LAPORAN Tugas 1: CIPHER KLASIK

Nama	:	Desi Ramadani
NPM	:	20123042
Kelas	:	C1. 23 Informatika Universitas Teknologi Digital
Mata Kuliah	:	Kriptografi
Dosen Pengampu	:	Kodrat Mahatma S.T.,M.Kom

A. Caesar Cipher

1. Teori

Program ini mengenkripsi teks dengan menggeser huruf sebesar nilai shift yang dimasukkan pengguna. Fungsi caesar_encrypt() dan caesar_decrypt() memakai rumus (ord(ch) - 65 ± shift) % 26 + 65, lalu mengubah semua huruf ke uppercase. Karakter non-alfabet tidak diubah.

2. Input-Output

```
=== Caesar Cipher ===
Pilih mode (E = Enkripsi, D = Dekripsi): E
Masukkan nilai shift: 3
Masukkan plaintext: DESIRAMADANI
Ciphertext: GHVLUDPDGDQL
```

```
=== Caesar Cipher ===
Pilih mode (E = Enkripsi, D = Dekripsi): D
Masukkan nilai shift: 3
Masukkan ciphertext: GHVLUDPDGDQL
Plaintext: DESIRAMADANI
```

Penjelasan:

Program pertama-tama mengenkripsi teks DESIRAMADANI dengan pergeseran 3 huruf sehingga menghasilkan ciphertext GHVLUDPDGDQL. Saat mode dekripsi dijalankan dengan shift yang sama, teks tersebut dikembalikan ke bentuk aslinya DESIRAMADANI. Ini menunjukkan bahwa fungsi enkripsi dan dekripsi pada kode berjalan sesuai logika pergeseran huruf Caesar Cipher.

3. Analisis Kelemahan

Meskipun program dapat mengenkripsi dan mendekripsi teks dengan benar, algoritma Caesar Cipher pada kode ini memiliki beberapa kelemahan. Salah satunya, nilai shift yang digunakan sebagai kunci sangat terbatas, hanya 25 kemungkinan, sehingga ciphertext mudah dipecahkan dengan mencoba semua pergeseran (brute force).

B. Affine Cipher

1. Teori Singkat

Program ini menggunakan algoritma Affine Cipher, yaitu setiap huruf pada plaintext diganti dengan rumus (a * (ord(ch) - 65) + b) % 26 + 65, di mana a dan b adalah kunci. Nilai a harus koprima dengan 26 agar proses dekripsi bisa dilakukan menggunakan invers modulo. Semua huruf diubah ke uppercase, dan karakter non-huruf tidak diubah.

2. Input-Output

```
=== Affine Cipher ===
Pilih mode (E = Enkripsi, D = Dekripsi): E
Masukkan nilai a (harus koprima dengan 26): 5
Masukkan nilai b: 8
Masukkan plaintext: DESIRAMADANI
Ciphertext: XCUWPIQIXIVW
```

```
=== Affine Cipher ===
Pilih mode (E = Enkripsi, D = Dekripsi): D
Masukkan nilai a (harus koprima dengan 26): 5
Masukkan nilai b: 8
Masukkan ciphertext: XCUWPIQIXIVW
Plaintext: DESIRAMADANI
```

Penjelasan:

Program mengenkripsi teks DESIRAMADANI dengan a = 5 dan b = 8 menjadi ciphertext XCUWPIQIXIVW, lalu berhasil mendekripsinya kembali ke bentuk asli menggunakan kunci yang sama.

3. Analisis Kelemahan

Affine Cipher pada program ini masih lemah karena ruang kunci terbatas (hanya 312 kombinasi), sehingga mudah dipecahkan dengan brute-force. Huruf yang sama di plaintext selalu menghasilkan huruf yang sama di ciphertext, membuatnya rentan terhadap analisis frekuensi. Selain itu, karakter non-huruf tidak diubah sehingga pola teks masih bisa dikenali.

C. Playfair Cipher

1. Teori

Playfair Cipher adalah algoritma sandi klasik yang bekerja dengan cara mengenkripsi pasangan huruf (digraf) menggunakan tabel 5x5 yang dibentuk dari kata kunci (key). Huruf "J" digabungkan dengan "I" agar tabel berisi 25 huruf. Proses enkripsi dilakukan dengan mengganti posisi huruf sesuai aturan pada tabel, sedangkan dekripsi dilakukan dengan langkah kebalikannya..

2. Input-Output

```
=== Playfair Cipher ===
Pilih mode (E = Enkripsi, D = Dekripsi): E
Masukkan key: CANTIK
Masukkan plaintext: DESIRAMADANI
Ciphertext: EFUTQNHTBNTC
```

```
=== Playfair Cipher ===
Pilih mode (E = Enkripsi, D = Dekripsi): D
Masukkan key: CANTIK
Masukkan ciphertext: EFUTQNHTBNTC
Plaintext: DESIRAMADANI
```

Penjelasan:

Pada program dijalankan dengan memilih mode E (Enkripsi), key yang dimasukkan yaitu CANTIK, dan plaintext DESIRAMADANI, maka menghasilkan ciphertext EFUTQNHTBNTC. Selanjutnya ketika mode D (Dekripsi) dipilih dengan ciphertext yang sama, hasilnya kembali menjadi plaintext DESIRAMADANI.

3. Analisis Kelemahan

Kelemahan Playfair Cipher terletak pada kemudahannya untuk dianalisis menggunakan analisis frekuensi pasangan huruf (digraph analysis). Selain itu, algoritma ini hanya menggunakan huruf alfabet tanpa angka atau simbol, sehingga pola huruf masih mudah dikenali. Ruang kunci yang kecil juga membuat algoritma ini rentan terhadap serangan brute force dengan teknologi modern.

D. Hill Cipher

1. Teori

Hill Cipher adalah algoritma kriptografi klasik yang menggunakan konsep aljabar linear untuk mengenkripsi teks. Setiap huruf diubah menjadi angka (A=0, B=1, dst), lalu dikelompokkan menjadi blok sesuai ukuran matriks kunci. Proses enkripsi dilakukan dengan perkalian matriks antara blok plaintext dan matriks kunci, sedangkan dekripsi dilakukan dengan menggunakan invers dari matriks kunci modulo 26.

2. Input-Output

```
=== Hill Cipher ===
Pilih mode (E = Enkripsi, D = Dekripsi): E
Masukkan plaintext: DESIRAMADANI
Ciphertext: VAAYZIKYJGLO
```

```
=== Hill Cipher ===
Pilih mode (E = Enkripsi, D = Dekripsi): D
Masukkan ciphertext: VAAYZIKYJGLO
Plaintext: DESIRAMADANI
```

Penjelasan:

Program dijalankan dengan memilih mode E (Enkripsi), lalu memasukkan plaintext DESIRAMADANI. Dengan kunci matriks [[3,3],[2,5]], hasil enkripsi menghasilkan

ciphertext VAAYZIKYJGLO. Saat mode D (Dekripsi) digunakan dengan ciphertext yang sama, program mengembalikan plaintext DESIRAMADANI.

3. Analisis Kelemahan

Kelemahan Hill Cipher terletak pada ketergantungannya terhadap invers matriks kunci. Jika determinan matriks tidak memiliki invers modulo 26, maka dekripsi tidak dapat dilakukan. Selain itu, Hill Cipher juga rentan terhadap known-plaintext attack, karena jika penyerang mengetahui beberapa pasangan plaintext dan ciphertext, matriks kunci dapat dihitung dengan mudah menggunakan persamaan linear.

E. Vigenere Cipher

1. Teori

Vigenere Cipher adalah algoritma kriptografi klasik berbasis substitusi polialfabetik, di mana setiap huruf pada plaintext dienkripsi menggunakan pergeseran huruf yang ditentukan oleh huruf pada key. Pergeseran tersebut diulang sesuai panjang key sehingga menghasilkan variasi enkripsi yang lebih kuat dibanding Caesar Cipher.

2. Input-Output

```
=== Vigenere Cipher ===
Pilih mode (E = Enkripsi, D = Dekripsi): E
Masukkan key: CANTIK
Masukkan plaintext: DESIRAMADANI
Ciphertext: FEFBZKOAQTVS
```

```
=== Vigenere Cipher ===
Pilih mode (E = Enkripsi, D = Dekripsi): D
Masukkan key: CANTIK
Masukkan ciphertext: FEFBZKOAQTVS
Plaintext: DESIRAMADANI
```

Penjelasan:

Program dijalankan dengan memilih mode E (Enkripsi) dan memasukkan key CANTIK. Saat plaintext DESIRAMADANI dienkripsi, diperoleh ciphertext FEFBZKOAQTVS. Sebaliknya, ketika mode D (Dekripsi) digunakan dengan ciphertext tersebut, hasilnya kembali menjadi plaintext DESIRAMADANI.

3. Analisis Kelemahan

Meskipun lebih kuat dari Caesar Cipher, Vigenere Cipher tetap memiliki kelemahan karena pola pengulangan kunci. Jika panjang key lebih pendek dari pesan, pola pergeseran akan berulang sehingga dapat dianalisis menggunakan metode seperti Kasiski Examination atau Frequency Analysis. Hal ini membuat algoritma Vigenere tidak aman terhadap serangan kriptanalisis modern.

F. Kesimpulan

Dari hasil analisis, dapat disimpulkan bahwa Caesar Cipher memiliki keamanan paling lemah karena hanya bergantung pada satu nilai pergeseran tetap, sedangkan Affine Cipher sedikit lebih baik namun tetap mudah dipecahkan. Playfair Cipher lebih kuat karena mengenkripsi pasangan huruf, tetapi masih rentan terhadap analisis frekuensi. Hill Cipher menawarkan keamanan lebih tinggi melalui operasi matriks dan aljabar linear, sementara Vigenere Cipher juga cukup kuat berkat kunci polialfabetik yang membuat pola enkripsi lebih sulit ditebak.

Secara keseluruhan, algoritma yang paling direkomendasikan adalah Hill Cipher dan Vigenere Cipher karena memiliki struktur enkripsi yang lebih kompleks, meskipun untuk keamanan modern tetap disarankan menggunakan algoritma seperti AES.

G. Lampiran

Link Github:
https://github.com/desiramadani-2004/Tugas1_CipherKlasik.git