CRIPTOGRAFIA PARA PROTEÇÃO DE DADOS

Como funciona.

Vantagens e Desvantagens

Sumário

- Serviços de segurança.
  - Ataques à Segurança
    - Passivo / Ativo
  - O que é um serviço de segurança?
  - Introdução aos Serviços de Segurança
  - Principais Serviços de Segurança
- Criptografia

ATAQUES A SEGURANÇA

- Qualquer ação que comprometa a segurança da informação pertencente a uma organização

- Podem ser ataques:
  - Passivo
  - Ativo

ATAQUES A SEGURANÇA

- Passivo
  - Ataques que deixam de alterar, perturbar ou afetar um sistema, recursos ou um fluxo de comunicação
  - Possuem a natureza de bisbilhotar ou monitorar transmissões
  - O objetivo é obter informações.
  - São muito difíceis de detectar.
  - Exemplos: Leitura desautorizada de uma mensagem ou
  - análise de tráfego

ATAQUES A SEGURANÇA

- Ativo
  - Ataques que modificam ou geram perturbação em um sistema, recursos ou um fluxo de comunicação
  - Exemplos: modificação de mensagens ou arquivos,
  - negação de serviço etc.
- Divide-se em 4 categorias
  - Disfarce
  - Repetição
  - Modificação
  - Negação de serviço

SERVIÇOS DE SEGURANÇA

- Um serviço de processamento ou comunicação que **aumenta** o controle e **a proteção** dos recursos dos sistemas e das transferências de informação.

- Servem para frustrar ou controlar ataques à segurança.
- Nada mais é do que **uma funcionalidade relacionada à segurança computacional**

- Serviços utilizam um ou mais mecanismos de segurança

SERVIÇOS DE SEGURANÇA

Principais serviços de segurança:

- Serviço de Confidencialidade
- Serviço de Autenticação
  - Usuário, parceiro e mensagem
- Serviço de Integridade
- Serviço de Irretratabilidade (não repudiação)
- Serviço de Disponibilidade
- Serviço de Controle de Acesso
- Serviço de Auditoria
- Serviço de Comprovação temporal.

SERVIÇOS DE SEGURANÇA

Mecanismo de Segurança

- Um mecanismo de segurança é qualquer processo ou meio projetado para detectar, impedir ou permitir recuperar-se de um ataque à segurança

- Alguns exemplos de mecanismos de segurança são:
  - algoritmos de criptografia,
  - assinaturas digitais
  - protocolos de autenticação

SERVIÇOS DE SEGURANÇA

- Serviço de Confidencialidade (sigilo)
  - Busca proteger uma informação ou mensagem armazenada ou em trânsito contra a divulgação a entidades não autorizada.
  - Proteção dos dados contra ataques passivos.

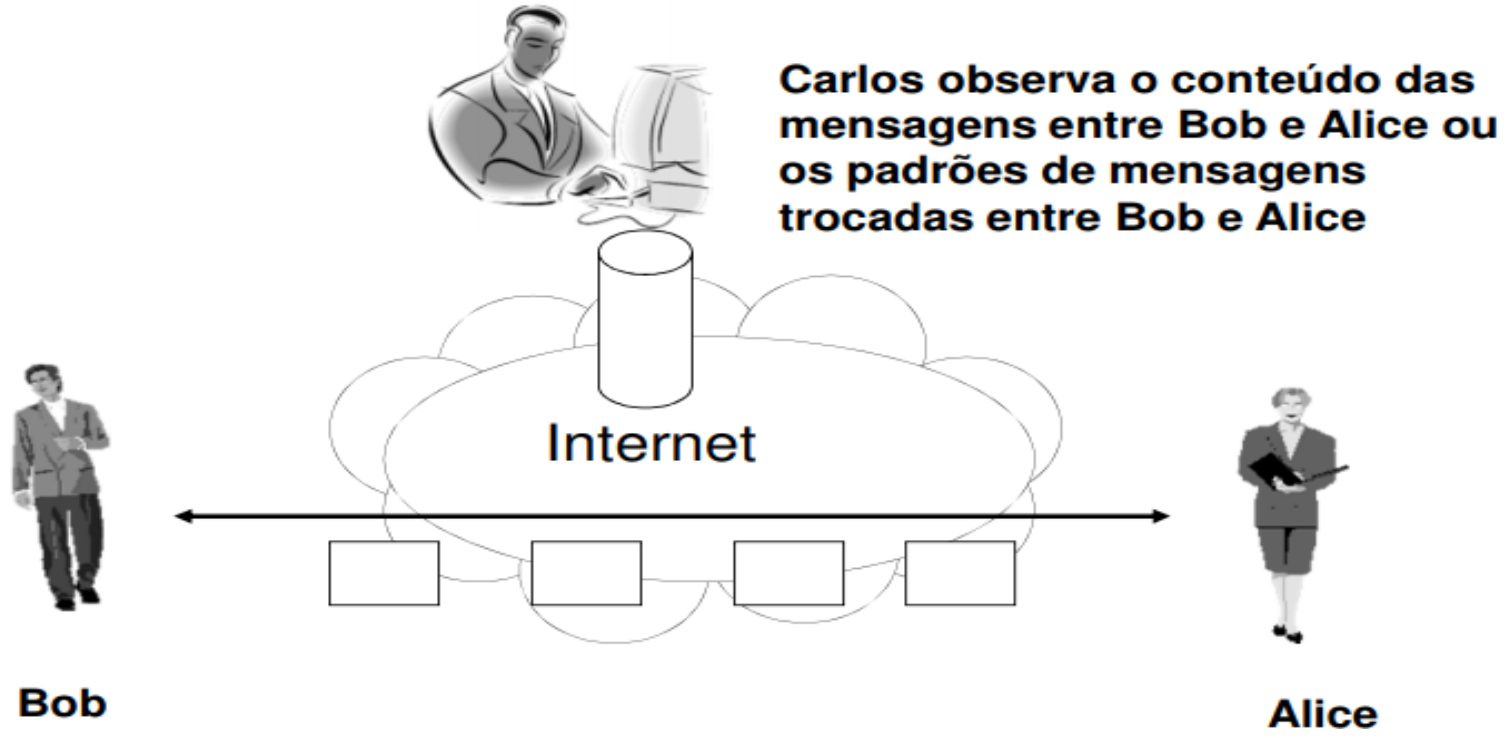
  - Exemplo:
  - Troca de arquivos entre duas entidades com sigilo (confidencialidade).

  - Métodos de implementação:
    - Criptografia
    - Segurança física do canal de comunicação ©

SERVIÇOS DE SEGURANÇA

Serviço de Confidencialidade

Serviço de confidencialidade visa proteger contra ataques passivos de "liberação de conteúdo da mensagem" e "análise de tráfego"



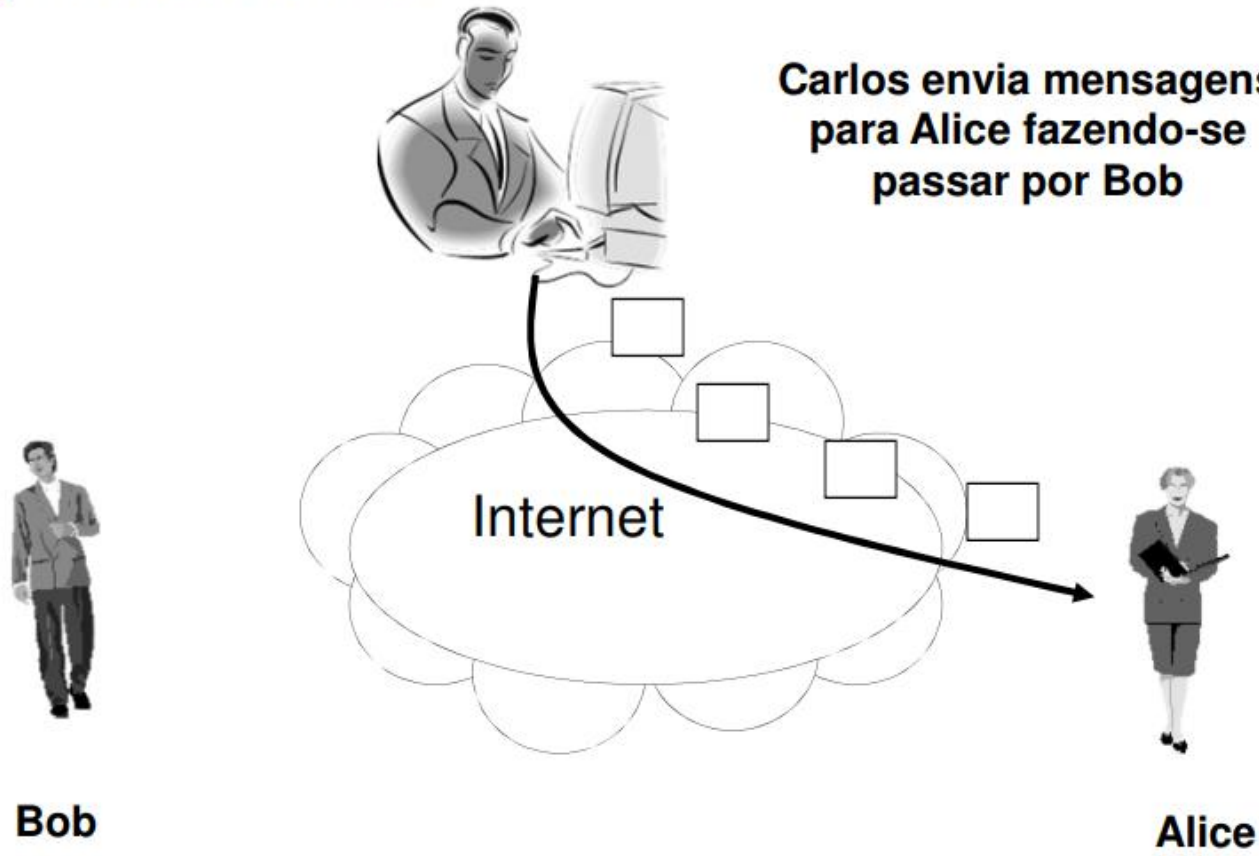
SERVIÇOS DE SEGURANÇA

- Serviço de autenticação
  - Comprovar ou verificar entidades autorizadas
  - **Autenticar um usuário no sistema**
    - Comprovar um usuário verdadeiro ou autorizado
  - **Autenticação de parceiro de comunicação**
    - Comprovar que a entidade parceira em conexão é verdadeira
  - **Autenticação de mensagem**
    - Chamado de serviço de autoria
    - Comprovar o autor(ou a origem) da mensagem
      - Garantir que a mensagem veio realmente da entidade esperada e não uma impostora

SERVIÇOS DE SEGURANÇA

Serviço de Autenticação

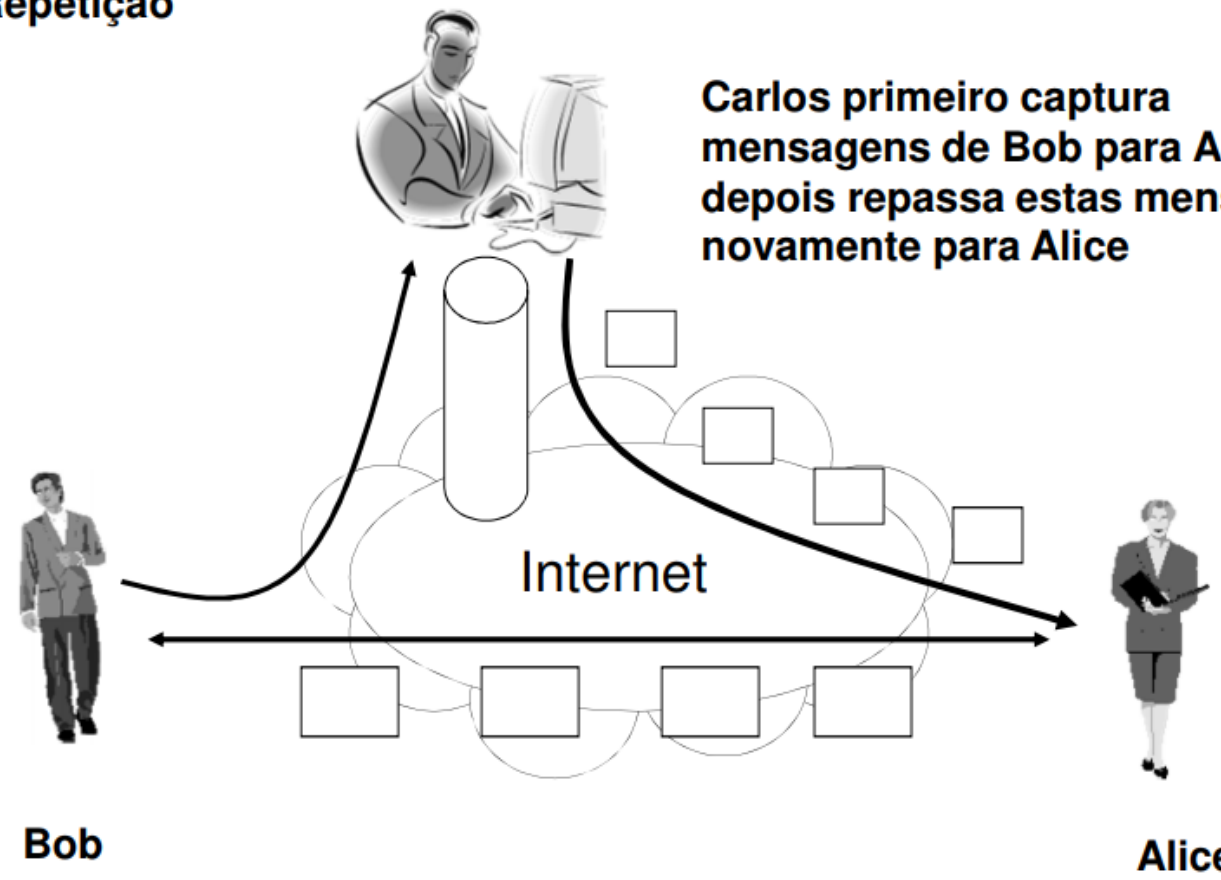
Serviço de autenticação visa proteger contra ataques ativos de "Masquerade ou Disfarce"



SERVIÇOS DE SEGURANÇA

Serviço de Autenticação

Serviço de autenticação visa proteger contra ataques ativos de "Replay ou Repetição"



SERVIÇOS DE SEGURANÇA

- **Serviço de Integridade**
  - Busca determinar se um recurso(armazenado ou em transito) foi modificado por entidade não autorizada.
  - O recurso deve estar idêntico ao que foi gerado pela entidade autorizada
  - Sem modificações, inserções, exclusões ou repetição de dados.

SERVIÇOS DE SEGURANÇA

- **Serviço de Irretratabilidade**
  - Assegurar que determinado ato não possa ser repudiado nem retratado.

  - Irretratabilidade de transmissão
    - Controlar que uma determinada entidade que tenha transmitido uma mensagem não possa alegar que não tenha feito o ato
    - O receptor tem condições de provar que o transmissor transmitiu a mensagem
  - Irretratabilidade da recepção
    - Controlar que uma determinada entidade que tenha recebido uma mensagem não possa alegar que não a tenha recebido.
    - O transmissor tem condições de provar que o receptor recebeu a mensagem

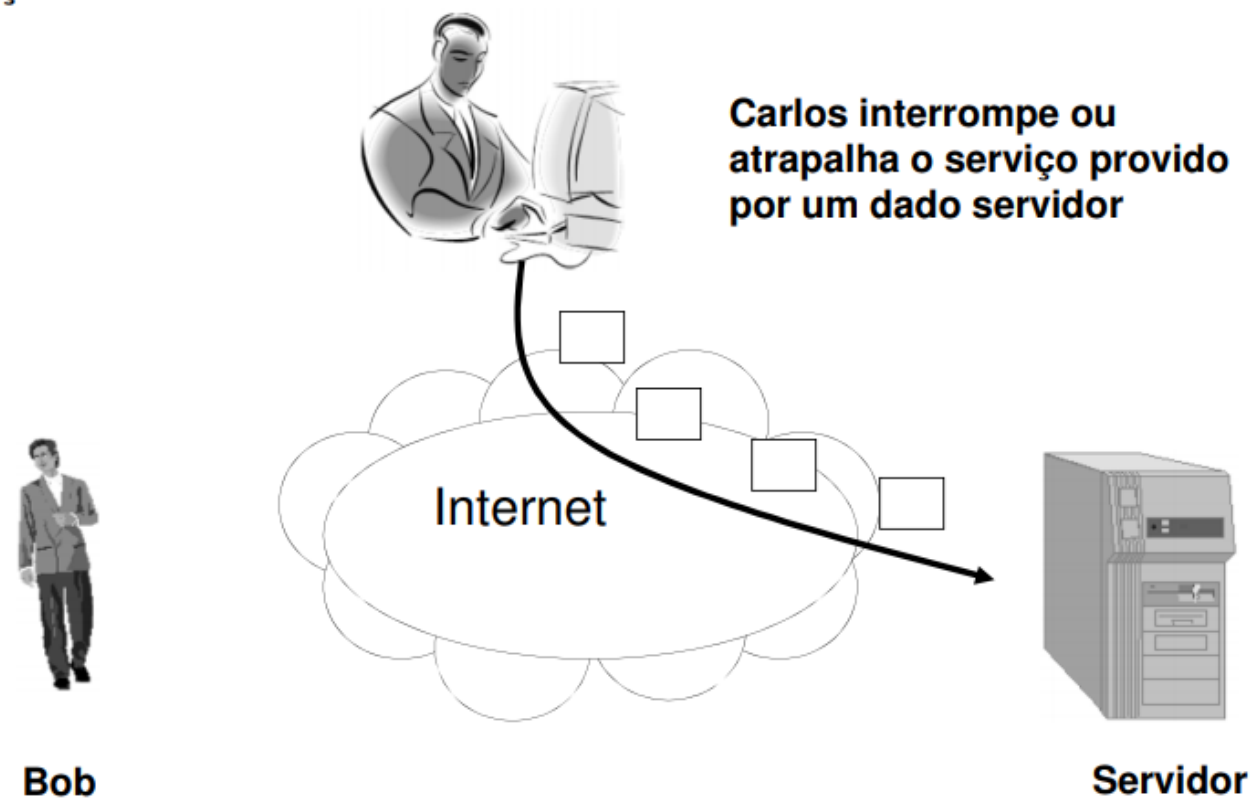
SERVIÇOS DE SEGURANÇA

- **Serviço de Disponibilidade**
  - Controlar ou proteger determinado recurso para que sempre esteja “disponível, acessível e utilizável”

SERVIÇOS DE SEGURANÇA

Serviço de Disponibilidade

Serviço de disponibilidade visa proteger contra ataques ativos de "Negação de Serviço"



SERVIÇOS DE SEGURANÇA

- **Serviço de Controle de Acesso**
  - Controlar que somente entidades autorizadas consigam acesso a determinado recurso.
    - Controla quem acessa e quais condições precisa atender para acessar.
  - Controla que as permissões de acesso sejam dadas apelas pelos responsáveis. E impedir suas alterações por terceiros.

SERVIÇOS DE SEGURANÇA

- **Serviço de Auditoria**
  - Possibilitar o rastreamento dos eventos ocorridos no sistema.
  - Para isto é necessário o armazenamento de informações sobre utilização de recursos do sistema

- **Possibilita:**
  - Verificar se a política de segurança está sendo cumprida
  - A identificação de acessos indevidos.
  - O rastreamento dos eventos.

MECANISMOS DE SEGURANÇA

- **Criptografia**
  - Criptografia Reversível
    - Envolve cifração e decifração de dados (dois sentidos de processamento)
  - Criptografia Irreversível
    - Envolvem algoritmos matemáticos para transformar dados legíveis apenas em códigos ilegíveis (cifração – apenas um sentido de processamento)
    - Incluem algoritmos de Hash e códigos de autenticação de mensagem .
  - **Assinatura digital**
  - **Controle de acesso e permissões em sistemas operacionais**

CRIPTOGRAFIA

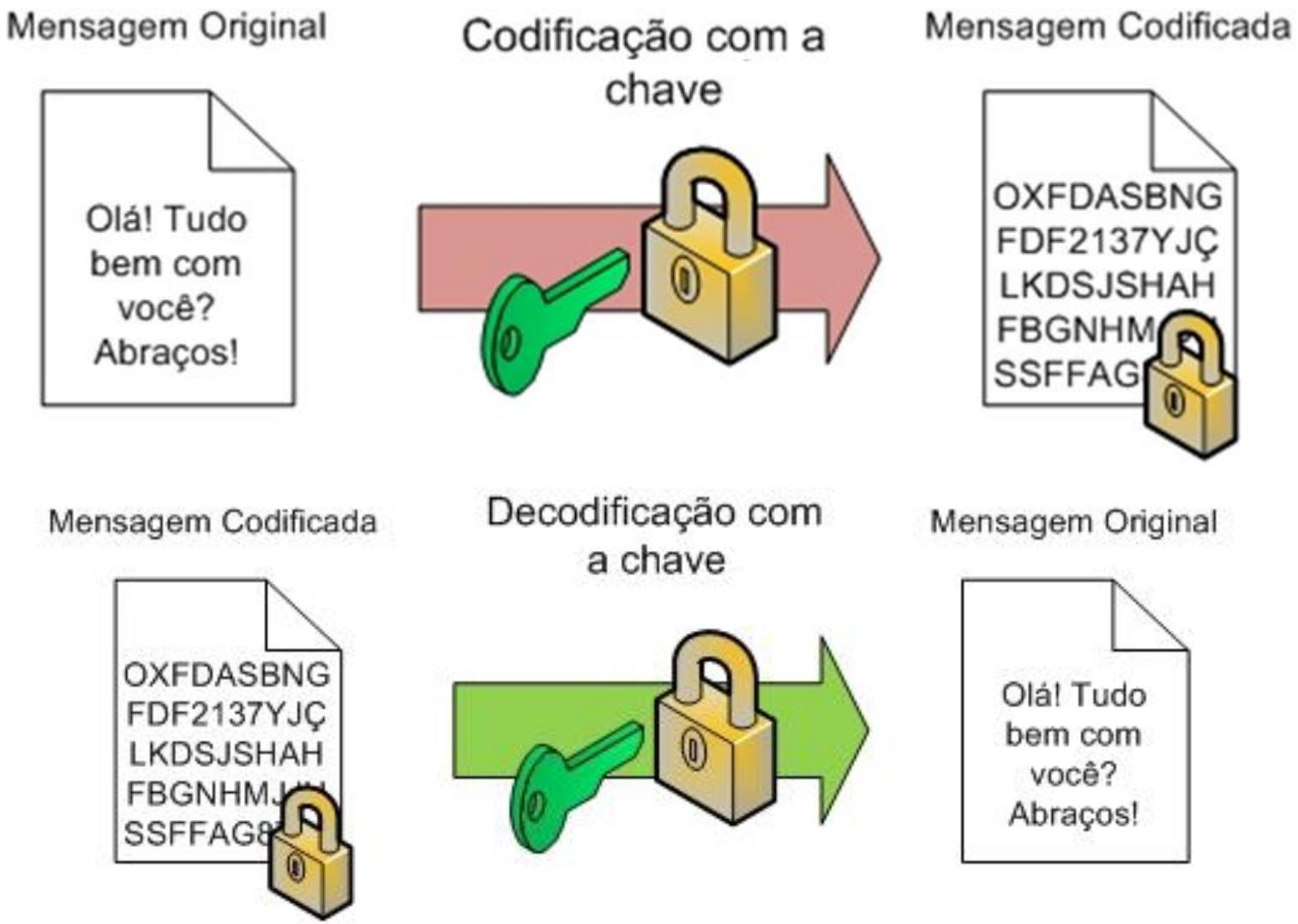
CRIPTOGRAFIA

- Processo de transformação, por meio de uma chave criptográfica, da informação legível (mensagem) em informação ilegível (texto cifrado)
- Processo de transformação é chamado de algoritmo de criptografia
- Somente os indivíduos que conhecem a chave criptográfica podem ter a capacidade de decifrar o texto cifrado e recriar o texto legível (mensagem)
- a maior dificuldade em decifrar deve residir em descobrir a chave secreta, ao contrário de manter o segredo do método utilizado (algoritmo)

CRIPTOGRAFIA

- Pode ser classificada segundo três critérios:
  - Quanto ao número de chaves utilizadas
    - Simétrica
    - Assimétrica
  - Quanto à forma de processamento do texto legível
    - Bloco
    - Stream (fluxo contínuo de informação)
  - Quanto ao tipo de operação usada para transformar o texto legível em texto cifrado
    - Substituição
    - Transposição

CRIPTOGRAFIA



CLASSIFICAÇÃO

Quanto ao número de chaves utilizadas

CRIPTOGRAFIA

- Simétrica
  - Convencional
    - A mesma chave é utilizada para cifrar e decifrar a mensagem.
- Assimétrica
  - Criptografia de chave publica
    - Uma chave para cifrar e outra chave para decifrar a mensagem.

CRIPTOGRAFIA

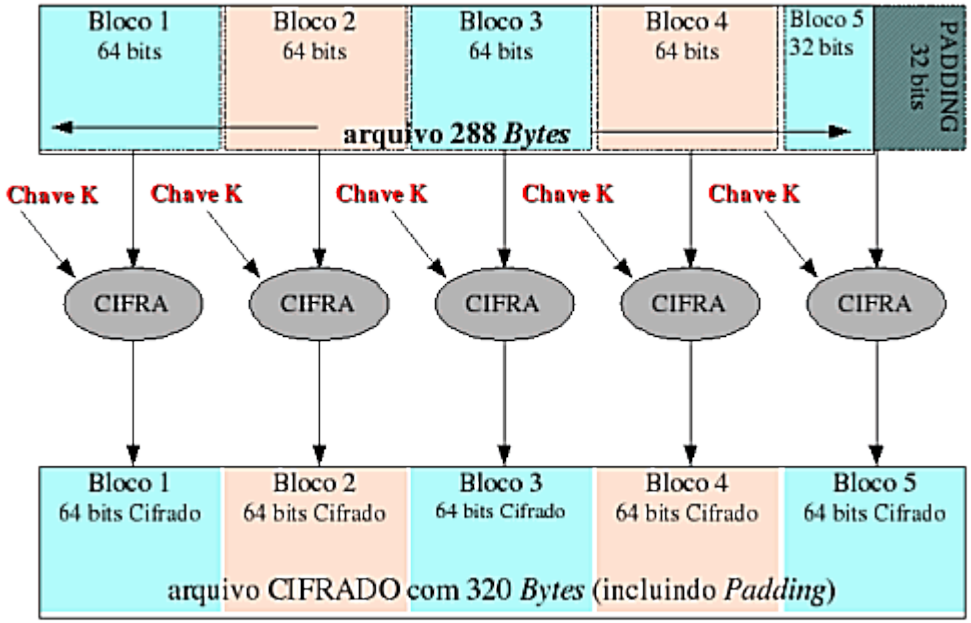
- Criptografia de chave pública ou assimétrica
  - Utiliza-se 2 chaves que atuam de forma complementar

CLASSIFICAÇÃO

Quanto à forma de processamento de texto legível

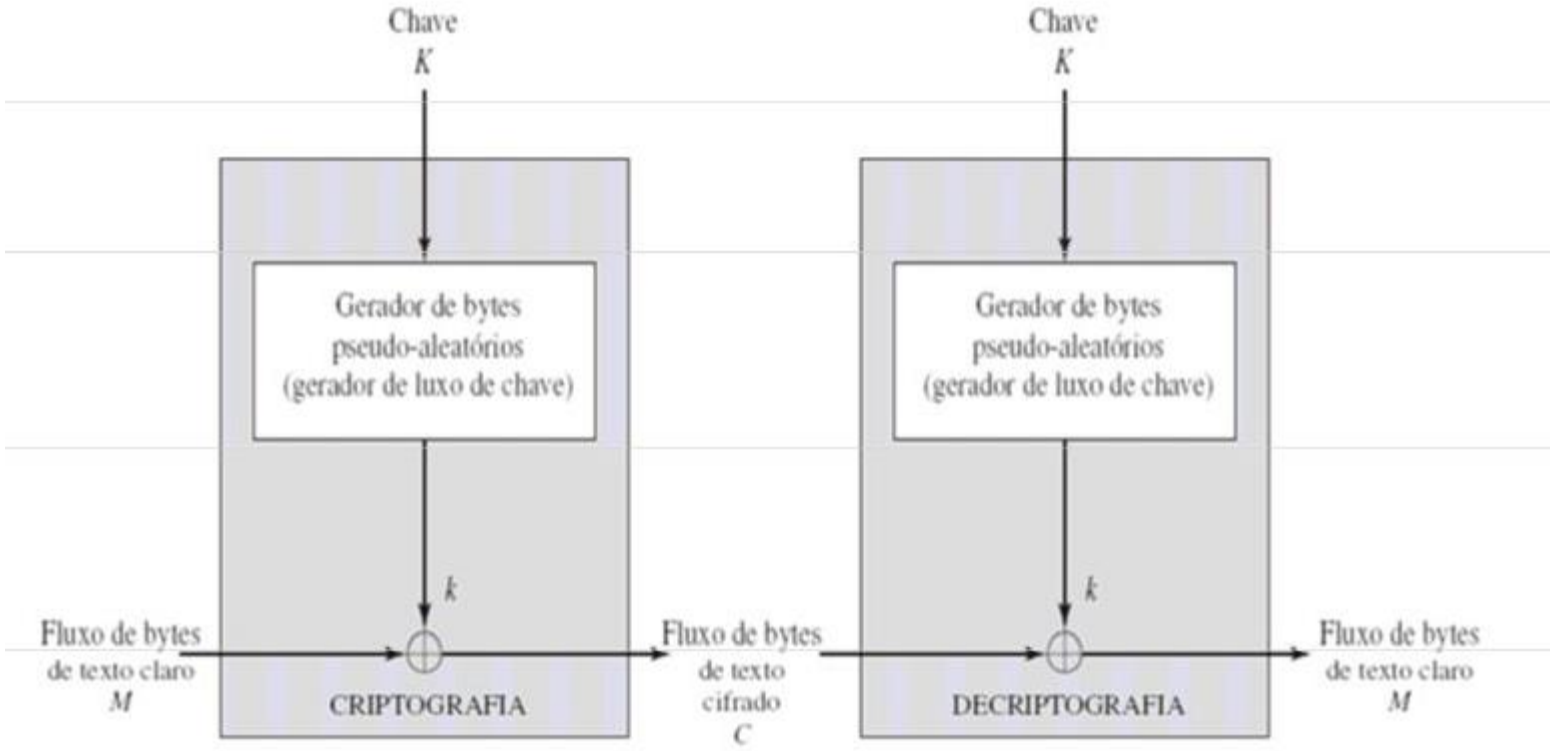
CRIPTOGRAFIA

- Por bloco
  - Processa um bloco de elementos por vez, produzindo assim um bloco de saída correspondente
- Principais características de cifras de bloco:
  - Possui um tamanho de bloco específico Possui um tamanho da chave específico
  - Quebra o texto a cifrar em blocos
  - Exemplos:
    - DES (64),
    - IDEA(64),
    - AES(128/192/256).
  - Mais lenta



CRIPTOGRAFIA

- Stream ou cifra de fluxo
  - Processa os elementos de entrada de forma contínua (bit a bit, ou byte a byte)

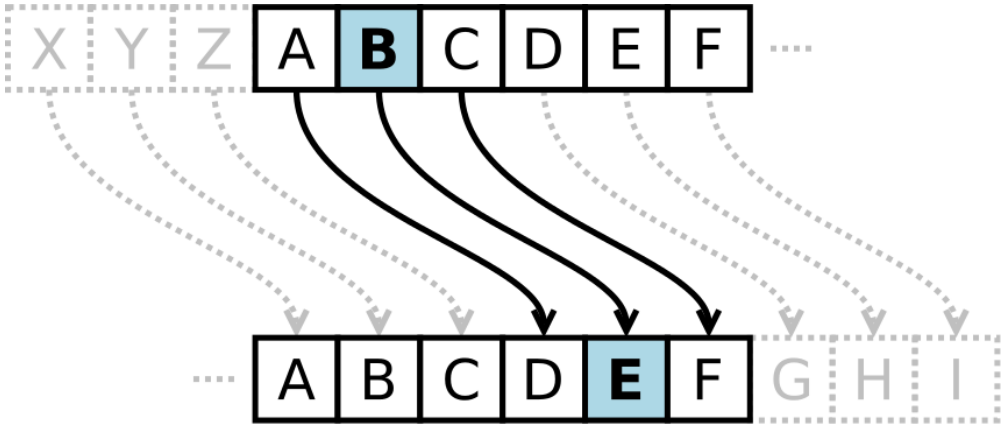


CLASSIFICAÇÃO

Quanto ao Tipo de operação usada para transformar o texto legível em cifrado.

CRIPTOGRAFIA

- Substituição
  - Cada elemento do texto legível (bit, letra, grupo de bits ou letras) é substituído ou mapeado em outro elemento diferente
- Transposição
  - Os elementos do texto legível são reorganizados.



Transposição só embaralha as letras

Canarana

Cafe -> fdih

aanaracn

CRIPTOGRAFIA

- **Esquema de Criptografia Incondicionalmente Seguro**
  - Esquema que produz texto cifrado desprovido de informações suficientes para determinar o texto legível correspondente (independentemente de quanto texto cifrado esteja à disposição de um atacante)
    - Deve ser impossível decifrar o texto cifrado

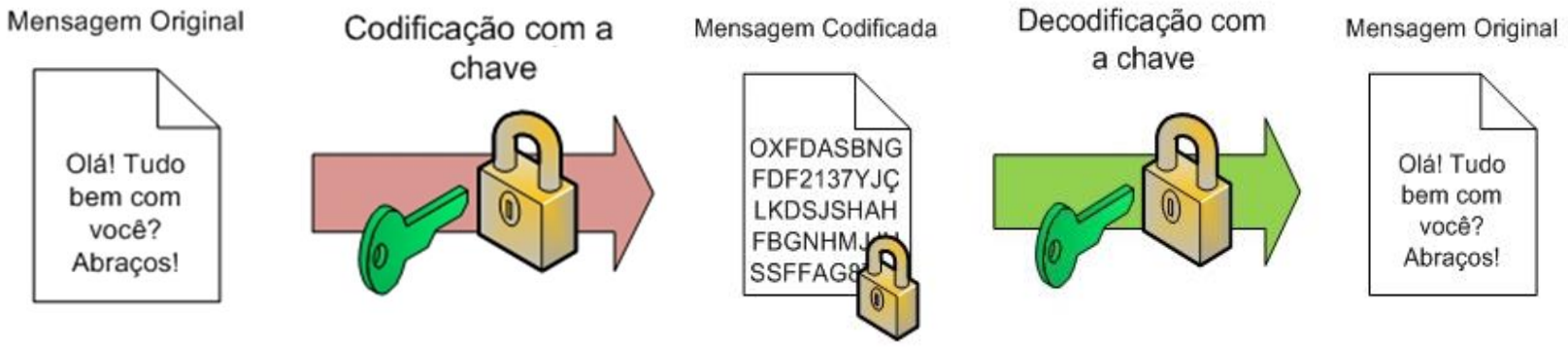
- **Esquema de Criptografia Computacionalmente Seguro**
  - Esquema que atende a um dos dois critérios definidos a seguir
    - 1. Custo para quebrar a cifra é superior ao valor da informação codificada
    - 2. Tempo exigido para quebrar a cifra é superior ao tempo de vida útil da informação

CRIPTOGRAFIA

- Princípio de segurança
  - Algoritmo de criptografia e de decifração sugere-se ser de **conhecimento público**
  - Ou seja:
    - A segurança do método **NUNCA** deve estar baseada na ocultação do algoritmo, mas sim no segredo da chave criptográfica

- Razões?
  - Caso a segurança seja baseada na ocultação do algoritmo e este seja divulgado, seria necessário trocar todas as implementações deste.
  - As pessoas que trabalharam no desenvolvimento conhecem o algoritmo

CRIPTOGRAFIA SIMÉTRICA



CRIPTOGRAFIA SIMÉTRICA

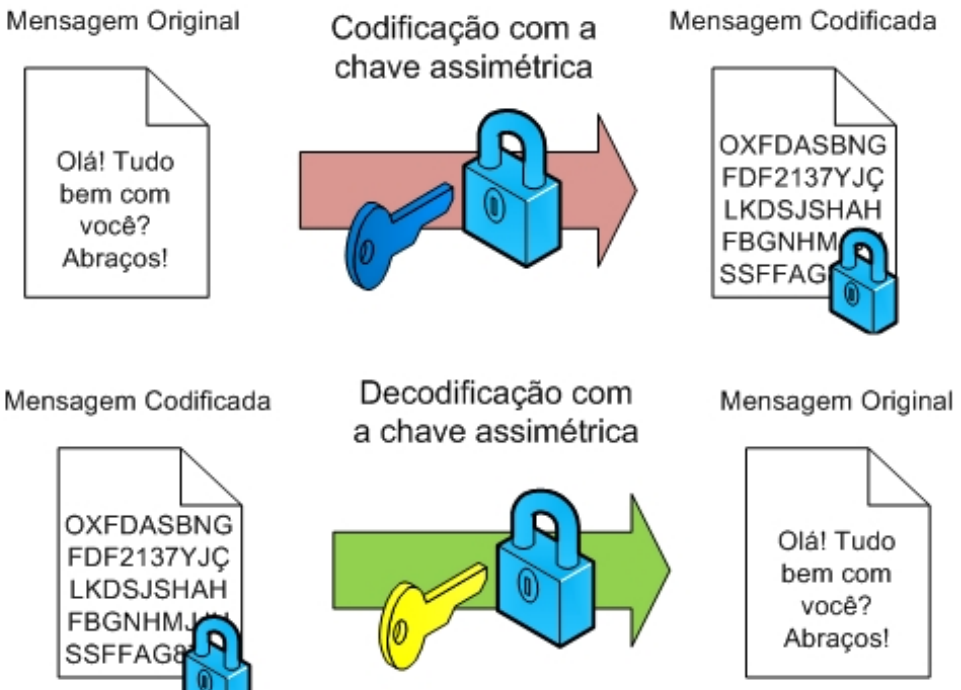
- **Requisitos para uso seguro da criptografia simétrica**
  - Algoritmo forte.
    - Quem conhece o algoritmo deve ser incapaz de decifrar o texto.
    - Resistente a ataques (força bruta)
  - Emissor e receptor devem manter a chave secreta protegida
  - **Apenas a chave deve ser secreta**
  - **Principal problema de segurança??**
  - Manter a chave em sigilo

Principais Algoritmos

Nome	Tipo	Tam. chave	Tam. bloco
DES	bloco	56	64
Triple DES (2 ch.)	bloco	112	64
Triple DES (3 ch.)	bloco	168	64
IDEA	bloco	128	64
BLOWFISH	bloco	32 a 448	64
RC5	bloco	0 a 2040	32,64,128
CAST-128	bloco	40 a 128	64
RC2	bloco	0 a 1024	64
RC4	stream	0 a 256	--
Rijndael (AES)	bloco	128,192,256	128, 192, 256
Twofish	bloco	128,192,256	128

CRIPTOGRAFIA ASSIMÉTRICA

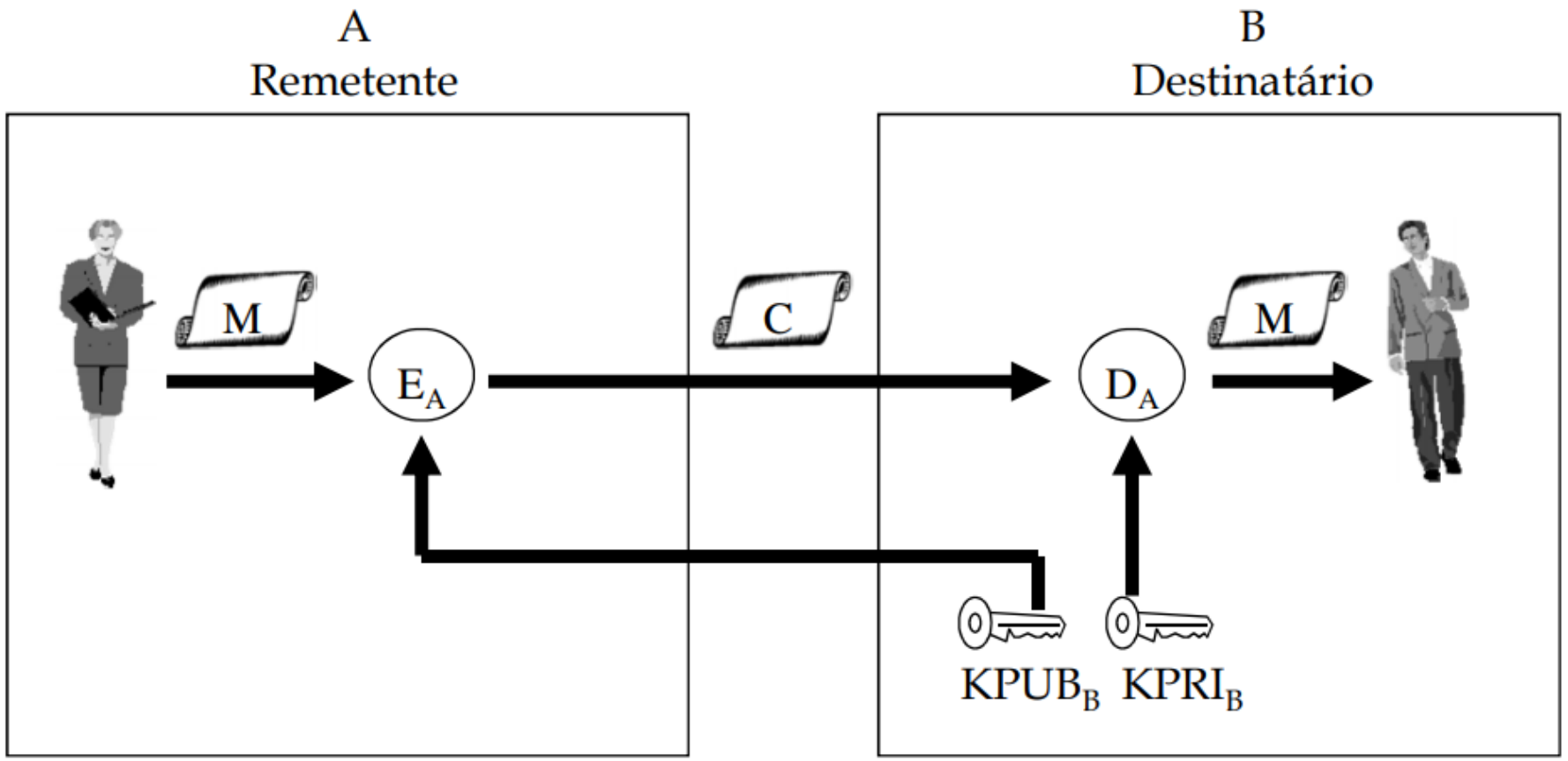
Criptografia de chave publica



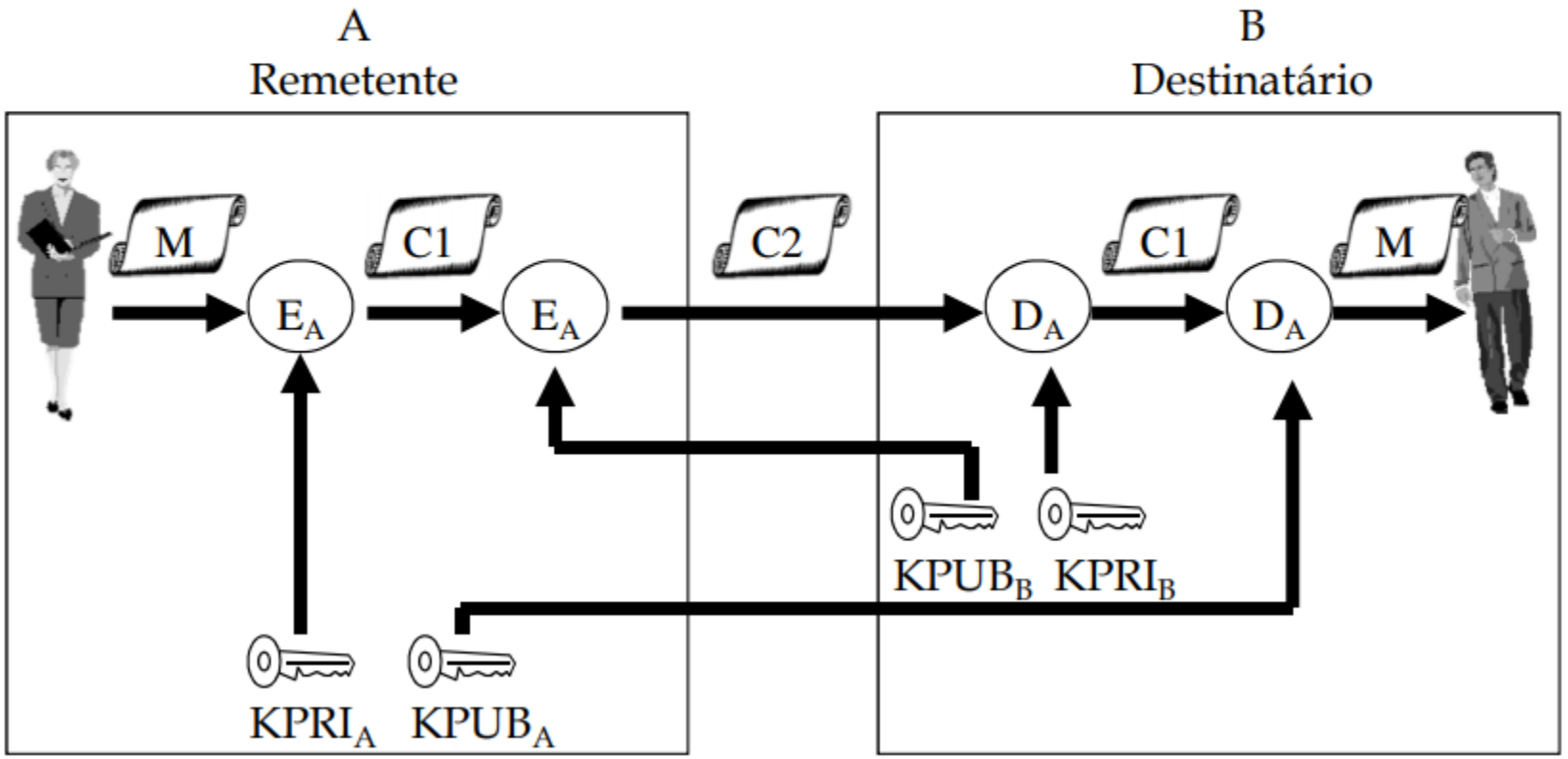
CRIPTOGRAFIA ASSIMÉTRICA

- Lançado para resolver os problemas da criptografia simétrica
  - Distribuição de chaves.
  - Autenticação.

- **Funcionamento**
  - O remetente cifra a mensagem utilizando a chave pública do destinatário e depois transmite
  - O destinatário recebe o texto cifrado e depois decifra a mensagem utilizando sua chave privada.
  - Como somente o destinatário conhece sua chave privada que se manteve secreta, somente ele pode recuperar a mensagem, e assim consegue-se obter o nível de sigilo desejado


A
Remetente
B
Destinatário
M
E_A
C
D_A
M
$KPUB_B$
$KPRI_B$

Utilização:
Confidencialidade e autenticação



FUNÇÕES HASH

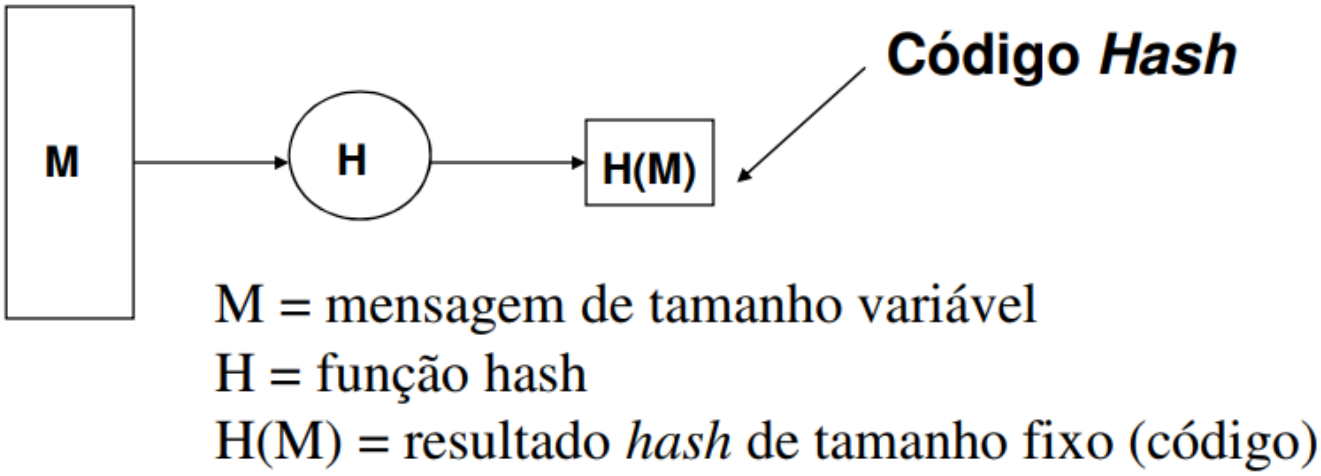
HASH

- Utilizado para resolver o problema de integridade de dados

- Exemplos de sistemas que apresentam mecanismos de integridade
  - Armazenamento de informações em disco
  - Comunicação de dados (troca de arquivos)

HASH

- **Função Hash Unidirecional**
  - Função matemática que envolve todos os bits da mensagem
  - Aceita como entrada uma mensagem M de tamanho variável e gera como saída um código *hash* de tamanho fixo
  - Bloco básico para implementação do serviço de integridade que depende apenas de M como entrada M

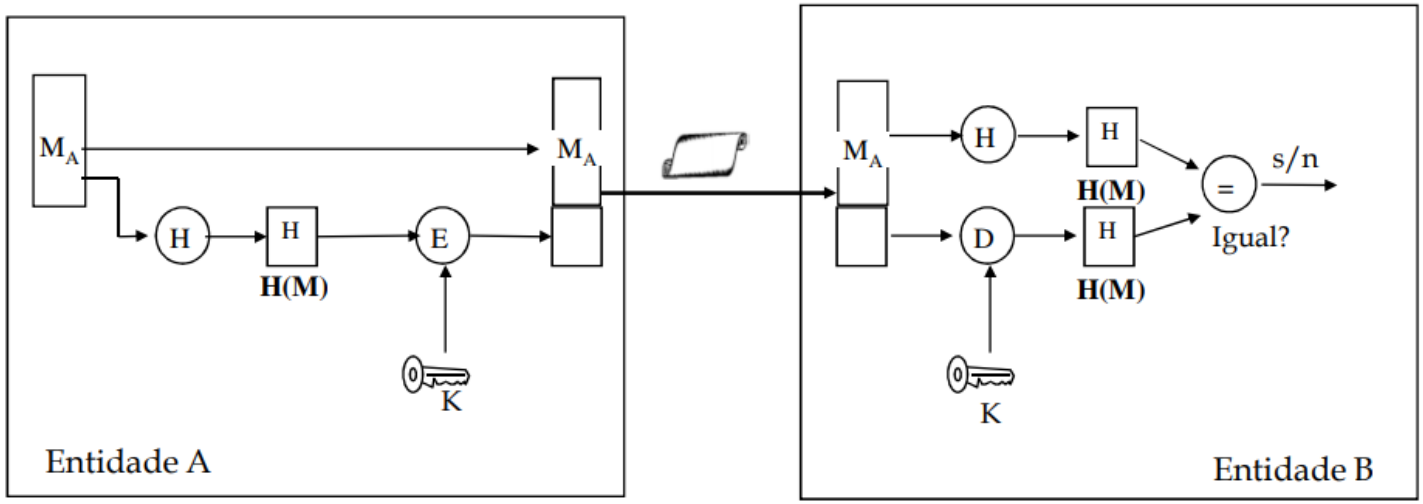


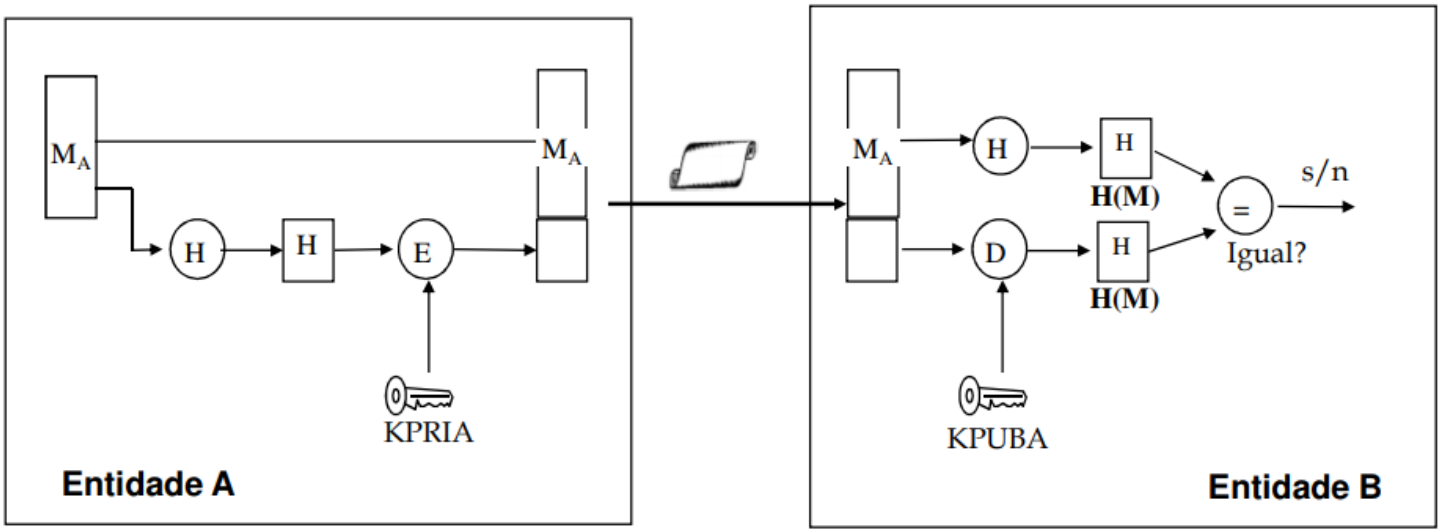
HASH

- **Isoladamente, a função hash não é suficiente para se evitar modificações intencionais!**

- São necessários mecanismos adicionais para evitar as modificações intencionais
- Neste caso, o código ou resultado *hash* deve ser protegido para impedir que seja alterado por entidades não autorizadas.
- **Existem duas formas de proteger o código *hash***
  - Criptografia simétrica
  - Criptografia assimétrica

HASH


M_A
H
H
H(M)
E
K
Entidade A
M_A
H
H
H(M)
D
H
H(M)
K
=
s/n
Igual?
Entidade B


M_A
H
H
E
KPRIA
Entidade A
M_A
H
H
H(M)
D
H
H(M)
KPUBA
=
s/n
Igual?
Entidade B

HASH

Principais algoritmos

Algoritmo de Hash	Compr. Hash	kbytes/s
GOST Hash	256	11
MD4 - Message Digest 4	128	236
MD5 - Message Digest 5	128	174
N-HASH (12 rounds)	128	29
N-HASH (15 rounds)	128	24
RIPE-MD	128	182
RIPE-MD-160	160	---
SHA-1 Secure Hash Algorithm	160	75
SHA-2 Family (224, 256, 512 etc)	----	----
SNEFRU (4 passos)	128	48
SNEFRU (8 passos)	128	23
WHIRLPOOL (ISO/IEC 10118-3:2004)	512	----

Fonte: Applied Cryptography

FONTES

Todos os dados apresentados foram retirados dos materiais desenvolvidos pelos professores aqui mencionados com prévia autorização

Prof. Dr. Adilson Eduardo Guelfi[1]
Prof. Dr. Volnys Borges Bernal[2]

(1) Faculdade de Informática de PP
UNOESTE

(2) Laboratório de Sistemas Integráveis
Escola Politécnica da USP

AGRADEÇO A ATENÇÃO E PARTICIPAÇÃO DE TODOS

Lucas Lanza