Tópicos de Ambiente Web

Segurança

Professora: Sheila Cáceres

Componentes dos sistemas de segurança de dados

- Política de segurança de dados
- Serviços básicos para segurança computacional (security)
- Controle e Auditoria

Política de segurança de dados

- Planejamento - Avaliação e análise de riscos e custos.
- Especificação para implementação de salvaguardas e serviços.
- Atribuição documentada de autorizações e responsabilidades

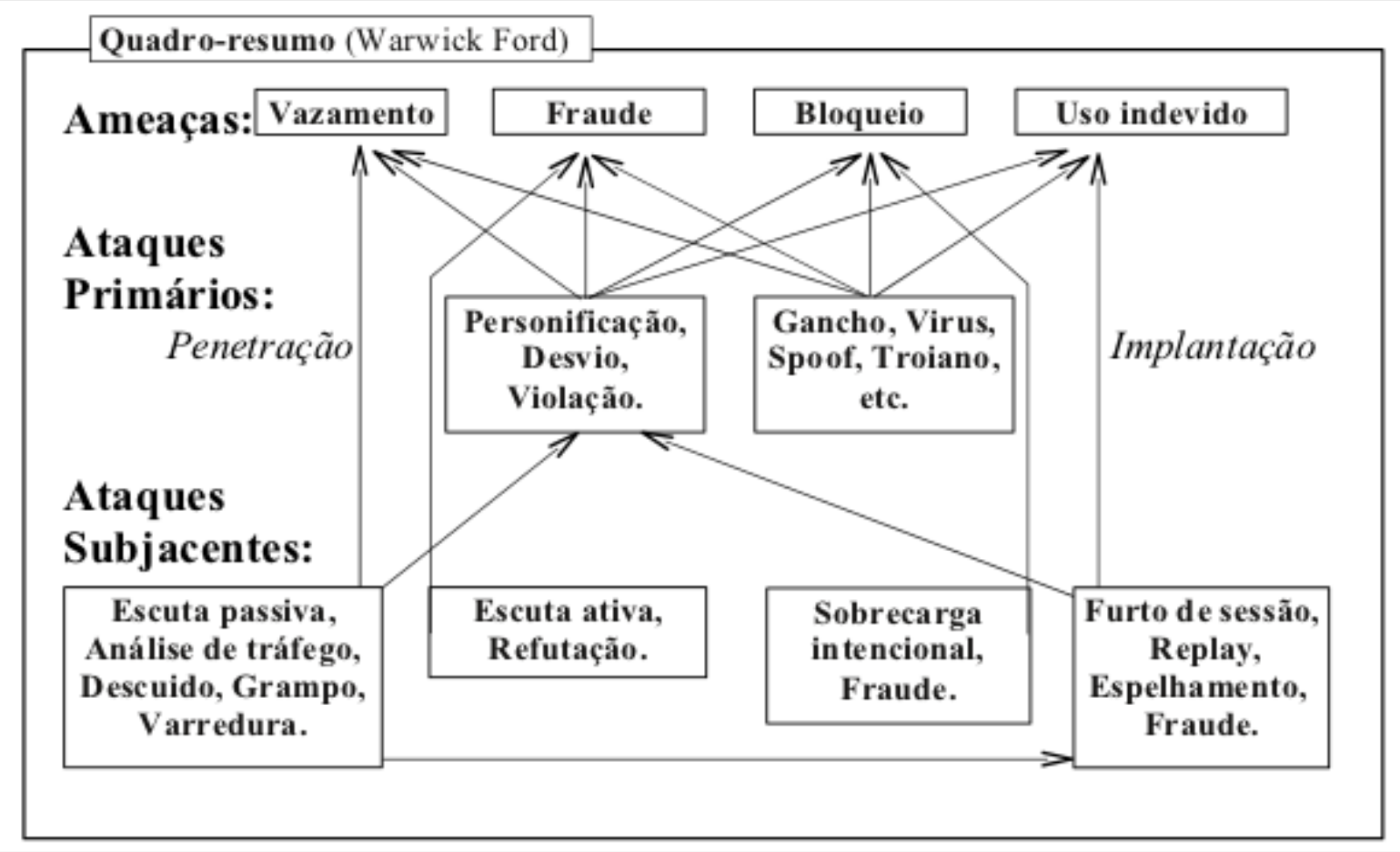
Serviços para segurança computacional (security)

- Autorização: identificação para controle de acesso.
- Cifragem: codificação para sigilo ou privacidade.
- Autenticação: validação de origem e/ou integridade de conteúdo.
- Certificação: autenticação recursiva com validação objetiva.

Controle e Auditoria

- Monitoramento: gerenciadores (rede, backup) logs, IDS, etc.
- Rastreamento: antivirus, firewalls, proxies, IDS, etc.
- Avaliação: testes de penetração, análise estatística, relatórios, revisão de políticas, de estratégias, etc.

Tipos de ataque a sistemas computacionais



Criptografia

Serviços Oferecidos

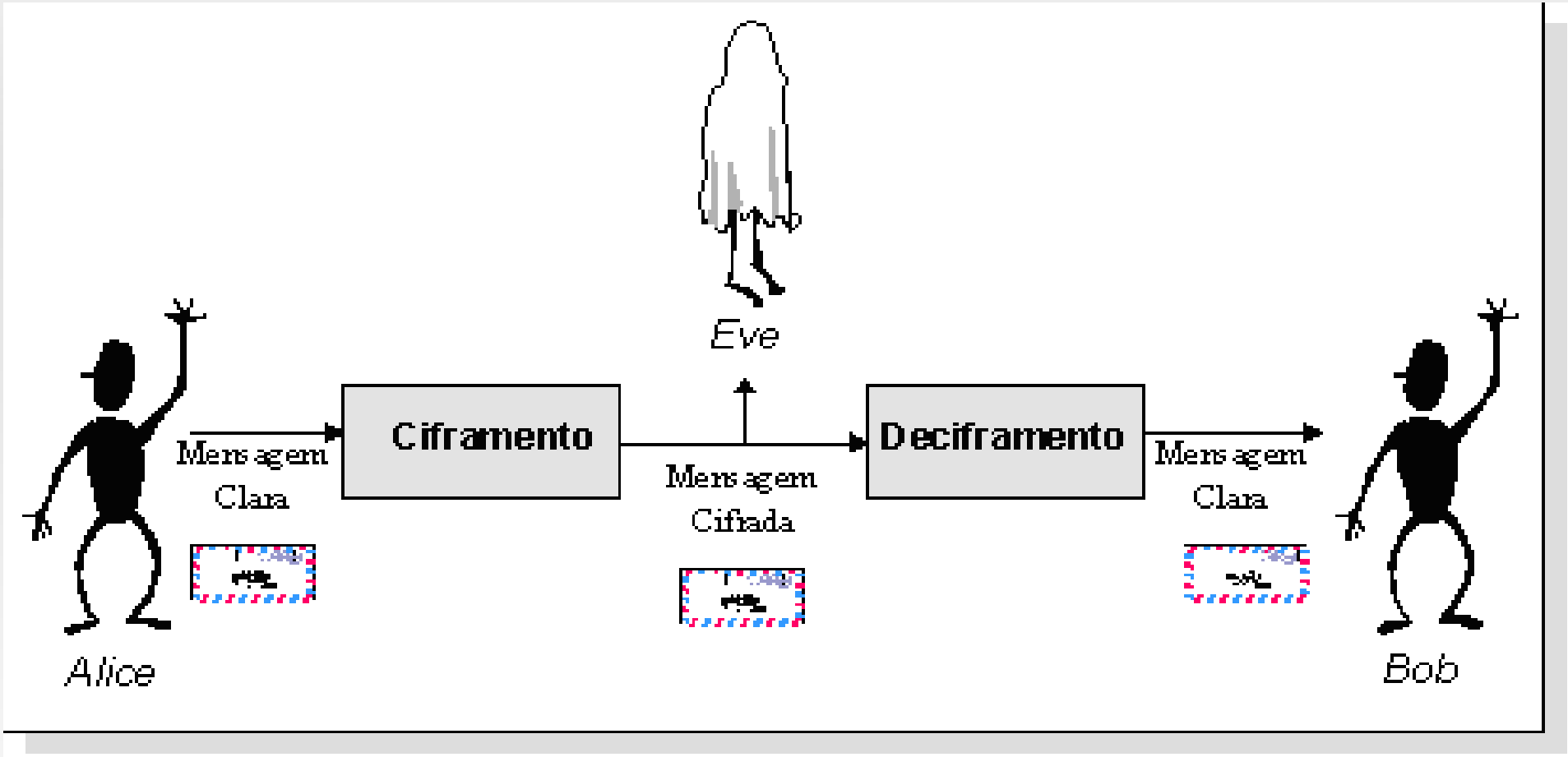
Serviços	Descrição
Disponibilidade	Garante que uma informação estará disponível para acesso no momento desejado.
Integridade	Garante que o conteúdo da mensagem não foi alterado.
Controle de acesso	Garante que o conteúdo da mensagem somente será acessado por pessoas autorizadas.
Autenticidade da origem	Garante a identidade de quem está enviando a mensagem.
Não-repudiação	Previne que alguém negue o envio e/ou recebimento de uma mensagem.
Privacidade (confidencialidade ou sigilo)	Impede que pessoas não autorizadas tenham acesso ao conteúdo da mensagem, garantindo que apenas a origem e o destino tenham conhecimento.

Ex: compra pela Internet: a informação que permite a transação precisa estar disponível no dia e na hora que o cliente desejar efetuá-la (disponibilidade), o valor da transação não pode ser alterado (integridade), somente o cliente que está comprando e o comerciante devem ter acesso à transação (controle de acesso), o cliente que está comprando deve ser realmente quem diz ser (autenticidade), o cliente tem como provar o pagamento; e o comerciante não têm como negar o recebimento (não-repúdio); e o conhecimento do conteúdo da transação fica restrito aos envolvidos (privacidade).

Criptografia Simétrica

- Baseia-se em dois componentes: um **algoritmo** e uma **chave**.
- Um algoritmo é uma transformação matemática. Ele converte uma mensagem em claro em uma mensagem cifrada e vice-versa.
- Exemplo Quando Alice (origem) cifra uma mensagem, ela utiliza um algoritmo de ciframento para transformar o conteúdo em claro da mensagem em texto cifrado. Quando Bob (destinatário) decifra uma mensagem, ele utiliza o algoritmo de deciframento correspondente para converter o texto cifrado de novo em uma mensagem clara.

Criptografia Simétrica

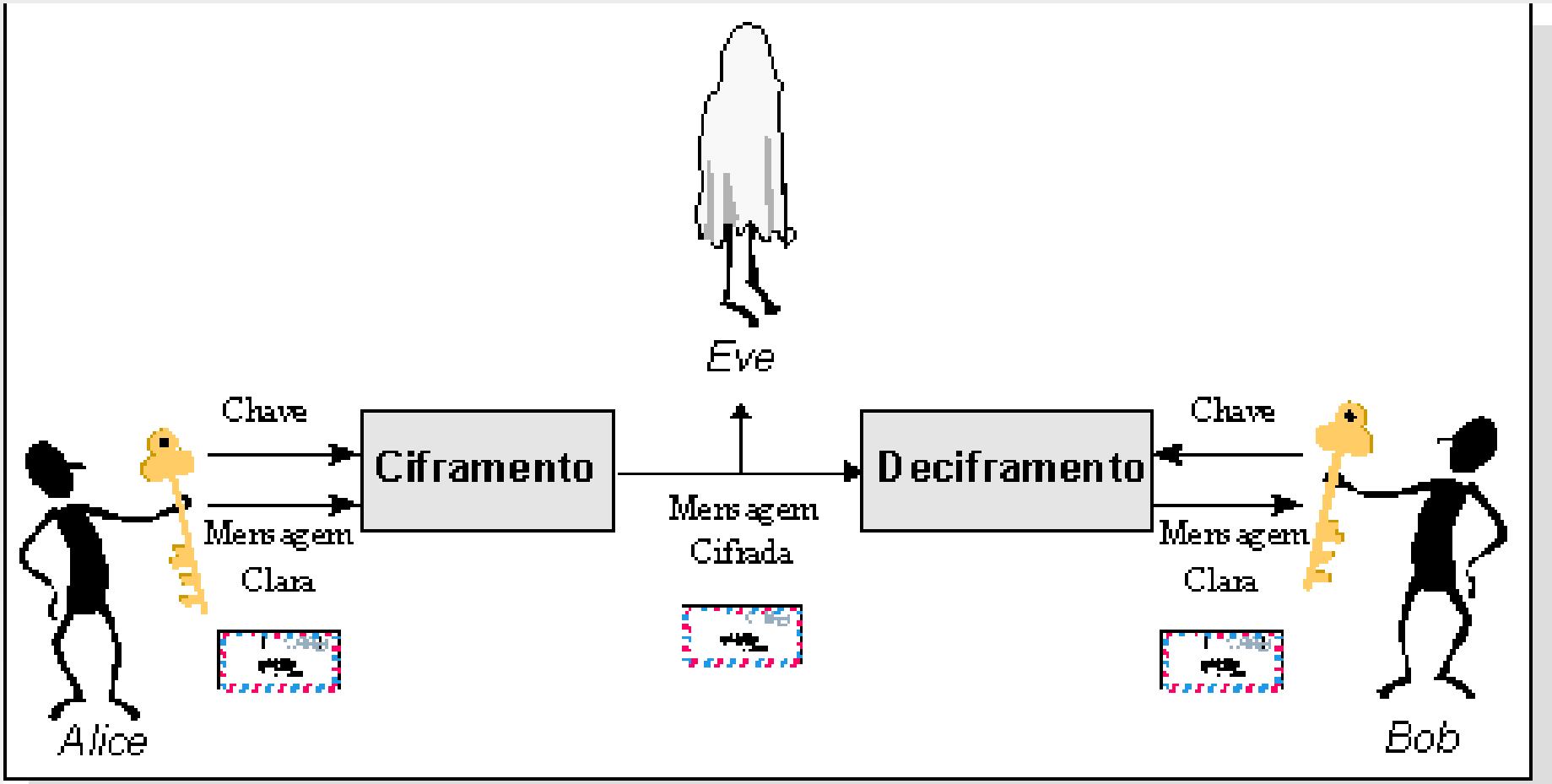


Antigamente, a segurança do criptamento estava baseada somente no sigilo do algoritmo criptográfico. Se eve conhecesse o algoritmo, poderia decifrar a mensagem

Criptografia Simétrica

- Para evitar esse problema usou-se a chave.
- Uma chave é uma cadeia aleatória de bits utilizada em conjunto com um algoritmo. Cada chave distinta faz com que o algoritmo trabalhe de forma ligeiramente diferente.
- A utilização da chave apresenta vantagens:
  - Permitir a utilização do mesmo algoritmo criptográfico para a comunicação com diferentes receptores, apenas trocando a chave.
  - Pode-se trocar facilmente a chave no caso de uma violação, mantendo o mesmo algoritmo.
- Número de chaves depende do tamanho (número de bits) da chave. Ex: Chave de 8 bits permite combinação de no máximo 256 chaves (2^8). Quanto maior o tamanho da chave, mais difícil quebra-la.

Criptografia Simétrica

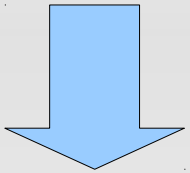


Mesmo que eve conheça o algoritmo, não conseguirá decifrar a mensagem pois não tem a chave.

A segurança do sistema passa a residir não mais no algoritmo e sim na chave empregada. É ela que agora, no lugar do algoritmo, deverá ser mantida em segredo por Alice e Bob.

Criptografia Simétrica

Chave de ciframento ~= Chave deciframento



Criptografia simétrica ou de chave secreta

Quando a chave de desciframento é facimente obtida a partir da chave de ciframento , tmb considera-se cript. Simétrica.

- Ambas precisam ser compartilhadas previamente entre origem e destinatário previamente, utilizando-se um canal seguro e independente.

Criptografia Simétrica - Problemas

- Para ***n*** usuários precisaríamos de algo da ordem de n^2 chaves.
- A chave deve ser trocada entre as partes e armazenada de forma segura, o que nem sempre é fácil de ser garantido;
- A criptografia simétrica não garante a identidade de quem enviou ou recebeu a mensagem (autenticidade e não-repudiação).

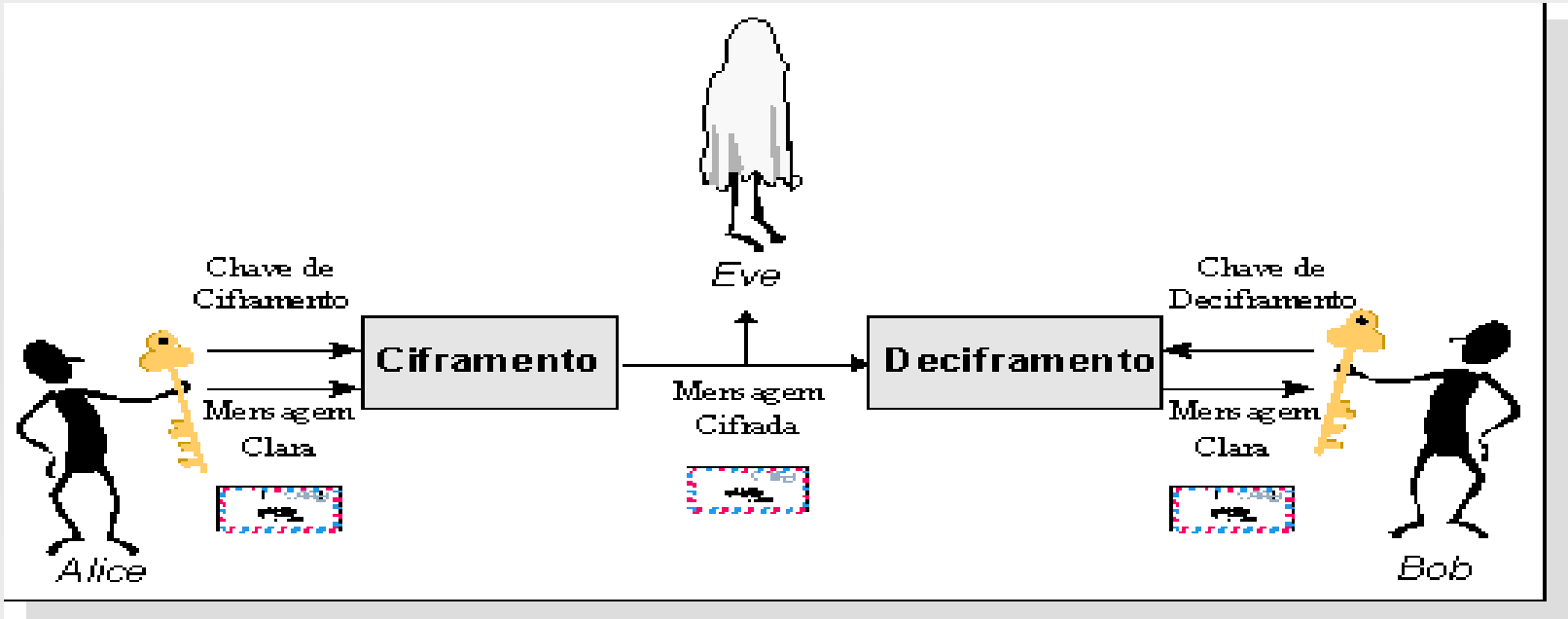
Algoritmos Simétricos

- O Data Encryption Standard (DES) é o algoritmo simétrico mais disseminado no mundo. Foi criado pela IBM em 1977 e, apesar de permitir cerca de 72 quadrilhões de combinações (256), seu tamanho de chave (56 bits) é considerado pequeno, tendo sido quebrado por "força bruta" em 1997 em um desafio lançado na Internet.
- O 3DES é uma simples variação do DES, utilizando-o em três ciframentos suscessivos. É seguro porém lento
- IDEA
- Blowfish
- RC2

Criptografia Assimétrica

- Chamada também criptografia de chave pública.
- Baseada no conceito de par de chaves: uma chave **privada** e uma chave **pública**. Qualquer uma das chaves é utilizada para cifrar uma mensagem e a outra para decifrá-la.
- As mensagens cifradas com uma das chaves do par só podem ser decifradas com a outra chave correspondente.
- A chave privada deve ser mantida secreta, enquanto a chave pública disponível livremente para qualquer interessado.

Criptografia Assimétrica



Bob e todos os que desejam comunicar-se de modo seguro geram uma chave de ciframento e sua correspondente chave de deciframento.

Ele mantém secreta a chave de deciframento (chave privada). Ele torna pública a chave de ciframento (chave pública).

A chave pública pode ser obtida por qualquer pessoa. Bob inclusive encoraja isto, enviando-a para seus amigos ou publicando-a em boletins.

Criptografia Assimétrica

- Alice deseja enviar uma mensagem a Bob
- Alice precisa primeiro encontrar a chave pública de Bob.
- Após, ela cifra sua mensagem utilizando a chave pública de Bob, despachando-a em seguida.
- Quando Bob recebe a mensagem, ele a decifra facilmente com sua chave privada (só ele pode).
- Eve, que interceptou a mensagem em trânsito, não conhece a chave privada de Bob, embora conheça sua chave pública. Mas este conhecimento não o ajuda a decifrar a mensagem.
- Mesmo Alice, que foi quem cifrou a mensagem com a chave pública de Bob, não pode decifrá-la agora.

Algoritmos Assimétricos

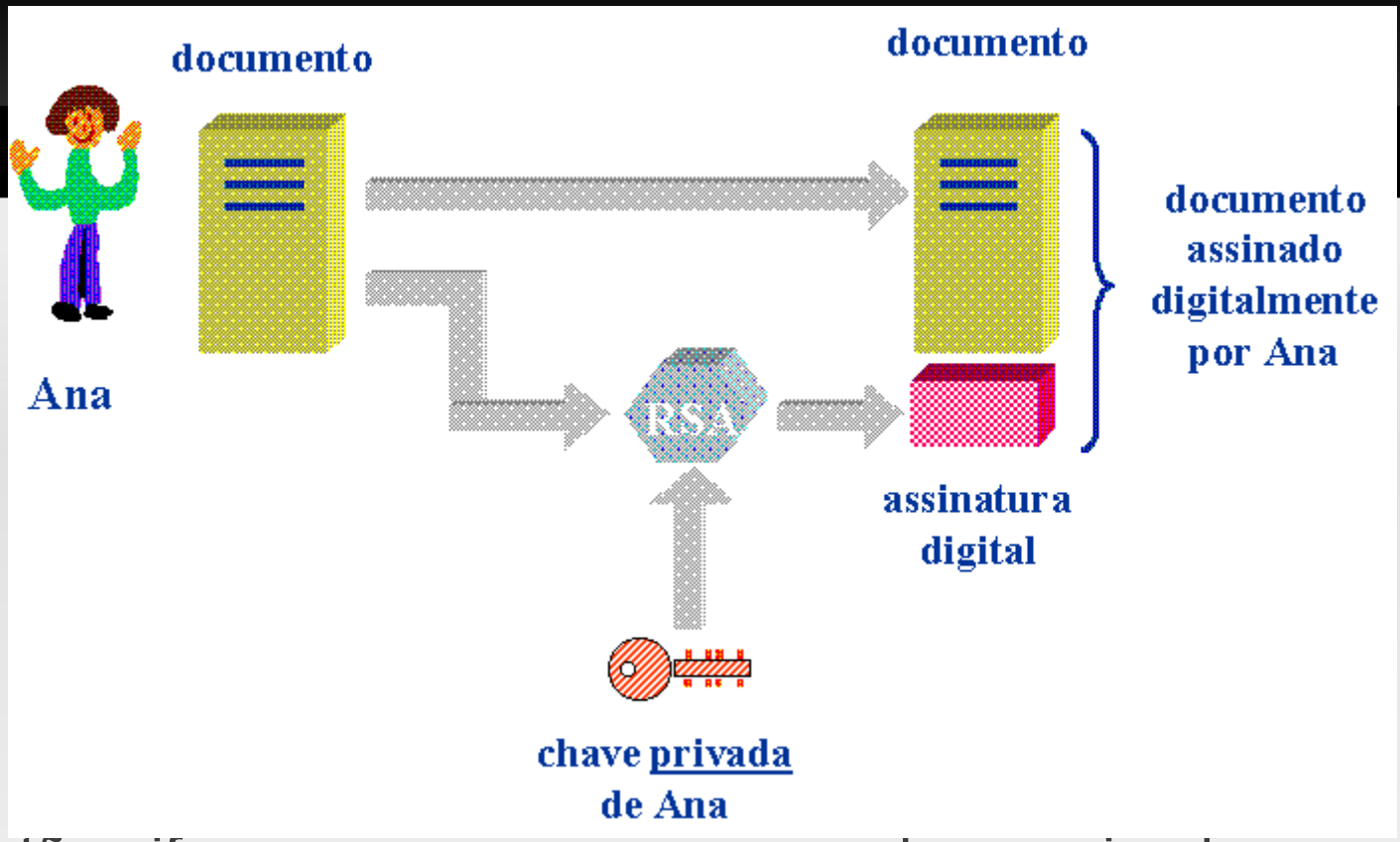
- **O RSA** é um algoritmo assimétrico que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. É, atualmente, o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. O RSA utiliza números primos.
  - A premissa por trás do RSA é que é fácil multiplicar dois números primos para obter um terceiro número, mas muito difícil recuperar os dois primos a partir daquele terceiro número.

Algoritmos Assimétricos

- O **ElGamal** envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto.
- **Diffie-Hellman** Também baseado no problema do logaritmo discreto
- **Curvas Elípticas** implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie e Hellman, usando curvas elípticas

Assinatura Digital

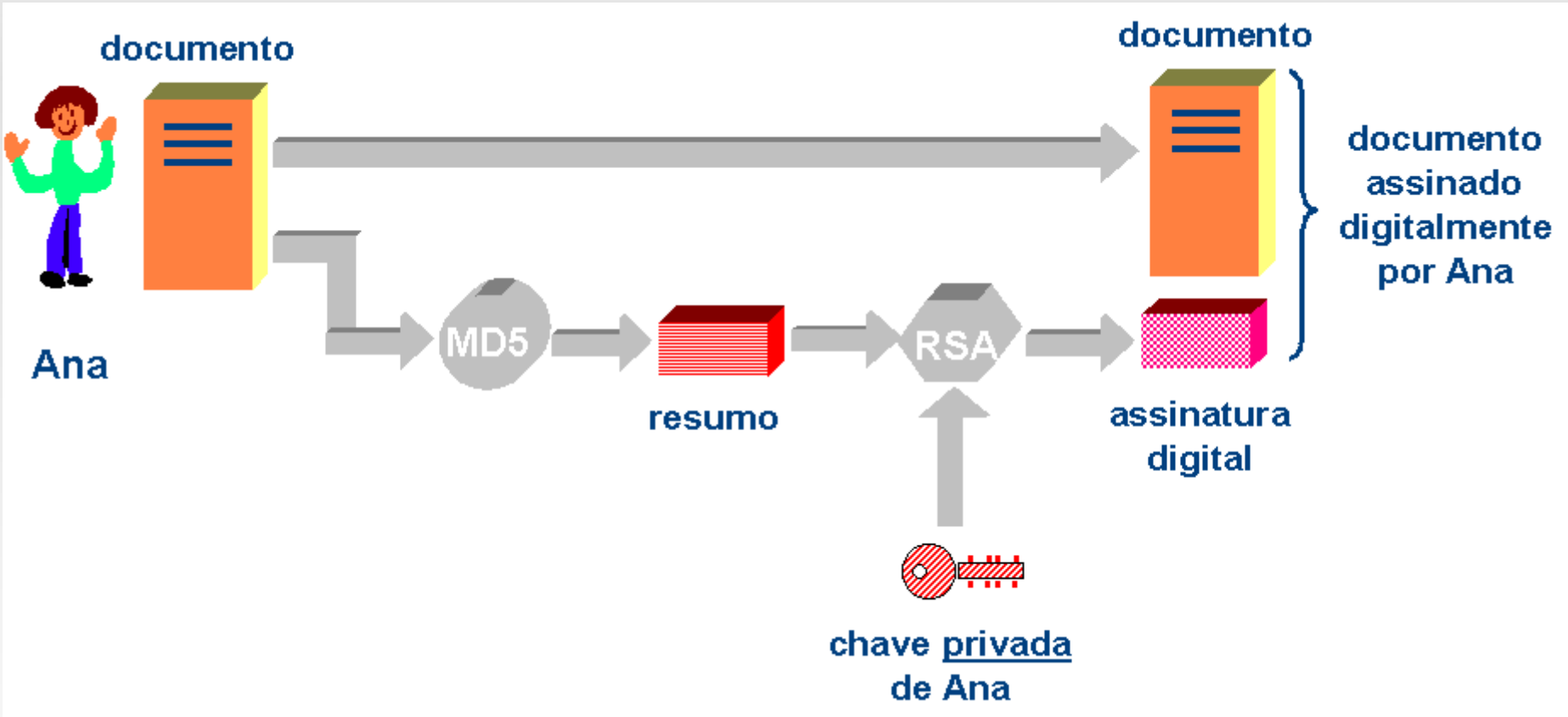
- A assinatura digital permite garantir a autenticidade de quem envia a mensagem, associada à integridade do seu conteúdo.
- Para isso tmb podemos usar criptografia com chave pública
- **Exemplo**, suponha que vocês(origem) têm trillizos e querem comunicar o nascimento deles para todos os seus amigos. Vcs desejam garantir aos mesmos que a mensagem foi enviada realmente por vcs.
  - Embora não se importe com o sigilo da mensagem, deseja que a mesma chegue integra aos destinatários, sem alterações como, por exemplo, do sexo da criança.



- Alice então cifra a mensagem com sua chave privada e a envia, em um processo denominado de assinatura digital. Cada um que receber a mensagem deverá decifrá-la, ou seja, verificar a validade da assinatura digital, utilizando para isso a chave pública de Alice. Como a chave pública de Alice apenas decifra (ou seja, verifica a validade de) mensagens cifradas com sua chave privada, fica garantida assim a autenticidade, integridade e não-repudiação da mensagem. Pois se alguém modificar um bit do conteúdo da mensagem ou se outra pessoa assiná-la ao invés de Alice, o sistema de verificação não irá reconhecer a assinatura digital de Alice como sendo válida.

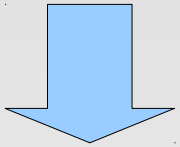
Função Hashing

- Mecanismo fundamental para o adequado emprego da assinatura digital.
- Sua utilização como componente de assinaturas digitais se faz necessário devido à lentidão dos algoritmos assimétricos, em geral cerca de 1.000 vezes mais lentos do que os simétricos.
- É inviável utilizar puramente algoritmos de chave pública para assinaturas digitais, debem ser integralmente "cifradas" com a chave privada de alguém.
- Ao invés disso, é empregada uma função Hashing, que gera um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar, de qualquer tamanho. Assim, a função Hashing oferece agilidade nas assinaturas digitais, além de integridade confiável, conforme descrito a seguir.
- Serve, portanto, para garantir a integridade do conteúdo da mensagem que representa.


documento
documento
documento assinado digitalmente por Ana
Ana
MD5
resumo
RSA
assinatura digital
chave privada de Ana

Criptografia Simétrica x Assimétrica: Protocolos Criptográficos

- Qual o modelo de criptografia que devemos utilizar? Simétrico ou assimétrico?



Os dois, em um modelo denominado híbrido.

- O algoritmo simétrico, por ser muito mais rápido, é utilizado no ciframento da mensagem em si.
- Enquanto o assimétrico, embora lento, permite implementar a distribuição de chaves e a assinatura digital. Além disso, o mecanismo de Hashing permite complementar a assinatura digital.

Criptografia Simétrica x Assimétrica

Criptografia Simétrica.	Criptografia Assimétrica.
Rápida.	Lenta.
Gerência e distribuição das chaves é complexa.	Gerência e distribuição simples.
Não oferece assinatura digital	Oferece assinatura digital.

Protocolos que empregam sistemas criptográficos híbridos:

- **SSL e TLS:** Oferecem suporte de segurança criptográfica para os protocolos NTTP, **HTTP**, SMTP e Telnet. Permitem utilizar diferentes algoritmos simétricos, message digest (hashing) e métodos de autenticação e gerência de chaves (assimétricos).
- **PGP:** Inventado por Phil Zimmermman em 1991, é um programa criptográfico **famoso** e bastante difundido na Internet, destinado a criptografia de e-**mail pessoal**. *Algoritmos suportados*: hashing: MD5, SHA-1, simétricos: CAST-128, IDEA e 3DES, assimétricos: RSA, Diffie-Hellman/DSS. Versão mais recente: 6.5.3.

- **O SET** é um conjunto de padrões e protocolos, para realizar transações financeira seguras, como as realizadas com cartão de crédito na Internet. Oferece um canal de comunicação seguro entre todos os envolvidos na transação. Garante autenticidade X.509v3 e privacidade entre as partes

Resumindo

- Algoritmos criptográficos podem ser combinados para a implementação dos três mecanismos criptográficos básicos:
  - o ciframento,
  - a assinatura e
  - o Hashing.
- Estes mecanismos são componentes dos protocolos criptográficos, embutidos na arquitetura de segurança dos produtos destinados ao comércio eletrônico.
- Viabilizam o **comércio eletrônico:** disponibilidade, sigilo, controle de acesso, autenticidade, integridade e não-repúdio.

Bibliografia

- [1] http://www.smartsec.com.br/criptografia.html

  Acessado no 14 de Maio, 2013.