ENKRIPSI

Keamanan Informasi

Teknik Informatika Kelas C

Nama Mahasiswa
Dimas Tri Mustakim (205150200111049)
Muhammad Firdaus Ardiansyah (205150201111036)

Dosen:

Adhitya Bhawiyuga, S.Kom., M.Sc.

Program Studi Teknik Informatika
Jurusan Teknik Informatika
Universitas Brawijaya

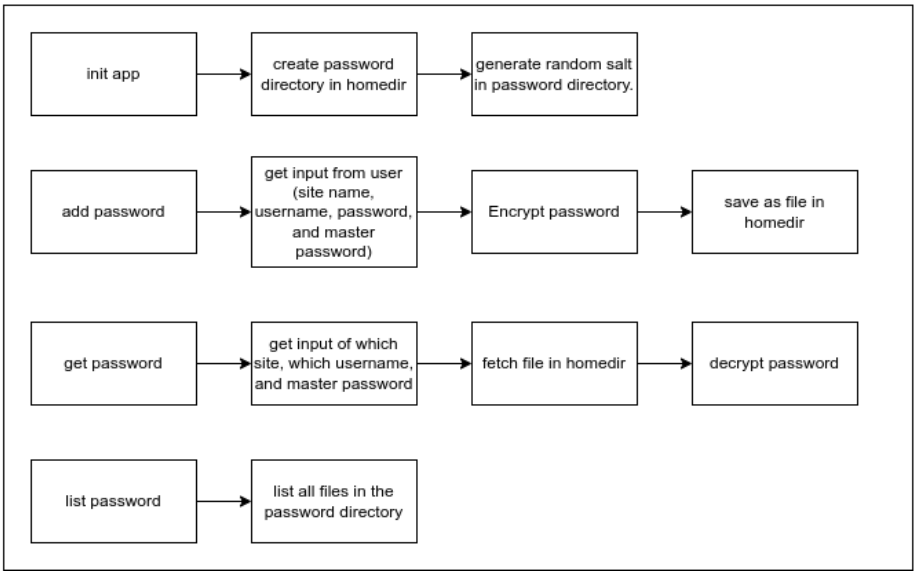
2022

Aplikasi penyimpanan password.

Aplikasi yang kami buat adalah aplikasi *password manager*. Aplikasi ini didesain untuk menyimpan dan memanajemen informasi kredensial pengguna. Aplikasi ini diharuskan untuk menyimpan password dengan aman, salah satu cara untuk mengamankan password adalah dengan menyimpannya ke dalam bentuk ciphertext.

Di program ini harus terdapat fungsi minimal untuk menambah password baru, melihat password yang telah disimpan, dan mendapatkan daftar password yang telah dimasukkan. Berikut adalah detail alur program dari aplikasi yang telah kami buat.

Alur Program



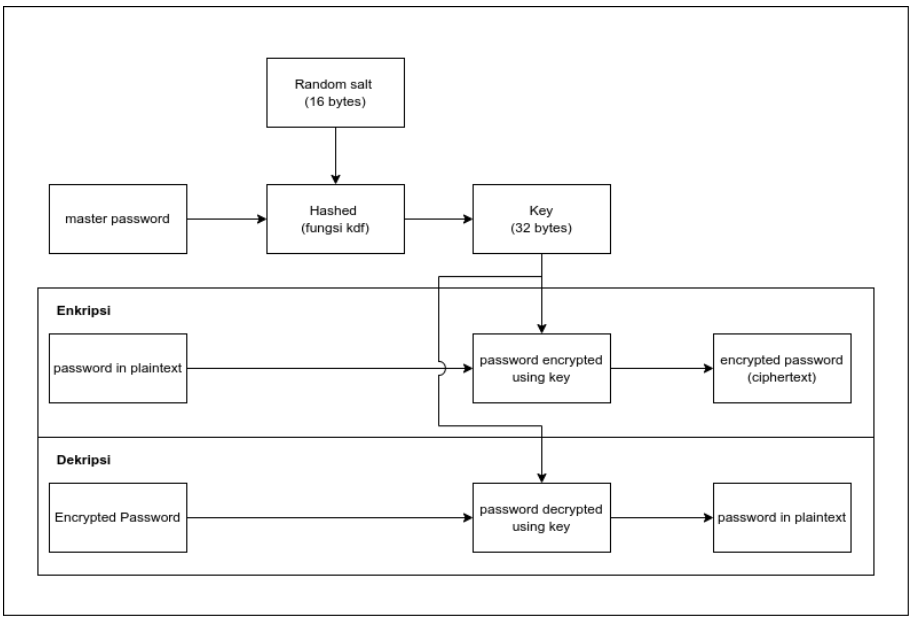
Fungsi inisialisasi digunakan untuk membuat sebuah folder baru di dalam *home directory* sebagai tempat untuk menyimpan password. Fungsi tersebut juga akan membuat *random salt* dan akan disimpan di directory tersebut. Fungsi ini harus dijalankan saat pertama kali kita menggunakan aplikasi ini.

Fungsi add password digunakan untuk menambahkan suatu password pada folder home directory yang telah dibuat pada fungsi inisialisasi. Fungsi bekerja dengan cara menerima input berupa site name, username, site password, dan main password. Kemudian kedua password yaitu site password dan main password akan dienkripsikan dan disimpan pada file di home directory.

Fungsi get password digunakan untuk mendapatkan password yang telah kita enkripsi pada file di home directory. Fungsi bekerja dengan cara menerima input berupa username dan main password yang telah diinput pada fungsi add password sebelumnya. Kemudian dilakukan pencarian file dan diambil file tersebut agar dilakukan dekripsi pada password tersebut.

Fungsi list password digunakan untuk menampilkan list semua file pada direktori password yang telah kita buat sebelumnya pada fungsi add password.

Alur Enkripsi dan Dekripsi



Untuk enkripsi dan deskripsi dari password kami menggunakan dua konsep yaitu symmetric encryption dan hashing. Di program ini, master password akan di hashing dan dilakukan salt (16 bytes) dengan fungsi KDF (Key Derivation Function) dan dihasilkan sebuah 32 byte keys. Key tersebut kemudian akan digunakan sebagai symmetric encryption key untuk melakukan enkripsi dan dekripsi password.

Algoritma
Untuk melakukan enkripsi kami memanfaatkan library *cryptography* yang ada di python. Untuk hashing master password kami terdapat dua algoritma yang digunakan yaitu PBKDF2HMAC dan Scrypt. Untuk algoritma yang digunakan sebagai symmetric encryption adalah 128-bit AES CBC yang digunakan di fungsi Fernet.

Hashing master password
Untuk hashing master password kami pilih menggunakan PBKDF2HMAC dan Scrypt untuk mempersulit serangan dictionary karena kedua algoritma tersebut jauh lebih lambat dibandingkan dengan algoritma hashing lainnya. Untuk hashing juga digunakan *salt* yang dibuat secara acak. Dalam kriptografi, *salt* adalah data acak yang digunakan sebagai input tambahan untuk fungsi satu arah yang meng-hash data. Salt digunakan untuk mengamankan kata sandi dalam penyimpanan dengan memperluas ruang pencarian dalam kasus brute-forcing dan menambah kesulitan untuk rainbow attack (tabel pelangi).

Algoritma PBKDF2HMAC dan Scrypt termasuk kedalam Key Derivation Function (KDF). Dalam kriptografi, KDF adalah algoritma kriptografi yang menurunkan satu atau lebih kunci rahasia dari nilai rahasia seperti kunci utama, kata sandi, atau frasa sandi menggunakan fungsi pseudorandom (yang biasanya menggunakan fungsi hash atau block cipher). KDF dapat digunakan untuk meregangkan kunci menjadi kunci yang lebih panjang atau untuk mendapatkan kunci dari format yang diperlukan, seperti mengonversi elemen grup yang merupakan hasil dari pertukaran kunci Diffie–Hellman menjadi kunci simetris untuk digunakan dengan AES. Fungsi HMAC adalah contoh populer dari fungsi pseudorandom yang digunakan untuk derivasi kunci.

- **PBKDF2HMAC**
  Merupakan salah satu KDF (Key Derivation Function), dimana pengguna dapat mengatur biaya komputasi yang bertujuan untuk memperlambat perhitungan kunci sehingga lebih tidak praktis untuk brute force. Dalam penggunaannya, dibutuhkan kata sandi, *salt*, dan sejumlah iterasi untuk menghasilkan panjang kunci tertentu yang juga dapat dibandingkan dengan hash karena ini juga merupakan fungsi satu arah.
- **Scrypt**
  Merupakan KDF (Key Derivation Function) yang didesain untuk menyimpan password agar tahan terhadap hardware-assisted attackers dengan memiliki biaya memori yang dapat disesuaikan.

Algoritma Symmetric Encryption
Algoritma *symmetric encryption* yang kami gunakan adalah fungsi yang digunakan oleh Fernet di modul cryptography. Fernet menggunakan 128-bit AES CBC untuk enkripsi. Fernet merupakan implementasi dari Symmetric(biasa dikenal sebagai “secret key”)Authenticated Cryptography. Fernet ideal untuk mengenkripsi data yang mudah disimpan di memori, namun tidak cocok apabila digunakan untuk mengenkripsi file dengan ukuran yang besar. Fernet juga menjamin bahwa file yang dienkripsi tidak dapat dibaca atau dimanipulasi.

Mode AES-CBC (cipher block chaining) adalah salah satu algoritma enkripsi simetris yang paling banyak digunakan. Ukuran data harus bukan nol dan kelipatan 16 byte, yang merupakan ukuran "blok". Data dipecah menjadi blok 16-byte sebelum enkripsi atau dekripsi dimulai, kemudian operasi dilakukan pada masing-masing blok. Setiap blok terhubung ("dirantai") ke dua blok sebelum dan sesudahnya, masing-masing. yaitu, sebuah blok mengambil 16-byte IV (vektor inisialisasi) dari blok sebelumnya sebagai input, dan mengeluarkan 16-byte IV ke blok yang segera mengikutinya. Tentu saja, ciphertext 16-byte juga dikeluarkan.

Kode Program

Kode program kami buat dengan menggunakan bahasa pemrograman python dan terdiri dari dua buah file, yaitu app.py dan PasswordManager.py. PasswordManager.py mengandung kelas dan fungsi-fungsi inti yang digunakan untuk melakukan fungsi-fungsi yang ada serta untuk enkripsi, sedangkan app.py berisi kode yang berfungsi sebagai interface untuk CLI yang akan menggunakan fungsi dari PasswordManager. Disini kami menggunakan library external yaitu Cryptography (berisi algoritma kriptografi) dan Typer (membuat aplikasi CLI).

Kode program dapat dilihat dan diakses dari repository Github berikut : https://github.com/tridims/passmanager