Lista de Exercícios: Criptografia Assimétrica

Prof. Gabriel Rodrigues Caldas de Aquino

Compilado em:
October 31, 2026

1 Criptografia Simétrica vs. Assimétrica

Compare criptografia simétrica e assimétrica em termos de:

1. Distribuição de chaves.
2. Aplicações de criptografia simétrica e assimétrica.
3. Assim como a criptografia simétrica, é correto afirmar que a criptografia assimétrica pode estar suscetível a ataques de criptoanálise e força bruta?
4. Explique por que sistemas práticos frequentemente usam ambos os tipos de criptografia.

2 RSA

Para aplicações do RSA precisamos escolher dois números primos. Dado os seguintes números:

$$p = 17, \quad q = 11$$

faça:

1. Calcule n e $\varphi(n)$.
2. Escolha $e = 7$ e calcule d tal que $e \cdot d \equiv 1 \pmod{\varphi(n)}$. Mostre os passos que você utilizou para encontrar (pode usar o algoritmo de euclides extendido ou outra forma).
3. Encripte $M = 88$ usando a chave pública (e, n) e mostre a decriptação com d.

3 Segurança do RSA

1. Como a dificuldade de fatoração se relaciona com a segurança do RSA?
2. Qual é o efeito de se utilizar um valor n pequeno no RSA?
3. Uma vez que o valor de $\varphi(n)$ seja conhecido, podemos dizer que a segurança do RSA foi comprometida? Justifique.

4 Diffie–Hellman

Considere o protocolo Diffie–Hellman com os parâmetros públicos:

$$q = 467, \qquad \alpha = 2$$

(ou seja, q é primo e α é uma base primitiva modulo q).

1. Escolham dois expoentes privados inteiros X_A e X_B. Escreva e justifique os valores escolhidos.
2. Para cada participante da comunicação, calcule os valores Y públicos de cada participante:

   $$Y_A \equiv \alpha^{X_A} \bmod q, \qquad Y_B \equiv \alpha^{X_B} \bmod q.$$

   Apresente os cálculos
3. Supondo que Y_A e Y_B sejam trocados publicamente, calcule a chave secreta comum K usando cada um dos lados e verifique que ambos obtêm o mesmo valor:

   $$K_A \equiv Y_B^{X_A} \bmod q, \qquad K_B \equiv Y_A^{X_B} \bmod q.$$

   Mostre os cálculos e verifique $K_A = K_B$.

5 Segurança do Diffie-Hellman

1. Explique por que um atacante que conheça apenas q, α, Y_A, Y_B não consegue, de forma prática, obter K
2. Em aplicações práticas, qual o problema de se escolher um valor pequeno em q. Justifique com base no conceito de função de mão única.
3. É correto afirmar que o diffie-Hellman é sucetível a ataques do tipo man-in-the-middle? Descreva uma forma de mitigar esse problema caso ele exista.

6 Aplicações da Criptografia Assimétrica

A criptografia assimétrica é amplamente utilizada em diversas aplicações reais de segurança da informação.

1. Cite duas aplicações práticas do uso de criptografia assimétrica e justifique.
2. Descreva o cenário em que cada uma dessas aplicações é preferível.

Considerando aplicações de criptografia assimetrica, faça:

1. Explique o papel das chaves pública e privada nas seguintes aplicações, indicando **quem usa qual chave** e **para quê**:
   (a) Assinatura digital.
   (b) Autenticação de usuários ou servidores (por exemplo, em SSH ou HTTPS).
   (c) Confidencialidade de mensagens.
2. Descreva como os **certificados digitais** garantem a autenticidade das chaves públicas em sistemas como HTTPS. Indique:
   - quem emite o certificado,
   - o que é assinado dentro dele,
   - e por que o navegador confia nessa assinatura.
3. A criptografia assimétrica é usada na **troca de chaves** (por exemplo, no início de uma conexão TLS). Explique como a combinação dos dois tipos de criptografia (assimétrica + simétrica) pode ser usada em um cenário real.
4. Em uma frase, resuma a principal diferença entre o uso da criptografia assimétrica para **autenticação** e para **confidencialidade**.