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 o uso de bibliotecas de criptografia (ex. bouncycaslte e pycrypto)
- Funções implementadas
    - Assinar um arquivo ou um texto
        - Entrada: arquivo/texto em claro + chave da assinatura (privada)
        - Saúda: arquivo/texto com a assinatura
    - Verificar assinatura
        - Entrada: arquivo/texto em claro + chave de verificação (pública) + arquivo/texto com a assinatura
        - Saúda: Verdadeiro ou Falso
    - Geração de chaves

Toda cifra assimétrica incluí um processo para criar a chave pública e a privada.

- Algoritmos criptográficos (exemplos)
    - Assimétrico: RSA
    - Função Hash: SHA
- Envio de instruções para execução do programa e do código fonte

OBS: Cuidado com a formatação da assinatura, pois o formato pode não ser legível e inviabilizar que seja fornecido como entrada da decifragem. Opções de notação: hexadecimal ou base64.