Lista de exercícios: Hash

1. Defina uma função hash criptográfica.

2. Explique as propriedades necessárias para uma hash criptográfica ser considerada segura.

3. O que é o ataque de aniversário?

4. Descreva o funcionamento da função SHA-1.

5. Escreva um texto para explicar para pessoas leigas como funções hash funcionam.

6. Porque funções hash são usadas no arquivo /etc/shadow de sistemas operacionais Unix ? Assuma que você é um intruso em um sistema Unix e obteve esse arquivo, descreva as consequências se ser capaz de realizar cada um dos seguintes ataques:

- Quebrar a propriedade de "uma via" da função hash
- Encontrar colisões

Qual é a quantidade mínima de bits que essa função hash deve ter? Porque?

7. Porque usar valores aleatórios (*salt*) junto à senha de usuários para calcular funções hash aumenta a segurança?

8. Computar a saída do primeiro turno do estágio 1 do SHA-1 para uma entada de 512 bits contendo

- $x = \{0, \ldots, 0\}$
- $x = \{0, 0, 0, \ldots, 0, 1\}$

Considere que valor inicial H_0 0.

9. Considere funções hashes com 64, 128 e 160 bits de saída. Quantas entradas aleatórias devem ser testadas para obter $\epsilon \in \{0.1, 0.5, 0.9\}$ probabilidade de colisão?

10. Escreva um algoritmo para encontrar um par de entradas x_1 e x_2 tal que $h(x_1) = h(x_2)$ para uma dada função $h(\cdot)$. Qual é a complexidade de espaço necessária para entradas de n bits?

11. Porque funções de hash usadas em tabelas hash não são boas função de hash para criptografia?

12. Explique como funciona a construção de Merkle-Damgard.

13. O que é uma função de compressão de Davies-Meyer?

14. Sendo $E(a, b)$ uma cifra que usa a como chave para criptografar uma mensagem b. Defina uma função hash da forma $h(H, m) = E(m, H)$.

Qual alternativa a seguir descreve uma maneira achar uma colisão de pares (H, m) e (H', m') definindo aleatoriamente (H, m, m') para essa função hash? Explique.

- $H' = D(m', E(m, H))$
- $H' = E(m', D(m, H))$
- $H' = E(m', E(m, H))$
- $H' = D(m', D(m, H))$

15. Qual é a relação entre funções hash e códigos de autenticação de mensagens?