



Trabalho de Segurança da Informação – SIN

Prof. Pedro Carlos da Silva Lara

pcslara@lncc.br

home page: www.lncc.br/~pcslara

Instituto Superior de Tecnologia em Ciência da Computação de Petrópolis

Data limite da entrega: 29/10/2013

Neste trabalho, o aluno irá rever, na prática, os conceitos de criptografia simétrica, assimétrica e funções de hash através de criação e manipulação de assinaturas digitais, certificados digitais e HMAC. Será usado o *software* livre e *opensource* de linha de comando **OpenSSL**. O trabalho será dividido em 4 itens. **Assinatura Digital, Certificado Digital, Criptografia Assimétrica e HMAC**. Para isso o aluno deverá gerar um par de chaves pública/privada **RSA** com **1024** bits.

Item 1: O aluno deverá criar um arquivo txt nomeado **name.txt** contendo o seu nome e turno. Por exemplo, um arquivo válido seria:

Pedro Carlos da Silva Lara - Manhã

Após isso, o arquivo **name.txt** será assinado usando a chave RSA gerada anteriormente. Esta assinatura deverá seguir o padrão DSS (*Digital Signature Standard*) usando o hash SHA-1 (*Secure Hash Algorithm 1*) e o algoritmo de assinatura RSA. Os nomes dos arquivos deverão ser: **priv_key.pem** (chave privada), **pub_key.pem** (chave pública), **name.txt.dss** (assinatura digital).

Item 2: O aluno deverá gerar um certificado digital. Neste caso, a autoridade certificadora será um o próprio aluno. Ou seja, será um certificado auto-assinado. Este certificado deverá ser entregue no formato **.pem** (**cert.pem**). Deverá ser utilizada a mesma chave do item anterior. Este certificado deverá seguir o padrão X.509.

Item 3: O aluno deverá criptografar o arquivo **name.txt** com a seguinte chave pública:

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC6sCdsV0v7bid7xfAQPbpfiORI
pgSn3auje36kSYJYbJdJP+jizEytK0ynKc2Igz11amZAhuHWBnMkLoiZ55WvHZCF
12miNewMQ6Bx+piHpdfcKVjdpEA4Frb07H7nL8CHGrRTwwilWfW5vdxk3R6yu8Sm
OcCTPldZb7HMxh73TwIDAQAB
-----END PUBLIC KEY-----
```

Tendo como saída o arquivo **name.txt.rsa**.

Item 4: Calcular o HMAC (Hash based Message Authentication Code) do arquivo **name.txt** usando como chave secreta o seguinte arquivo

"Time flies like an arrow"

e o hash SHA-2. O resultado será **name.txt.hmac**.

O aluno deverá pesquisar o funcionamento da ferramenta **OpenSSL** para resolver os itens deste trabalho. Na data da entrega o aluno irá apresentar todos os arquivos e os comandos utilizados. O trabalho é individual e vale **2,00 pontos** para a N_1 .