MAC-0332 - 5723 - Criptografia e Segurança de Dados 2019 - Lista de exercícios 2

- prazo de entrega: veja no paca.ime.usp
- resolver *individualmente*
- entregue as suas soluções no sistema PACA, em formato PDF
- MANUSCRITOS não serão corrigidos
- escreva no cabeçalho o seu NUSP e nome completo

Exercício 1 (25%) Dados n como no algoritmo RSA, e $\Phi(n)$, como entradas, projetar um algoritmo *rápido* para fatorar n. Demonstrar que é rápido e correto.

Exercício 2 (25%) Aplicar o Algoritmo de Miller e Rabin para calcular e escrever os valores de $t, c, r_0, r_1, ...r_t$ e verificar se a resposta final é correta ou não, para os seguintes inteiros:

1. $n = 21$, $a = 5$
2. $n = 13$, $a = 2$

Exercício 3 (25%) Exercício 4 na página 267 do livro-texto.

Exercício 4 (25%) Exercício 5 na página 267 do livro-texto.