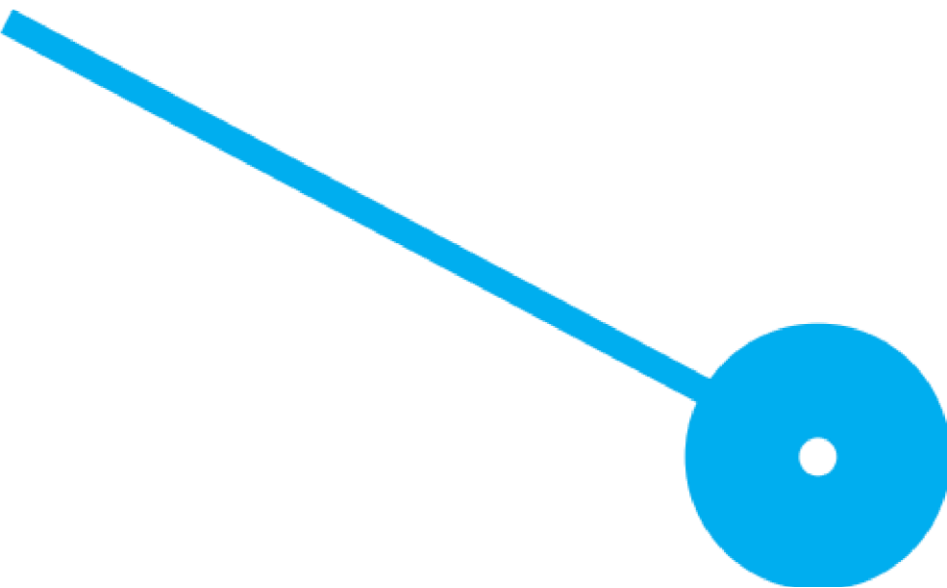


Encriptação e Desencriptação

Segurança Informática

Pedro Antunes
8230068



Índice

Resumo.....	2
1.Definição dos Objetivos.....	3
2.Análise dos requisitos	4
3.Pesquisa e estudo.....	4
4. Desenvolvimento do Sistema	4
5.Resultados	5
7.Discussão.....	8
8.Conclusão	9

Resumo

A proteção de dados sensíveis é uma preocupação fundamental na era digital, onde o armazenamento e o compartilhamento de informações ocorrem de forma frequente. Nesse contexto, a criptografia desempenha um papel crucial na garantia da segurança e privacidade dos dados dos utilizadores. Este projeto concentra-se no desenvolvimento de um sistema de criptografia destinado a armazenar dados sensíveis de um utilizador, como passwords e informações de login, de forma segura e confiável.

O sistema proposto implementa a cifra de César para encriptar passwords, oferecendo aos utilizadores uma maneira simples e eficaz de proteger as suas informações de login. A cifra de César é um método de encriptar por substituição, onde cada letra no texto original é deslocada para frente ou para trás no alfabeto por um número fixo de posições. Essa abordagem proporciona uma camada básica de segurança, tornando as senhas ilegíveis para pessoas não autorizadas.

Além disso, o sistema oferece uma funcionalidade de encriptar ficheiros, utilizando a biblioteca Fernet em Python. Essa funcionalidade permite que os utilizadores protejam arquivos sensíveis, garantindo que apenas pessoas autorizadas possam aceder ao seu conteúdo.

Este relatório detalha a metodologia adotada para o desenvolvimento do sistema, descreve suas principais características e funcionalidades, e apresenta os resultados obtidos durante o processo de implementação. No final, serão discutidas as conclusões do projeto e sugestões para possíveis melhorias futuras.

1. Definição dos Objetivos

O principal objetivo deste projeto é fornecer aos utilizadores uma maneira segura e conveniente de armazenar suas credenciais (username e passwords) para diversos serviços online. Para alcançar esse objetivo, foram estabelecidos os seguintes objetivos específicos:

1. Utilização da Cifra de César para Criptografar Senhas:

- Implementar a cifra de César em Python para encriptar e desencriptar senhas de forma simples e eficaz.
- Garantir que as senhas encriptadas sejam armazenadas num ficheiro .txt para que depois o utilizador consiga encriptar o mesmo usando a app.

2. Integração da Biblioteca Fernet em Python para Encriptação de Ficheiros:

- Integrar a biblioteca Fernet em Python ao sistema para permitir a encriptação e desencriptação.
- Proporcionar aos utilizadores uma maneira segura de proteger seus ficheiros sensíveis, garantindo que apenas pessoas autorizadas possam aceder seu conteúdo.

3. Desenvolvimento de uma Interface de Fácil Interação com o utilizador:

- Desenvolver uma interface para o utilizador intuitiva e amigável, facilitando a interação dos utilizadores com o sistema.
- Priorizar a usabilidade e a experiência do utilizador, garantindo que o sistema seja acessível e fácil de usar para utilizadores de diferentes níveis de habilidade.

Ao atingir esses objetivos, espero criar uma solução abrangente e eficaz que não apenas proteja as informações sensíveis dos utilizadores, mas também promova a conscientização sobre a importância da segurança de dados no ambiente digital.

2. Análise dos requisitos

Com este projeto pretendi, logo desde o início fazer uma espécie de app para que os futuros utilizadores da mesma possam usufruir de forma segura, protegendo os seus dados e acima de tudo incentivar os utilizadores a não usarem a mesma password em diferentes plataformas. Para atingir o objetivo, a aplicação deve implementar a Cifra de César para encriptação de passwords, e a biblioteca Fernet será integrada para permitir a encriptação de arquivos, proporcionando uma camada adicional de segurança. O user interface deve ser intuitiva e de fácil e simples de utilização. Esses requisitos garantem que a aplicação seja segura, fácil de usar e eficiente, mas sempre com o objetivo principal de proteger as informações sensíveis do utilizador.

3. Pesquisa e estudo

Antes de iniciar o desenvolvimento da aplicação, pesquisei técnicas de encriptação (fornecidas nos PowerPoint de SI) e bibliotecas disponíveis em Python. A Cifra de César foi a escolhida devido à sua simplicidade para encriptar passwords, e a biblioteca Fernet, para encriptação de arquivos, devido ao feedback bastante positivo na comunidade/internet.

4. Desenvolvimento do Sistema

4.1 Implementação da Cifra de César

- **Algoritmo:** A primeira coisa a pensar foi no algoritmo que ia usar, optei por fazer um deslocamento de 5 casas para a direita.
- **Armazenamento em arquivo .txt:** As senhas encriptadas são armazenadas em um ficheiro txt, juntamente com o username/email e o site, estes últimos em texto claro.

4.2 Implementação da biblioteca Fernet

- **Biblioteca Fernet:** foi implementada para encriptar e desencriptar arquivos.
- **Funções de criptografia:** Desenvolvi funções em Python para encriptar e desencriptar ficheiros, para que o utilizador consiga ainda ter uma maior segurança em relação aos seus dados sensíveis.

4.3 Desenvolvimento da interface do utilizador

- **Ferramentas utilizadas:** utilizei a biblioteca Tkinter para desenvolver a interface gráfica.
- **Funcionalidades da interface:** a interface disponibiliza aos utilizadores a opção de colocarem as informações principais a onde fizeram o registo (website, email/username e password), dando também outra funcionalidade de encriptar e desencriptar arquivos.

4.4 Teste e validações

- Realizei teste para garantir que o sistema está a funcionar como é previsto, fazendo teste inserindo os dados e depois verificar se estes mesmo eram encriptados e guardados. Também foram realizados teste para a encriptação e descriptação de arquivos.

5.Resultados

Os resultados do projeto incluem uma aplicação funcional com um GUI intuitivo e de fácil utilização(figura1), que permite aos utilizadores armazenarem informações relativamente ao um site (figura2), permitindo também a funcionalidade de encriptar ficheiro(figura3) , onde mostra as informações relativas à figura2, e também a função de desencriptar uma password referente a um site que utilizador queira saber (figura 4 e 5) e também a funcionalidade de desencriptar ficheiros (figura 5 e 6).

A interface que o utilizador tem para adicionar, encriptar ficheiros, desencriptar ficheiros e desencriptar password de determinado site que o utilizador tenha feita o registo.

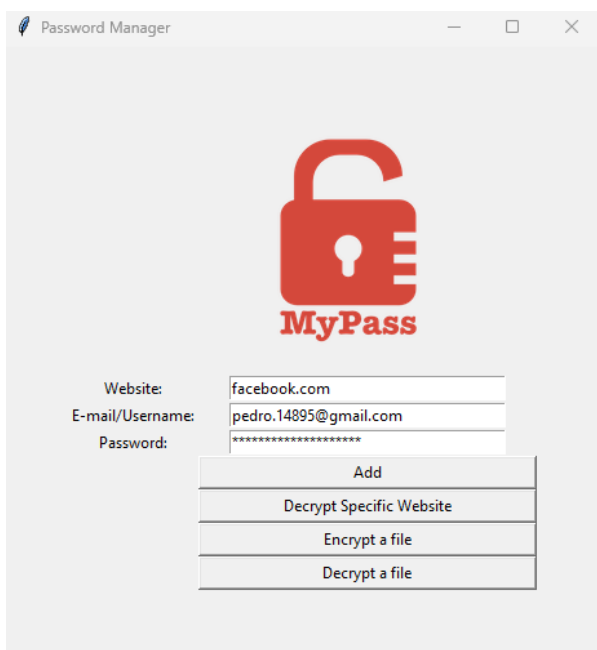
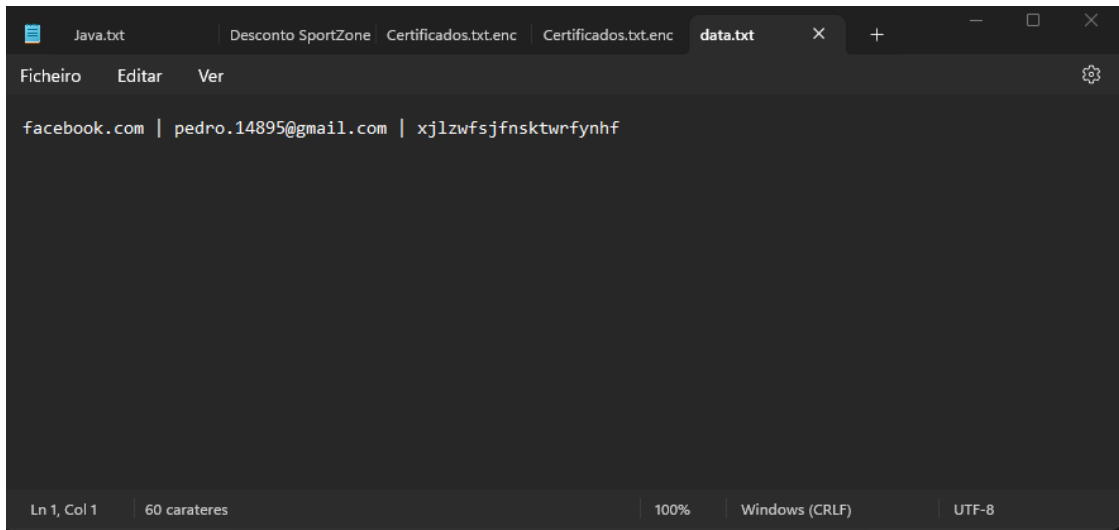


Figura 1

Dados são guardados em ficheiro txt, sendo que o username e o website que o utilizador digitou estão em texto claro e a password encriptada.

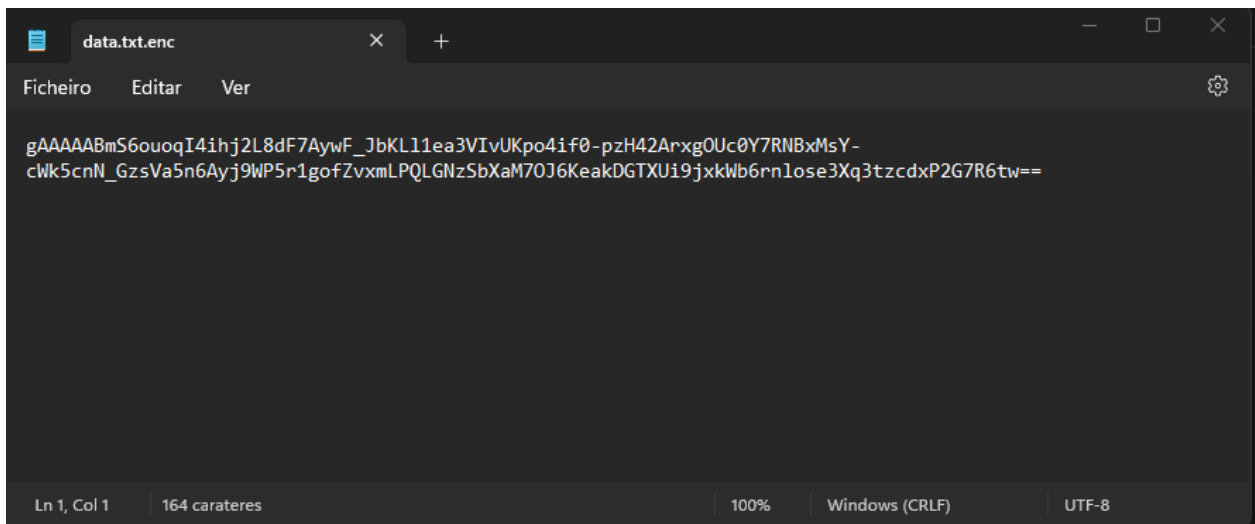


The screenshot shows a text editor window with the title bar 'data.txt'. The menu bar includes 'Ficheiro', 'Editar', and 'Ver'. The text area contains the string 'facebook.com | pedro.14895@gmail.com | xjlzwsjfnsktwrfynhf'. The status bar at the bottom indicates 'Ln 1, Col 1', '60 caracteres', '100%', 'Windows (CRLF)', and 'UTF-8'.

```
facebook.com | pedro.14895@gmail.com | xjlzwsjfnsktwrfynhf
```

Figura 2

Quando o utilizador tiver guardado tudo, podemos encriptar o ficheiro para que este mesmo fique ainda mais seguro como podemos ver na figura 3.



The screenshot shows a text editor window with the title bar 'data.txt.enc'. The menu bar includes 'Ficheiro', 'Editar', and 'Ver'. The text area contains the encrypted string 'gAAAAABmS6ouoqI4ihj2L8dF7AywF_JbKL11ea3VIvUKpo4if0-pzH42ArxgOUc0Y7RNBxMsY-clWk5cnN_GzsVa5n6Ayj9WP5r1gofZvxmLPQLGNzSbXaM70J6KeakDGTXUi9jxkwb6rnlose3Xq3tzcdxP2G7R6tw=='. The status bar at the bottom indicates 'Ln 1, Col 1', '164 caracteres', '100%', 'Windows (CRLF)', and 'UTF-8'.

```
gAAAAABmS6ouoqI4ihj2L8dF7AywF_JbKL11ea3VIvUKpo4if0-pzH42ArxgOUc0Y7RNBxMsY-clWk5cnN_GzsVa5n6Ayj9WP5r1gofZvxmLPQLGNzSbXaM70J6KeakDGTXUi9jxkwb6rnlose3Xq3tzcdxP2G7R6tw==
```

Figura 3

Funcionalidade para descriptar uma password consoante o website que o utilizador quer saber a password que guardou.

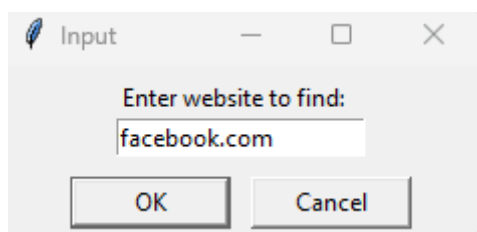


Figura 4

Aqui podemos ver a password descriptada e os dados todos que o utilizador usou para guardar no respetivo site.

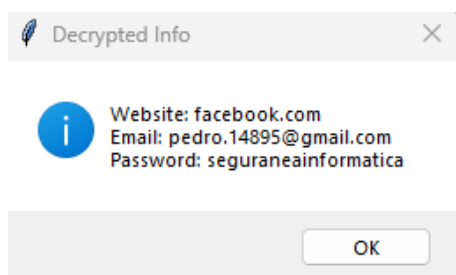


Figura 5

A opção de encriptação de ficheiros para uma maior segurança.

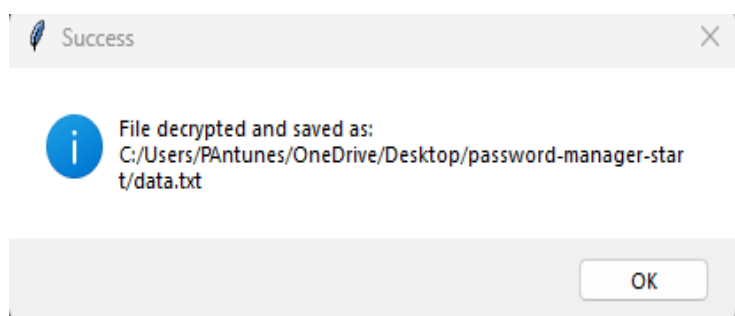


Figura 6

A descriptação do ficheiro que posteriormente foi encriptado, reparando que a password não foi descriptada, garantindo assim uma camada maior de segurança.

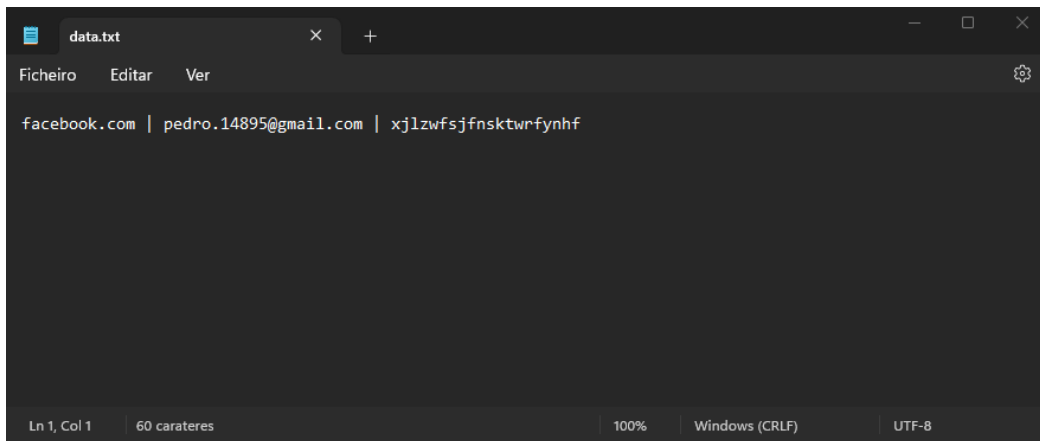


Figura 7

7.Discussão

Os resultados obtidos demonstram que a aplicação cumpre com os objetivos estabelecidos, proporcionando uma solução funcional e segura para o armazenamento de credenciais e a encriptação de arquivos. No entanto, existem algumas áreas que poderiam ser melhoradas:

- **Métodos de Armazenamento:** Atualmente, as senhas encriptadas são armazenadas em um arquivo .txt. Uma melhoria futura poderia incluir o uso de uma base de dados segura, como SQLite ou MySQL, que oferece melhor gerenciamento e segurança dos dados armazenados.
- **Métodos de Criptografia:** A cifra de César, embora útil para fins educacionais, não é segura para aplicações práticas. A implementação de métodos de criptografia mais robustos, como AES (Advanced Encryption Standard), poderia aumentar significativamente a segurança das passwords armazenadas.
- **Autenticação de Usuários:** A adição de um sistema de autenticação de utilizadores poderia melhorar a segurança da aplicação, garantindo que apenas utilizadores autorizados possam aceder e gerenciar as credenciais e arquivos encriptados.

8.Conclusão

Neste relatório, desenvolvi um sistema de encriptação de passwords e ficheiros de fácil utilização e simples para poder compreender as diversas funcionalidades de encriptação e a importância da mesma para a presente era tecnológica.

A cifra de César, oferece uma camada básica de segurança, embora seja uma técnica simples ele cumpre com o papel fornecendo uma proteção inicial e de fácil entender para os utilizadores. No entanto, para colmatar essa segurança básica decidi implementar a encriptação de ficheiros utilizando a biblioteca Fernet em Python para encriptar ficheiros, oferecendo assim uma camada mais segura para os utilizadores.

No entanto, devido à facilidade de que a cifra de César pode não ser suficiente para proteger informações altamente sensíveis contra ataques mais avançados. Por isso, recomenda-se a utilização de métodos mais avançados e mais seguros para a encriptação da mesma.

Para futuras melhorias, sugiro a implementação de mecanismos adicionais de segurança, como a exigência de login e password para autenticação na aplicação, além do uso de dados biométricos e autenticação multifator. Essas medidas adicionais aumentariam significativamente a segurança do sistema, tornando-o mais resistente a tentativas de acesso não autorizado.

Este projeto contribui para a proteção de dados sensíveis ao fornecer uma solução simples e prática de criptografia. Espero que este trabalho incentive as pessoas a protegerem melhor os seus dados sensíveis e a diversificarem as suas credenciais para diferentes tipos de uso, aumentando assim a segurança das suas informações pessoais.

Em suma, o sistema desenvolvido oferece uma introdução acessível às técnicas de encriptação, enquanto destaca a necessidade contínua de aprimorar as medidas de segurança para acompanhar as ameaças emergentes na era digital.