Exercícios sobre Criptografia de Chave Pública

Exercício 1

Criptografia RSA. Execute a criptografia e a descriptografia 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 = 11; q = 13, e = 11; M = 7.

Exercício 2

Criptografia RSA. Em um sistema de chave pública usando RSA, você intercepta o texto cifrado C = 10 enviado para um usuário cuja chave pública é e = 5, n = 35. Qual é o texto simples M?

Exercício 3

Criptografia RSA. Em um sistema RSA, a chave pública de um determinado usuário é e = 31, n = 3599. Qual é a chave privada desse usuário?

Exercício 4

Função hash. Suponha que H(m) seja uma função hash resistente à colisão que mapeia uma mensagem de comprimento de bit arbitrário em um valor de hash de n bits. É verdade que, para todas as mensagens x, x' com $x \neq x'$, temos $H(x) \neq H(x')$? Explique sua resposta.