Universidade Tecnológica Federal do Paraná (UTFPR)
Departamento Acadêmico de Informática (DAINF)

Introdução à Criptografia

Professor: Rodrigo Minetto

Lista de exercícios (escolha 5 para entregar)

---

1) Cara ou coroa: suponha que Alice e Bob queiram resolver uma disputa por cara e coroa. Se eles estão fisicamente no mesmo lugar, o procedimento típico é:

- Alice escolhe um lado da moeda;
- Bob joga a moeda;
- Se Alice acertar o lado que vira ela vence, senão Bob vence.

O problema acontece caso eles não estejam no mesmo no lugar (por exemplo, ambos travam a disputa por telefone), pois Bob pode enganar Alice quanto ao lado da moeda que virou. Mostre um procedimento que permita a ambos confiar no resultado. Teste a sua solução com um colega via http://dontpad.com (um joga a moeda e nenhum dos dois consegue trapacear, mesmo um não vendo a moeda).

---

2) Use uma ferramenta ou biblioteca para calcular o hash SHA-256 das seguintes strings:

1. "senha123"
2. "Senha123"
3. "senha1234"

O que você observa?

---

3) Suponha que alguém encontrou duas mensagens diferentes com o mesmo hash SHA-256.

- Por que isso representa um risco para assinaturas digitais?
- Por que usamos SHA-256 e não MD5 ou SHA-1?

4) Um computador calcula 1 bilhão de hashes SHA-256 por segundo. Quantos segundos seriam necessários (em média) para encontrar uma colisão por ataque de aniversário?

---

5) Dado o hash:

ef92b778bafe771e89245b89ecbc5c1c6e27f7d21aa5c6d44258d14c54e3f9d0

Sabendo que foi gerado de uma senha de até 8 letras minúsculas, como você tentaria descobrir a senha?

---

6) Liste cinco aplicações de funções de hash e explique o papel delas.

---

7) Você baixou um arquivo e o site forneceu o hash SHA-256.

- Como verificar integridade?
- O que acontece se 1 byte mudar?

---

8) Explique o papel das funções hash no processo de mineração de Bitcoin.

---

9) Mostre como um Merkle Tree utiliza funções de hash para verificar a integridade de um grande conjunto de dados.

---

10) Por que o uso de salt torna o armazenamento de hashes de senha mais seguro? Explique a diferença entre usar e não usar salt.