# RELATÓRIO SELEÇÃO PBAD/LABSEC - ETAPA FINAL

Rafael Niederauer Meyer

## - Primeira etapa — obter o resumo criptográfico de um documento.

Nesta primeira etapa, foi utilizada da classe “Resumidor”, que contém o método “resumir”. O método resumir recebe como parâmetro um arquivo a ser processado, sendo ele o “textoPlano.txt” e o transforma em bytes. Assim a classe “MessageDigest” consegue digerir esse número arbitrário de bytes e o transforma em um número fixo de bytes, sendo ele o resumo criptográfico.

## - Segunda etapa — gerar chaves assimétricas.

Na segunda etapa, utilizando o algoritmo de criptografia “ECDSA”, é gerado 2 pares de chaves assimétricas, 1 par de 256 bits para o usuário e o outro par de 512 bits para a “AC-RAIZ”, esses pares de chaves serão usados no futuro para cifrar e decifrar o documento. Após isso, as chaves são armazenadas em disco no repositório destino em formato “PEM”.

## - Terceira etapa — gerar certificados digitais.

A terceira etapa é disposta de gerar certificador digitais. Nela, é criado uma estrutura de certificado com o método “gerarEstruturaCertificado”. Neste método, a estrutura contendo a chave pública do emissor, número de série do certificado, nome do emissor, nome da autoridade certificadora e o número de dias após a criação que este certificado será valido é criada. Após criar a estrutura do certificado, é gerado o valor da assinatura deste, com o método “geraValorAssinatura”, o qual é utilizada a chave privada da autoridade certificadora que emitirá este certificado. Assim, tendo a estrutura do certificado e o valor da assinatura, é gerado o próprio com o método “gerarCertificado”.

Após os métodos preparados para criarem um certificado, dois certificados são originados. Um para a “AC-RAIZ”, assinado por ela mesma e outro para o usuário, assinado pela “AC-RAIZ”.

## - Quarta etapa — gerar repositório de chaves seguro.

Esta etapa serve para gerar um repositório seguro paras os certificados e as chaves assimétricas privadas no formato “PKCS12”.

## - Quinta etapa — gerar uma assinatura digital.

Nesta quinta etapa, uma assinatura digital é gerada a partir do resumo criptográfico feito na primeira etapa (no enunciado é pedido para assinar o documento “textoPlano.txt”, porém na teoria diz para gerar o resumo criptográfico dos dados e depois utilizar a chave privada para assiná-lo). Assim, o usuário (no caso eu), assina os dados com o certificado e com a chave privada (retiradas do repositório “PKCS12”). Após assinado, a assinatura é escrita em disco.

## - Sexta etapa — verificar uma assinatura digital.

A última etapa serve para verificar a assinatura digital. Nela, de um jeito mais simples que a “vida real”, basta decifrar o valor da assinatura usando a chave pública do assinante e comprar com o valor do resumo criptográfico da primeira etapa.