



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 implementar obrigatoriamente 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 e nem instanciar um atributo** da 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" (a string do padrão de assinatura é fornecida como argumento do método *getInstance*).

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 **arquivos-fontes das classes** (*MySignature.java* e *MySignatureTest.java*) devem ter um comentário no início identificando os membros do grupo (nome e matrícula) e devem ser submetidos no sistema de EAD da PUC-Rio **por cada membro do grupo**.

Atenção: Não devem ser submetidos arquivos compactados (.ZIP, .RAR, .TGZ e etc).

Prazo de entrega: 13/4/2022 – 13:00h (limite para submissão: 13/4/2022 (23:59h)).