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: Envelope Digital

- Atividade em grupo (até 3 alunos)
- A linguagem de programação utilizada é livre
- É recomendado o uso de bibliotecas de criptografia
- Funções implementadas
  - Criar um envelope
    - Entrada: arquivo em claro + arquivo da chave RSA pública do destinatário + algoritmo simétrico (AES / DES / RC4)
    - Processamento: Gerar chave simétrica temporária/aleatória. Cifrar arquivo em claro com a chave gerada. Cifrar a chave temporária com a chave do destinatário.
    - Saída: dois arquivos (um com a chave assinada e outro do arquivo criptografado).
  - Abrir um envelope assinado
    - Entrada: arquivos com a mensagem e a chave criptografada + arquivo da chave RSA privada do destinatário + algoritmo simétrico (AES / DES / RC4)
    - Processamento: Decifrar a chave temporária com a chave do destinatário. Decifrar arquivo em claro com a chave obtida.
    - Saída: arquivo decifrado.

  - 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. Além disso, é necessário permitir o uso de diferentes algoritmos, simulando a flexibilidade de alguns protocolos.
O programa deve permitir que o usuário informe o nome dos arquivos de entrada e/ou saída.