

The slide features a decorative arrangement of seven circles. Three circles are filled with a light purple color, while four are hollow with a thin purple outline. They are scattered around the main text.

O que é Segurança da Informação

Introdução à Criptografia

O que é Segurança da Informação

- Segurança de Informação relaciona-se com **vários e diferentes aspectos referentes à:**

- confidencialidade / privacidade,
- autenticidade,
- integridade,
- não-repúdio
- disponibilidade

O que é Segurança da Informação



- **mas também, a que não estão restritos:**
 - **à sistemas computacionais,**
 - **nem a informações eletrônicas,**
 - **ou qualquer outra forma mecânica de armazenamento.**

O que é Segurança da Informação



- Ela se aplica à **todos os aspectos de proteção e armazenamento** de informações e dados, em qualquer forma.

Aspectos não computacionais da Segurança da Informação

- Normativos
 - Conceitos, Diretrizes, Regulamentos, Padrões
- Planos de Contingência
- Estatísticas
- Legislação
- Fóruns de Discussão



Recursos da Informação

- Arquivos.
- Objetos.
- Banco de dados.

Valor da Informação



- Muitos **recursos de informação** que são disponíveis e mantidos em sistemas de informação distribuídos através de redes, têm um **alto valor** intrínseco para seus usuários.
- Toda informação tem valor e precisa ser protegida contra **acidentes** ou **ataques**.



Proteção da Informação

- **Códigos**

- **Cifras**



Para cifrar Criptografia

- Uma das ferramentas mais importantes para a segurança da informação é a **criptografia**.
- Qualquer **método** que **transforme** **informação legível em informação legível ilegível**.



Por que Criptografia ?

- O fato é que todos nós temos informações que queremos manter em sigilo:
 - Desejo de Privacidade.
 - Autoproteção.
 - Empresas também têm segredos.
 - Informações estratégicas.
 - Previsões de vendas.
 - Detalhes técnicos como produtos.
 - Resultados de pesquisa de mercado.
 - Arquivos pessoais.

O papel da criptografia na segurança da informação

- Mundo real

- Se as **fechaduras nas portas e janelas** da sua casa são relativamente fortes, a ponto de que um ladrão não pode invadir e furtar seus pertences ...
- ... **a sua casa está segura.**

O papel da criptografia na segurança da informação

- Mundo real

- Para maior proteção contra invasores, talvez você tenha de ter um **sistema de alarme de segurança**.
- **A sua casa estará mais segura.**

O papel da criptografia na segurança da informação

- Mundo real

- Se alguém tentar fraudulentamente **retirar dinheiro de sua conta bancária**, mas se o banco não confiar na história do ladrão ...

- ... **seu dinheiro estará seguro.**

O papel da criptografia na segurança da informação

- Mundo real

- Quando você **assina um contrato**, as **assinaturas são imposições legais** que orientam e impelem ambas as partes a honrar suas palavras.

O papel da criptografia na segurança da informação

- Mundo Digital

- Confidencialidade ou Privacidade

- Ninguém pode invadir seus arquivos e ler os seus **dados pessoais sigilosos (Privacidade)**.
- Ninguém pode invadir um meio de comunicação e **obter a informação trafegada**, no sentido de usufruir vantagem no uso de recursos de uma rede (**confidencialidade**).

O papel da criptografia na segurança da informação

- Mundo Digital

- A **privacidade** é a fechadura da porta.

- **Integridade** refere-se ao mecanismo que informa **quando algo foi alterado**.
Integridade é alarme da casa.

O papel da criptografia na segurança da informação

- Mundo Digital

- Aplicando a prática da **autenticação**, pode-se verificar as identidades.
- A **irretratabilidade** (não-repúdio) é a imposição legal que impele as pessoas a honrar suas palavras.

O papel da criptografia na segurança da informação

- De algum modo a **criptografia** contribui para resolver os problemas de:
 - confidencialidade,
 - privacidade,
 - integridade,
 - autenticação,
 - irretratabilidade,
 - disponibilidade.

O papel da criptografia na segurança da informação

- Assim, uma das ferramentas mais importantes para a **segurança da informação** é a criptografia.

O papel da criptografia na segurança da informação

- Qualquer um dos **vários métodos** que são utilizados **para transformar informação legível para algo ilegível**, pode contribuir para resolver os conceitos anteriores.

O papel da criptografia na segurança da informação

- Mas, **de modo algum a criptografia é a única ferramenta** para assegurar a segurança da informação.
- Nem resolverá todos os problemas de segurança.
- Criptografia **não é a prova de falhas.**

O papel da criptografia na segurança da informação

- Toda criptografia pode ser quebrada e , sobretudo, se for **implementada incorretamente**, não agrega nenhuma segurança real.
- O que veremos: uma **visão da criptografia.**

O papel da criptografia na segurança da informação

- Não se trata de uma análise completa de tudo o que se deve conhecer sobre criptografia.
- Veremos as **técnicas de criptografia mais amplamente usadas** no mundo atual.

A decorative graphic at the top of the slide consists of two groups of circles. The first group on the left has a solid light purple circle on the left and an empty light purple circle outline on the right. The second group on the right has a solid light purple circle on the left, an empty light purple circle outline in the middle, and a solid light purple circle on the right.

Conceitos

- A palavra “Criptografia”
- Trabalhos sobre o história da criptografia
- Conceito de Código
- Conceito de **Cifra**

Significado da palavra “Criptografia”

- A palavra **criptografia** vem das palavras gregas que significam “**escrita secreta**”.
- *Kriptos* (em grego) = Secreto + Grafia (de escrever)
- *Criptografia* = Escrita secreta.
- **Criar mensagens cifradas.**
- História de milhares de anos.

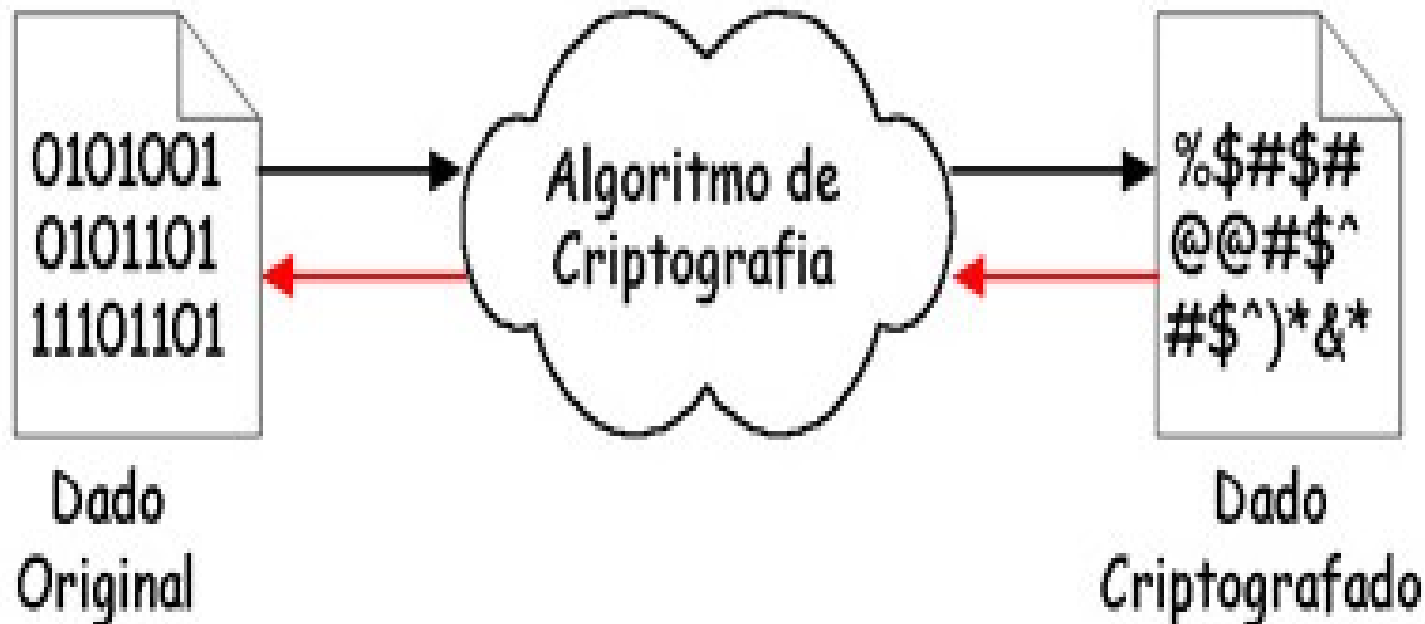
Jargões da Criptografia



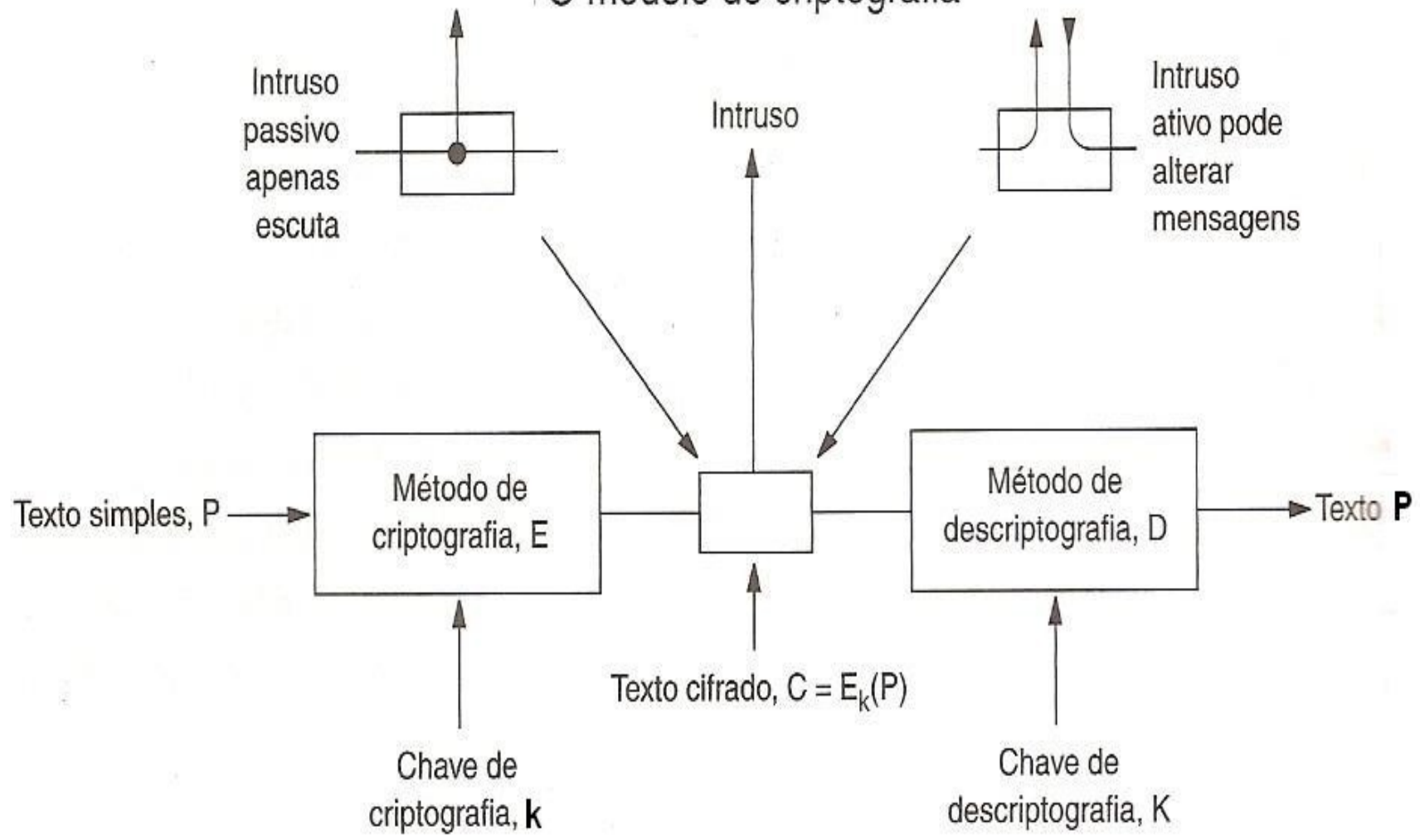
- Encripta (codifica, criptografa, cifra)
- Decrypta (decodifica, decryptografa, decifra)

Procedimentos da Criptografia

- Os procedimentos de **criptografar** e **descriptografar** são obtidos através de um algoritmo de criptografia.



O modelo de criptografia



Equações da Criptografia



$$D_K (E_K(P)) = P$$

E e D são funções matemáticas

K é uma **chave**



Criptografia

- Possui emprego nas mais diferentes áreas de atuação, mas em todas, tem o mesmo significado:
 - **proteger informações consideradas ‘especiais’ ou de qualidade sensível.**

Criptografia

A decorative graphic consisting of two groups of three circles. The first group on the left has a solid light purple circle on the left, a white circle with a light purple outline in the middle, and a solid light purple circle on the right. The second group on the right has a solid light purple circle on the left, a white circle with a light purple outline in the middle, and a solid light purple circle on the right.

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

Criptografia

A decorative graphic consisting of two rows of circles. The top row has a solid purple circle on the left and an outlined purple circle on the right. The bottom row has a solid purple circle on the left, an outlined purple circle in the middle, and a solid purple circle on the right.

- É o ato de **alterar uma mensagem para esconder o significado** desta.
- Mas, como esconder ?
 - Criando um **código** ?
 - Criando **cifra** ?

Conceito de Código

- Substitui uma **palavra por outra palavra** ou uma **palavra por um símbolo**.
- **Códigos, no sentido da criptografia, não são mais utilizados**, embora tenham tido uma história ...
 - O código na linguagem navajo dos índios americanos, utilizado pelos mesmos contra os japoneses na Segunda Guerra Mundial.

Conceito de Código

- A **linguagem navajo** era caracterizada apenas por **sons**.
- Um código é uma **transformação que envolve somente duas partes**.
- O que é gerado chama-se uma **codificação**.

Conceito de Código



- A transformação leva em conta a **estrutura linguística da mensagem** sendo transformada.
- Lembre da transformação em um compilador.

Conceito de Cifra

- É uma **transformação de caractere por caractere** ou **bit por bit**, **sem levar em conta** a estrutura linguística da mensagem.
- Substituindo um por outro.
- Transpondo a ordem dos símbolos.

Criptografia Tradicional



- Historicamente, os **métodos tradicionais de criptografia** são divididos em duas categorias:

- Cifras de **Substituição**
- Cifras de **Transposição**

Cifras de Substituição

- Cada **letra** ou **grupo de letras** é substituído por **outra letra** ou **grupo de letras**, de modo a criar um “disfarce”.
- Exemplo: A Cifra de César (Caeser Cipher).
Considerando as 26 letras do alfabeto inglês (a,b,c,d,e,f,g,h,i,j,k,m,n,o,p,q,r,s,t,u,v,x,w,y,z),
Neste método, a se torna d, b se torna e, c se torna f,, z se torna c.

Generalização da Cifra de César

- Cada letra se desloca k vezes, em vez de três. Neste caso, k passa a ser uma chave para o método genérico dos alfabetos deslocados de forma circular.
- A Cifra de César pode enganado os cartagineses, mas nunca mais enganou a mais ninguém.

Cifra de Substituição



- As **cifras de substituição** preservam a ordem dos símbolos no texto claro, mas disfarçam esses símbolos.

Cifra de Transposição



- **Cifras de Transposição** reordenam os símbolos, mas não os disfarçam.

Exemplo de Cifra de Transposição

Fonte: Redes de Computadores, A. S. Tanenbaum, Cap. 8

- A cifra se baseia numa chave que é uma palavra ou uma frase que não contém letras repetidas.
- Seja a chave: **MEGABUCK**
- O objetivo da chave é numerar as colunas de modo que a coluna 1 fique abaixo da letra da chave mais próxima do início do alfabeto e assim por diante.

Exemplo de Cifra de Transposição

Fonte: Redes de Computadores, A. S. Tanenbaum, Cap. 8

- O texto simples é escrito horizontalmente, em linhas.
- O texto cifrado é lido em colunas, a partir da coluna cuja letra da chave tenha a ordem mais baixa no alfabeto.
- A numeração abaixo da chave, significa a ordem das letras no alfabeto.

Exemplo de Cifra de Transposição

Fonte: Redes de Computadores, A. S. Tanenbaum, Cap. 8

M E G A B U C K
7 4 5 1 2 8 3 6
p l e a s e t r
a n s f e r o n
e m i l l i o n
d o l l a r s t
o m y s w i s s
b a n k a c c o
u n t s i x t w
o t w o a b c d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwo

Ciphertext

AFLLSKSOSELAWAIATOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUEOERIRICXB

Exemplo de Cifra de Transposição

Fonte: Redes de Computadores, A. S. Tanenbaum, Cap. 8

- Algumas cifras de transposição aceitam um bloco de tamanho fixo como entrada e produzem um bloco de tamanho fixo como saída.
- Essas cifras podem ser completamente descritas fornecendo-se uma lista que informe a ordem na qual os caracteres devem sair.

Exemplo de Cifra de Transposição

Fonte: *Redes de Computadores*, A. S. Tanenbaum, Cap. 8

- No exemplo, a cifra pode ser vista como uma **cifra de blocos de 64 bits de entrada**.
- Para a saída, a lista para a ordem de saída dos caracteres é 4, 12, 20, 28, 36, 44, 52, 60, 5, 13, ... 62.
- Neste exemplo, o quarto caractere de entrada, **a**, é o primeiro a sair, seguido pelo décimo segundo, **f**, e assim por diante.

Dois princípios fundamentais da criptografia



- **Redundância**

Princípio Criptográfico #1

As mensagens criptografadas devem conter alguma redundância.

- **Atualidade**

Princípio Criptográfico #2

Algum método é necessário para anular ataques de repetição.

Redundância



- Informações não necessárias para compreensão da mensagem clara.
- A moral da história é que **todas as mensagens devem conter informações redundantes suficientes para que os intrusos ativos sejam impedidos de transmitir dados inválidos que possam ser interpretados como uma mensagem válida.**

Atualidade

A decorative graphic at the top of the slide consists of two groups of circles. The first group on the left has a solid light purple circle on the left and an outlined light purple circle on the right. The second group on the right has a solid light purple circle on the left, an outlined light purple circle in the middle, and a solid light purple circle on the right.

- Tomar algumas medidas para assegurar que cada mensagem recebida possa ser confirmada como uma mensagem atual, isto é, enviada muito recentemente.

Atualidade

A decorative graphic at the top of the slide consists of two groups of circles. The first group on the left has a solid light purple circle on the left and an outlined light purple circle on the right, with the word 'Atualidade' centered over them. The second group on the right has a solid light purple circle on the left, an outlined light purple circle in the middle, and a solid light purple circle on the right.

- Medida necessária para impedir que intrusos ativos reutilizem (repitam) mensagens antigas por intermédio de interceptação de mensagens no meio de comunicação.

Atualidade



- Incluir em cada mensagem um timbre de hora válido apenas por 10 segundos.
- O receptor pode manter as mensagens durante 10 segundos, para poder comparar as mensagens recém-chegadas com mensagens anteriores e assim filtrar duplicatas.



Elementos básicos de Cifras

- Caixa P
- Caixa S
- Cifra de Produto

Trabalhos sobre o História da Criptografia

- Histórico completo (Khan, 1995)
- Estado da arte em segurança e protocolos criptográficos (Kaufman et al., 2002)
- Abordagem mais matemática (Stinson, 2002)
- Abordagem menos matemática (Burnett e Paine (2001))



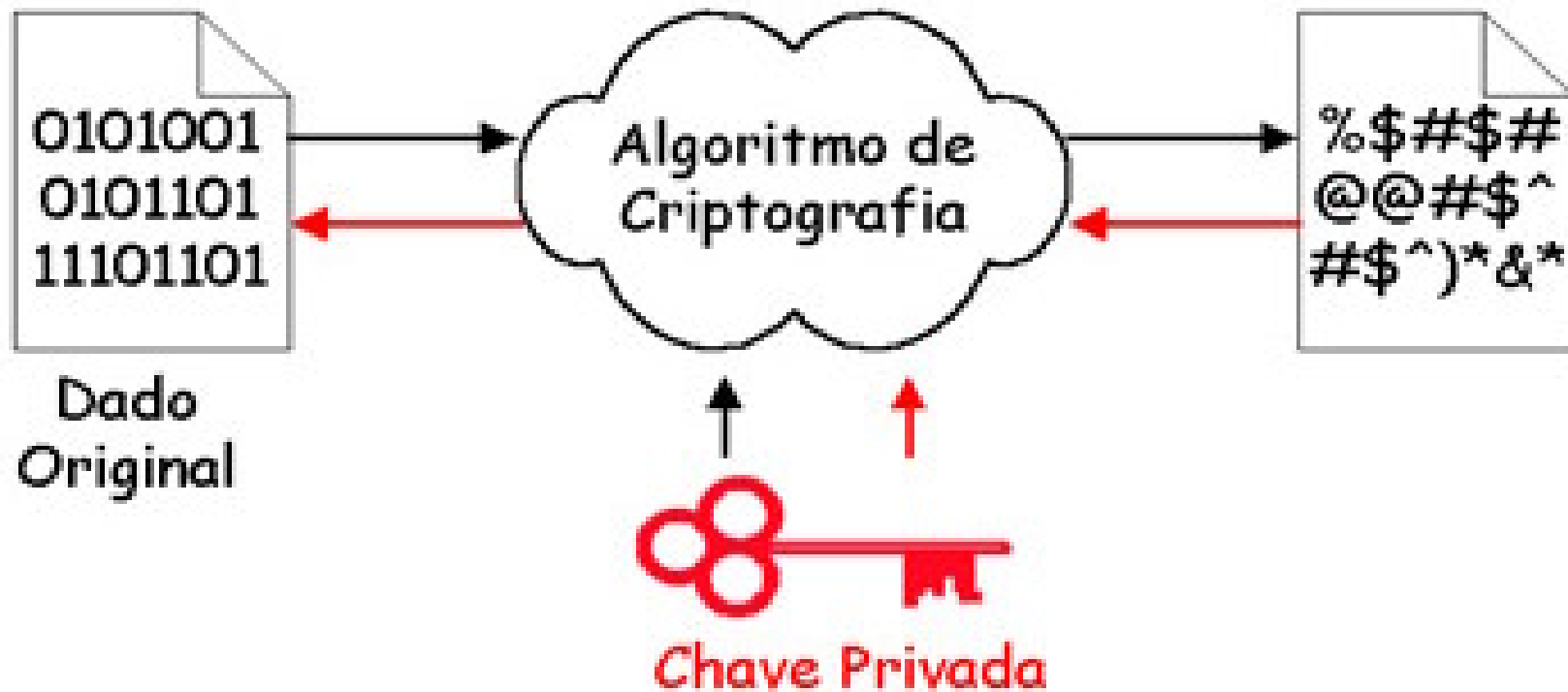
Estrutura de Estudo

**Criptografia e Segurança da
Informação**

Técnicas envolvendo criptografia

- **Garantia de Confidencialidade**
- **Garantia de Privacidade**

Criptografia Simétrica

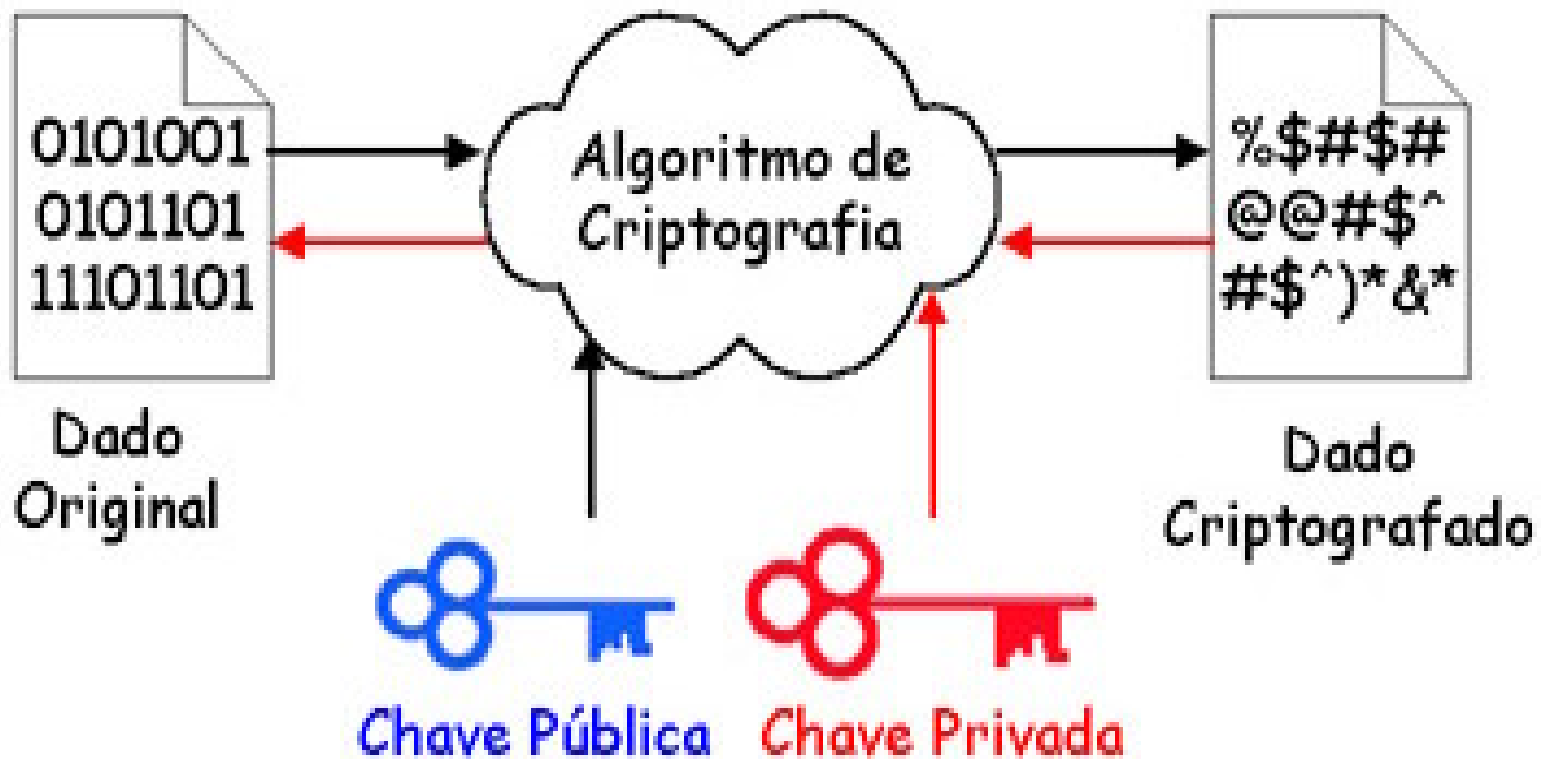


Técnicas envolvendo criptografia simétrica



- Algoritmos de Criptografia de **Chave Simétrica**,
- Gerenciamento de Chaves Simétricas,

Criptografia Assimétrica



Técnicas envolvendo criptografia de chave pública

- Algoritmos de Criptografia de **Chaves Públicas**
- O problema de **distribuição de chaves**
- **Infra-estrutura de chaves públicas**

Técnicas envolvendo criptografia

- Mas, se não houver preocupação com sigilo da informação ...
- Ou o desempenho da criptografia de chave pública é imprescindível.

Resumos de Mensagem



- Uma **forma mais rápida de criptografia** (simétrica ou assimétrica).
- Um **representante dos dados**.
- Garantia de **Integridade**
- Algoritmos **Hash**

Problema

A diagram consisting of two groups of three circles. The first group has a solid light purple circle on the left, a white circle with a light purple outline in the middle, and a solid light purple circle on the right. The second group has a solid light purple circle on the left, a white circle with a light purple outline in the middle, and a solid light purple circle on the right.

- Mas, a **mensagem** e o **resumo** são preparadas e transmitidas em separado, **um intruso pode capturar a mensagem e também pode capturar o resumo** correspondente.



Duas maneiras de resolver o problema

- Utilizar uma **assinatura digital**.
- Uma **chave-resumo (HMAC)**, resume a **chave e os dados, nesta ordem**.

Códigos de Autenticação de Mensagem

- Resolvem o problema de se transmitir mensagem e resumo, **não mais separadamente.**



HMAC

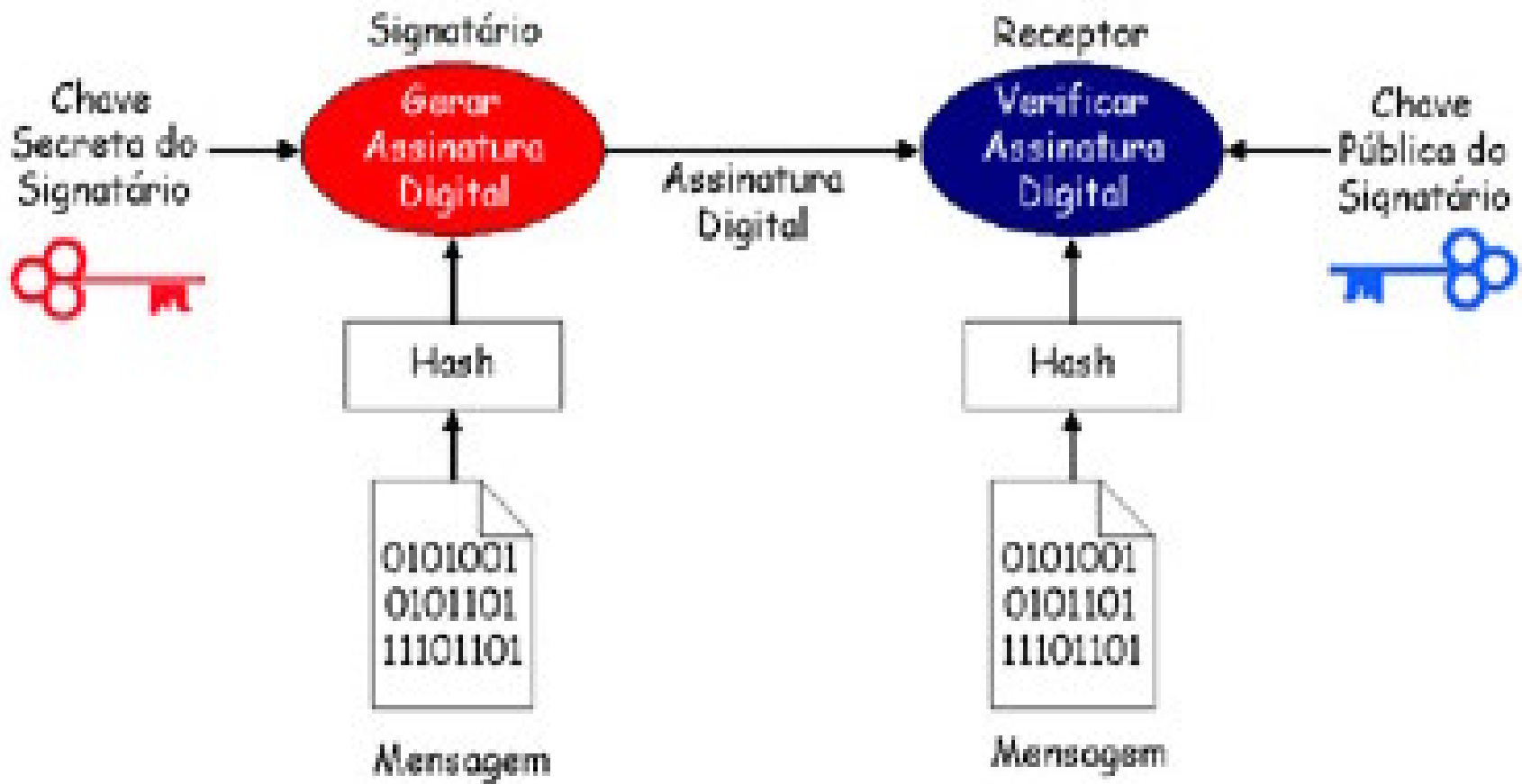
- São utilizadas apenas para verificar se o conteúdo não foi alterado durante o trânsito.
- É uma verificação instantânea e não um registro permanente.

Assinaturas Verificáveis



- Por essa razão, **necessitamos de uma outra maneira de criar assinaturas verificáveis** e essa maneira é **encriptar o resumo com a chave privada do assinante** (que é o que se chama de assinatura digital).

Assinatura Digital



Assinatura Digital



- Garantia de **Autenticidade**
- Garantia de **Integridade**
- Garantia de **Não-Repúdio**



Problema com as assinaturas

- Assinaturas são suficientes num número limitado de pessoas, quando as pessoas, de certa forma, se conhecem.
- Quando alguém tem que verificar uma assinatura, deve obter a chave pública do remetente da mensagem.



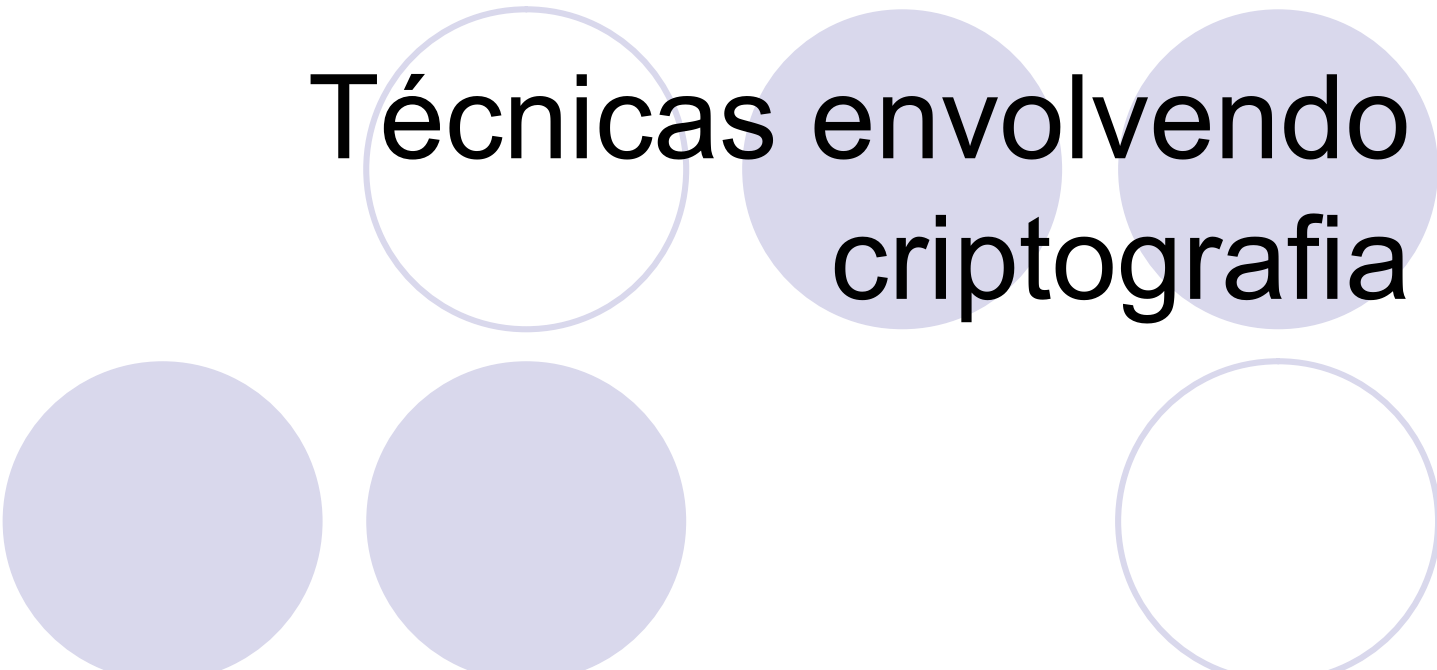
Problema com as assinaturas

- Como o destinatário da mensagem pode ter certeza de que a chave pública recebida é de fato o dono da chave pública quando enviou a mensagem ?



Uma solução ...

- Servidor on-line de chaves públicas na Internet 24 horas ?
- On-Line ?
- Replicação de servidores ?
- **Certificados Digitais**

The slide features five decorative circles. Two are solid light purple, and three are hollow with a light purple outline. They are arranged in two rows: the top row has three circles and the bottom row has two circles.

Técnicas envolvendo criptografia

Protocolos com Criptografia

Segurança nas Camadas



- Com exceção da **segurança na camada física**, quase **toda segurança se baseia em princípios criptográficos**.

Criptografia de Enlace



- Na camada de enlace, os quadros em uma linha ponto-a-ponto podem ser codificados, à medida que saem de uma máquina, e decodificados quando chegam em outra.

Criptografia de Enlace



- Vários detalhes de criptografia **poderiam ser tratados na camada de enlace**, no entanto, **essa solução se mostra ineficiente, quando existem vários roteadores.**



Criptografia de Enlace

- Pois é necessário decriptar os pacotes, em cada roteador, o que pode tornar esses, **vulneráveis a ataques dentro do roteador.**
- Também, algumas sessões de aplicações são protegidas, mas outras, não.

Criptografia na Camada de Rede

- A segurança do **Protocolo IP** funciona nesta camada.
- Estudar o **Protocolo IPSec**

Criptografia na Camada de Transporte

- É possível criptografar conexões fim-a-fim, ou seja processo-a-processo.
- **SSL** (Security Socket Level)
- **TLS** (transport Level Security)
- **Stunnel** para criptografia com **protocolos não SSL** (por exemplo, **SSH**)

Criptografia na Camada da Aplicação

- **S/MIME** (**S**ecure/**M**ultipurpose **I**nternet **M**ail **E**xtensions)
- **SET** (Secure Electronic Transactions)
- **HTTPS** (HTTP sobre SSL)

Criptografia na Camada da Aplicação

- **Autenticação** de usuários
- **Não-Repúdio**
- Só podem ser tratadas na camada da aplicação.

Uma aplicação da Criptografia Simétrica

The title is centered and overlaid on a decorative graphic consisting of five circles. Three circles are solid light purple, and two are hollow with a light purple outline. They are arranged in two rows: the top row has three circles and the bottom row has two circles.

Segurança de Bancos de Dados Oracle

- Apenas as pessoas apropriadas podem ter acesso às informações no BD (**autenticação de usuários**).
- **Os dados precisam ser protegidos** e uma maneira de proteger os dados é por **criptografia**.

Segurança de Bancos de Dados Oracle

- **Geração da Chave:**
- Alguns **bytes aleatórios** ou **pseudo-aleatórios** são gerados e utilizados como uma **chave** para a criptografia simétrica DES ou TripleDES.

Segurança de Bancos de Dados Oracle

- **Armazenamento da Chave:**
- Precisa-se também **salvar essa chave gerada em algum lugar** (não no mesmo lugar onde foi gerada). O próximo capítulo ensina como armazenar a **chave simétrica**.

Criptografando em um BD Oracle

- **A chave é usada para criptografia ...**
- **dbms obfuscation toolkit.DESEncrypt (**
inputstring => **plaintext,**
key => **keydata,**
encrypted string => **ciphertex);**

Decriptografando em um BD Oracle

- **A chave é recuperada e ...**
- **dbms obfuscation toolkit.DESDecrypt (**
inputstring => **ciphertex**,
key => **keydata**,
encrypted string => **plaintext**);

Utilidades na Segurança da Informação

The title is centered and overlaid on a decorative arrangement of six circles. The top row consists of three circles: a white circle with a light purple outline on the left, a solid light purple circle in the middle, and another solid light purple circle on the right. The bottom row consists of three circles: a solid light purple circle on the left, a solid light purple circle in the middle, and a white circle with a light purple outline on the right.

Utilidades na Segurança da Informação

- Segurança e Privacidade em um Navegador.
- Segurança de Emails.
- Criptografia de Diretórios, Subdiretórios Arquivos.
- Transferência de Arquivos.



Garantindo os requisitos de segurança

- Confidencialidade
- Privacidade
- Autenticidade
- Integridade
- Não-Repúdio