Descritivo do trabalho de Segurança Computacional 2021.1

Mateus Luis Oliveira

Agosto 2021

1 Introdução

A cifra de Vigenère é um exemplo de cifra polialfabética, que é uma cifra baseada na substituição, usando vários alfabetos de substituição. Nestre trabalho iremos tratar da implementação de um cifrador/decifrador/quebrador de cifra de Vigenère.

2 Implementação

2.1 Arquitetura do Projeto

Para definir a forma que o projeto foi estruturado decidi tomar como base uma interface de usuário criada pelo RAD tool (Rapid-application development) wxFormBuilder, que gera uma inteface de usuário usando como base os objetos de inteface wxPython. Um arquivo de interface é gerado dentro da ferramenta contendo todas as classes de telas (frames) e outros objetos que compoem a interação com usuário, como botões e caixas de texto, conforme descrito na figura 1.

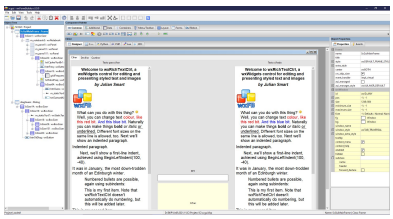

Figura 1: Projeto criado no wxFormBuilder.

O arquivo gerado pelo wxFormBuilder usado como base no projeto é o aqruivo ../scgui.py, que é importado dentro do arquivo principal do projeto para que seus componentem sejam consumidos pelo arquivo principal ../main.py.

2.2 Desenvolvimento

Dentro da implementação do projeto foi usado como base uma estrutura de dado Criada de acordo com o código descrito na figura 2.

```
12  #criação da matrix de Vigenere:
13  def createMatrix():
14      a = []
15      vigenereMatrix = list(string.ascii_lowercase)
16      alphabets = list(string.ascii_lowercase)
17      start_index = 0
18      length = len(alphabets)
19
20      for i in range(length):
21          for i in range(length):
22              element_index = start_index % length
23              a.append(alphabets[element_index])
24              start_index += 1
25          vigenereMatrix = np.vstack((vigenereMatrix,a))
26          a=[]
27          start_index += 1
28      vigenereMatrix = np.delete(vigenereMatrix, 0,0)
29      return vigenereMatrix
```

Figura 2: Implementação da matriz de Vigenère.

A estrutura consiste em uma lista de listas que contém todas as 26 letras do alfabeto. Onde cada lista varia apenas a letra de início. Usando essa matriz a cifração e decifração se torna mais simples, pois conseguimos acessar a letra cifrada ou decifrada com índices.

2.2.1 Cifração

2.2.2 teste2