SEGURANÇA DA INFORMAÇÃO E DE REDES

Prof. Milton Palmeira Santana

Um pouco mais sobre criptografia

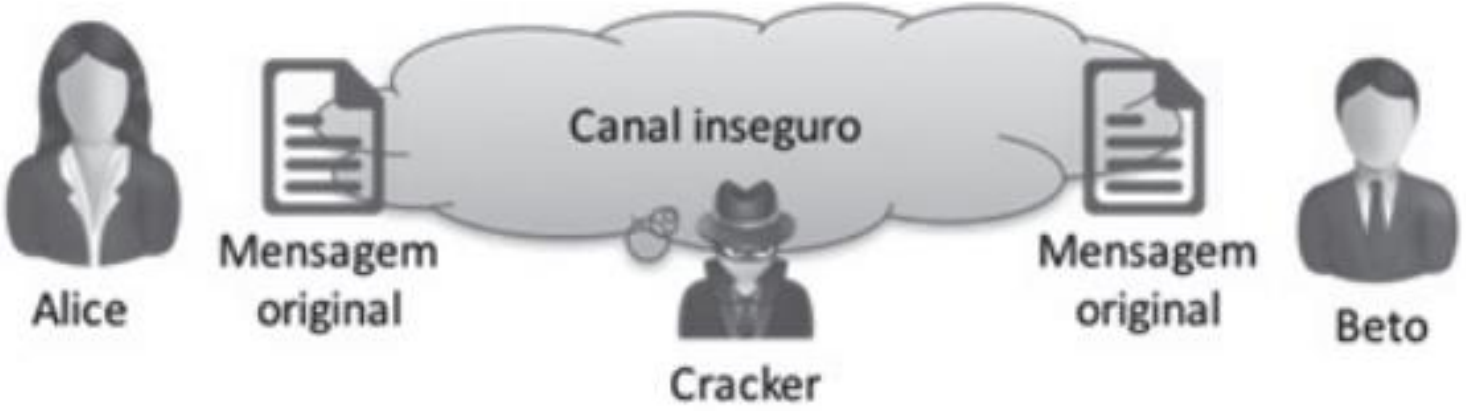
- A criptografia é o estudo de técnicas matemáticas relacionadas a aspectos da segurança da informação como confidencialidade, integridade, autenticação de entidade e autenticação de origem de dados.
- A criptografia é baseada em um conjunto de técnicas que incluem a cifragem, funções de hash e assinaturas digitais. A escolha da melhor técnica depende de critérios como:
  - Nível de segurança requerido.
  - Funcionalidade ou objetivo de segurança.
  - Métodos de operação dos algoritmos, que podem ser diferentes para cada funcionalidade.
  - Desempenho.
  - Facilidade de implementação.

Um pouco mais sobre criptografia

- Há uma grande quantidade de técnicas em criptografia. Alguns exemplos são:
  - Criptografia de chave privada ou simétrica.
  - Criptografia de chave pública ou assimétrica.
  - Funções de hash criptográfico.
  - Assinatura digital.

Criptografia de chave privada

- A função essencial da criptografia é a garantia de confidencialidade ou de sigilo da informação, em que há a proteção dos dados contra divulgação não autorizada.
- Imagine que Alice quer enviar uma mensagem para Beto por um canal, que normalmente é inseguro. Nesse canal, um atacante pode escutar a mensagem, afetando a privacidade ou a confidencialidade da comunicação entre Alice e Beto.



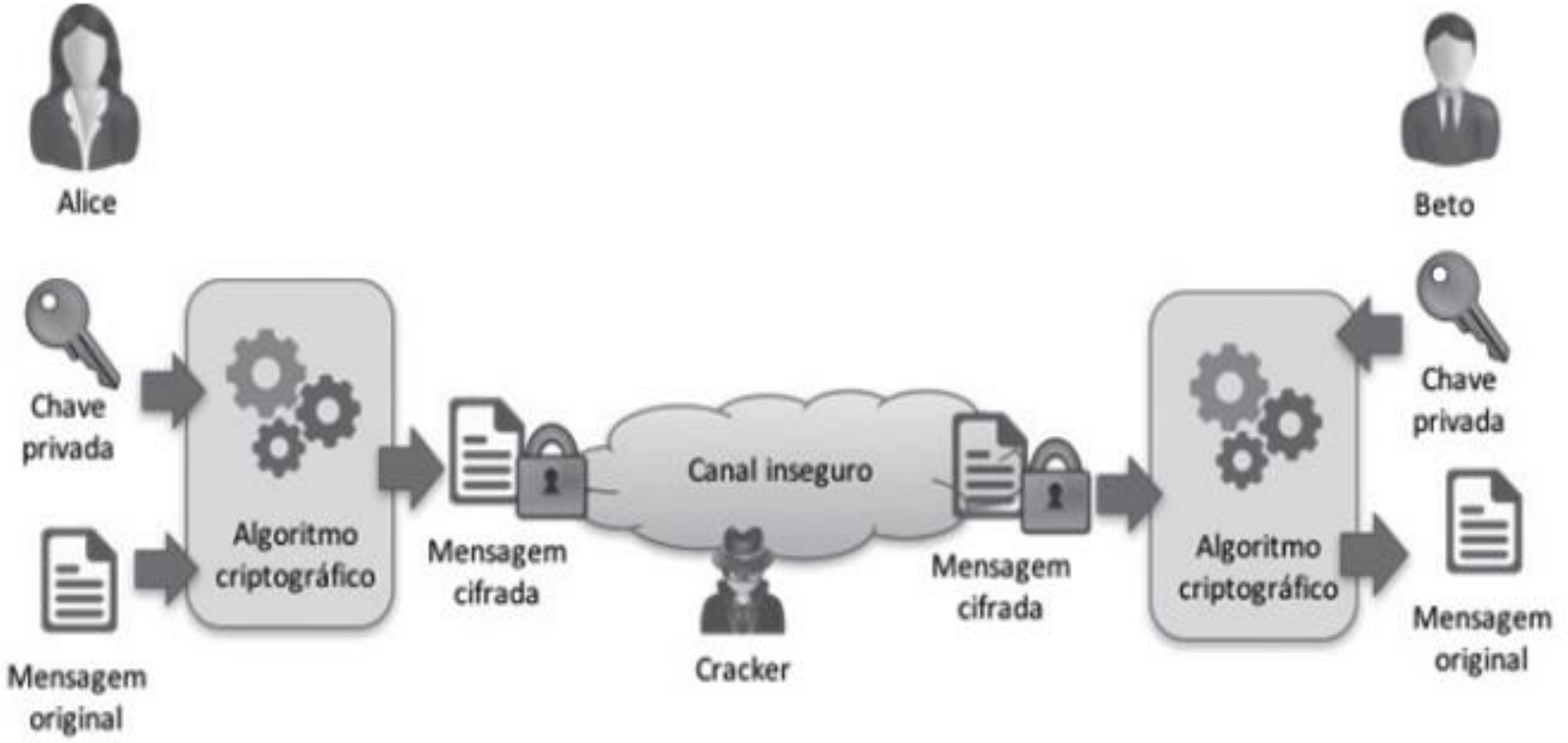
Criptografia de chave privada

- Com o uso da criptografia, Alice pode enviar uma mensagem cifrada para Beto. Alice utiliza um algoritmo criptográfico e uma chave secreta privada para cifrar a mensagem original.

- O resultado é um texto incompreensível para o atacante. Beto recebe a mensagem cifrada e utiliza a mesma chave secreta (compartilhada com Alice) para decifrar a mensagem e chegar ao conteúdo original.

- Os processos de cifragem e decifragem são realizados via uso de algoritmos com funções matemáticas que transformam os textos claros, que podem ser lidos, em textos cifrados, que são inteligíveis, e vice-versa.

Criptografia de chave privada



Criptografia de chave privada

- Esse é o funcionamento básico da criptografia simétrica ou de chave privada, em que a chave secreta é a mesma (simétrica) para a cifragem e a decifragem, e que, portanto, deve ser compartilhada. Este é um dos grandes desafios deste tipo de criptografia: como fazer a troca segura de chaves.

- No exemplo de Alice e Beto, ambos têm que combinar a chave privada para que eles possam cifrar e decifrar a mensagem. No caso de uso do mesmo canal inseguro para a troca da chave privada, a mensagem poderá ser comprometida, pois o atacante poderá ficar “escutando” o canal para a obtenção da chave privada, uma vez que é utilizada para cifrar e decifrar a mensagem.

Criptografia de chave privada

- Quais seriam as minhas alternativas?
- Utilizar o mesmo local inseguro, por mais que tenha o problema citado anteriormente?
- Utilizaria um caminho alternativo?
- E se você precisasse se comunicar com 100 pessoas diferentes. Utilizaria a mesma chave para todas as mensagens/pessoas?
- E para enviar individualmente a mensagem para essas 100 pessoas?

Criptografia de chave privada

- Assim, a troca de chaves, é um dos grandes desafios da criptografia simétrica. Mais do que a troca de chaves, o gerenciamento delas, que envolve tempo de validade, armazenamento, geração, uso e substituição, é fundamental.

- A criptografia de chave privada ou simétrica é rápida de ser executada em termos de processamento computacional, porém incorpora o desafio da troca de chaves. A criptografia de chave pública ou assimétrica é computacionalmente mais pesada, porém é adequada para ser utilizada na troca de chaves.

Criptografia de chave privada

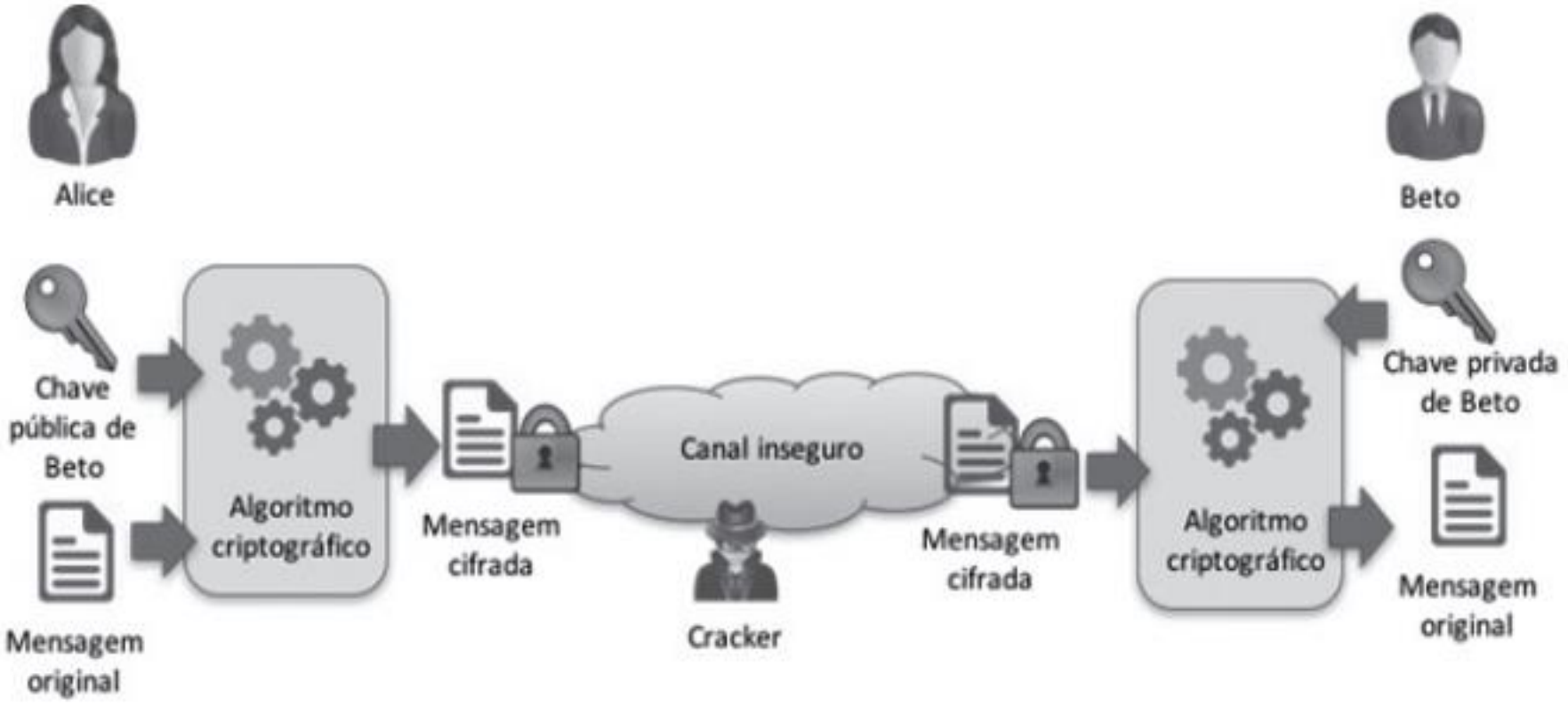
- Exemplos de algoritmos simétricos:
  - Cifras de fluxo: a cifragem é feita normalmente a cada dígito (byte).
  - Cifras de blocos: agrupa um conjunto de bits da mensagem em blocos, e a cifragem é feita sobre cada um desses blocos
- O AES (Advanced Encryption Standard), também conhecido por Rijndael, é considerado o padrão de criptografia, substituindo o DES (Data Encryption Standard). O AES é uma cifra de blocos de 128 bits.

Criptografia de chave pública

- A criptografia de chave pública ou assimétrica utiliza um par de chaves para a troca de mensagens. Uma chave do par é utilizada para cifrar a mensagem, que só pode ser decifrada pelo par correspondente. Dessa forma, diferentemente da criptografia de chave privada, em que a chave é compartilhada, na criptografia de chave pública não é necessária a troca de chaves privadas.

- O par de chaves da criptografia de chave pública é composto por uma chave pública e uma chave privada. A chave pública pode ser divulgada publicamente, e é utilizada para cifrar uma mensagem. Uma vez cifrada, essa mensagem só poderá ser decifrada pelo detentor da chave privada, que nunca é compartilhada.

Criptografia de chave pública



Criptografia de chave pública

- Desta forma, caso a mensagem seja capturada em um canal inseguro, o atacante não poderá recuperar a mensagem original sem a chave privada correspondente, que está com o seu dono. Essa chave privada, em tese, nunca foi transmitida, o que reduz as chances de seu comprometimento.

- O que está por trás do par de chaves utilizado na criptografia assimétrica é a função matemática conhecida como trapdoor ou “alçapão”, em que é fácil realizar o cálculo em uma direção, porém dificílimo na direção oposta sem o uso de uma informação especial.

Criptografia de chave pública

- Exemplo:
- O número 6895601 é o produto de dois números primos. A fatoração é difícil sem que um dos números primos seja revelado. O algoritmo criptográfico RSA utiliza a fatoração de números primos bastante grandes para proteger as informações, e é um dos algoritmos mais conhecidos de chave pública. A chave pública do RSA é gerada com base nesses dois grandes números primos e publicada. A mensagem é decifrada com a chave privada correspondente, que possui a informação especial que ajuda na fatoração dos dois números primos.

Esteganografia

- A esteganografia tem origem nos termos gregos “steganos”, que significa “coberta, escondia ou protegida”, e “graphein”, que significa “escrita”, e é o uso de técnicas para ocultar a existência de uma mensagem dentro de outra. O termo foi utilizado primeiramente em 1499 por Johannes Trithemius, na obra Steganographia, que foi publicada apenas em 1606, e era considerada um livro de mágicas.

- A diferença entre a criptografia e esteganografia é que a primeira oculta o significado da mensagem, enquanto a segunda oculta a existência da mensagem.

Esteganografia

- Alguns exemplos de uso da esteganografia são:
  - Uso de tintas invisíveis.
  - Mensagens escondidas no corpo do mensageiro, como na cabeça raspada, que era depois escondida após o crescimento dos cabelos.
  - Código Morse costurado na roupa do mensageiro.
  - Mensagens escritas nos envelopes nas áreas dos selos.
  - Inserção de mensagens nos bits menos significativos de áudios ou imagens.
  - Inserção de mensagens em seções de arquivos.
  - Uso de caracteres Unicode que se parecem com conjunto de caracteres ASCII padrão.

Esteganografia

- Exemplos de utilização famosos:

- Livro/Filme Código da Vinci

- Estudiosos debatem há séculos se Leonardo da Vinci escondeu ou não mensagens secretas na Mona Lisa.

Criptografia de chave pública

- Um dos desafios do uso da criptografia é o processo de troca de chaves. Na criptografia de chave privada ou simétrica, em que as chaves para cifragem e decifragem são as mesmas, a troca de chaves por um canal inseguro está sujeita ao ataque man-in-the-middle, no qual a chave pode ser capturada, o que faz com que a mensagem possa ser naturalmente aberta pelo inimigo.

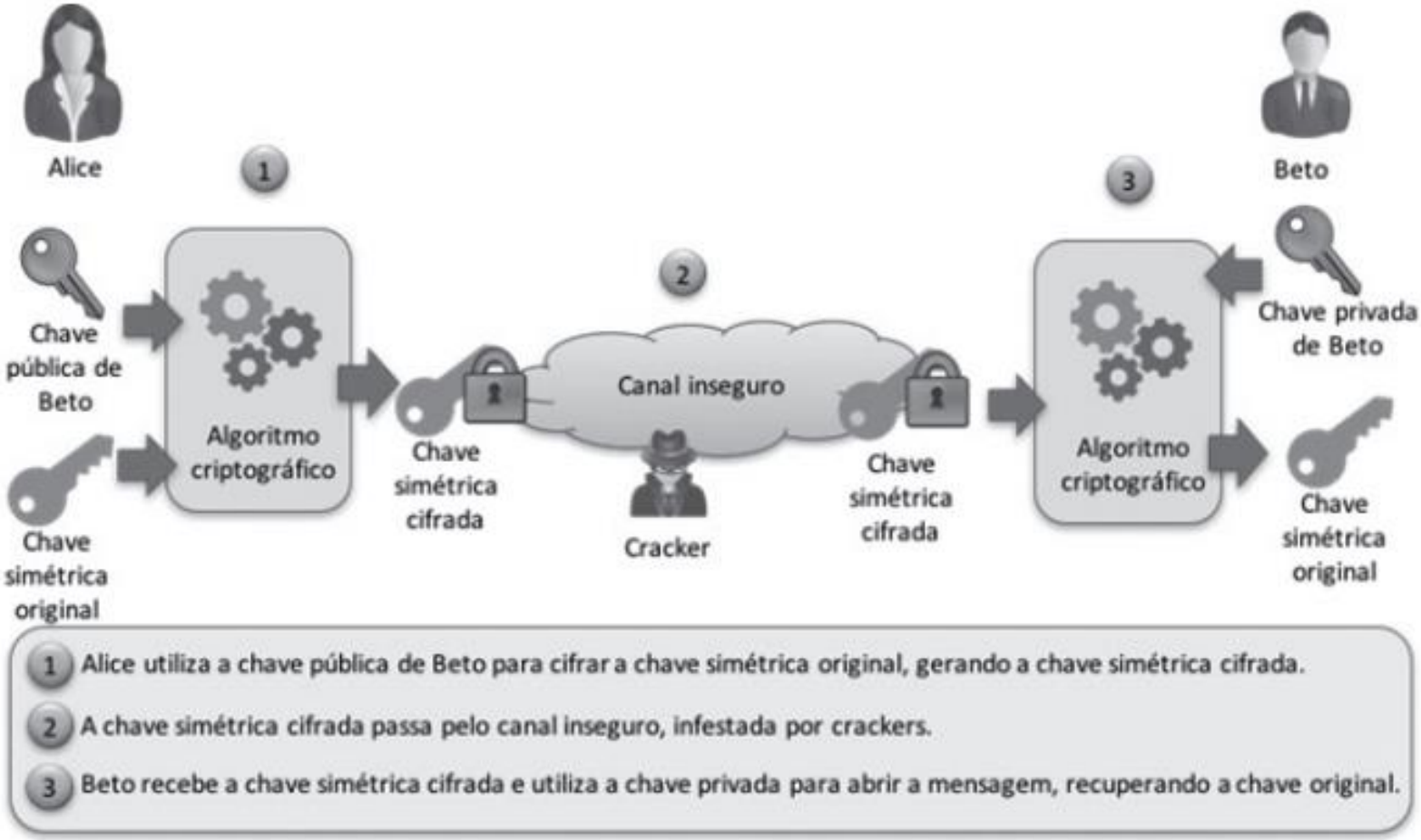
- Já a criptografia de chave pública ou assimétrica utiliza um par de chaves (pública e privada), que são utilizadas em conjunto para a cifragem (com a chave pública) e decifragem (com a chave privada).

- Como a chave é pública, não há o problema de a chave ser capturada por man-in-the-middle como ocorre com a criptografia simétrica. O lado negativo, porém, está no poder de processamento necessário para a cifragem e decifragem, que é maior na criptografia assimétrica.

Um pouco mais sobre criptografia

- Dessa forma, é muito custoso o uso da criptografia de chave pública para proteger mensagens inteiras, e isso faz com que ela seja mais utilizada para a proteção da chave privada da criptografia simétrica que é, de fato, utilizada para proteger as mensagens. A Figura 3.4 mostra a criptografia de chave pública sendo utilizada para a troca de chave privada compartilhada entre Alice e Beto.

Um pouco mais sobre criptografia



Um pouco mais sobre criptografia

- Esse mecanismo de uso em conjunto da criptografia de chave pública com a criptografia de chave privada é bastante comum em várias aplicações, como é o caso do SSL (Secure Sockets Layer, para transmissões seguras), por exemplo.

- O início da criptografia de chave pública foi na década de 70, quando o pesquisador norte-americano Ralph Merkle divulgou um trabalho sobre distribuição de chaves públicas, o que fez com que Whitfield Diffie e Martin Hellman criassem, em 1976, um sistema de troca de chaves, o Diffie-Hellman.

Um pouco mais sobre criptografia

- Porém, antes do Diffie-Hellman, ainda na década de 70, os criptógrafos britânicos James H. Ellis, Clifford Cocks e Malcolm J. Williamson conceberam os principais mecanismos da criptografia de chave pública, que se tornaram públicas após a reclassificação como não confidencial pelo governo britânico em 1997.

Assinatura Digital

- Na criptografia de chave pública, a cifragem é realizada com o uso da chave pública do destinatário, enquanto a decifragem é realizada com o uso da chave privada correspondente.

- Para cada operação de cifragem-decifragem, há o uso de um par de chaves (pública e privada). O processo inverso, em que uma mensagem é “cifrada” com a chave privada, é o mecanismo utilizado para validar a origem de uma mensagem.

- O destinatário recebe a mensagem “cifrada” ou “assinada” pelo detentor da chave privada e utiliza a chave pública correspondente para realizar a validação da assinatura. Caso a validação não seja possível, a mensagem não foi originada no detentor real da chave privada.

Assinatura Digital

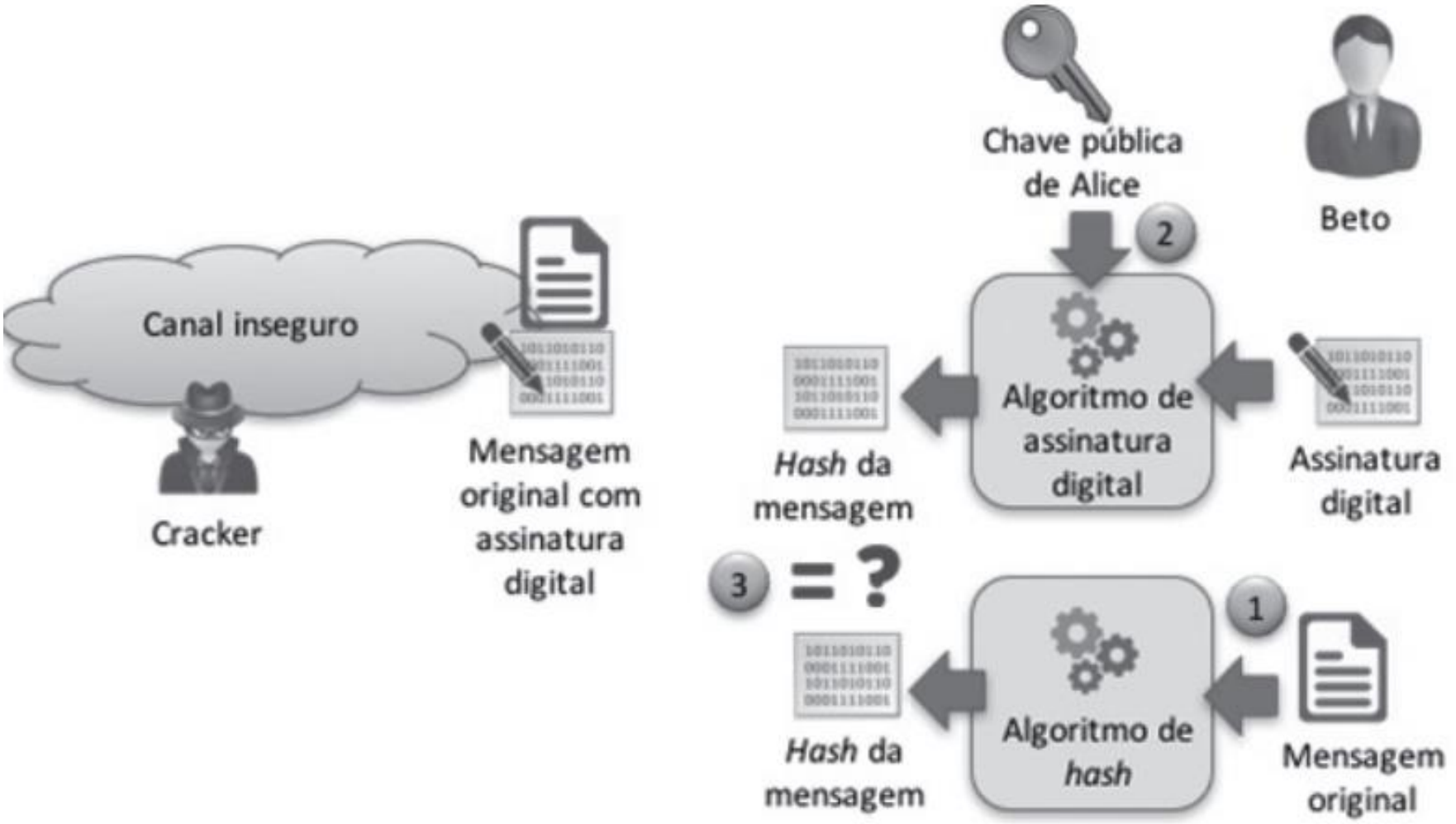
1. Um *hash* da mensagem original é gerado.
2. Alice utiliza a sua chave privada para assinar digitalmente o *hash* da mensagem original.
3. A assinatura digital é enviada para Beto, junto com a mensagem original.

Assinatura Digital

- Alice utiliza sua chave privada para assinar a mensagem. A assinatura é realizada sobre um hash da mensagem, que é o resultado de um cálculo matemático em uma via (não é possível a reversão, ou seja, não é possível chegar à mensagem original a partir de um hash).

- O que é enviado ao destinatário é a mensagem original, juntamente com a assinatura digital, um algoritmo que é aplicado sobre o hash da mensagem original.

Assinatura Digital



Assinatura Digital

- Beto realiza o processo de verificação da assinatura digital, a partir da mensagem original e da assinatura digital recebidas. Beto utiliza a chave pública de Alice sobre a assinatura digital para chegar ao hash, realizando a “decifragem” correspondente ao uso da chave privada por Alice.

- Ao mesmo tempo, Beto gera um hash da mensagem recebida. Caso os dois hashes obtidos sejam iguais, então a mensagem realmente veio de Alice.

RSA

- Os pesquisadores do MIT, Ron Rivest, Adi Shamir e Leonard Adleman, publicaram o algoritmo RSA em 1978, com o uso de exponenciação modular do produto de dois números primos muito grandes para cifragem e decifragem, além da assinatura digital.

- O algoritmo RSA é composto por 3 partes:
  - 1. Geração de chaves pública e privada.
  - 2. Cifragem.
  - 3. Decifragem.

RSA

- De uma forma bastante geral, a geração das chaves pública e privada é feita a partir de dois números primos, que passam por uma série de cálculos até que se chegue às chaves pública e privada.

- A quebra da chave privada, que é utilizada na decifragem, é considerada improvável, já que não há algoritmos eficientes para realizar a operação matemática envolvida, uma fatoração de inteiros em fatores primos, principalmente quando o número de algarismos é 100 ou maior. O tempo de cifragem de uma mensagem é desprezível, porém o tempo de decifragem pode tornar o processo inviável.

Aplicações de Criptografia

- Os diferentes tipos de criptografia, em especial as de chave privada e de chave pública, possibilitam o estabelecimento de um mundo mais seguro com as suas diferentes implementações em variadas aplicações.

- As mensagens instantâneas, como o aplicativo para dispositivos móveis WhatsApp e o Messenger do Facebook, são um tipo de comunicação que aplica a criptografia. Outras comunicações que também aplicam a criptografia são a voz (como o Skype) e os e-mails. Para as empresas, as redes privadas virtuais (VPN, Virtual Private Network) são fundamentais para a comunicação segura.

Aplicações de Criptografia

- No caso do WhatsApp, a criptografia utilizada é ponta a ponta, ou seja, entre os dispositivos que estão trocando as mensagens. Com esse tipo de criptografia, somente quem está conversando possui a chave para ler a mensagem. Tudo é feito de uma forma transparente para o usuário, não sendo possível desabilitá-la.

- O Messenger do Facebook, passou a adotar em julho de 2016 a criptografia ponta a ponta, já utilizada pelo WhatsApp, que também é de propriedade do Facebook. A implementação, porém, é diferente. Enquanto no WhatsApp toda a comunicação é cifrada com a criação de uma camada adicional de criptografia, no Messenger do Facebook a cifragem é feita especificamente em uma conversação, que depende da sessão e do dispositivo que está sendo utilizado para a comunicação.

Aplicações de Criptografia

- O Skype também aplica a criptografia para as comunicações de voz e também para a troca de mensagens, com uso tanto da criptografia de chaves privadas (algoritmo AES de 256 bits) quanto quanto da criptografia de chaves públicas (algoritmo RSA de 1536 ou 2048 bits).

- Já no caso de e-mails, os baseados na nuvem, como o Gmail ou o Yahoo!, a criptografia é aplicada na camada de transporte, normalmente com o uso do protocolo TLS (Transport Layer Security), que é utilizado para proteger o tráfego HTTP (HyperText Transfer Protocol), pelo HTTPS (HyperText Transfer Protocol Secure).

Aplicações de Criptografia

- Outra aplicação importante de criptografia para as comunicações é a rede privada virtual ou VPN (Virtual Private Network). A VPN possibilita, com a aplicação da criptografia, que entidades em uma rede pública ou compartilhada acessem uma rede privada como se estivessem nela.

- A criptografia possibilita o tunelamento das comunicações, por exemplo o uso de protocolos como IPSec ou TLS.

Aplicações de Criptografia – Dados armazenados

- Em sistemas Windows, por exemplo, é possível aplicar a criptografia em arquivos específicos ou em todo o sistema de arquivos com o BitLocker.

- Existem também diversas opções de softwares específicos no mercado.

EXERCÍCIOS ENTREGA ATÉ DIA 03/06

Criar um algoritmo que permita ao usuário escolher entre 2 opções:
1 – Criptografar uma mensagem
2 – Descriptografar uma mensagem

Para criptografar a mensagem utilize o método de César com 3 casas.
A -> D

REFERÊNCIAS

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação: princípios e controle de ameaças**. [S. l.]: ÉRICA, 2014.

FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. [S. l.]: SARAIVA, 2007.

SMULDERS, André; BAARS, Hans; HINTZBERGEN, Jule; HINTZBERGEN, Kees. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. [S. l.]: BRASPORT, 2018.

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. [S. l.]: Cengage Learning, 2014.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. [S. l.]: Bookman Editora, 2013.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes**: Princípios e práticas. 6. ed. [S. l.]: Pearson Universidades, 2014.

SINGH, Simon. **O livro dos códigos**: A ciência do sigilo – do antigo Egito à criptografia quântica. [S. l.]: Record, 2001.


Anhanguera