

Princípios Básicos de Criptografia

Prof. Dr. Kelton Costa

kelton.costa@unesp.br

Fundamentos

- Há muito tempo o ser humano se preocupa em proteger informações, garantindo que outras pessoas não vejam ou saibam o conteúdo da mensagem a ser transmitida. Vários métodos foram inventados ao longo do tempo para atingir esse objetivo e garantir a confidencialidade da informação.

Fundamentos

- **Criptografia:** estudo e práticas de princípios e técnicas para comunicação segura na presença de terceiros.
- Ou seja, na prática, é qualquer técnica que garanta que um terceiro não tenha acesso a sua informação ou não consiga ler ou entender o verdadeiro significado da mensagem.

Princípios

- Até pouco tempo atrás, a criptografia era somente sinônimo de **criptação**, que é o processo de converter um texto comum (texto claro) para um texto ilegível (cifra).
- Hoje a criptografia possui mais objetivos e princípios:
 - Confidencialidade;
 - Integridade;
 - Autenticidade;
 - Irretratabilidade.

Princípios

- **Confidencialidade:** só o destinatário autorizado da mensagem é capaz de extrair o conteúdo e entender a mensagem. Em uma analogia simples, é como um cofre, só quem possui a chave é que terá acesso ao conteúdo do cofre.

Princípios

- **Integridade:** o destinatário consegue verificar se a mensagem foi alterada durante a transmissão. Isso garante que alguém malicioso não envie alguma mensagem correta, porém antiga, que não é mais válida. O destinatário vai conseguir abrir a mensagem e verificar todo o conteúdo, mas ela já não é mais válida.

Princípios

- **Autenticidade:** o destinatário consegue verificar que a mensagem foi realmente enviada por quem diz ser enviada. De forma simples, é como uma assinatura em um contrato ou em um cheque.

Princípios

- **Irretratabilidade:** o remetente da mensagem não consegue negar a autoria da mensagem enviada. Uma vez publicada ou enviada, o remetente não pode se retratar ou dizer que não enviou, já que somente ele pode ter o conhecimento ou a chave para gerar a mensagem.

Princípios

- É bom notar que nem todos os sistemas ou algoritmos cobrem todos esses princípios ao mesmo tempo e que, na maioria das aplicações, é necessária a aplicação de mais um algoritmo em conjunto para atender a todos os requisitos.

Técnicas de Criptografia

- Existem várias técnicas de criptografia (e, conseqüentemente, algoritmos) que são aplicadas atualmente, mas as principais são: **criptografia de chave secreta, de chave pública e hashing.**

Esquematização

- Criptografia simétrica possui os seguintes itens:
 - i) **Texto claro**: mensagens originais para transmissão;
 - ii) **Alg. Criptografia**: procedimento que realiza substituições/transformações;
 - iii) **Chave secreta**: mais uma entrada para o alg. Chave independe do texto;
 - iv) **Texto cifrado**: mensagem “embaralhada” produzida como saída;
 - v) **Alg. Decriptografia**: alg. de cript. Executado no modo inverso.

Tipos de criptografia

- **Substituição:** cada elemento do texto claro (bit, letra) é mapeado para outro elemento;
- **Transposição:** os elementos do texto claro são reorganizados entre si.

Cifra de César

- O algoritmo mais antigo de uma cifra de substituição, sendo criada por Júlio Cesar.
- Consiste basicamente em substituir cada letra do alfabeto pela letra que fica 3 posições adiante.
- Frequentemente incorporado como parte de esquemas mais complexos: cifra de Vigenère e ROT13.

Texto Claro: CRIPTOGRAFIA

Texto Cifrado: FULSWRJUDTLD

<https://www.dcode.fr/caesar-cipher>



Técnica de Transposição

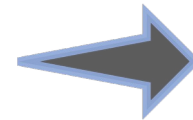
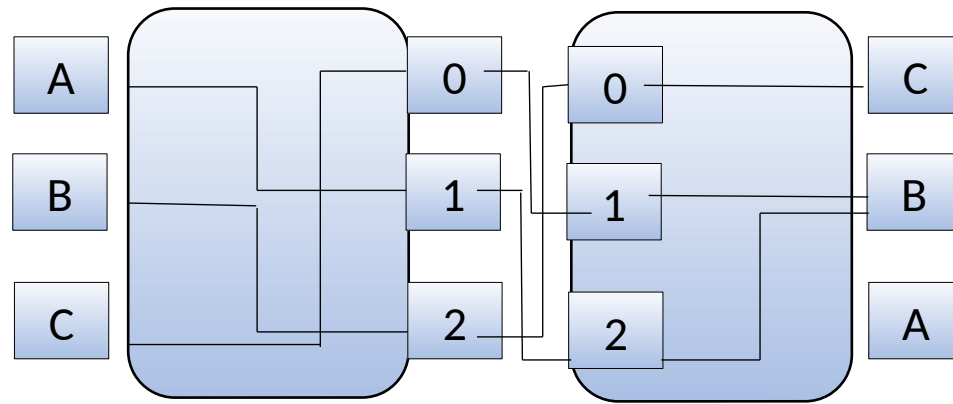
- Técnica em que os caracteres de texto claro são permutados entre si com o intuito de gerar o texto cifrado.
- **Rail Fence**: técnica mais simples em que o texto claro é escrito como uma sequência de diagonais e lido como uma sequência de linha.

C		I		T		G		A		I	
	R		P		O		R		F		A

CRIPTOGRAFIA = CITGAIRPORFA
(RF de profundidade 2)

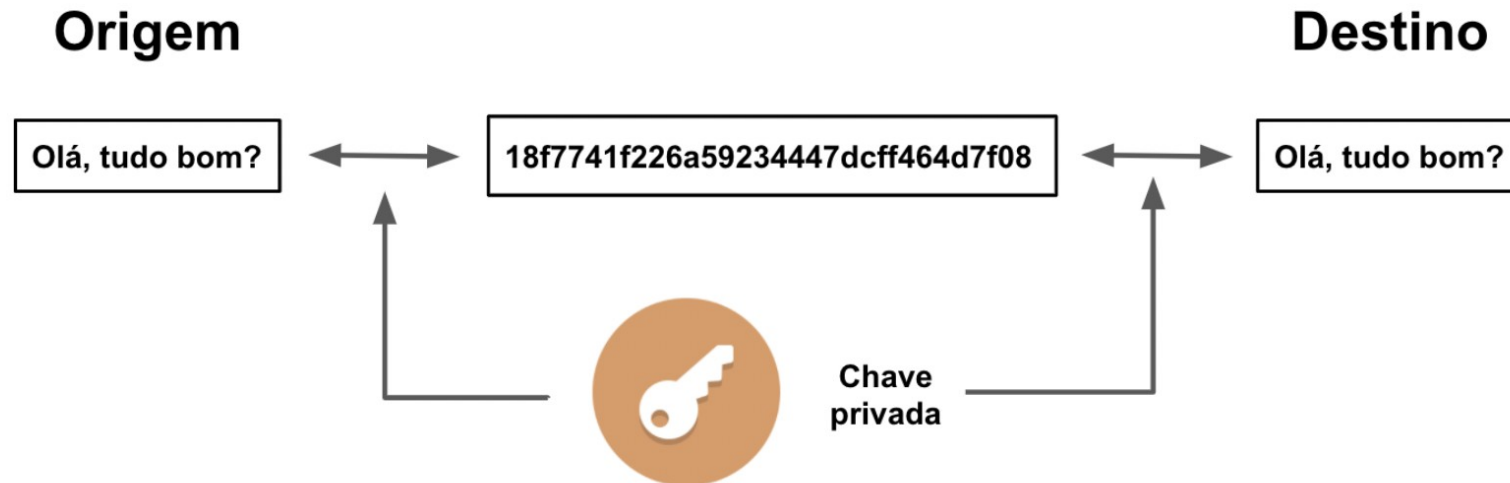
Máquinas de Rotor

- Abordagem que equivale ao princípio de uma máquina de rotor, composta por cilindros, o qual contém, cada um, 26 pinos de entrada e um de saída para cada um.



Técnicas de Criptografia

- **Chave Secreta (Simétrica):** Tipo de criptografia que usa somente uma chave tanto para encriptar quanto para decriptar uma mensagem. Ambas as partes devem possuir uma cópia da chave para poder trocar a mensagem.



Técnicas de Criptografia

- Este modo é usado para o princípio da confidencialidade. Este tipo pode ter 2 modos de algoritmos:
 - **EM BLOCO**: a mensagem é encriptada em blocos de tamanhos específicos. EX: DES, AES, etc.
 - **EM STREAM**: a mensagem é encriptada pegando-se byte a byte da informação. EX: RC4, Salsa20, etc.

Técnicas de Criptografia

- Por a mesma chave ser usada nas duas pontas do processo, ela deve ser compartilhada de forma segura entre as partes. Isso pode trazer problemas se não for feito com cuidado.

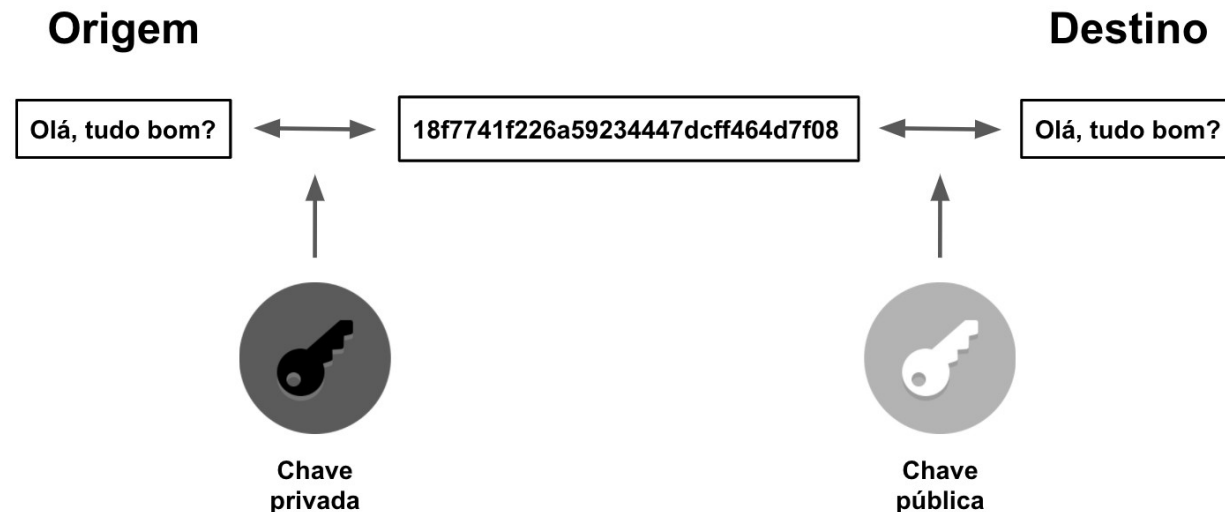
Técnicas de Criptografia

- **Chave Pública (Assimétrica):** esta técnica utiliza duas chaves diferentes para o processo, uma para encriptar e outra para decriptar.



Técnicas de Criptografia

- **Chave Pública (Assimétrica):** a chave usada para encriptar é a chave pública e pode ser conhecida por qualquer pessoa. A chave usada para decriptar é conhecida como chave privada e deve ser mantida em sigilo por apenas uma das partes.



Técnicas de Criptografia

- Este modo é usado para os princípios de confidencialidade e autenticidade.
- Para o caso de autenticar (ou assinar) uma mensagem, a ordem é invertida. A chave privada é usada para assinar a mensagem, enquanto a chave pública é usada para a sua verificação.
- Este modo é usado para a troca segura de chaves simétricas. EX: SSL (usado no HTTPS), que usa em conjunto criptografia simétrica e assimétrica para criptografar e autenticar uma página web.

Técnicas de Criptografia

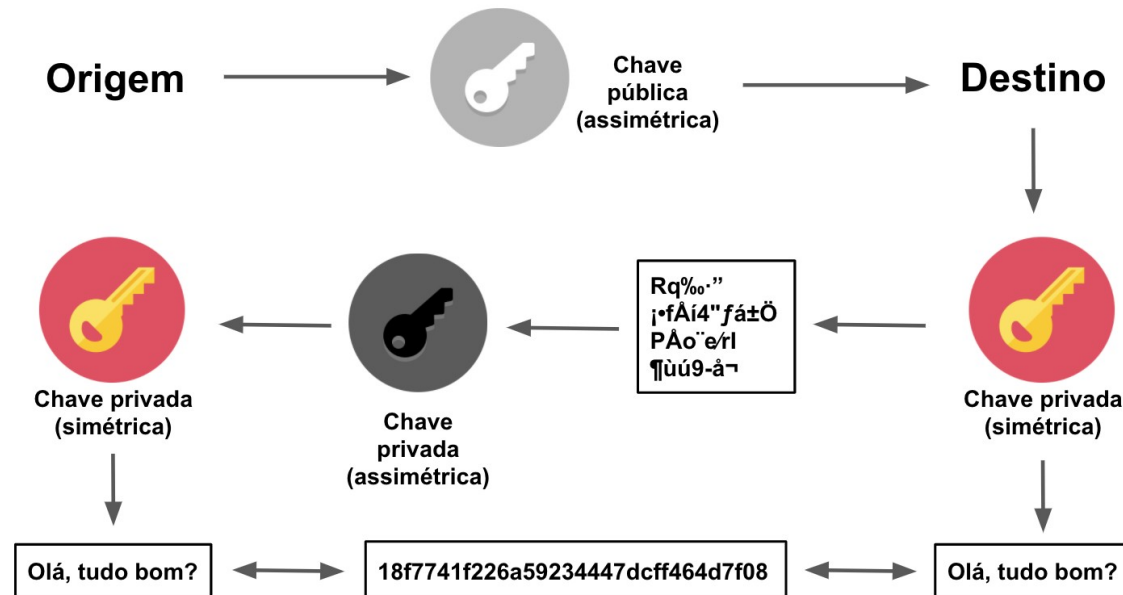
- Exemplos de técnicas de chave assimétrica:
 - Protocolo Diffie-Hellman
 - DSS (Digital Signature Standard)
 - ElGamal
 - Curvas elípticas

Combinando Simétrica e Assimétrica

- O uso apenas da criptografia simétrica possui o problema de como compartilhar a chave privada com o destinatário sem que nenhum invasor consiga interceptar e também obter essa chave privada.
- Uma solução para esse problema é combinar o uso da criptografia simétrica e assimétrica, podemos fazer isso em 4 passos:

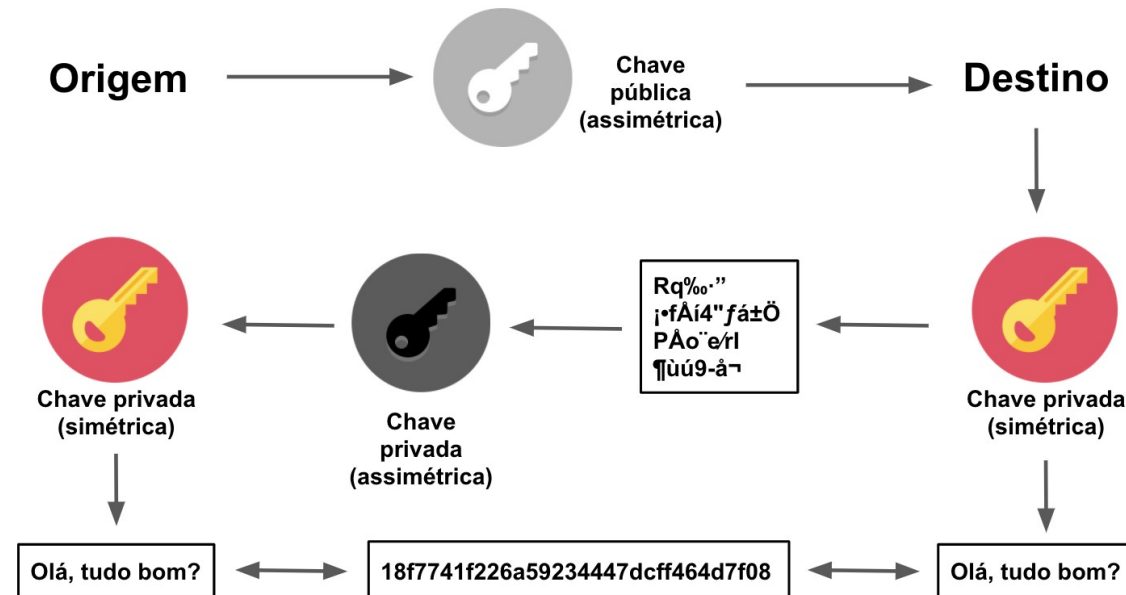
Combinando Simétrica e Assimétrica

- Origem manda chave pública (Assimétrica) para o Destino. Como a chave pública pode ser de conhecimento de qualquer um, não importa se um invasor também obter essa chave.



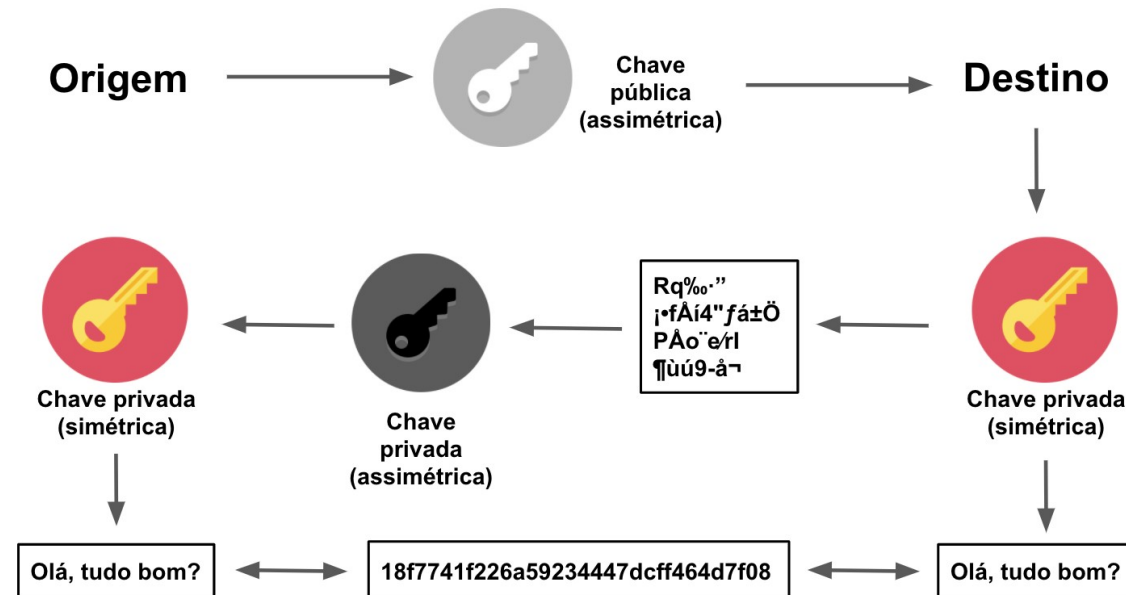
Combinando Simétrica e Assimétrica

- Destino utiliza a chave pública (Assimétrica) recebida e criptografa sua chave privada (Simétrica) e envia para a Origem. Nesse momento a chave simétrica está criptografada, e apenas a Origem possui a chave privada (Assimétrica) capaz de descriptografá-la.



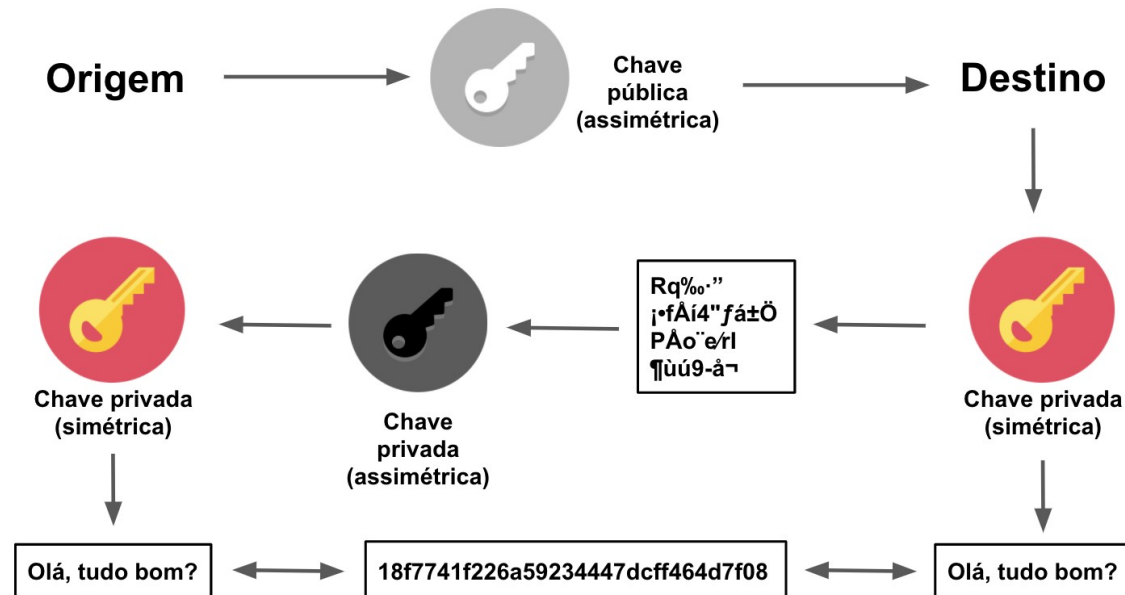
Combinando Simétrica e Assimétrica

- Origem descriptografa usando sua chave privada (Assimétrica). Agora ambos origem e destino possuem a mesma chave privada (Simétrica).



Combinando Simétrica e Assimétrica

- Origem criptografa os dados usando a chave privada (Simétrica) e envia para o destino que também possui a mesma chave privada (Simétrica) e consegue descriptografar esses dados.



Técnicas de Criptografia

- **Hashing:** é uma forma de **criptografia** que não envolve nenhuma chave.
- É o processo de converter uma **informação qualquer de qualquer tamanho** em um **código de tamanho fixo** de texto por meio de uma **função matemática**.
- São inúmeros os usos dessa técnica no mundo real.
Das **comunicações** às *passwords*, a **criptação é fundamental** para assegurar uma segurança maior e a confidencialidade da informação.

Técnicas de Criptografia

- Existem inúmeras outras **funções hash** que podem ser utilizadas para transformar uma **informação** qualquer em um **valor hash**. EX: **SHA1, SHA-256, SHA-512, MD2, MD5, etc.**
- O hash é uma função de via única, ou seja, não se consegue recuperar a mensagem original a partir somente do valor final.

Três métodos

- Por que usar 3 métodos? Por que não usar somente um que cubra todos os princípios?
- Resposta: Cada técnica é otimizada para uma aplicação específica. Em aplicações reais, para garantir todos os princípios, uma combinação das 3 técnicas é aplicada. Por exemplo, podemos usar o modo simétrico para encriptar a mensagem (confidencialidade) e enviar junto o hash (integridade) e a assinatura (autenticidade), como modo assimétrico.

Aplicações

- **Assinatura digital:** uma forma de mandar documentos e garantir ao destinatário que esse documento é autêntico.
- Normalmente, se adquire uma chave privada de uma autoridade e, com essa chave, pode assinar os documentos.
- Na outra ponta, o destinatário possui uma chave pública da mesma autoridade e consegue verificar a validade da assinatura e, consequentemente, a autenticidade do documento.

Aplicações

- **Encriptação de e-mail:** envio de e-mails com dados sensíveis pode ser perigoso e facilmente interceptado por terceiros, podendo gerar prejuízos ao negócio. Existem meios de se encriptar os dados enviados. EX: OpenPGP.

Aplicações

- **Encriptação de dados sensíveis:** salvar dados sensíveis ao negócio (como senhas ou financeiro) deve ser feito de forma cuidadosa.

Aplicações

- **HTTPS/SSL**: uma combinação de hash, criptografia e assinatura é usada no protocolo HTTPS, que está presente na maior parte dos sites na web. Isso garante que o site que você está acessando realmente é de quem você espera e que as informações trafegadas estão seguras (tais como senha, dados pessoais, etc).

Aplicações

- **Blockchain:** tecnologia bastante aplicada atualmente e se utiliza fortemente dos princípios de criptografia para armazenar os dados e também verificar sua autenticidade.

Conclusão

- A criptografia é estudada e usada há muito tempo pelo ser humano e a cada dia que passa, com a maior conectividade das pessoas e dos dados, se exige que se tenha maior segurança e confiabilidade dos seus dados que são tanto armazenados quanto trafegados pelos sistemas.