Lista de exercícios: Distribuição de chaves

1. Como chaves podem ser estabelecidas de maneira eficiente e segura com criptografia simétrica? Quantas chaves devem existir ao todo?

2. Como chaves podem ser estabelecidas de maneira eficiente e segura com criptografia assimétrica? Quantas chaves devem existir ao todo?

3. Quais são os problemas de segurança relacionados com distribução de chaves com criptografia assimétrica?

4. O que são e como funcionam esquemas de estabelecimento de chaves baseados em transporte?

5. O que são e como funcionam esquemas de estabelecimento de chaves baseados em concordância/negociação?

6. Qual é o papel de um centro de distribuição de chave (key distribution center)? O que é uma chave de encriptação de chaves (Key Encryption Key - KEKs)?

7. Apresente com detalhes o ataque Man-in-the-Middle.

8. O que são certificados e como eles são usados?

9. Como funciona a troca de chaves de Diffie-Hellman com certificados?

10. Apresente o modelo de confiança Roots of trust.

11. O que e como são certificados X.509?

12. Apresente o modelo de confiança Web of trust.

13. Apresente 5 motivos diferentes para fazer revocação de certificados.