BCC361 – Redes de Computadores

Universidade Federal de Ouro Preto
Departamento de Ciência da Computação

Prof. Saul Emanuel Delabrida Silva
www.decom.ufop.br/sauldelabrida

2013/01

Segurança

Agenda

- Introdução;
- Criptografia;
- Assinaturas digitais;
- Gerenciamento de chaves públicas;
- Segurança da comunicação;
- Protocolos de autenticação;
- Segurança de Correio Eletrônico e Web;
- Questões sociais.

Introdução;
Criptografia;
Assinaturas digitais;
Gerenciamento de chaves públicas;
Segurança da comunicação;
Protocolos de autenticação;
Segurança de Correio Eletrônico e Web;
Questões sociais.

INTRODUÇÃO

Introdução

- No início as redes de computadores eram utilizadas principalmente por pesquisadores em condições que não exigiam muitos cuidados com segurança;

- Posteriormente, milhões de pessoas e milhares de empresas passaram a utilizar as redes para executar inúmeras ações:
  - Operações bancárias;
  - Compras;
  - Trabalho colaborativo;
  - Etc.;

- Assim, nos últimos anos o problema de segurança tomou grandes proporções.

Introdução

- A segurança é um assunto abrangente, que inclui inúmeros problemas:
  - Impedir que pessoas mal-intencionadas leiam ou modifiquem secretamente mensagens enviadas a outros destinatários;
  - Pessoas tenham acesso a serviços remotos aos quais não estejam autorizadas a utilizar;
  - Meios para saber se uma mensagem supostamente verdadeira é um trote;
  - Também trata situações em que mensagens legítimas são capturadas e reproduzidas, além de lidar com pessoas que tentam negar o fato de ter enviado certas mensagens.

Introdução

- Problemas de segurança em rede podem ser divididos nas seguintes áreas interligadas:
  - **Sigilo** (ou **confidencialidade**): manter as informações longe de usuários não autorizados;
  - **Autenticação**: garantir que as pessoas são realmente quem elas afirmam que são;
  - **Não repúdio**: como provar que seu cliente realmente fez um pedido eletrônico de dez milhões de unidades de um produto que custa R$ 0,89?
  - **Controle de integridade**: como se certificar de que uma mensagem recebida é de fato legítima e não foi alterada?

Introdução

- A segurança **não** está relacionada a uma parte específica da pilha de protocolos, cada camada pode aplicar um certo nível de segurança:
  - **Camada Física**: “Grampos” podem ser evitados mantendo-se linhas de transmissão em tubos lacrados contendo gás inerte em alta pressão;
  - **Camada de Enlace**: Os pacotes podem ser codificados em uma máquina e decodificados quando chegar à outra máquina;
  - **Camada de Rede**: Podem ser utilizados firewalls para manter ou descartar pacotes;
  - **Camada de Transporte**: É possível criptografar conexões inteiras ponto-a-ponto, ou seja, processo-a-processo;
  - **Camada de Aplicação**: Pode tratar questões de autenticação e não repudio;

Introdução

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

- Por fim, vale ressaltar que muitos problemas de segurança não estão relacionados às técnicas aplicadas em cada camada da arquitetura:
  - Muitas falhas de segurança em empresas está relacionada a funcionários insatisfeitos ou incompetentes;
  - Clientes enganados para revelar detalhes de suas contas;
  - Bugs de implementações que deixam brechas para acesso remoto não autorizado;
  - Etc.;

Introdução;
Criptografia;
Assinaturas digitais;
Gerenciamento de chaves públicas;
Segurança da comunicação;
Protocolos de autenticação;
Segurança de Correio Eletrônico e Web;
Questões sociais.

CRIPTOGRAFIA

Tópicos

- Introdução;
- Tipos de cifras:
  - Cifras de substituição;
  - Cifras de transposição;
  - Cifras de chave única;
- Algoritmos de chave simétrica;
- Algoritmos de chave pública.

Introdução

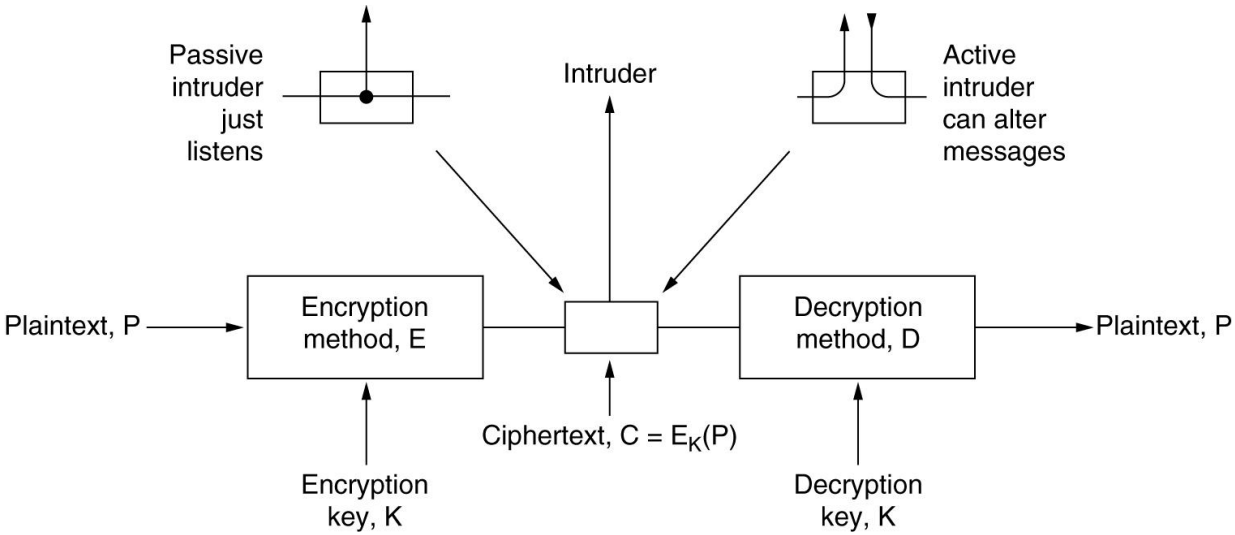
- Significa "**escrita secreta**";

- Distinção entre **Cifra** e **Código**:
  - **Cifra**: transformação caractere por caractere ou bit por bit, sem levar em conta a estrutura linguística da mensagem;
  - **Código**: substitui uma palavra por outra palavra ou símbolo;

- Códigos não são utilizados em redes, embora possuam muita história prática:
  - Um bom exemplo está na Segunda Guerra Mundial, os EUA usaram índios Navajos para se comunicarem utilizando seu idioma, que é altamente tonal e extremamente complexo;
  - Um diferencial dos americanos na guerra é que seu código não foi quebrado, mas eles conseguiram quebrar o código japonês.

Introdução

- **Modelo de criptografia*** (1):

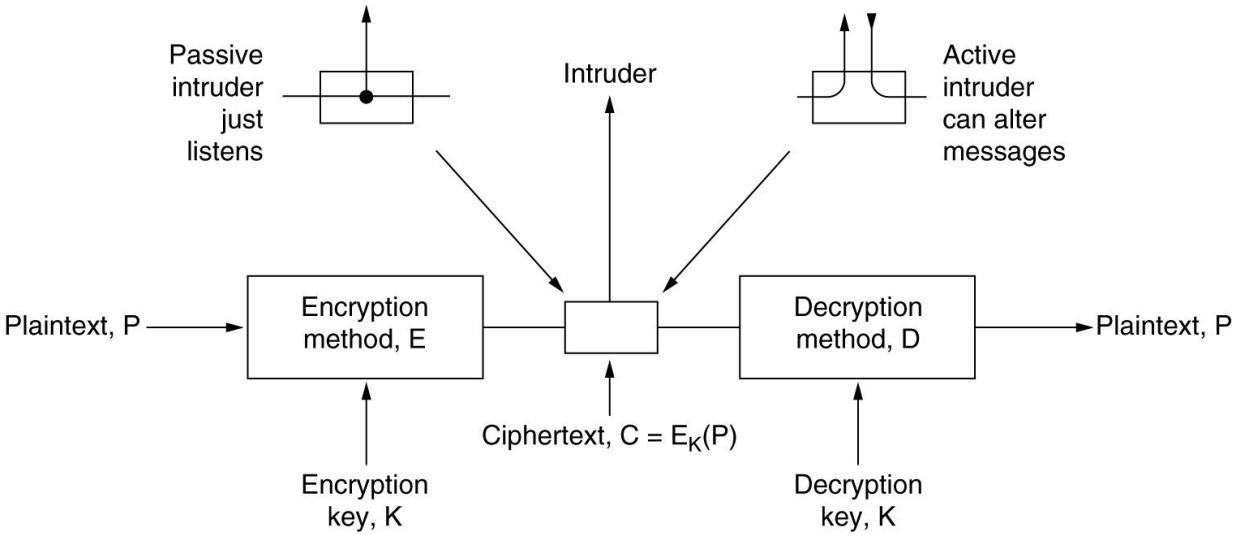


  - Um **texto simples** (*plaintext*, ***P***) é transformado (*criptografado*), por meio de uma função parametrizada por uma **chave** (*key*, ***K***), em um **texto cifrado** (*Ciphertext*, ***C***);
  - O **texto cifrado** é transmitido pelo meio;

** Para uma cifra de chave simétrica.*

Introdução

- **Modelo de criptografia*** (2):



  - Conhecendo a **chave** o destinatário pode realizar a transformação inversa (*descriptografar*) no **texto cifrado**, obtendo como resultado o **texto simples**;
  - Presume-se que um **intruso** possa "escutar" a mensagem transmitida, mas, sem o conhecimento da **chave** não terá como interpretá-la;

** Para uma cifra de chave simétrica.*

Introdução

- **Notação**:
  - ***P***, texto simples;
  - ***C***, texto cifrado;
  - ***K***, chave;
  - ***E***, função de criptografia;
  - ***D***, função de descriptografia;
  - Então:
    - $C = E_K(P)$;
    - $P = D_K(C)$;
  - Assim:
    - $D_K(E_K(P)) = P$;

Introdução

- ***Princípio de Kerchoff**:*
  - *Todos os algoritmos devem ser públicos; apenas as chaves são secretas*;

- Tentar manter o algoritmo secreto, estratégia conhecida como "**segurança pela obscuridade**", não é eficiente;

- O sigilo deve estar na chave, e o seu tamanho é uma questão importante;
  - Para uma chave de dois dígitos, significa cem possibilidades;
  - Já uma de três dígitos, significa mil possibilidades;
  - Uma de seis dígitos, um milhão de possibilidades;

Introdução

- Para se ter uma ideia:
  - Para impedir que seu irmão leia suas mensagens de correio eletrônico, serão necessárias chaves de 64 bits;
  - Para uso comercial de rotina, devem ser utilizados ao menos chaves de 128 bits;
  - Para manter o governo de outros países distantes, serão necessárias chaves de pelo menos 256 bits;

- Tipos de cifras:
  - Cifras de substituição;
  - Cifras de transposição;
  - Chave única.

Cifras de substituição

- Cada letra ou grupo de letras é substituído por outra letra ou grupo de letras;
- Uma das cifras mais antigas é a **cifra de César**, atribuída a *Júlio César*;
- Nesta cifra, ***a*** se torna ***D***, ***b*** se torna ***E***, ***c*** se torna ***F***, ...;
- Assim, ***ataque*** se tornaria ***DWDTXH***;
- Generalizando, o *texto cifrado* será composto pelo deslocamento de **k** letras no alfabeto aplicado a cada letra do *texto simples*;

Cifras de substituição

- Outra possível estratégia é mapear cada símbolo do alfabeto para outros símbolos, como por exemplo:

texto simples:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
texto cifrado:	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

- Este sistema é chamado ***cifra de substituição monoalfabética***;

- À primeira vista este sistema parece seguro, afinal, descobrir qual das 26! possíveis chaves está em uso é muito caro computacionalmente;

- Entretanto, existem estratégias interessantes para a descoberta da chave, que são eficientes, principalmente para mensagens pequenas;

Cifras de substituição

- Uma das estratégias se beneficia de propriedades estatísticas dos idiomas:
  - No inglês por exemplo, as letras *e*, *t*, *o*, *a*, *n* e *i* são as mais comuns;
  - Os *digramas* mais comuns são: *th*, *in*, *er*, e *an*;
  - Já os *trigramas* mais comuns são: *the*, *ing*, *and* e *ion*;
  - Um *criptoanalista* começaria contando a frequência das palavras e atribuiria valores àquelas que mais ocorrem, depois poderia analisar os digramas e trigramas para ampliar as letras descobertas;
  - Com isso, o número de iterações (tentativas) seria muito inferior;
- Outra alternativa seria utilizar palavras comuns a um determinado contexto:
  - Em uma mensagem de uma empresa de contabilidade, a palavra ***financia**** é muito comum, perceba a existência de padrões na palavra.

Cifras de transposição

- As cifras de substituição preservam a ordem, mas disfarçam as letras;
- Por outro lado, as cifras de transposição reordenam as letras, mas não as disfarça (1):

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
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

- A cifra se baseia em uma chave que não contém letras repetidas;
- O objetivo da chave é numerar as colunas de modo que a coluna 1 fique abaixo da letra mais próxima do início do alfabeto e assim por diante;

Cifras de transposição

- As cifras de substituição preservam a ordem, mas disfarçam as letras;
- Por outro lado, as cifras de transposição reordenam as letras, mas não as disfarça (2):

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
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

- O *texto simples* é escrito horizontalmente, em linhas;
- O *texto cifrado* é lido em colunas, a partir da coluna cuja letra seja a mais baixa e assim por diante.

Cifras de transposição

- Assim como as cifras de substituição, as de transposição também possui suas fragilidades;
- Primeiramente o *criptoanalista* precisa identificar de qual cifra se trata:
  - Ao examinar a frequência de letras (*E*, *T*, *A*, *O*, ...), é fácil constatar se essas letras se encaixam no padrão normal;
  - Caso haja correspondência, significa que trata-se de uma cifra de transposição;
- A próxima etapa é descobrir o número de colunas:
  - Para cada tamanho de chave é produzido um conjunto de digramas diferente no texto cifrado;
  - Ao tentar diferentes possibilidades, muitas vezes é possível determinar com facilidade o tamanho da chave;

Cifras de transposição

- Por fim, é necessário encontrar a ordem das colunas:
  - Quando o número de colunas *k* é pequeno, cada um dos *k*(k – 1)* pares de colunas pode ser examinado para que se constate se suas frequências de digramas correspondem às de texto simples;
  - O par com melhor correspondência será considerado na sequência correta;
  - Em seguida, cada uma das colunas restantes é experimentada como sucessora deste par (com base em digramas e trigramas);
  - O processo continua até encontrar uma ordenação em potencial;

Chave única

- Na verdade, é fácil criar uma cifra inviolável;
- Primeiro escolha como chave uma sequencia de bits aleatória;
- Em seguida, converta o *texto simples* em uma sequência de bits, utilizando por exemplo o ASCII;
- Por fim, calcule o OU Exclusivo (XOR) das duas sequências, obtendo assim o *texto cifrado*;

Chave única

- No exemplo:
  - *Message 1*: "*I Love You*" convertida para ASCII de 7 bits;
  - *Pad 1*: chave única gerada aleatoriamente;
  - *Pad 2*: chave única experimentada para tentar interpretar a *chave cifrada* (*Ciphertext*);
  - *Plaintext 2*: texto simples interpretado com a chave única *Pad 2*, que identifica como texto simples: "*Elvis lives*";

Message 1:	1001001	0100000	1101100	1101111	1110110	1100101	0100000	1111001	1101111	1110101	0101110
Pad 1:	1010010	1001011	1110010	1010101	1010010	1100011	0001011	0101010	1010111	1100110	0101011
Ciphertext:	0011011	1101011	0011110	0111010	0100100	0000110	0101011	1010011	0111000	0010011	0000101
Pad 2:	1011110	0000111	1101000	1010011	1010111	0100110	1000111	0111010	1001110	1110110	1110110
Plaintext 2:	1000101	1101100	1110110	1101001	1110011	0100000	1101100	1101001	1110110	1100101	1110011

Chave única

- Assim como os demais tipos de cifras, a *chave única* também possui desvantagens:
  - "Exigência de uma chave secreta compartilhada, com uma cópia em cada extremidade. As chaves estão sujeitas à descoberta potencial por um *adversário criptográfico*, por isso necessitam ser mudadas frequentemente." (*Wikipédia*);
  - "Apesar deste método ser bastante eficiente em relação ao tempo de processamento, ou seja, o tempo gasto para codificar e decodificar mensagens, tem como principal desvantagem a necessidade de utilização de um meio seguro para que a chave possa ser compartilhada entre pessoas ou entidades que desejem trocar informações criptografadas." (*Cartilha de segurança CERT*).

Algoritmos de chave simétrica

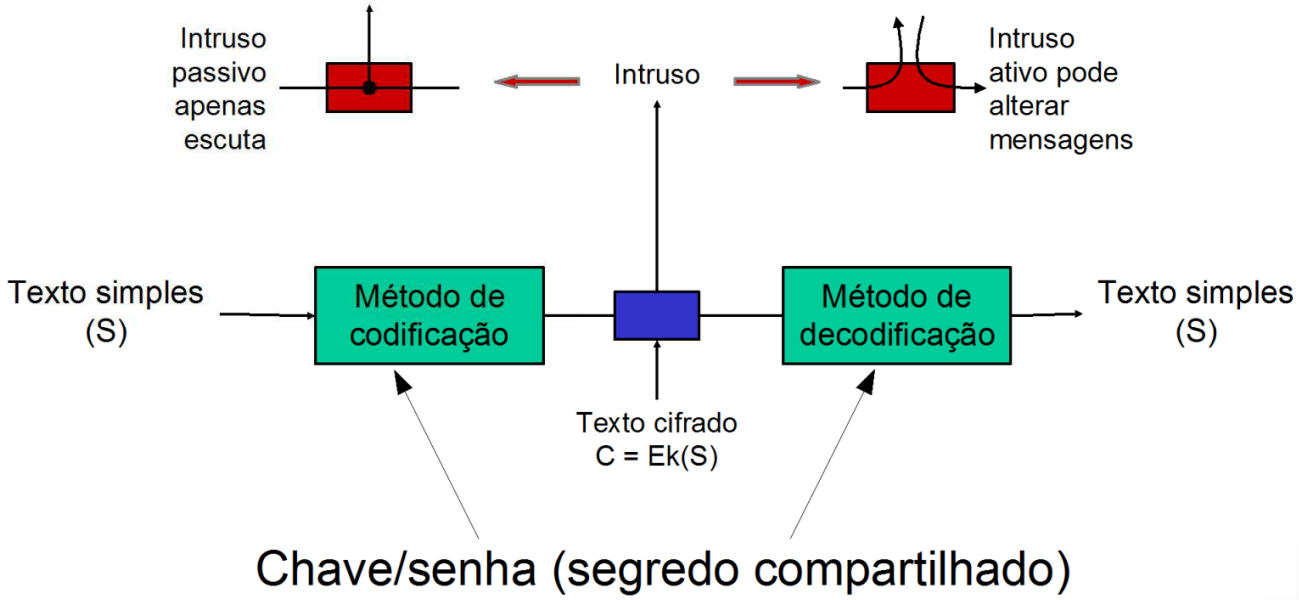
- Embora a criptografia moderna utilize as mesmas ideias básicas da criptografia tradicional (transposição e substituição), sua ênfase é diferente:
  - Ao contrário da criptografia tradicional, atualmente o objetivo é tornar o algoritmo tão complexo e emaranhado que, mesmo que o *criptoanalista* adquira enormes volumes de texto cifrado, sem a chave ele não seja capaz de entender nada;

- A primeira classe destes algoritmos é a de *chave simétrica*;
  - A outra classe abordada será a de *chave pública*.

Algoritmos de chave simétrica

- São denominados *algoritmos de chave simétrica* pois a chave usada para *criptografar* é a mesma usada para *descriptografar* (*cifra de chave única*);

- Utiliza o mesmo modelo apresentado na introdução:



Algoritmos de chave simétrica

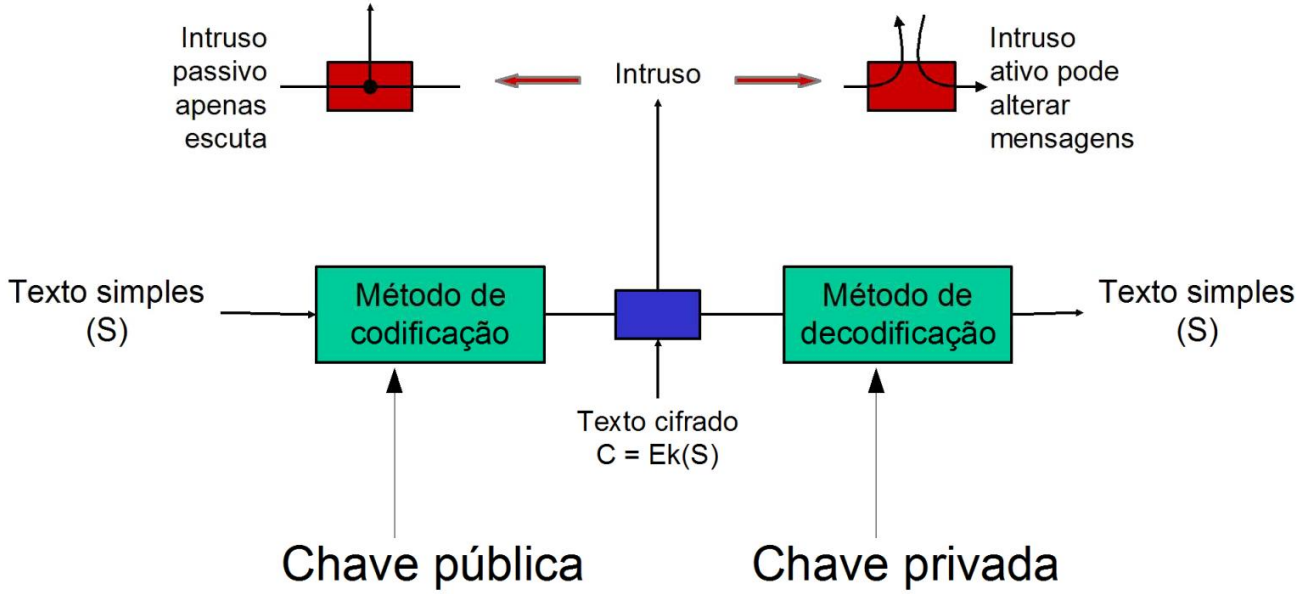
- Alguns algoritmos de chave simétrica:

Cifra	Autor	Comprimento da Chave (bits)	Comentários
DES	IBM	56	Muito fraco para utilizar atualmente.
RC4	Ronald Rivest	1 a 2.048	Atenção: algumas chaves são fracas.
RC5	Ronald Rivest	128 a 256	Bom, mas patenteado.
AES	Daemen e Rijmen	128 a 256	Melhor escolha.
Serpent	Anderson, Biham, Knudsen	128 a 256	Muito forte.
DES triplo	IBM	168	Bom, mas está ficando ultrapassado.
Twofish	Bruce Schneider	128 a 256	Muito forte; amplamente utilizado.

Algoritmos de chave pública

- O problema de distribuição de chaves sempre foi o elo mais fraco da maioria dos sistemas de criptografia;
- Como a chave para criptografar e descriptografar é única, ela precisa ser distribuída a todos os usuários do sistema, causando uma situação paradoxal:
  - As chaves precisam ser protegidas, mas ao mesmo tempo precisam ser divulgadas;
- Em 1976, dois pesquisadores (Diffie e Hellman) propuseram um sistema de criptografia novo, que utiliza chaves distintas para criptografar e descriptografar (também conhecido como *algoritmo de chave assimétrica)*;

Algoritmos de chave pública



- Em sua proposta, o algoritmo de criptografia (chaveado) ***E*** e o algoritmo de descriptografia (chaveado) ***D***, precisam atender aos requisitos:
  - *D(E(P)) = P*;
  - É extremamente difícil deduzir ***D*** a partir de ***E***;
  - ***E*** não pode ser decifrado por um ataque de *texto simples* escolhido;

Algoritmos de chave pública

- Assim, a criptografia de chave pública exige que cada usuário tenha duas chaves:
  - **Chave pública**: usada por qualquer outro usuário criptografar uma mensagem que deseje enviar a este usuário;
  - **Chave privada**: usada pelo usuário para descriptografar as mensagens recebidas.
- Exemplos de algoritmos de chave pública:
  - RSA;
  - ECC (*Elipce Curve Cryptography*).

Introdução;
Criptografia;
Assinaturas digitais;
Gerenciamento de chaves públicas;
Segurança da comunicação;
Protocolos de autenticação;
Segurança de Correio Eletrônico e Web;
Questões sociais.

ASSINATURAS DIGITAIS

Tópicos

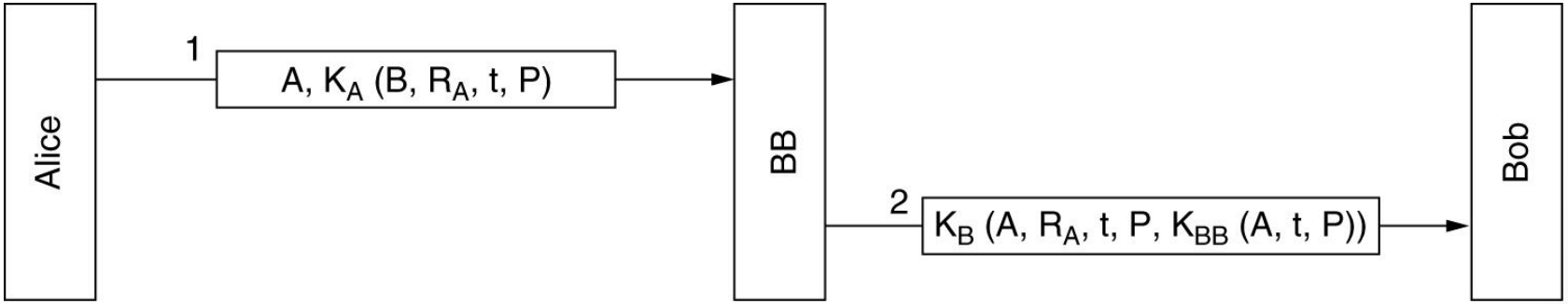
- Introdução;
- Assinaturas de chave simétrica;
- Assinaturas de chave pública;
- Sumário de mensagens.

Introdução

- A autenticidade de muitos documentos legais é determinada pela presença de uma assinatura manual (muitas vezes autenticada em cartório);
- Como possibilitar que documentos eletrônicos sejam "assinados" de forma que não possam ser forjados?
- É necessário um sistema que possa enviar uma mensagem para a outra parte de forma que:
  1. O receptor possa verificar a identidade do transmissor;
  2. Mais tarde, o receptor não possa repudiar o conteúdo da mensagem;
  3. O receptor não possa inventar ele mesmo uma mensagem.

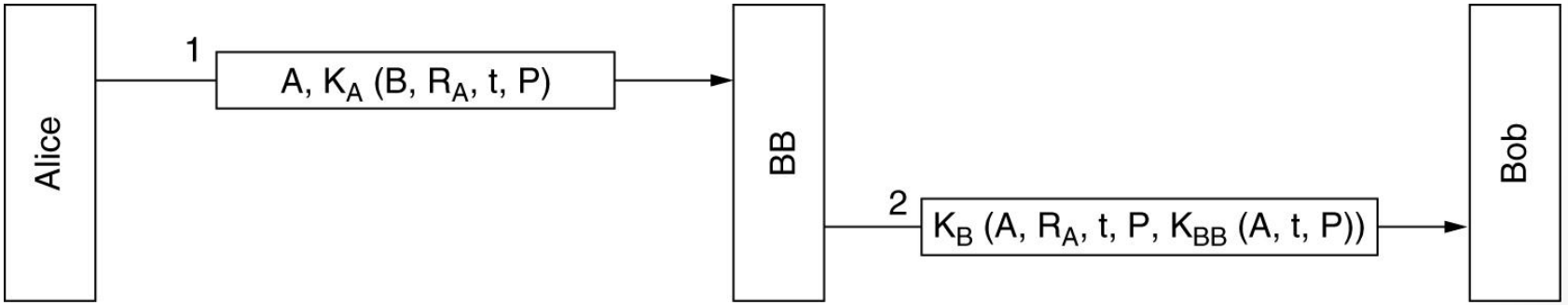
Assinaturas de chave simétrica

- Uma estratégia é ter uma autoridade central que saiba de tudo e na qual todos confiem, digamos, *Big Brother* (BB);
  - Cada um escolhe uma chave secreta e leva ao escritório BB;
  - Somente o dono da chave e o BB conhecerão a chave;
  - Pode ser comparado aos nossos cartórios;



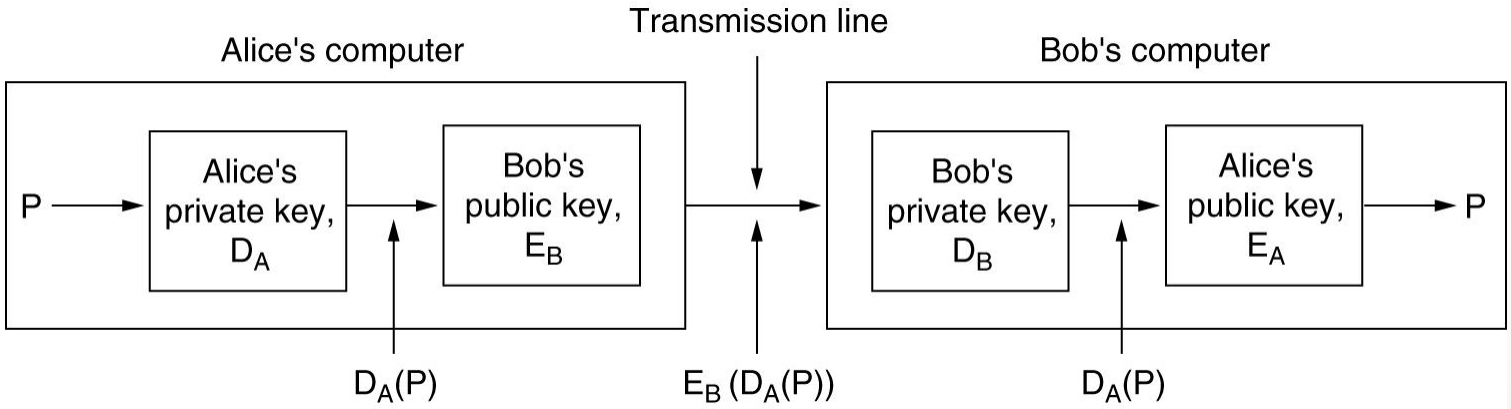
Assinaturas de chave simétrica

- Uma estratégia é ter uma autoridade central que saiba de tudo e na qual todos confiem, digamos, *Big Brother* (BB);
  - Cada um escolhe uma chave secreta e leva ao escritório BB;
  - Somente o dono da chave e o BB conhecerão a chave;
  - Pode ser comparado aos nossos cartórios;



Assinaturas de chave pública

- Confiar no *Big Brother* (BB) pode ser um problema;
- Seria interessante que o ato de assinar um documento não exigisse a presença de uma autoridade confiável;
- A criptografia de chave pública pode resolver esta questão;

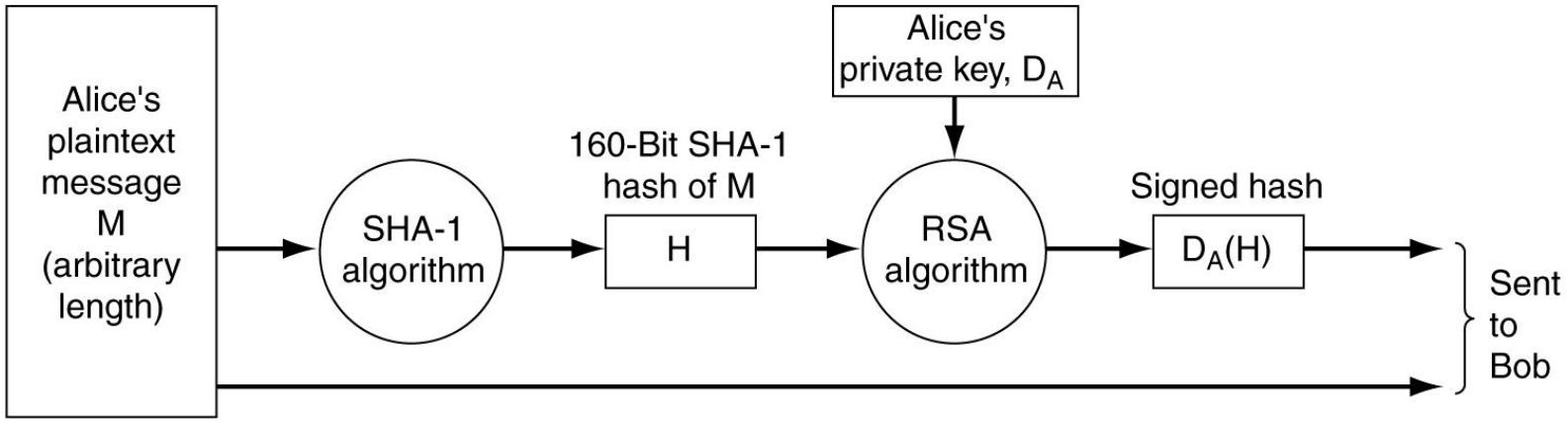


Sumário de mensagens

- Os métodos de assinatura baseados em criptografia vistos anteriormente fornecem: **autenticação** e **sigilo**;
- Muitas vezes o sigilo não é necessário;
- O **sumário de mensagem** se baseia na ideia de uma *função hash unidirecional* (***MD*** – *Messsage Digest*) que calcula uma sequência de bits de tamanho fixo a partir do texto da mensagem;
- Possui quatro propriedades importantes:
  - Se ***P*** for fornecido, o cálculo de ***MD(P)*** será muito fácil;
  - Se ***MD(P)*** for fornecido, será efetivamente impossível encontrar ***P***;
  - Dado ***P***, ninguém pode encontrar ***P'*** tal que ***MD(P') = MD(P)***;
  - Uma mudança na entrada de ate mesmo 1 bit produz uma saída muito diferente.

Sumário de mensagens

- O *sumário da mensagem* é enviado utilizando *criptografia de chave pública* e a mensagem é enviada separadamente sem criptografia;



Introdução;
Criptografia;
Assinaturas digitais;
Gerenciamento de chaves públicas;
Segurança da comunicação;
Protocolos de autenticação;
Segurança de Correio Eletrônico e Web;
Questões sociais.

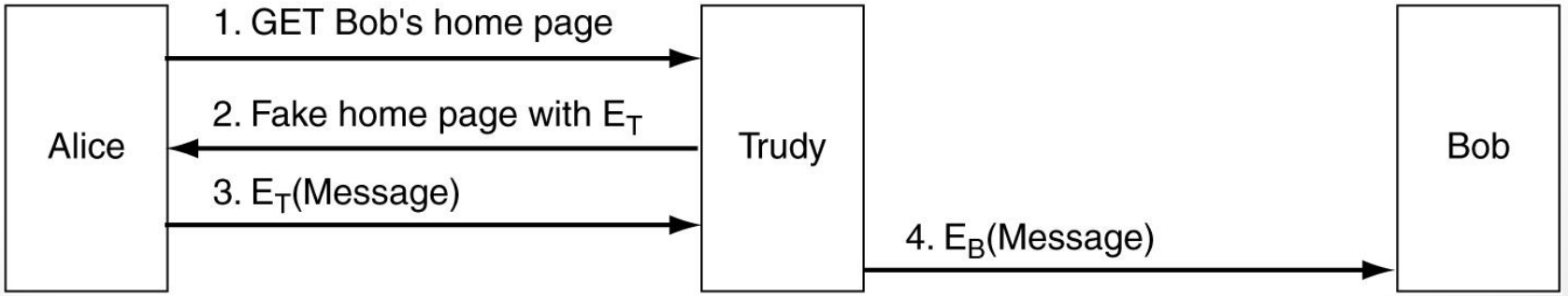
GERENCIAMENTO DE CHAVES PÚBLICAS

Tópicos

- Introdução;
- Certificados;
- Infraestrutura.

Introdução

- A criptografia de chave pública torna possível a comunicação segura a pessoas que não compartilham uma chave comum;
- Também elimina a necessidade de uma terceira parte confiável;
- Mas, um novo problema aparece: e se Alice e Bob não se conhecerem? Como obter as chaves públicas necessárias?
  - Alice pode procurar a chave pública de Bob na Internet, em sua página pessoal?



Certificados

- Como uma primeira tentativa de solução para o problema poderíamos imaginar um centro de distribuição de chaves: **KDC** (***Key Distribution Center***);
  - Disponível 24 horas;
  - Entrega de chaves públicas sob demanda;

- **Problemas**:
  - Solução centralizada pode não ser escalável;
  - Se ficar inativo, a segurança da Internet ficaria paralisada;

- **Solução**: ?.

Certificados

- **Solução**:
  - Autoridades de certificação descentralizadas, **CA** (***Certification Autorities***);
  - Organizações que certificam chaves públicas;
  - Não precisa estar on-line todo o tempo;
  - Um possível certificado:

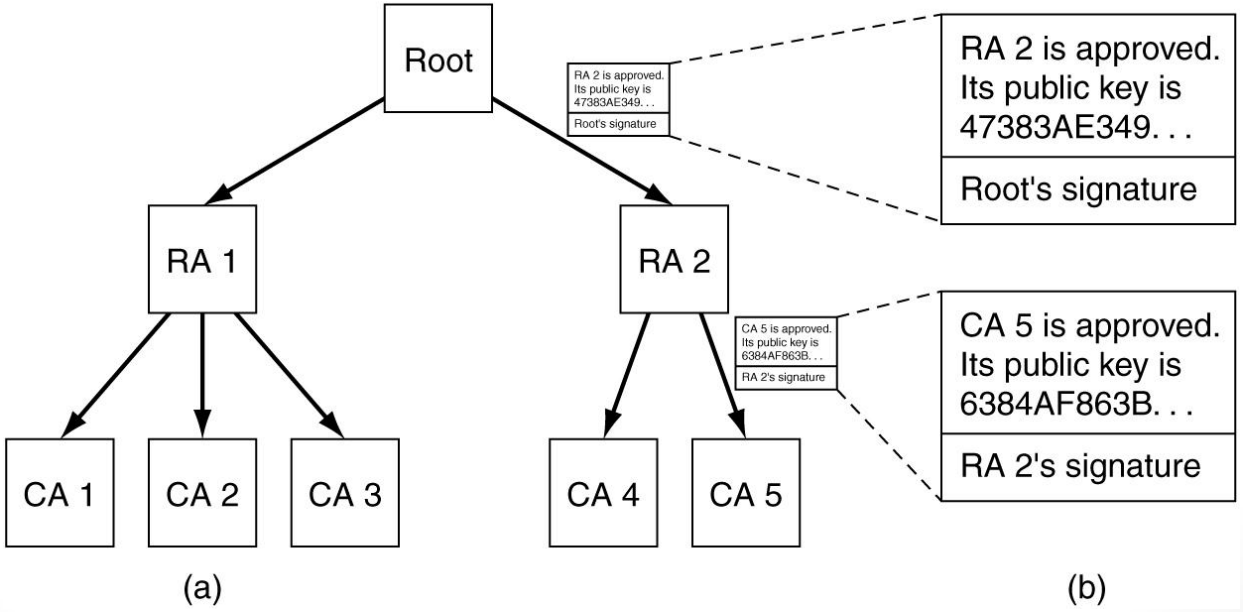
I hereby certify that the public key
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
belongs to
Robert John Smith
12345 University Avenue
Berkeley, CA 94702
Birthday: July 4, 1958
Email: bob@superdupernet.com

SHA-1 hash of the above certificate signed with the CA's private key

Infraestrutura

- Como vimos centralizar não é a melhor solução;

- A infraestrutura é baseada em uma arquitetura hierárquica chamada **PKI** (***Public Key Infraestrutura***):
  - A CA de nível superior, raiz, certifica CAs do segundo nível (**RAs** – ***Regional Authorities***);



Introdução;
Criptografia;
Assinaturas digitais;
Gerenciamento de chaves públicas;
Segurança da comunicação;
Protocolos de autenticação;
Segurança de Correio Eletrônico e Web;
Questões sociais.

SEGURANÇA DA COMUNICAÇÃO

Tópicos

- Introdução;
- IPsec;
- *Firewalls*;
- Redes Privadas Virtuais;
- Segurança em redes sem fio.

Introdução

- O problema agora é como garantir a segurança da comunicação:
  - Como levar os bits secretamente e sem alteração da origem até o destino?
  - Como manter bits indesejáveis do lado de fora?

IPsec

- Padrão de segurança da camada de rede;
- O **IPsec** (***IP security***) foi descrito nas RFCs 2401, 2402, 2406, e outras;
- Uma conexão é denominada associação de segurança, ou **SA** (***Security Association***);
- Possui duas partes principais:
  1. Dois novos cabeçalhos;
  2. Tratamento do estabelecimento de chaves;

IPsec

1. **Dois novos cabeçalhos** (1):

   - Cabeçalho de Autenticação, ou **AH** (***Autentication Header***):
     - Fornece verificação de integridade e segurança contra reprodução, mas não oferece sigilo;
     - No IPv4 ele é inserido entre o cabeçalho IP e o cabeçalho TCP;
     - No protocolo IPv6 ele é inserido como um cabeçalho de extensão;

IPsec

1. **Dois novos cabeçalhos** (2):

   - Cabeçalho **ESP** (***Encapsulating Security Payload***):
     - É um cabeçalho alternativo;
     - Faz tudo que o AH faz e algo mais (como garantir segurança);
     - É possível que o AH fique defasado no futuro;

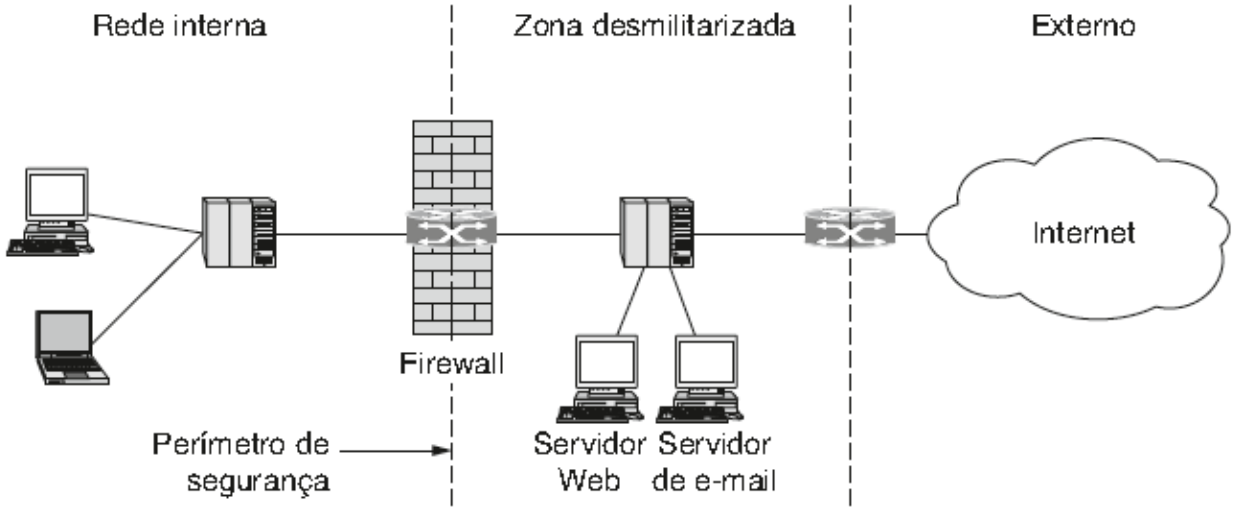
IPsec

2. **Tratamento do estabelecimento de chaves**:

- Consiste do protocolo **ISAKMP** (***Internet Security Association and Key Management Protocol***);
- Definido na RFC 2408, é usado para o estabelecimento de **SAs** (***Security Associations***) e chaves de criptografia;
- Trata-se de um framework para prover autenticação e troca de chaves, protocolos como **IKE** (***Internet Key Exchange***) ou **KINK** (***Kerberized Internet Negotiation of Keys***) devem ser usados em conjunto para realizar o serviço.

Firewalls

- Basicamente trata-se de uma adaptação de uma antiga prática de segurança medieval:
  - Cavar um fosso profundo em torno do castelo;
  - Isto força que todos que entram ou saiam do castelo sejam obrigados a passar por uma ponte levadiça, onde poderão ser revistados;



Firewalls

- O *firewall* atua como um filtro de pacotes, inspecionando quaisquer pacotes que entram e saem da rede;
- O administrador da rede define regras de avaliação dos pacotes, com base na análise da regra um pacote pode seguir ou será descartado;
- Outro nível de segurança, *gateway em nível de aplicação*, permite que o *firewall* examine dentro dos pacotes;
- Nesta estratégia ele seria capaz de distinguir entre o tráfego HTTP usado para navegação Web ou usado para compartilhameto de arquivo *peer-to-peer*;

Firewalls

- Este tipo de recurso mostra claramente que o *firewall* viola a disposição de camadas do padrão de protocolos:
  - Eles estão na camada de rede, mas, para realizar a sua filtragem, examinam as camadas de transporte e aplicação;
  - Apesar disso, a Internet é um "lugar perigoso" e os *firewalls* contribuem com a proteção, e por isso, provavelmente permanecerão;

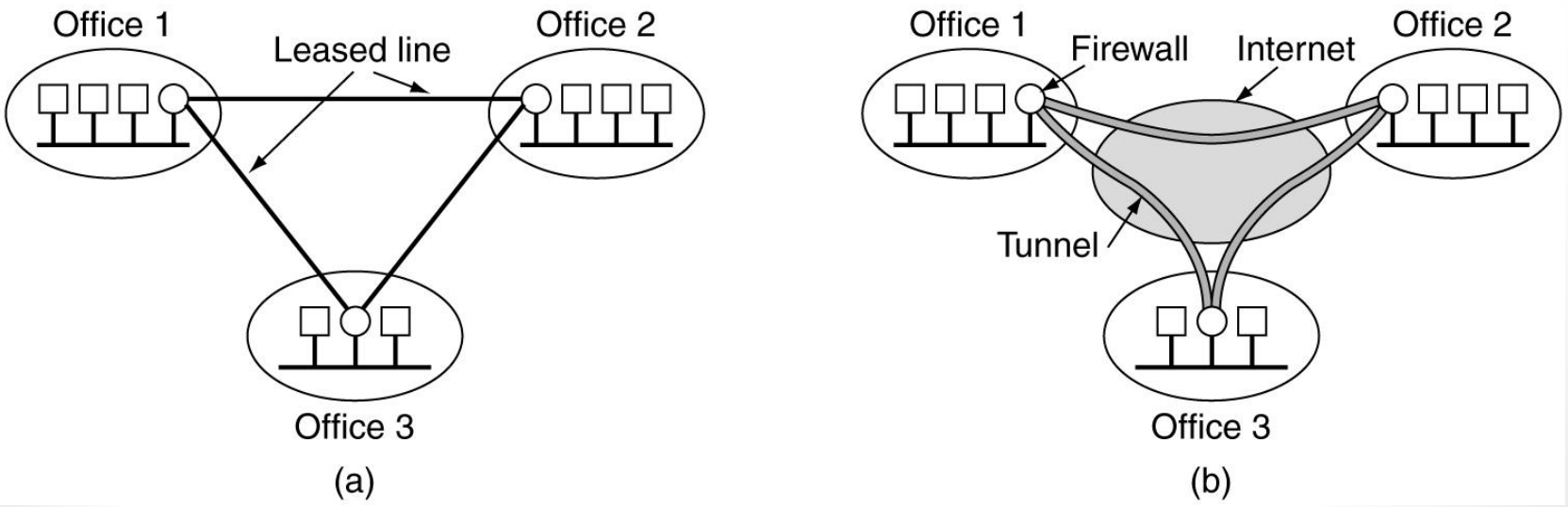
- Mesmo perfeitamente configurado, a proteção não será 100% garantida:
  - **DoS** (***Denial of Service***);
  - **DDoS** (***Distributed DoS***);

Redes Privadas Virtuais

- Muitas empresas possuem escritórios espalhados pelo mundo, ou alguns de seus funcionários precisam trabalhar remotamente acessando os recursos de sua rede;
- É comum que estas empresas contratem serviços de comunicação dedicada para interligar suas redes, formando **redes privadas**;
- O problema é que serviços de comunicação dedicados são caros e limitam aspectos de localização;
- Com o advento de redes públicas de dados e a Internet, muitas empresas optam por mover seu tráfego através delas, sem abrir mão da segurança;

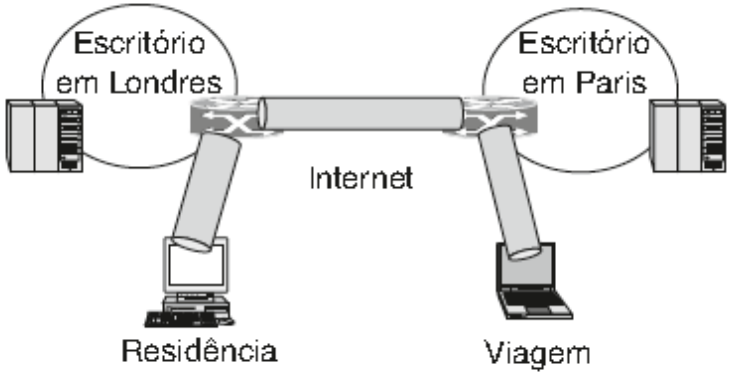
Redes Privadas Virtuais

- Essa demanda levou à criação de redes privadas virtuais, ou **VPNs** (***Virtual Private Networks***);
- Uma técnica popular é construir as VPNs diretamente sobre a Internet, equipando cada escritório com um *firewall* e criando túneis entre todos os pares de escritórios;
- Uma representação de linhas dedicadas e VPN:



Redes Privadas Virtuais

- Uma vantagem no uso de VPN sobre a Internet é que os túneis podem ser criados sob demanda, incluindo o computador de um funcionário em sua residência ou em viagem:



(a)

Redes Privadas Virtuais

- Alternativas para criação de VPNs:
  - Usando **IPsec**:
    - SAs são negociadas e estabelecidas entre pares;
  - Contratando um ISP:
    - Os caminhos para o tráfego da VPN podem ser criados pela rede do ISP, mantendo um tráfego seguro entre os hosts da VPN, isolado dos demais tráfegos da rede do ISP;
    - Pode garantir ainda os níveis de QoS desejados.

Segurança em redes sem fio

- A rede sem fios é um sonho que se tornou realidade para o espião: dados gratuitos sem nenhum trabalho.
- Assim, não é preciso ressaltar a importância da segurança nestes ambientes;
- Redes Bluetooth:
  - A partir da versão 2.1 oferece quatro modos de segurança, de nenhuma até total criptografia de dados e controle de integridade;
  - Basicamente utiliza algoritmos de chave compartilhada;

Segurança em redes sem fio

- **Redes 802.11**:
  - Principais protocolos:
    - **WEP** (***Wired Equivalent Privacy***):
      - Primeira geração de protocolos de segurança 802.11;
      - Opera no nível de enlace de dados;
      - Apresentou algumas falhas de projeto que o comprometeram;
    - **WPA2** (***WiFi Protected Access 2***):
      - Um substituto para o WEP;
      - Admite uso de IPsec na camada de rede;
      - Admite **SSL** (***Secure Sockets Layer***) na camada de transporte;
      - Admite autenticação HTTP.

Introdução;
Criptografia;
Assinaturas digitais;
Gerenciamento de chaves públicas;
Segurança da comunicação;
Protocolos de autenticação;
Segurança de Correio Eletrônico e Web;
Questões sociais.

PROTOCOLOS DE AUTENTICAÇÃO

Protocolos de autenticação

- **Autenticação** é uma técnica pela qual um processo confirma que seu parceiro na comunicação é quem deve ser, e não um impostor;

- Confirmar a identidade de um processo remoto, diante de um intruso ativo mal-intencionado, é uma tarefa muito difícil, que exige protocolos complexos;

- Não se deve confundir **Autenticação** com **Autorização**:
  - **Autenticação**: Você é quem afirma ser?
  - **Autorização**: Você tem permissão para fazer o que deseja?

Protocolos de autenticação

- Já vimos alguns recursos capazes de realizar e garantir autenticação:
  - Criptografia com chave secreta compartilhada;
  - Criptografia com chave pública;

- Alguns protocolos:
  - **Troca de chaves de Diffie-Hellman**: estabelecimento de chave secreta entre pessoas que não se conhecem;
  - **Autenticação de Needham-Schroeder**: protocolo sofisticado que envolve autenticação mútua usando um distribuidor central de chaves (KDC);
  - **Kerberos**: desenvolvido pelo MIT com base no protocolo de *Needham-Schroeder*, usado em muitos sistemas reais (Windows 2000 e posteriores, por exemplo);

Introdução;
Criptografia;
Assinaturas digitais;
Gerenciamento de chaves públicas;
Segurança da comunicação;
Protocolos de autenticação;
Segurança de Correio Eletrônico e Web;
Questões sociais.

SEGURANÇA DE CORREIO ELETRÔNICO E WEB

Seg. no Correio Eletrônico

- Quando mensagens de correio eletrônico são enviadas, elas percorrem dezenas de máquinas até chegarem ao seu destino;
- Qualquer uma destas máquinas pode lê-las e armazená-las para uso posterior;
- Entretanto, muitas vezes é necessário que apenas o destinatário consiga ler as mensagens enviadas a eles;

Seg. no Correio Eletrônico

- Assim, foram criados sistemas específicos para garantir segurança de correio eletrônico:
  - **PGP** (***Pretty Good Privacy***):
    - Pacote completo para segurança de mensagens de correio eletrônico que fornece privacidade, autenticação, assinaturas digitais e compactação;
    - Multiplataforma, código fonte aberto, gratuito e fácil de usar;
  - **S/MIME** (***Secure/MIME***):
    - Empreendimento da IETF relacionado à segurança de correio eletrônico, descrito nas RFCs 2632 a 2643;
    - Oferece autenticação, integridade, sigilo e não repúdio;
    - Admite uma variedade de algoritmos de criptografia.

Segurança na Web

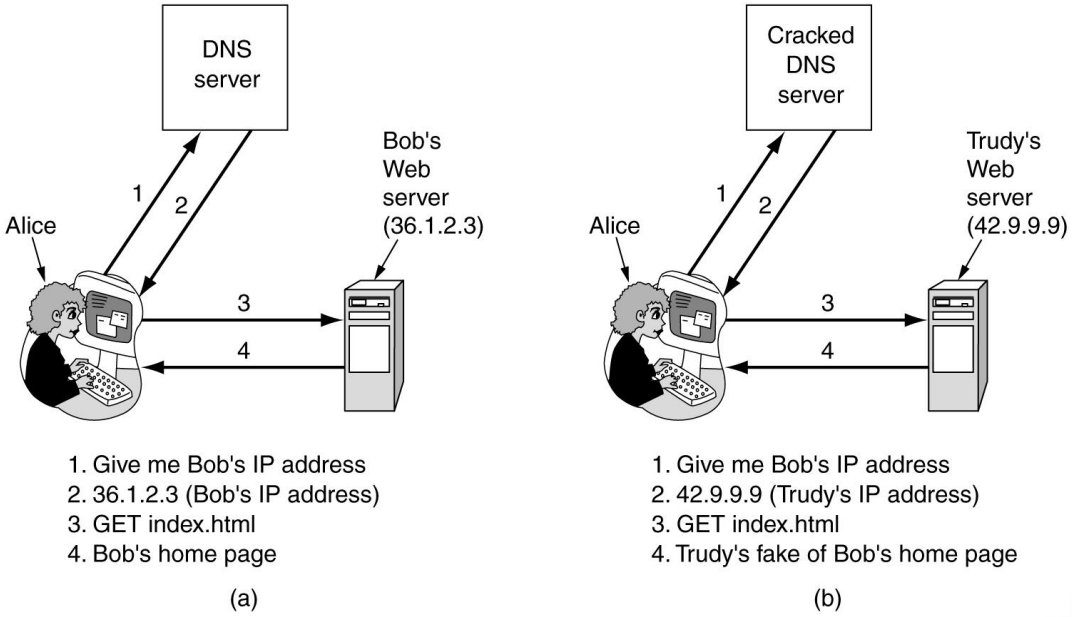
- Onde se encontra a maioria de intrusos;
- Pode ser dividida em três partes:
  1. Como os objetos e recursos são nomeados com segurança?
  2. Como é possível estabelecer conexões seguras e confiáveis?
  3. O que acontece quando um site envia a um cliente um fragmento de código executável?

Segurança na Web

- Onde se encontra a maioria de intrusos;
- Pode ser dividida em três partes:
  1. Como os objetos e recursos são nomeados com segurança?
  2. Como é possível estabelecer conexões seguras e confiáveis?
  3. O que acontece quando um site envia a um cliente um fragmento de código executável?

Segurança na Web

1. Como os objetos e recursos são nomeados com segurança?
   - **DNS spoofing**: enganar um servidor DNS fazendo-o instalar um falso endereço IP;
   - ***DNSsec*** (***DNS security***): esforço contínuo da IETF para tornar o DNS fundamentalmente seguro (ainda não totalmente implementado);



Segurança na Web

2. Como é possível estabelecer conexões seguras e confiáveis?
   - Depois de garantir nomes seguros é necessário garantir conexões seguras;
   - Para isso é usado o **SSL** (***Secure Sockets Layer***);
     - Constrói uma conexão segura, incluindo:
       1. Negociação de parâmetros entre cliente e servidor;
       2. Autenticação mútua de cliente e servidor;
       3. Comunicação secreta;
       4. Proteção de integridade dos dados;
   - Fica entre a camada de aplicação e transporte;
   - Quando o **HTTP** é usado sobre o **SSL** ele se denomina **HTTPS** (***Secure HTTP***);
   - Não está restrito ao uso nos navegadores.

Segurança na Web

3. O que acontece quando um site envia a um cliente um fragmento de código executável?
   - Atualmente as aplicações Web estão recheadas de pequenos programas que executam na máquina do cliente;
   - Baixar e executar este código móvel é sem dúvida um grande risco de segurança;
   - Alguns métodos foram criados para minimizar este risco:
     - Utilização de um **monitor de segurança**, que limita os recursos do sistema ao qual o código poderá ter acesso;
     - Utilização de **assinatura de código**, para garantir que o código é original e confiável;
     - Configurações de navegador para impedir a execução de códigos móveis;

Introdução;
Criptografia;
Assinaturas digitais;
Gerenciamento de chaves públicas;
Segurança da comunicação;
Protocolos de autenticação;
Segurança de Correio Eletrônico e Web;
Questões sociais.

QUESTÕES SOCIAIS

Questões sociais

- Normalmente envolve 3 áreas:
  - Privacidade;
  - Liberdade de expressão;
  - Direitos autorais;

- Algumas questões foram discutidas na primeira parte da disciplina;

Fim!

REFERÊNCIAS:

- **A.S. TANENBAUM, *Redes de Computadores*, Prentice Hall, 5a. edição, 2011;**
- Materiais didáticos dos professores:
  - **Rande A. Moreira**, UFOP / 2011-01
    Disponível em: http://randearievilo.com.br/redes/ (acesso em 17/08/2011);
  - **Marcos Vieira**, UFMG / 2011-01
    Disponível em: http://homepages.dcc.ufmg.br/~mmvieira/redes/redes.html
    (acesso em 17/08/2011);