# Trabalho 2 - Segurança Computacional

Isabelle Alex dos Santos - 170105636

Gustavo Barbosa de Almeida - 202037589

## 1 Introdução

Este relatório aborda a implementação da cifra de bloco AES (Advanced Encryption Standard) em Python. O AES é uma cifra de bloco amplamente reconhecida e adotada em todo o mundo para a criptografia de dados. Neste código, nos concentramos na implementação da cifra AES com chaves de 128 bits, fornecendo funcionalidades para criptografar e descriptografar mensagens.

### 1.1 Cifra AES - Visão Geral

O AES é uma cifra simétrica que opera em blocos de 128 bits (16 bytes) e suporta chaves de 128, 192 e 256 bits. Ele é amplamente utilizado em várias aplicações, incluindo a proteção de comunicações pela Internet, segurança de arquivos e criptografia de dispositivos de armazenamento.

## 2 Funcionalidades do Código

O código está organizado em uma série de funções que realizam as operações essenciais da cifra AES. Vamos explorar essas funcionalidades em detalhes:

### 2.1 Substituição de Bytes (SubBytes)

A função substitute_bytes implementa a substituição de bytes no bloco de dados usando a tabela S-Box do AES. Essa operação é uma camada de confusão e difusão.

### 2.2 Deslocamento de Linhas (ShiftRows)

A função shift_rows realiza o deslocamento das linhas no bloco de dados. Esse deslocamento reorganiza os bytes dentro do bloco para fornecer maior difusão.

### 2.3 Mistura de Colunas (MixColumns)

A função mix_columns executa a mistura de colunas no bloco de dados. Essa operação cria uma camada de confusão nas colunas do bloco.

### 2.4 Adição da Chave da Rodada (AddRoundKey)

A função add_round_key adiciona a chave da rodada ao bloco de dados atual. Isso introduz a chave específica da rodada para cada bloco, o que é fundamental para a segurança do AES.

### 2.5 Expansão de Chave (expand_encryption_key)

A função expand_encryption_key gera uma chave expandida a partir da chave de criptografia de 128 bits fornecida. Essa chave expandida é usada nas várias rodadas de cifração.

### 2.6 Criptografia (encrypt)

A função encrypt é responsável por criptografar uma mensagem dividida em blocos de 128 bits. Ela aplica as operações do AES a cada bloco da mensagem e retorna o texto cifrado.

### 2.7 Descriptografia (decrypt)

A função decrypt descriptografa o texto cifrado usando a chave de descriptografia correspondente. Ela aplica as operações inversas do AES para recuperar a mensagem original.

## 3 Execução do Código

O código inclui uma chave de exemplo (encryption_key) e uma mensagem de exemplo (test_message). A mensagem é convertida em bytes e criptografada usando a chave. Em seguida, o texto cifrado é descriptografado usando a chave de descriptografia correspondente, e a mensagem original é recuperada.

## 4 Considerações de Segurança

Para uso em ambientes de produção, é fundamental considerar aspectos de segurança, como o armazenamento seguro de chaves e o gerenciamento adequado de chaves. A criptografia AES é apenas um componente de sistemas de segurança mais amplos, que podem incluir autenticação, integridade de dados e outros mecanismos de segurança.

## 5 Conclusão

Este código Python fornece uma implementação didática e funcional da cifra de bloco AES com chaves de 128 bits. Compreender como o AES funciona é fundamental para a segurança da informação. A criptografia AES é uma ferramenta valiosa para proteger dados sensíveis e confidenciais em várias aplicações.

No entanto, a implementação do AES em cenários de produção requer cuidados adicionais, incluindo a consideração de ameaças de segurança, o gerenciamento adequado de chaves e a conformidade com os padrões de criptografia. Portanto, este código deve ser considerado como uma base de aprendizado e não como uma implementação segura para uso em produção.