**ESQUEMA DE PLANO DE AULA PRÁTICA**

**TAREFAS 4a:** "Executando o RSA"

Tópico no Moodle: “Tarefa 4b – Criptografia de Chave Pública com RSA”

Data: 11-04-2014  
  
Tempo de Aula: 2 horas-aula  
  
Grupo: <Aluno\_1> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

**ASSUNTO**

**RSA** é um algoritmo de [criptografia](http://pt.wikipedia.org/wiki/Criptografia) de chave pública, que deve o seu nome a três professores do [MIT](http://pt.wikipedia.org/wiki/Instituto_MIT) (fundadores da actual empresa [RSA Data Security, Inc.](http://pt.wikipedia.org/wiki/RSA_Data_Security,_Inc.)), [Ronald **R**ivest](http://pt.wikipedia.org/wiki/Ronald_Rivest), [Adi](http://pt.wikipedia.org/wiki/Adi_Shamir" \o "Adi Shamir)**[S](http://pt.wikipedia.org/wiki/Adi_Shamir" \o "Adi Shamir)**[hamir](http://pt.wikipedia.org/wiki/Adi_Shamir" \o "Adi Shamir) e [Leonard **A**dleman](http://pt.wikipedia.org/wiki/Leonard_Adleman), que inventaram este algoritmo, a mais bem sucedida implementação de [sistemas de chaves assimétricas](http://pt.wikipedia.org/wiki/Sistemas_de_chaves_assim%C3%A9tricas), e fundamenta-se em [teorias clássicas dos números](http://pt.wikipedia.org/wiki/Teoria_dos_n%C3%BAmeros). É considerado um algoritmo seguro. Foi também o primeiro algoritmo a possibilitar criptografia e assinatura digital, e uma das grandes inovações em [criptografia de chave pública](http://pt.wikipedia.org/wiki/Criptografia_de_chave_p%C3%BAblica), no final dos anos 70.

**BIBLIOGRAFIA BÁSICA**

<http://pt.wikipedia.org/wiki/RSA>

**OBJETIVOS DA AULA**

Conhecer a o algoritmo de criptografia simétrico RSA.

**SELEÇÃO DE CONTEÚDO – A PRÁTICA**

Execute a implementação do RSA em Java, fornecida na página da disciplina.

**RESPONDA AS SEGUINTES QUESTÕES**

1. A maior parte dos produtos que utilizam a criptografia de chave pública, para criptografia e assinaturas digitais, usa o RSA. Que tipo de limitação atual, existe sobre o RSA, nos tempos de hoje, que tem feito surgir outras formas de criptografia (ECC - criptografia de curva elíptica). Existe, um análogo ao acordo de chaves Diffie-Hellman, para cálculo do par de chaves, pública-privada e uma chave secreta compartilhada, para criptografia simétrica.

**CONCLUSÃO**

A **Criptografía de Curvas Elípticas**, ou ***ECC***, das iniciais em inglës *Eliptic Curve Cryptography*, é uma variante da [criptografia assimétrica](http://pt.wikipedia.org/wiki/Criptografia_assim%C3%A9trica) ou de chave pública, baseada na [matemática](http://pt.wikipedia.org/wiki/Matem%C3%A1tica) das [curvas elípticas](http://pt.wikipedia.org/wiki/Curva_el%C3%ADptica). Seus criadores argumentam que a ECC pode ser mais rápida e usar chaves mais curtas do que os métodos antigos—como [RSA](http://pt.wikipedia.org/wiki/RSA) --, e proporcionar ao mesmo tempo um nível de segurança equivalente. A utilização de curvas elípticas em criptografia foi proposta de modo independente por [Neal Koblitz](http://pt.wikipedia.org/w/index.php?title=Neal_Koblitz&action=edit&redlink=1" \o "Neal Koblitz (página não existe)) e [Victor Miller](http://pt.wikipedia.org/w/index.php?title=Victor_Miller&action=edit&redlink=1) em [1985](http://pt.wikipedia.org/wiki/1985).

**MOSTRE SEU EXPERIMENTO**

O Moodle será fechado a partir de 22:00 na data desta aula. É a comprovação de sua participação na Tarefa 4a da disciplina.