LEARNING TOGETHER

CRYPTOGRAPHY FOR TODDLERS

written by Elizabeth A. Quaglia
illustrated by Alex Thompson

LEARNING TOGETHER

CRYPTOGRAPHY FOR TODDLERS

ELIZABETH A. QUAGLIA is Associate Professor in the Information Security Group at Royal Holloway, University of London. Her research area is Cyber Security, with a focus on Cryptography. She is a mum of two toddlers, Ale and Leo, who love eating cake.

ALEX THOMPSON is a digital product designer with a knack for illustration. When she isn't drawing dinosaurs, she's working to build international commerce and marketing tools in London.
Find her at @userologist.

This booklet has been created with the help of
DR. VALENTINA ZAMBON, psychologist,
and MICHELE VILLA, designer.

We also thank DR. JORGE BLASCO ALIS
and DR. JASSIM HAPPA for their advice and support.

HOW TO READ THIS BOOK

With this booklet we want to provide an opportunity for children and grown-ups to learn together about cryptography.

To help children understand the concepts, we suggest the grown-ups involve them in the description and discussion of the story in the following pages.

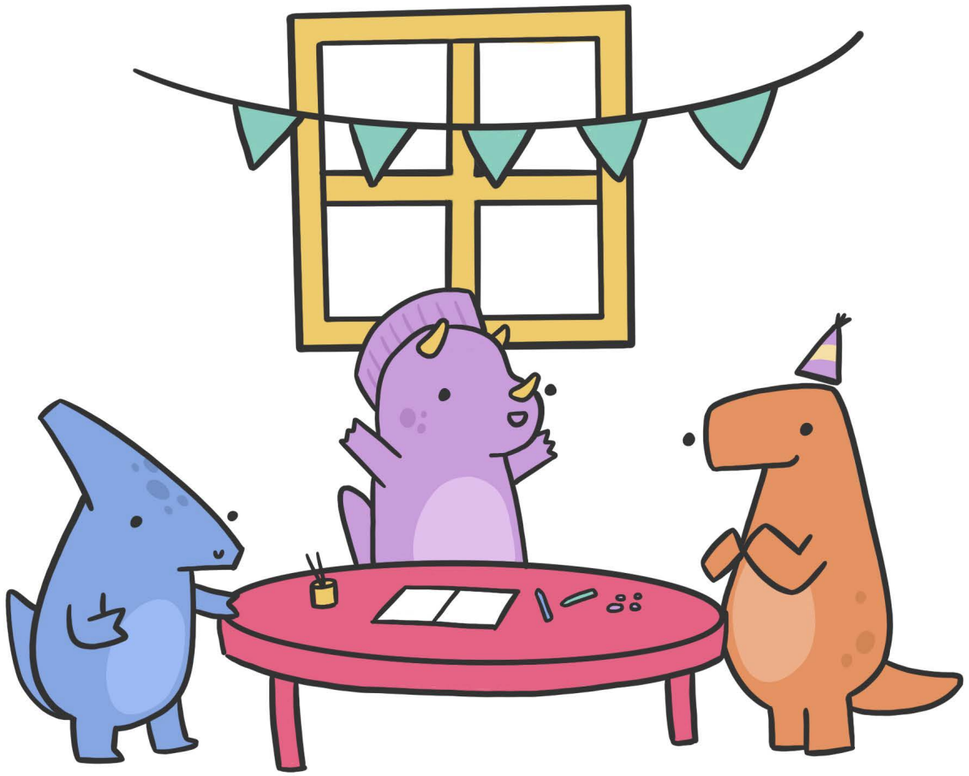
Questions like "Where is the dog?" or "What is the dog trying to do?" can be a useful way to engage the children. So… ask lots of questions!

For example, on page 7, why is the birthday card put in an envelope? And similarly, on page 13, why is the cake being covered? Further, on page 17, what happens if only two pieces of the treasure map are found? And on page 19 and 22, why is not needing a secret key better than keeping four keys safe?

For the grown-ups, a glossary is provided at the end of the booklet, defining the cryptographic terminology we capture in our story and providing links to additional resources for further learning on the topic.

It's T-Rex's BIRTHDAY today!

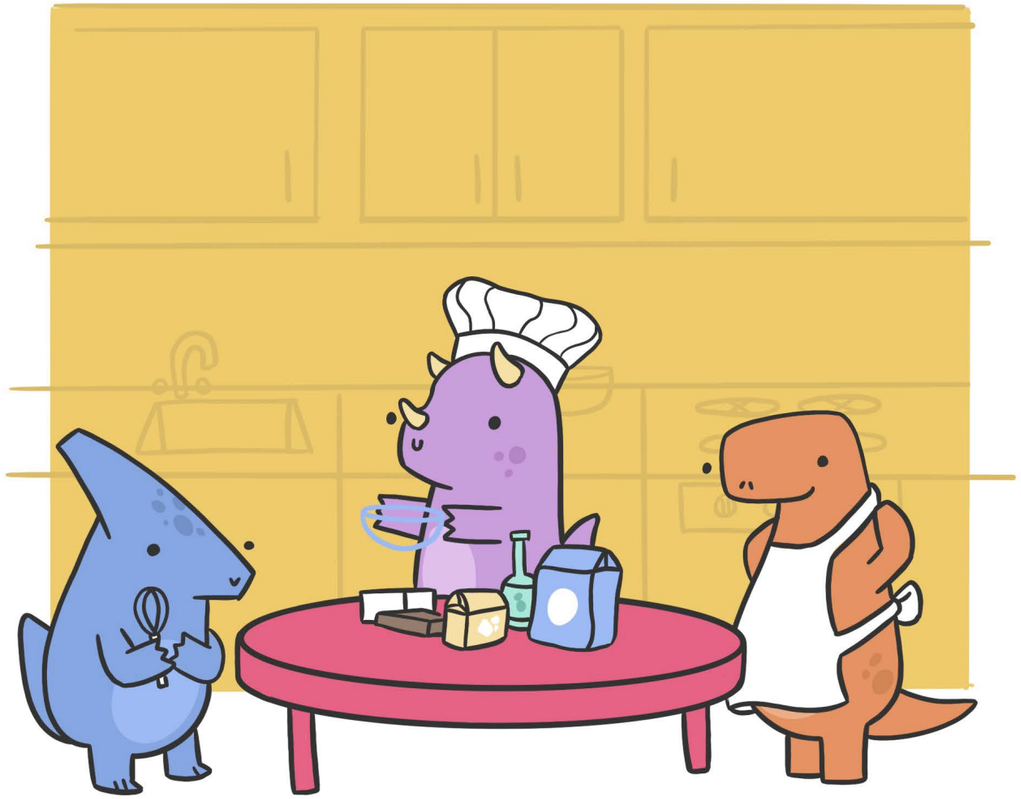
Let's throw T-Rex a surprise birthday party!



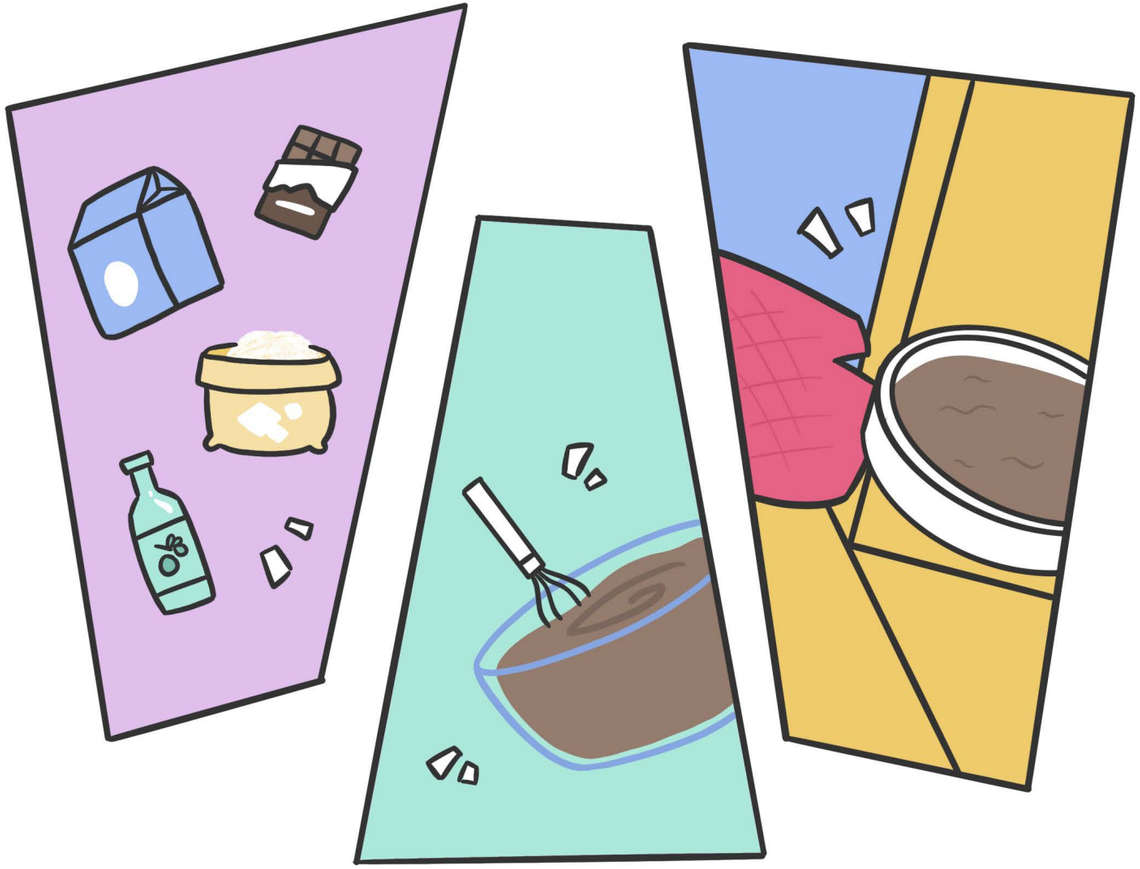
Let's SIGN the birthday card!

Let's put the card in an ENVELOPE to keep it safe.

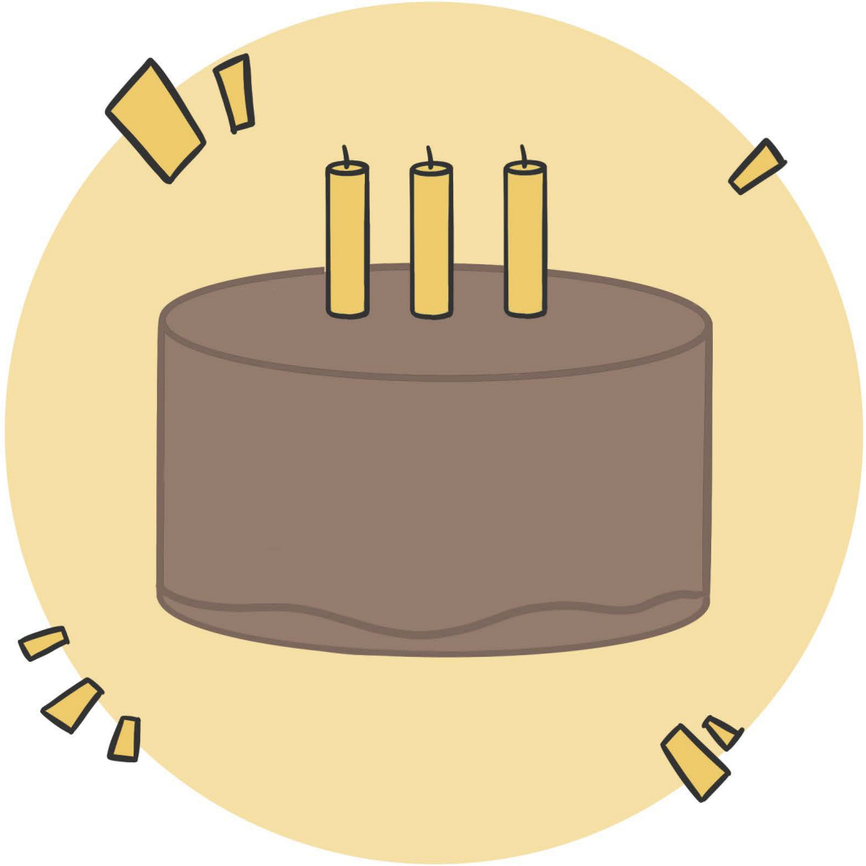
And now let's bake a birthday cake!



Let's mix the ingredients together
and put the mix in the oven!

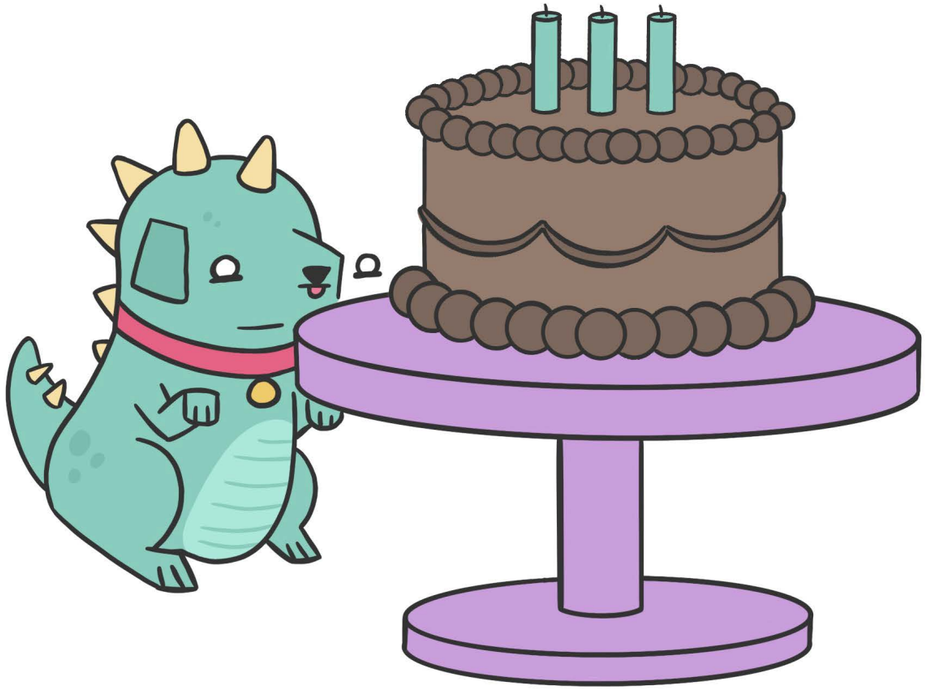


And here is the cake!

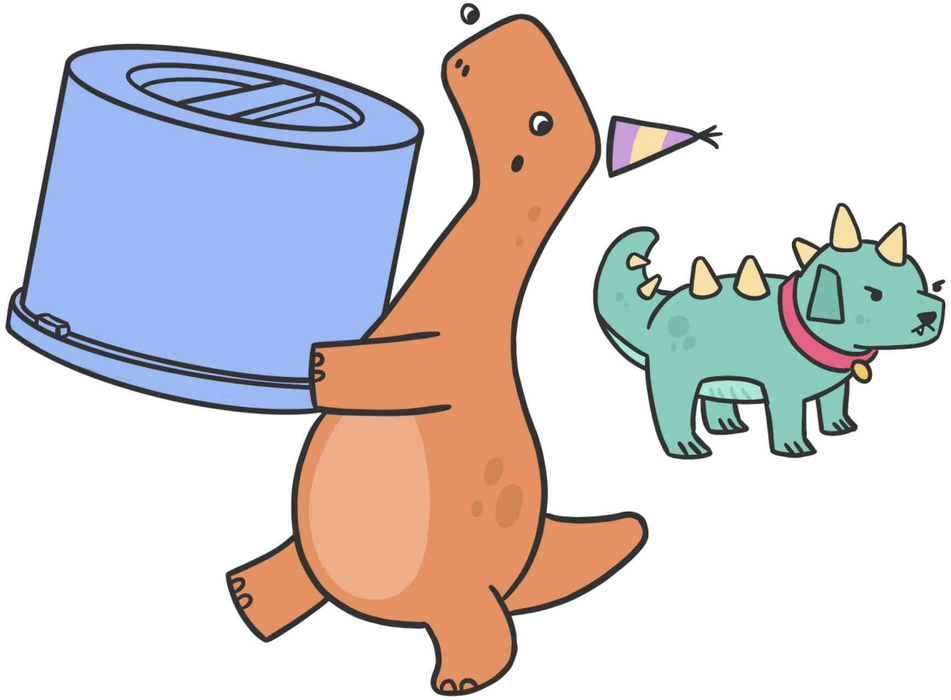


Let's give it a final touch.
How can we decorate the cake?

The dog would like a piece of the cake.



We'd better HIDE the cake!

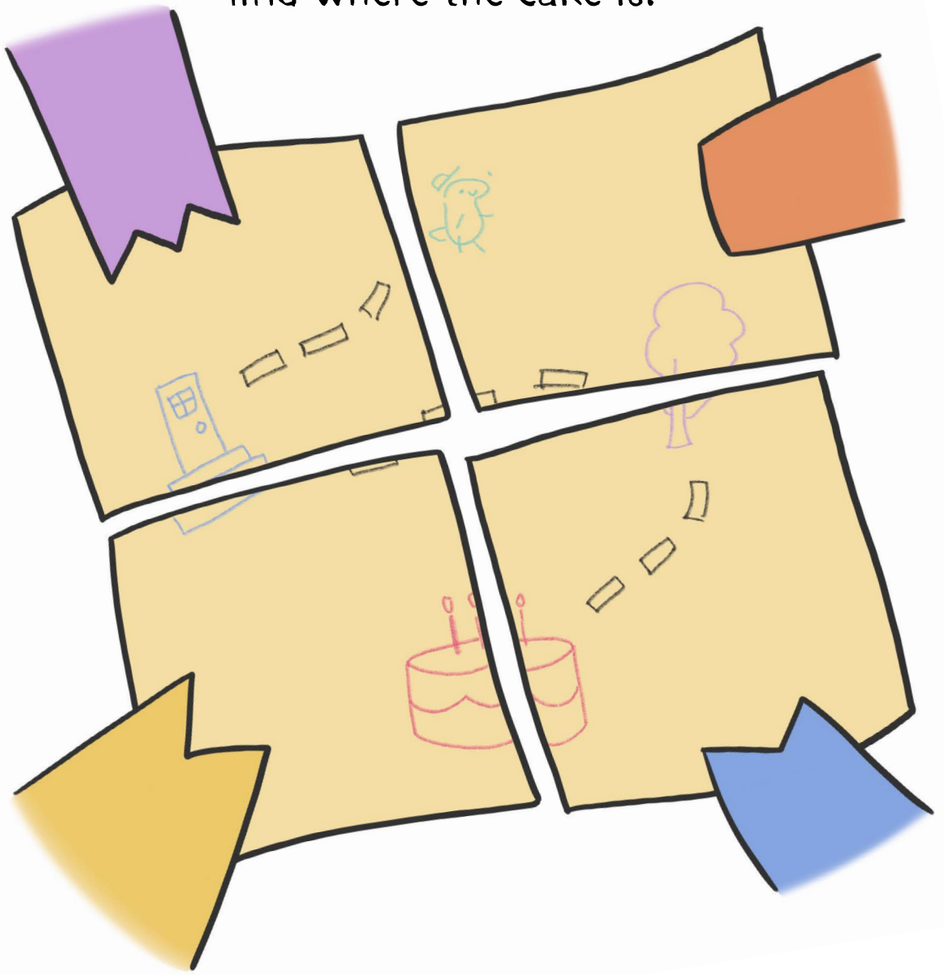


T-Rex has arrived!
Let's play a game now. Find the cake!

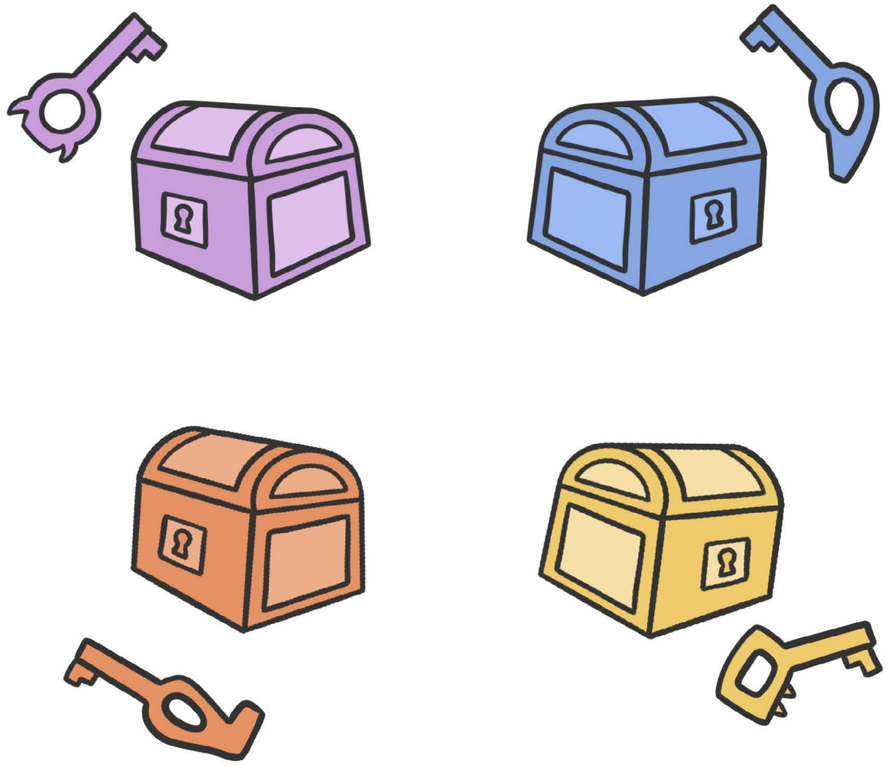
This is the treasure map
to find the hidden cake.

Everyone gets ONE piece
of the treasure map.

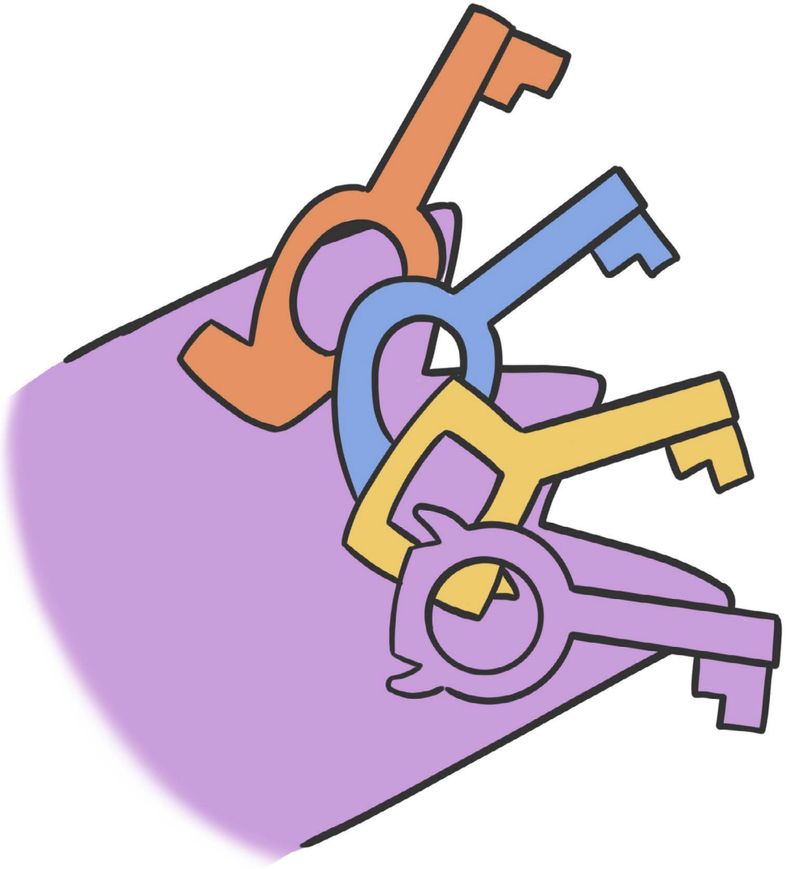
ALL pieces are needed to
find where the cake is!



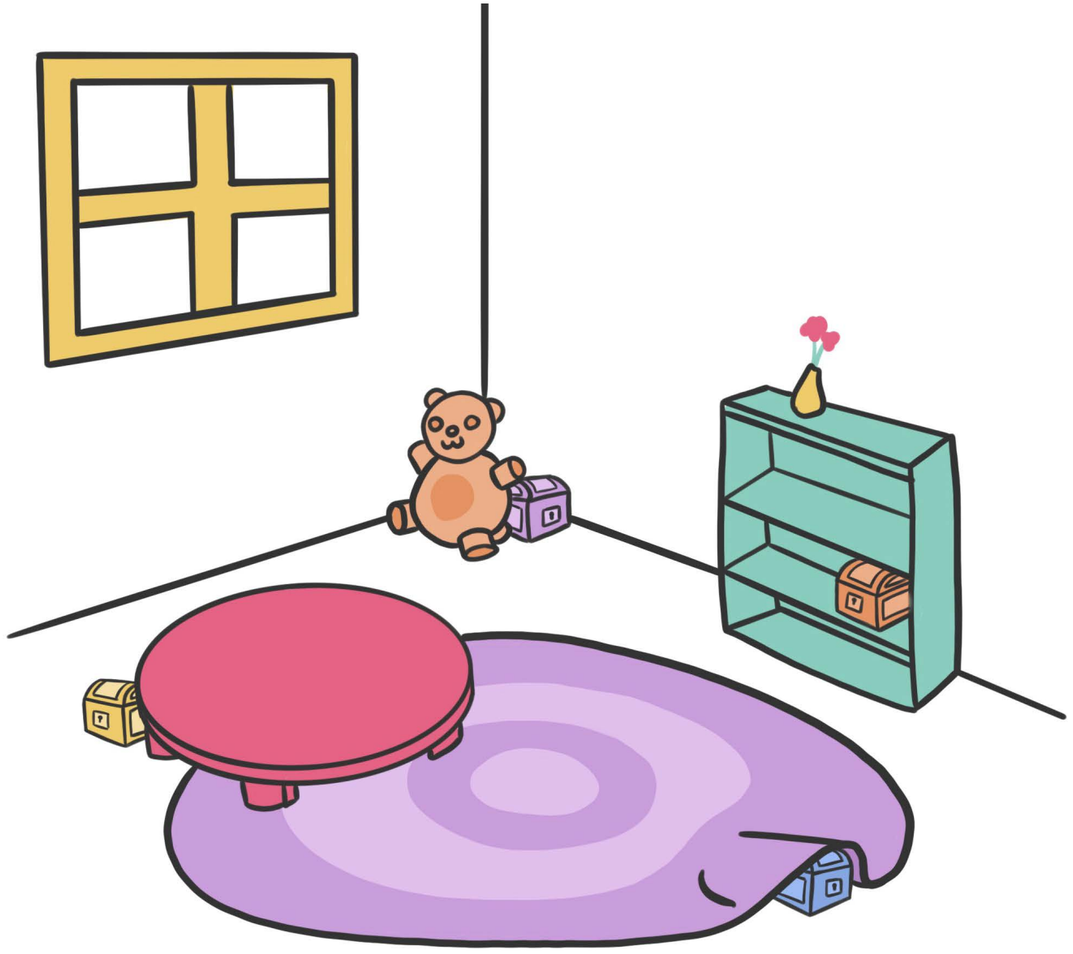
Triceratops locks each piece in a box,
using a different key for every box.



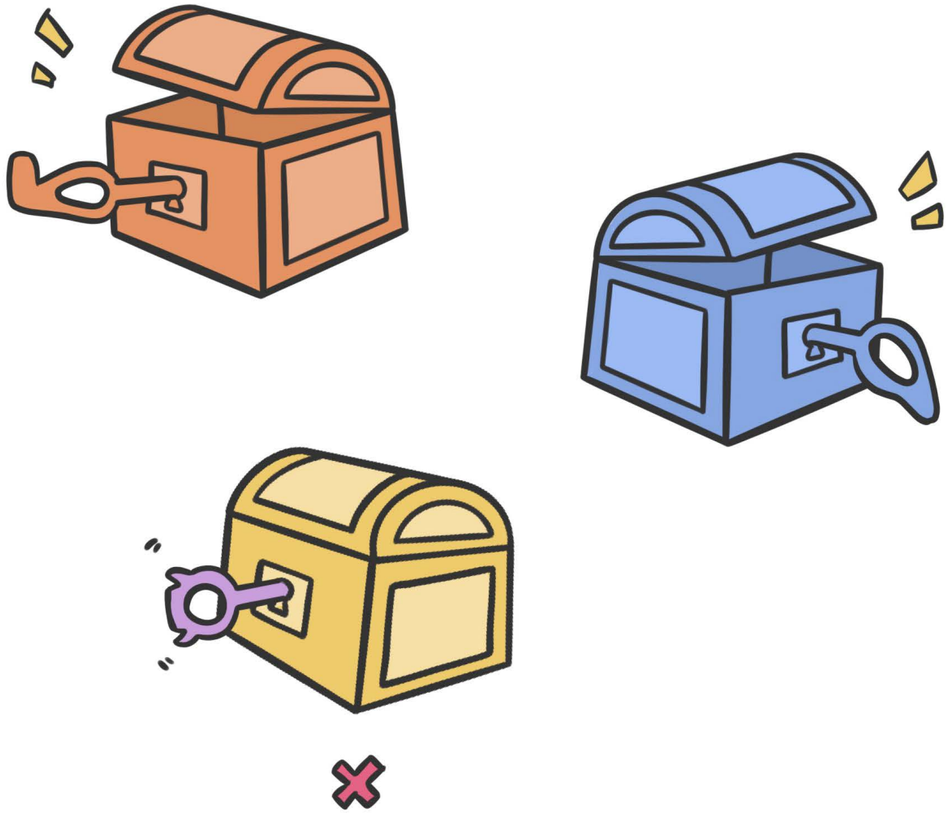
Triceratops needs to keep
FOUR keys safe!



Everyone needs to find their box!



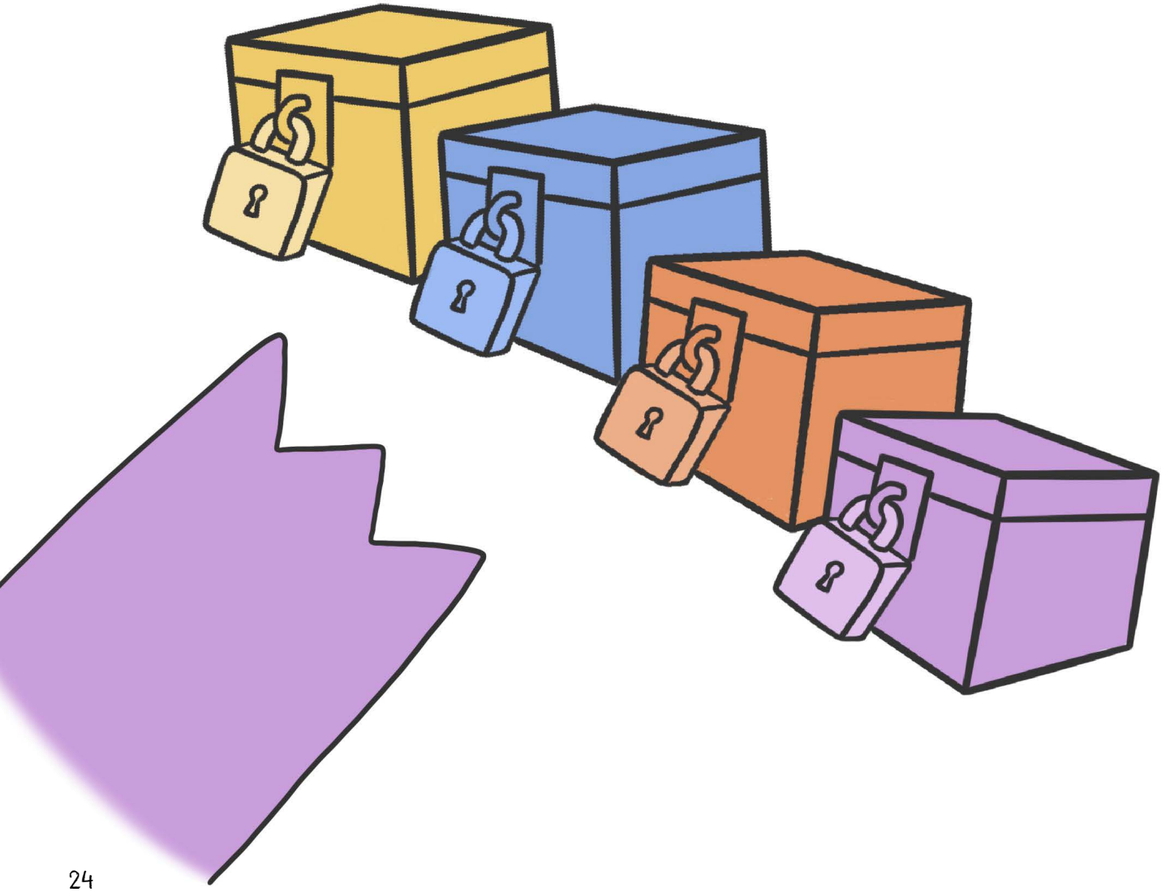
To open the box, you need the SAME key that locked it!



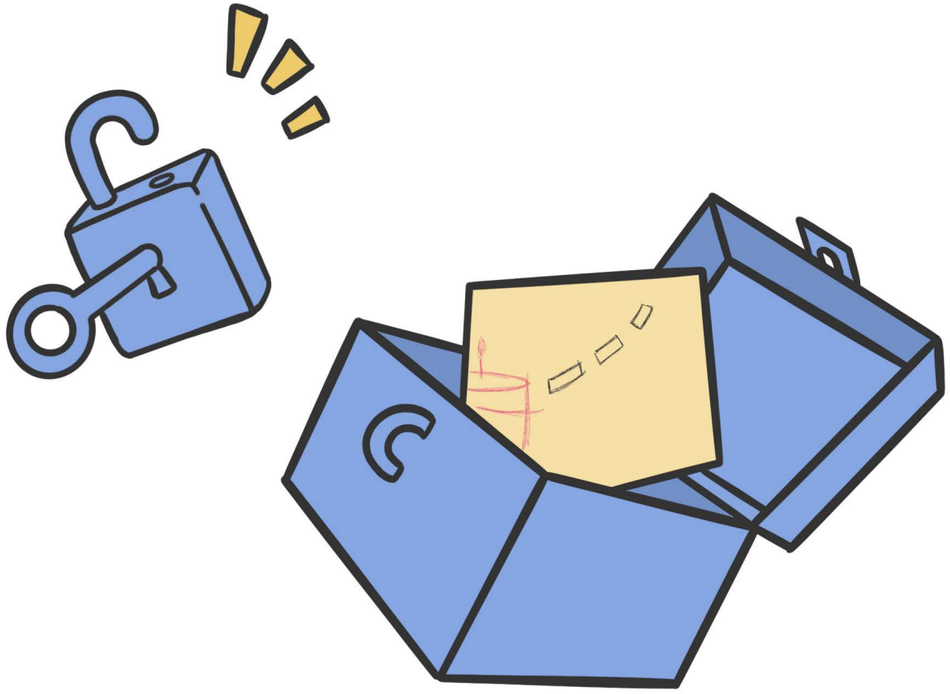
Can Triceratops lock the boxes WITHOUT needing any secret keys?

This is a PADLOCK.
You don't need a key to lock it.
You need one to unlock it.

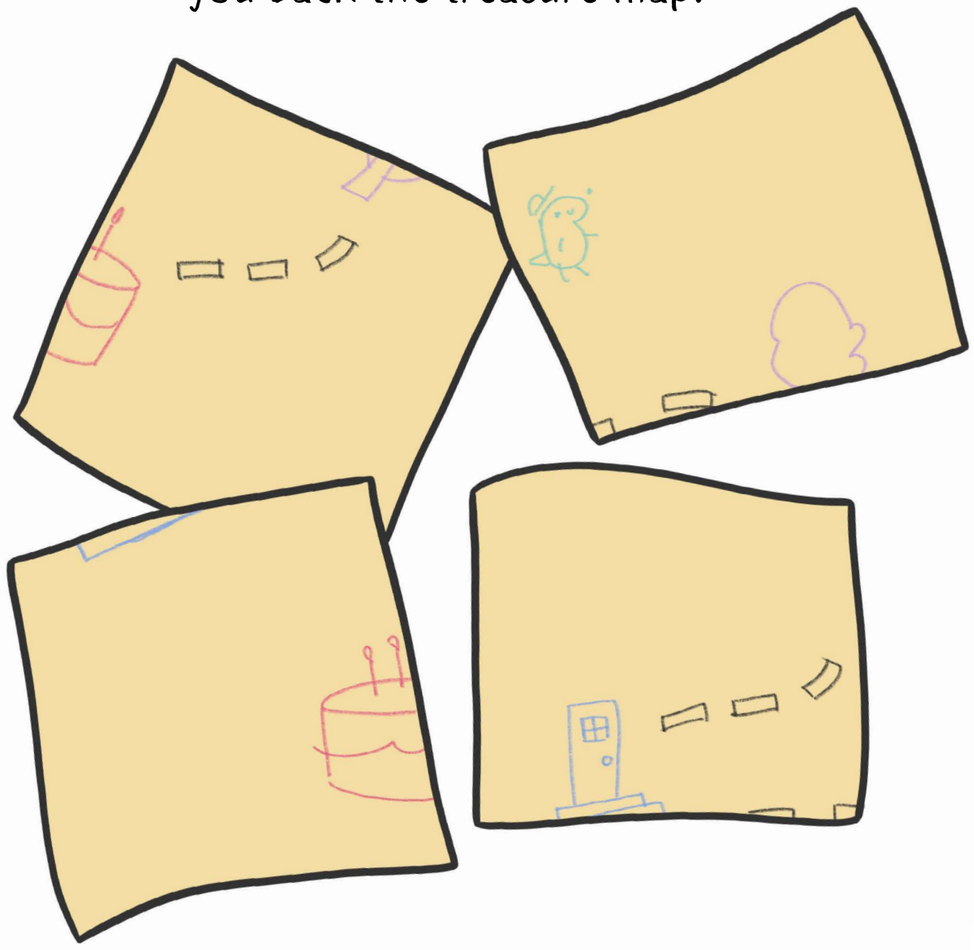
Triceratops could lock all the padlocks,
and would not need ANY secret key to do this!



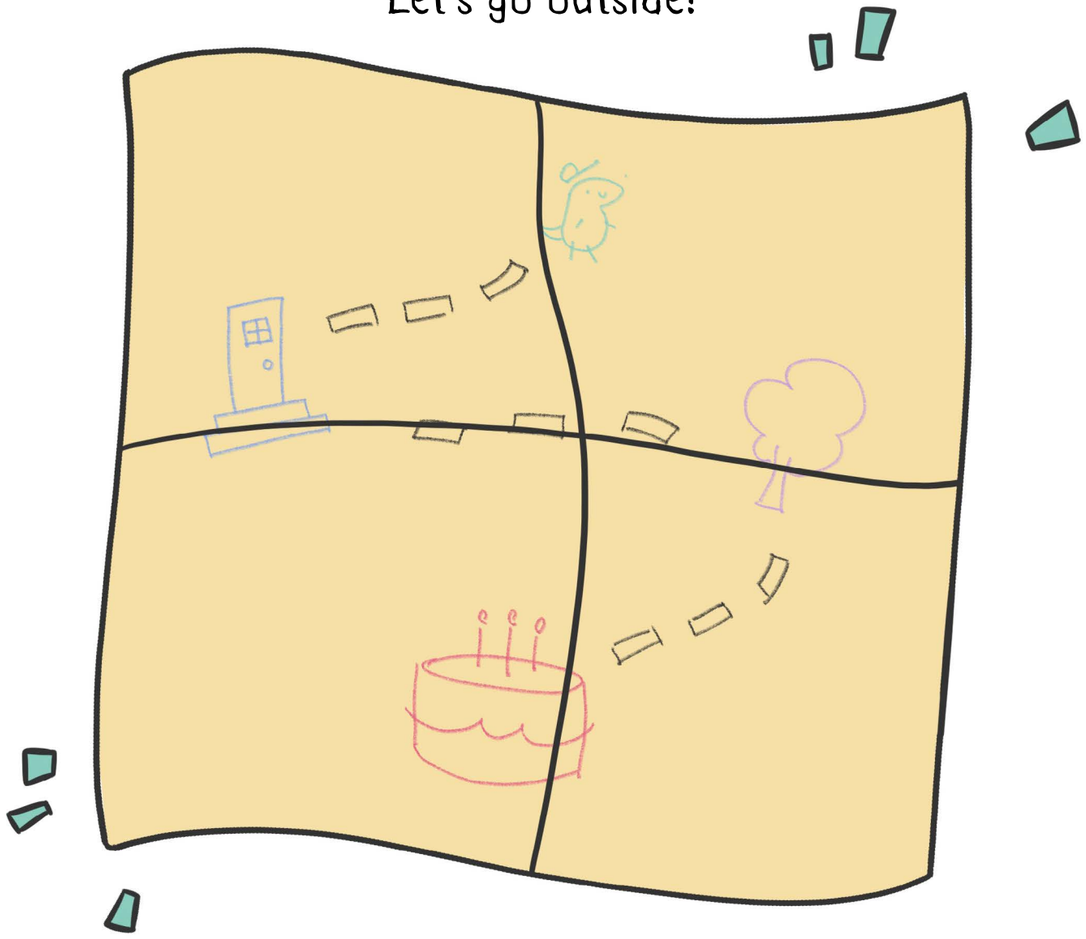
Each friend could get their piece of the
treasure map back using their padlock's key.



All the pieces put together give
you back the treasure map!



The cake is in the garden!
Let's go outside!



Surprise!
Happy Birthday T-Rex!

GLOSSARY

DIGITAL SIGNATURES are a mechanism to provide evidence that data was created by a specific party (the signer) and not modified. In our story, each friend physically signs the birthday card to ensure T-Rex knows it is from them.

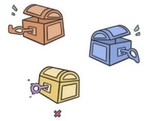
COMMITMENTS are a mechanism to allow an entity to commit to some secret piece of information, which can be revealed later. In our story, this is captured by putting the birthday card in a sealed envelope, so that the dog cannot add anything to it.

A **HASH FUNCTION** is a mathematical object that takes as input information of arbitrary size and maps it to values of fixed size. We capture this through the image of a pastry bag, which takes as input some amount of icing and outputs icing of a fixed size.

The **COMMUNICATION AND ADVERSARIAL MODEL** we work with is based on the assumption that communication between parties is done over an insecure channel, i.e., a channel over which an adversary can eavesdrop and even interfere with the content being transmitted. In our story this is captured by the presence of the dog, interested in eating the cake, and the dinosaur hiding the cake from the dog while moving it to a different location.

SECRET SHARING is the process of splitting a secret value into pieces so that a threshold or all pieces are necessary for its reconstruction. We capture this by breaking the treasure map into pieces, and by requiring all friends contribute with their piece to find the secret location of the cake.

ENCRYPTION is the process of using a key to transform information so that the result of the transformation does not reveal the original content, i.e. the information is hidden. In our story, this is captured by locking the pieces of the treasure map in a box



DECRYPTION is the reverse process of encryption, which enables you to recover the information with the help of a secret key. In our story, this is represented by unlocking the locked boxes, using the right key.

SYMMETRIC KEY is some secret information/value used both in the encryption and decryption processes. In our story, the same key is used to lock and unlock the box.

ASYMMETRIC KEYS are a pair of values. One is public, and is used to encrypt, and the other is secret, and is used to decrypt. In our story, Triceratops thinks of using padlocks to lock the boxes. The padlock is public, anyone can use it to encrypt (because a secret key is not needed to lock it), but only the dinosaur with the correct secret key can unlock it.

For more information on these concepts, and on cryptography as a whole, please visit https://www.cybok.org.

ADDITIONAL RESOURCES

An introduction to cryptographic concepts and constructions

A CyBOK webinar introducing cryptography

A CyBOK podcast introducing cryptography