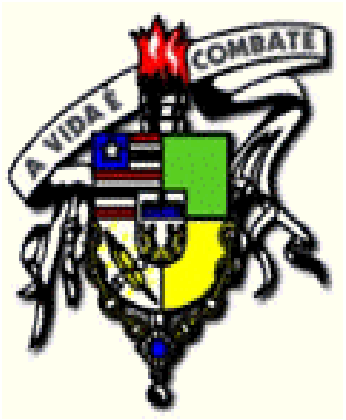


UNIVERSIDADE FEDERAL DO MARANHAO - UFMA

Banco de Dados II

Segurança

Carlos Eduardo **Portela** Serra de Castro

*

Segurança

- Introdução
- Identificação e autenticação
- Regras de autorização
- Classificação dos Dados
- Banco de Dados Estatísticos
- Criptografia
- Considerações Finais

Introdução

Objetivo:

Proteção do banco de dados contra exposição, alteração ou destruição desautorizadas.

Aspectos a considerar

1 – Aspectos legais, sociais e éticos (a pessoa que está fazendo o pedido, de um crédito ao cliente, possuirá direito legal à informação solicitada?);

2 – Controles físicos (a sala dos servidores deve ser fechada ou guardada de alguma forma?);

3 – Questões políticas (como a empresa decide quem deve ter permissão de acesso aos dados?);

Aspectos a considerar

4 – Problemas operacionais (se for utilizado um esquema de senhas, como as próprias senhas serão mantidas em segredo?);

5 – Controles de hardware (os servidores fornecem algum recurso de operação privilegiada?);

6 – Segurança do Sistema Operacional (o SO apaga o conteúdo da memória e dos arquivos de dados quando eles são liberados?);

Aspectos a considerar

7 – questões que são a preocupação específica do próprio sistema de banco de dados (o usuário pode acessar simultaneamente o campo A e ter acesso negado ao campo B, se A e B forem ambos parte do mesmo registro do banco de dados?);

Mecanismos de Segurança

Dois tipos de mecanismos de segurança

- Mecanismo Arbitrário
  - Usado para dar privilégios a usuários para acessar arquivos, registros ou campos de dados
- Mecanismo Obrigatório
  - Usado para garantir a segurança classificando dados e usuários nas diversas classes de segurança

Controle de acesso

- Prevenir contra pessoas não autorizadas

Exemplo

EMPREGADO (EMP#, NOME, ENDERECO, DEPT#, SALARIO, AVALIACAO)

1 – O usuário tem acesso a toda relação, para todos os tipos de operação;

2 – O usuário não tem nenhum acesso a qualquer parte da relação para qualquer tipo de operação;

3 – O usuário poderá ver qualquer parte da relação mas ao pode atualizá-la;

Exemplo

EMPREGADO (EMP#, NOME, ENDERECO, DEPT#, SALARIO, AVALIACAO)

4 – O usuário poderá ver somente o seu próprio registro da relação mas não pode modificá-lo;

5 – O usuário poderá ver somente o seu próprio registro da relação, e dentro daquele registro poderá alterar os valores de NOME e ENREDECO e nada mais;

Exemplo

EMPREGADO (EMP#, NOME, ENDERECO, DEPT#, SALARIO, AVALIACAO)

6 – O usuário poderá ver apenas os campos EMP#, NOME, ENDERECO e DEPT# dentro de qualquer registro, e poderáalterar apenas os valores de NOME, ENDERECO e DEPT# ;

7 - ...

Identificação e Autenticação

Identificação: quem você é? (usuário)

Autenticação: você é quem diz ser? (senha)

Perfil: especifica os objetos que o usuário está autorizado a acessar e as operações que ele está autorizado a realizar sobre esses objetos.

Perfil do objeto: especifica os usuários que tem permissão para acessá-lo (usado alternativamente).

Regras de Autorização

O sistema deve permitir que as regras de autorização sejam expressas em alguma linguagem de alto nível.

Essas regras são compiladas e armazenadas no dicionário do sistema e, e, uma vez lançadas dentro do sistema, serão cumpridas a partir daquela ocasião.

Segurança

grant select **on** agencia **to** user1

Permite ao usuário user1 realizar operações de SELECT sobre a relação agencia.

Granularidade dos objetos

Autorização a nível de relações inteiras.

Autorização a nível de campos individuais.

Granularidade dos objetos

Controle independente de valor.

```
Select * from S
```

Controle dependente de valor.

```
Select * from S
where SAL <  R$3.000,00
```

Segurança do BD e o DBA

Responsabilidades do DBA

- Dar privilégios a usuários
- Classificar usuários e dados de acordo com a política da organização

Ações do DBA

- Abrir contas
  - Conta e senha permitindo o acesso ao SGBD
- Atribuir privilégios
  - Atribuir certos privilégios a certas contas
- Retirar privilégios
  - Cancelar privilégios atribuídos anteriormente
- Definir as contas de usuários nos níveis de segurança apropriados.

DBA = Responsável pela segurança geral do sistema de BD.

Controle de acesso arbitrário

Baseado em Privilégios

Considerar o contexto relacional

Método Típico

Dar (GRANT)

Retirar (REVOKE)

No nível de Conta

Privilégios particulares de uma conta independente das relações do BD

Controle de acesso arbitrário

Privilégios

- Criar esquemas ou tabelas
- Criar visão
- Alterar tabelas ou atributos
- Remover tabelas ou visões
- Modificar tuplas
- Acessar o BD (SELECT)

No nível de Relação

- Controle de acesso a cada relação em particular ou visão do BD

Controle de acesso arbitrário

Propagação de privilégios

Quando se dá privilégios a uma conta, pode-se dar ou não a ela a opção de dar privilégios a outras:

GRANT OPTION

Riscos:

Propagação de privilégios sem o conhecimento do proprietário;

Se o privilégio da primeira conta for retirado, todas as outras também serão automaticamente retiradas.

Controle de acesso obrigatório

Baseado em Segurança Multinível

- Mecanismo de segurança que classifica dados e usuários baseado em classes de segurança
- Pouco utilizado em SGBD

Classes de segurança usuais

- • Muito secreta (TS)
- • Secreta (S)
- • Confidencial (C)
- • Não classificada (U)

  Onde TS > S > C > U

Noções de segurança multinível no relacional

- A cada atributo é associado um atributo de classificação e cada valor de atributo com sua classificação de segurança correspondente

Banco de Dados Estatísticos

È um banco de dados que

(a)contém um grande número de registros individualmente sensíveis, mas

(b)tem a finalidade de só fornecer informações de resumo estatístico e a seus usuários, e não informações referentes a algum indivíduo específico.

Perigo: dedução de informação confidencial por inferência.

Banco de Dados Estatísticos

Select count (*)

From stats

Where sex = ‘m’

And occupation = ‘programmer’

Resposta = 1

Select sum (salary)

From stats

Where sex = ‘m’

And occupation = ‘programmer’

Resposta = R$ 2.500,00

Criptografia

CRIPTOGRAFIA é definida como a ciência que oculta e/ou protege informações – escrita, eletrônica ou de comunicação.

CRIPTOGRAFIA é um conjunto de técnicas usadas para transformar textos legíveis em textos não legíveis, de forma que somente pessoas autorizadas tenham acesso a essas informações.

Criptografia

A linguagem dos índios navajo , utilizado pelos americanos contra os japoneses na Segunda Guerra Mundial.

Filme: Códigos de Guerra, de John Woo

A língua do “P”.

Esse filme é ótimo. →

Epessepe filpilmepe épe opotipimopo.

Criptografia

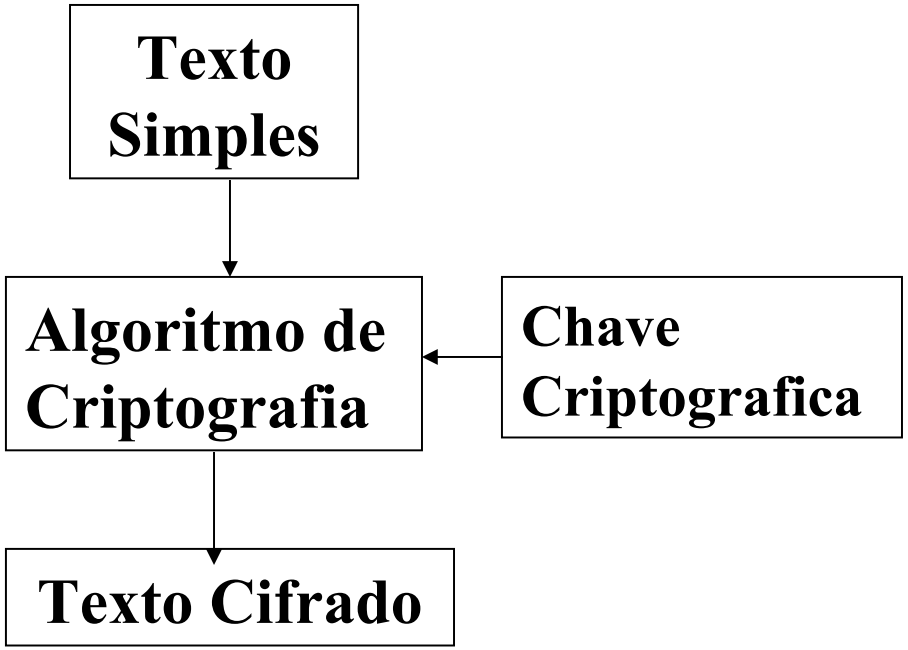
A criptografia busca garantir:

Autenticação dos participantes;

Integridade da informação ;

Confidencialidade.

Criptografia



Normas de Criptografia

- Substituição
- Permutação

Tipos de Criptografia

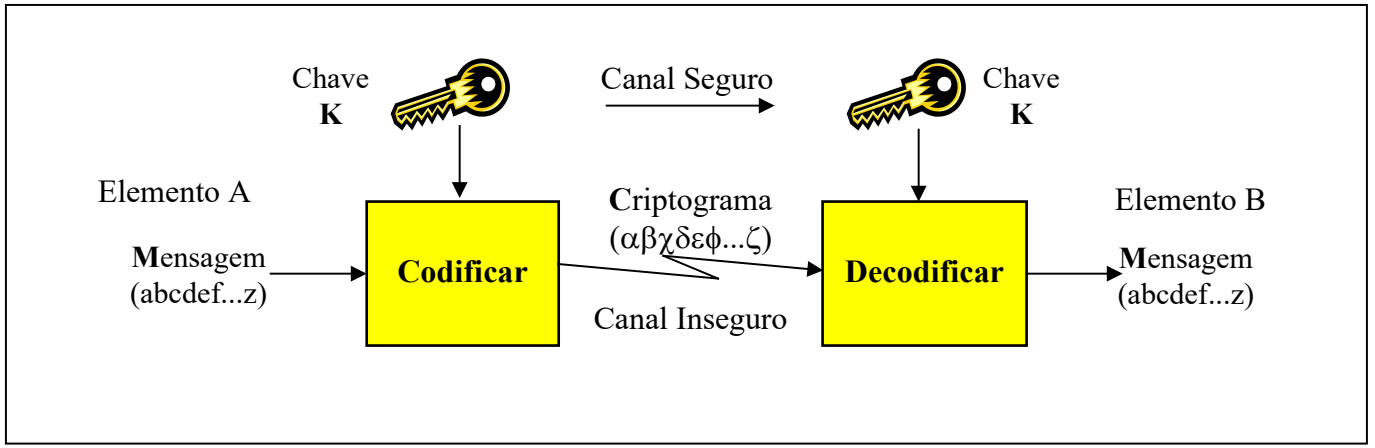
- Criptografia Simétrica
- Criptografia Assimétrica

Criptografia Simétrica

A criptografia simétrica tem como característica principal à utilização de somente uma chave para autenticar, garantir a integridade e a confidencialidade de uma mensagem.

Criptografia Simétrica

A figura representa o processo da criptografia simétrica (chave privada).



Criptografia Assimétrica

A criptografia assimétrica conhecida também como criptografia de chave pública utiliza duas chaves diferentes, matematicamente relacionadas.

Criptografia Assimétrica

Qualquer pessoa pode enviar uma mensagem confidencial apenas utilizando chave pública, mas esta mensagem só poderá ser decriptografada com a chave privada do destinatário.

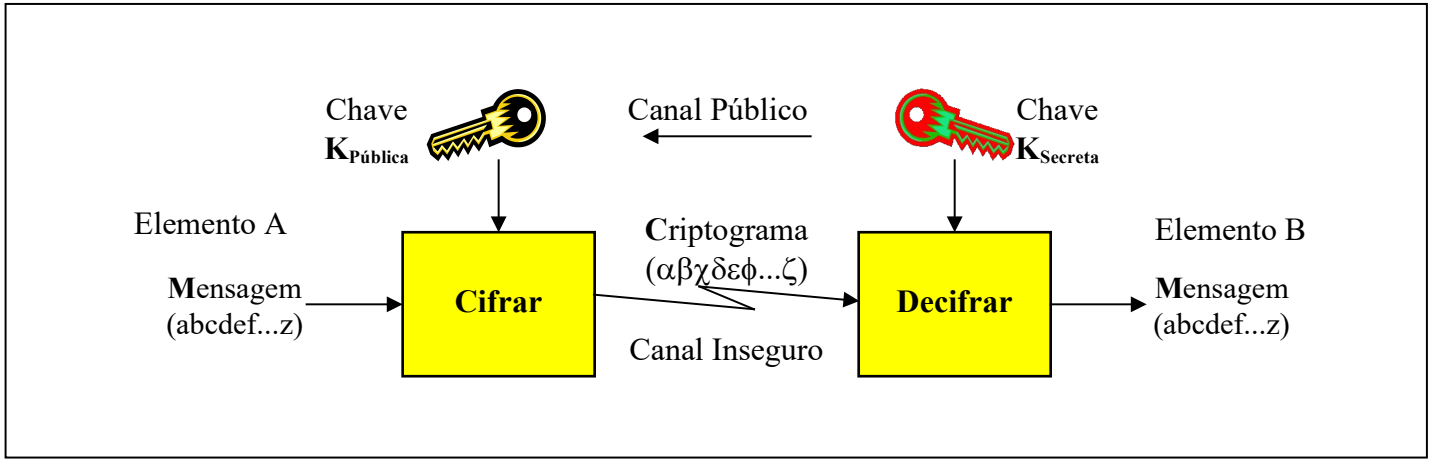
Criptografia Assimétrica

A chave privada deve ser mantida em segredo e não poderá ser utilizada por ninguém, exceto pela pessoa a qual ela pertence.

A chave pública, ao contrário, deve ser disponibilizada para ser utilizada por qualquer aplicação ou indivíduo.

Criptografia Assimétrica

Uso de algoritmo criptográfico **assimétrico** (chave pública).



Bibliografia

- *Navathe*
  - *Capítulo 23:* Introdução às Questões de Segurança em Bancos de Dados