Segurança Computacional
Advanced Encryption Standard

Pedro Henrique de Brito Agnes, 18/0026305
Pedro Pessoa Ramos, 18/0026488

Dep. Ciência da Computação - Universidade de Brasília (UnB)

1 Implementação do AES

A implementação do AES foi feita fixa para a versão de 128 bits e para isso foi criado o arquivo `aes.py` na pasta `src` usando a linguagem python preferencialmente na versão 3.6 ou acima. Para executar o programa para cifrar um arquivo `sample/teste.txt` por exemplo com uma chave aleatória usando o padrão de 10 *rounds* e salvar o criptograma no arquivo sample/output.txt, deve ser usado o seguinte comando:

```
1 python src/aes.py sample/teste.txt -o output.txt
```

O primeiro argumento que o programa recebe é o arquivo que contém a mensagem e o argumento `-o` é obrigatório e representa o arquivo onde será impresso o criptograma. Existem outros argumentos opcionais que podem ser listados com o `-h`:

```
1 python src/aes.py -h
```

Segue a lista de argumentos aceitos:

- **-k** - Arquivo com a chave para criptografar/descriptografar. Argumento obrigatório se for acionada a opção para descriptografar.
- **-o** - Arquivo onde será feito o output. Obrigatório.
- **-r** - Número positivo que representa a quantidade de *rounds* que o AES irá usar. Se não passado um valor, será usado o padrão de 10.
- **-d** - Argumento que indica que o programa vai descriptografar. Deve ser passado no final sem parâmetros adicionais.

Portanto, como exemplo, para decifrar um criptograma no arquivo `sample/ex.txt` usando a chave `keys/key_sample` e 3 *rounds* e colocando o output no arquivo `sample/out.txt`, pode ser usado o seguinte comando:

```
python src/aes.py sample/ex.txt -k keys/key_sample -r 3 -o
    sample/out.txt -d
```

1.1 Aspectos Técnicos