UNIVERSIDADE FEDERAL DO PIAUÍ – UFPI
CENTRO DE CIÊNCIAS DA NATUREZA – CCN
DEPARTAMENTO DE COMPUTAÇÃO
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

Disciplina: ***Segurança em Sistemas Computacionais***
Professor da disciplina: ***Carlos André Batista de Carvalho***

Trabalho 01 – Implementação de um programa de assinatura digital

- Atividade em grupo (até 3 alunos)
- A linguagem de programação utilizada é livre
- É permitido/recomendado o uso de bibliotecas de criptografia (ex. bouncycaslte e pycrypto)
- Funções implementadas
    - Assinar um texto com RSA e SHA
        - Entrada: texto em claro + chave da assinatura (privada) + versão do SHA
        - Processamento: Gerar hash (em hexadecimal e cifrar o hash como se o resultado em hexadecimal fosse um texto em claro/ASCII)
        - Saída: texto da assinatura (notação base64)
    - Verificar assinatura
        - Entrada: texto em claro + chave de verificação (pública) + texto da assinatura (base64) + versão do SHA
        - Saída: Verdadeiro ou Falso
    - Geração de chaves compatível com o padrão openssl
      Trecho da chaves (modo texto)

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCkMqJJLrxXQz9e
r6oMx21wkOgY3P1WFb9dvuBxK+/EUn/Jri7dsLfBv/eS2fUZBsmGyfqwSdJNYwNP
dFrNqgwYq00n53+f5V6sKNEhKWXN7a0OJm9yrc4YXXuyKKgzXPh5Rff7droj/xUF
-----END PRIVATE KEY-----
-----BEGIN PUBLIC KEY-----
dFrNqgwYq00n53+f5V6sKNEhKWXN7a0OJm9yrc4YXXuyKKgzXPh5Rff7droj/xUF
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCkMqJJLrxXQz9e
r6oMx21wkOgY3P1WFb9dvuBxK+/EUn/Jri7dsLfBv/eS2fUZBsmGyfqwSdJNYwNP
-----END PUBLIC KEY-----
```

- Envio de instruções para execução do programa e do código fonte

OBS: Um dos propósitos do trabalho é que a implementação funcione como um protocolo, de modo que seja possível criar chaves, assinar ou verificar assinaturas por outros programas. Diante disso foi estabelecido que a notação de entrada/saída usada em cada algoritmo, permitindo não apenas a "legibilidade" dos resultados. Além disso, é necessário permitir o uso de versões diferentes do SHA, simulando a flexibilidade de alguns protocolos.