APRENDENDO JUNTOS

CRIPTOGRAFIA PARA INFANTES

escrito por Elizabeth A. Quaglia
ilustrado por Alex Thompson

APRENDENDO JUNTOS

CRIPTOGRAFIA PARA INFANTES

ELIZABETH A. QUAGLIA é Professora Associada no Information Security Group da Universidade Royal Holloway de Londres. A sua área de investigação é CiberSegurança, com foco em Criptografia. Tem dois filhos Ale e Leo, que adoram comer bolo.

ALEX THOMPSON é uma designer de produtos digitais com um talento para a ilustração. Quando não está a desenhar dinossauros, trabalha no desenvolvimento de ferramentas comerciais e de marketing em Londres.
Encontre-a em @userologist.

Este livrete foi criado com o apoio de
DRª. VALENTINA ZAMBON, psicóloga
e MICHELE VILLA, designer.

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

CYBOK Crown Copyright, The National Cyber Security Centre 2022, licenciado sob Open Government License http://www.nationalarchives.gov.uk/doc/open-govenment licence/

Adaptado para português por
AP2SI - Associação Portuguesa para a Promoção da Segurança da Informação
https://ap2si.org

COMO LER ESTE LIVRETE

Com este livrete queremos proporcionar uma oportunidade para que crianças e adultos possam aprender juntos sobre criptografia.

Para que as crianças entendam os conceitos, sugerimos que os adultos se envolvam na leitura, descrição e discussão da história contada nas páginas seguintes.

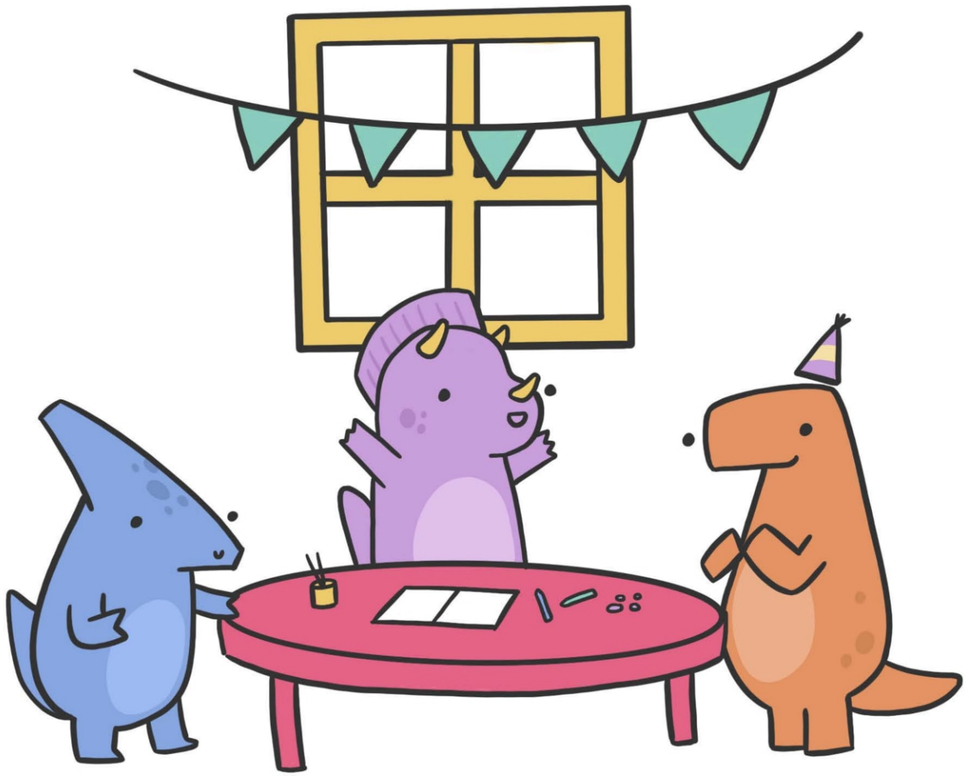
Questões como "Onde está o cão?" ou "O que é que o cão está a tentar fazer?" podem ser uma forma de envolver as crianças.
Portanto... façam muitas perguntas!

Por exemplo, na página 7, porque é que o postal de aniversário é colocado num envelope? E, na página 13, porque é que o bolo está tapado? Também na página 17, o que acontece se forem descobertas apenas duas peças do mapa do tesouro? E nas páginas 19 e 22, porque é que é melhor não ter uma chave secreta para proteger as quatro chaves?

Para os adultos, é fornecido um glossário no final do livrete, com definições da terminologia da criptografia que é utilizada durante a nossa história, bem como ligações (em inglês) de recursos adicionais para uma aprendizagem futura sobre o tópico.

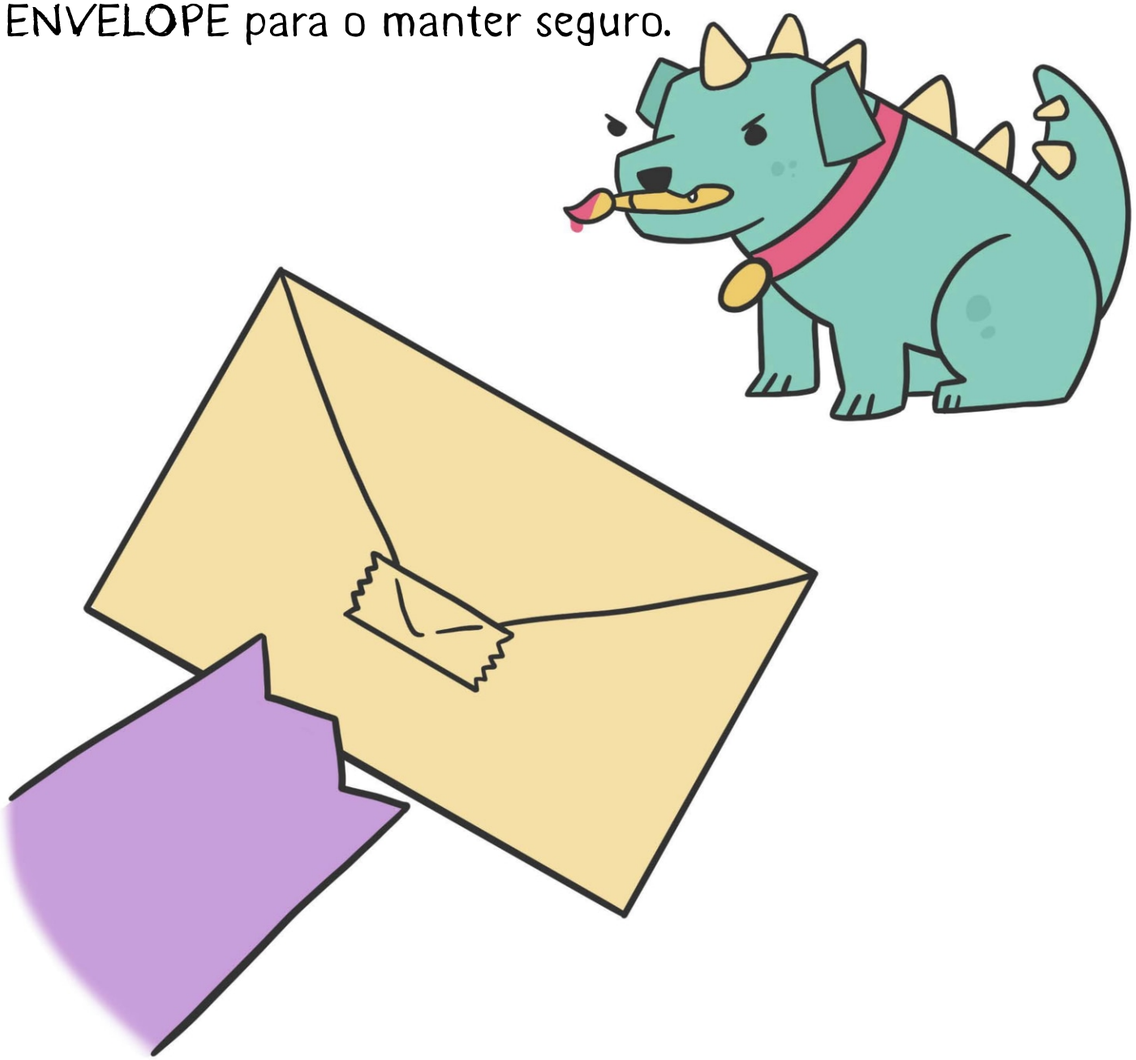
O ANIVERSÁRIO do T-Rex é hoje!

Vamos fazer uma festa surpresa de aniversário para o T-Rex!

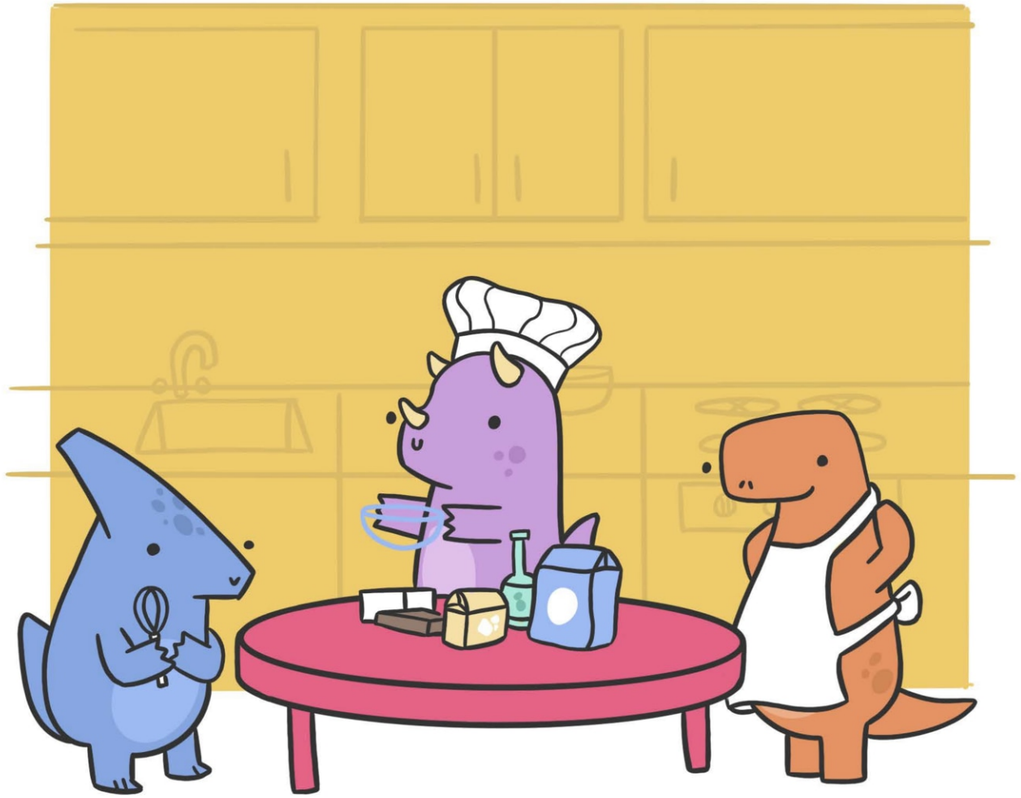


Vamos ASSINAR o
postal de aniversário!

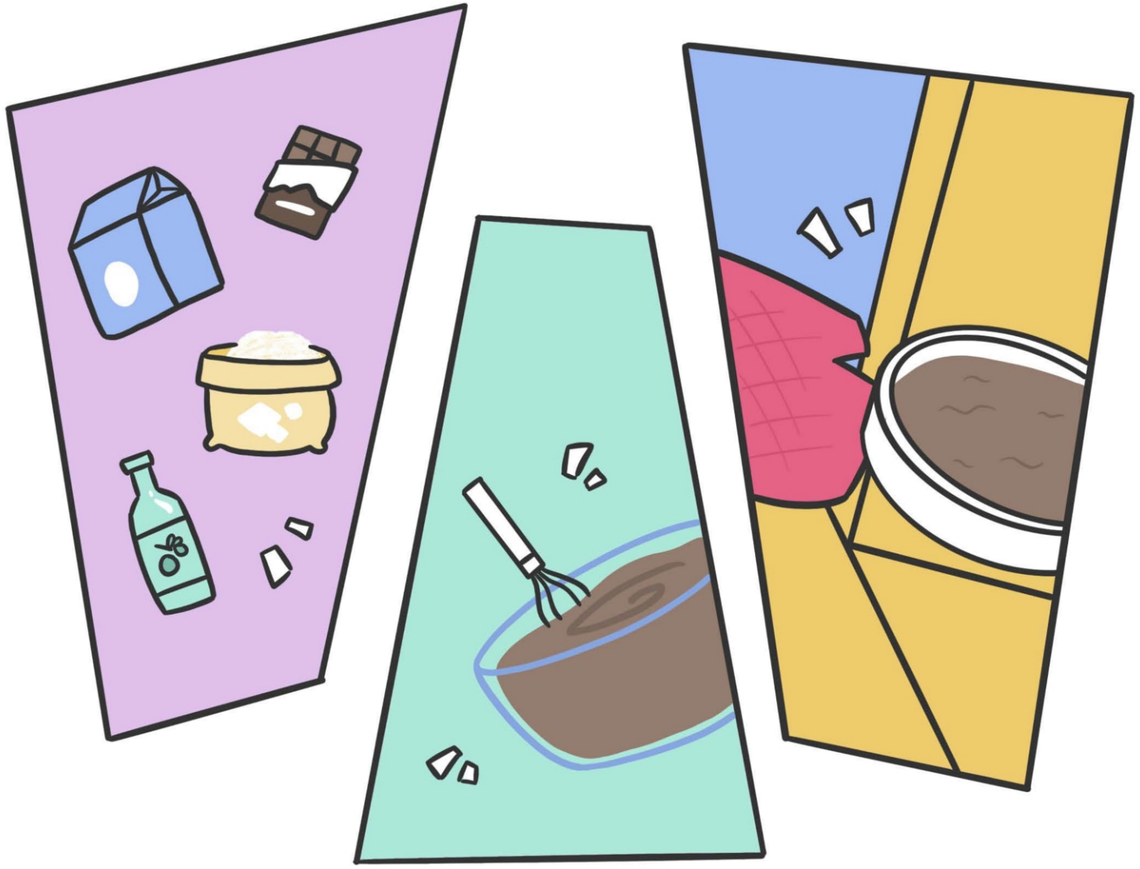
Vamos colocar o postal num
ENVELOPE para o manter seguro.



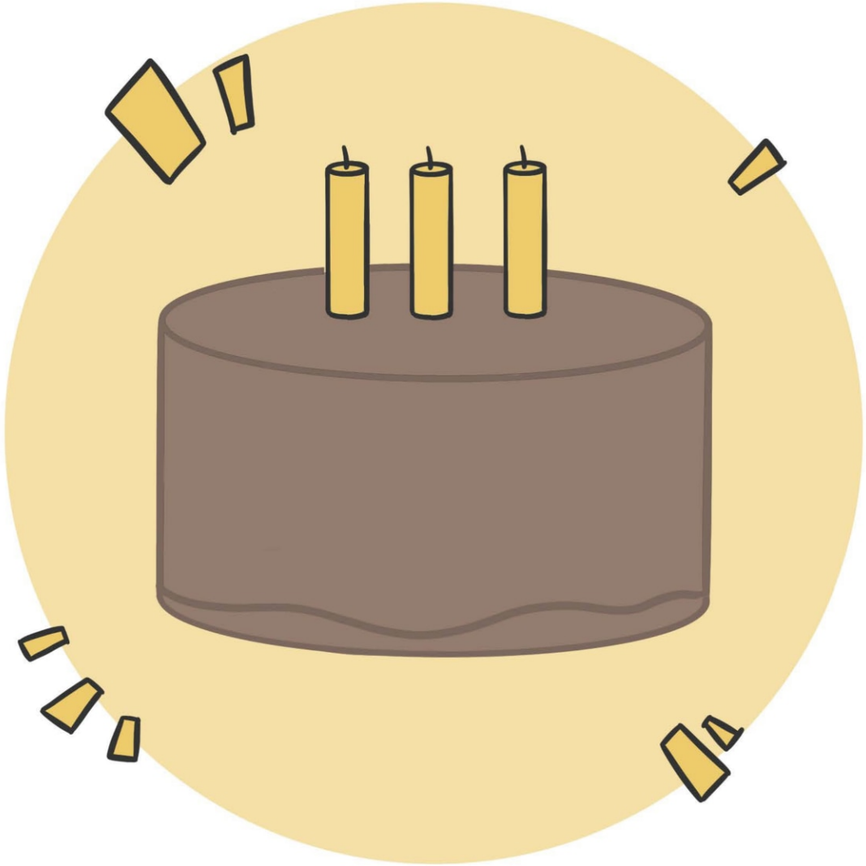
E agora vamos fazer um bolo de aniversário!



Vamos misturar os ingredientes
e colocar a massa no forno!

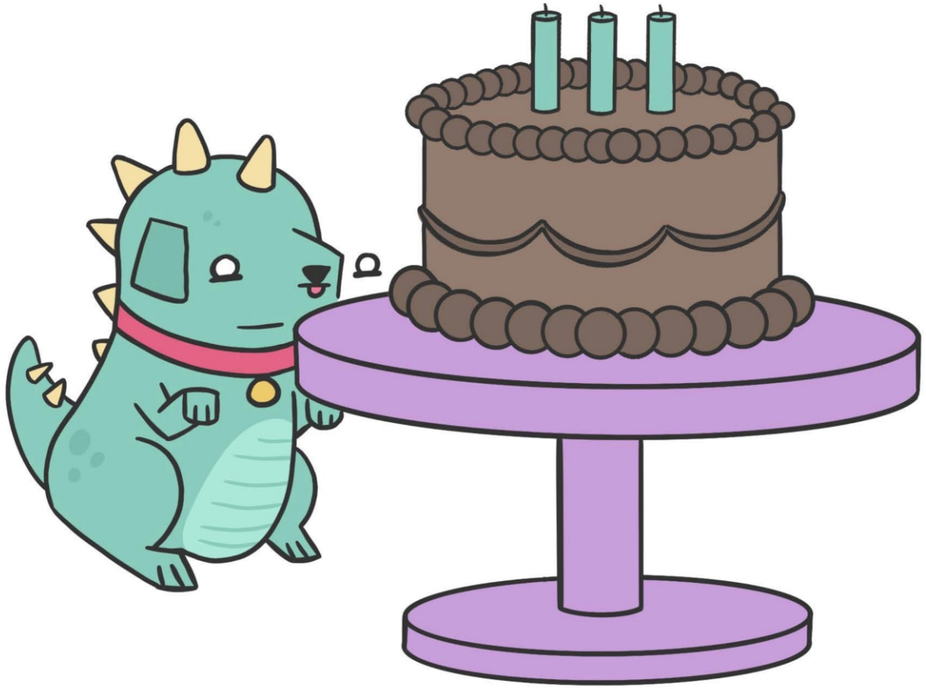


E aqui está o bolo!

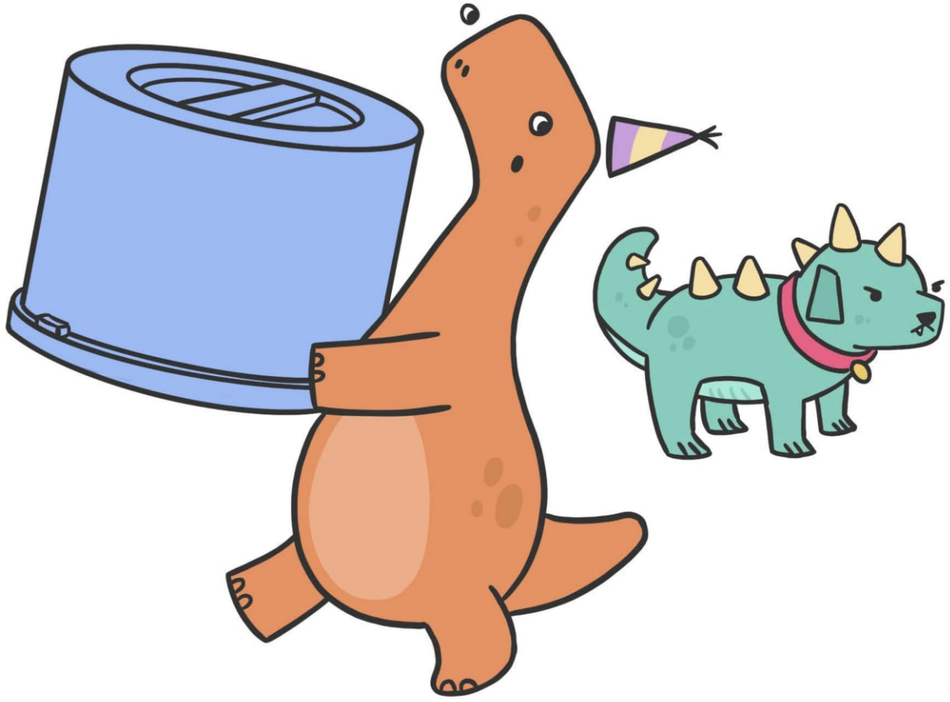


Vamos dar-lhe um toque final.
Como é que podemos decorar o bolo?

O cão está interessado num pedaço do bolo.

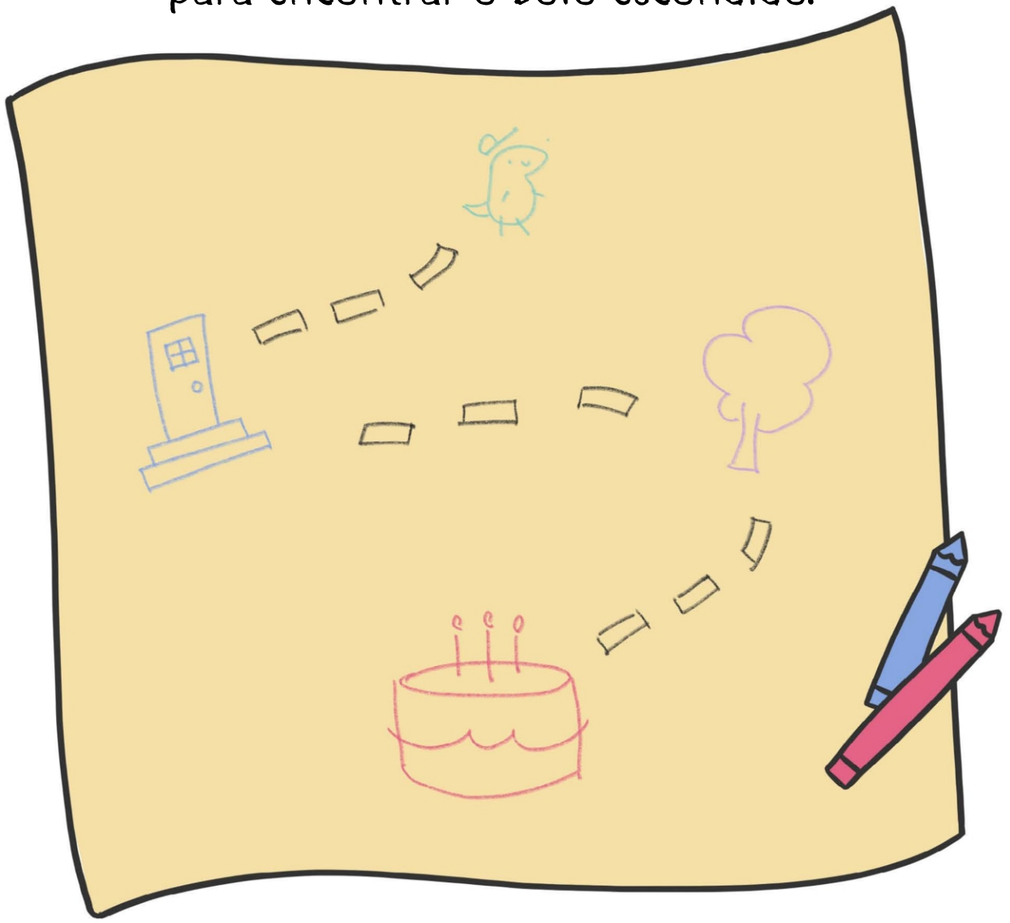


É melhor ESCONDERMOS o bolo!



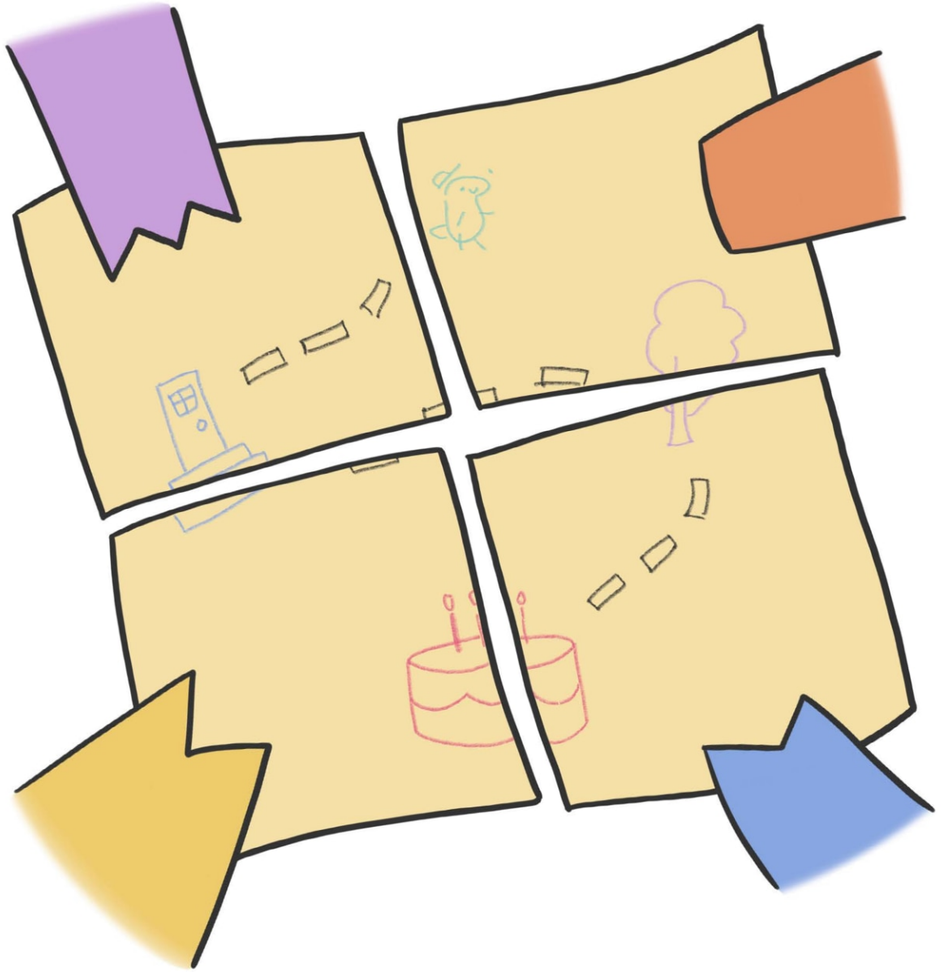
O T-Rex chegou!
Agora vamos jogar um jogo. Encontrar o bolo!

Este é o mapa do tesouro
para encontrar o bolo escondido.

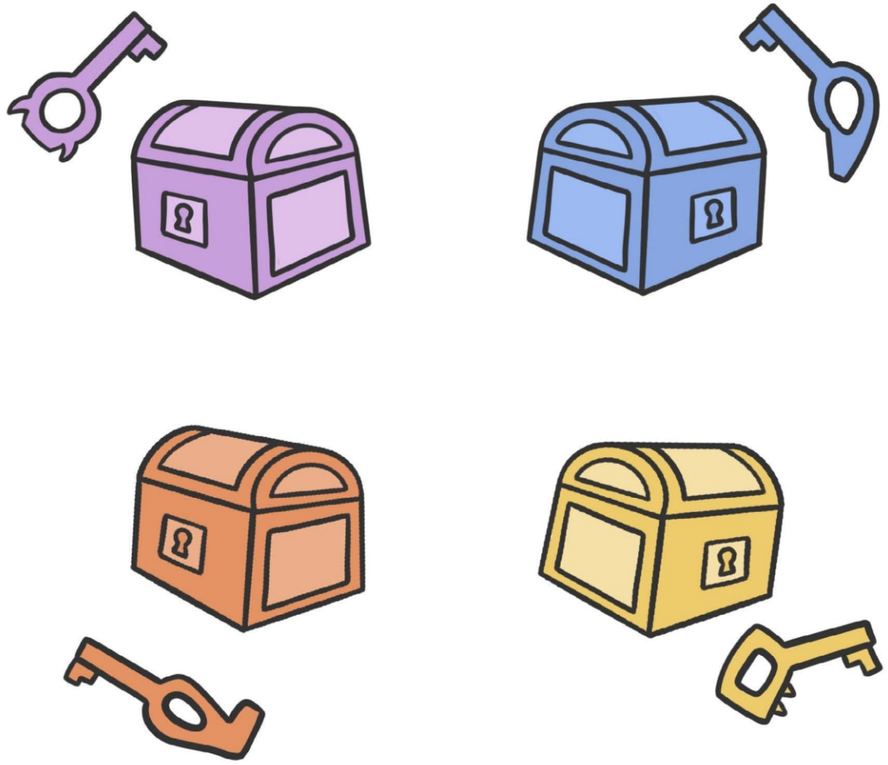


Todos ficam com UM
pedaço do mapa.

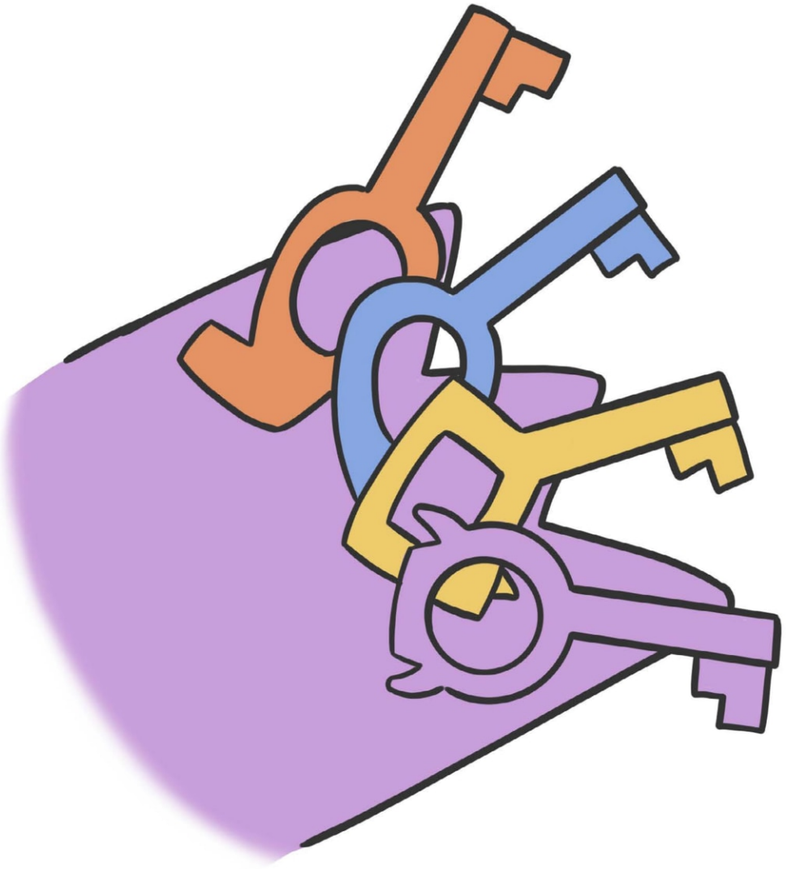
TODOS os pedaços são necessários
para descobrir onde está o bolo!



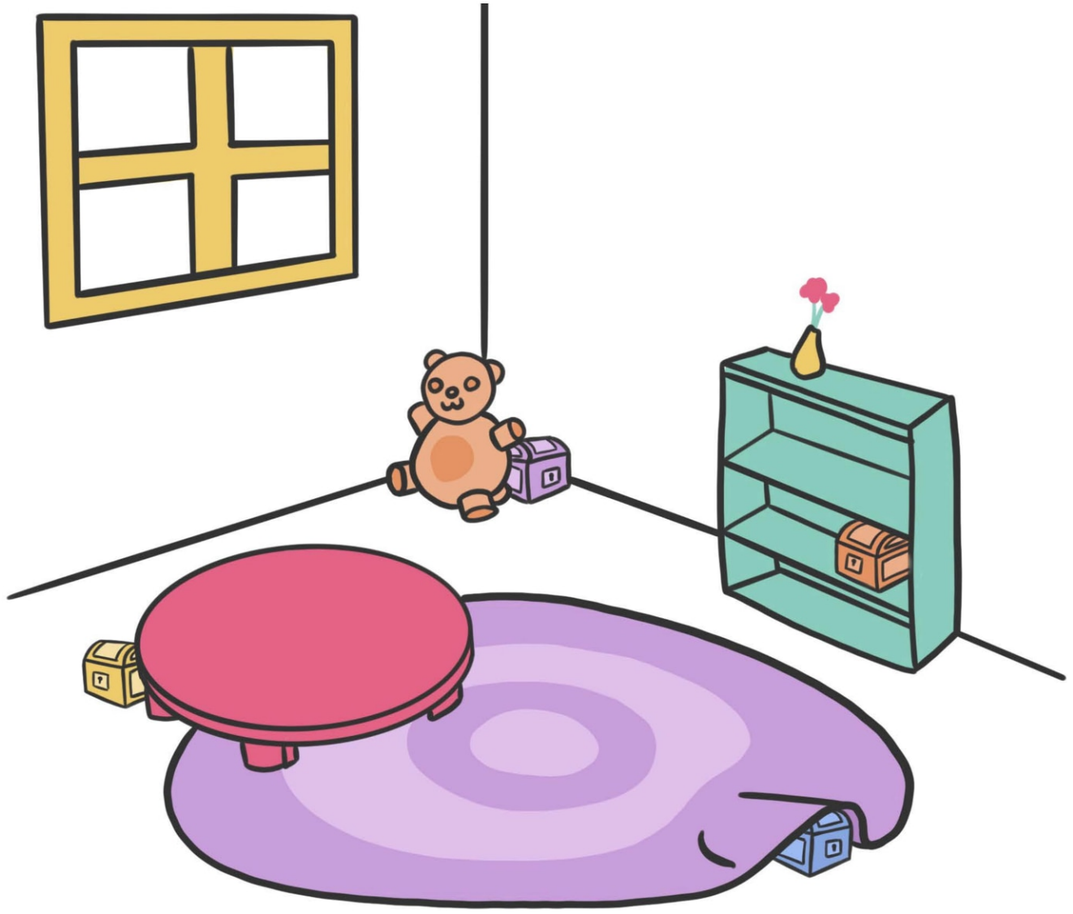
O Triceratops colocou cada uma das peças do mapa numa caixa, e usou uma chave diferente para cada uma.



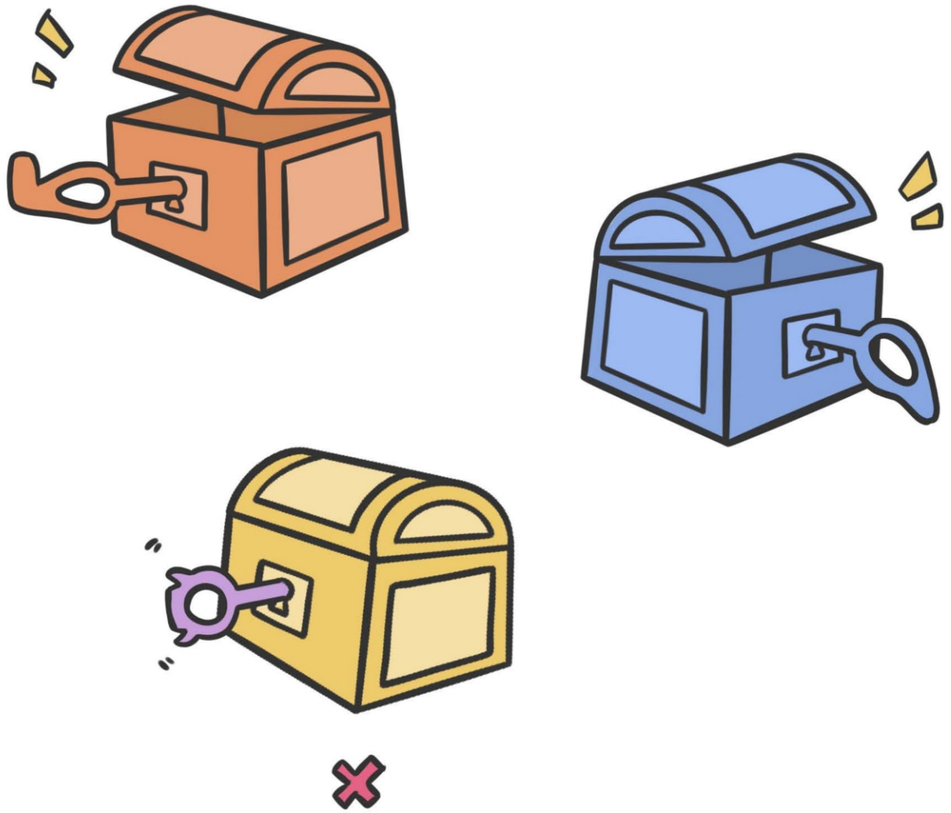
O Triceratops precisa de manter as **QUATRO** chaves seguras!



Agora todos precisam de encontrar as caixas!



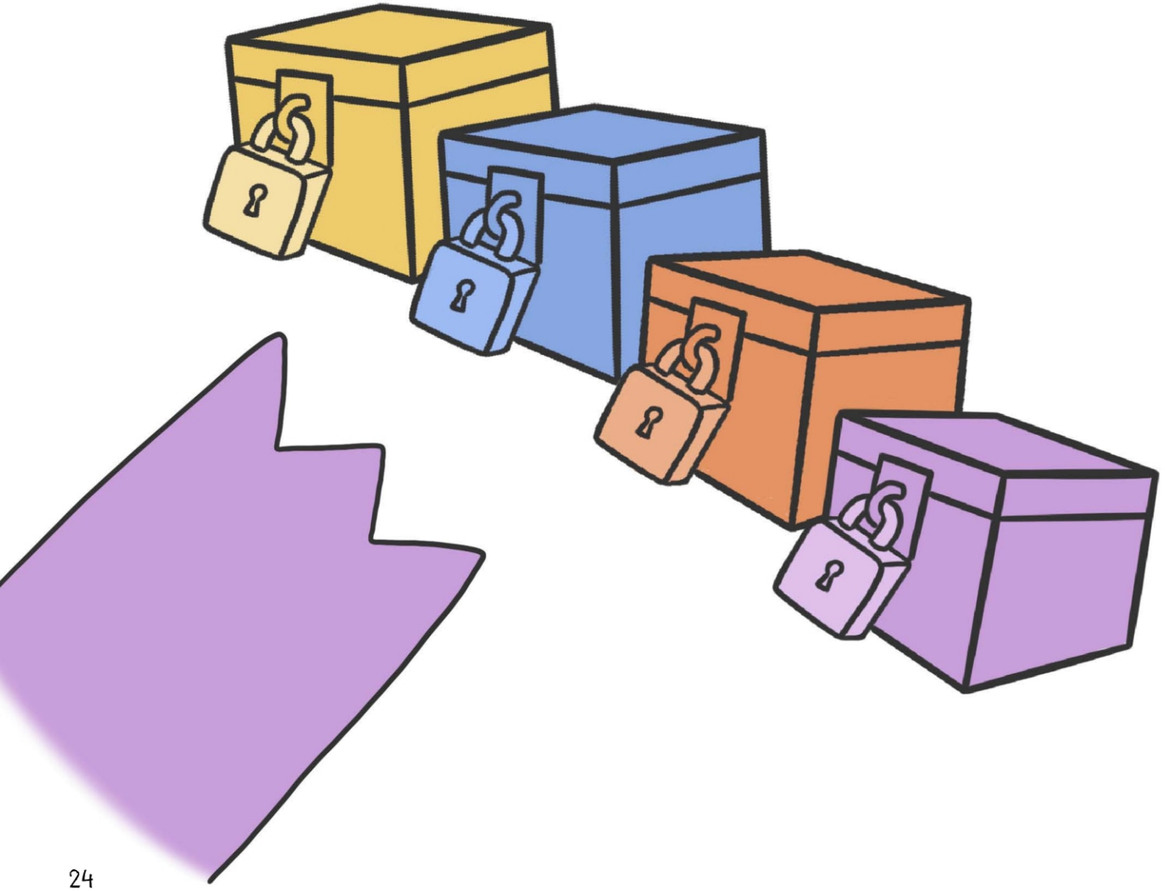
Para abrir uma caixa, precisam
da chave com a MESMA cor!



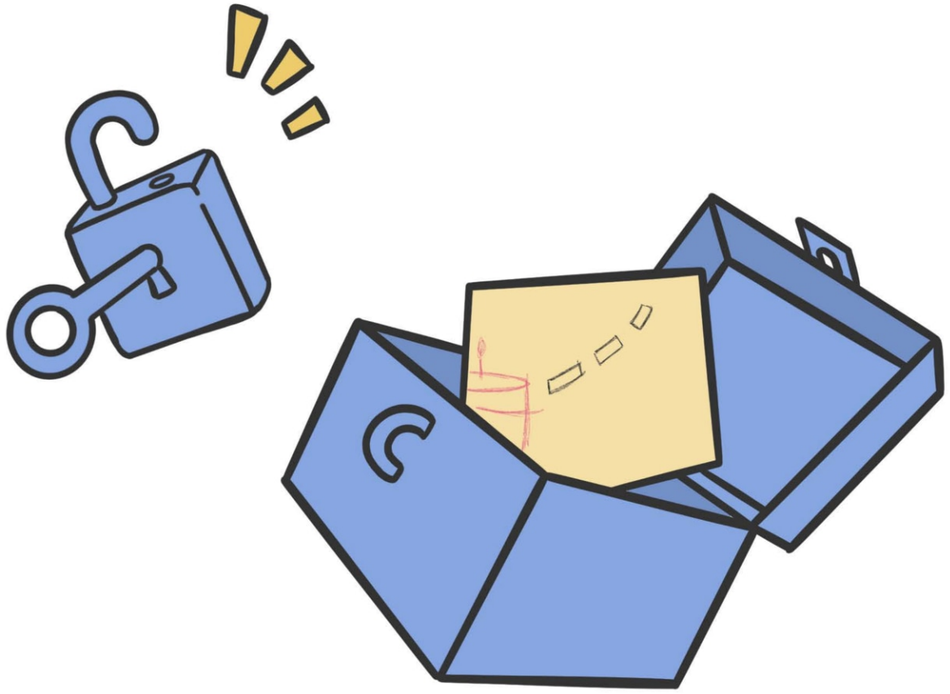
Será que o Triceratops
consegue fechar as caixas
SEM PRECISAR
de chaves secretas?

Isto é um CADEADO.
Não precisa de uma chave para fechar.
Apenas para abrir.

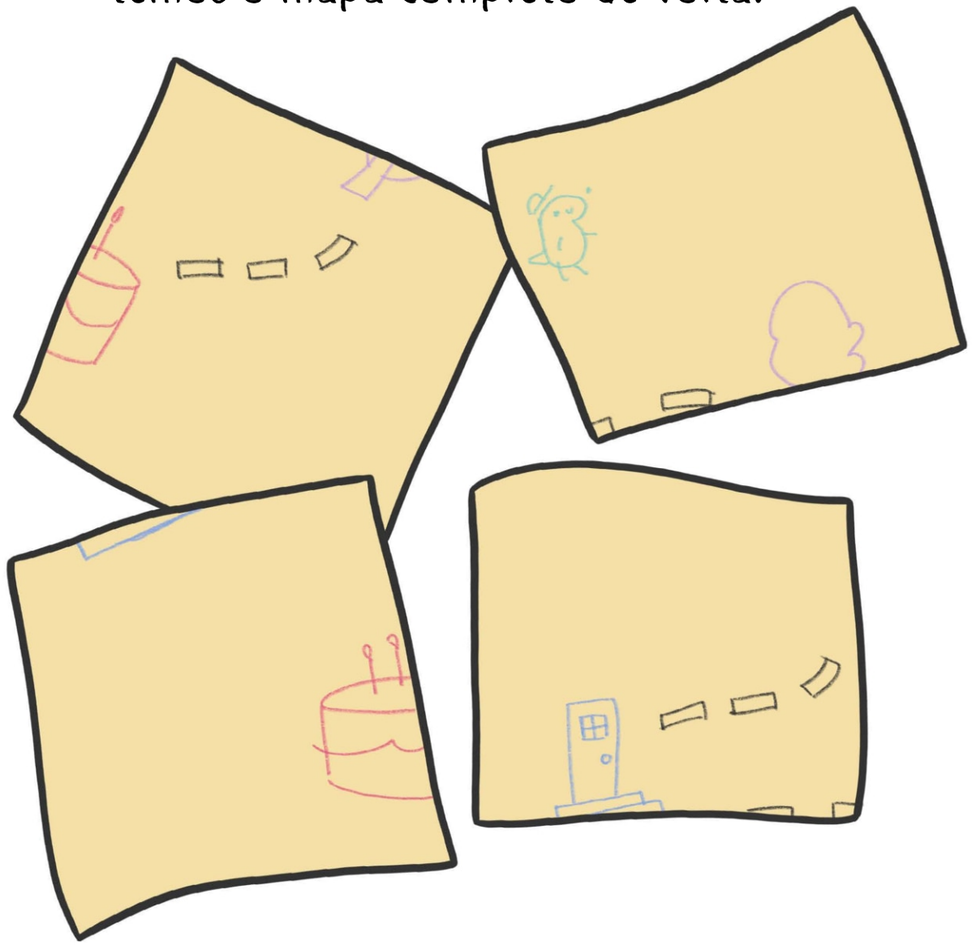
O Triceratops pode agora fechar todas as caixas sem precisar de NENHUMA chave secreta!



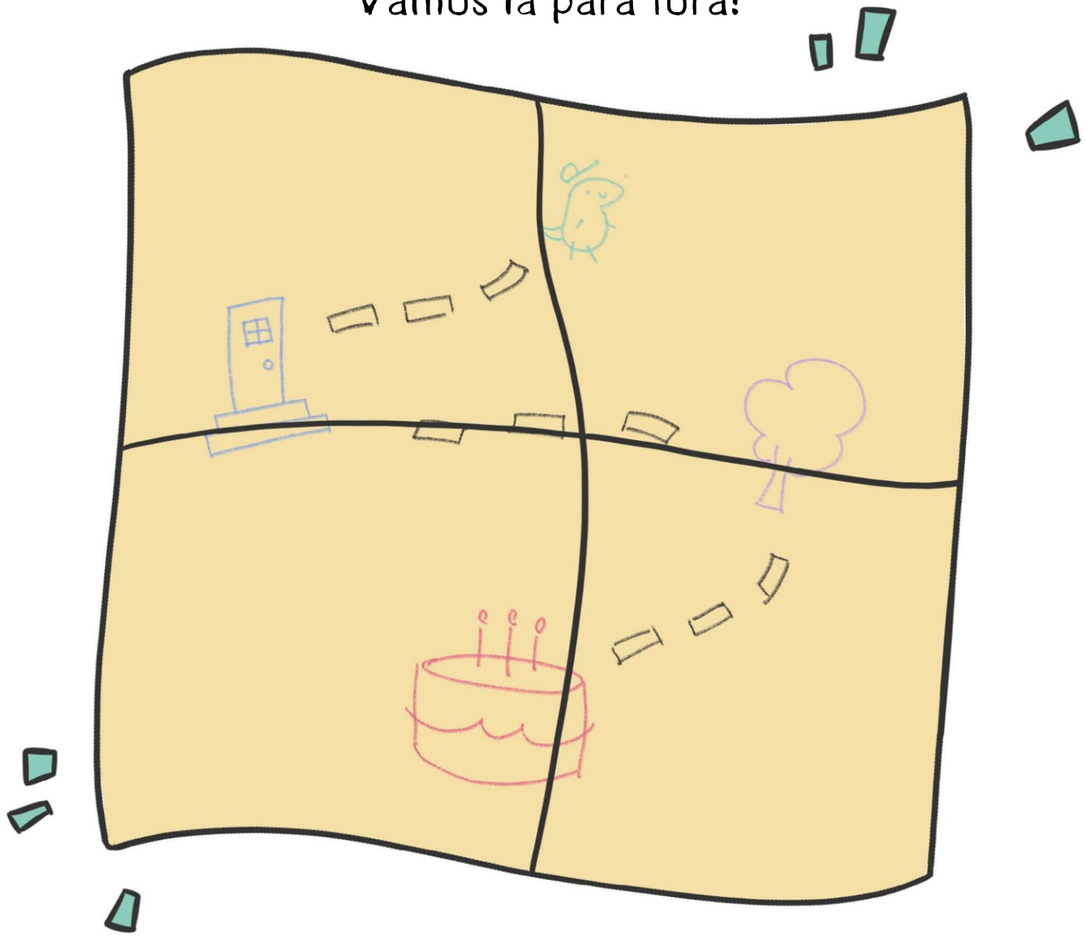
Cada um dos amigos pode ter acesso à sua peça do mapa com a sua chave para abrir o cadeado correspondente.



Juntando as peças todas
temos o mapa completo de volta!



O bolo está no jardim!
Vamos lá para fora!



Surpresa!
Feliz Aniversário T-Rex!

GLOSSÁRIO

ASSINATURAS DIGITAIS são um mecanismo para demonstrar que os dados foram criados por uma entidade específica (o signatário) e não foram modificados. Na nossa história, cada amigo assina fisicamente o cartão de aniversário para garantir que o T-Rex saiba que é deles.

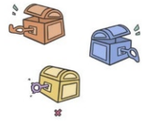
COMPROMISSOS são um mecanismo que permite a uma entidade comprometer-se com alguma informação secreta, que pode ser revelada posteriormente. Na nossa história, isso é representado colocando o postal de aniversário num envelope fechado, para que o cão não possa adicionar nada posteriormente.

Uma **FUNÇÃO DE HASH** é uma função matemática que recebe como entrada informações de tamanho arbitrário e converte-as para valores de tamanho fixo. Representamos isso pela imagem de um saco de pasteleiro, que recebeu como entrada uma quantidade de cobertura que foi usada para uma decoração de tamanho fixo à volta do bolo.

O **MODELO DE COMUNICAÇÃO E ADVERSÁRIO** com o qual trabalhamos baseia-se na suposição de que a comunicação entre as partes é feita por meio de um canal inseguro, ou seja, um canal no qual um adversário pode interceptar e até interferir no conteúdo transmitido. Na nossa história, isto é representado pela presença do cão, interessado em comer o bolo, e pelo dinossauro escondendo o bolo do cão.

A **PARTILHA DE SEGREDO** é o processo de dividir um valor secreto em pedaços, de modo a que todos os pedaços (ou um número mínimo) sejam necessários para a sua reconstrução. Representámos isso dividindo o mapa do tesouro em pedaços e tornando necessário que todos os amigos contribuam com a sua parte para encontrarem a localização secreta do bolo.

CIFRAR é o processo de usar uma chave para transformar informações de modo que o resultado da transformação não revele o conteúdo original, ou seja, as informações estão ocultas. Na nossa história, isso é representado ao colocar os pedaços do mapa do tesouro dentro das caixas deixando de ser possível ver o conteúdo.



DECIFRAR é o processo reverso da cifra, que permite recuperar as informações com a ajuda de uma chave secreta. Na nossa história, isso é representado ao abrir as caixas trancadas, usando a chave correta e tornando a ser possível ver o seu conteúdo.

A **CHAVE SIMÉTRICA** é uma informação ou valor secreto utilizado tanto para cifrar como para decifrar. Na nossa história, a mesma chave é usada para trancar e destrancar a caixa.

As **CHAVES ASSIMÉTRICAS** são um par de valores em que um dos valores é público e é usado para cifrar, enquanto o outro é secreto e é usado para decifrar. Na nossa história, o Triceratops pensa em usar cadeados para fechar as caixas. O cadeado é público, qualquer um pode usá-lo para cifrar (porque uma chave secreta não é necessária para trancá-lo), mas apenas o dinossauro com a chave correta pode destrancá-lo.

RECURSOS ADICIONAIS

(em inglês)

Uma introdução aos conceitos e construções da criptografia

Um webinar CYBOK de introdução à criptografia

Um podcast CYBOK de introdução à criptografia