INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Criptografia e Criptanalise Aplicadas

Aplicação de Cifra

Martinho José Novo Caeiro - 23917
Paulo António Tavares Abade - 23919

Beja, outubro de 2025

INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Criptografia e Criptanalise Aplicadas

Aplicação de Cifra

Martinho José Novo Caeiro - 23917
Paulo António Tavares Abade - 23919

Orientador: Rui Miguel Silva

Beja, outubro de 2025

Resumo

Este relatório descreve o desenvolvimento de uma aplicação de cifra e decifra de ficheiros, implementada em Python, uma linguagem de alto nível. O objetivo é explorar cifras de criptografia simétrica e demonstrar a aplicação prática das mesmas. Esta aplicação é desenvolvida no âmbito da unidade curricular de Criptografia e Criptanalise Aplicadas IPBeja, 2025.

Keywords: python, criptanalise, criptografia simétrica

Abstract

This report describes the development of a file encryption and decryption application, implemented in Python, a high-level language. The objective is to explore symmetric encryption ciphers and demonstrate their practical application. This application is developed within the scope of the course Cryptography and Applied Cryptanalysis IPBeja, 2025.

Keywords: python, cryptanalysis, symmetric cryptography

Índice

Índice de Figuras

1 Introdução

Esta aplicação consistirá na junção de 4 cifras de criptografia simétrica, AES, DES, Vigenère e PlayFair. A aplicação será desenvolvida em Python (Python Software Foundation, 2025) e tem como base uma interface gráfica simples (GUI), permitindo ao utilizador interagir com o sistema de forma simples e eficiente. Todo o progresso do projeto será documentado no repositório GitHub (Martinho Caeiro & Paulo Abade, 2025).

2 Introdução Teórica

2.1 AES

O AES (Advanced Encryption Standard) (Wikipedia, 2025a) é um padrão de criptografia simétrica amplamente utilizado para proteger dados. Ele utiliza blocos de 128 bits e chaves de 128, 192 ou 256 bits, oferecendo alta segurança e eficiência.

2.2 DES

O DES (Data Encryption Standard) (Wikipedia, 2025d) é um algoritmo de criptografia simétrica que foi amplamente utilizado no passado. Ele opera em blocos de 64 bits e utiliza uma chave de 56 bits. Embora tenha sido substituído por algoritmos mais seguros, o DES ainda é relevante para fins educacionais.

2.3 Vigenère

A cifra de Vigenère (Wikipedia, 2025c) é um método de criptografia que utiliza uma palavra-chave para cifrar o texto. Ela é baseada na cifra de César, mas em vez de usar um único deslocamento, ela aplica deslocamentos diferentes com base nas letras da palavra-chave.

2.4 PlayFair

A cifra de PlayFair (Wikipedia, 2025b) é um método de criptografia que utiliza uma matriz de 5x5 para cifrar pares de letras. Ela é mais segura do que a cifra de César, pois não utiliza um deslocamento fixo.

3 Desenvolvimento dos Scripts

Todos os seguintes scripts foram desenvolvidos em Python com o uso do VS Code (Microsoft Corporation, 2025) e todos verificam se a maquina possui os pacotes necessários para o funcionamento da ferramenta, irá perguntar se quer instalar para poder continuar a utilizar. Caso o utilizador deseje prosseguir, o script irá instalar os pacotes necessários e depois irá ativá-los.

3.1 GUI

O menu GUI é o metodo principal de interação com a ferramenta. Para aceder a um dos metodos de cifra/decifra, o utilizador deve selecionar a aba correspondente. Para executar o menu apenas é necessário escrever 'python gui.py'.

O menu GUI apresenta-se da seguinte forma:

3.2 AES

3.3 DES

3.4 Vigenère

3.5 PlayFair

4 Conclusão

O desenvolvimento desta aplicação permitiu explorar conceitos fundamentais sobre cifras simétricas. Apesar de alguns desafios encontrados, foi possível implementar as cifras solicitadas e configurar uma interface centralizada para facilitar a utilização das mesmas. Durante este processo, foram revistos conceitos previamente estudados na licenciatura de Engenharia Informática.

Bibliografia

IPBeja. (2025). *Disciplina: Criptografia e Criptanalise Aplicadas | IPBeja* [Página LPD]. Obtido outubro 30, 2025, de https://cms.ipbeja.pt/course/view.php?id=544

Martinho Caeiro & Paulo Abade. (2025). *Decipher-Tool - Repositório de Código* [Repositório da Aplicação Decipher-Tool]. Obtido outubro 30, 2025, de https://github.com/MartinhoCaeiro/Decipher-Tool

Microsoft Corporation. (2025). *Visual Studio Code* [Editor de Texto Visual Studio Code]. Obtido outubro 30, 2025, de https://code.visualstudio.com/

Python Software Foundation. (2025). *Welcome to Python.org* [Linguagem de Programação Python]. Obtido outubro 30, 2025, de https://www.python.org/

Wikipedia. (2025a). *Advanced Encryption Standard*. Obtido outubro 30, 2025, de https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Wikipedia. (2025b). *Cifra de Playfair*. Obtido outubro 30, 2025, de https://en.wikipedia.org/wiki/Playfair_cipher

Wikipedia. (2025c). *Cifra de Vigenère*. Obtido outubro 30, 2025, de https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

Wikipedia. (2025d). *Data Encryption Standard*. Obtido outubro 30, 2025, de https://en.wikipedia.org/wiki/Data_Encryption_Standard