

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

- Ameaças
- Nomenclatura segura
- SSL – a camada de soquetes seguros
- Segurança em código móvel



PUC Minas

Nomenclatura segura (1)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

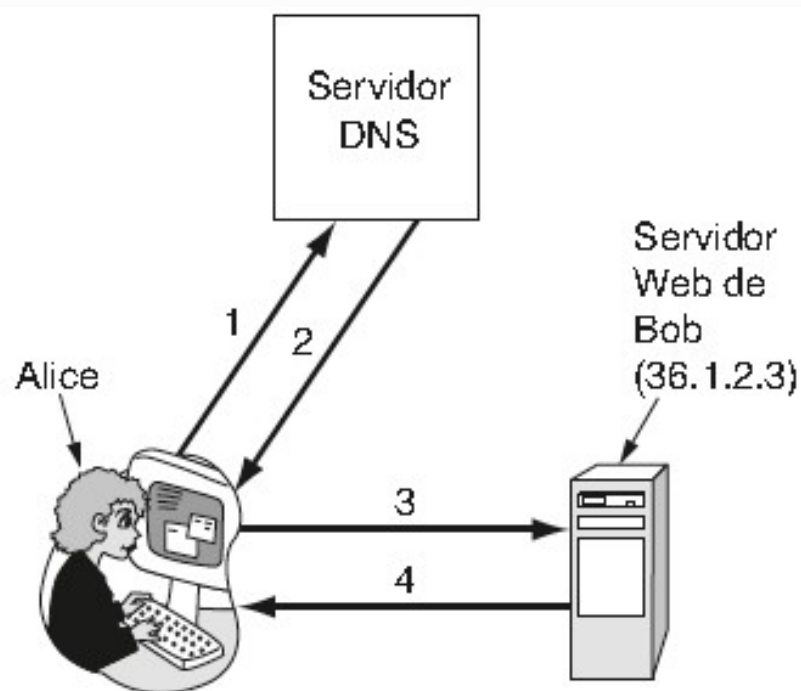
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



1. Dê-me o endereço IP de Bob
2. 36.1.2.3 (endereço IP de Bob)
3. GET index.html
4. Home page de Bob

Situação normal.



PUC Minas

Nomenclatura segura

(2)

Sumário

Criptografia

Alg. de Chave
Simétrica

Alg. de Chave
Pública

Assinaturas
Digitais

Ger. de Chaves
Públicas

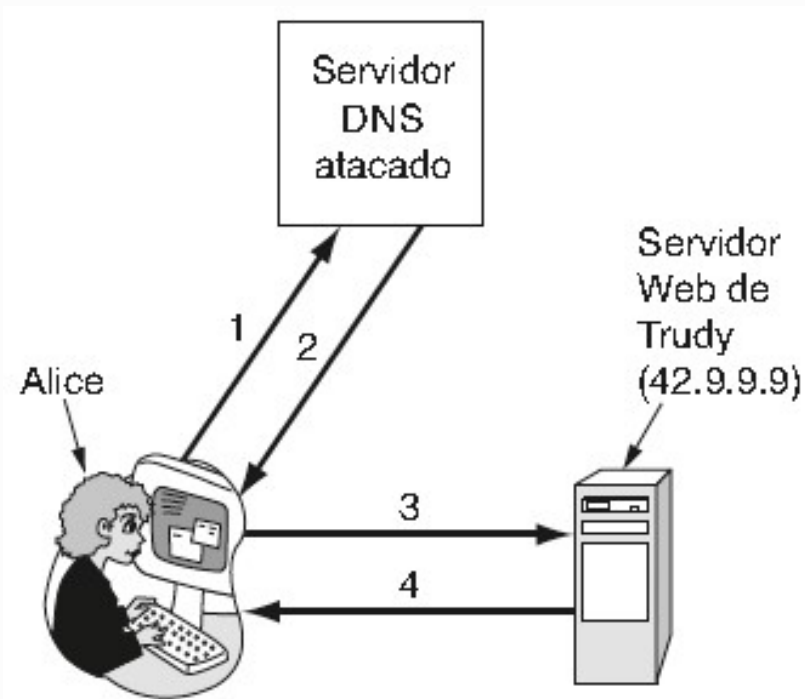
Seg. da
Comunicação

Protocolos de
Autenticação

Seg. de Correio

Seg. da WEB

Questões
Sociais



1. Dê-me o endereço IP de Bob
2. 42.9.9.9 (endereço IP de Trudy)
3. GET index.html
4. Home page de Bob modificada por Trudy

Ataque baseado na
invasão do DNS
e modificação do
registro de Bob.

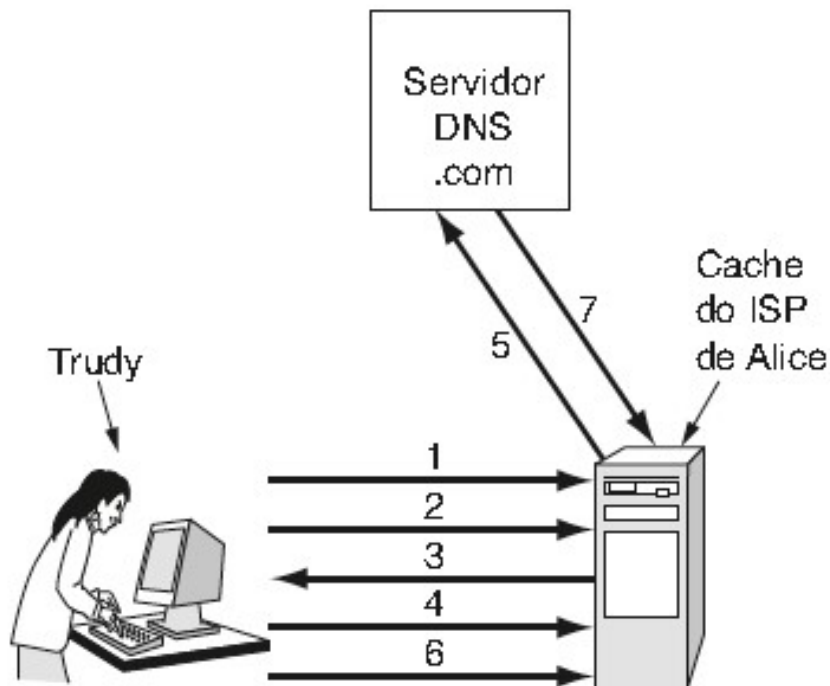


PUC Minas

Nomenclatura segura

(3)

Sumário



1. Procura foobar.trudy-the-intruder.com (para forçá-lo para o cache do ISP)
2. Procura www.trudy-the-intruder.com (para obter o próximo número de sequência do ISP)
3. Pedido para www.trudy-the-intruder.com (para forçar o ISP a consultar o servidor .com na etapa 5)
4. Rapidamente, procura bob.com (para forçar o ISP a consultar o servidos no passo 5)
5. Consulta legítima para bob.com com $\text{seq} = n+1$
6. Resposta forjada de Trudy: Bob é 42.9.9.9, $\text{seq} = n+1$
7. Resposta real (rejeitada; tarde demais)

Autenticação

Seg. de Correio

Seg. da WEB

Questões
Sociais

Como Trudy engana o ISP de Alice.



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

Serviços fundamentais do DNSsec:

- Prova de onde os dados são originados
- Distribuição de chave pública
- Autenticação de transação e solicitação



PUC Minas

Nomenclatura segura

(5)

Sumário

Criptografia

Alg. de Chave
Simétrica

Alg. de Chave
Pública

Assinatura

Gerenciamento
Pública

Sistema de
Comunicação

Protocolos de
Autenticação

Seg. de Correio

Seg. da WEB

Questões
Sociais

Responsável - Com

Nome de domínio	Tempo de vida	Classe	Tipo	Valor
bob.com.	86400	IN	A	36.1.2.3
bob.com.	86400	IN	KEY	3682793A7B73F731029CE2737D...
bob.com.	86400	IN	SIG	86947503A8B848F5272E53930C...

Exemplo de RRSet para *bob.com.* O registro *KEY* é a chave pública de Bob. O registro *SIG* é o hash assinado do servidor .com de alto nível dos registros *A* e *KEY*, a fim de verificar a autenticidade.



PUC Minas

Nomenclatura segura (6)

Sumário

Criptografia

Alg. de Chave
Simétrica

Alg. d
Públic

Assina
Digita

Ger. de Chaves
Públicas

Seg. da
Comunicação

Protocolos de
Autenticação

Seg. de Correio

Seg. da WEB

Questões
Sociais

$SHA-1(\text{Dados do Site})$
Sm

Server SHA-1 (Server, Server's Public key) File name
http://www.bob.com:2g5hd8bfjkc7mf6hg8dgany23xds4pe6/photos/bob.jpg

- Um URL autocertificado contendo um hash do nome e da chave pública do servidor



PUC Minas

SSL – camada de soquetes seguros (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

Conexão segura inclui:

- Negociação de parâmetro entre cliente e servidor
- Autenticação do servidor pelo cliente
- Comunicação secreta
- Proteção da integridade dos dados

fui pl whitelab



PUC Minas

Sumário

Criptografia

Alg. de Chave
Simétrica

Alg. de Chave
Pública

Assinaturas
Digitais

Ger. de Chaves
Públicas

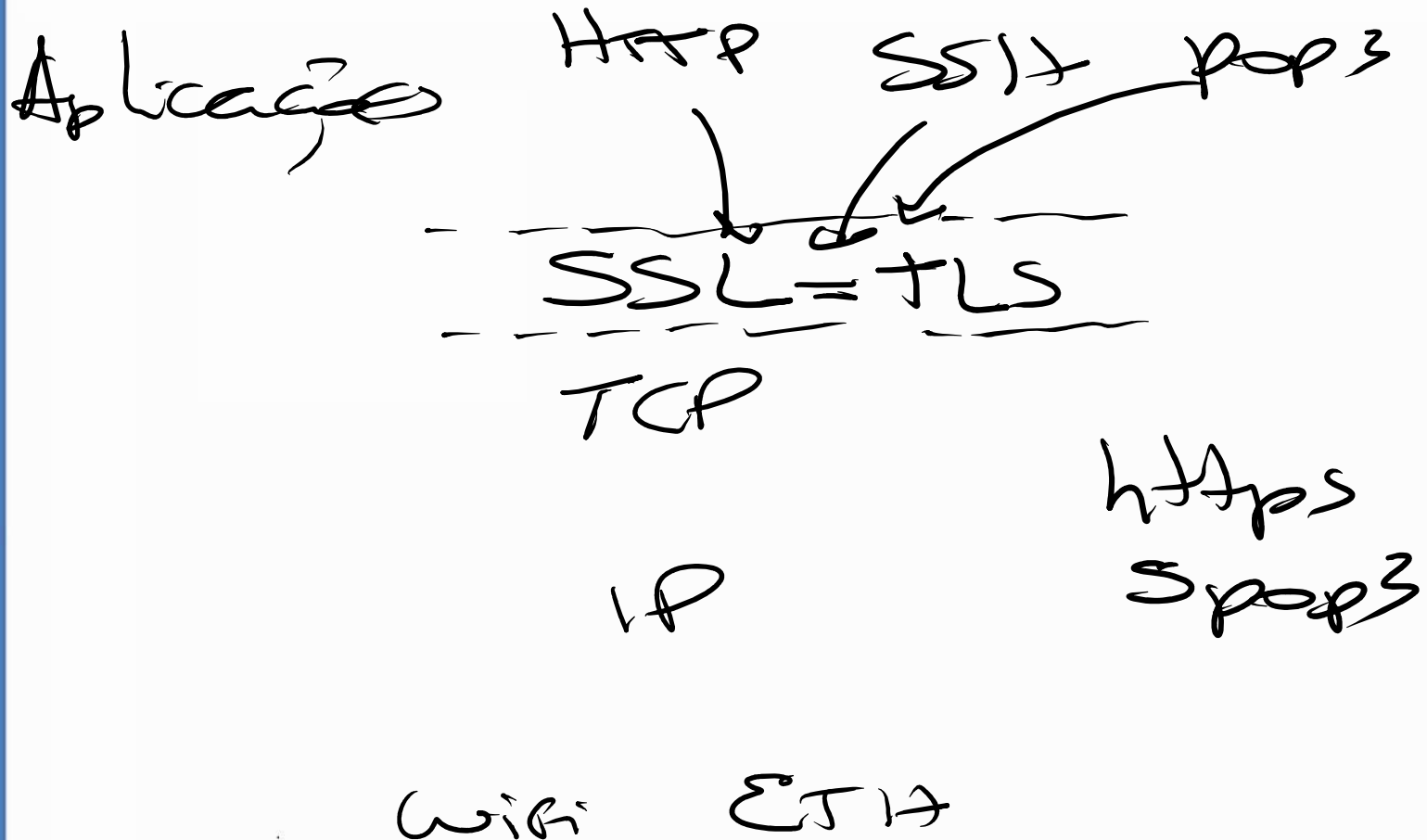
Seg. da
Comunicação

Protocolos de
Autenticação

Seg. de Correio

Seg. da WEB

Questões
Sociais





PUC Minas

SSL – camada de soquetes seguros (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

Aplicação (HTTP)
Segurança (SSL)
Transporte (TCP)
Rede (IP)
Enlace de dados (PPP)
Física (modem, ADSL, TV a cabo)

Camadas (e protocolos) para usuário
doméstico navegando com SSL.



PUC Minas

SSL – camada de soquetes seguros (3)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

Seg. da Comunicação

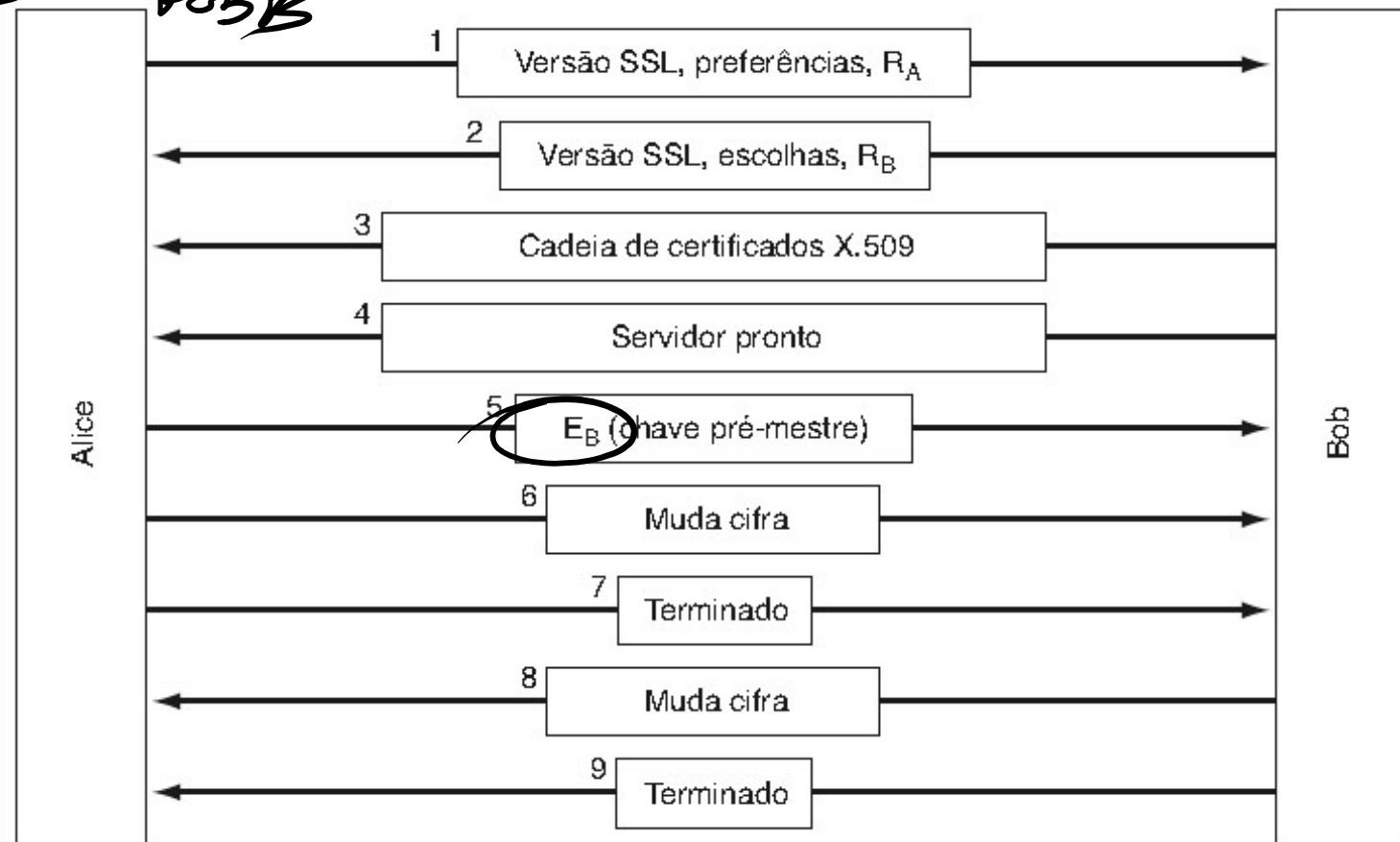
Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais

$$E_B = K_{PB} B$$



Versão simplificada do subprotocolo de estabelecimento de conexões SSL.



PUC Minas

SSL – camada de soquetes seguros (4)

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

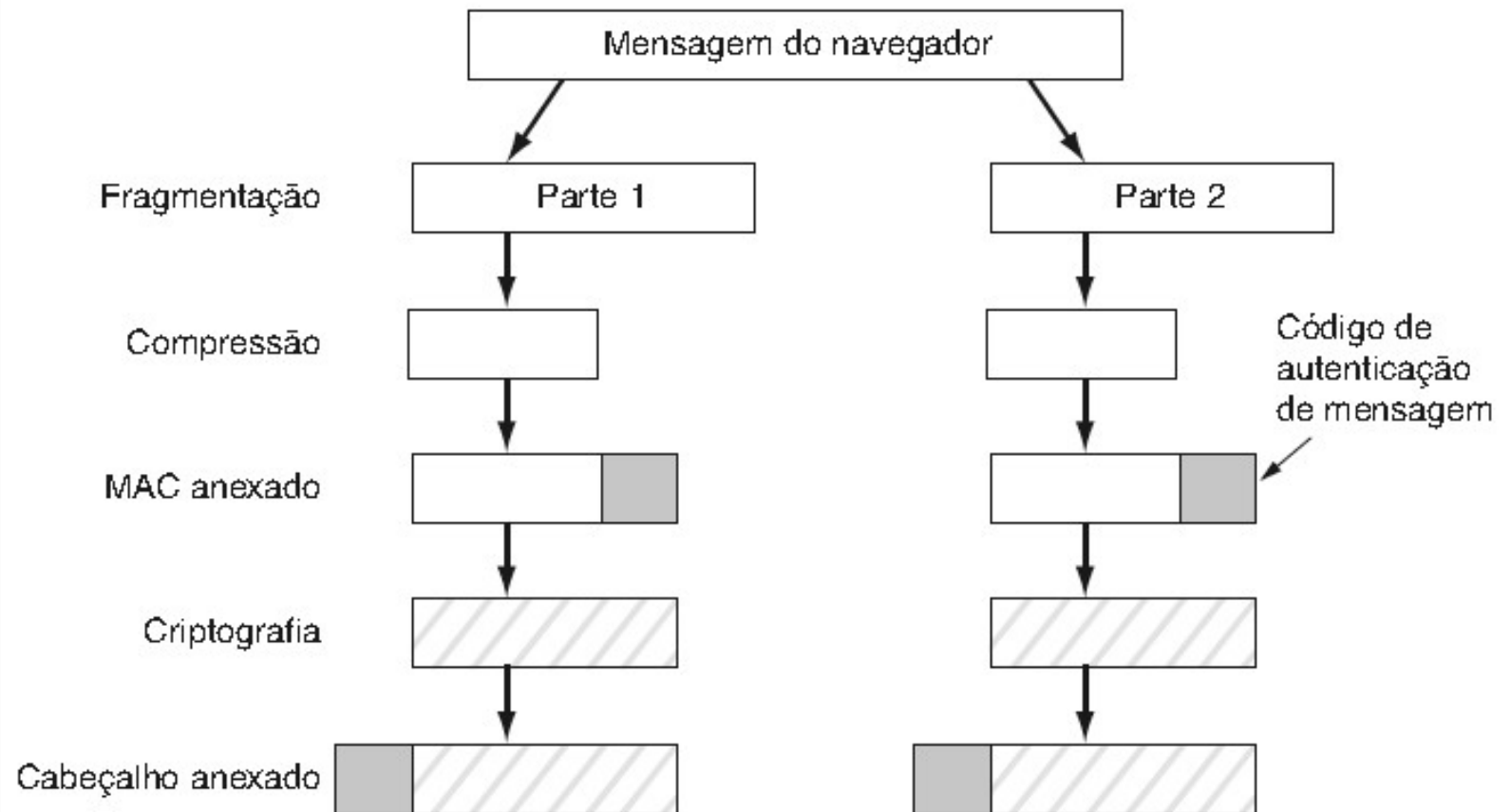
Seg. da Comunicação

Protocolos de Autenticação

Seg. de Correio

Seg. da WEB

Questões Sociais



Transmissão de dados com SSL.

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**

- Privacidade
- Liberdade de expressão
- Direitos autorais



PUC Minas

Liberdade de expressão

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

Possíveis materiais restritivos:

- Impróprio para crianças
- Ódio objetivando vários grupos
- Informações sobre democracia
- História que contradiz a versão do governo
- Manuais de atividades potencialmente ilegais

Sumário

Criptografia

Alg. de Chave Simétrica

Alg. de Chave Pública

Assinaturas Digitais

Ger. de Chaves Públicas

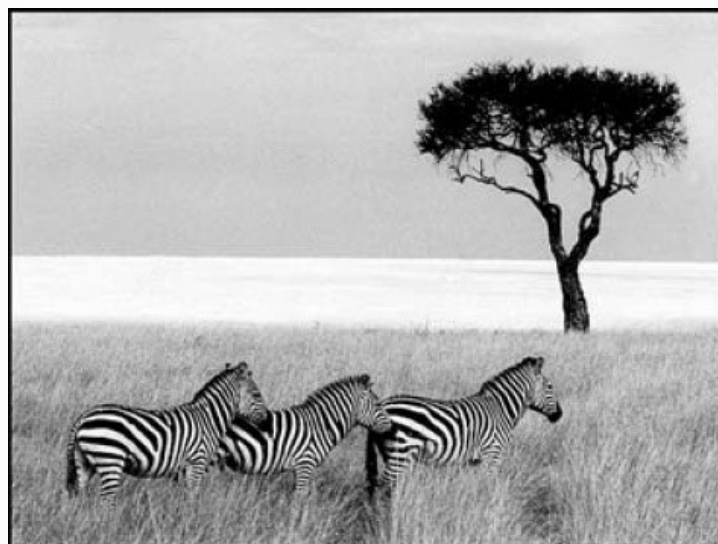
Seg. da Comunicação

Protocolos de Autenticação

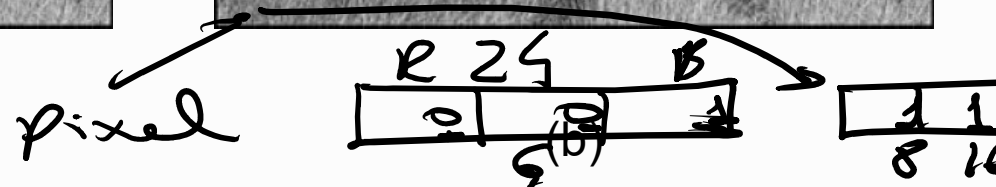
Seg. de Correio

Seg. da WEB

Questões Sociais



(a)



(a) As três zebras e uma árvore.

(b) As três zebras, uma árvore, e o texto completo de cinco peças de William Shakespeare.

00 1 11 2 20 2