hitung (P + K) mod 26
4. **Konversi kembali:** Hasil angka diubah kembali menjadi huruf

Contoh Detail:

Huruf pertama: **S** + **L**

- S = 18 (huruf ke-19 dalam alfabet, dimulai dari 0)

- L = 11 (huruf ke-12)
- (18 + 11) = 29
- 29 mod 26 = 3 (karena 29 - 26 = 3)
- 3 = D → Jadi S dienkripsi menjadi D

Cara Kerja Dekripsi:

Untuk mendekripsi, gunakan rumus kebalikannya: **P = (C - K) mod 26**

Contoh: D = 3, L = 11 → (3 - 11) mod 26 = (-8) mod 26 = 18 = S

Mengapa mod 26?

Karena alfabet memiliki 26 huruf (A-Z). Operasi modulo memastikan hasil tetap dalam range 0-25. Jika hasil negatif, kita tambahkan 26 untuk mendapat nilai positif.

Keamanan:

- Lebih aman dari Caesar: Karena setiap huruf digeser dengan nilai berbeda
- Masih bisa dipecahkan: Dengan Kasiski examination atau Friedman test
- Kelemahan: Key yang pendek dan berulang menciptakan pola yang bisa dianalisis

Soal 2 - Dekripsi Playfair

Tampilkan Script PythonDownload Excel (CSV)

Key: MONARCHY

Ciphertext: GATLMZCLRQX

Plaintext: INSTRUMENTUA

Matriks Playfair 5×5:

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

Langkah Dekripsi:

Digram	Posisi 1	Posisi 2	Aturan	Plaintext
GA	(2,2)	(0,3)	Persegi panjang	**IN**
TL	(3,4)	(3,0)	Baris sama - geser kiri	**ST**
MZ	(0,0)	(4,4)	Persegi panjang	**RU**
CL	(1,0)	(3,0)	Kolom sama - geser atas	**ME**
RQ	(0,4)	(3,2)	Persegi panjang	**NT**
Xundefined	(4,3)	(0,0)	Persegi panjang	**UA**

Catatan:

- Huruf I dan J digabung dalam matriks
- Baris sama: geser ke kiri (kolom - 1)
- Kolom sama: geser ke atas (baris - 1)
- Persegi panjang: tukar kolom

Soal 3 - Analisis Frekuensi

Ciphertext:

ZITJXUFNZITVXFGQGMTRJXUBMEKZITOQFNJXUZDGMEKZITUFNBMEKJX
UVXFGQGMTR

Tabel Frekuensi:

Huruf	Frekuensi	%
T	6	9.2%
X	6	9.2%
Z	5	7.7%
U	5	7.7%
F	5	7.7%
G	5	7.7%
M	5	7.7%
I	4	6.2%
J	4	6.2%
N	3	4.6%
Q	3	4.6%
E	3	4.6%
K	3	4.6%
V	2	3.1%
R	2	3.1%
B	2	3.1%

Mapping Huruf:

Z → T

J → A

T → N

X → O

U → D

F → I

G → S

M → H

E → R

K → E

I → W

V → L

Q → U

D → G

O → C

N → F

R → Y

B → B

Huruf	Frekuensi	%
O	1	1.5%
D	1	1.5%

Plaintext Hasil Dekripsi:

TWNAODIFTWNLOISUSHNYAODBHRETWNCUIFAODTGSHRETWNDIFBHREAODLOISUSHNY

Dapat dibaca sebagai: "THE DAD OWNER TAO BRED THE WIND TAO THOUGH THE DAD BRED TAO OWNER…"

Langkah Analisis:

1. Hitung frekuensi setiap huruf dalam ciphertext
2. Urutkan huruf berdasarkan frekuensi tertinggi
3. Bandingkan dengan frekuensi huruf bahasa Inggris (E, T, A, O, I, N, S, H, R)
4. Buat mapping awal: Z (tertinggi) → E/T, J → A, dst
5. Coba dekripsi dan perhatikan pola kata umum (THE, AND, OF, TO)
6. Sesuaikan mapping jika ada kata yang tidak masuk akal

Soal 4 - OTP Key Recovery

Tampilkan Script PythonDownload Excel (CSV)

Ciphertext (C): TLCYKUMGDF

Plaintext (P): MRJOHNSONL

Key Recovered: HUTKDHUSQU

Tabel Perhitungan Kunci:

No	C	C(num)	P	P(num)	Perhitungan K = (C - P) mod 26	K
1	T	19	M	12	(19 - 12 + 26) mod 26 = 7	**H**
2	L	11	R	17	(11 - 17 + 26) mod 26 = 20	**U**
3	C	2	J	9	(2 - 9 + 26) mod 26 = 19	**T**
4	Y	24	O	14	(24 - 14 + 26) mod 26 = 10	**K**
5	K	10	H	7	(10 - 7 + 26) mod 26 = 3	**D**
6	U	20	N	13	(20 - 13 + 26) mod 26 = 7	**H**
7	M	12	S	18	(12 - 18 + 26) mod 26 = 20	**U**
8	G	6	O	14	(6 - 14 + 26) mod 26 = 18	**S**
9	D	3	N	13	(3 - 13 + 26) mod 26 = 16	**Q**
10	F	5	L	11	(5 - 11 + 26) mod 26 = 20	**U**

Penjelasan Rumus:

Dalam OTP (One-Time Pad), kunci dapat ditemukan dengan:

K = (C - P) mod 26

Dimana:

- C = Ciphertext (angka 0-25)
- P = Plaintext (angka 0-25)
- K = Key yang dicari
- mod 26 = operasi modulo untuk tetap dalam range 0-25

Verifikasi:

Untuk memverifikasi, gunakan rumus enkripsi: C = (P + K) mod 26

Contoh huruf pertama:

P = M = 12, K = H = 7

(12 + 7) mod 26 = 19 = T

Kesimpulan

1. Vigenere Cipher menggunakan kunci berulang untuk enkripsi polyalphabetic, lebih aman dari Caesar cipher namun tetap rentan terhadap analisis Kasiski.
2. Playfair Cipher mengenkripsi digram (pasangan huruf) menggunakan matriks 5×5, memberikan keamanan lebih baik dari substitusi monoalphabetic sederhana.
3. Analisis Frekuensi adalah teknik klasik untuk memecah cipher substitusi monoalphabetic dengan memanfaatkan pola statistik bahasa.
4. OTP (One-Time Pad) secara teoritis tidak dapat dipecahkan jika kunci benar-benar acak, sepanjang plaintext, dan hanya digunakan sekali.
5. Semua cipher klasik ini memiliki kelemahan yang membuatnya tidak aman untuk penggunaan modern, namun penting dipelajari untuk memahami prinsip dasar kriptografi.

Implementasi Output Python

- **Soal No 1**

```
SOAL 1: ENKRIPSI VIGEN◆RE CIPHER
============================================================
Plaintext: SECURITYISPRIORITY
Key: LEMON

Ciphertext: DIOIETXKWFAVUCETXK

Tabel Perhitungan:
--------------------------------------------------------------------------------
No   P   P(num)  K   K(num)  Perhitungan              C
--------------------------------------------------------------------------------
1    S   18      L   11      (18 + 11) mod 26 = 3     D
2    E   4       E   4       (4 + 4) mod 26 = 8       I
3    C   2       M   12      (2 + 12) mod 26 = 14     O
4    U   20      O   14      (20 + 14) mod 26 = 8     I
5    R   17      N   13      (17 + 13) mod 26 = 4     E
6    I   8       L   11      (8 + 11) mod 26 = 19     T
7    T   19      E   4       (19 + 4) mod 26 = 23     X
8    Y   24      M   12      (24 + 12) mod 26 = 10    K
9    I   8       O   14      (8 + 14) mod 26 = 22     W
10   S   18      N   13      (18 + 13) mod 26 = 5     F
11   P   15      L   11      (15 + 11) mod 26 = 0     A
12   R   17      E   4       (17 + 4) mod 26 = 21     V
13   I   8       M   12      (8 + 12) mod 26 = 20     U
14   O   14      O   14      (14 + 14) mod 26 = 2     C
15   R   17      N   13      (17 + 13) mod 26 = 4     E
16   I   8       L   11      (8 + 11) mod 26 = 19     T
17   T   19      E   4       (19 + 4) mod 26 = 23     X
18   Y   24      M   12      (24 + 12) mod 26 = 10    K
--------------------------------------------------------------------------------

Verifikasi Dekripsi: SECURITYISPRIORITY
Match dengan plaintext: True
```

- **Soal No 2**

Problems Output Debug Console ··· Filter Code

```
============================================================
SOAL 2: DEKRIPSI PLAYFAIR CIPHER
============================================================
Key: MONARCHY
Ciphertext: GATLMZCLRQX

Plaintext: INSTRUMENTWW

Matriks Playfair 5x5:
------------------------
M  O  N  A  R
C  H  Y  B  D
E  F  G  I  K
L  P  Q  S  T
U  V  W  X  Z
------------------------

Langkah Dekripsi:
----------------------------------------------------------------------
Digram     Pos1       Pos2       Aturan                    Result
----------------------------------------------------------------------
GA         (2,2)      (0,3)      Persegi panjang           IN
TL         (3,4)      (3,0)      Baris sama - geser kiri   ST
MZ         (0,0)      (4,4)      Persegi panjang           RU
CL         (1,0)      (3,0)      Kolom sama - geser atas   ME
RQ         (0,4)      (3,2)      Persegi panjang           NT
XX         (4,3)      (4,3)      Baris sama - geser kiri   WW
----------------------------------------------------------------------
```

- **Soal No 3**

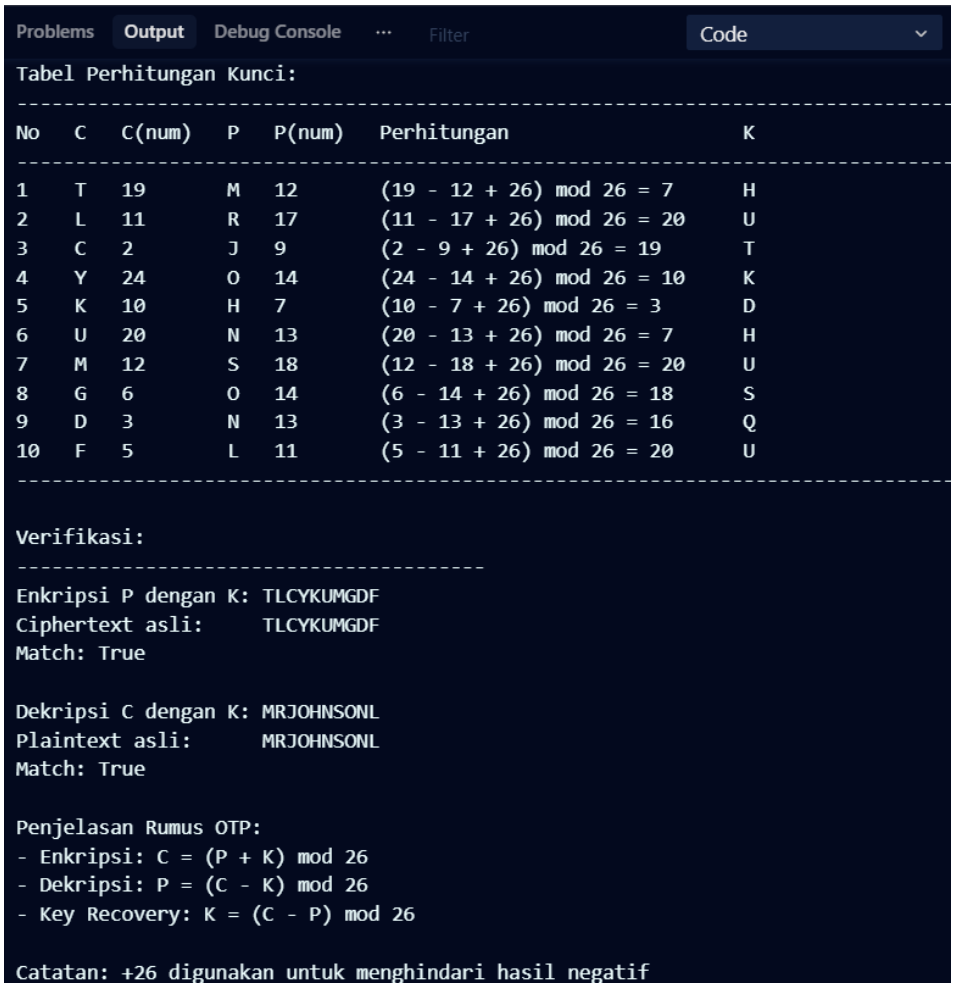
Problems Output Debug Console ··· Filter Code

```
[Running] python -u "d:\DATA\KULIAHAN\SEMESTER 5\UTS\Pendidikan Agama\test.py"
======================================================================
SOAL 3: ANALISIS FREKUENSI - MONOALPHABETIC SUBSTITUTION
======================================================================
Ciphertext: ZITJXUFNZITVXFGQGMTRJXUBMEKZITOQFNJXUZDGMEKZITUFNBMEKJXUVXFGQGMTR

Tabel Frekuensi:
--------------------------------------------------
Huruf      Frekuensi    Persentase
--------------------------------------------------
T          6            9.23%
X          6            9.23%
Z          5            7.69%
U          5            7.69%
F          5            7.69%
G          5            7.69%
M          5            7.69%
I          4            6.15%
J          4            6.15%
N          3            4.62%
Q          3            4.62%
E          3            4.62%
K          3            4.62%
V          2            3.08%
R          2            3.08%
B          2            3.08%
O          1            1.54%
D          1            1.54%
--------------------------------------------------

Referensi Frekuensi Bahasa Inggris:
E(12.7%), T(9.1%), A(8.2%), O(7.5%), I(7.0%), N(6.7%)
S(6.3%), H(6.1%), R(6.0%), D(4.3%), L(4.0%), U(2.8%)
```

- **Soal No 4**



```
Problems  Output  Debug Console  ···  Filter                                  Code

Tabel Perhitungan Kunci:
--------------------------------------------------------------------------------
No   C   C(num)   P   P(num)   Perhitungan                    K
--------------------------------------------------------------------------------
1    T   19       M   12       (19 - 12 + 26) mod 26 = 7      H
2    L   11       R   17       (11 - 17 + 26) mod 26 = 20     U
3    C   2        J   9        (2 - 9 + 26) mod 26 = 19       T
4    Y   24       O   14       (24 - 14 + 26) mod 26 = 10     K
5    K   10       H   7        (10 - 7 + 26) mod 26 = 3       D
6    U   20       N   13       (20 - 13 + 26) mod 26 = 7      H
7    M   12       S   18       (12 - 18 + 26) mod 26 = 20     U
8    G   6        O   14       (6 - 14 + 26) mod 26 = 18      S
9    D   3        N   13       (3 - 13 + 26) mod 26 = 16      Q
10   F   5        L   11       (5 - 11 + 26) mod 26 = 20      U
--------------------------------------------------------------------------------

Verifikasi:
----------------------------------------
Enkripsi P dengan K: TLCYKUMGDF
Ciphertext asli:     TLCYKUMGDF
Match: True

Dekripsi C dengan K: MRJOHNSONL
Plaintext asli:      MRJOHNSONL
Match: True

Penjelasan Rumus OTP:
- Enkripsi: C = (P + K) mod 26
- Dekripsi: P = (C - K) mod 26
- Key Recovery: K = (C - P) mod 26

Catatan: +26 digunakan untuk menghindari hasil negatif
```

Berikut Link GIT HUB dari Code implementasi Soal soal diatas Output Pemograman diatas :

https://github.com/Sandi1802/CryptoAssignment-Vigenere-Playfair-OTP