

Universidade Tecnológica Federal do Paraná (UTFPR)
Departamento Acadêmico de Informática (DAINF)
Introdução à Criptografia
Professor: Rodrigo Minetto

Lista de exercícios (escolha três exercícios para entregar)

1) Suponha um esquema de assinatura por RSA com a chave pública $k_{pub} = (e = 131, n = 9797)$, quais das seguintes assinaturas são válidas?

- assinatura(x) = 6292 e $x = 123$;
- assinatura(x) = 4768 e $x = 4333$;
- assinatura(x) = 1424 e $x = 4333$;

2) Suponha que Alice deseja enviar uma mensagem criptografada e assinada para Bob através do esquema RSA. Descreva os passos para que Alice consiga realizar essa tarefa.

3) Suponha os seguintes dados: chave pública e privada de Alice $ka_{pub} = (e = 14641, n = 127273)$ e $ka_{priv} = (d = 28369, n = 127273)$, chave pública e privada de Bob $kb_{pub} = (e = 38651, n = 135379)$ e $kb_{priv} = (d = 57251, n = 135379)$ e o texto cifrado E assinado (nessa ordem) por Alice $y = 51859$. Qual o texto em claro para Bob?

4) Um outro jeito de trabalhar com chave pública e privada é conforme definido no gpg (gnu privacy guard). Leia, pratique e discuta como seria esse esquema. Pergunta: existe autoridade certificadora nesse esquema?

<https://www.digitalocean.com/community/tutorials/how-to-use-gpg-to-encrypt-and-sign-messages>

<https://cran.r-project.org/web/packages/gpg/vignettes/intro.html>

5) Discuta como é feita as assinaturas na plataforma sougov. Onde são armazenadas as chaves privadas?