Criptografia

Introdução à criptografia

Roadmap

- Histórico
- Diferença entre código e cifra
- Nomenclatura básica
- Princípio de Kerckhoffs
- Visão geral da criptologia

Universidade Federal do Ceará
Campus de Crateús

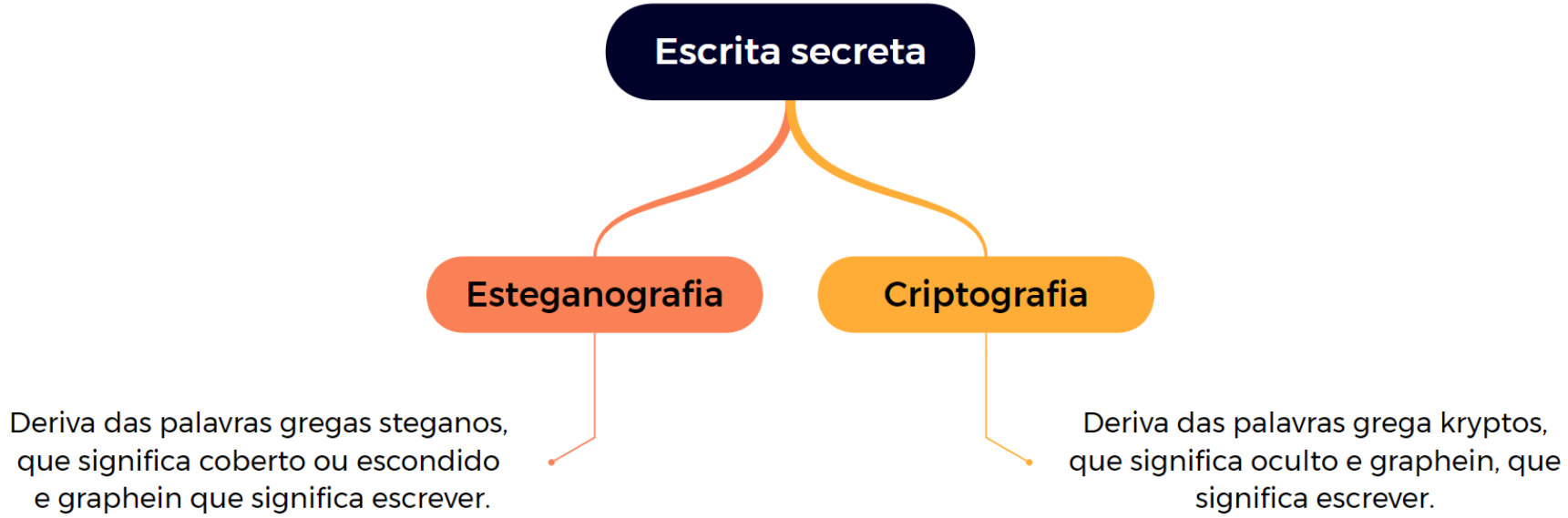
Ciência da Computação
Sistemas de Informação

emerson@crateus.ufc.br

Introdução à criptografia

Histórico

- Os primeiros relatos sobre **escrita secreta** datam do século V a. C.
- Há dois ramos de escrita secreta:



Introdução à criptografia

Histórico

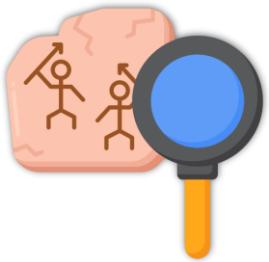
- A **esteganografia** tem o objetivo de ocultar a *existência* da mensagem.
- A **criptografia** tem o objetivo de ocultar o *significado* da mensagem.

O processo que torna a mensagem incompreensível é conhecido como ***cifração****, em que o texto é "misturado" de acordo com um protocolo que já foi estabelecido previamente pelas parte — o transmissor e receptor.*

Assim, o receptor da mensagem pode aplicar o protocolo para reverter o processo e tornando a mensagem compreensível.

Introdução à criptografia

Histórico



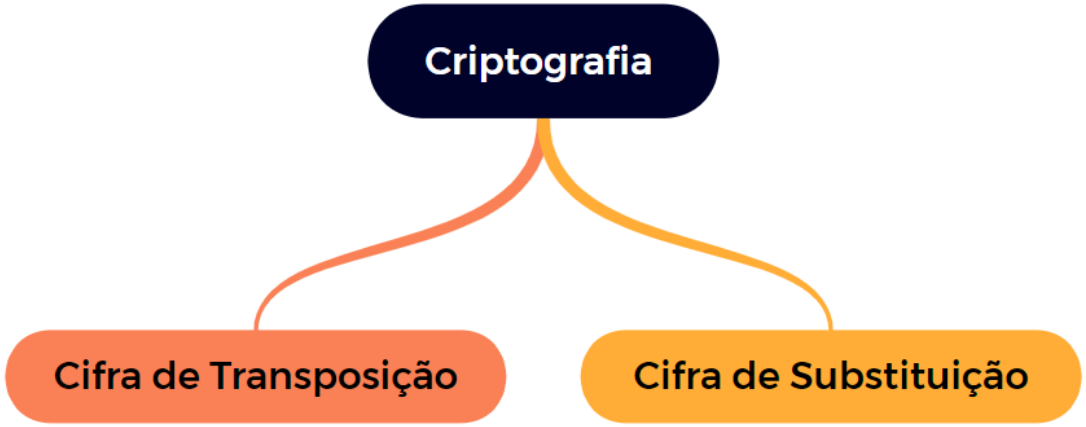
A **esteganografia** tem uma fraqueza fundamental — se o mensageiro for revistado e a mensagem descoberta, então o conteúdo da comunicação secreta é imediatamente revelado.

A vantagem da **criptografia** é que se o inimigo interceptar a mensagem cifrada ela será incompreensível e seu significado não poderá ser relevado.

Introdução à criptografia

Histórico

- Inicialmente, a criptografia pode ser dividida em dois ramos:



Histórico

Cifra de transposição

- As letras da mensagem são simplesmente rearranjadas, de modo a gerar uma série de letras aparentemente sem sentindo.

Cifra de substituição

- Cada letra do texto é substituído por uma letra diferente.

*A **transposição** faz com que cada letra mantenha sua identidade, mas muda a sua posição.*

*A **substituição** faz com que as letras mudem de identidade, mas mantém a posição.*

Histórico

Cifra de transposição

- O primeiro caso documento de *cifra de transposição* data do final do século V a. C. na Grécia antiga, usando uma ferramenta chamada ***citale espartano.***
- **Citale espartano** consiste em um bastão de madeira que em volta do qual é enrolada uma tira de couro.

Cifração

O remetente escreve a mensagem ao longo do comprimento do bastão e depois desenrola a tira, que agora parece com uma série de letras sem sentidos.

Decifração

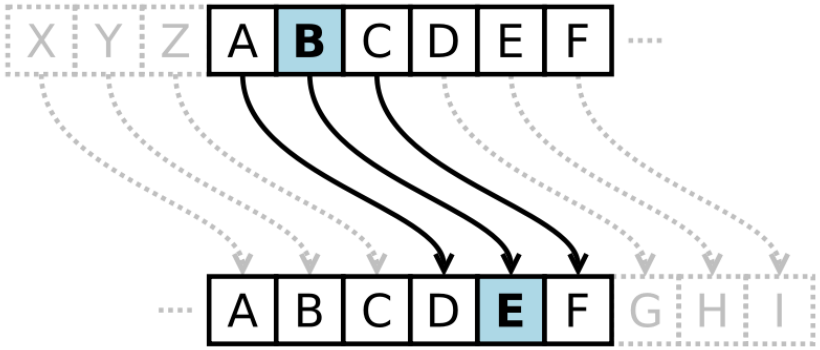
Ao receber a mensagem, o destinatário enrola a tira de couro em torno de um *citale* de mesmo **diâmetro** que foi usado pelo remetente.

Histórico

Cifra de substituição

- O primeiro documento a usar uma ***cifra de substituição*** para proposito militar é da época de Júlio César — general do império romano.

- César simplesmente **substituía cada letra** na mensagem por **outra que estive três posições** à frente no alfabeto. Assim, essa cifra ficou conhecida como ***Cifra de César***.



Histórico

Cifra de substituição

- Nesse contexto, há o ***alfabeto original***, usada para escrever a mensagem; e o ***alfabeto cifrado***, formado pelas letra usadas na substituição.

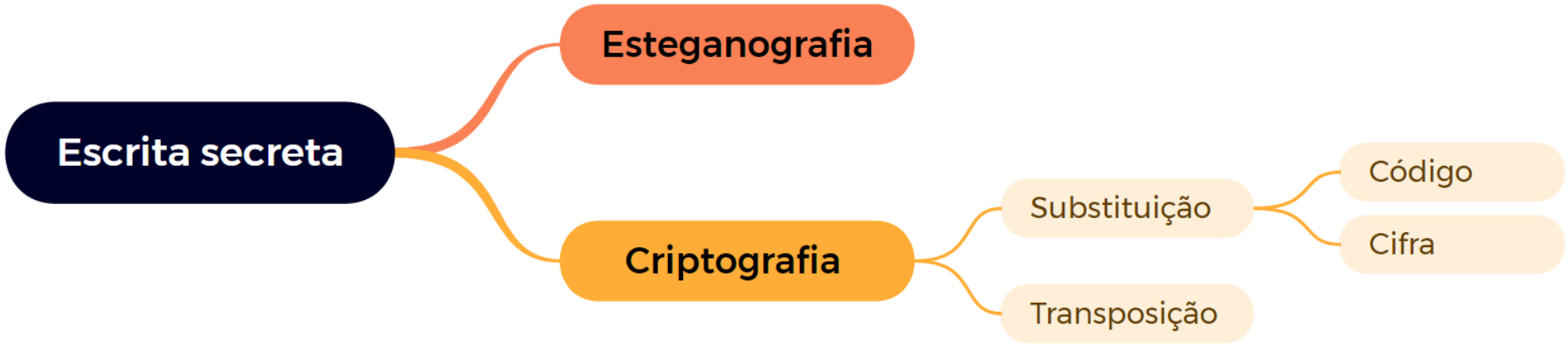
- Embora César costumasse deslocar as letras em **três** posições à frente, fica claro que empregando-se qualquer deslocamento entre **1** e **25** posições, é possível criar 25 cifras distintas.

Disco de cifra desenvolvido em 1470 pelo arquiteto italiano Leon Battista Alberti.

Introdução à criptografia

Nomenclatura

- Vamos apresentar alguma definições básicas e jargões da criptografia.
- Vamos começar pela ciência da *escrita secreta* e sua principais ramificações.



Nomenclatura

Criptografia

- De modo geral, a criptografia é a ciência da escrita secreta com o objetivo de esconder o significado de uma mensagem.

> **Definição (Criptografia).** *Tradicionalmente, a* ***criptografia*** *é definida como o estudo de técnicas capazes de tornar uma mensagem incompreensível, de forma que somente o destinatário legítimo seja capaz de decifrá-la e compreendê-la*

- Nessa definição **tradicional**, o objetivo da criptografia é garantir a **confidencialidade** da comunicação entre duas entidades quando estas utilizam um canal inseguro.

Nomenclatura

Criptografia moderna

- Atualmente, esse cenário básico não representa todos os objetivos da criptografia moderna.
  - Desde a década de 1970, problemas como:
    i. Construção de assinaturas digitais não falsificáveis;
    ii. Protocolos tolerantes a falhas;
  - Também foram considerados como **domínio da criptografia**.

Definição (Criptografia moderna). *A criptografia é o estudo de técnicas matemáticas relacionadas a aspectos de segurança da informação, tais como a confidencialidade, integridade de dados, autenticação de entidade e autenticação da origem dos dados.*

Nomenclatura

Domínios da criptografia moderna

- Fornecer **confidencialidade** não é mais o único objetivo da criptografia.
- A criptografia moderna também é usada para fornecer soluções para outros problemas.
- Portanto, os esquema criptográfico atuais então relacionados aos seguintes objetivos:

Confidencialidade

Integridade

Autenticidade

Não-repúdio

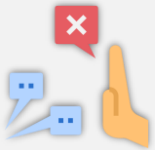
Nomenclatura

Domínios da criptografia moderna

Confidencialidade. A mensagem não deve estar disponível para terceiros não autorizados.

Autenticidade. O receptor de uma mensagem deve ser capaz de verificar a origem dela. Ninguém deve ser capaz de enviar uma mensagem fingindo ser outra pessoa (**autenticação de origem de dados**).

Integridade. O receptor deve ser capaz de verificar se a mensagem foi modificada durante a transmissão—acidental ou deliberadamente.



Não-repúdio. O remetente não deve poder negar posteriormente que enviou uma mensagem.

Nomenclatura

Domínios da criptografia moderna

- A criptografia surgiu devido a necessidade de proteger informações importantes, sobretudo **informações militares.**

- No entanto, hoje a criptografia tem impacto maior nas **atividades civis**—como por exemplo, operações bancárias via Internet.

Nomenclatura

Código vs. Cifra

- Em geral, um **código** assume a forma de um livro (o *livro de código*), onde uma palavra ou frase do texto original é substituída por uma **palavra-código.** É simplesmente um mapeamento.

> **Definição (Código).** *Método para esconder o significado de uma mensagem por meio da substituição de **cada palavra** ou **frase** da mensagem original por uma outra **palavra**, um **número** ou um **símbolo**.*

Portanto, o termo codificar significa ocultar uma mensagem usando um código; e de forma semelhante, decodificar significa revelar uma mensagem codificada.

Nomenclatura

Código vs. Cifra

- Numa cifra não existe um *livro de códigos*. Em vez disso, usa-se um ***algoritmo*** que transforma os símbolos individualmente.
- O algoritmo precisa de uma informação secreta — conhecida como **chave**, para transformar uma letra/símbolo em outra.

Definição (Cifra). *Método para esconder o significado de uma mensagem transformando* ***cada letra*** *da mensagem original em* ***uma outra*** *letra.*

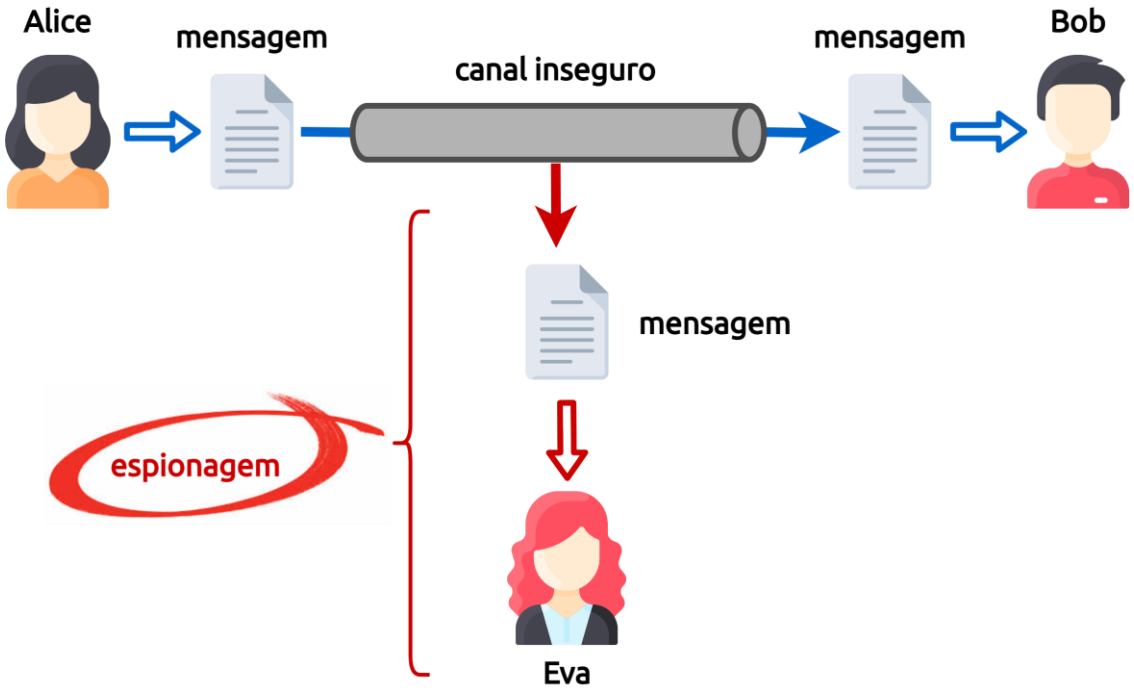
Portanto, o termo cifrar significa ocultar uma mensagem usando uma cifra; e decifrar significa revelar uma mensagem cifrada.

Nomenclatura

Modelo básico de comunicação

- Nos cenários de exemplo em criptografia é comum nomear os *players* envolvidos.
- Tradicionalmente, os dois principais *players* se chamam **Alice** e **Bob**.
- Mas também, temos **Eva**, que deseja ler as mensagens de Alice e Bob.

*Assumimos que o **canal de comunicação** entre Alice e Bob é **inseguro** e Eva tem acesso ao canal.*

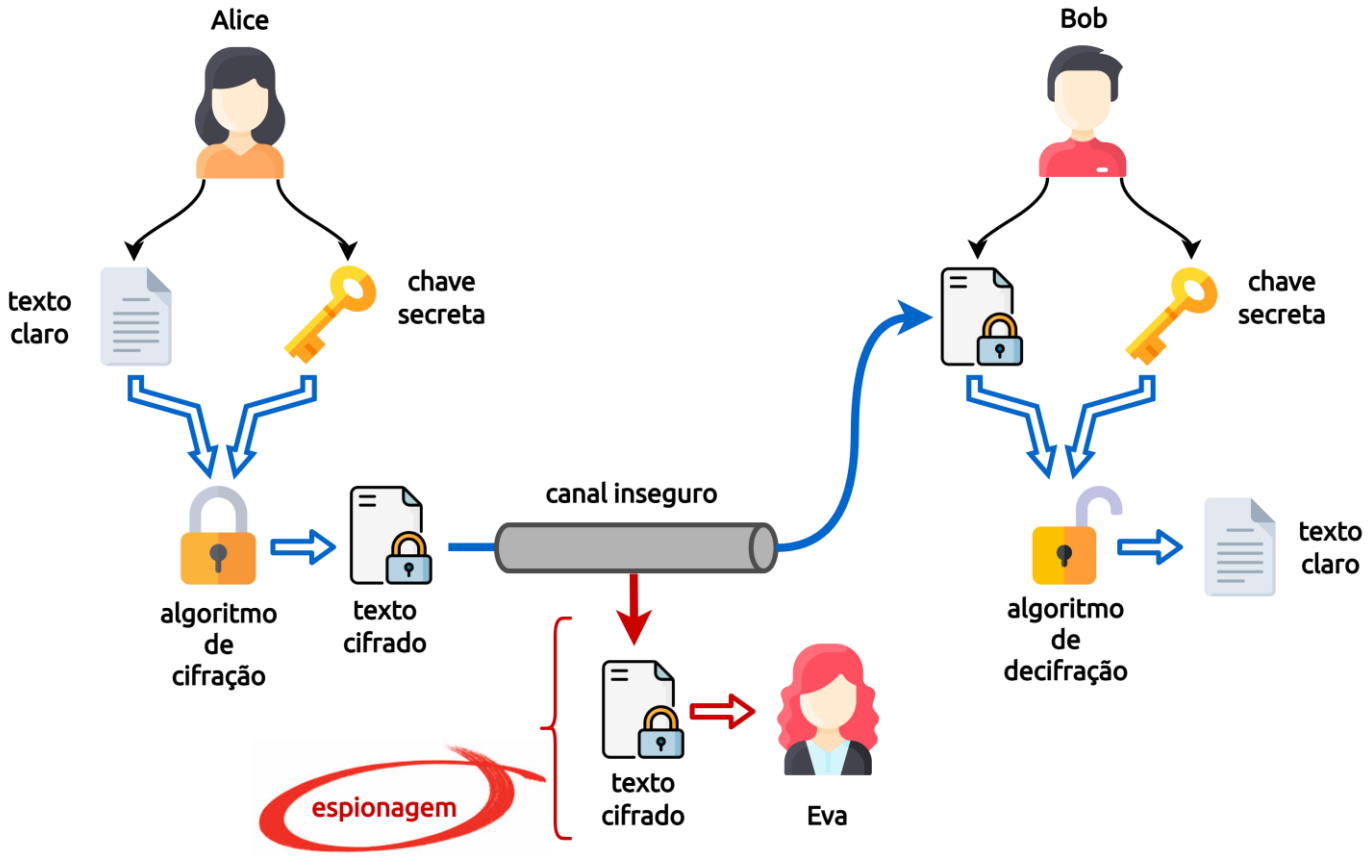


Nomenclatura

Modelo básico de comunicação segura

- Num cenário com criptografia, Alice **cifra** a mensagem original, produzindo uma **mensagem cifrada**.
- Bob recebe a mensagem cifrada e a **decifra**.

Assim, mesmo que Eva capture a mensagem cifrada, ***não poderá revelar*** *o significado da mensagem.*



Nomenclatura

- Note que na figura anterior, temos, portanto, um modelo de ***criptossistema*** (sistema criptográfico ou uma cifra). Um criptossistema envolve:

Texto claro (texto simples)

Mensagem original.

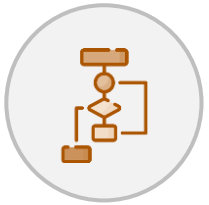
Texto cifrado (criptograma)

Mensagem ininteligível resultado da transformação do texto claro.

Chave

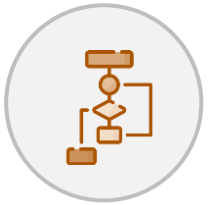
Valor **numérico** ou uma ***string*** usada por um algoritmo para cifrar ou decifrar uma mensagem.

O algoritmo produzirá uma saída diferente, dependendo da chave usada.



Algoritmo de cifração

Protocolo que transforma o texto simples em texto cifrado.



Algoritmo de decifração

Protocolo que representa a operação inversa, realizando a transformação do texto cifrado em texto claro.

Nomenclatura

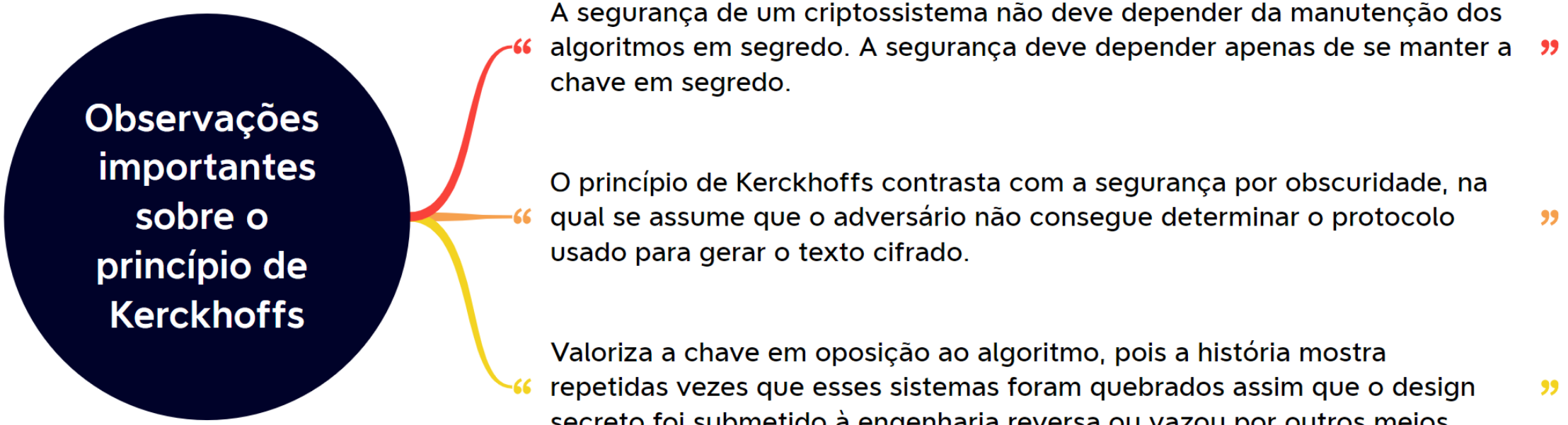
Definição (Criptossistema). *É um par de algoritmos — um para cifrar e o outro para decifrar. Para gerar o texto cifrado é necessário uma* ***chave específica****, a qual define exatamente quais transformações o algoritmo deve realizar no texto simples.*

- Note que, para uma **determinada mensagem**, **duas chaves** diferentes produzirão **dois textos cifrados** diferentes.
  - O texto cifrado é um fluxo aparentemente aleatório de dados e, portanto, é ininteligível.

- Um adversário deve ser incapaz de decifrar o texto ou descobrir a chave — mesmo se ele/ela estiver de posse de vários textos cifrados juntamente com o texto simples que produziu cada texto cifrado.
- *Isso nós leva ao Princípio de* ***Kerckhoff*** *(1883).*

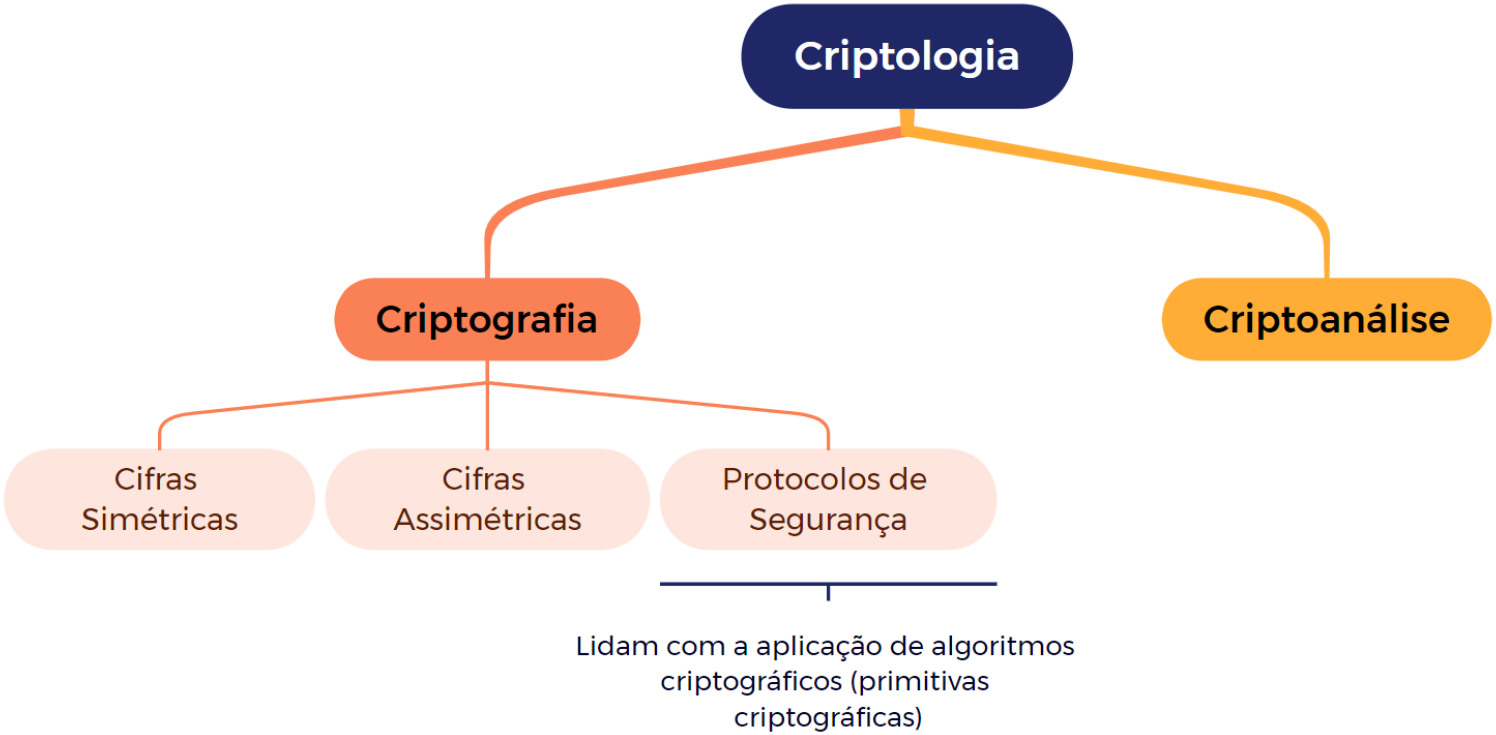
Princípio de Kerckhoffs

Definição (Princípio de Kerckhoffs). *Um criptossistema deve ser seguro mesmo que tudo sobre o sistema seja de conhecimento público, exceto a* ***chave secreta****.*



Visão geral do campo da criptologia

- A ciência da **criptologia** pode ser dividida em duas partes.
- Uma é a **criptografia**, que se preocupa com a criação de esquemas criptológicos.
- A outras é a **criptoanálise**, que estuda técnicas para descobrir o segredo do texto cifrado — conhecida popularmente como "quebra do código".



Fim!

[Aula 01] Introdução à criptografia