

O Avançado Padrão de Criptografia (AES)

Rafael Campos Nunes¹, Rafael Henrique Nogalha de Lima²
19/0098295¹ 19/0036966²

Contents

1	Introdução	2
2	O AES	2
3	Configuração de Ambiente	2

1 Introdução

2 O AES

O algoritmo AES é uma evolução do DES - sendo este utilizador de estruturas de Feistel -.

3 Configuração de Ambiente

O ambiente utilizado para construção e teste do trabalho é o GNU/Linux, com o python na versão 3.6.9. No Windows o python3 é instalado com o nome python. ertifique-se de que está utilizando a versão correta com 'python -version'.

O programa na sua configuração atual suporta diversos tipos de parâmetros, todos listados e documentos ao executar o comando `python3 src/main.py -help`. Exemplos de utilização são listados abaixo.