Aluno: Renan Luiz Babinski

Matéria: Segurança e auditoria de sistemas

Professor: Emilio Wuerges

Instruções para cada etapa da atividade

OBS: Utilizei como subsidio para este trabalho o conteúdo do livro proposto para a matéria “Cracking Codes with Python”. Os textos estão na língua inglesa. O dicionário está na língua inglesa.

1) O programa que cifra e decifra está no diretório principal, seu nome é ***cifra_sub_simples.py***

   O programa possui um menu interativo com a opção de criptografar e descriptografar.
   Ao selecionar **criptografar:**
   - Você pode utilizar uma chave manual ou uma chave aleatória
   - Você deve informar o nome de um arquivo .txt que contenha um texto claro, este arquivo deve estar na pasta **plain_text**
   - No final você pode escolher um nome para o arquivo de saída que ficará na pasta **saída**

   Ao selecionar **descriptografar:**
   - Você deve informar a chave
   - Você deve informar o nome de um arquivo .txt que contenha um texto criptografado, este arquivo deve estar na pasta **cypher_text**
   - No final você pode escolher um nome para o arquivo de saída que ficará na pasta **saída**

2) Os 3 textos em linguagem natural estão na pasta **plain_text**. Os 3 textos criptografados estão na pasta **cypher_text**.

3) O programa ***decrypt_plain_and_cypher.py*** recebe um texto em claro e seu correspondente cifrado, devem estar nas pastas **plain_text** e **cypher_text** respectivamente. Como saída o programa mostra a chave que é o caractere original e seu correspondente cifrado.

4) O programa ***cifra_sub_simples_crack_dict.py*** decifra um texto cifrado de posse de um dicionário analisando padrões de palavras. O programa ***gerar_padrão_palavras.py*** utiliza o dicionário inglês para gerar um dicionário completo de padrões ***padrão_palavras.py*** que é utilizado pelo programa principal para fazer a análise. Como entrada digite o nome de um arquivo cifrado .txt que deve estar na pasta **cypher_text** e será mostrado o texto original, a chave encontrada, e o texto decifrado.

5) O programa da atividade anterior já resolve o problema

6) Relatório abaixo:

Relatório

A cifra de substituição apesar de ser invulnerável a força bruta pode ser facilmente quebrada utilizando a criptoanálise. Porém, eficiência de obtenção da chave/texto em claro depende do tamanho do texto e da qualidade do dicionário utilizado, além de precisarmos adivinhar a língua utilizada na cifra.

Utilizando os programas para decifrar anexados nesta atividade, apenas o texto large_cypher.txt foi decifrado completamente, nos outros 2 casos onde os textos eram menores o algoritmo não consegue mapear determinadas letras e assim gera uma chave incompleta e um texto decifrado parcialmente.