**PLANO DE AULA PRÁTICA**

**TAREFA 2.1** "Criptografia Simétrica com RC4"

Tópico no Moodle: “Tarefa 2.2 – Criptografia Simétrica com RC4”

Data: 28-03-2014  
  
Tempo de Aula: 2 horas-aula  
  
Grupo: <Aluno\_1> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

# ASSUNTO RC4

**OBJETIVOS DA AULA**

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

1. Cifra de Fluxo

**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** e **Estrutura Geral** nos impressos fornecidos.
2. O que se pode dizer sobre o tamanho da chave usada ?
3. Por que não é desejável reutilizar uma chave de cifra de fluxo ?

Se dois textos claros forem criptografados com a mesma chave, usando

uma cifra de fluxo, então a criptoanálise normalmente será bastante

simples. Se dois fluxos de texto cifrado passarem por uma operação XOR,

o resultado será o XOR dos dois textos claros originais. Se os textos claros

forem strings de texto, números de cartão de crédito ou outros fluxos de

bytes com propriedades conhecidas, então a criptoanálise poderá ter

sucesso.

**MOSTRE SEU EXPERIMENTO**

Ao final da aula, deposite sua tarefa no Moodle, no tópico Tarefa 2.2.

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.
* Ainda pode ser utilizado em SSL (protocolo navegador-servidor web), WEP (redes sem fio) e WPA (redes sem fio).
* Mas, relativamente fácil de se descobrir a chave, via uso de uma ferramenta de análise de tráfego, o que é facilmente realizado para chave WEP.