

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

**Introdução à Criptografia**

Professor: Rodrigo Minetto

## Lista de exercícios

1) Calcule as expressões abaixo **SEM** utilizar uma calculadora. Dica: utilize, se necessário, a decomposição rápida do expoente.

- (a)  $2 \times 5 \bmod 13$
- (b)  $2 \times 29 \bmod 13$
- (c)  $20 \times 29 \bmod 13$
- (d)  $-11 \times 3 \bmod 13$
- (e)  $3^2 \bmod 13$
- (f)  $7^2 \bmod 13$
- (g)  $3^{10} \bmod 13$
- (h)  $5^{-1} \bmod 13$
- (i)  $5^{-1} \bmod 7$

2) Nesse exercício você irá combinar uma chave com um colega na sala por e-mail (e somente por e-mail) utilizando o protocolo DHKE (qualquer conversa pessoal sobre dados necessários para a troca de chaves não é permitida). Esse exercício é MUITO importante pois ele mostra um aspecto bem inconveniente do DHKE. Para realizá-lo primeiramente codifique o algoritmo DHKE para facilitar os cálculos. Primeiramente escolha um número primo de 6 dígitos que será utilizado na comunicação e ache um número  $q$  aleatoriamente no intervalo de  $\{2, \dots, p - 2\}$ . As chaves privadas podem ser achadas da mesma maneira que o valor  $q$ . Note que você pode testar o programa localmente antes de iniciar a comunicação para ver se está tudo funcionando.

Primos com 6 dígitos:

<https://primes.utm.edu/curios/index.php?start=6&stop=6>

.

3) Suponha que  $y = q^x \bmod n$ . Indique o valor de  $y$  e tempo de execução dos algoritmos para exponenciação modular Naive, Improved e Square-Mult para os seguintes valores:

- $q = 5$ ,  $x = 6$  e  $n = 23$ .
- $q = 5$ ,  $x = 15$  e  $n = 23$ .
- $q = 5$ ,  $x = 36$  e  $n = 97$ .
- $q = 5$ ,  $x = 58$  e  $n = 97$ .
- $q = 98$ ,  $x = 1000000000$  e  $n = 65$ .

4) Neste exercício vamos testar a confiabilidade do DHKE. Suponha que Eva interceptou as seguintes informações:

- $p = 211$ ,  $q = 199$ ,  $A = 58$  e  $B = 171$ . Qual a chave trocada entre Alice e Bob?
- $p = 6547$ ,  $q = 5747$ ,  $A = 4571$  e  $B = 2393$ . Qual a chave trocada entre Alice e Bob?
- $p = 12889$ ,  $q = 260$ ,  $A = 4176$  e  $B = 6598$ . Qual a chave trocada entre Alice e Bob?