**Project**

Nama : Fawwaz Zulfaa

NIM : 2301955844

Github : <https://github.com/fawwazzulfaa/project>

Project : enkripsi dan dekripsi message pada server dan client

Penjelasan project :

Pada project yang saya buat yakni membuat lapisan keamanan pada message client dan server menggunakan enkripsi dan dekripsi.

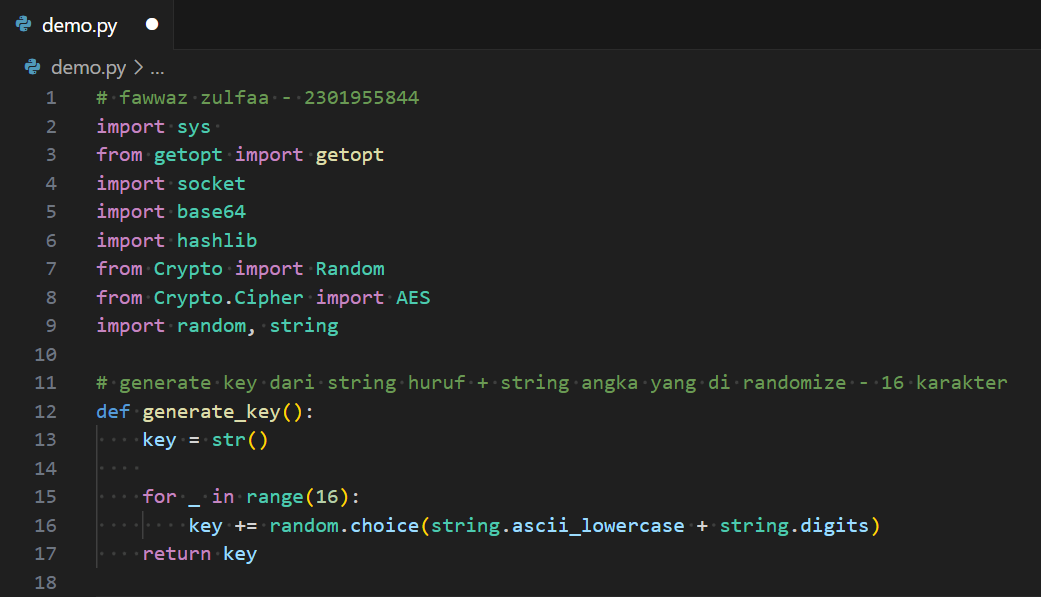
* Metode enkripsi dekripsi yang digunakan yakni AES CFB 256

AES-CFB adalah mode operasi block cipher yang digunakan untuk enkripsi. Untuk AES-256-CFB menggunakan iv yang diperlukan untuk enkripsi. Jika tidak ada iv yang diberikan, kemungkinan besar itu hanya nol (yang berarti 16 0x00 byte, karena iv sama dengan ukuran blok, yaitu 128bit).

* Dalam program enkripsi dan dekripsi pada key nya saya menggunakan generate key yang menggunakan *library import random.* Jadi pada proses generate key diambil dari string huruf + string angka yang di randomize - 16 karakter pada generate keynya.

**code :**

A computer screen with a black background

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screen shot of a computer code

Description automatically generated

A screen shot of a computer program

Description automatically generated

**demo run code :**

A computer screen with white text

Description automatically generated

Jalankan sebagai server dengan command “python demo.py -i 127.0.0.1 -p 2000 -s”

A screen shot of a computer

Description automatically generated

Lalu jalankan sebagai client “python demo.py -i 127.0.0.1 -p 2000”

A computer screen shot of a computer code

Description automatically generated

Setelah terkoneksi server dengan client maka tampilan nya seperti diatas, disini kita sudah bisa mengirim pesan pada client dan server.

A screen shot of a computer

Description automatically generated

Kemudian saya melakukan aktivitas mengirim pesan dari server ke client.

Pada gambar diatas saya mengirim pesan “saya mau lulus” sebagai server lalu pesan tersebut di enkripsi dan key (dari string huruf + string angka yang di randomize - 16 karakter) yang digenerate di enkrispsi juga . Lalu pesan di dekripsi oleh client untuk dapat melihat isi pesan tersebut, aktifitas mengirim pesan enkripsi dan dekripsi dengan server dan client atau sebaliknya berhasil dilakukan.

* Pada gambar diatas yang **digaris bawahi merah** berisi key yang sudah di randomize : + pesan dan key password yang di encrypt.

**Manfaat dari penggunaan enkripsi dan dekripsi pada pesan**

* Menjaga Kerahasiaan Data

Dengan menerapkan enkripsi dan dekripsi, dapat memastikan bahwa pesan tidak akan dapat diakses oleh pihak yang tidak berwenang sehingga memberikan kemanan

* Menghindari Penyadapan

Dengan enkripsi dan dekripsi, pesan yang terbaca hanya berupa teks acak yang tidak memiliki arti bahkan jika informasi tersebut disadap oleh orang yang tidak bertanggung jawab.

* Keamanan dalam Transfer Data

enkripsi dan dekripsi dapat menjaga keamanan selama proses transfer atau pengiriman pesan. Hal ini mencegah data dari potensi peretasan atau pemalsuan yang bisa terjadi dalam serangan Man-in-the-Middle.

**Kekurangan dari AES-CFB**

* Data yang corrupt tidak dapat dipulihkan karena setiap ciphertext bergantung pada ciphertext lainnya untuk didekripsi.
* Sequential Processing: AES-CFB memproses data secara berurutan, artinya setiap blok bergantung pada enkripsi blok sebelumnya. Hal ini dapat membatasi kemampuan pemrosesan paralel, sehingga kurang cocok untuk skenario komputasi performa tinggi tertentu.
* Overhead performance: Sifat berurutan dari AES-CFB dapat menimbulkan overhead performence dibandingkan dengan mode lain yang memungkinkan pemrosesan paralel, terutama dalam implementasi hardware
* Sensitivitas terhadap Bit Flipping: Mode CFB sensitif terhadap serangan bit-flipping. Jika penyerang dapat memanipulasi ciphertext, mereka mungkin dapat mengontrol atau memodifikasi output yang didekripsi.