Rede de Computadores

Lista de Exercícios Nº 3 - Semestre 2016.2
Prazo final para entrega: 26/05/2017
Prof.: Edmar José do Nascimento

1. Explique a diferença entre os sistemas de criptografia simétrica e assimétrica.

2. Por que se recorre a uma criptografia simétrica como o AES ao invés de se usar uma criptografia assimétrica como o RSA em todo o processo de criptografia?

3. Qual é o papel de uma autoridade certificadora no processo de criptografia? Quais são os riscos de se usar uma chave não certificada?

4. Para que serve uma função de *hash*? Em que consiste uma colisão para uma função de *hash*?

5. Por que se usa um vetor de inicialização (IV) diferente para cada sessão em um encadeamento de cifras de bloco (CBC)?

6. Gere um par de chaves pública e privada usando RSA com os números primos $p = 13$ e $q = 17$.