Primeira Avaliação - Tópicos III

Entrega: 30/05/2018

1. Implemente o esquema de criptografia RSA.

   - **Aplicação de criptografia:** O usuário entra com um texto (.txt) e uma chave pública. A aplicação devolve um texto (.txt) criptografado através do esquema de criptografia RSA.
   - **Aplicação de decriptografia:** O usuário entra com um texto (.txt criptografado) e sua chave privada. A aplicação devolve um texto (.txt) decriptografado.

2. Implemente a assinatura digital via RSA.

   - **Aplicação de assinatura:** O usuário entra com um texto (.txt) e com sua chave privada. A aplicação devolve a assinatura do usuário sobre o texto (outro .txt).
   - **Aplicação de verificação da assinatura:** O usuário entra com um texto (.txt), entra com uma assinatura sobre tal texto (.txt) e entra com a chave pública de quem assinou. A aplicação devolve SIM (a assinatura é válida) ou NÃO (a assinatura não é válida).

3. Implemente o esquema de distribuição de Diffie-Hellman. Vamos supondo que A deseja enviar uma "mensagem" m para B, e que exista uma chave pública (p, α), onde p é um número primo grande e α é um gerador de $\mathbb{Z}_p$

   - **Aplicação de criptografia:** O usuário A entra com um texto (.txt) e entra com um segredo criptografado y_B de B (o usuário A entra com $y_B = \alpha^{x_B}$ que depende do segredo x_B de B). A aplicação devolve o par (c_1, c_2), onde
     - $c_1 \equiv \alpha^t (\text{mod } p)$, onde t é um número inteiro escolhido ao acaso em $\{0, 1, \ldots, p-1\}$; e
     - $c_2 \equiv Km (\text{mod } p)$, onde $K \equiv (y_B)^t (\text{mod } p)$.
   - **Aplicação de decriptografia:** O usuário B entra com o par (c_1, c_2) e decriptografa a mensagem fazendo
     - $K \equiv c_1^{x_B} (\text{mod } p)$ (encontrando K); e
     - $m \equiv K^{-1} c_2 (\text{mod } p)$ (aplicando o inverso de K sobre m).