Universidade Tecnológica Federal do Paraná (UTFPR)
Departamento Acadêmico de Informática (DAINF)

Introdução à Criptografia

Professor: Rodrigo Minetto

Lista de exercícios

1) Jogo da verdade: faça algumas perguntas de verdadeiro ou falso para o seu colega e associe números a elas. Por exemplo:

- Você almoçou no RU hoje? (x = 345)
- Você irá se formar em 4 anos? (x = 800)
- Você tem carro? (x = 128)

Troque com o seu colega somente sua chave pública (para facilitar você pode fazer todo esse processo pelo http://dontpad.com/). Se a assinatura for válida significa verdadeiro para a sua pergunta, se a assinatura for inválida (você pode forjar um valor para a assinatura) significa falso (troque os papéis ao final).

2) Suponha um esquema de assinatura por RSA com a chave pública $k_{pub} = (e = 131, n = 9797)$, quais das seguintes assinaturas são válidas? (**questão 10.5 do livro texto**)

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

3) 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.

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

5) 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. Pegunta: 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`