**PLANO DE AULA PRÁTICA**

**TAREFA 2.1** "Criptografia Simétrica com AES"

Tópico no Moodle: “Tarefa 2.1 – Criptografia Simétrica com AES”

Data: 21-03-2014

Tempo de Aula: 2 horas-aula

Grupo: <Aluno\_1> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 <Aluno\_2> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# ASSUNTO Advanced Encryption Standard

**OBJETIVOS DA AULA**

Conhecer um algoritmo de criptografia simétrica, relativo às seguintes características:

1. Tamanhos de chave variável: 128, 192, 256 bits
2. Modo de Cifra usado: encontre na Internet algum AES com um determinado Modo de Operação.

**SELEÇÃO DE CONTEÚDO – A PRÁTICA**

Um conteúdo mínimo, consistindo de um roteiro de aula para o DES, visando os objetivos acima, pode ser colocada como:

1. Veja sua **Descrição**, **Estrutura Geral**,
2. Use os arquivos no link da Tarefa 2.1 e realize a execução do código correspondente.
3. Identifique no **JCE** (**Java Cryptography Extension**), um conjunto de extensões da [Java](http://pt.wikipedia.org/wiki/Java) [API](http://pt.wikipedia.org/wiki/API) que provê um *framework* para ser utilizado durante a criptografia de dados.
4. Qual o tamanho da chave usada ?
5. O que você pode concluir com este tamanho de chave usado no AES ?
6. Qual o modo de cifra usado ? Poderia existir um modo de cifra para este algoritmo ?

**MOSTRE SEU EXPERIMENTO**

Ao final da aula, deposite sua tarefa no Moodle, no tópico Tarefa 2.1.

O Moodle será fechado a partir de 22:00 na data desta aula. É a comprovação de sua participação na Tarefa 2.1 da disciplina.

**CONCLUSÃO**

* É muito bem adequado a ambientes de espaço restrito. Possui requistos muito baixos de RAM e ROM (se implementado em hardware).
* As funções de criptografia e decriptografia são diferentes.