Instituto Superior Técnico, Tagus Park

**Disciplina de Aplicações e Implementações de Algoritmos Criptográficos**

MERC: 1º ano, 2º semestre, 2012/13

65963 – David Dias Data: 22/03/2013, Segunda-feira

63520 – Fábio Domingos

AES – Implementação em Java

# **Abstract:** Implementação em Java do algoritmo de cifra AES e analise da sua performance face aos vários modos de cifra (ECB e CBC)

# Introdução

O AES(1998) é uma algoritmo de cifra simétrica baseado na cifra Rijandael, que vem para substituir o DES(1977). Os 4 passos fundamentais do AES são a Substituição de Bytes (SubBytes), troca de linhas (ShiftRows), mistura de colunas(MixColumns) e o XOR com a chave(AddRoundKey), especifica por cada Ronda.

Este documento apresenta a implementação desenvolvida em Java para chaves com 128 bits e para os modos de cifra de blocos ECB e CBC.

# Funcionamento

A implementação desenvolvida apresenta uma interface:

init

update

doFinal

A invocação pode ser feita com:

dasdasdad

Gerar as chaves para todas as rondas à priori e esta ficam guardadas até a cifra terminar

10 cycles of repetition for 128-bit keys

melhor velocidade a partir indexação dos padrões no ECB

# Analise de performance

Analise ao ECB

Analise ao CBC

Fazer gráficos no Excell com os tempos do crypto do API do Java e o nosso para ambos os casos

# Propostas de aumento de performance

# Conclusões