SEGURANÇA DE REDES - Trabalho I - Implementação de cifradores numéricos

Aluna: Maria Eduarda Rebelo Pinho

>Cifrador de César

Cifrador que fará a operação encriptação/decriptação (texto_aberto.txt <> texto_cifrado.txt). Para realizar uma operação é preciso que pelo menos um dos documentos não esteja vazio.

Para executar: python cesar.py

As instruções para execução do código são apresentadas no terminal

Faça a criptanálise da mensagem cifrada com o cifrador de César e mostre a chave usada. Qual é o texto criptografado?

Texto original: Pouco conhecimento faz com que as pessoas se sintam
orgulhosas. Muito conhecimento que se sintam
humildes. Eh assim que as espigas sem graos erguem
desdenhosamente a cabeca para o ceu enquanto as
cheias as baixam para a terra sua mae.
Leonardo Da Vinci.

```
mpinho@mpinho:~/Documents/UTFPR/9-semestre/Segurança de redes$ python cesar.py
Choose: 1-Encript / 2-Decrypt
1
Choose k (1 - 62)
10
Encripting...
Zy4my myxromswox3y pk9 myw 04o k2 zo22yk2 2o 2sx3kw
y1q4vry2k2  W4s3y myxromswox3y  04o 2o 2sx3kw
r4wsvno2  Or k22sw 04o k2 o2zsqk2 2ow q1ky2 o1q4ow
no2noxry2kwox3o k mklomk zk1k y mo4  ox04kx3y k2
mrosk2 k2 lks7kw zk1k k 3o11k  24k wko
Voyxk1ny Nk fsxms
Choose: 1-Encript / 2-Decrypt
```

>Cifrador de Frequência

Cifrador que fará a operação decriptação (texto_cifrado.txt -> texto_aberto.txt).
Código analisará o texto considerando que o caractere que mais se repete é a letra “a”
Para realizar uma operação é preciso que o texto cifrado não esteja vazio.

Para executar: python frequencia.py

As instruções para execução do código são apresentadas no terminal

>Cifrador de Vernam

Cifrador que fará a operação encriptação/decriptação (texto_cifrado.txt <> texto_aberto.txt). Para realizar uma operação é preciso que pelo menos um dos documentos não esteja vazio.

Para executar: python vernam.py

As instruções para execução do código são apresentadas no terminal

Geração de chave: A geração da chave foi feita do seguinte modo:

- Para cada letra do texto foi gerado um número aleatório no intervalo de 0 até a quantidade de caracteres possíveis para se fazer este trabalho (0-9,A-Z,a-z).

- Este valor é então guardado em um vetor. Para este código, a chave foi considerada como um vetor de tamanho igual ao tamanho do texto. O que cumpre com os requisitos de um cifrador de vernam. O vetor de chaves substitui uma chave grande gerada para todo o texto.
- O resto da operação é similar ao cifrador de césar, com a diferença é que à cada uma das letras do texto será atribuída uma chave diferente

O algoritmo é vulnerável a análise de frequência? Não, pois, como cada letra tem um valor de k diferente do anterior, não há um padrão a ser seguido. Isso significa que um mesmo texto, ao ser criptografado mais de uma vez gerará um texto cifrado diferente. Assim como textos diferentes podem gerar um texto cifrado igual.

OBS: Como o código usa um vetor como chave, eu optei por salvar a chave na hora de encriptar e usá-la para descriptografar, de modo que o usuário não poderá descriptografar antes de encriptografar.

>Cifrador de RC4

Cifrador que fará a operação decriptação (texto_aberto.txt ->output.rc4 / output.rc4 -> input.txt).

Para realizar uma operação é preciso que o documentos texto_aberto.txt não esteja vazio.

Para executar: python cr4.py

As instruções para execução do código são apresentadas no terminal

O algoritmo é vulnerável a análise de frequência? Não. Apesar de este algoritmo não ser o mais seguro, ele se utiliza de um array fazendo uma permutação de suas posições, e o mesmo é misturado com a chave. Além disso, o algoritmo se preocupa com o s bytes, e não necessariamente com os caracteres. Desse modo, a análise de frequência não consegue “quebrar” o algoritmo, já que faz a análise em cima dos caracteres, o que não faz sentido para este caso. Essa análise pode ser observada também na execução do código (No fim, há uma análise de frequência do texto aberto e do cifrado).