NAMA : HISYAM MOHAMAD ALAM
NIM : 1203210069

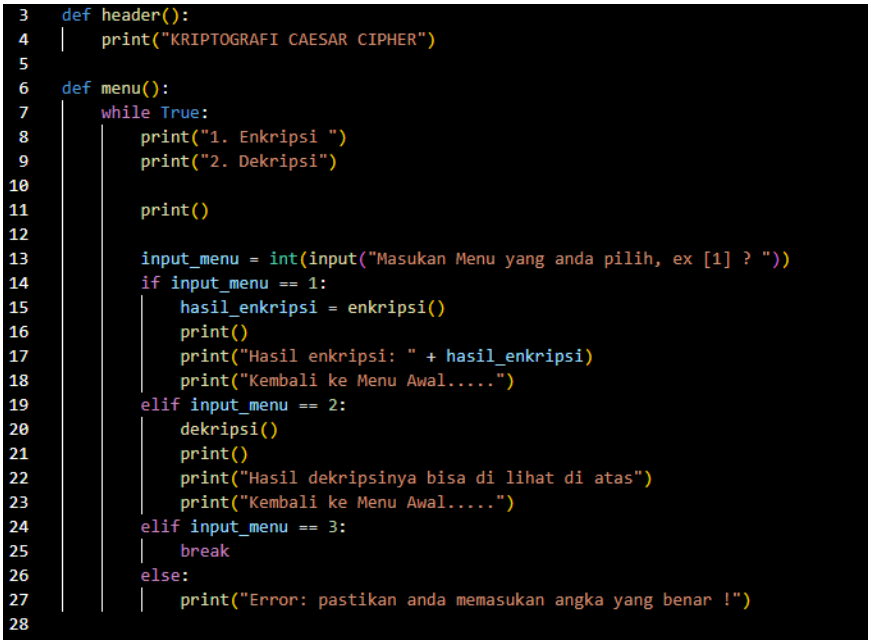
KEAMANAN INFORMASI DAN JARINGAN

DENGAN KRIPTOGRAFI CAESAR CHIPER

Kriptografi :
(cryptography) berasal dari bahasa yunani, kryptos berarti tersembunyi dan graphein berarti tulisan, adalah seni dan ilmu membuat komunikasi tidak dapat dipahami oleh semua orang kecuali penerima yang dituju . Kriptografi adalah seni mengirim pesan yang diubah sehingga hanya bisa dipahami oleh penerimanya Kriptografi dilakukan dengan mengubah pesan asli menjadi kode dengan aturan tertentu, sehingga pesan asli hanya dapat diterima oleh penerima pesan yang memahami aturan tertentu tersebut. Kriptografi mencakup teknik seperti microdots, menggabungkan kata-kata dengan gambar, dan cara lain untuk menyembunyikan informasi dalam penyimpanan . Kriptografi bisa dilakukan dengan beberapa cara berbeda antara lain menggunakan ciphers, codes, dan subtitusi, sehingga hanya orang yang berwenang yang bisa melihat dan menafsirkan pesan sebenarnya dengan benar . Kriptografi merupakan salah satu cara praktis untuk melindungi informasi yang dikirimkan melalui jaringan komunikasi publik, seperti saluran telepon, gelombang mikro, atau satelit . Tujuan kriptografi adalah untuk memperoleh integritas (keutuhan), kerahasiaan dan keaslian semua sumber informasi . Kriptografi tidak hanya melindungi data dari pencurian ataupun pengubahan (alternation) pesan tapi juga dapat digunakan untuk menautentikasi pengguna . Terdapat beberapa istilah yang dipakai dalam kriptografi, diantaranya yaitu: kode disebut ciphers, informasi yang disembunyikan disebut plaintext, setelah informasi diubah ke bentuk rahasia, pesan yang dikirim disebut ciphertext. Proses perubahan dari plaintext ke ciphertext disebut enkripsi (encrypting), sedangkan proses sebaliknya perubahan dari ciphertext kembali ke plaintext disebut dekripsi (decrypting) .

Caesar chiper
Caesar chiper adalah salah satu teknik enkripsi yang paling sederhana dan paling dikenal. Caesar Cipher adalah algoritma yang digunakan oleh sistem kriptografi simetri dan digunakan jauh sebelum sistem kriptografi public key ditemukan, kriptografi klasik yang ada dan beberapa bentuk algoritma klasik dianggap optimal karena mudah dipecahkan . Caesar chiper merupakan jenis cipher substitusi di mana setiap huruf dalam plaintext digantikan oleh sebuah huruf dengan beberapa posisi tetap di bawah alfabet . Teknik ini juga dikenal sebagai single cipher alphabet . Caesar chiper pertama kali digunakan oleh Julius Caesar. Caesar mengkodekan informasi dengan menggubah setiap huruf dalam informasi menjadi tiga huruf di setelah informasi asli dalam urutan alfabet . Algoritma kriptografi Caesar Cipher sangat mudah digunakan. Inti dari algoritma kriptografi ini menggeser semua karakter dalam plaintext dengan nilai pergeseran yang sama

Contoh Implementasi Caesar Chiper :



```
def header():
    print("KRIPTOGRAFI CAESAR CIPHER")

def menu():
    while True:
        print("1. Enkripsi ")
        print("2. Dekripsi")

        print()

        input_menu = int(input("Masukan Menu yang anda pilih, ex [1] ? "))
        if input_menu == 1:
            hasil_enkripsi = enkripsi()
            print()
            print("Hasil enkripsi: " + hasil_enkripsi)
            print("Kembali ke Menu Awal.....")
        elif input_menu == 2:
            dekripsi()
            print()
            print("Hasil dekripsinya bisa di lihat di atas")
            print("Kembali ke Menu Awal.....")
        elif input_menu == 3:
            break
        else:
            print("Error: pastikan anda memasukan angka yang benar !")

```

def menu(): Ini adalah definisi dari fungsi menu(). Fungsi ini digunakan untuk menampilkan menu kepada pengguna dan mengelola pilihan mereka.

while True: Loop tak terbatas dimulai di sini, yang berarti menu akan ditampilkan berulang-ulang sampai pengguna memilih untuk keluar (dalam kasus ini, dengan memilih opsi 3).

Pilihan menu ditampilkan kepada pengguna menggunakan print(). Terdapat dua opsi menu:

1. Enkripsi: Ini adalah opsi untuk melakukan enkripsi.

2. Dekripsi: Ini adalah opsi untuk melakukan dekripsi.

input_menu = int(input("Masukan Menu yang anda pilih, ex [1] ? ")): Program meminta pengguna untuk memasukkan nomor menu yang mereka inginkan.

Kode di bawahnya memeriksa nilai yang dimasukkan oleh pengguna dan berperilaku sebagai berikut:

Jika pengguna memilih 1 (Enkripsi), maka fungsi enkripsi() dipanggil untuk melakukan enkripsi pesan. Hasil enkripsi dicetak ke layar.

Jika pengguna memilih 2 (Dekripsi), maka fungsi dekripsi() dipanggil untuk melakukan dekripsi pesan.

Jika pengguna memilih 3, program keluar dari loop while dengan break dan berhenti.

Jika pengguna memasukkan nomor yang tidak valid, program mencetak pesan kesalahan.

Setelah enkripsi atau dekripsi selesai, program mencetak pesan "Kembali ke Menu Awal....." untuk memberi tahu pengguna bahwa mereka dapat memilih menu lagi.

```python
def enkripsi():
    input_text = str(input("Masukan Text yang akan anda enkripsi, ex [lindo] ? "))
    input_key = int(input("Masukan key/shift yang akan anda pakai, ex [number] ? "))
    result = ""
    #transfer ke teks biasa
    for i in range(len(input_text)):
        char = input_text[i]
    # Enkripsi karakter huruf  dalam teks biasa

        if char.isupper():
            result += chr((ord(char) + input_key - 65) % 26 + 65)
        # Enkripsi karakter huruf kecil dalam teks biasa
        elif char == " ":
            result += " "
        else:
            result += chr((ord(char) + input_key - 97) % 26 + 97)

    return result
```

input_text = str(input("Masukan Text yang akan anda enkripsi, ex [lindo] ? ")): Program meminta pengguna untuk memasukkan teks yang akan dienkripsi.

input_key = int(input("Masukan key/shift yang akan anda pakai, ex [number] ? ")): Program meminta pengguna untuk memasukkan jumlah pergeseran karakter (kunci) yang akan digunakan dalam enkripsi. Ini adalah angka yang menentukan sejauh berapa karakter akan digeser.

result = "": Variabel result digunakan untuk menyimpan teks terenkripsi.

Loop for: Loop ini akan mengiterasi melalui setiap karakter dalam input_text untuk mengenkripsi setiap karakter.
char = input_text[i]: Variabel char digunakan untuk menyimpan karakter saat ini yang sedang diproses dalam teks.

Selanjutnya, program melakukan enkripsi karakter dengan langkah-langkah berikut:

Jika char adalah huruf besar (uppercase), maka program menghitung nilai karakter terenkripsi dengan menggunakan rumus (ord(char) + input_key - 65) % 26 + 65. Ini memastikan bahwa karakter terenkripsi tetap berada dalam jangkauan huruf besar ASCII ('A' sampai 'Z').
Jika char adalah spasi (' '), maka spasi tersebut tetap dipertahankan dalam teks terenkripsi.
Untuk karakter huruf kecil (lowercase), program menghitung nilai karakter terenkripsi dengan rumus (ord(char) + input_key - 97) % 26 + 97. Ini memastikan bahwa karakter terenkripsi tetap berada dalam jangkauan huruf kecil ASCII ('a' sampai 'z').
Hasil enkripsi untuk setiap karakter ditambahkan ke variabel result.

Setelah loop selesai, variabel result berisi teks yang telah dienkripsi.

```python
def dekripsi():
    Alpabeth1 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"
    #Alpabeth2 = "abcdefghijklmnopqrstuvwxyz"
    input_encrypted = str(input("Masukan pesan yang akan di dekripsi, ex [grgr wdpsdq] ?" ))

    for key in range(len(Alpabeth1)):
        translated = ""
        for symbol in input_encrypted:
            if symbol in Alpabeth1:
                num = Alpabeth1.find(symbol)
                num = num - key
                if num < 0:
                    num = num + len(Alpabeth1)
                translated = translated + Alpabeth1[num]
            else:
                translated = translated + symbol

        print('Hacking key #%s: %s' % (key, translated))
```

Alpabeth1 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz": Ini adalah alfabet yang digunakan untuk mencoba semua kemungkinan pergeseran karakter (kunci) dalam enkripsi Caesar. Ini mencakup huruf besar dan huruf kecil dalam alfabet.

input_encrypted = str(input("Masukan pesan yang akan di dekripsi, ex [grgr wdpsdq] ?")): Program meminta pengguna untuk memasukkan pesan yang akan di-dekripsi.

Loop pertama (for key in range(len(Alpabeth1)):): Program mengiterasi melalui setiap kemungkinan kunci, dari 0 hingga panjang alfabet.

translated = "": Variabel translated digunakan untuk menyimpan hasil dekripsi dengan menggunakan kunci yang sedang diuji.

Loop kedua (for symbol in input_encrypted:): Program mengiterasi melalui setiap karakter dalam pesan yang dienkripsi.

if symbol in Alpabeth1:: Program memeriksa apakah karakter saat ini adalah bagian dari alfabet yang digunakan dalam pengujian. Jika iya, maka karakter tersebut adalah karakter yang akan di-dekripsi.

num = Alpabeth1.find(symbol): Program mencari posisi karakter tersebut dalam alfabet yang digunakan.

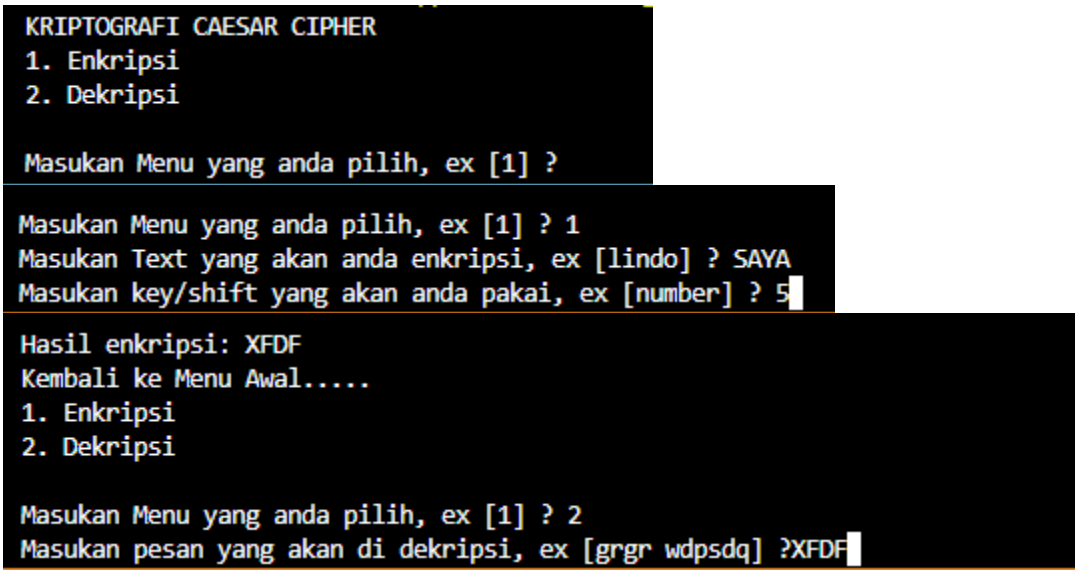
num = num - key: Program menghitung karakter terdekripsi dengan mengurangkan kunci yang sedang diuji.

if num < 0:: Jika hasil perhitungan di atas kurang dari 0, itu berarti kita harus memulai perhitungan dari akhir alfabet, sehingga kita menambahkannya dengan panjang alfabet (len(Alpabeth1)).

translated = translated + Alpabeth1[num]: Karakter terdekripsi ditambahkan ke variabel translated.

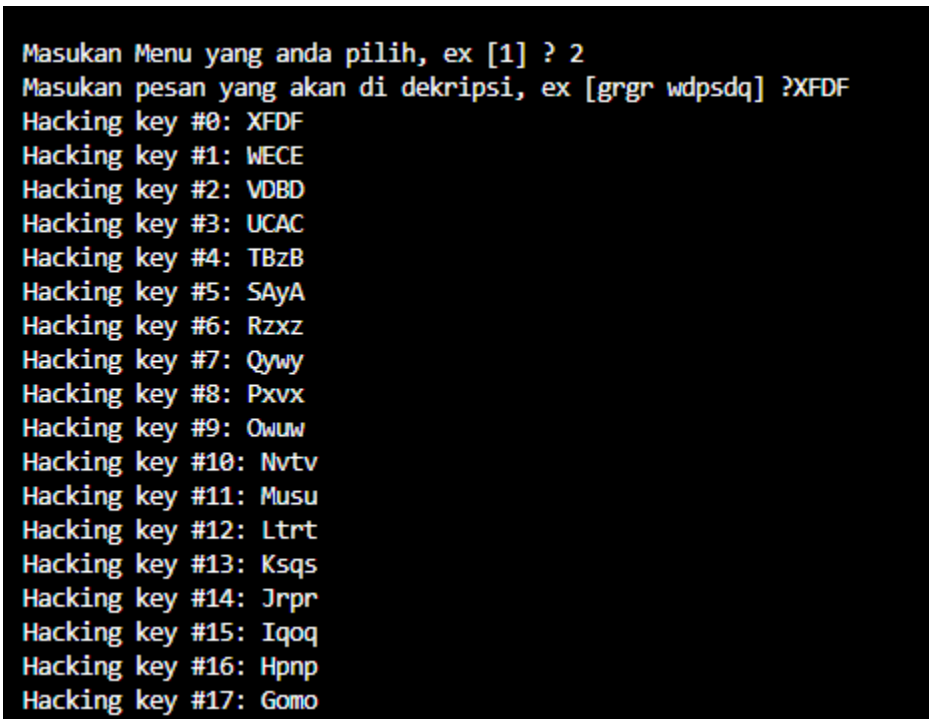
Jika karakter saat ini tidak ada dalam alfabet yang digunakan (else), maka karakter tersebut tetap dipertahankan dalam pesan terdekripsi.

Setelah loop kedua selesai, pesan terdekripsi dengan kunci yang sedang diuji dicetak ke layar dengan pesan "Hacking key #<kunci>: <pesan_terdekripsi>". Ini akan menampilkan hasil dekripsi dengan semua kemungkinan kunci yang dicoba.



Panduan penggunaan Enkripsi :
1. Pilih menu yang ingin dilakukan
2. Masukan pesan atau kata yang ingin di proses
3. Masukan keyshift dimana kalian ingin menyimpan kata ,hal ini dilakukan di proses enkripsi
4. Tunggu Hasil dari Enkripsi Pesan atau kata yang kalian masukan

Panduan penggunaan Deskripsi :
1. Pilih menu yang ingin dilakukan
2. Masukan kata yang telah di enkripsi tadi
3. Setelah itu akan muncul keyshift 1-50
4. Cari kata yang paling benar dan masuk akal



Ini adalah hasil dari deskripsi, kata yang kita dekripsi akan muncul dimana kita meletakan atau menggunakan keyshift pada saat melakukan enkripsi, hasil nya di acak random mulai dari keyshift 1-50

REFERENSI YANG DI GUNAKAN :

http://seminar.uny.ac.id/semnasmatematika/sites/seminar.uny.ac.id.semnasmatematika/files/full/T-41.pdf

Implementasi Keamanan Data menggunakan Kriptografi Caesar Chiper Desi Fitriani Ningrum1 , Muhlis Tahir2 , Wahyu Dwi Angelina3 , Eliza Permatasari4 , Fifi Rinazah Rofiq5 , Miftakhul Hidayati6 , Fatimatus Sahroh7 , Andi Setiawan8 **(PDF dalam FILE)**

https://medium.com/bisa-ai/kriptografi-klasik-caesar-cipher-a33334fe2965

Youtube : https://youtu.be/jVeZsqLmY04?si=cAPv3mkUcTYQEyY9

Dan beberapa bantuan dari https://chat.openai.com/

LINK GIT : https://github.com/H-syam/Chaesar-Chiper