NÃO PODE FALTAR

# CRIPTOGRAFIA

Emilio Tissato Nakamura

## HISTÓRIA DA CRIPTOGRAFIA

Conhecer a história da criptografia, sua constante evolução e as nuances que existem nos algoritmos vai ajudá-lo na definição de controles de segurança para a proteção da informação, incluindo dados pessoais.

Fonte: Shutterstock.

**Deseja ouvir este material?**

Áudio disponível no material digital.

## PRATICAR PARA APRENDER

Nesta seção, vamos entrar no mundo da criptografia, um assunto que faz mais parte da sua vida do que você imagina. As informações de seu dispositivo móvel estão protegidas por criptografia, bem como as do seu notebook. Sua comunicação com familiares e amigos também está protegida com a criptografia, de modo que as escutas não levarão ao conteúdo.

Aliás, você sabia que a criptografia não visa esconder a mensagem ou a informação, mas, sim, torná-la sem valor, mesmo sendo interceptada? Mas há uma tecnologia que visa esconder a mensagem ou a informação: a **esteganografia**. Com ela, você pode estar olhando para uma foto, mas ela pode trazer informações codificadas escondidas.

Há diferentes tipos de criptografia. Se no início a criptografia foi criada para proteger as mensagens, a evolução levou a novas possibilidades, como a de verificar a integridade da informação ou a de garantir a autenticidade da origem. Com isso, você deve pensar na criptografia como um conjunto de controles de segurança que vai além da proteção da confidencialidade. E a evolução da criptografia levou às criptomoedas e continua evoluindo. Pense na computação quântica. O que será da criptografia com o poder computacional que facilita ataques de força bruta? Há estudos em criptografia pós-quântica que visam proteger a informação no mundo da computação quântica. Assim, a evolução continua incluindo ainda a computação leve, destinada a dispositivos de Internet das Coisas, ou *Internet of Things* (IoT), que apresentam limitações que comprometem o uso da criptografia.

Você é o responsável pela segurança da informação de uma empresa do setor químico, a qual conta com os maiores cientistas brasileiros. A empresa tem unidades em São Paulo, Rio de Janeiro e Salvador. Além disso, tem cooperação internacional com uma empresa chinesa e outra suíça. A empresa tem grandes investidores financiando seus projetos.

A sua atividade será focada em um grande projeto em andamento que já chegou a grandes resultados, com os cientistas tendo descoberto um novo composto que será utilizado na indústria agrícola. Você está preocupado com a forma como os resultados do desenvolvimento estão sendo protegidos. O impacto pode ser gigantesco em caso de incidentes de segurança, principalmente com a concorrência também mobilizando grandes equipes para colocar no mercado os avanços para o setor.

Prepare uma **apresentação** para a diretoria executiva da empresa com uma **estratégia de segurança** que considera as seguintes situações:

- A documentação com os resultados do projeto é armazenada no servidor de arquivos, que está na nuvem.
- O desenvolvimento do projeto é colaborativo, na própria nuvem, entre brasileiros, chineses e suíços.
- Alguns cientistas gravam o documento em seus equipamentos para trabalharem no fim de semana na fazenda, onde há limitações de conectividade.
- Outros cientistas gravam os documentos em *pendrives* para *backup*.
- Quando um cientista vai de Salvador para Pequim, ele leva a documentação em seu *notebook* e também em um *pendrive*.
- Resultados intermediários são discutidos entre São Paulo, Rio de Janeiro e Salvador, e, às vezes, com os parceiros chineses e suíços, com troca de documentos anexados em e-mails e uso de serviço de troca de arquivos como o *Dropbox*.

Na apresentação, faça uma **correlação dos controles de segurança propostos com a ameaça correspondente**, como o vazamento do projeto, a invasão seguida de alteração dos resultados e a inserção de documentos fraudulentos nos arquivos do projeto.

Não esqueça de inserir em sua apresentação uma explicação breve para a diretoria executiva sobre os **algoritmos criptográficos propostos para cada caso**.

Conhecer a história da criptografia, a sua constante evolução e as nuances que existem nos algoritmos vai ajudá-lo na definição de controles de segurança para a proteção da informação, incluindo dados pessoais. Como profissional de segurança, é preciso conhecer e entender as possibilidades da criptografia para que a sua estratégia de segurança tenha ainda mais sucesso.

Ver anotações

CONCEITO-CHAVE

Em 2016, o *Federal Bureal of Investigation* (FBI) dos Estados Unidos tentou de tudo, sem sucesso, para ter acesso às informações de um dispositivo móvel do principal suspeito de um tiroteio que vitimou 14 pessoas em dezembro de 2015 em San Bernardino (KAHNEY, 2019). Esta história mostra o poder de um dos principais controles de segurança: a criptografia. Este caso ilustra também que a segurança em camadas é fundamental, já que a criptografia foi utilizada em conjunto com outros controles de segurança, como a autenticação, para proteger os dados do legítimo dono.

Da origem para ocultar o significado de uma mensagem até o uso em aplicações como *WhatsApp* e acesso a *websites*, passando pelo uso em guerras e por agentes secretos, a criptografia evoluiu de uma arte para uma ciência e, atualmente, faz parte de nossas vidas, incluindo os objetivos de autenticação de mensagens, assinatura digital, protocolos para troca de chaves secretas, protocolos de autenticação, leilões e eleições eletrônicas, além de dinheiro digital (NAKAMURA, 2016).

> **REFLITA**
>
> A criptografia surgiu para proteger as mensagens há séculos, envolvendo histórias de amor, guerras e traições. Atualmente ela é considerada um controle de segurança da informação, junto de uma série de outros controles que surgiram no mundo digital. Será que existe um controle de segurança tão amplo no seu uso, tão antigo e que seja de conhecimento da grande maioria das pessoas?

## CONCEITOS DE CRIPTOGRAFIA

A criptografia deriva de duas palavras gregas: *kryptos*, que significa oculto, e *graphien*, que significa escrever. O Dicionário Oxford define criptografia como a arte de escrever ou resolver códigos. Estas definições podem ser consideradas um reflexo do seu objetivo original, que era ocultar o significado das mensagens. Note que o objetivo não é esconder a existência da mensagem, de modo que ela pode cair nas mãos de um intruso, mas fazer com que essa pessoa não consiga compreendê-la. Com a criptografia, apenas o remetente e o destinatário, em princípio, com um acordo preestabelecido (as chaves), têm acesso ao significado da mensagem (NAKAMURA, 2016).

> **ASSIMILE**
>
> O termo criptografia é usado muitas vezes como sinônimo de criptologia, abrangendo assim a criptanálise, que tem por função descobrir os segredos, ou quebrar a confidencialidade entre emissor e receptor (FIARRESGA, 2010).

Com o advento científico, em especial da matemática, a criptografia também evoluiu. Uma definição mais recente do termo se refere ao estudo de técnicas matemáticas relacionadas a aspectos da segurança da informação, tais como confidencialidade, integridade, autenticação de entidade e autenticação de origem de dados (MENEZES; OORSCHOT; VANSTONE 2001). As aplicações atuais da criptografia incluem os seguintes objetivos (KATZ; LINDELL, 2007; FIARRESGA, 2010):

- **Sigilo:** proteção dos dados contra divulgação não autorizada.
- **Autenticação:** garantia que a entidade se comunicando é aquela que ela afirma ser.
- **Integridade:** garantia que os dados recebidos estão exatamente como foram enviados por uma entidade autorizada.
- **Não repúdio:** garantia que não se pode negar a autoria de uma mensagem.

- **Anonimato:** garantia de não rastreabilidade de origem de uma mensagem.

> **REFLITA**
>
> A criptografia é apresentada em cursos de segurança da informação, de ciência da computação, mas também de matemática. Você sabia que os grandes inventores dos algoritmos criptográficos são matemáticos? E que a matemática possibilita a proteção da confidencialidade, além de permitir que você autentique entidades, verifique se uma informação foi modificada, garanta que quem enviou uma mensagem só pode ser a própria pessoa e ainda possibilita o anonimato? Sobre esse último ponto, veja o *bitcoin*, que utiliza vários conceitos criptográficos para transações anônimas.

## CRIPTOGRAFIA AO LONGO DA HISTÓRIA

A criptografia é um dos principais controles de segurança da informação e tem uma história fascinante, que envolve o seu uso inicial por governos, militares e acadêmicos. Esta história tem início no Egito, em 1900 a.C., com o uso de hieróglifos, os quais têm origem grega e significado de inscrição sagrada. Um dos modelos de hieróglifos eram estruturados na forma de pictogramas, que consiste em um conjunto de imagens de objetos, pessoas ou animais que funcionavam como uma palavra. A Figura 1.10 ilustra um exemplo de hieróglifos egípcios.

Figura 1.10 | Hieróglifos egípcios

Fonte: Pixabay.

## CIFRA DE CÉSAR

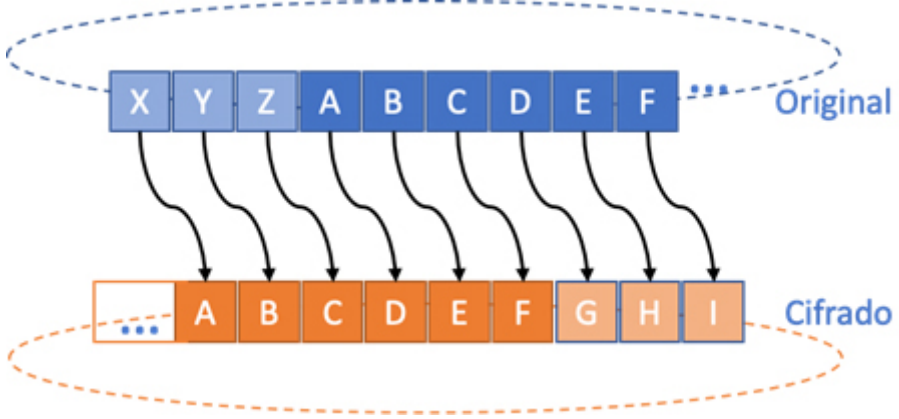
Entre 600 a.C. e 500 a.C. surgiu a Cifra de César criada por Júlio César. Ela consiste na substituição simples de letras do alfabeto por letras avançando algumas letras na sequência, e uso de 25 combinações possíveis com o objetivo de parecer sem significado ao ser interceptada. Essa sigla foi utilizada por vários militares ao longo dos anos.

Vamos exemplificar a Cifra de César: imagine que você deseja enviar a mensagem “INTERNET” com uma chave 3, e para isso foi gerada uma mensagem cifrada “L Q W H U Q H W”.

Para decifrarmos a mensagem e chegarmos à mensagem original, fazemos o processo inverso, retornando 3 letras. Assim, “L” se torna “I”, “Q” se torna “N”, “W” se torna “T, e assim por diante, formando a mensagem original “I N T E R N E T”.

Observe a Figura 1.11 com as possíveis substituições para o alfabeto considerando chave 3.

Figura 1.11 | Cifra de César e as substituições feitas com uma chave 3




Fonte: elaborada pelo autor.

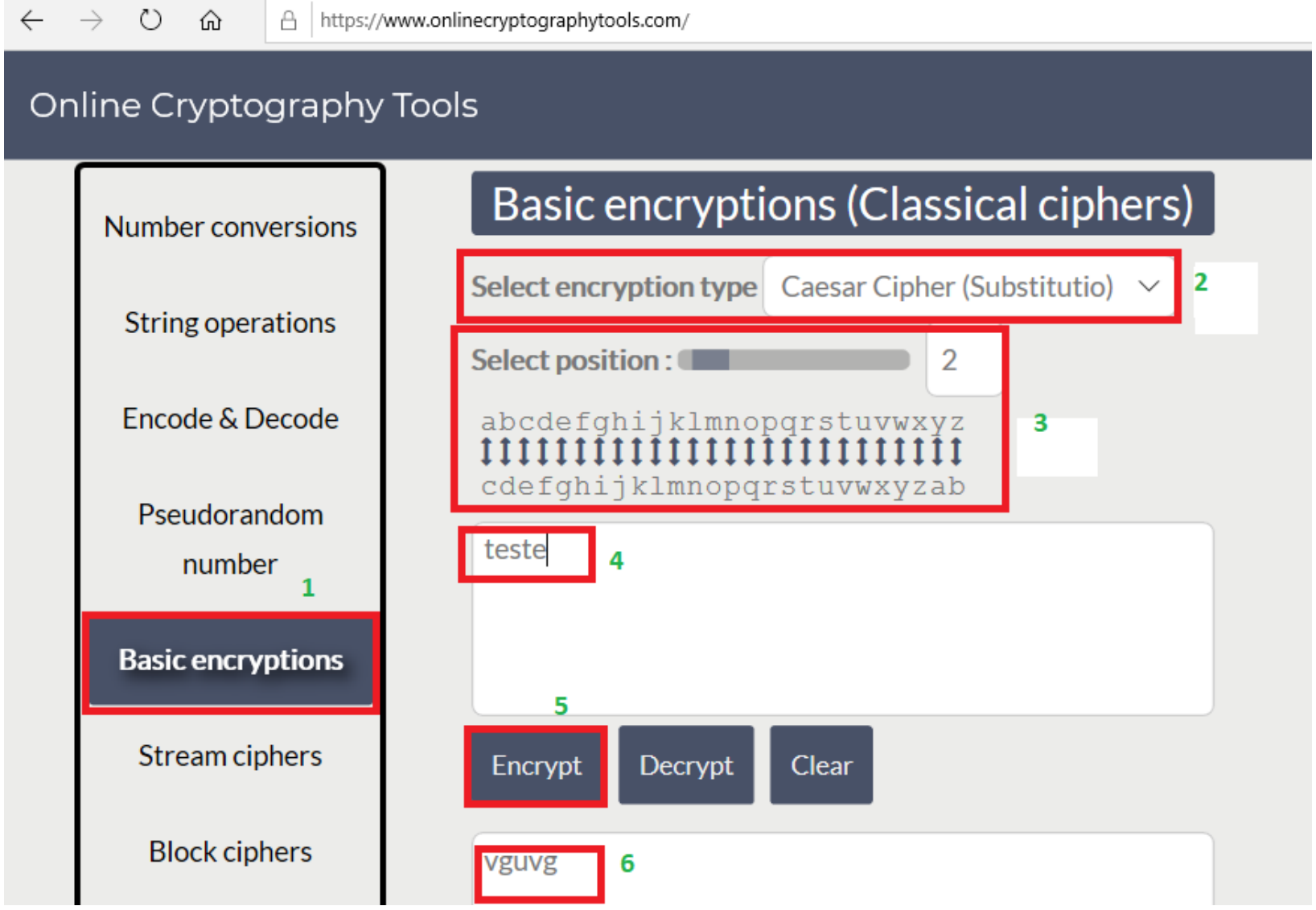
**PESQUISE MAIS**

Você pode testar alguns algoritmos de criptografia em uma ferramenta online chamada **Online Cryptography Tools**, disponível em: https://www.onlinecryptographytools.com. Acesso em: 2 nov. 2020.

Essa ferramenta contém exemplos de cifras simples, como a cifra de César, a criptografia de chave simétrica e *hash*.

A ferramenta contém exemplos decifras simples, como a cifra de César, a criptografia de chave simétrica e *hash*. Observe a Figura 1.12, em que temos um exemplo de aplicação da Cifra de César. Vamos utilizar como senha a palavra “teste” e substituir cada letra da palavra avançando duas letras no alfabeto. Por exemplo, a letra “t” vamos substituir por “v”, a letra “e” será alterada para letra “g” e a letra “s” pela letra “u”. Para testar o exemplo, siga os passos enumerados na imagem:

Figura 1.12 | Cifra de César e as substituições feitas com uma chave 3 na palavra teste




Fonte: elaborada pelo autor.

**Passo 1:** Ao acessar o site, vá em Basic encryptions.

**Passo 2:** Em “Select encryption type”, selecione a Caesar Cipher (Cifra de César).

**Passo 3:** Em “Select Position”, selecione o número de posições que será avançado no alfabeto para a substituição das letras. No caso, foi selecionado 2. Observe que a letra “a” será trocada por “c”, “b” por “d”, conforme podemos visualizar no passo 3.

**Passo 4:** Incluímos a palavra “teste”.

**Passo 5:** Ao clicar em “Encrypt”, a palavra será criptografada.

**Passo 6:** É gerada a palavra correspondente “vguvg”.

Teste outros exemplos e selecione mais posições a serem avançadas no alfabeto.

A partir daí, a criptografia continua evoluindo, como mostra o advento da criptografia pós-quântica e das criptomoedas e *blockchain* hoje (MARTIN, 2019; PRADO, 2017).

Desde 2015, um padrão para a criptografia pós-quântica tem sido estudado. O objetivo é proteger as informações quando o ataque teórico ao RSA se tornar prática com a computação quântica. A criptografia quântica é diferente da criptografia pós-quântica e é também conhecida como comunicação quântica ou segurança quântica. Ela provê uma solução teórica para a distribuição de chaves, com a *Quantum Key Distribution* (QKD) (RICE, 2020).



## CRIPTOGRAFIA E SUAS TÉCNICAS

### ESTEGANOGRAFIA

A esteganografia tem origem nos termos gregos *steganos*, que significa "coberta, escondida ou protegida", com *graphein*, que significa "escrita". É o uso de técnicas para ocultar informações ou mensagens dentro de outra fonte (mensagem). A diferença entre a criptografia e esteganografia é que a criptografia oculta o significado da mensagem, enquanto a esteganografia oculta a existência da mensagem (SIMON, 1999). Além disso, os esquemas de codificação da esteganografia dependem de segredos como dicionários que decodificam as informações. E, uma vez revelado o dicionário, o sistema de codificação é permanentemente comprometido. Com isso, o risco de exposição aumenta conforme aumenta o número de usuários que conhecem o segredo.

> **EXEMPLIFICANDO**
>
> Você pode testar a esteganografia com a ferramenta **Steghide**, disponível em: https://steghide.sourceforge.net. Acesso em: 2 nov. 2020. A ferramenta possibilita a inserção de dados em arquivos de imagem e de áudio.
>
> Outra ferramenta é a **OpenPuff**, disponível em: https://bit.ly/2MTGMy1. Acesso em: 13 nov. 2020.

De acordo com Nakamura (2016), 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 (Figura 1.13).
- Inserção de mensagens em seções de arquivos.
- Uso de caracteres Unicode que se parecem com conjunto de caracteres ASCII padrão.

Figura 1.13 | Exemplo de esteganografia


Fonte: adaptado de Ward (2010).

**REFLITA**

Você sabia que vários hackers estão utilizando a técnica de esteganografia para esconder códigos maliciosos, como vírus em arquivos de imagens e áudios? Muitos desses arquivos são os famosos "memes". Portanto, fique atento ao receber uma imagem. Existem vários casos da inclusão de códigos maliciosos em imagens e áudios. Mas como se proteger desse tipo de ameaça?

## CRIPTOGRAFIA DE CHAVE PRIVADA OU SIMÉTRICA

A função mais conhecida da criptografia é proteger a confidencialidade ou o sigilo da informação, fazendo com que a informação chegue ao seu destino sem que qualquer pessoa não autorizada tenha acesso ao seu conteúdo. Nakamura (2016) apresenta o exemplo de Alice e Beto, que

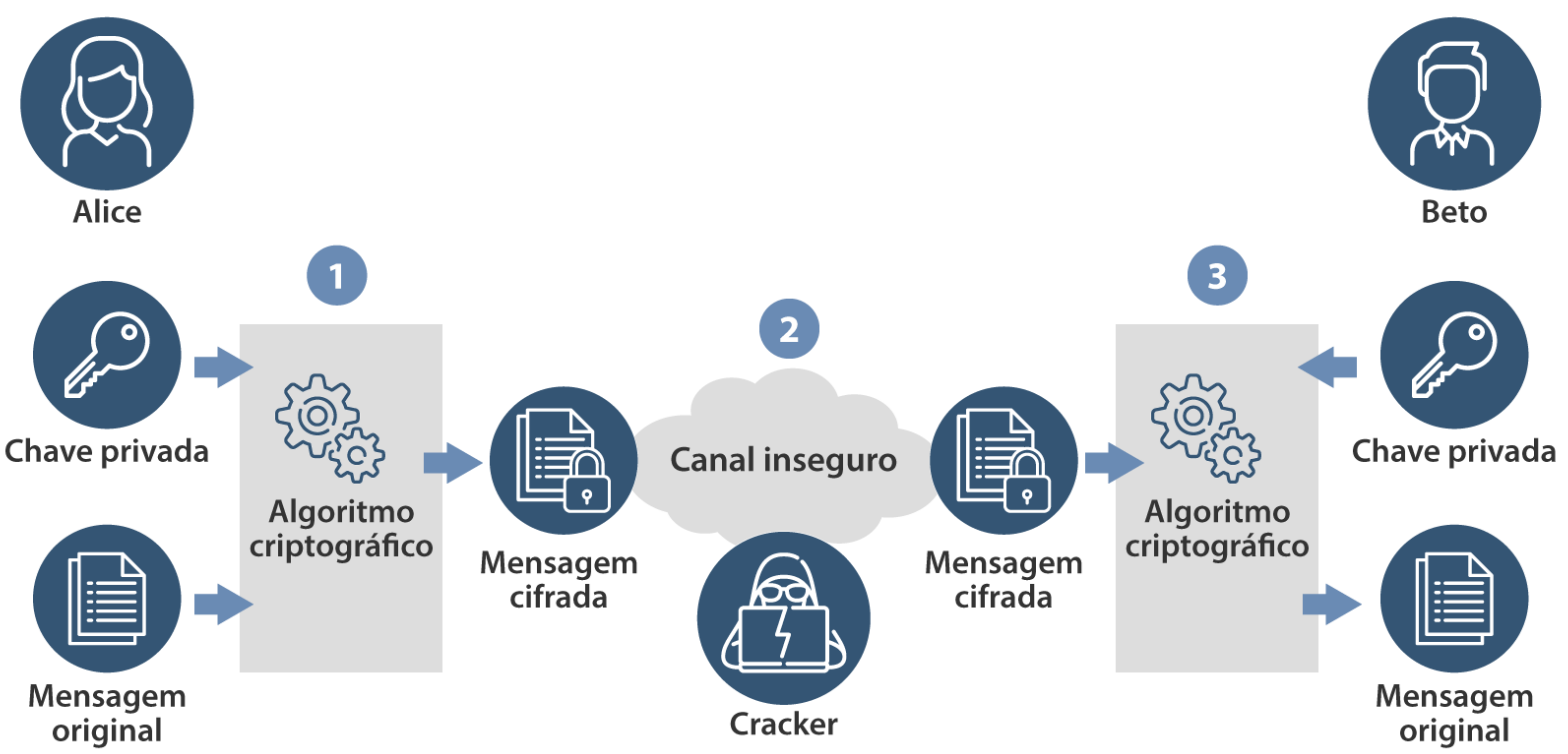
trocam mensagens por um canal, normalmente inseguro, tornando possível que um atacante escute a mensagem, afetando assim a privacidade e a confidencialidade da comunicação.



> **REFLITA**
>
> Na criptografia de chave privada ou simétrica, a chave criptográfica é a mesma para cifrar e decifrar a informação. Ela também precisa ser compartilhada entre o remente e o destinatário. Como você faz para trocar esta chave privada com o seu interlocutor? Você utiliza o mesmo canal inseguro pelo qual vai enviar a mensagem cifrada ou usa um canal alternativo?

A Figura 1.14 mostra a comunicação entre Alice e Beto com o uso da criptografia. 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) ou simétrica para decifrar a mensagem e retornar ao conteúdo original.

Figura 1.14 | Alice e Beto utilizam criptografia para a troca de mensagem



Fonte: Nakamura (2016).

---

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.

---

Ver anotações 0

Estes algoritmos podem ser baseados em cifras de fluxo, em que a cifragem é feita a cada dígito (byte), ou em cifras de blocos, em que um conjunto de *bits* da mensagem é agrupado em blocos, que então são cifrados (NAKAMURA, 2016).

**EXEMPLIFICANDO**

O algoritmo padrão de criptografia de chave privada ou simétrica é o *Advanced Encryption Standard* (AES), também conhecido por Rijndael, que é uma cifra e blocos de 128 bits. O AES substituiu o *Data Encryption Standard* (DES), que teve sua efetividade invalidada em 1997, quando uma mensagem cifrada com o algoritmo foi quebrada pela primeira vez. Em 1998, um equipamento com custo de US$ 250 mil quebrou uma chave de 56 bits em aproximadamente 2 dias, mostrando a redução dos custos de equipamentos para os ataques de força bruta, assim como do tempo para a quebra (NOMIYA, 2010).

*KEY ESCROW*

O acesso a informações protegidas por criptografia é uma discussão grande, que reflete em aspectos de privacidade e de segurança nacional. Apesar de polêmica, há mecanismos para que o acesso seja possível. Um desses mecanismos é a **custódia de chaves ou caução de chaves**, ou *key escrow*, que faz com que cópias de chaves criptográficas existam para o acesso a informações cifradas no caso de ordens judiciais, por exemplo. Com este mecanismo, o sistema criptográfico cria

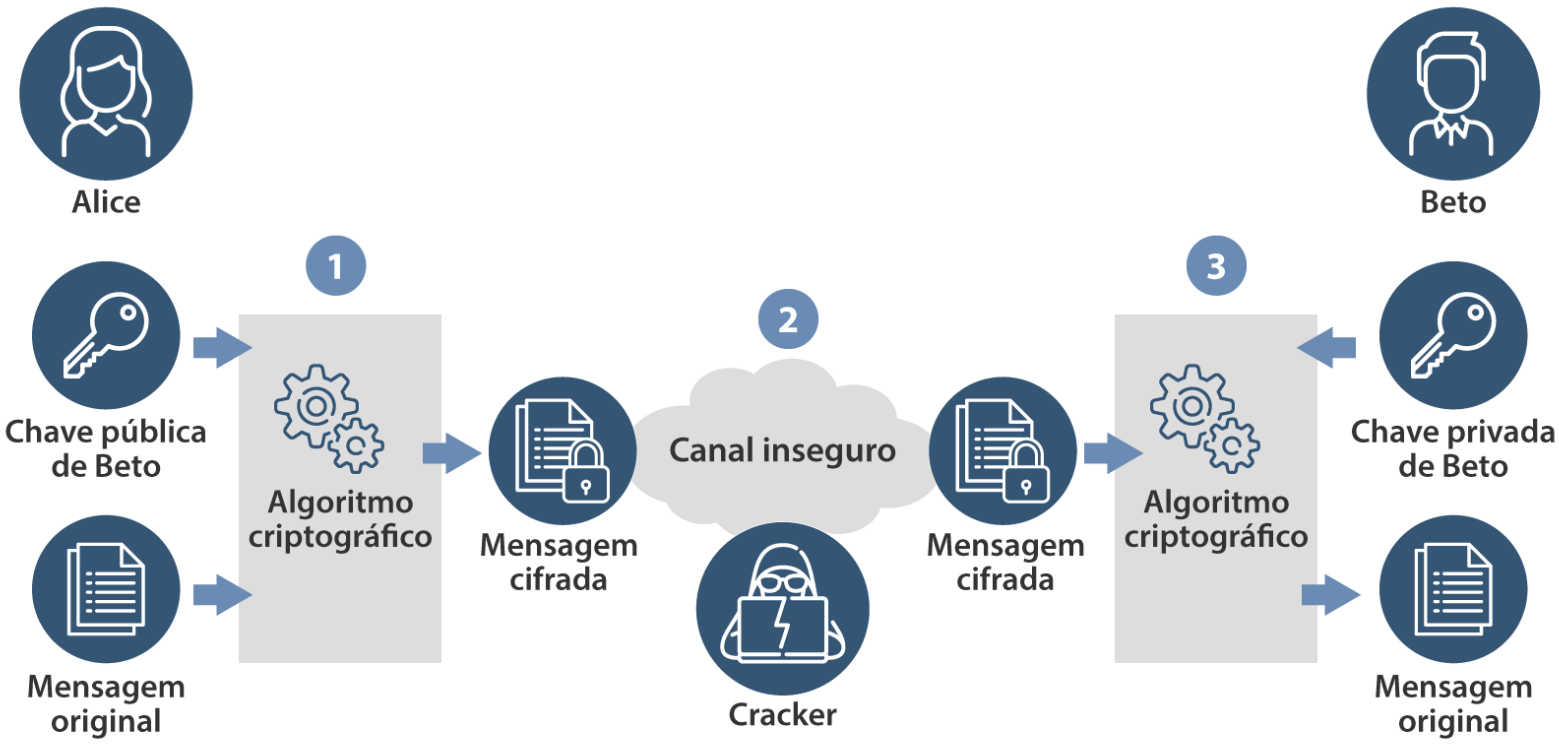
múltiplas chaves que dão acesso às informações. A justiça, neste caso, seria um custo diante de uma das múltiplas chaves, e teria uma cópia das chaves para acessar as informações em caso de necessidade (NAKAMURA, 2016).

## CRIPTOGRAFIA DE CHAVE PÚBLICA OU ASSIMÉTRICA

Uma característica que você precisa saber sobre a criptografia de chave privada ou simétrica é que ela apresenta o desafio da troca de chaves (GOYA, 2006; NAKAMURA; GEUS, 2007), porém é rápida de ser executada, em termos de processamento computacional. Já a criptografia de chave pública ou assimétrica é computacionalmente mais pesada, porém é adequada para ser utilizada na troca de chaves.

A criptografia de chave pública ou assimétrica utiliza um par de chaves (pública e privada) que são utilizado em conjunto para a cifragem (com a chave pública) e decifragem (com a chave privada). Na Figura 1.15, Alice cifra a mensagem utilizando a chave pública de Beto, que pode ser compartilhada. Para abrir a mensagem, somente a chave equivalente é utilizada, que é a chave privada de Beto, que não é compartilhada e fica sempre de posse do dono.

Figura 1.15 | Alice e Beto utilizam criptografia de chave pública para a troca de mensagem




Fonte: Nakamura (2016).

**EXEMPLIFICANDO**

O RSA, publicado em 1978 por Ron Rivest, Adi Shamir e Leonard Adleman, é composto pela geração de chaves pública e privada, cifragem e decifragem. O algoritmo faz uso da exponenciação modular do produto de dois números primos muito grandes, para cifragem e decifragem, além da assinatura digital. 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, que no caso é a 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 (SILVA, 2006).

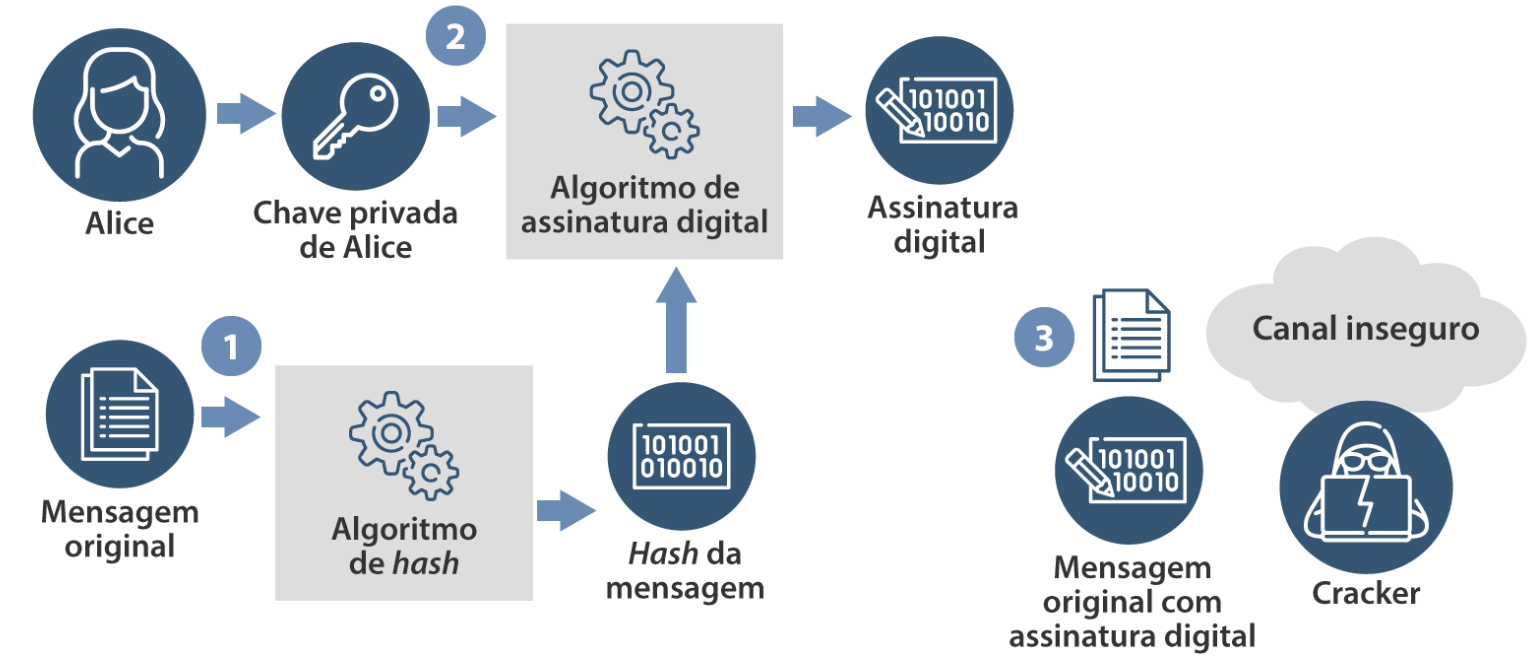
## ASSINATURA DIGITAL

O par de chaves pública e privada de cada entidade é utilizado na criptografia de chave pública ou assimétrica. Para cifrar uma mensagem, é utilizada a chave pública do destinatário, enquanto a decifragem é

realizada com o uso da chave privada correspondente. Além da cifragem, a criptografia de chave pública pode ser utilizada para validar a origem de uma mensagem.

A Figura 1.16 ilustra Alice assinando digitalmente uma mensagem. Neste processo, Alice utiliza sua chave privada para "cifrar" o *hash* da mensagem. O *hash* é o resultado de um cálculo matemático em uma via, ou seja, não é possível a sua reversão, ou seja, não é possível chegar à mensagem original a partir de um *hash*.

Figura 1.16 | Alice assina digitalmente uma mensagem




Fonte: Nakamura (2016).

**EXEMPLIFICANDO**

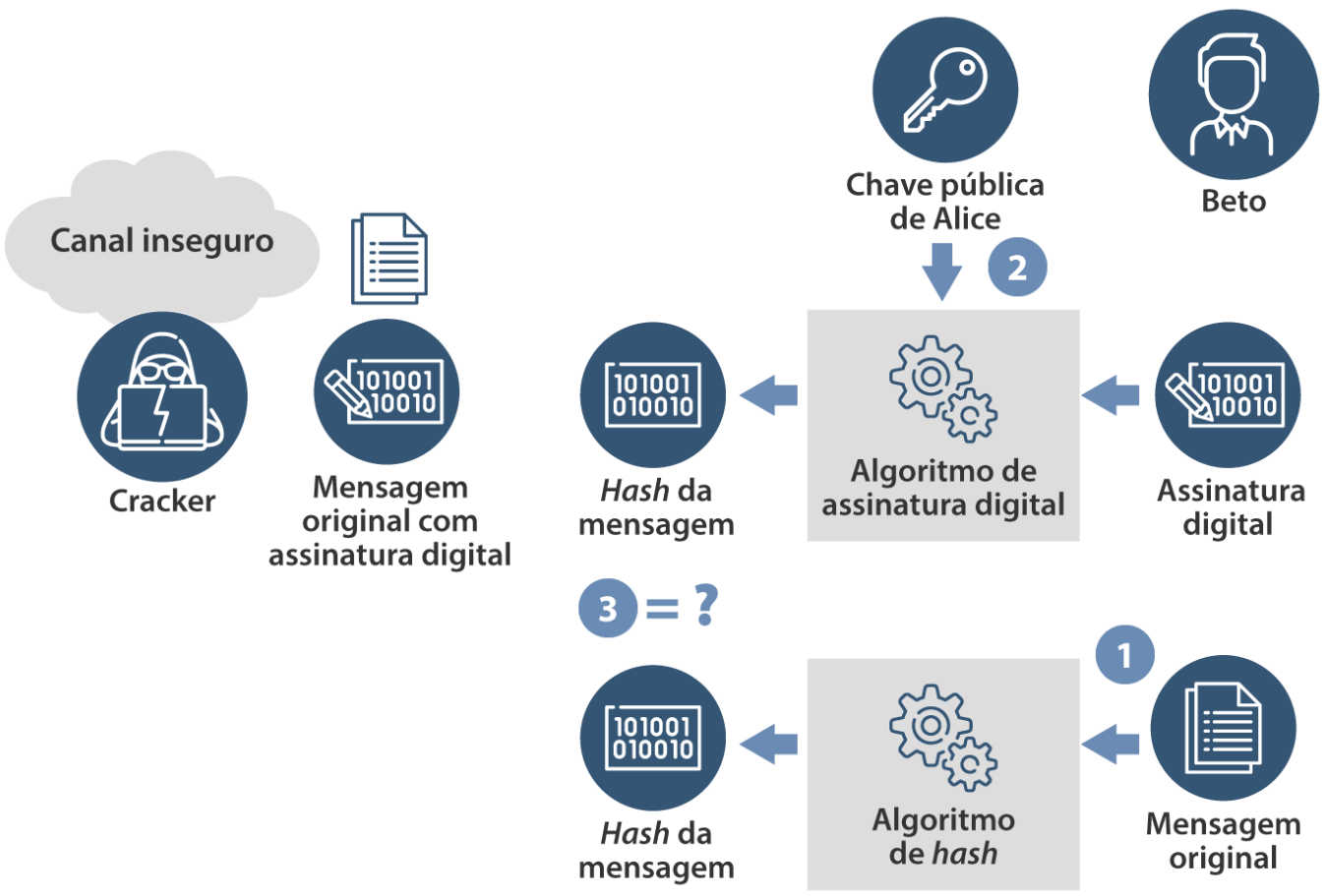
Funções de *hash* são utilizadas para a verificação da integridade. Estes algoritmos realizam um cálculo matemático nas mensagens ou nos documentos. O receptor recebe a mensagem juntamente com o *hash* e utiliza o mesmo algoritmo para calcular o *hash* da mensagem recebida. O *hash* recebido e o *hash* calculado devem ser comparados, e devem ser iguais, o que garante a integridade da mensagem ou do documento. Alguns exemplos de funções de *hash* são o MD5 e a família SHA (SHA-1, SHA-256 e

SHA-512). É importante ressaltar que o MD5 e o SHA-1 não devem mais ser utilizados na prática, pois são suscetíveis a ataques de colisão. Neste ataque, mensagens diferentes podem gerar o mesmo *hash*, impossibilitando a validação da integridade.

Ver anotações

Beto recebe e "decifra" o *hash* da mensagem utilizando a chave pública correspondente, de Alice. Na Figura 1.17, Beto ainda calcula o *hash* da mensagem, o compara com o *hash* decifrado vindo de Alice. Os dois *hashes* devem ser idênticos, o que comprova que foi mesmo Alice quem assinou digitalmente a mensagem, já que somente ela possui a chave privada.

Figura 1.17 | Beto verifica a assinatura digital de Alice




Fonte: Nakamura (2016).

**REFLITA**

E se algum impostor se passar por Alice, divulgando uma chave pública como se fosse ela? Este é o cenário para o certificado digital e a autoridade certificadora, que têm a

função de publicar os certificados digitais, que são as chaves públicas com alguns atributos adicionais. Além disso, a autoridade certificadora valida os certificados digitais, estabelecendo uma relação de confiança.

## TROCA DE CHAVES CRIPTOGRÁFICAS

Você já viu que a criptografia de chave privada é rápida, mas há o desafio da troca de chaves. E a criptografia de chave pública é mais lenta, com a vantagem de não ser preciso trocar chaves. Desta forma, usar criptografia de chave pública em toda comunicação pode não ser muito eficiente. Então, por que não utilizar a criptografia de chave pública para a troca da chave privada da criptografia simétrica, que seria utilizada na comunicação?

---

Além do desafio da troca de chaves, é fundamental o seu gerenciamento, envolvendo parâmetros como o tempo de validade, armazenamento, geração, uso e substituição. O uso em conjunto da criptografia de chave pública e a de chave privada é tradicionalmente utilizado para a criação de um canal seguro, que por sua vez pode ser utilizado para a troca de chaves privadas.

---

Um exemplo é o *Secure Sockets Layer* (SSL), utilizado para proteger comunicações *Web*, que implementa em conjunto mecanismos de gerenciamento de chaves criptográficas.

Outro exemplo é o Diffie-Hellman, criado em 1976 por Whitfield Diffie e Martin Hellman e utilizado até hoje. Ele foi o primeiro método criptográfico para troca de chaves, que permite que duas entidades que não possuem conhecimento prévio uma da outra possam compartilhar uma chave secreta mesmo com o uso de um canal inseguro. Matematicamente, o Diffie-Hellman utiliza o cálculo de logaritmos discretos em um campo infinito para gerar e estabelecer uma chave secreta compartilhada, a partir de uma informação prévia comum que

não é crítica no caso de ser comprometida. Assim, com o Diffie-Hellman, uma chave secreta compartilhada é gerada pelas entidades, sem que sejam transmitidas em um canal de comunicação (NAKAMURA, 2016).

## SEGURANÇA DOS SISTEMAS CRIPTOGRÁFICOS

Você sabia que a segurança de um sistema criptográfico está no tamanho das chaves, e não no algoritmo criptográfico? Os algoritmos criptográficos mais utilizados são públicos, tendo sido avaliados por toda a comunidade científica. Porém, a segurança não pode ser medida somente pelo tamanho da chave utilizada, sendo necessário conhecer o algoritmo e a matemática envolvida no processo de codificação de dados.

Um atacante pode fazer o ataque explorando o algoritmo ou tentando descobrir a chave secreta. Deste modo, um algoritmo que utiliza chaves de 256 bits não significa que seja necessariamente mais seguro do que outros algoritmos, como o DES de 128 bits, caso existam falhas no algoritmo ou em sua implementação. A segurança de sistemas criptográficos depende de uma série de fatores, tais como (NAKAMURA; GEUS, 2007):

- **Geração de chaves:** sem uma geração aleatória de chaves, o algoritmo utilizado pode revelar padrões que diminuem o espaço de escolha das chaves, o que facilita a sua descoberta.
- **Mecanismo de troca de chaves:** as chaves precisam ser distribuídas e trocadas para o estabelecimento das comunicações seguras, e, para tanto, protocolos como o Diffie-Hellman são utilizados.
- **Taxa de troca das chaves:** quanto maior a frequência de troca automática das chaves, maior será a segurança, pois isso diminui a janela de oportunidade de ataques, pois, caso uma chave seja quebrada, em pouco tempo ela já não é mais útil para a comunicação.

- **Tamanho da chave:** são diferentes para a criptografia de chave privada ou simétrica e para a criptografia de chaves públicas ou assimétricas.

> **SAIBA MAIS**
>
> Sistemas criptográficos já apresentaram problemas de segurança, o que demonstra que a criptografia deve ser considerada uma das camadas de segurança. Um dos problemas mais conhecidos foi o do algoritmo de chave privada RC4, que foi o pivô de problemas no WEP (*Wired Equivant Privacy*), protocolo de segurança utilizado em redes Wi-Fi, em 2001. Atualmente o WEP não pode ser utilizado devido a este problema com o RC4. Nos últimos anos, o protocolo SSL foi alvo de diferentes ataques, o que culminou na recomendação pela não utilização do SSL e na expansão do uso da nova versão do TLS. Alguns ataques relacionados são o ataque de renegociação do protocolo (2009), BEAST (2011), CRIME, BREACH, Truncation (2013), Heartbleed, BERserk, Cloudfare, FREAK, PODDLE (2014), Logjam (2015), DROWN, Unholy PAC (2016).

## APLICAÇÕES DE CRIPTOGRAFIA

A criptografia de chave privada e a criptografia de chave pública têm uma série cada vez maior de aplicações. Algumas delas são:

- **Proteção da comunicação:** autenticação de entidades, integridade e confidencialidade em mensagens pessoais como os do aplicativo *WhatsApp*, em comunicação de voz como o do *Skype*, em e-mails com o uso de sistemas como o *Pretty Good Privacy* (PGP), ou em acesso remoto por *Virtual Private Network* (VPN).
- **Proteção de dados armazenados:** confidencialidade de dados em dispositivos móveis, em notebooks e desktops diretamente pelo sistema operacional ou por sistema específico, ou na nuvem.

- **Proteção de transações:** autenticação de entidades, integridade e confidencialidade no uso de cartões, em transações bancárias, em compras online.

Um dos principais protocolos de segurança para transações é o *Hyper Text Transfer Protocol Secure* (HTTPS), que é um *Uniform Resource Identifier* (URI) para o uso do *Hyper Text Transfer Protocol* (HTTP) sobre uma sessão *Secured Socket Layer* (SSL) ou *Transport Layer Security* (TLS).

Este conjunto de protocolos é utilizado para transações Web com a criação de um túnel seguro por onde trafegam as informações. Além de garantir a **confidencialidade** (dados cifrados com chave simétrica de sessão), eles podem visar também a **integridade dos dados** (uso de *Message Authentication Code*, MAC) e a **autenticidade das partes** (as entidades podem ser autenticadas com o uso de criptografia de chave pública).

De forma geral, o SSL evoluiu para o TLS, de modo que o SSL 3.1 é o TLS 1.0. Já o HTTPS é o HTTP dentro do SSL/TLS. O túnel bidirecional do HTTP é criado entre duas entidades, e quando este túnel é seguro por uma conexão SSL/TLS, então o conjunto é conhecido como HTTPS. No HTTPS, a conexão SSL/TLS é estabelecida antes, e os dados HTTP são trocados sobre essa conexão SSL/TLS (NAKAMURA, 2016).

O funcionamento é:

1. Cliente se conecta a um servidor com TLS, requisitando uma conexão segura, apresentando uma lista de algoritmos suportados.
2. O servidor escolhe um algoritmo simétrico e de *hash* que ele também suporta e notifica o cliente.
3. O servidor envia sua identificação como um certificado digital, com nome, autoridade certificadora (CA) e a chave pública.
4. O cliente confirma a validade do certificado antes de prosseguir.

5. Para gerar a chave de sessão, o cliente cifra um número aleatório com a chave pública do servidor e envia o número cifrado para o servidor.

6. Como somente o servidor consegue abrir o número aleatório, os dois podem gerar uma chave de sessão única a partir dele.

7. Diffie-Hellman é utilizado para gerar uma chave de sessão única.

Outra aplicação importante de criptografia para as comunicações é a rede privada virtual ou ***Virtual Private Network*** **(VPN)**. A criptografia possibilita o tunelamento das comunicações, como o uso de protocolos como o IPSec ou TLS, de modo que entidades em uma rede pública ou compartilhada acessem uma rede privada como se estivessem nela. O acesso pode ser individual, como no caso de um acesso remoto, ou pode ser de uma rede para outra (*gateway-to-gateway* VPN) (NAKAMURA; GEUS, 2007).

---

A criptografia tem um papel importante para a proteção de dados armazenados, ainda mais em um mundo em que as informações estão distribuídas em *datacenters* de empresas, dispositivos de usuários e nuvem. São diferentes níveis de proteção, que vão desde a cifragem de dados diretamente no banco de dados até o cifragem de arquivos ou disco rígido de notebooks que utilizam o Windows, com o BitLocker.

---

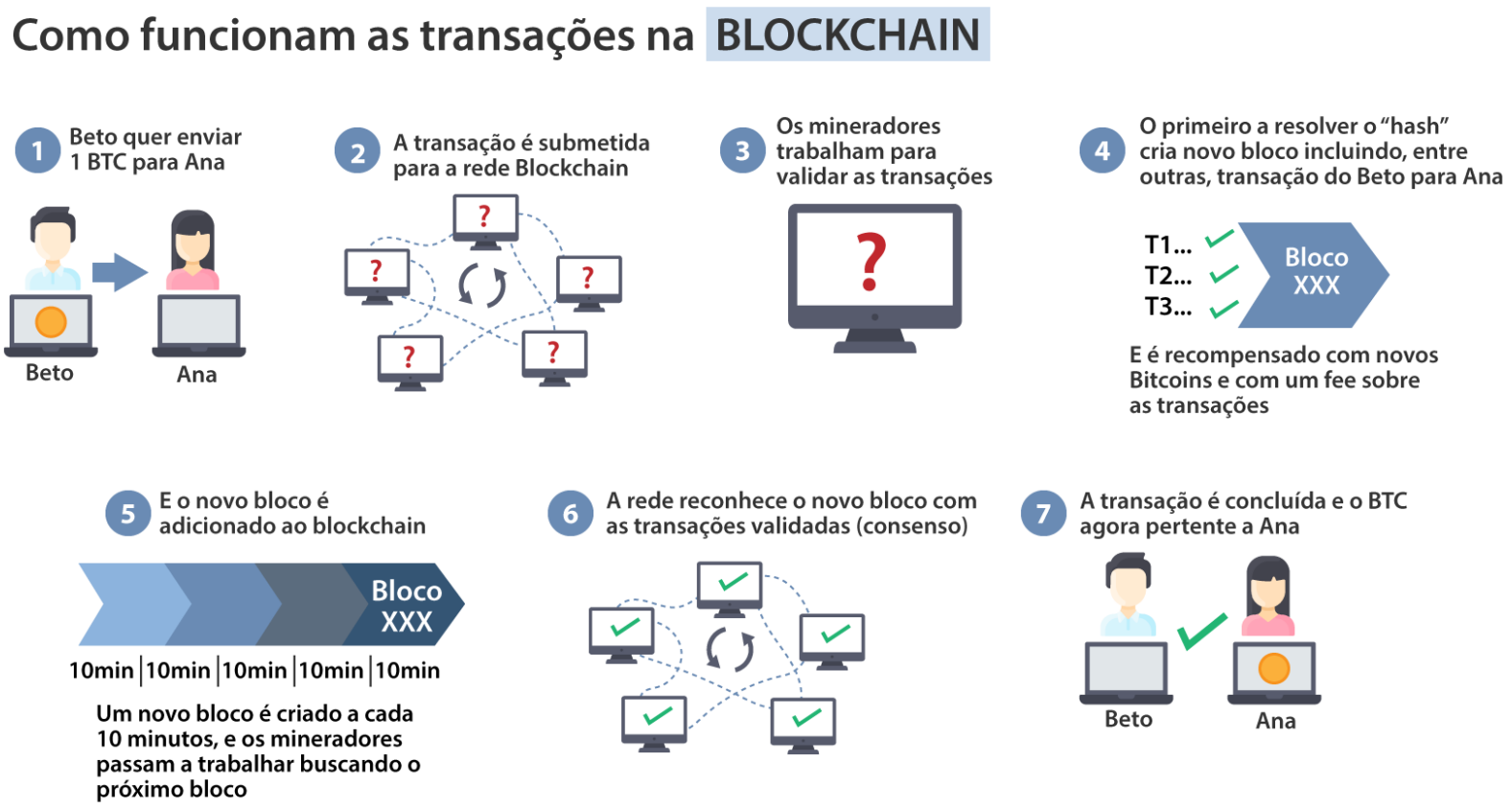
Quando pensamos no nosso cotidiano online, há ainda uma série de aplicações da criptografia. Quando realizamos uma compra pela Internet, por exemplo, temos que ter a tranquilidade de saber que os dados de nosso cartão do banco estão sendo transferidos de forma segura até a loja. Além disso, uma vez que a transferência dos dados de cartão foi feita de forma segura, estes dados devem estar protegidos no banco de dados e no servidor da loja virtual.

Para completar o entendimento de que a criptografia faz parte de nossas vidas, podemos contar com a segurança em nossas comunicações quando utilizamos aplicativos como o *WhatsApp*, *Skype* ou outros similares. Alguns utilizam criptografia fim-a-fim, o que garante que ninguém no meio do caminho tenha acesso ao conteúdo e à troca de chaves, que ocorre de forma transparente para os usuários. Já o dispositivo móvel também já conta com a criptografia dos dados armazenados. Além disso, o acesso Web, tanto de aplicações de redes sociais quanto de negócios, financeiros e de comércio online, conta com o HTTPS, e até mesmo uma camada adicional específica de criptografia em alguns casos. E os dados que partem de nós trafegam pela rede e chegam às empresas são protegidos também por criptografia no armazenamento.

Outra aplicação que utiliza conceitos de criptografia que tem sido muito explorada nos últimos anos é a tecnologia ***blockckain***. *Blockchain* é a tecnologia por trás do *bitcoin* e utiliza, de forma conjunta, uma série de algoritmos computacionais que incluem criptografia e sistemas distribuídos, criando um ambiente de confiança distribuído.

Figura 1.18 ilustra como uma transação é feita usando a *blockchain* (JUNGES, 2018).

Figura 1.18 | Uma transação utilizando *blockchain*




Fonte: adaptada de Junges (2018).

No exemplo, Beto quer enviar 1 BTC, que é a unidade da criptomoeda *bitcoin* para Ana. A carteira digital de Ana é baseada na criptografia de chave pública, e Beto utiliza a chave pública de Ana para realizar a transação. Esta chave pública pode ser representada por meio de um código QR, que indica ainda o endereço *bitcoin* de Ana. Você deve lembrar que somente Ana consegue abrir a sua carteira digital, pois somente ela possui a chave privada correspondente. A transação é enviada para a *blockchain*, que é uma rede distribuída em que os nós tentam validar a transação com a mineração. A mineração, neste exemplo, é a resolução do *hash* envolvido com a transação, que consome muitos recursos computacionais. O primeiro que resolver o desafio do *hash* valida a transação e é recompensado. A transação, assim, passa a fazer parte de um bloco da *blockchain*, e será usada para validar outras transações. E Ana possa a ter o BTC transacionado por Beto e validado pela rede (JUNGES, 2018).



**PESQUISE MAIS**

O livro de Stallings (2015) traz uma série de elementos de criptografia, focando também nas teorias matemáticas e nos cálculos realizados (STALLINGS, 2015). Na parte 1 do livro são tratadas as cifras simétricas, com técnicas clássicas de encriptação, cifras de bloco e DES, conceitos básicos de teoria dos números e corpos finitos, AES, operação de cifra de blocos e geração de número pseudoaleatório e cifras de fluxo. Já a parte 2 trata de cifras assimétricas, com mais teoria dos números, criptografia de chave pública e RSA, além de outros criptossistemas de chave pública. Já na parte 3 são tratados os algoritmos criptográficos para integridade dos dados, incluindo funções de *hash* criptográficas, códigos de autenticação de mensagem, assinaturas digitais, gerenciamento e distribuição de chaves.

STALLINGS, W. **Criptografia e Segurança de Redes:** Princípios e Práticas. 6. ed. São Paulo: Pearson, 2015.

Assim, finalizamos esta seção, em que discutimos aspectos que mostram a razão de a criptografia ser considerada um dos principais controles de segurança, a qual vem sendo utilizada desde muito antes de a informação passar a ser digital. Em seus projetos de segurança, nunca se esqueça de proteger a confidencialidade dos dados que trafegam e que são armazenados, cuidando ainda da integridade e da autenticidade.



FAÇA VALER A PENA

**Questão 1**

A criptografia é um dos principais controles de segurança da informação, sendo utilizada para uma série de necessidades, como para garantir a confidencialidade, integridade ou autenticidade. Para cada uma dessas necessidades, há algoritmos específicos.

Assinale a alternativa que apresenta a função do algoritmo Diffie-Hellman.

a. Para cifrar mensagens.

b. Para assinar mensagens.

c. Para a troca de chaves criptográficas.

d. Para verificar a segurança.

e. Para enviar mensagens seguras.

**Questão 2**

Um cliente deseja enviar uma mensagem ao seu advogado. Apesar de ele ser uma figura pública, o cliente quer preservar a confidencialidade desta mensagem, de modo que somente o advogado tenha acesso a ela. O cliente não deseja, inclusive, que ninguém além do advogado saiba desta mensagem, ou seja, a mensagem deve passar despercebida por todos.

Diante ao exposto, assinale a alternativa que apresenta técnica, tecnologia ou algoritmo que o cliente deve utilizar para enviar a mensagem para o advogado.

a. AES.

b. RSA.

c. Diffie-Hellman.

d. *Hash* criptográfico.

e. Esteganografia.

Ver anotações

**Questão 3**

O serviço de mensagens *WhatsApp* utiliza criptografia em todas as suas comunicações, incluindo mensagens de voz e outros arquivos, entre seus usuários. Com o que chamam de "criptografia de ponta a ponta", as mensagens são cifradas ao deixar o dispositivo móvel da pessoa que as envia e só conseguem ser decodificadas no dispositivo móvel de quem as recebe. Segundo um comunicado da empresa, Quando você manda uma mensagem, a única pessoa que pode lê-la é a pessoa ou grupo para quem você a enviou. Ninguém pode olhar dentro da mensagem. Nem cibercriminosos. Nem *hackers*. Nem regimes opressores. Nem mesmo nós. Com a criptografia de ponta a ponta, um canal seguro é estabelecido entre o remetente e o destinatário, com a criptografia de chave pública. Este canal seguro é utilizado para trocar uma chave privada do algoritmo de criptografia simétrica entre as duas entidades, que é efetivamente utilizado para cifrar as mensagens.

Assinale a alternativa que apresenta as chaves criptográficas utilizadas neste processo, primeiro para o estabelecimento do canal seguro e depois a cifragem das mensagens.

a. Esteganografia.

b. Chave privada compartilhada entre remetente e destinatário, e chave pública do remetente.

c. Chave privada compartilhada entre remetente e destinatário, e chave pública do destinatário.

d. Par de chaves do remetente e destinatário, e chave privada compartilhada.

e. Par de chaves do destinatário, e chave privada compartilhada.

Ver anotações 0

## REFERÊNCIAS


ANCHISESLANDIA –Brazilian Security Blogger. **[Segurança] A Cifra Macônica.** 12 de julho de 2017. Disponível em: https://bit.ly/3oNuHIa. Acesso em: 7 out. 2020.

COPELAND, B. J. Britannica. **Ultra – Allied intelligence project.** Disponível em: https://bit.ly/3pRCLJd. Acesso em: 8 out. 2020.

CRYPTO Corner. **Vigenère Cipher.** Disponível em: https://bit.ly/3jdMGq4. Acesso em: 7 out. 2020.

FIARRESGA, V. M. C. **Criptografia e Matemática.** Dissertação (Mestrado em Matemática para Professores) – Faculdade de Ciências, Universidade de Lisboa. Lisboa, 2010. Disponível em: https://bit.ly/2O5hbmC. Acesso em: 7 out. 2020.

GRABBE, O. J. **The DES Algorithm Illustrated.** Disponível em: https://bit.ly/3oPMluR. Acesso em: 8 out. 2020.

JUNGES, F. **Blockchain descomplicado.** Livecoins. Disponível em: https://bit.ly/2MUyZAk. 4 de abril de 2018. Acesso em: 26 out. 2020.

KAHNEY, L. The FBI Wanted a Back Door to the iPhone. Tim Cook Said No. **Wired**, 16 abr. 2019. Disponível em: https://bit.ly/2Ms1Pbs. Acesso em: 7 out. 2020.

KATZ, J.; LINDELL, Y. L. **Introduction to Modern Cryptography.** Flórida: CRC Press, 2007.

MARSH, A. The Hidden Figures Behind Bletchley Park's Code-Breaking Colossus. **IEEE Spectrum**, 31 dez. 2019. Disponível em: https://bit.ly/3aArNkS. Acesso em: 8 out. 2020.

LOEFFLER, J. How Peter Shor's Algorithm Dooms RSA Encryption to Failure. **Interesting Engineering**, 2 maio 2019. Disponível em: https://bit.ly/36GiO0t. Acesso em: 2 nov. 2020.

MARR, B. F. What Is Homomorphic Encryption? And Why Is It So Transformative?. **Forbes**, 15 nov. 2019. Disponível em: https://bit.ly/3oNc4US. Acesso em: 2 nov. 2020.

MARTIN, G. Explainer: What is post-quantum cryptography? **MIT Technology Review**, 12 jul. 2019. Disponível em: https://bit.ly/36GHzK6. Acesso em: 7 out. 2020.

MCCULLOUGH, M. Making sense of an Enigma. **Ingenium**. Canada's Museums of Science and Innovation. 24 out. 2018. Disponível em: https://bit.ly/3jgxBnD. Acesso em: 8 out. 2020.

MEDEIROS, F. Uma breve história sobre Criptografia. **CryptID**, 6 jul. 2015. Disponível em: https://bit.ly/36F29du. Acesso em: 20 out. 2020.

MENEZES, A. J.; OORSCHOT, P. C. van. VANSTONE, S. A. **Handbook of Applied Criptography**, ago. 2020 Disponível em: https://cacr.uwaterloo.ca/hac/. Acesso em: 6 out. 2020.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. **Bitcoin.Org.** 31 out. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 2 nov. 2020.

NAKAMURA, E. T., GEUS, P. L. **Segurança de redes em ambientes cooperativos.** São Paulo: Novatec, 2007.

NAKAMURA, E. T. **Segurança da informação e de redes**. Londrina: Editora e Distribuidora Educacional, 2016.

NIST. National Institute of Standards and Technology. U.S. Department of Commerce. Computer Security Division. Applied Cybersecurity Division. **Lightweight Cryptography**. Disponível em: https://bit.ly/3pO9PBH. Acesso em: 2 nov. 2020.

PRADO, J. **O que é blockchain?** [indo além do bitcoin]. **Tecnoblog**. Disponível em: https://bit.ly/3rgSGks. Acesso em: 7 out. 2020.

RICE, D. What Is the Difference Between Quantum Cryptography and Post-Quantum Cryptography? **FedTech**, 4 mar. 2020. Disponível em: https://bit.ly/3ttZBZu. Acesso em: 2 nov. 2020.

SIMON, S. **O livro dos códigos**. Rio de Janeiro: Record, 2010.

TOWSEND Security. AES vs. DES Encryption: Why Advanced Encryption Standard (AES) has replaced DES, 3DES and TDEA. **Preciserly**, 1 jun. 2020. Disponível em: https://bit.ly/3tt5GFC. Acesso em: 8 out. 2020.

WARD, M. **The ancient art of hidden writing**. BBC News, 2 jul. 2010. Disponível em: https://bbc.in/3rmYHw2. Acesso em: 8 out. 2020.