

CRIPTOGRAFIA E SEGURANÇA DE DADOS

Lucas Steffens de Oliveira
Trabalho II,

3 de fevereiro de 2020

1 Instruções de uso

Para realizar este trabalho foi utilizado o sistema operacional Unbutu 18.04.3 LTS e a linguagem Python em sua versão 3.7.5 com o auxilio das biblioteca sys e binascii. Também foi utilizado as funções para conversão de string para binário e vice versa, retirados deste [link](#).

Para utilizar o programa:

- Abra o terminal Linux no diretório onde esta salvo os arquivos do programa.
- Execute o comando **\$ python cript.py steffenssteffens teste.txt c**
- Os parâmetros devem ser passados nesta ordem, onde **cript.py** representa o código do trabalho, **teste.txt** é o arquivo de texto a ser cifrado , **steffenssteffens** representa a chave de 128 bits utilizada para a criptografia (a chave poderia de ser 64 bits), o comando **c** indica para o código entrar no modo de criptografia.
- As chaves devem ser de 128 bits (16 caracteres) ou 16 bits (8 caracteres) impreterivelmente.
- As extensões de cada arquivo são indispensáveis.
- Para decifrar utilize o comando **\$python cript.py steffenssteffens criptografado.txt d**
- Os parâmetros devem ser passados nesta ordem, onde **cript.py** representa o código do trabalho, **criptografado.txt** é o arquivo de texto a ser decifrado , **steffenssteffens** representa a chave de 128 bits utilizada para a criptografia (a chave poderia de ser 64 bits caso tenha sido criptografada em 64 bits), o comando **d** indica para o código entrar no modo de descriptografia.
- As chave deve ser a mesma usada na etapa de criptografia.
- As extensões de cada arquivo são indispensáveis.