APRENDENDO JUNTOS

CRIPTOGRAFIA PARA CRIANÇAS

escrito por Elizabeth A. Quaglia
ilustrado por Alex Thompson

APRENDENDO JUNTOS

CRIPTOGRAFIA PARA CRIANÇAS

ELIZABETH A. QUAGLIA é uma Professora Associada no Grupo de Segurança da Informação em Royal Holloway, University of London. Sua área de pesquisa é Cibersegurança com enfoque em Criptografia. Ela é mãe de duas crianças, Ale e Leo, que amam comer bolo.

ALEX THOMPSON é uma designer de produtos digitais com um pé na ilustração. Quando ela não está desenhando dinossauros, ela está trabalhando para construir o comércio internacional e ferramentas de marketing em Londres. Encontre-a em @userologist.

Este livreto foi criado com a ajuda da
DRA. VALENTINA ZAMBON, psicóloga,
e MICHELE VILLA, designer.

Também agradecemos ao DR. JORGE BLASCO ALIS
e ao DR. JASSIM HAPPA pelos conselhos e apoio.

Adaptação para o português brasileiro feita por LUIZA BARROS REIS SOEZIMA

COMO LER ESTE LIVRO

Com este livreto, gostaríamos de dar a oportunidade às crianças e aos adultos de aprenderem juntos criptografia.

Para ajudar as crianças a entenderem os conceitos, sugerimos que os adultos também se envolvam na descrição e na discussão da história nas próximas páginas.

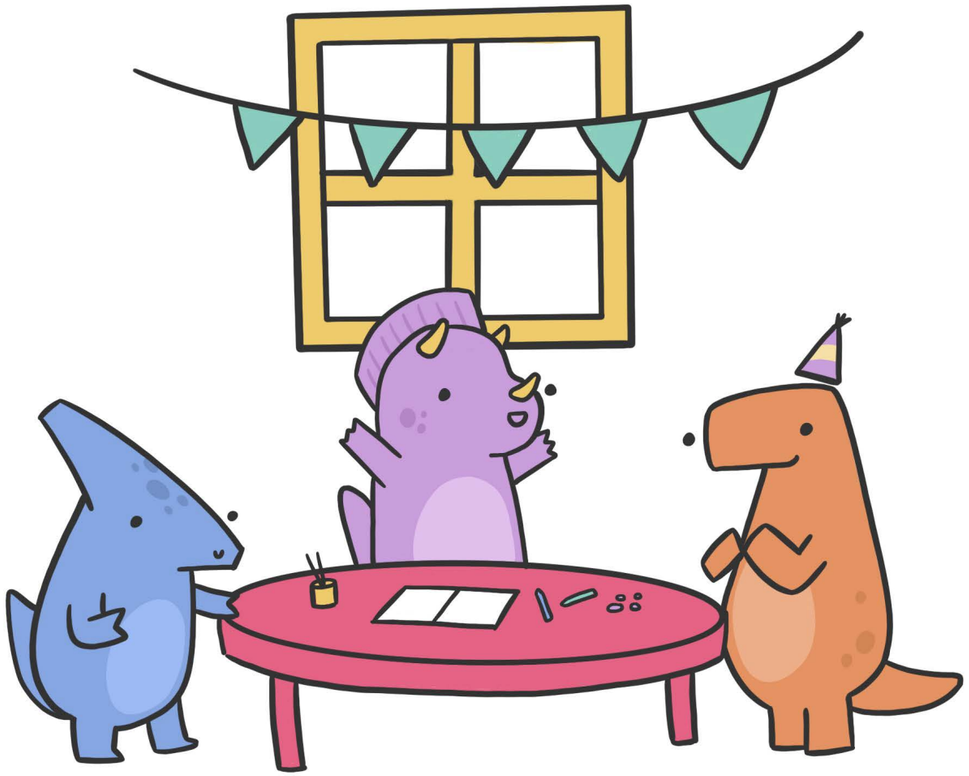
Perguntas como "Onde está o cachorro?" ou "O que o cachorro está tentando fazer?" podem ser formas úteis de engajar a criança. Então… façam muitas perguntas!

Por exemplo, na página 7, por que o cartão de aniversário é colocado em um envelope? Da mesma forma, na página 13, por que o bolo está sendo coberto? Ainda, na página 17, o que acontece se só dois pedaços do mapa do tesouro fossem encontrados? Ah, e na página 19 e 22, por que não é melhor usar uma chave secreta do que guardar as quatro chaves de forma segura?

Para os adultos, há um glossário no final deste livreto, definindo algumas terminologias criptográficas que aparecem ao longo da história e também há alguns links sugeridos (em inglês) que auxiliam na conexão com outros recursos adicionais para o aprendizado do tópico.

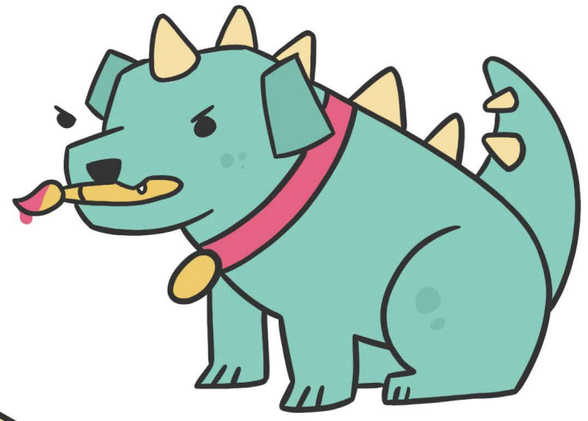
Hoje é o ANIVERSÁRIO DO T-REX!

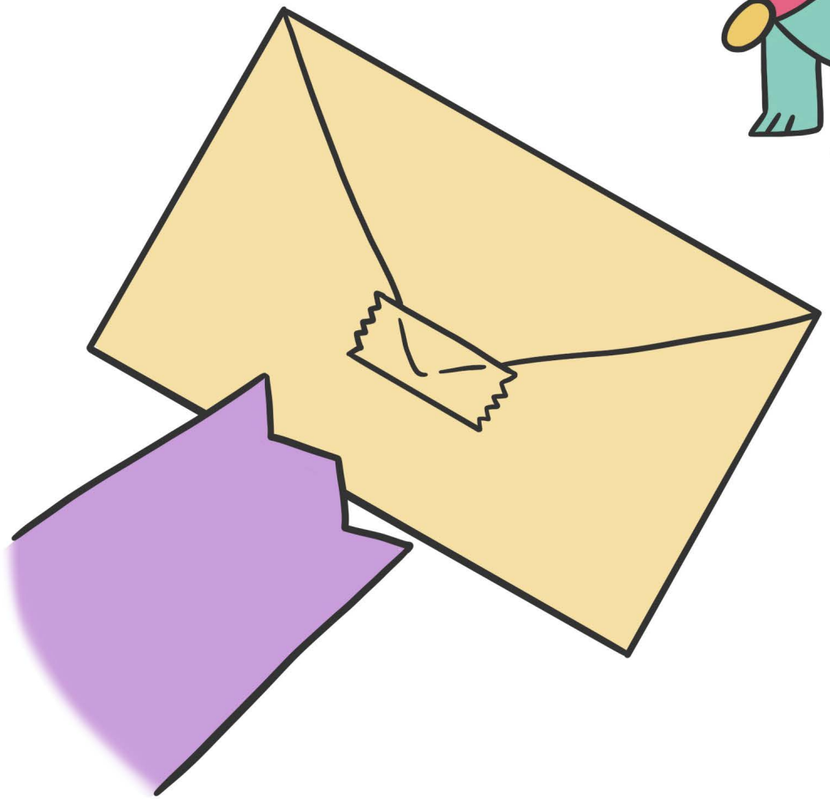
Vamos fazer uma festa surpresa para o T-Rex!



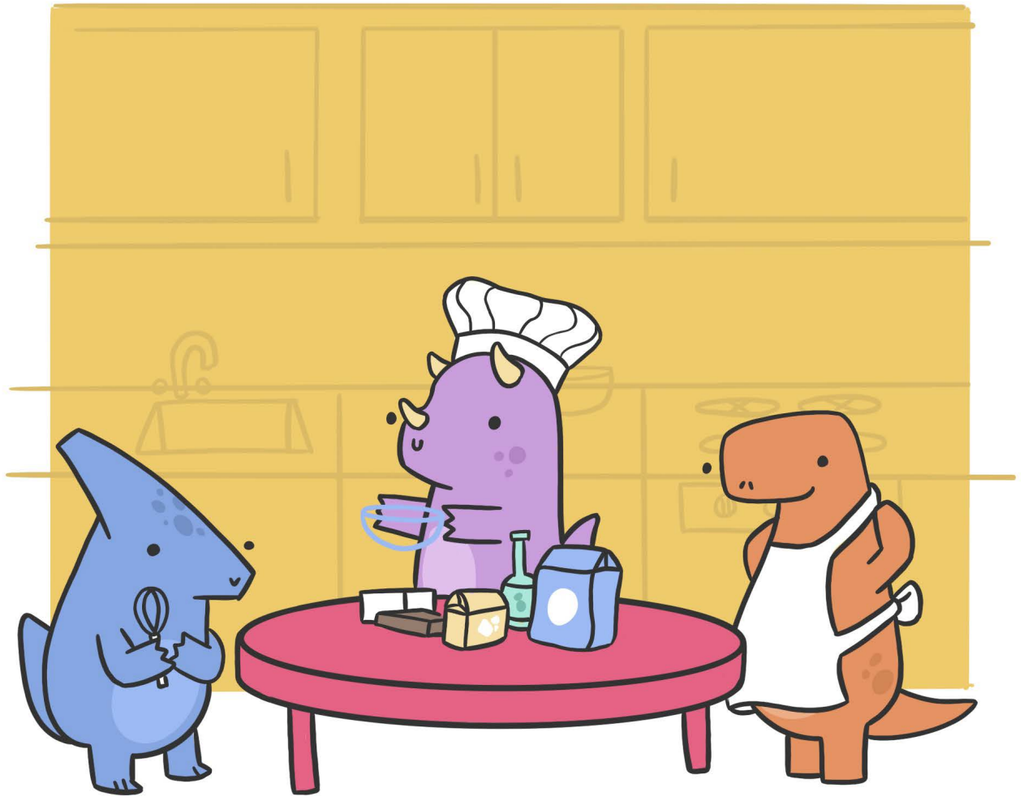
Vamos ASSINAR
o cartão de
aniversário!

Vamos colocar o cartão
em um ENVELOPE para
deixá-lo bem protegido.

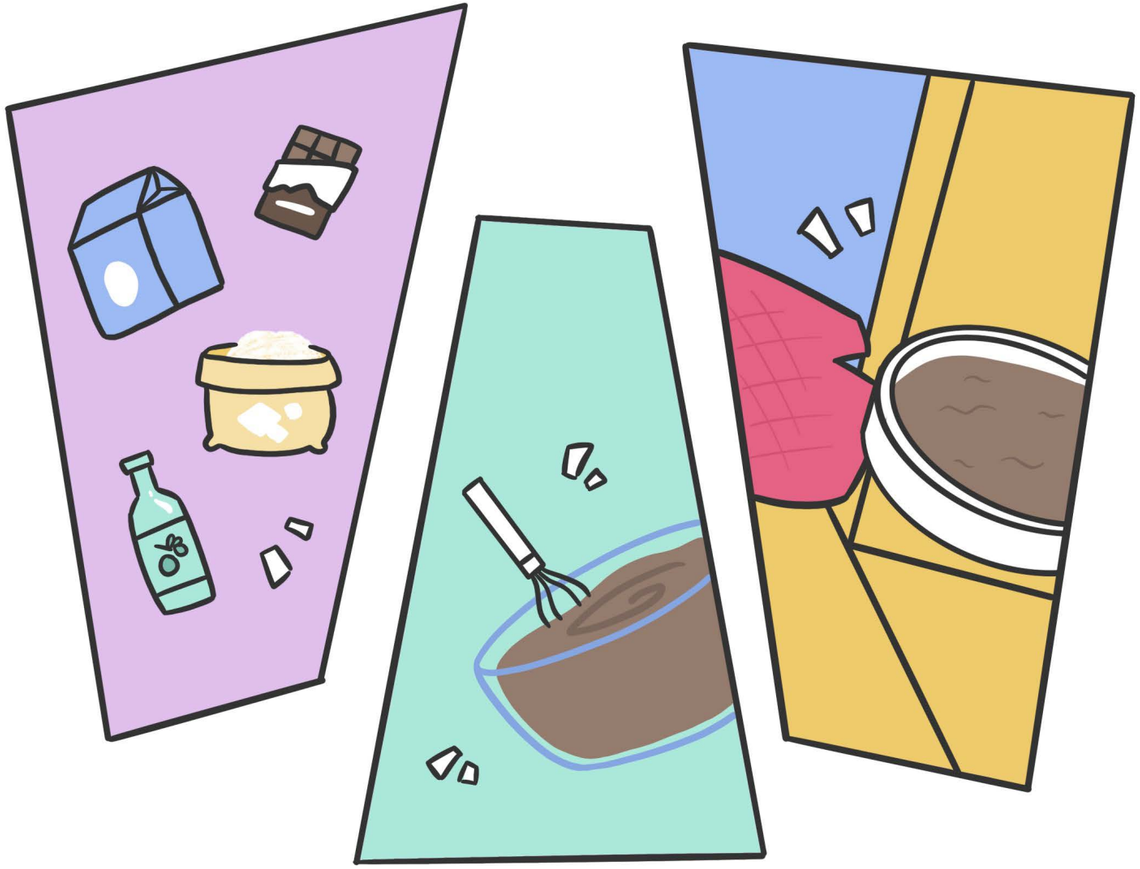




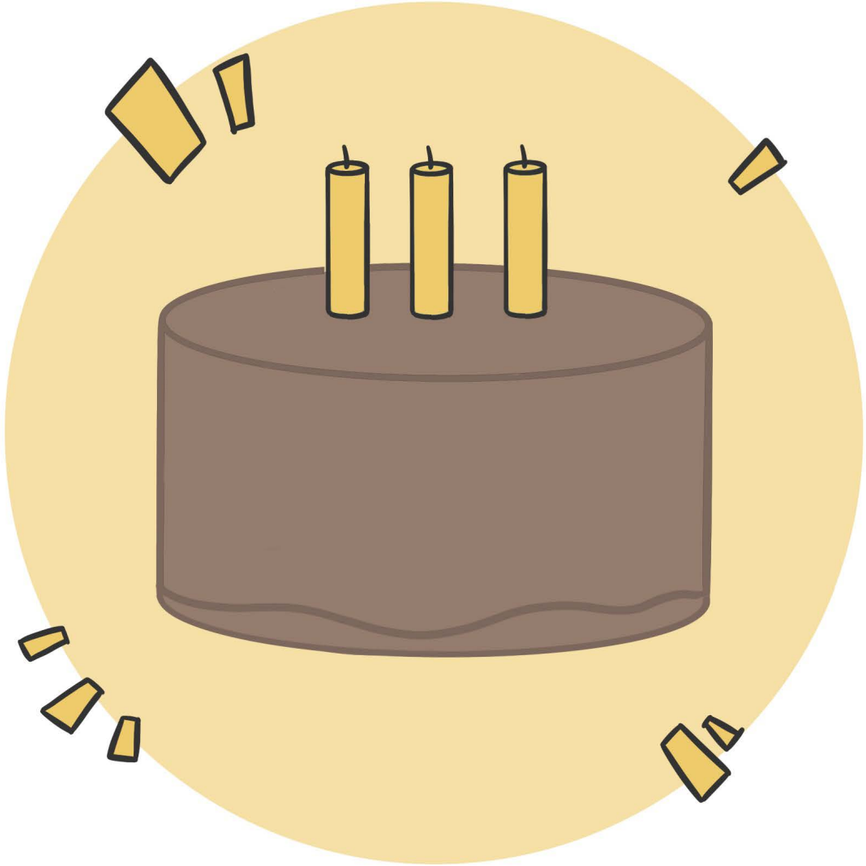
E agora vamos fazer um bolo de aniversário!



Vamos misturar os ingredientes juntos e colocar a mistura que fizemos no forno!

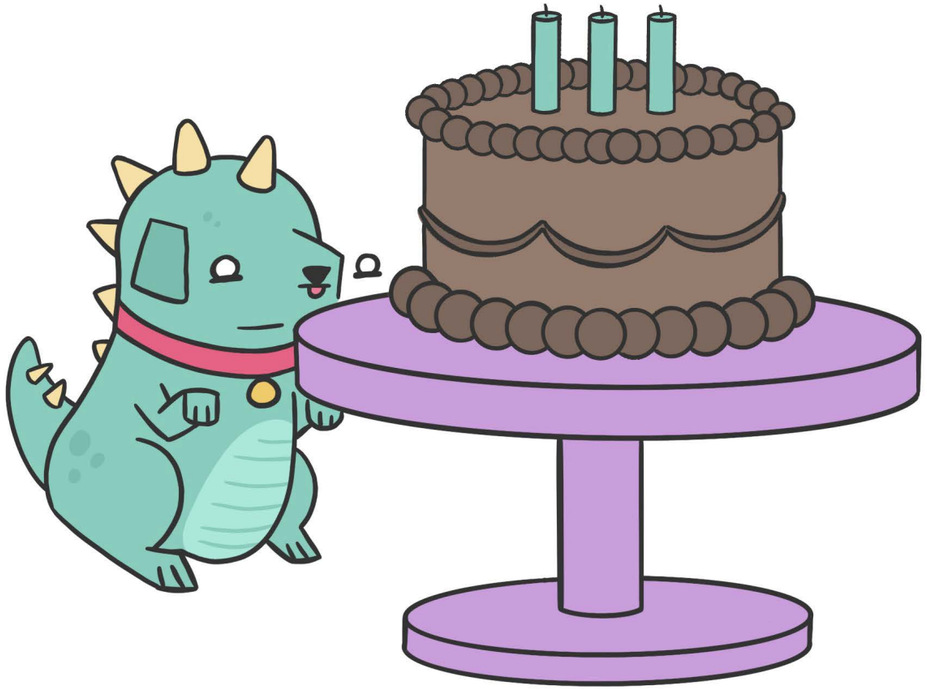


E aqui está o bolo!

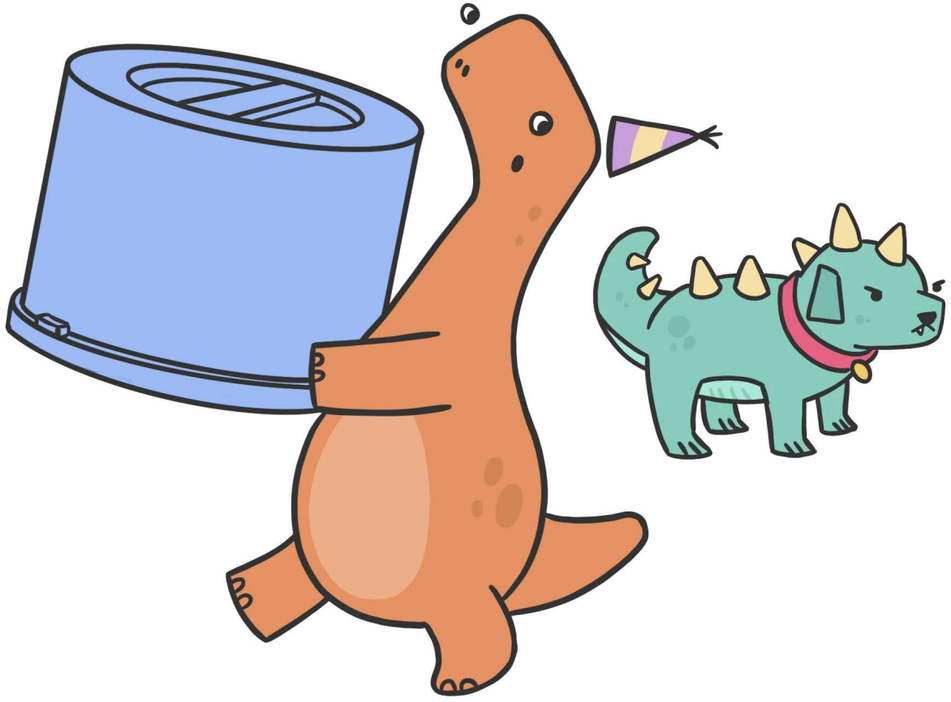


Vamos dar um toque final. Como podemos decorar o bolo?

Parece que o cachorro também gostaria de um pedaço do bolo.



Acho melhor ESCONDERMOS o bolo!

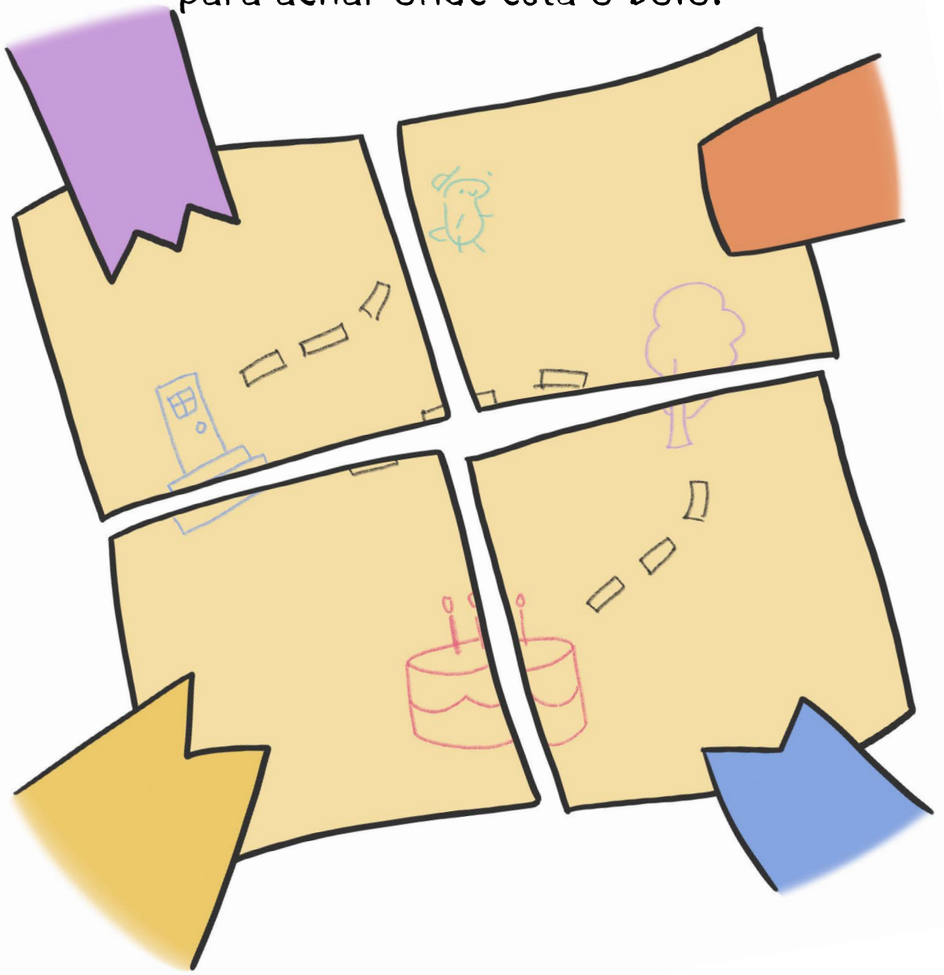


T-REX chegou!
Que tal jogarmos um jogo agora?
Vamos achar o bolo de aniversário!

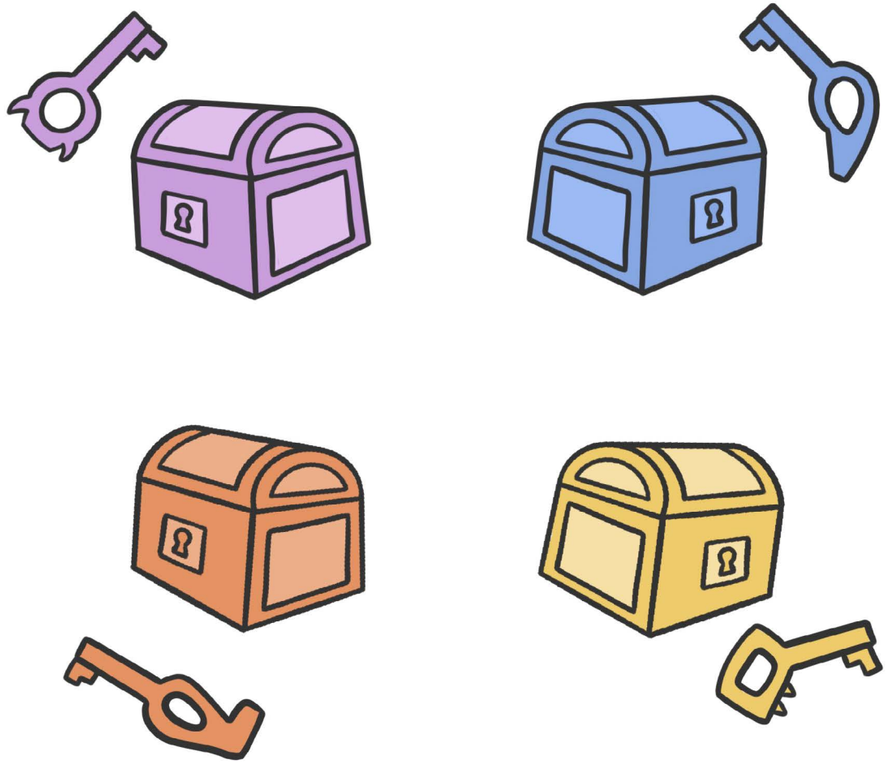
Este aqui é o mapa do tesouro
para achar o bolo escondido.

Todos pegam UM pedaço do
mapa do tesouro.

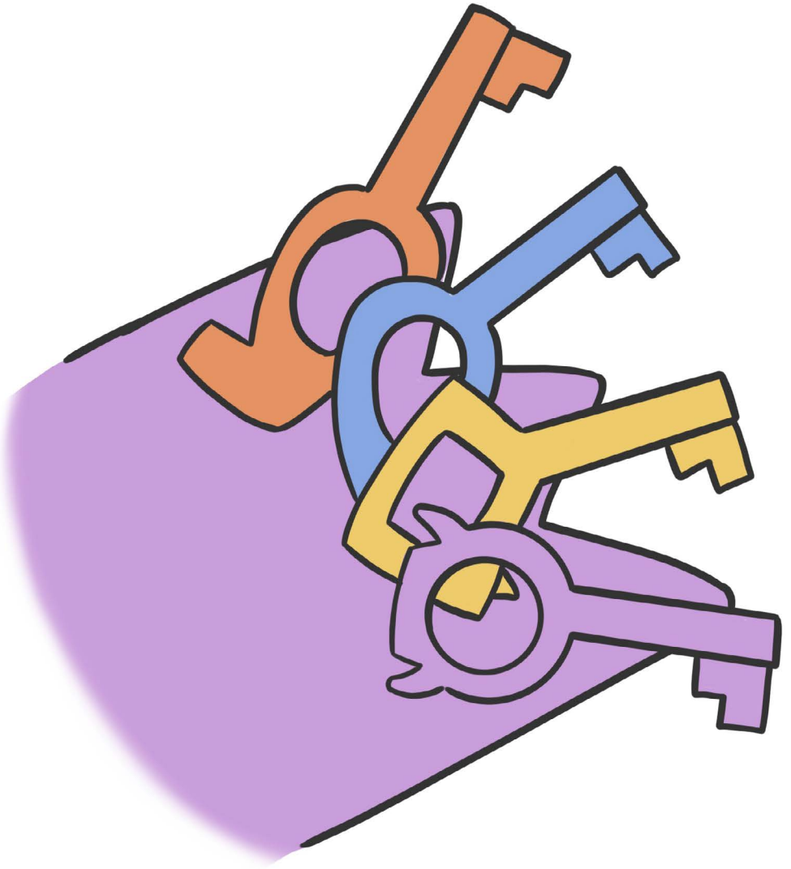
Precisamos de TODOS os pedaços
para achar onde está o bolo!



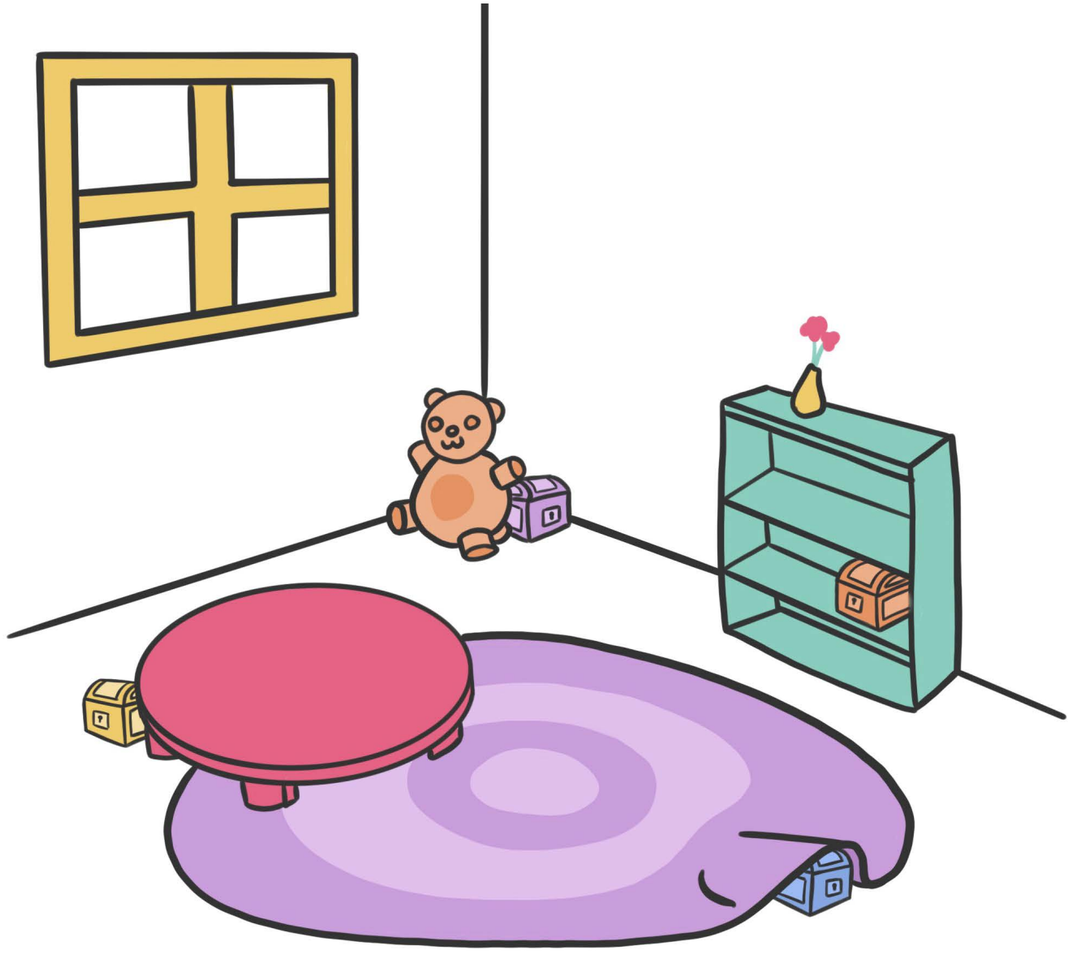
Triceratops tranca cada pedaço em uma caixa, usando chaves diferentes para cada uma das caixas.



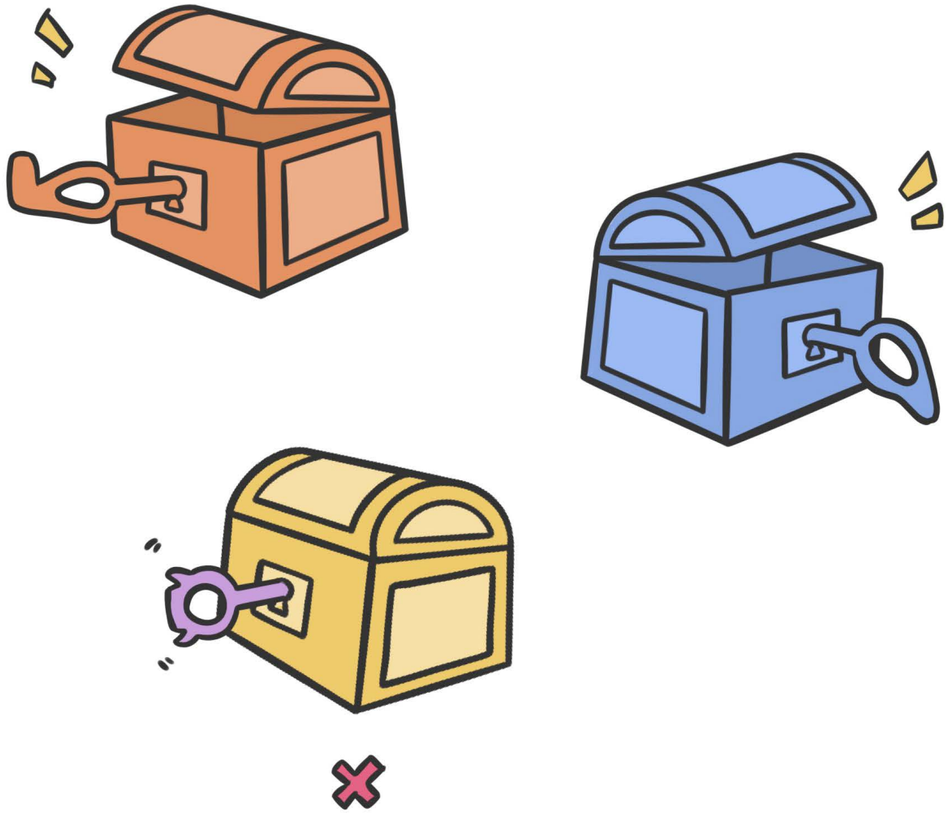
Triceratops precisa guardar muito bem as **QUATRO** chaves!



Todos têm que achar as suas caixas agora!



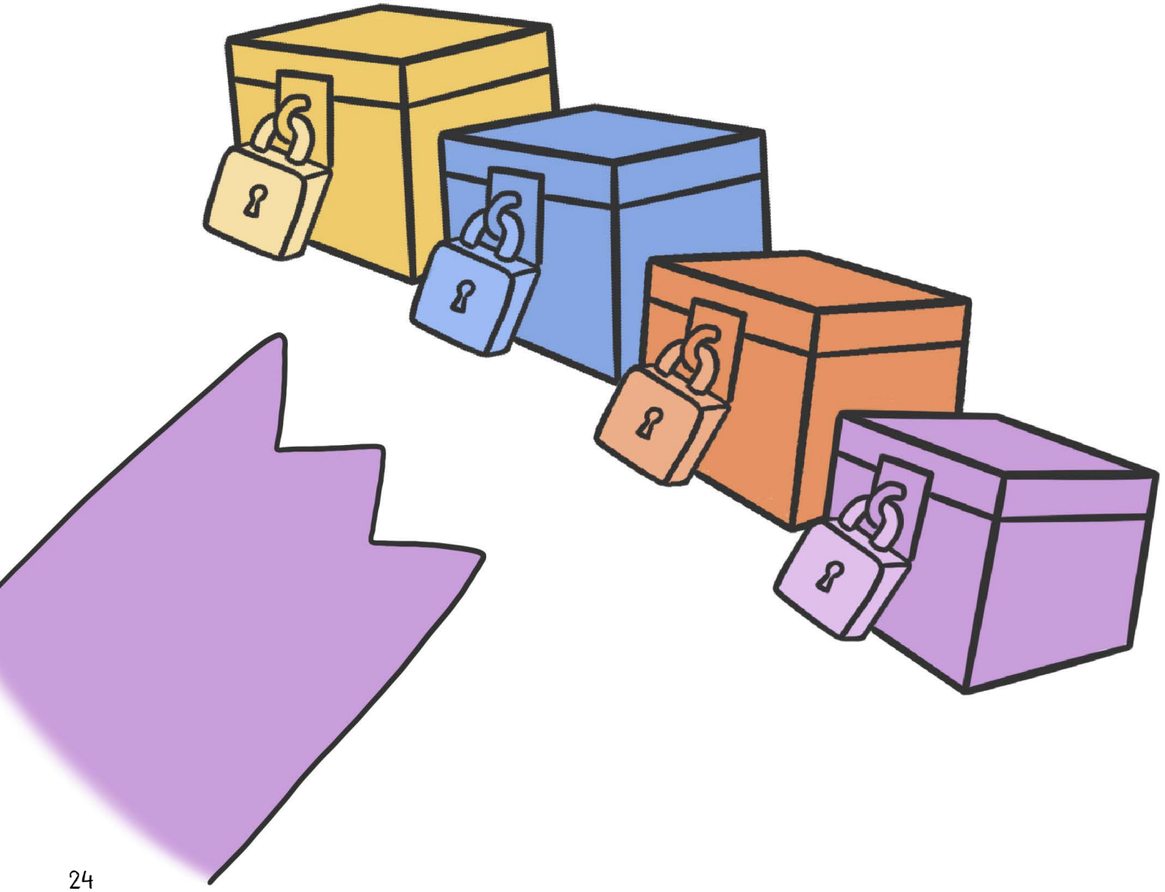
Para abrir a caixa, precisamos da MESMA chave que a trancou!



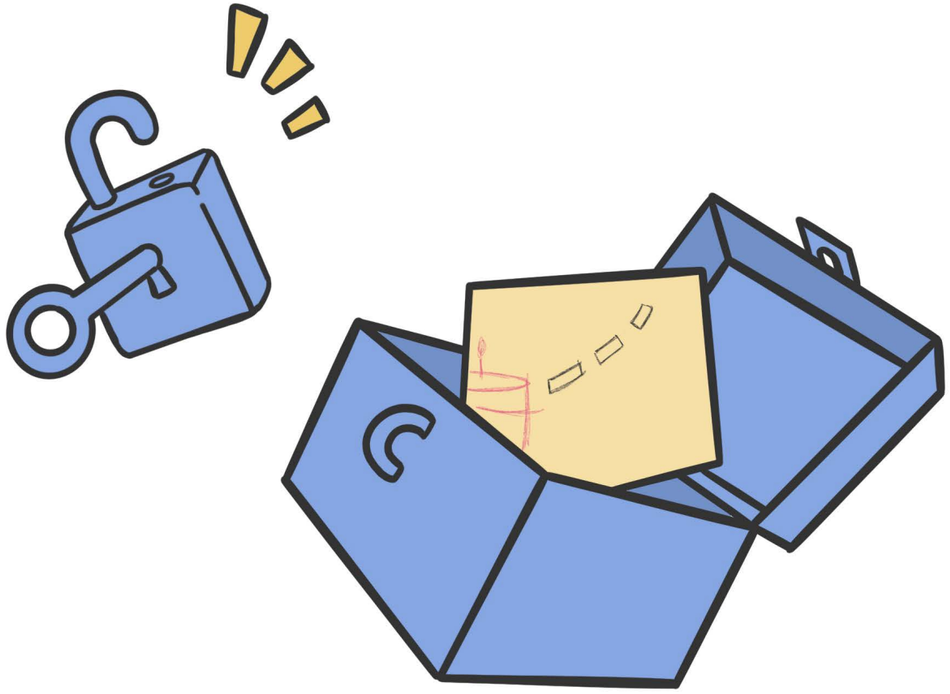
Hmm, será que Triceratops conseguiria trancar as caixas SEM precisar de nenhuma chave?

Isto é um **CADEADO**. Você não precisa de uma chave para trancá-lo. Mas você precisa de uma chave para abri-lo.

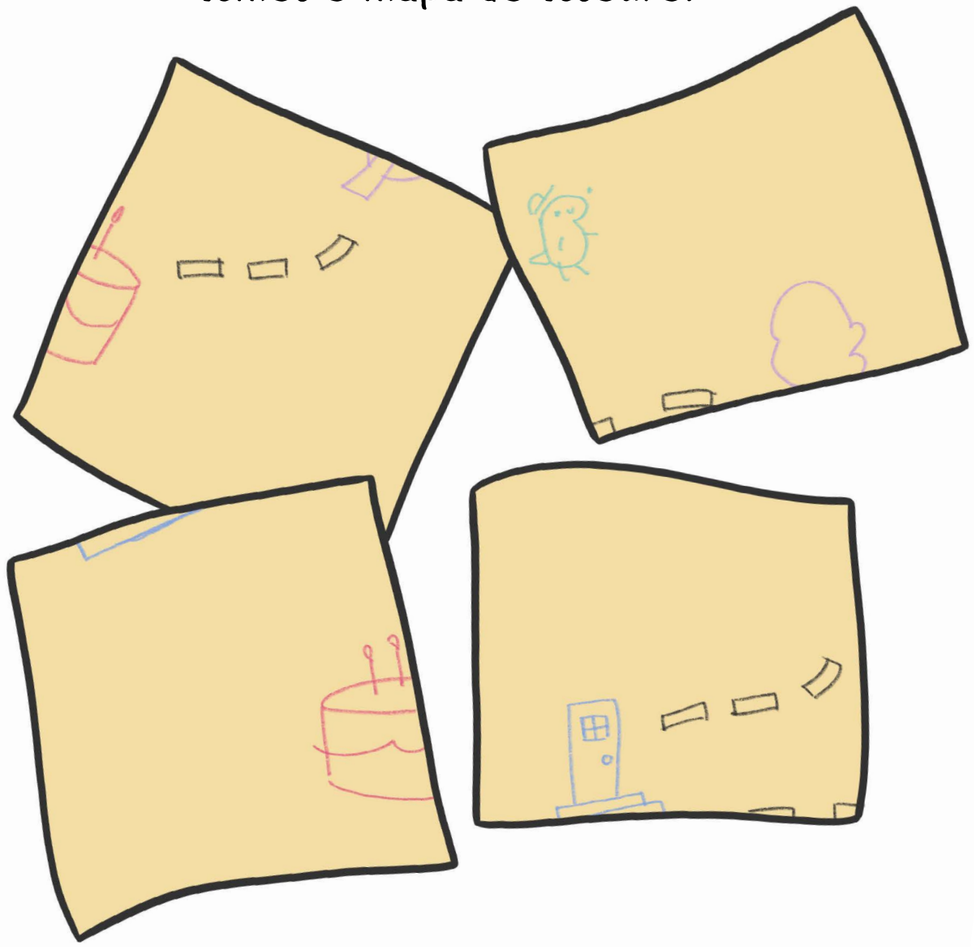
Triceratops poderia trancar todos os cadeados e não precisaria de NENHUMA chave secreta para fazer isso!



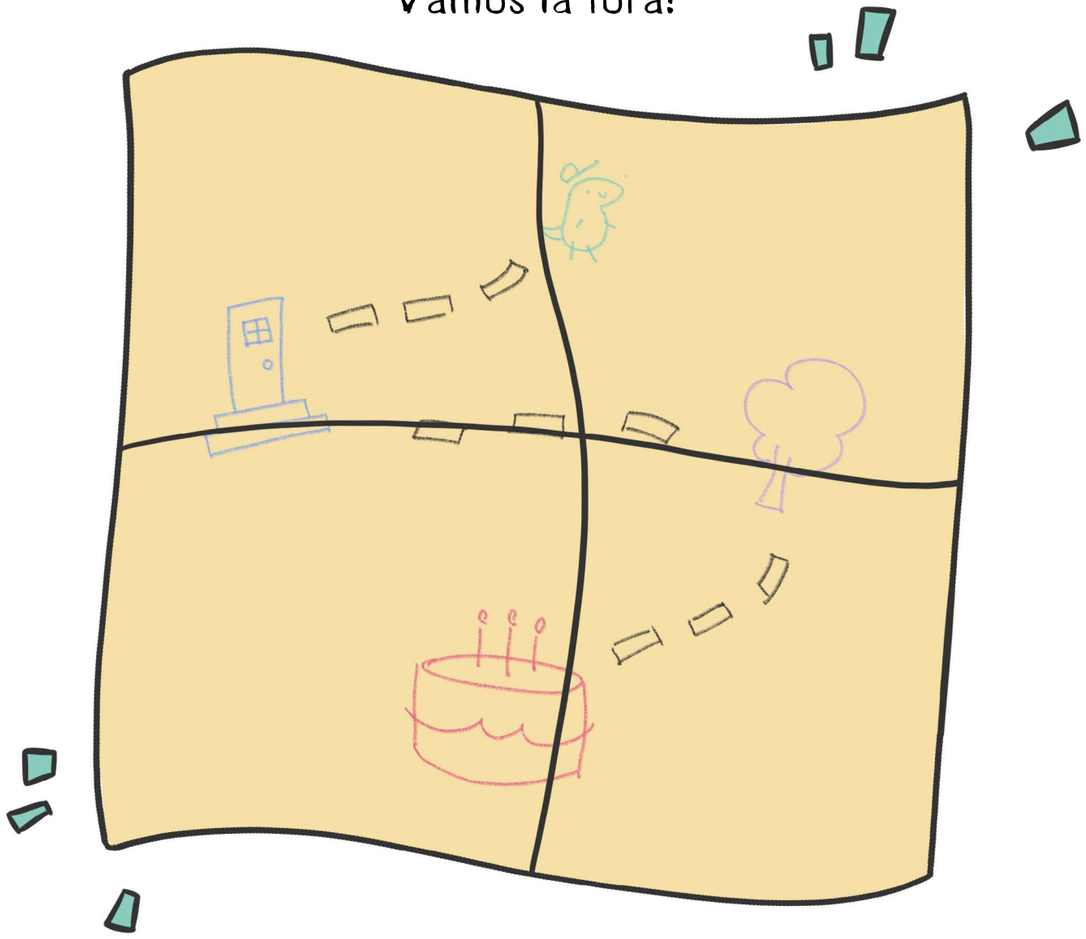
Cada amigo pode achar seu pedaço do mapa do tesouro usando a sua chave no cadeado certo.



Juntando todos os pedaços do mapa,
temos o mapa do tesouro!



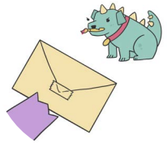
O bolo está no jardim.
Vamos lá fora!



Surpresa!
Feliz Aniversário T-Rex!

GLOSSÁRIO

ASSINATURAS DIGITAIS são mecanismos que dão evidência de que o dado foi criado por uma parte específica (o assinante) e não foi modificado por ele. Na nossa história, cada amigo assina fisicamente o cartão de aniversário para garantir que o T-Rex saiba que veio deles.



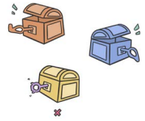
COMPROMISSOS são mecanismos que permitem uma entidade a se comprometer com um pedaço secreto de informação, que poderá ser revelado depois. Na nossa história, isso é feito ao colocarmos o cartão de aniversário em um envelope selado para que o cachorro não consiga adicionar nada mais nele.

Uma **FUNÇÃO HASH** é um objeto matemático que pega uma informação de entrada de tamanho arbitrário e mapeia ela em valores de tamanho fixo. Na nossa história, isso é representado pela imagem de um saco de confeitaria, que tem como entrada uma quantidade de glacê e tem como saída uma quantidade fixa de glacê.

O **MODELO DE COMUNICAÇÃO E DE ADVERSÁRIO** que nós trabalhos é baseado na suposição que a comunicação entre as partes é feita através de um canal inseguro, ou seja, um canal no qual um intruso pode escutar o que é falado ou ainda interferir no conteúdo sendo transmitido. Na nossa história, isso é representado pela presença do cachorro interessado em comer o bolo, e no dinossauro escondendo o bolo do cachorro mudando o bolo de lugar.

SECRET SHARING é o processo de quebrar um segredo em pedaços para que uma quantidade mínima ou todos os pedaços sejam necessários para sua reconstrução. Na nossa história, isso é representado ao quebrarmos o mapa do tesouro em pequenos pedaços, e também é representado ao precisarmos dos amigos cada um com seu pedaço para achar a localização secreta do bolo.

CRIPTOGRAFIA é o processo de usar uma chave para transformar uma informação de forma que o resultado dessa transformação não mostre o conteúdo original, ou seja, a informação é escondida. Na nossa história, isso é representado ao trancar os pedaços do mapa do tesouro em uma caixa.



DESCRIPTOGRAFIA é o processo reverso da criptografia, no qual permite recuperar a informação com a ajuda de uma chave secreta . Na nossa história, isso é representado ao destrancar os cadeados das caixas usando a chave correta.

CHAVE SIMÉTRICA é uma informação secreta ou um valor secreto usado no processo de criptografar e descriptografar. Na nossa história, a mesma chave é usada para trancar e destrancar a caixa.

CHAVES ASSIMÉTRICAS são pares de valores. Um valor é público e usado para criptografar e o outro valor é secreto, usado para descriptografar. Na nossa história, o Triceratops pensa em usar cadeados para trancar as caixas. O cadeado é público, todos podem utilizá-lo para criptografar (porque uma chave secreta não é necessária para trancá-lo), mas apenas o dinossauro com a chave secreta certa consegue destrancar esse cadeado.

Para mais informações sobre esses conceitos, e sobre criptografia como um todo, visite, por favor, https://www.cybok.org.

RECURSOS ADICIONAIS (em inglês)

Uma introdução aos conceitos e construções criptográficas.

Um webinar CyBOK introduzindo criptografia.

Um podcast CyBOK introduzindo criptografia.