Lista de exercícios: RSA

1. Sejam dois primos $p = 41$ e $q = 17$ usados em um esquema RSA simplificado.

- Qual dos parâmetros $e_1 = 32$ ou $e_2 = 49$ é um expoente RSA válido? Justifique.
- Compute a chave privada correspondente $K_{priv} = (p, q, d)$. Use o algoritmo de Euclides extendido para a inversão.

2. Compute as seguintes exponenciações $x^e \mod m$ com o algoritmo "elevar ao quadrado e multiplicar":

- $x = 2, e = 79, m = 101$
- $x = 3, e = 197, m = 101$

3. Encripte e decripte usando o algoritmo RSA com os seguintes valores:

- $p = 3, q = 11, d = 7, x = 5$
- $p = 5, q = 11, e = 3, x = 9$

4. Para acelerar os cálculos do RSA os números 3, 17 e $2^{16} + 1$ são muito usados como expoentes públicos. Porquê? Seria possível usar também como sendo o expoente d?

5. Escreva um pseudo-código para gerar números primos.

6. Explique como funciona o teste de primalidade de Fermat.

7. Explique como funciona o teste de primalidade de Miller-Rabin.

8. Considere o esquema simplificado da encriptação RSA em chave pública igual a $(n = 55, e = 3)$.

- Quantos elementos estão em $\mathbf{Z}_{55}^*$?
- Compute o expoente privado d.
- Compute a encriptação da mensagem $m = 6$.
- Compute a decriptação do texto cifrado $c = 2$.

9. O que é o PKCS#1?

10. Como funciona o padding no PKCS#1 v1.5?

11. Como funciona o padding OEAP? Com sua relação com RSA-FDH (Full Domain Hash) ?