PUC-Rio – Departamento de Informática
Cursos: Sistemas de Informação/
Ciência da Computação/
Engenharia da Computação
Disciplina: INF1416 – Segurança da Informação
Prof.: Anderson Oliveira da Silva

Trabalho 2: MySignature

Implementar a classe ***MySignature*** para gerar e verificar a assinatura digital padrão RSA de strings. A classe pode usar os recursos dos provedores criptográficos da JCA, mas o processo de geração e verificação da assinatura digital **não pode utilizar a classe *Signature***.

A classe *MySignature* deve ser implementada obrigatoriamente com os métodos *getInstance*, *initSign*, *update*, *sign*, *initVerify* e *verify* com funcionalidades equivalentes aos respectivos métodos da classe *Signature* da JCA. A classe *MySignature* **não pode herdar** a classe *Signature*. Os métodos obrigatórios devem ser implementados pelo programador. Outros métodos auxiliares podem ser desenvolvidos. Os padrões de assinatura suportados devem ser MD5withRSA, SHA1withRSA, SHA256withRSA, SHA512withRSA.

O programador também deve implementar a classe *MySignatureTest* para testar a classe MySignature. Essa classe deve executar as seguintes funções:

(i) Receber a string e o padrão de assinatura na linha de comando como argumento;
(ii) Gerar o par de chaves assimétricas para gerar e verificar a assinatura digital da string recebida na linha de comando;
(iii) Instanciar e usar os métodos da classe MySignature para gerar e verificar a assinatura digital da string no padrão solicitado;
(iv) Imprimir, na saída padrão, todos os passos executados durante a geração e verificação da assinatura digital;
(v) Imprimir, na saída padrão, o resumo de mensagem (digest) e a assinatura digital no formato hexadecimal.

Ambos os fontes das classes *MySignature* e *MySignatureTest* devem ser enviados como anexo no e-mail com o título *INF1416-Gn: Trabalho 2*, onde *n* identifica o número do grupo.

Prazo de entrega: 20/4/2020 - 23:59h.