

## Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

**Assinaturas  
Digitais**

Ger. de Chaves  
Públicas

Seg. da  
Comunicação

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- **Criptografia**
  - Motivação, mostrei números de incidentes. A Internet cada vez mais com recursos financeiros envoldidos....
  - Tipos (Substituição, Transposição, Uso único, quântico)
  - Modos (ECB, Feedback, Cifra de fluxo, Contador,...?)
- **Algoritmos Simétricos:** Mesma K abre e fecha, alg vistos (DES, 3DES, AES). Qual é o problema desse algoritmo? Como mandar a K para o outro lado?



PUC Minas

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

**Assinaturas  
Digitais**

Ger. de Chaves  
Públicas

Seg. da  
Comunicação

Protocolos de  
Autenticação

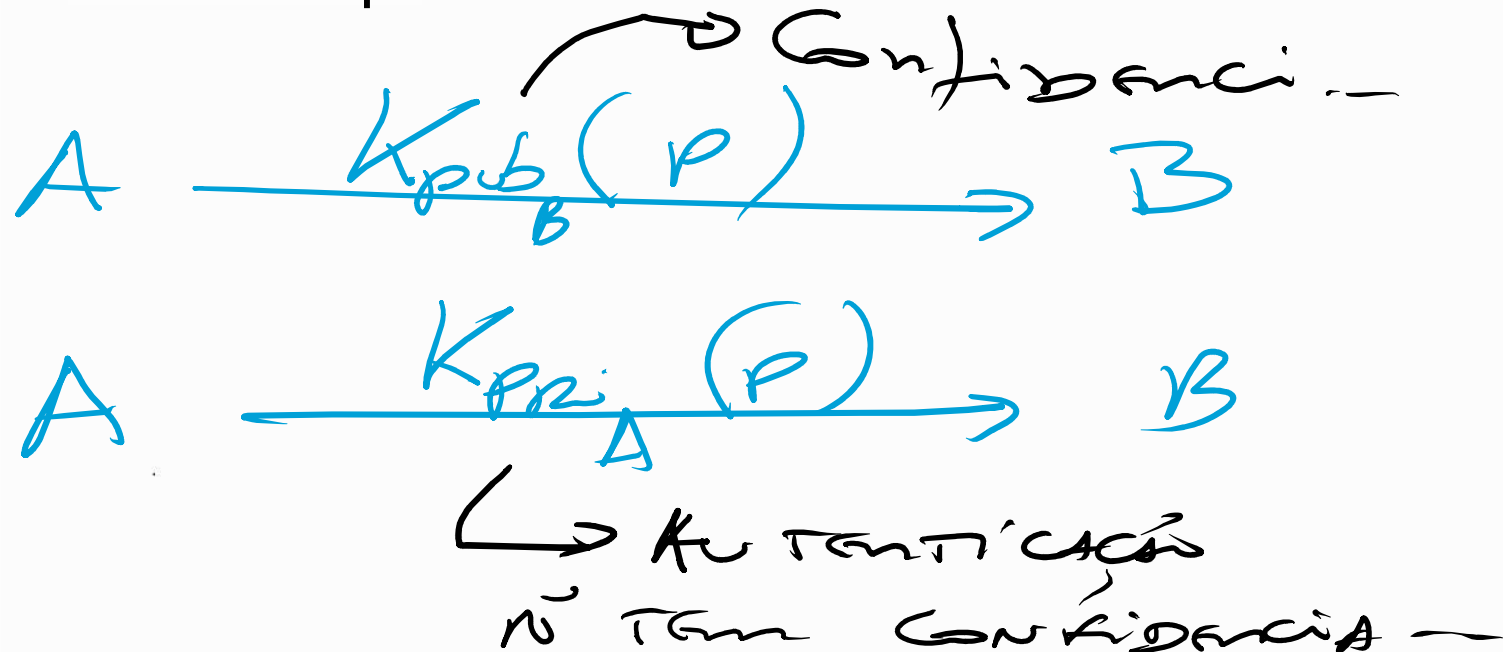
Seg. de Correio

Seg. da WEB

Questões  
Sociais

- Algoritmo Assimétrico: Uso  $K$ 's diferentes. Uma fecha e a outra abre. Neste par de  $K$  eu tenho uma pública que todos podem conhecer e eu tenho uma privada que mantenho em sigilo. Exemplos de Algoritmos (RSA, mochila, logaritmos...). Problema? Mais lento + Como eu sei que estou com a pública correta?

# Revisão





PUC Minas

# Promessa que eu fiz

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

**Assinaturas  
Digitais**

Ger. de Chaves  
Públicas

Seg. da  
Comunicação

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- Ensinar os Algoritmos
  - Simétrico
  - Assimétrico
- Aplicar os Algoritmos
  - Assinatura Digital

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

**Assinaturas  
Digitais**

Ger. de Chaves  
Públicas

Seg. da  
Comunicação

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- Condições Exigidas
- Tipos:
  - Assinaturas de chave simétrica
  - Assinaturas de chave pública
  - Sumário de mensagens
- O ataque do aniversário

$K_{pub}$ ?  
 $K_{priv}$ ?

# Condições Exigidas

Simétrica  $K_{xy}$

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

**Assinaturas  
Digitais**

Ger. de Chaves  
Públicas

Seg. da  
Comunicação

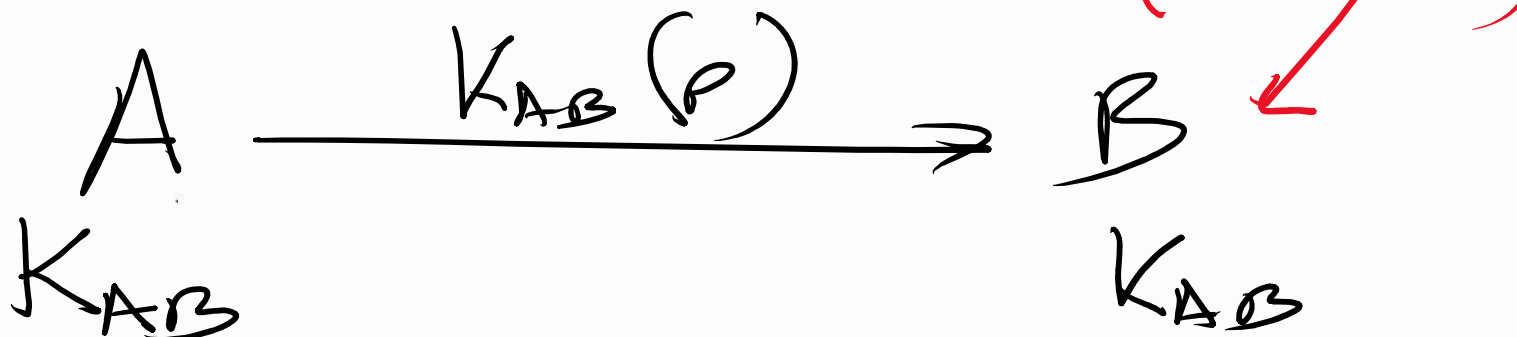
Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

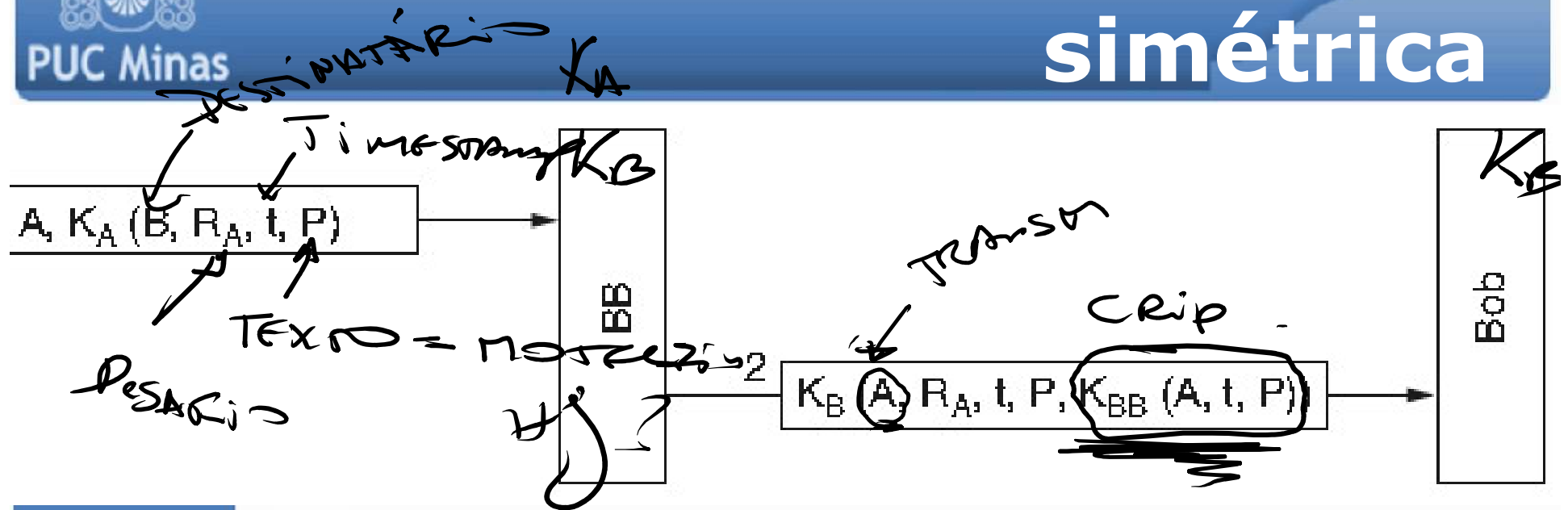
1. O receptor pode verificar a identidade alegada pelo transmissor
2. O transmissor não pode repudiar o conteúdo da mensagem posteriormente
3. O receptor não tem a possibilidade de criar a mensagem por si próprio





PUC Minas

# Assinaturas de chave simétrica



Ger. de Chaves  
Públicas

Seg. da  
Comunicação

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

Assinaturas digitais com Big Brother.

- Problema:
  - Todos devem confiar em BB;
  - Todas as mensagens assinadas devem ser lidas por BB.



PUC Minas

# Assinaturas de chave pública (1)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

**Assinaturas Digitais**

Ger. de Chaves Públicas

Seg. da Comunicação

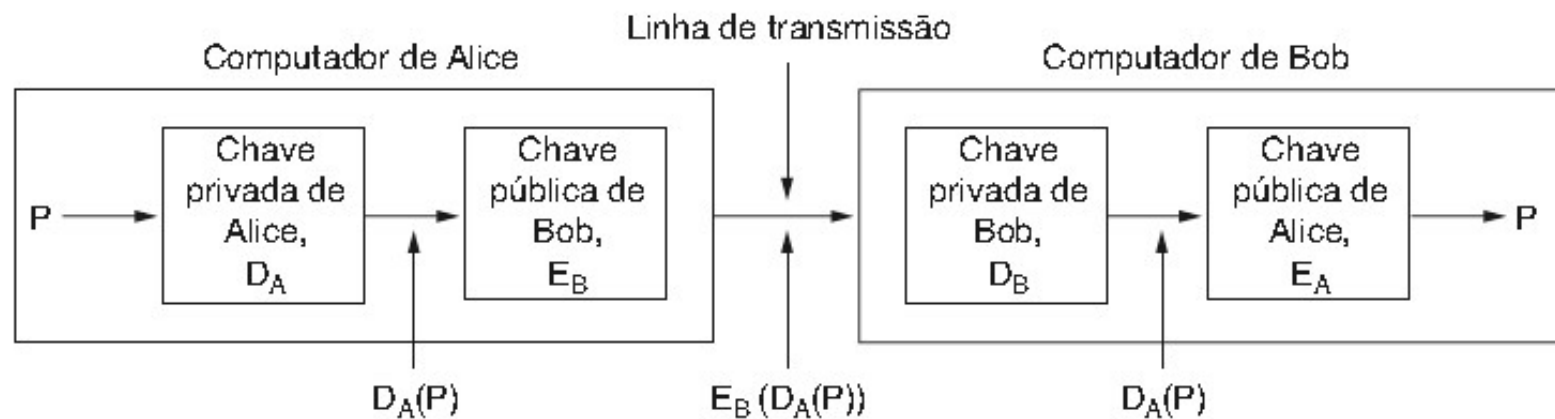
Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

$$D_A = K_{\text{priv}A}(P)$$
$$E_A = K_{\text{pub}A}(P)$$



Assinaturas digitais usando criptografia de chave pública.

# Assinaturas de chave pública (2)

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

**Assinaturas  
Digitais**

Ger. de Chaves  
Públicas

Seg. da  
Comunicação

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

## Críticas ao DSS:

1. Supersecreto
2. Muito lento
3. Muito recente
4. Muito inseguro





PUC Minas

# Sumário de mensagens (1)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

**Assinaturas Digitais**

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

Propriedades:

1. Dado  $P$ , fácil calcular  $MD(P)$
2. Dado  $MD(P)$ , efetivamente impossível determinar  $P$
3. Dado  $P$  ninguém pode encontrar  $P'$  tal que  $MD(P') = MD(P)$
4. Uma mudança na entrada de 1 bit apenas produz uma saída muito diferente



PUC Minas

# Sumário de mensagens (2)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

**Assinaturas Digitais**

Ger. de Chaves Públicas

Seg. da Comunicação

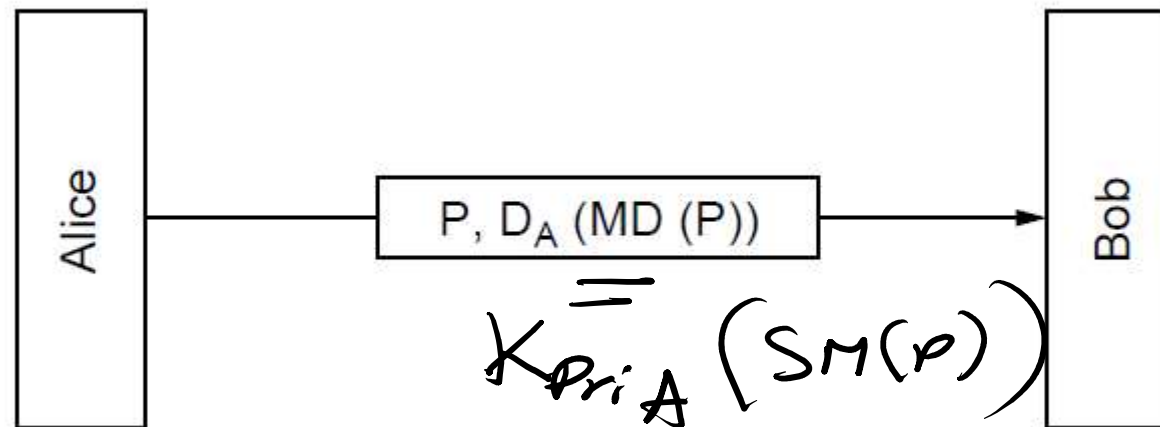
Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

Assinaturas digitais usando sumário de mensagens.





PUC Minas

# Sumário de mensagens (3)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

**Assinaturas Digitais**

Ger. de Chaves Públicas

Seg. da Comunicação

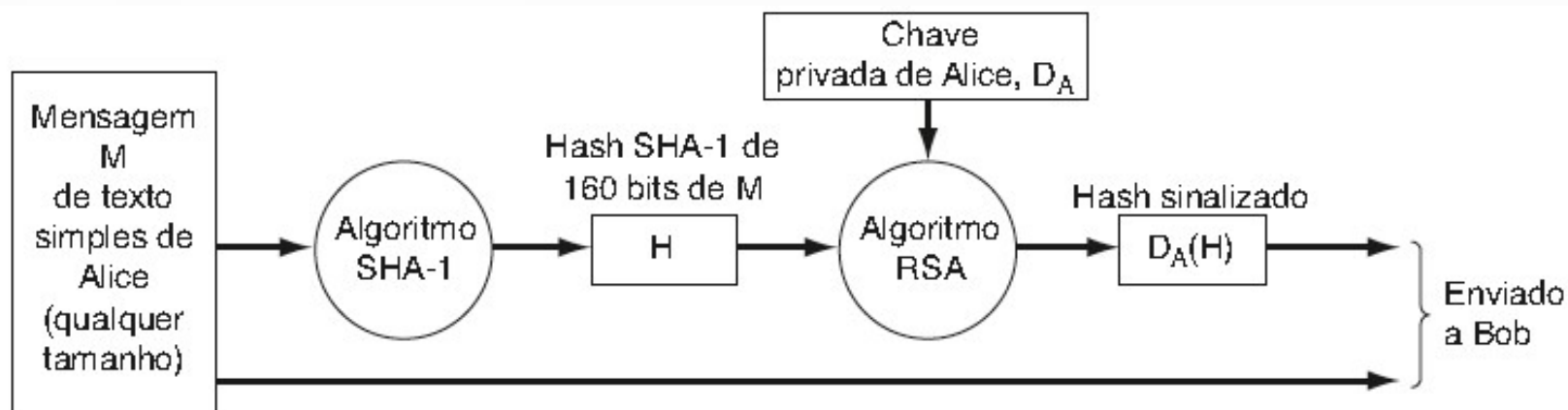
Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

Uso do SHA-1 e RSA na assinatura de mensagens não secretas.





PUC Minas

# Sumário de mensagens (4)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

**Assinaturas Digitais**

Ger. de Chaves Públicas

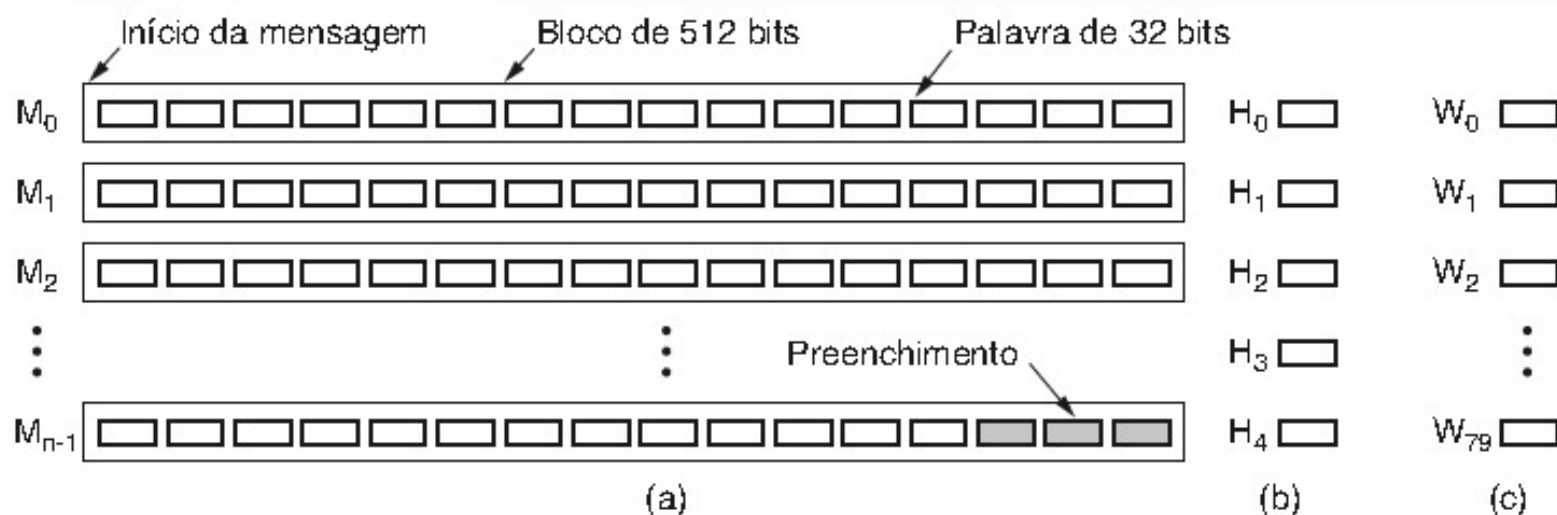
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



(a) Uma mensagem preenchida até um múltiplo de 512 bits.

(b) Variáveis de saída. (c) Array de palavras.

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

**Assinaturas  
Digitais**

Ger. de Chaves  
Públicas

Seg. da  
Comunicação

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

## Características:

O item segurança considera que o ataque do aniversário em um message digest de tamanho  $n$  produz uma colisão com fator de trabalho de aproximadamente  $2^{n/2}$ .

Algoritmo	Tamanho da mensagem (bits)	Tamanho do bloco (bits)	Tamanho da palavra (bits)	Tamanho do message digest (bits)	Segurança (bits)
SHA-1	$< 2^{64}$	512	32	160	80
SHA-256	$< 2^{64}$	512	32	256	128
SHA-384	$< 2^{128}$	1024	64	384	192
SHA-512	$< 2^{128}$	1024	64	512	256

# Ataque do Aniversário

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

**Assinaturas  
Digitais**

Ger. de Chaves  
Públicas

Seg. da  
Comunicação

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- *Plaintext* diferentes mas com uma quantidade razoável de texto semelhante pode gerar assinaturas iguais que levariam a possibilidade de transmissões adulteradas com assinaturas corretas;



PUC Minas

# Resumo em 02-10

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

→ MOTIVAÇÃO, tipos, modos

→ MESMA K abre e fecha

→ Chaves diferentes uma abre e outra fecha.

→ 3 requisitos

3 soluções

→ Risco de ataque do Adm  
então preciso de uma

PKI = Certificado



PUC Minas

# Gerenciamento de chaves públicas (1)

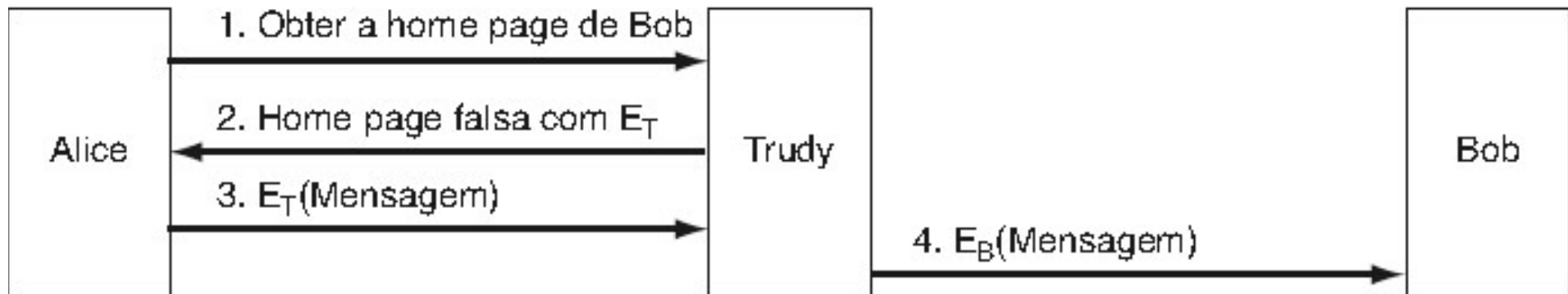
Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Problema: Como obter a chave pública da pessoa desejada ao invés da Trudy?



Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

Um modo de Trudy subverter a criptografia de chave pública. Conhecido Ataque do Homem do meio.



# Gerenciamento de chaves públicas (2)

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

**Gerenciamento  
de Chaves  
Públicas**

Seg. da  
Comunicação

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

- Certificados
- X.509
- Infraestruturas de chave pública



PUC Minas

# Certificados

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave

Púb

Ass

Dig

Ge

de

Púb

Seg

Car

Pro

Aut

Seg

Seg. da WEB

Questões Sociais

Ver

Keri

256 bits

Um possível certificado e seu hash assinado.

Certifico que a chave pública

19836A8B03030CF83737E3837837FC3s7092827262643FFA82710382828282A

pertence a

João Roberto da Silva

Avenida Brasil, 12345

Rio das Ostras, RJ 28890-000

Nascimento: 7 de setembro de 1958

E-mail: bob@supernet.com.br

= 64 hexade  
=  
256 bits

Hash SHA-1 do certificado acima assinado com a chave privada da CA



PUC Minas

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

**Gerenciamento  
de Chaves  
Públicas**

Seg. da  
Comunicação

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

A

BB

Reg BB

$K_{pubBB}$

Certified

$V_{procc}(SM(RegBB))$  \*

Certificado Digital



PUC Minas

# X.509

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

**Gerenciamento  
de Chaves  
Públicas**

Seg. da  
Comunicação

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

## Campos básicos de um certificado X.509.

Campo	Significado
Version	A versão do X.509
Serial number	Este número, somado ao nome da CA, identifica o certificado de forma exclusiva
Signature algorithm	O algoritmo usado para assinar o certificado
Issuer	Nome X.500 da CA
Validity period	Períodos inicial e final de validade
Subject name	A entidade cuja chave está sendo certificada
Public key	A chave pública da entidade certificada e a ID do algoritmo utilizado
Issuer ID	Uma ID opcional que identifica de forma exclusiva o emissor do certificado
Subject ID	Uma ID opcional que identifica de forma exclusiva a entidade certificada
Extensions	Muitas extensões foram definidas
Signature	A assinatura do certificado (assinado pela chave privada da CA)



PUC Minas

# Infraestruturas de chave pública

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

**Gerenciamento de Chaves Públicas**

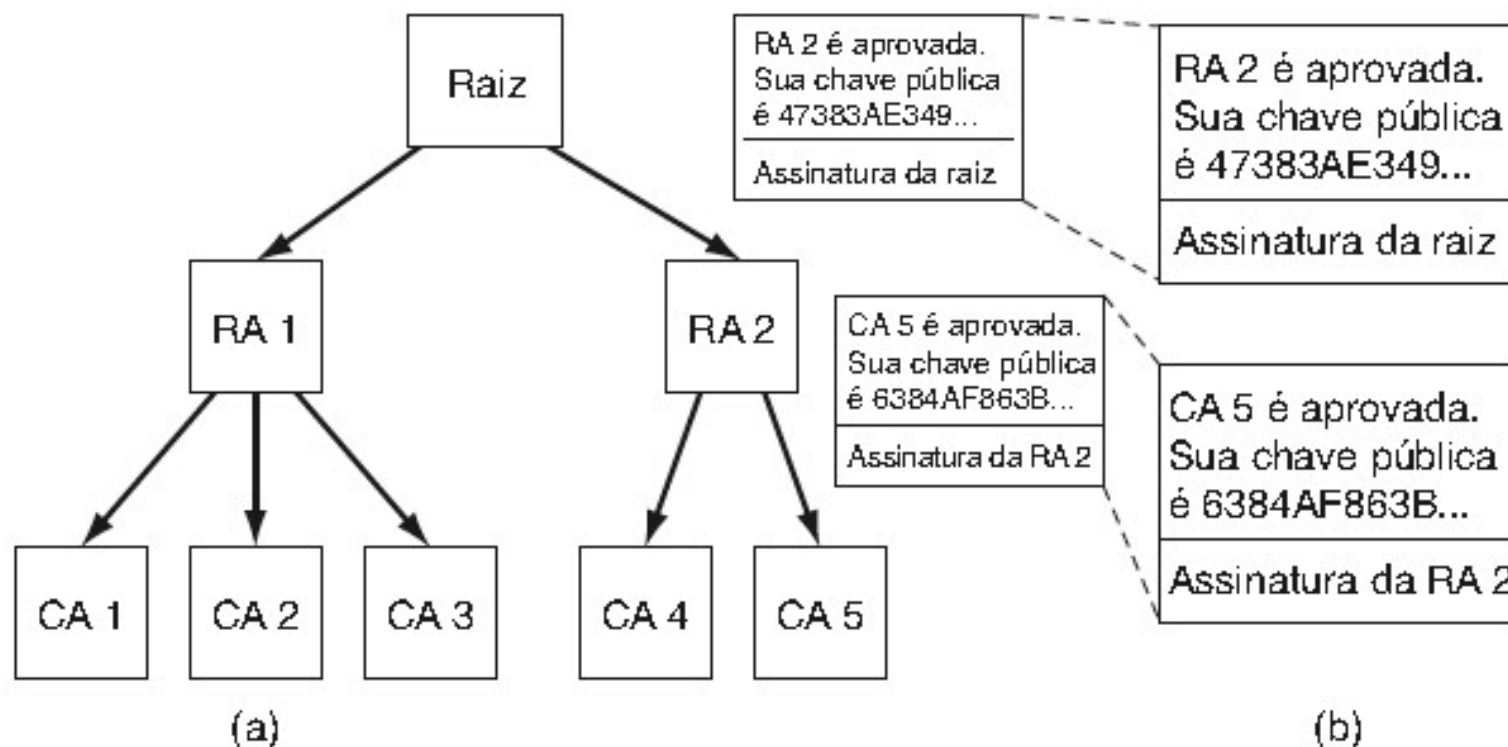
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



(a) Uma PKI hierárquica. (b) Cadeia de certificados.



PUC Minas

# Desempenho

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

**Gerenciamento  
de Chaves  
Públicas**

Seg. da  
Comunicação

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

- DES e MD5 são muitas ordens de magnitude mais rápida do que o RSA
  - Alpha workstation:
    - DES: 36Mbps ← *Simétrico*
    - MD5: 85Mbps
    - RSA: 1Kbps ← *Assimétrico*
- Geralmente RSA é utilizado para encriptar pequenas quantidades de dados, tais como chave secreta ou algum número sigiloso



PUC Minas

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

**Gerenciamento  
de Chaves  
Públicas**

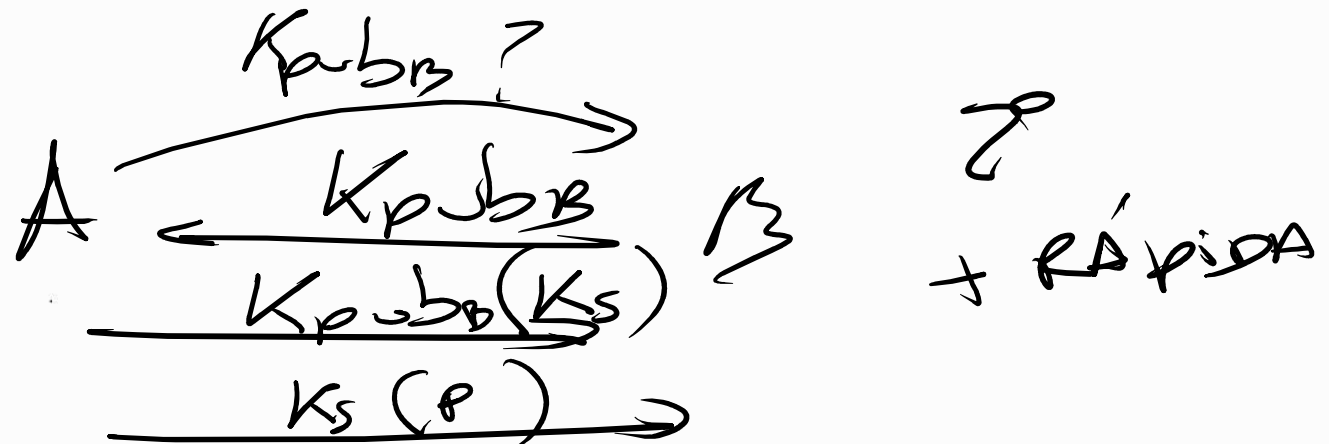
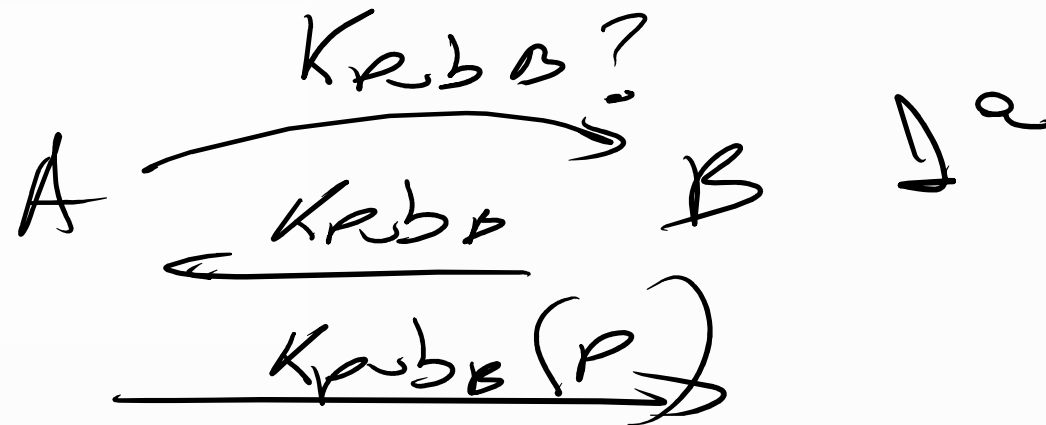
Seg. da  
Comunicação

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- Firewalls
- UTM
- VPNs (Virtual Private Networks)
- Segurança em redes sem fio





Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- Vimos que a Internet não é um local seguro.
- Do ponto de vista de um administrador, as pessoas são divididas entre “bons” – os que podem ter acesso aos dados. E aos vilões – todo o resto de fora da rede.
- As pessoas devem ser identificadas para poder ter acesso.
- Em rede de computadores, o tráfego que entre e sai pela rede deve ser inspecionado, isto é feito pelo firewall



PUC Minas

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

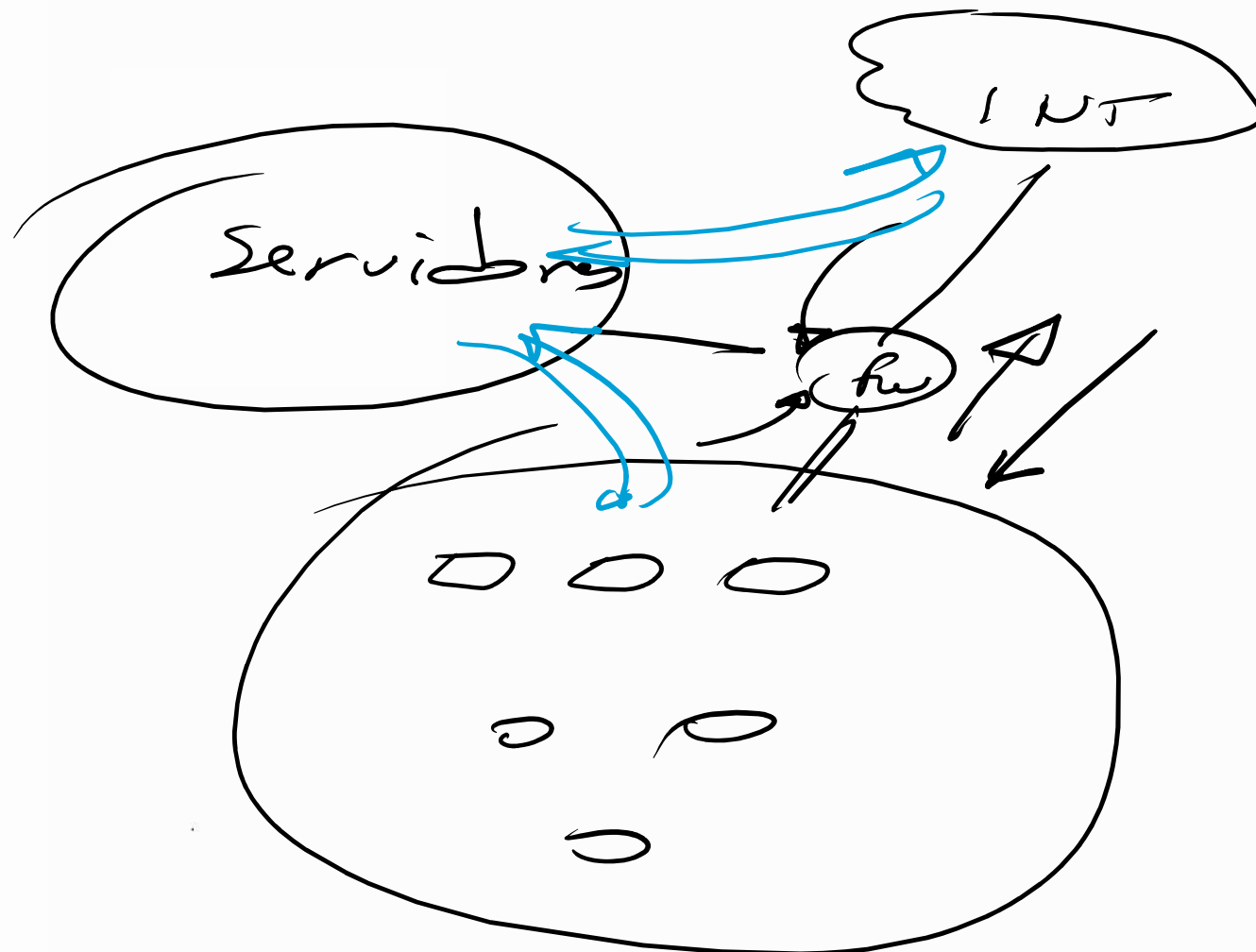
**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais





PUC Minas

# Firewall

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

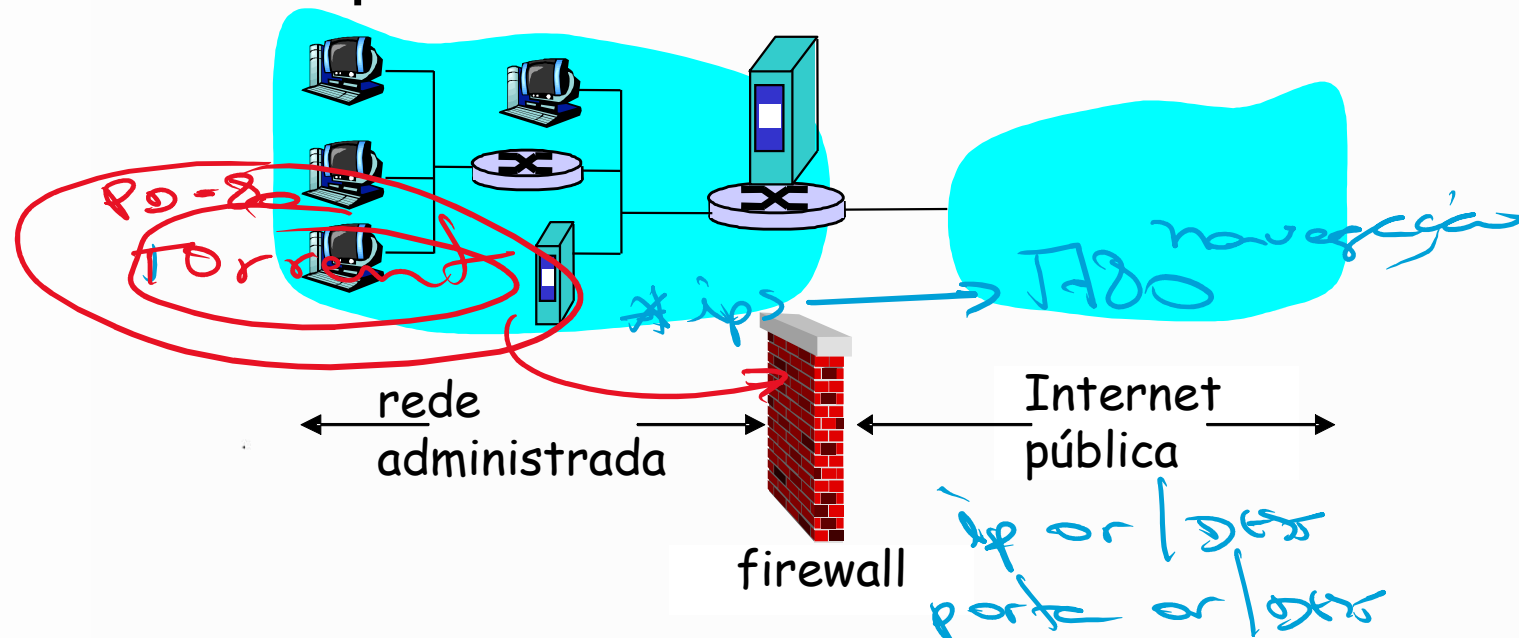
Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- É uma combinação de Hardware e Software que isola a rede interna de uma organização da internet geral. Permite que alguns pacotes passem e bloqueia outros.



Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

**impedir ataques de negação de serviço:**

- inundação de SYN: atacante estabelece muitas conexões TCP falsas, sem recursos deixados para conexões "reais"

**impedir modificação/acesso ilegal de dados internos**

- p. e., atacante substitui página inicial da companhia por algo diferente

**permite apenas acesso autorizado à rede interna** (conjunto de usuários/hospedeiros autenticados)



PUC Minas

# Firewall

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- **Técnicas Gerais:**
  - **Controle de Serviço**
    - Determina os tipos de serviços da Internet que podem ser acessados: *Inbound* ou *Outbound*.
  - **Controle de Direção**
    - Determina a direção na qual as requisições de serviços podem fluir: *Incoming* ou *Outgoing*.
  - **Controle de Usuário**
    - Controla o acesso aos serviços de acordo com os usuários que tentam acessá-los.
  - **Controle de Comportamento**
    - Controla a forma como serviços são utilizados (p. ex., filtrar e-mail)



Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- Possuir três objetivos:
  - Todo tráfego que entra e sai passa pelo firewall, um firewall situado em um ponto de acesso a rede facilita o gerenciamento e a execução de uma política de acesso seguro.
  - Somente o tráfego autorizado poderá passar: limita o acesso ao tráfego autorizado.
  - O próprio firewall é imune a penetração.



PUC Minas

# Firewall

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

## três tipos de firewalls:

- filtros de pacotes sem estado
- filtros de pacotes com estado
- gateways de aplicação

verificando  
IP's de or. Dest  
portas



PUC Minas

# Filtragem de pacotes **SEM** estado

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

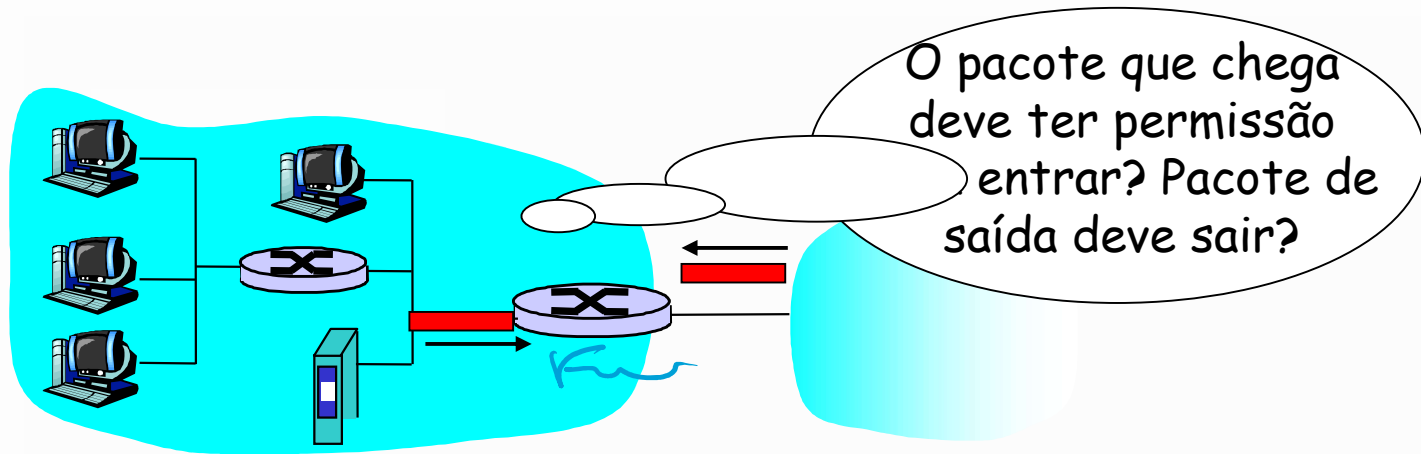
**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais



- Todo o tráfego que entra e sai da empresa passa pelo roteador, onde ocorre a **filtragem de pacotes**.
- roteador **filtra pacote-por-pacote**, decisão de repassar/descartar pacote com base em:
  - endereço IP de origem, endereço IP de destino
  - números de porta de origem e destino do TCP/UDP
  - tipo de mensagem ICMP
  - etc





PUC Minas

# Filtragem de pacotes SEM estado: exemplo

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- Exemplo: para bloquear conexão de entrada, exceto para o servidor de Web público:
  - bloqueia todos os segmentos TCP com exceção dos seguimentos para a porta destino 80 e endereço IP correspondente ao do servidor
- exemplo: bloco entrando e saindo datagramas com campo de protocolo IP = 17 e com porta de origem ou destino = 23
  - todo UDP entrando e saindo fluxos e conexões telnet são bloqueados

# Filtragem de pacotes SEM estado: exemplo

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- Exemplo: se a organização não quer que sua rede interna seja mapeada (rastreio de rota) por um estranho, ela bloqueia todas as mensagens ICMP TTL que saem da rede da administração

# Outros exemplos

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

<u>Política</u>	<u>configuração de firewall</u>
sem acesso externo à Web	descarta todos os pacotes que saem para qualquer endereço IP, porta 80
sem conexões TCP entrando, exceto aquelas apenas para o servidor Web público da instituição	descarta todos pacotes TCP SYN que chegam a qualquer IP, exceto 130.207.244.203, porta 80
impedir que Web-rádios devorem a largura de banda disponível	descarta todos os pacotes UDP que chegam - exceto DNS e broadcasts do roteador
impedir que sua rede seja usada para um ataque DoS smurf	descarta todos os pacotes ICMP indo para um endereço de "broadcast" (p. e., 130.207.255.255)
impedir que sua rede interaja com o programa Traceroute	descarta todo tráfego ICMP TTL de saída



PUC Minas

# Parênteses

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- Um ataque de negação de serviço (DoS Attack - Denial of Service), torna os recursos de um sistema indisponíveis para seus utilizadores
- **DoS smurf:** o endereço IP de retorno do pacote do ping é forjado com o IP do computador de destino. O ping é emitido ao endereço IP de broadcast. Esta técnica faz com que cada computador responda aos falsos pacotes de ping e envie uma resposta ao computador de destino, inundando-o.
  - Fonte: Norton

# Listas de controle de acesso

Sumário

Criptografia

Alg. de Chave  
Simétrica

- **ACL:** tabela de regras, aos pacotes que chegam: pares (ação, condição)

Ação	Endereço de origem	Endereço de destino	Protocolo	Porta de origem	Porta de destino	Flag bit
Permitir	222.22/16	Fora de 222.22/16	TCP	>1023	80	Qualquer um
Permitir	Fora de 222.22/16	222.22/16	TCP	80	>1023	ACK
Permitir	222.22/16	Fora de 222.22/16	UDP	>1023	53	—
Permitir	Fora de 222.22/16	222.22/16	UDP	53	>1023	—
Recusar	Todos	Todos	Todos	Todos	Todos	Todos

Questões  
Sociais

# Listas de controle de acesso

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- **ACL:** tabela de regras, aos pacotes que chegam: pares (ação, condição)

Permite que usuários internos naveguem na internet

Ação	Endereço de origem	Endereço de destino	Protocolo	Porta de origem	Porta de destino	Flag bit
Permitir	222.22/16	Fora de 222.22/16	TCP	>1023	80	Qualquer um
Permitir	Fora de 222.22/16	222.22/16	TCP	80	>1023	ACK
Permitir	222.22/16	Fora de 222.22/16	UDP	>1023	53	—
Permitir	Fora de 222.22/16	222.22/16	UDP	53	>1023	—
Negar	Todos	Todos	Todos	Todos	Todos	Todos

# Listas de controle de acesso

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

**Seg. da Comunicação**

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

- **ACL:** tabela de regras, aos pacotes que chegam: pares (ação, condição)

Permite que pacotes DNS entrem e saiam da rede

Ação	Endereço de origem	Endereço de destino	Protocolo	Porta de origem	Porta de destino	Flag bit
Permitir	222.22/16	Fora de 222.22/16	TCP	>1023	80	Qualquer um
Permitir	Fora de 222.22/16	222.22/16	TCP	80	>1023	ACK
Permitir	222.22/16	Fora de 222.22/16	UDP	>1023	53	—
Permitir	Fora de 222.22/16	222.22/16	UDP	53	>1023	—
Negar	Todos	Todos	Todos	Todos	Todos	Todos

# Filtragem de pacotes COM estado

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- filtro de pacotes sem estado: ferramenta pesada
  - admite pacotes que “não fazem sentido”, p. e., porta destino = 80, bit ACK marcado, mesmo sem conexão TCP estabelecida:

ação	endereço de origem	endereço de destino	protocolo	porta de origem	porta de destino	bit de flag
permitir	fora de 222.22/16	222.22/16	TCP	80	> 1023	ACK

- ***filtro de pacotes com estado:*** rastreia status de cada conexão TCP
  - rastrear configuração de conexão, encerramento: pode determinar se pacotes de entrada e saída “fazem sentido”
  - timeout de conexões inativas no firewall: não admite mais pacotes (uma inatividade de uma conexão por mais de 60 segundos, por exemplo)





PUC Minas

# Filtragem de pacotes COM estado

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chave  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Comunicação

Seg. da Web

Questões  
Sociais

- ACL aumentada para indicar necessidade de verificar tabela de estado da conexão antes de admitir pacote

Ação	Endereço de origem	Endereço de destino	Protocolo	Porta de origem	Porta de destino	Flag bit	Conexão de checagem
Permitir	222.22/16	Fora de 222.22/16	TCP	>1023	80	Qualquer um	
Permitir	Fora de 222.22/16	222.22/16	TCP	80	>1023	ACK	X
Permitir	222.22/16	Fora de 222.22/16	UDP	>1023	53	—	
Permitir	Fora de 222.22/16	222.22/16	UDP	53	>1023	—	X
Negar	Todos	Todos	Todos	Todos	Todos	Todos	



PUC Minas

# Filtragem de pacotes COM estado

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- Estabelecida uma conexão, o firewall passa a rastreá-la.
- Imagine que um intruso tente enviar um pacote defeituoso com datagrama na porta de origem TCP 80
- O firewall verifica a lista de controle de acesso onde a tabela de conexão deve ser também verificada antes de permitir o acesso de pacotes.
- O firewall verifica este pacote de constata que ele não faz parte de uma conexão em andamento e o rejeita.

# Gateways de aplicação

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- filtra pacotes nos dados da aplicação, além de campos IP/TCP/UDP.
- exemplo: fornecer serviço de telnet a um conjunto restrito de usuários internos (em vez de endereços IPs). Ou seja, permitir seleção de usuários internos ao telnet externo

# Gateways de aplicação

## Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

**Seg. da Comunicação**

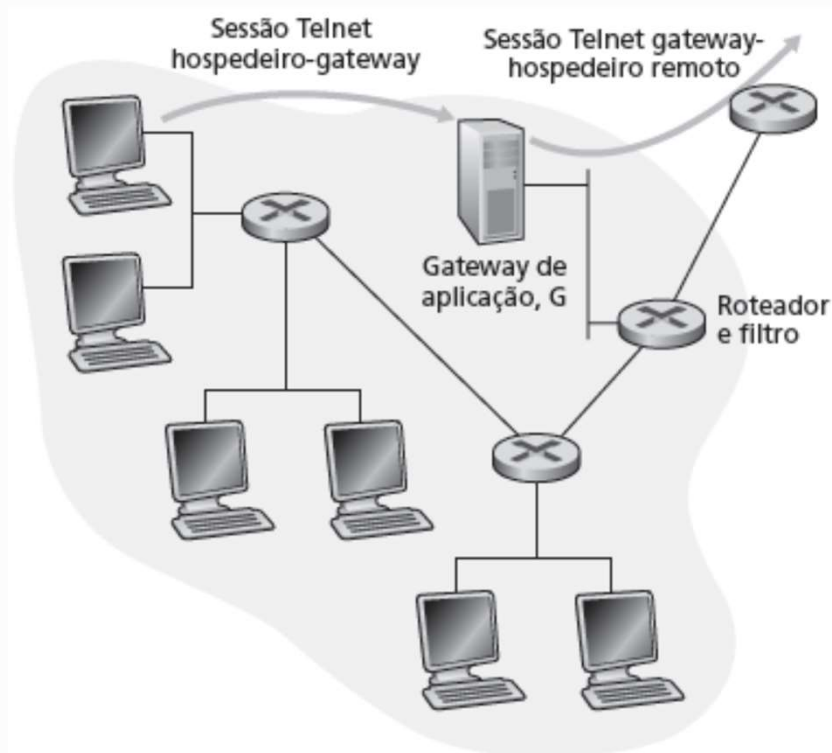
Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

1. requer que todos os usuários telnet passem pelo gateway.
2. para usuários autorizados (o gateway verifica usuário e senha), gateway estabelece conexão telnet ao hospedeiro de destino. Gateway repassa dados entre 2 conexões
3. filtro do roteador bloqueia todas as conexões telnet não originando do gateway.



# Limitações de firewalls

Sumário

Criptografia

Alg. de Chave  
Simétrica

Alg. de Chave  
Pública

Assinaturas  
Digitais

Ger. de Chaves  
Públicas

**Seg. da  
Comunicação**

Protocolos de  
Autenticação

Seg. de Correio

Seg. da WEB

Questões  
Sociais

- falsificação de IP: roteador não sabe se os dados "realmente" vêm de fonte alegada
- filtros normalmente usam toda ou nenhuma política para UDP.
- dilema: grau de comunicação com mundo exterior, nível de segurança
- muitos sites altamente protegidos ainda sofrem de ataques.



PUC Minas

# Sistemas de detecção de invasão

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

**Seg. da Comunicação**

Protocolos de Autenticação

Seg. de Correio

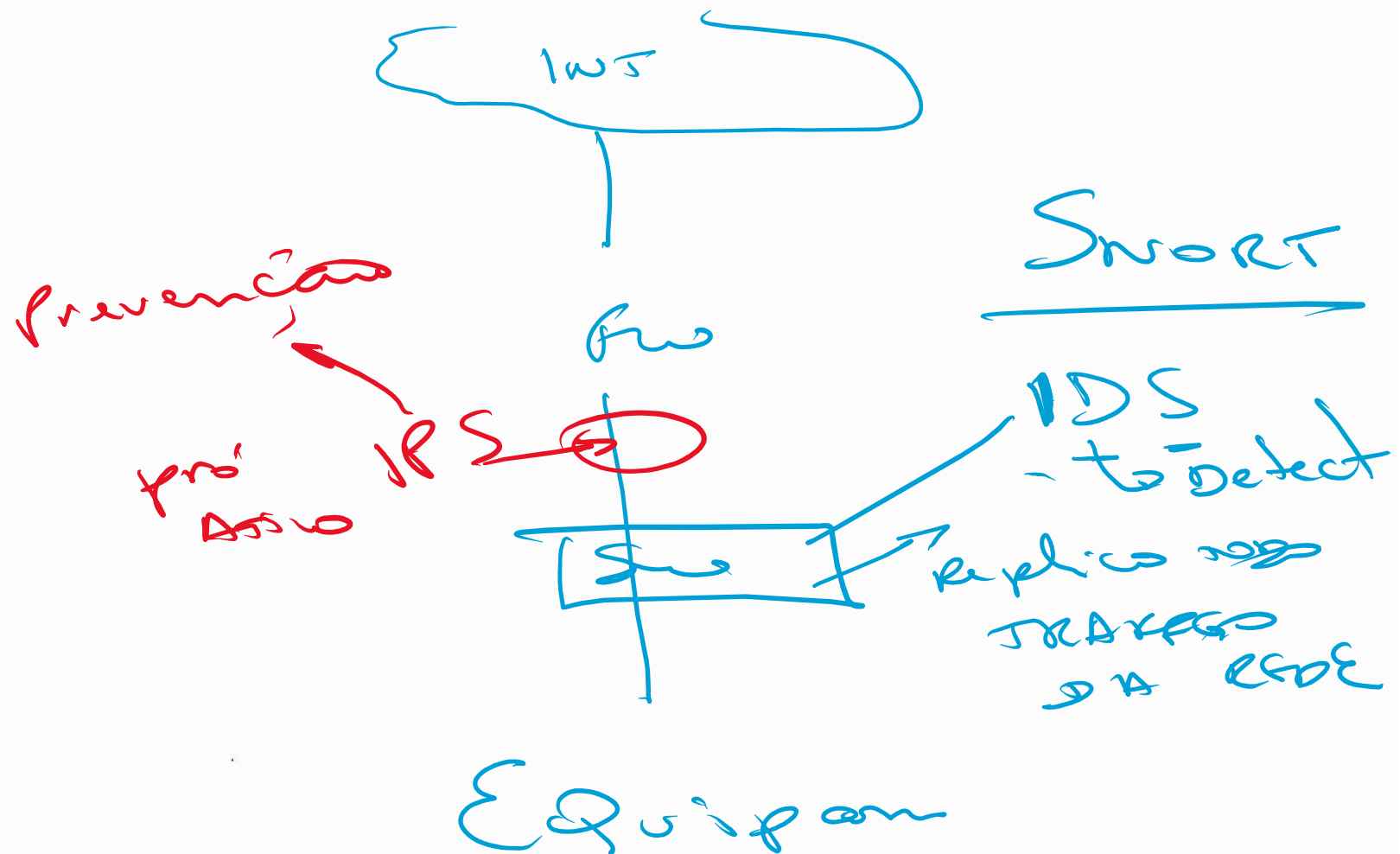
Seg. da WEB

Questões Sociais

- Vimos que a filtragem de pacotes:
  - opera apenas sobre cabeçalhos TCP/IP
  - sem verificação de correlação entre sessões
- *IDS: Intrusion Detection System (sistema de detecção de intrusão)*
  - *profunda inspeção de pacotes:* examina conteúdo do pacote (p. e., verifica strings de caracteres no pacote contra banco de dados de vírus conhecidos e sequências de ataque)
  - *examine correlação* entre múltiplos pacotes
    - escaneamento de portas
    - mapeamento de rede
    - ataque de DoS (negação de serviço)



Questões  
Sociais



# Sistemas de detecção de invasão

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

**Seg. da Comunicação**

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

- múltiplos IDSs: diferentes tipos de verificação em diferentes locais

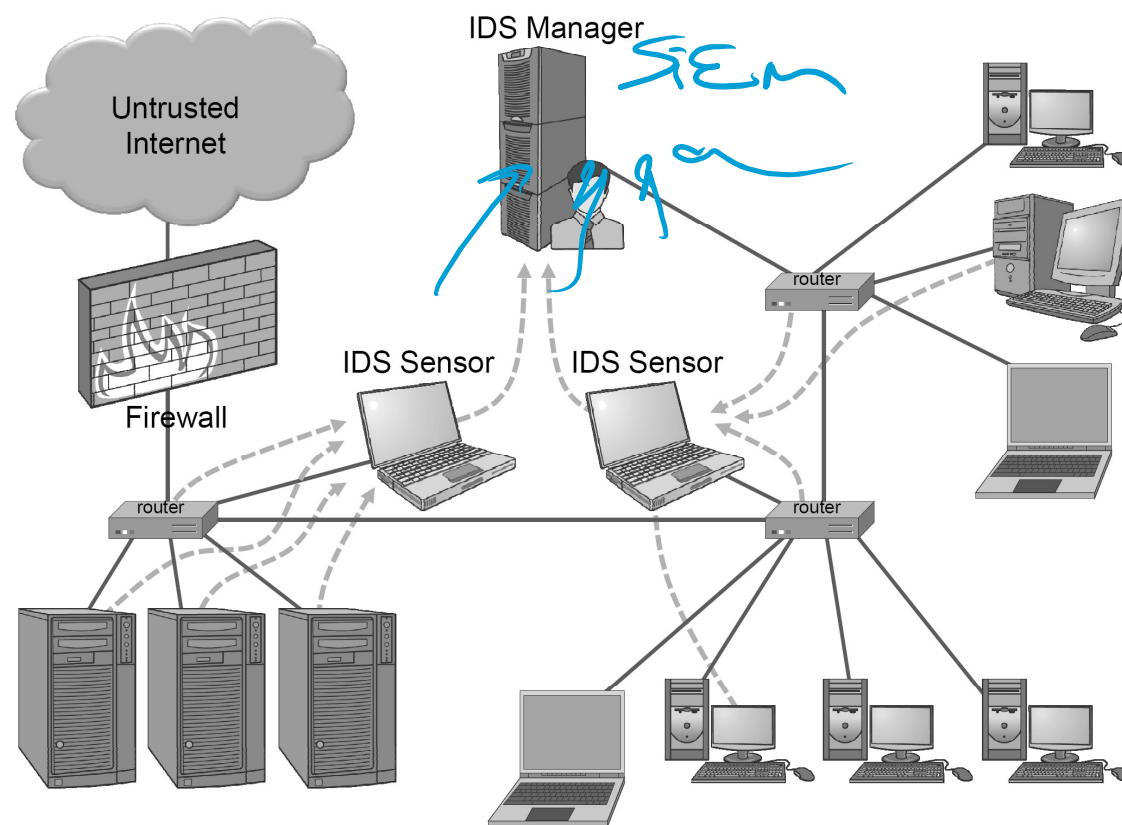


Figure 6.17: A local-area network monitored by an intrusion detection sys-





PUC Minas

# Sistemas de detecção de invasão

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas


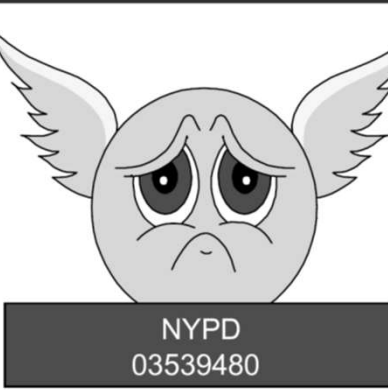
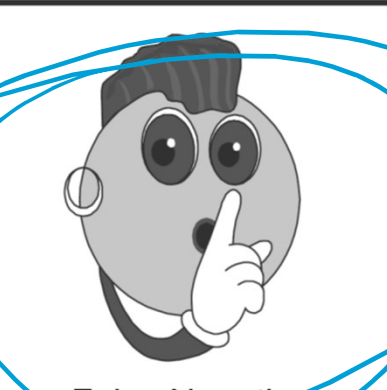
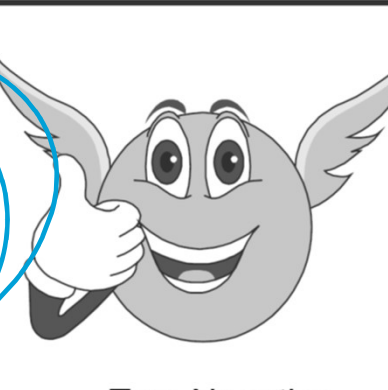
**Seg. da Comunicação**

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

	Intrusion Attack	No Intrusion Attack
Alarm Sounded	 True Positive	 False Positive
No Alarm Sounded	 False Negative	 True Negative

**Figure 6.18:** The four conditions for alarm sounding by an intrusion detection system.



PUC Minas

# Honeypot

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

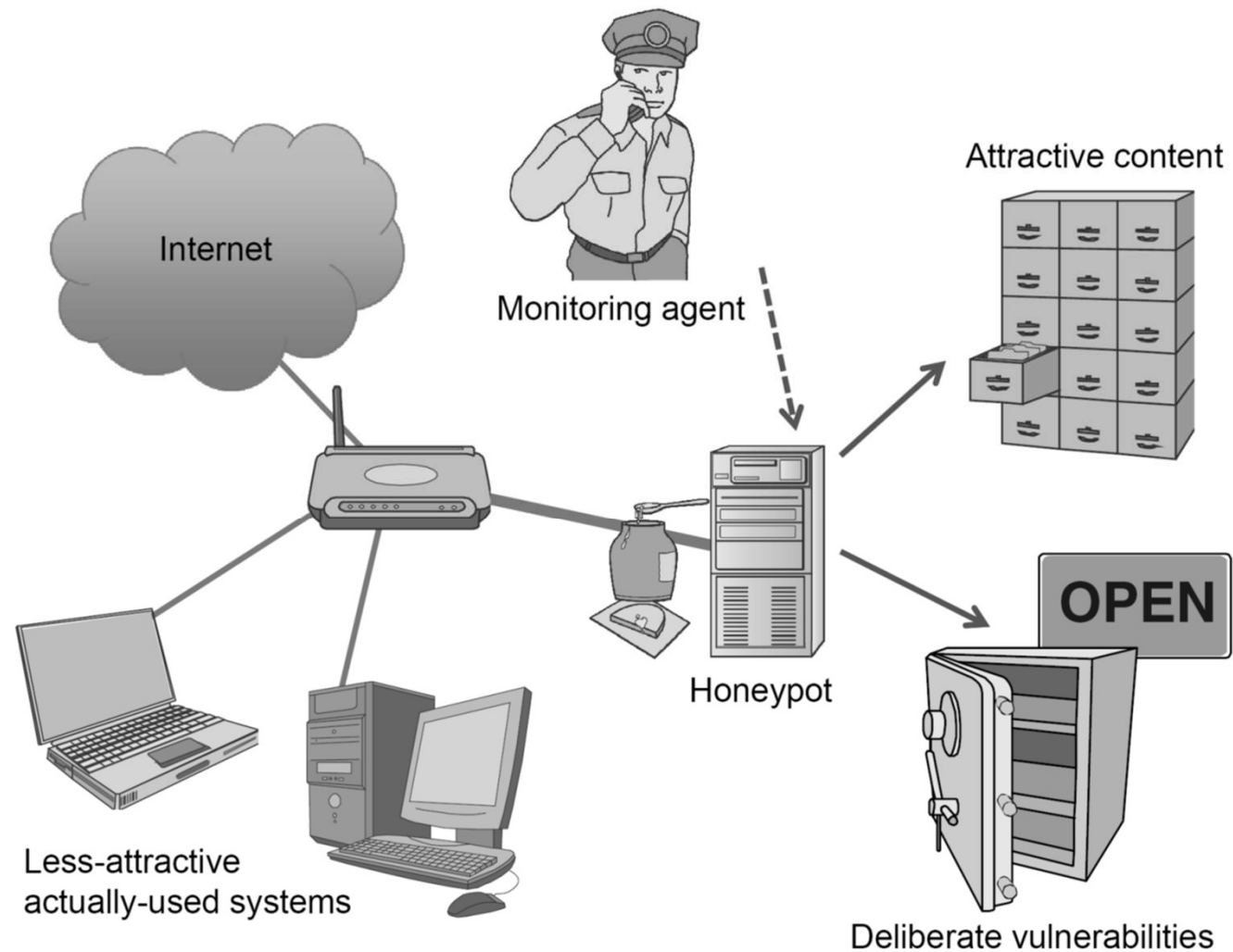
**Seg. da Comunicação**

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



**Figure 6.22:** A honeypot computer used for intrusion detection.



PUC Minas

# Firewall Localização/Arquitetura

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

**Seg. da Comunicação**

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

