CIC0201 - Segurança Computacional – 2024/2

Disciplina: Segurança Computacional

Professora: Lorena Borges

Lista de Exercício 02

Ex1: Realize a encriptação e decriptação usando o algoritmo RSA, para o seguinte:

a. $p = 3$; $q = 11$, $e = 7$; $M = 5$

b. $p = 5$; $q = 11$, $e = 3$; $M = 9$

c. $p = 7$; $q = 11$, $e = 17$; $M = 8$

d. $p = 11$; $q = 13$, $e = 11$; $M = 7$

e. $p = 17$; $q = 31$, $e = 7$; $M = 2$

Ex2: Em um sistema de chave pública usando RSA, você intercepta o texto cifrado $C = 10$ enviado a um usuário cuja chave pública é $e = 5$, $n = 35$. Qual é o texto claro M?

Ex3: Realize a encriptação e decriptação RSA da mensagem binária m = 0111001. Considere p = 11, q = 23, e = 3.

Ex4: Utilizando a codificação ASCII, realize a encriptação e decriptação RSA da mensagem "HELLO" Primos: p=11, q=17 Chave Pública: e=7