Resumo: Criptografia - Pontos Essenciais para Prova

1. Definição e Conceitos Básicos

O que é Criptografia?

- **Definição**: Escrita (grafia) Secreta (cripto)
- **Objetivo**: Esconder a informação daqueles a quais a informação não se destina
- **Aplicação**: Solução tecnológica para problemas de segurança em computação e comunicação

Terminologia Importante

- **Plain Text/Clear Text**: Texto claro/plano/aberto - conteúdo legível para todos
- **Ciphered Text/Encrypted Text**: Texto encriptado/criptografado/cifrado - resultado da criptografia
- **Chave**: Elemento utilizado pelo algoritmo para criptografar as informações

Princípio de Kerckhoff (1883)

> ***"A segurança de um criptossistema não deve depender da manutenção de um criptoalgoritmo em segredo. A segurança depende apenas de se manter em segredo a chave."***

---

2. Objetivos da Criptografia (4 Pilares)

□ Confidencialidade

- Apenas as partes comunicantes devem interpretar o conteúdo da mensagem

□ Integridade

- A mensagem não deve ser modificada durante a transmissão

□ Autenticidade

- O destinatário deve garantir que o autor da mensagem foi o remetente esperado

□ Não-repúdio

- O remetente não deve poder negar a autoria da mensagem

> ***Importante**: Esses objetivos não precisam ser atingidos todos simultaneamente - dependem da necessidade.*

---

3. Tipos de Ameaças à Comunicação

Tipos de Ataques

1. **Interceptação**: Adversário captura a mensagem
2. **Interrupção**: Bloqueio da comunicação
3. **Modificação**: Alteração do conteúdo da mensagem
4. **Fabricação**: Criação de mensagens falsas

---

4. Criptografia Simétrica (Chave Secreta)

Características

- **Uma única chave** para cifrar e decifrar
- **Mesma chave** compartilhada entre emissor e receptor
- Requer **canal seguro** para troca de chaves

Vantagens

- □ **Rapidez** na criptografia e descriptografia
- □ **Privacidade segura**

Desvantagens

- □ Chave deve ser trocada de forma segura
- □ Não garante identidade do remetente
- □ **Problema de escalabilidade**: Para n pessoas = n(n-1)/2 chaves

Exemplos de Algoritmos

- **AES** (Advanced Encryption Standard) - Simétrico
- **3DES** (Data Encryption Standard) da IBM - Simétrico

Tabela de Gerenciamento de Chaves

Participantes	Chaves Necessárias
2	1
4	6
8	28
16	120

---

5. Criptografia Assimétrica (Chave Pública)

Características

- **Par de chaves**: pública e privada
- **Chave pública**: divulgada livremente
- **Chave privada**: mantida em sigilo
- **Cifragem**: com chave pública
- **Decifragem**: com chave privada

Vantagens

- □ Não compartilha segredo
- □ Provê autenticação
- □ Provê não-repúdio
- □ **Escalável**: Para n pessoas = 2n chaves

Desvantagens

- □ **Lenta** (computacionalmente intensiva)
- □ Requer autoridade de certificação

Comparação de Escalabilidade

Participantes	Simétrica	Assimétrica
2	1	4
4	6	8
8	28	16
16	120	32

Exemplos de Algoritmos

- **RSA** (Ronald Rivest, Adi Shamir e Leonard Adleman)

- **Diffie-Hellmann** (Whitfield Diffie e Martin Hellman)

---

6. Tipos de Segurança com Criptografia Assimétrica

Configurações de Chaves

Codificação	Decodificação	Segurança Fornecida
Pública de A	Privada de A	Integridade e Confidencialidade
Privada de A	Pública de A	Autenticação e Não-repúdio
Pública B + Privada A	Pública A + Privada B	**Todos os 4 objetivos**

---

7. Autoridade Certificadora (CA)

Problema

- Como saber se a chave pública realmente pertence ao usuário desejado?

Solução

- **Certificação das Chaves** por uma autoridade confiável
- **Autoridade Certificadora**: Entidade que certifica a autenticidade das chaves públicas
- O transmissor deve possuir a chave pública do certificador

Componentes do Certificado

- Chave pública a ser certificada
- Identificação do proprietário
- Assinatura eletrônica da CA

---

8. Assinatura Digital

Definição

- **Identifica o transmissor** e fornece mecanismos para **verificar a integridade**
- Valor numérico função de:
    - Conteúdo do documento
    - Chave do transmissor

Características

- Combinação de **criptografia assimétrica** + **funções de hashing**
- Garante **autenticidade** e **integridade**

Verificação da Integridade

1. Receptor recalcula a assinatura digital
2. Aplica mesmo algoritmo com mesma chave na mensagem recebida
3. Se assinatura calculada = recebida → mensagem íntegra

---

9. Funções de Hashing

Definição

- Gera **código de tamanho fixo** (hash/message digest) a partir de mensagem de qualquer tamanho

Propriedades Essenciais

1. **Consistente**: Mesma mensagem → mesmo hash
2. **Aleatória**: Evita adivinhar a mensagem original
3. **Única**: Probabilidade infinitesimal de colisão
4. **Unidirecional**: Impossível determinar informação original a partir do hash

Exemplos de Algoritmos

- **MD5** (Message Digest 5): 128 bits - Ron Rivest (MIT)
- **SHA** (Secure Hash Algorithm): 160 bits - NIST

Uso em Segurança

- **Adição simples de hash**: NÃO garante integridade
- **Garantia de integridade**: Hash + assinatura digital (criptografar hash con chave privada)

---

10. Pontos de Atenção para a Prova

Fórmulas Importantes

- **Criptografia Simétrica**: n(n-1)/2 chaves
- **Criptografia Assimétrica**: 2n chaves

Conceitos Críticos

1. **Princípio de Kerckhoff**: Segurança na chave, não no algoritmo
2. **4 Objetivos**: Confidencialidade, Integridade, Autenticidade, Não-repúdio
3. **Diferenças Simétricas vs Assimétricas**: Velocidade vs Escalabilidade
4. **Papel da CA**: Certificação de chaves públicas
5. **Assinatura Digital**: Hash + Criptografia assimétrica

Exemplos Históricos

- **Máquina Enigma (1919)**: Baseada em rotores, usada pelos alemães na Segunda Guerra
- **Importância das chaves**: Quebra da Enigma pelos Aliados

Dicas de Estudo

- Foque nas **diferenças práticas** entre simétrica e assimétrica
- Memorize as **fórmulas de quantidade de chaves**
- Entenda o **papel das funções de hash** na assinatura digital
- Pratique **cenários de uso** para cada tipo de criptografia