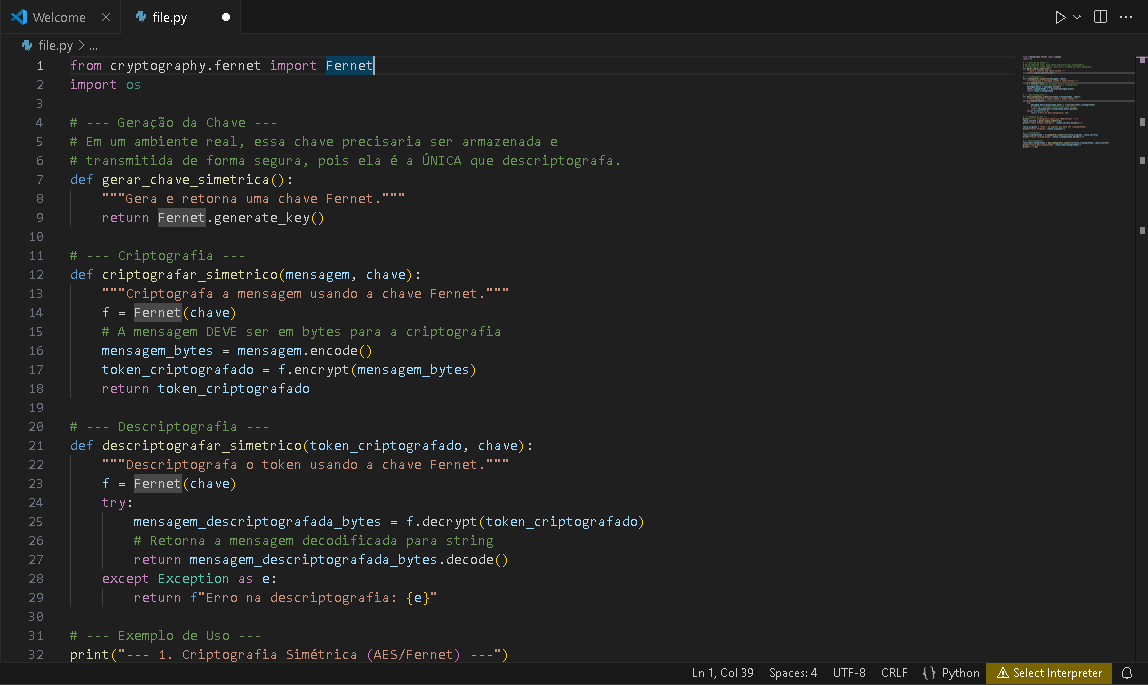
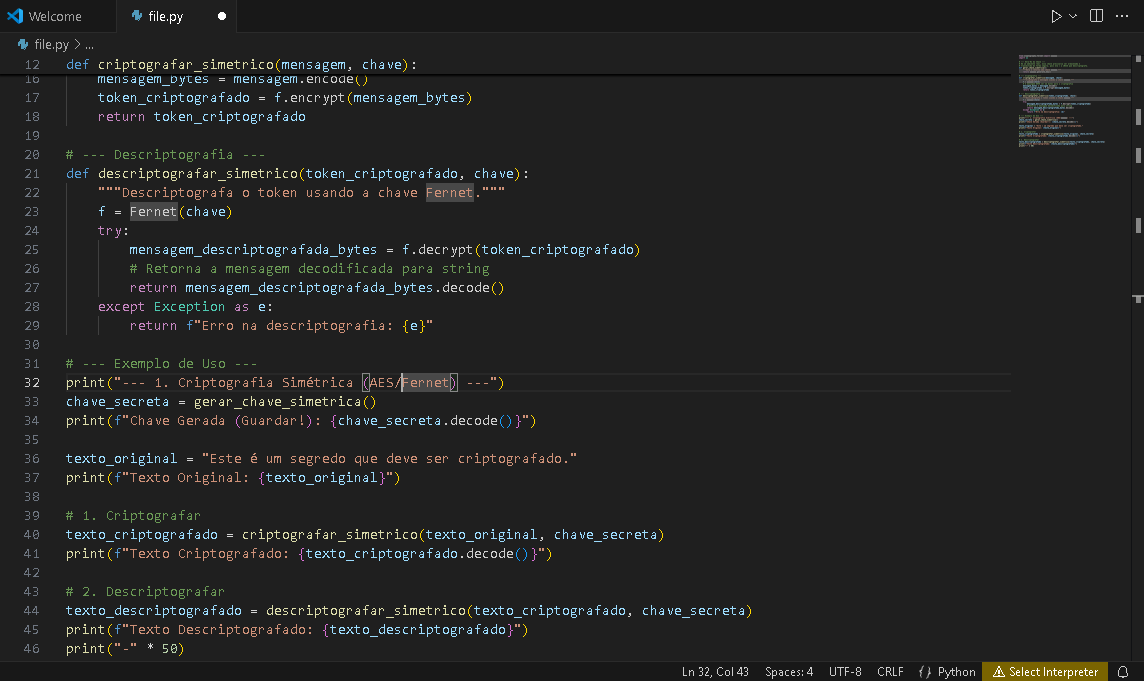
**Algoritmos de Criptografia (Chave Simétricas, Chave Assimétrica e Função Hash)**

Criptografia Simétrica (AES)

Na criptografia simétrica é utlizada a mesma chave para criptografar dados e descriptografar os mesmos. O algoritmo utilizado é um comumente utilizado e muito seguro.

No exemplo é utilizado a biblioteca Cryptography com uma implementação do Fernet baseada na criptografia simétrica AES.

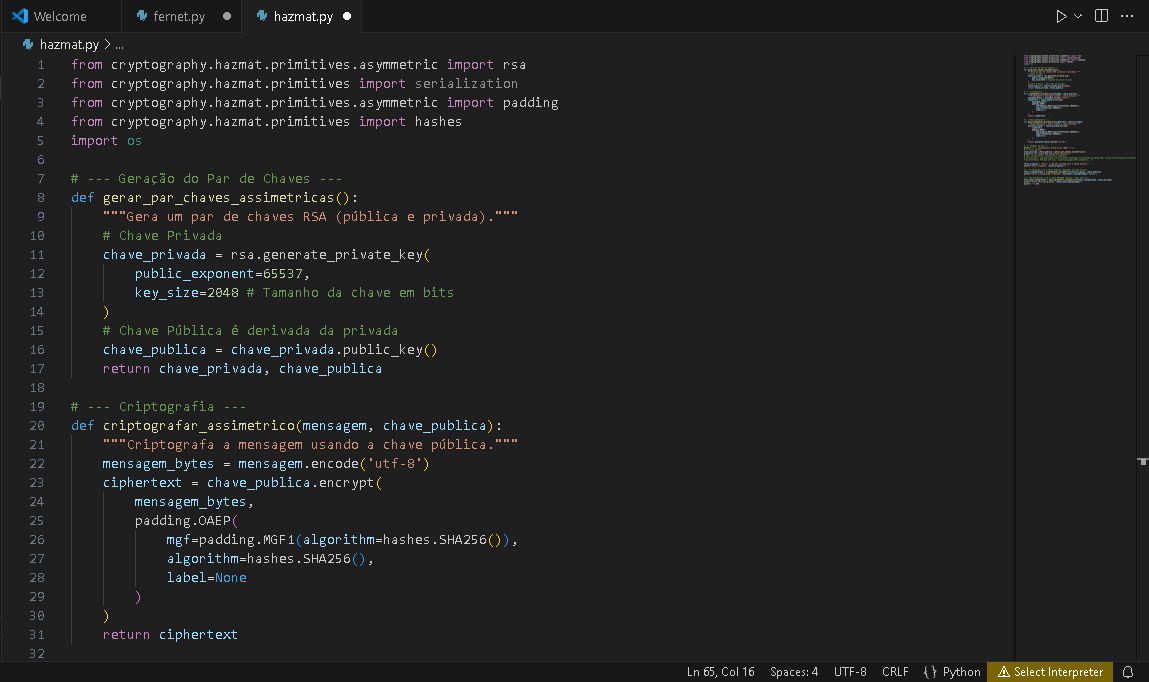


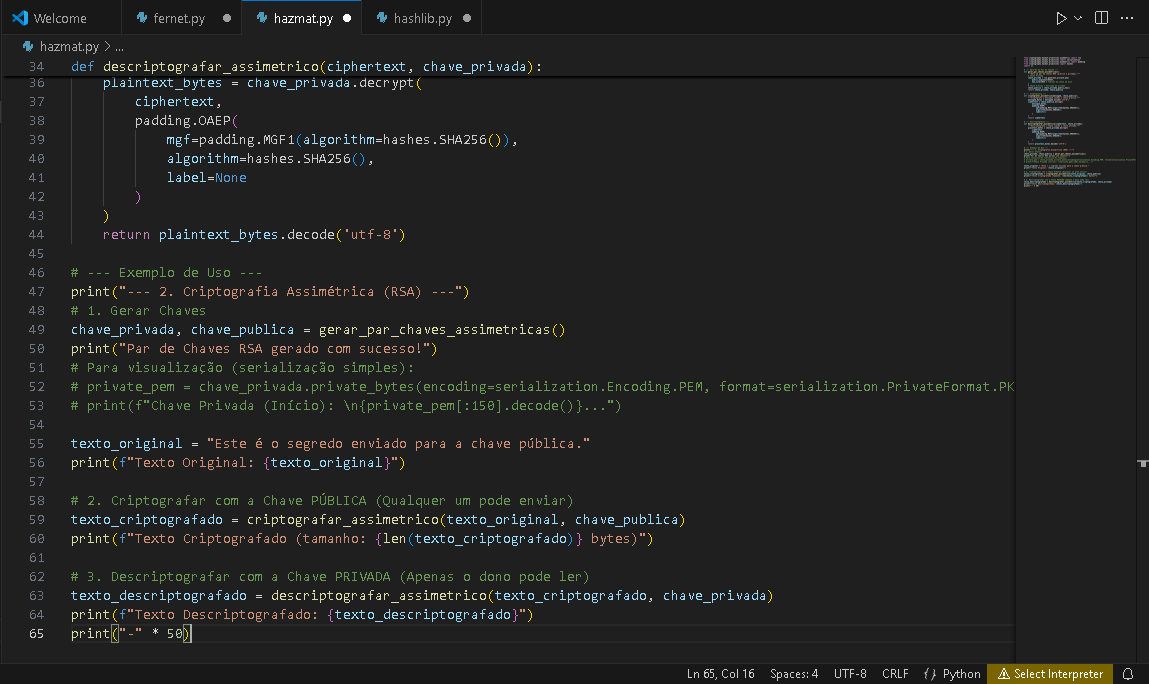


Criptografia Assimétrica (RSA)

A Criptografia Assimétrica, diferente da Simétrica, usa par de chaves: uma chave pública e uma chave privada, e o algoritmo mais utlizado e conhecido é o RSA.

No exemplo será utilizado a biblioteca cryptography novamente, porém com a implmentação Hazmat para gerar e utilizar o par de chaves RSA.



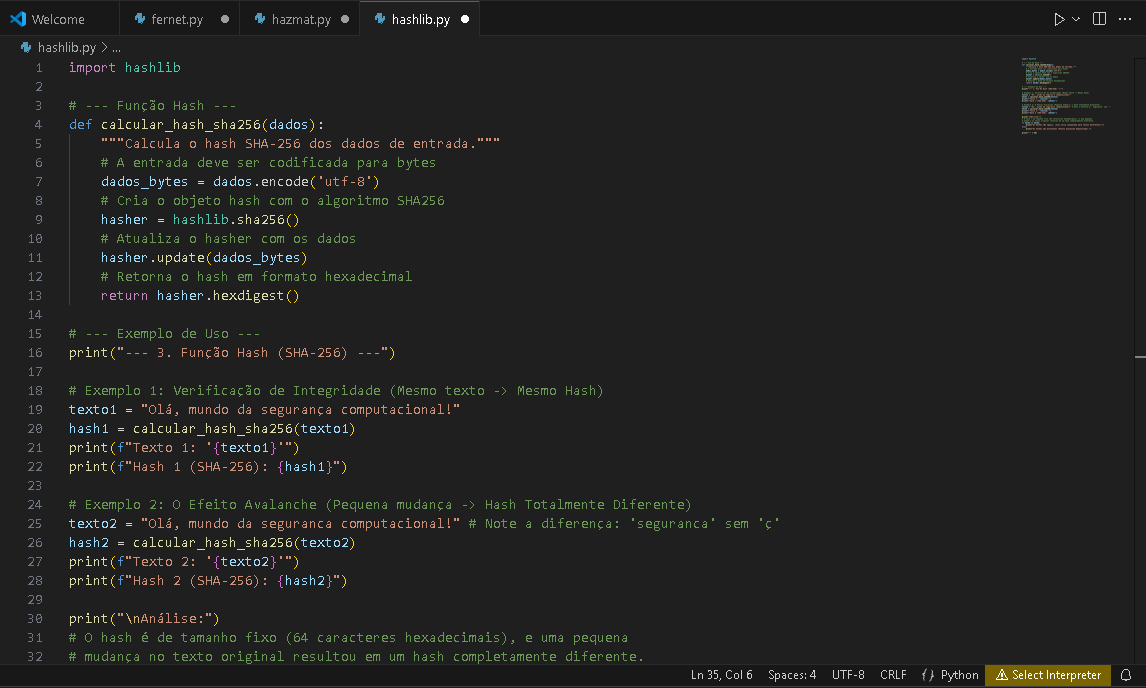


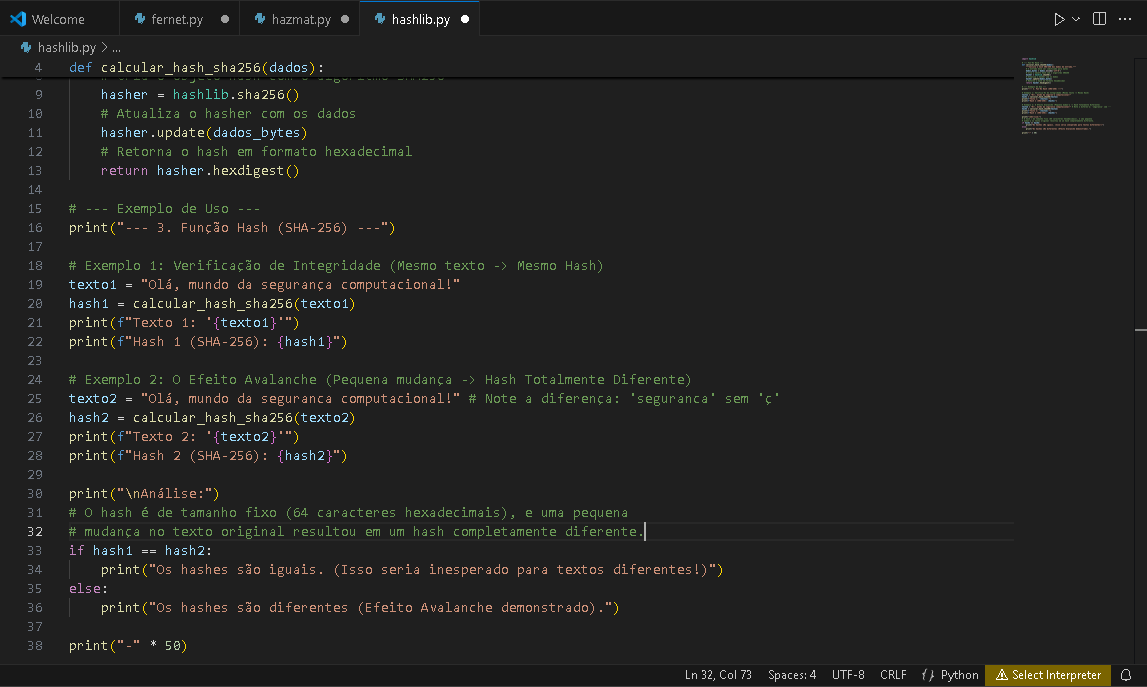
Função Hash

Uma função hash pega uma entrada de qualquer tamanho e produz uma saída de tamanho fixo (o hash ou digest). É um processo unidirecional (não é possível reverter o hash para a mensagem original).

O SHA-256 (Secure Hash Algorithm 256-bit) é amplamente usado para verificação de integridade e armazenamento seguro de senhas.

Nesse exemplo referente a função hash, é utilizada o módulo padrão do Python Hashlib, esse modulo não requer instalaçao de biblioteca ou qualquer outra extensão.





Diante desses exemplos podemos entender que a escolha correta e a **implementação cuidadosa** desses mecanismos criptográficos são o que tornam um sistema robusto e confiável para quem o utiliza.

A segurança moderna funciona como uma equipe:

* Temos a **velocidade** dos **métodos simétricos** (como o Fernet), que agem rapidamente para proteger nossos dados mais importantes, garantindo que ninguém os leia sem permissão.
* Em seguida, a **autenticidade** dos **métodos assimétricos** (como o RSA) entra em cena para criar uma "identidade digital" segura, permitindo que a gente saiba, com certeza, quem está do outro lado da comunicação.
* Por fim, as **funções hash** (como o SHA-256) funcionam como uma prova de que a mensagem não foi adulterada, garantindo a **integridade** e a verdade do que foi enviado.

Compreender e aplicar corretamente essa **interação inteligente** de ferramentas é o que nos capacita a criar soluções digitais que realmente protegem as pessoas.

Victor Domingos Moreira - 825155879

Lucas Gonçalves da Silva - 825113362

Victor de Morais Nelson - 825243925