



## **Trabalhos de Laboratório**

1. Construir um programa Java utilizando a JCA que recebe um texto na linha de comando e assina o mesmo. O processo de geração da assinatura e verificação da mesma deve ser feito **sem a utilização da classe Signature**, detalhando-se na saída padrão cada um dos passos executados, inclusive apresentando o digest e a assinatura no formato hexadecimal. O programa fonte deve ser enviado como anexo via e-mail com o título INF1416 – TrabLab 1 – Grupo N, onde N identifica o número do grupo. Prazo de entrega: 08/09/2010.
2. Construir um programa Java utilizando a JCA que não use interface gráfica e que seja executado em uma linha de comando com argumentos, da seguinte forma:

*DigestCalculator*<SP>*TipoDigest*<SP>*Caminho\_ArqListaDigest*<SP>*Caminho\_Arq1*<SP>*Caminho\_Arq2* ... *Caminho\_ArqN*

onde,

*TipoDigest* - Informa o algoritmo de message digest que deve ser utilizado (MD5 ou SHA1).

*Caminho\_ArqListaDigest* - Informa a localização do arquivo que contém uma lista de digests conhecidos para arquivos.

*Caminho\_Arq1 Caminho\_Arq2 ... Caminho\_ArqN* - Informa a localização dos N arquivos que devem ser processados.

<SP> - Caracter espaço em branco.

O arquivo com a lista de digests utiliza o formato ASCII e é formado por zero ou mais linhas formatadas da seguinte maneira:

*Nome\_Arq*<SP>*TipoDigest*<SP>*Digest\_Hex* <EOL>

onde,

*Nome\_Arq* - Informa o nome de um arquivo qualquer, sem informar o caminho.

*TipoDigest* - Informa o tipo de digest conhecido (MD5 ou SHA1).

*Digest\_Hex* - Informa o digest em hexadecimal com base no tipo de digest especificado.

<SP> - Caracter espaço em branco.

<EOL> - Caracteres que marcam o fim de linha.

O programa deve executar o seguinte procedimento:

- 1 - Calcular o digest solicitado do conteúdo de cada um dos N arquivos fornecidos;
- 2 - Comparar os digests calculados com os respectivos digests presentes no arquivo ArqListaDigest, se existirem;
- 3 - Imprimir na saída padrão uma lista com o seguinte formato:

Nome\_Arq1<SP>TipoDigest<SP>Digest\_Hex\_Arq1<SP>(STATUS)  
Nome\_Arq2<SP>TipoDigest<SP>Digest\_Hex\_Arq2<SP>(STATUS)  
.....  
Nome\_ArqN<SP>TipoDigest<SP>Digest\_Hex\_ArqN<SP>(STATUS)

onde:

<SP> - Caracter espaço em branco.

*Nome\_Arq1 .. Nome\_ArqN* - Correspondem aos nomes dos arquivos fornecidos na linha de comando, descartando o caminho.

*TipoDigest* - Corresponde ao tipo de digest fornecido na linha de comando (MD5 ou SHA1).

*STATUS* - Corresponde a um dos status definidos abaixo:

OK = Status do arquivo cujo digest calculado é igual ao digest fornecido no arquivo ArqListaDigest.

NOT OK = Status do arquivo cujo digest não é igual ao digest fornecido no arquivo ArqListaDigest.

NOT FOUND = Status do arquivo cujo digest não foi encontrado no arquivo ArqListaDigest.

4 - Os digests calculados para os arquivos com status NOT FOUND devem ser acrescentados no final do arquivo de lista de digests, mantendo seu formato padrão.

**Observação 1:** O nome do programa executável deve ser DigestCalculator.

**Observação 2:** O código fonte deve ser compilado com o Sun JDK 1.5 ou 1.6.

**Observação 3:** Utilize o método *update(byte[] input, int offset, int len)* da classe *MessageDigest* que atualiza o digest utilizando o array de bytes *input*, iniciando em *offset*.

**Observação 4:** Se os argumentos da linha de comando forem omitidos ou insuficientes para a execução do programa, deve-se imprimir uma mensagem com a orientação de execução e, em seguida, o programa deve ser encerrado.

O programa fonte deve ser enviado como anexo via e-mail com o título INF1416 – TrabLab 2 – Grupo N, onde N identifica o número do grupo. Prazo de entrega: 15/09/2010.