Passwords

Outline

- **Explaining Password Restrictions**
- **Password-Free Passwords**
  - Zero-Knowledge Proofs
  - Passwords in Muscle Memory

General Password Advice:

Pick Long Passwords

Use Different Types Of Characters

Don't Pick Simple Passwords

Pick Long Passwords

- Suppose your password consists only of the upper-case letters A, B, and C.
- How many ***one***-character passwords are there?

A   B   C

Pick Long Passwords

- Suppose your password consists only of the upper-case letters A, B, and C.
- How many ***two***-character passwords are there?

	A	B	C
A	AA	AB	AC
B	BA	BB	BC
C	CA	CB	CC

Pick Long Passwords

- Suppose your password consists only of the upper-case letters A, B, and C.
- How many ***two***-character passwords are there?

	A	B	C
A	AA	AB	AC
B	BA	BB	BC
C	CA	CB	CC

Pick Long Passwords

- Suppose your password consists only of the upper-case letters A, B, and C.
- How many ***two***-character passwords are there?

	A	B	C
A	AA	AB	AC
B	BA	BB	BC
C	CA	CB	CC

Pick Long Passwords

- Suppose your password consists only of the upper-case letters A, B, and C.
- How many ***two***-character passwords are there?

	A	B	C
A	AA	AB	AC
B	BA	BB	BC
C	CA	CB	CC

Pick Long Passwords

- Suppose your password consists only of the upper-case letters A, B, and C.
- How many ***two***-character passwords are there?

	A	B	C
A	AA	AB	AC
B	BA	BB	BC
C	CA	CB	CC

Pick Long Passwords

- Suppose your password consists only of the upper-case letters A, B, and C.
- How many ***two***-character passwords are there?

	A	B	C
A	AA	AB	AC
B	BA	BB	BC
C	CA	CB	CC

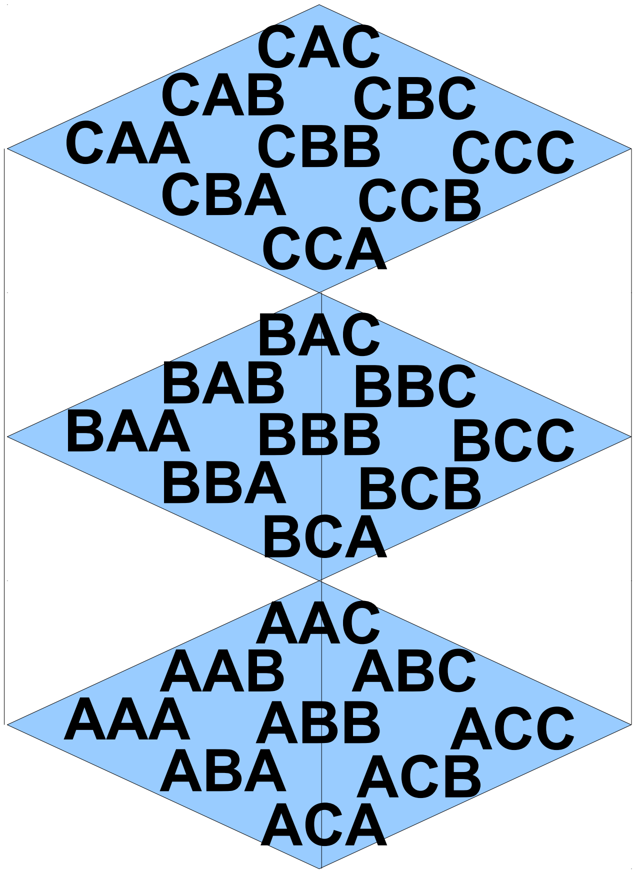
Pick Long Passwords

- Suppose your password consists only of the upper-case letters A, B, and C.
- How many ***two***-character passwords are there?

	A	B	C
A	AA	AB	AC
B	BA	BB	BC
C	CA	CB	CC

Pick Long Passwords

- Suppose your password consists only of the upper-case letters A, B, and C.
- How many ***three***-character passwords are there?



Pick Long Passwords

- When made from the letters A, B, and C, there are
  - **3** = 3^1 passwords of length 1,
  - **9** = 3^2 passwords of length 2,
  - **27** = 3^3 passwords of length 3,
  - …
  - $\mathbf{3^{n}}$ passwords of length n.
- Each added character *triples* the number of possible passwords!

Suppose your password consists of all upper-case letters. There are $\mathbf{26^{\mathit{n}}}$ possible passwords of length n.

For perspective…


Sweden has an area of 449,964 km^2.
$26^4 = 456,976$


US Population in 2009: 306.8 Million
26^6 = 308.9 Million


Number of atoms in the universe: $\approx 10^{80}$
$26^{57} \approx 4.5 \times 10^{80}$

Attacking Passwords

Some Math

- Suppose you can try entering 10^9 passwords per second.
- If all passwords are made from upper-case letters (26 options), time to figure out a password of
  - length 6: < 1 second
  - length 8: 2.5 minutes
  - length 10: 1.6 days
  - length 15: 53,000 years

Some Math

- Suppose you can try entering 10^9 passwords per second.
- If all passwords are made from upper and lower-case letters (52 options), time to figure out a password of
  - length 6: 19 seconds
  - length 8: 15 hours
  - length 10: 4.5 years
  - length 15: 1.7 billion years

Some Math

- Suppose you can try entering 10^9 passwords per second.
- If all passwords are made from letters, digits, and punctuation (94 options), time to figure out a password of
  - length 6: 11 minutes
  - length 8: 10 weeks
  - length 10: 1707 years
  - length 15: 12 trillion years

General Password Advice:

Pick Long Passwords
Use Different Types Of Characters
Don't Pick Simple Passwords

Random 15-Symbol Passwords

```
:t$bk~jN__akL_B
xv&lA};$:xV[k^2
W;7nFir5|[@/Wfu
p9Ep[.>w!\cJ?DH
M$UhvrVm:SA}!@q
```

The RockYou! List

32 Million Accounts
1.4 Million Distinct Passwords

The US nuclear arsenal has passwords to prevent unauthorized missile launches.

For fifteen years the password was...

00000000

Redoing the Math

- Approximate size of a college graduate's vocabulary, in words: **15,000**.
- Approximate number of common names in the United States: **5,000**.
- Total number of passwords that are a common word or name: **20,000**.
- Time to brute-force this on a computer: ***less than one second***.
- Trying to guess a password from a list of common passwords is called a ***dictionary attack***.

Multiword Passwords

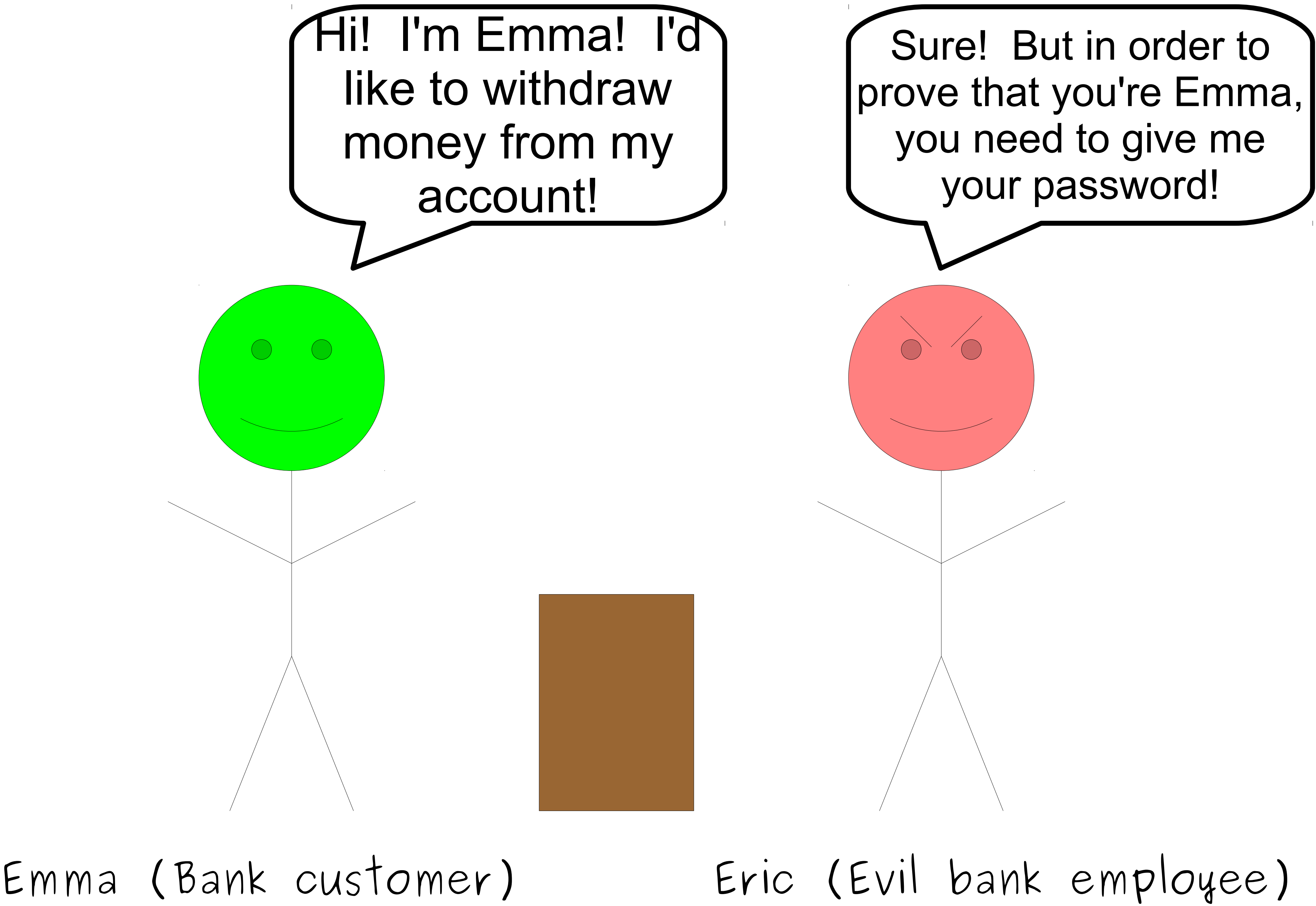
- If you choose two totally random common words or names and use it as your password, there are **800 million** possibilities.
  - Easily attacked by a computer.
- If you choose *four* totally random common words or names and use them as your password, there are **160 quadrillion** possibilities.
  - Takes a *long* time to brute-force.
- If you choose *six* totally random common words or names and use them as your password, there are **64 septillion** possibilities.
  - Well beyond the reach of a computer attack.

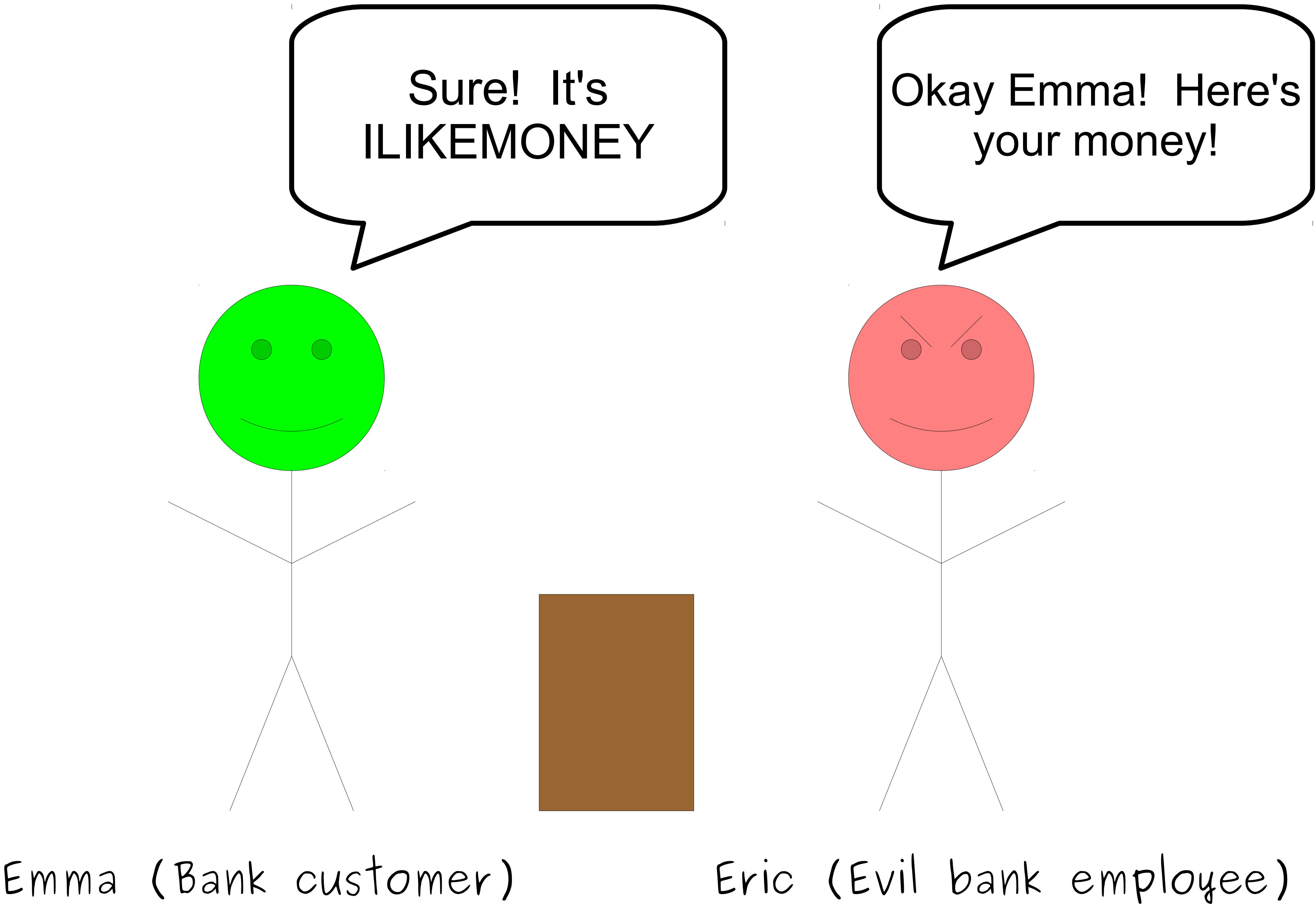
A Fun NYTimes Article:

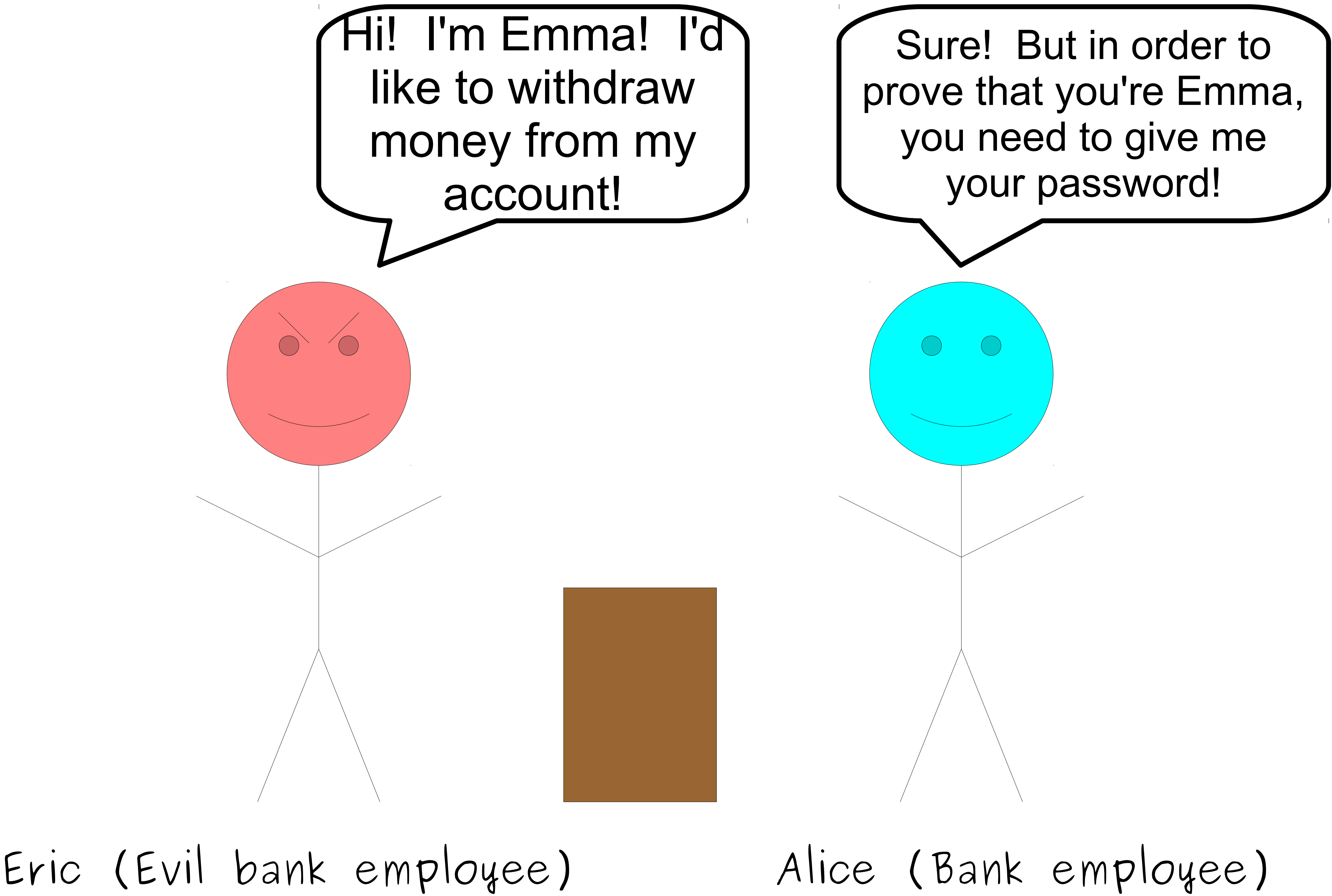
http://www.nytimes.com/2014/11/19/magazine/the-secret-life-of-passwords.html?_r=0

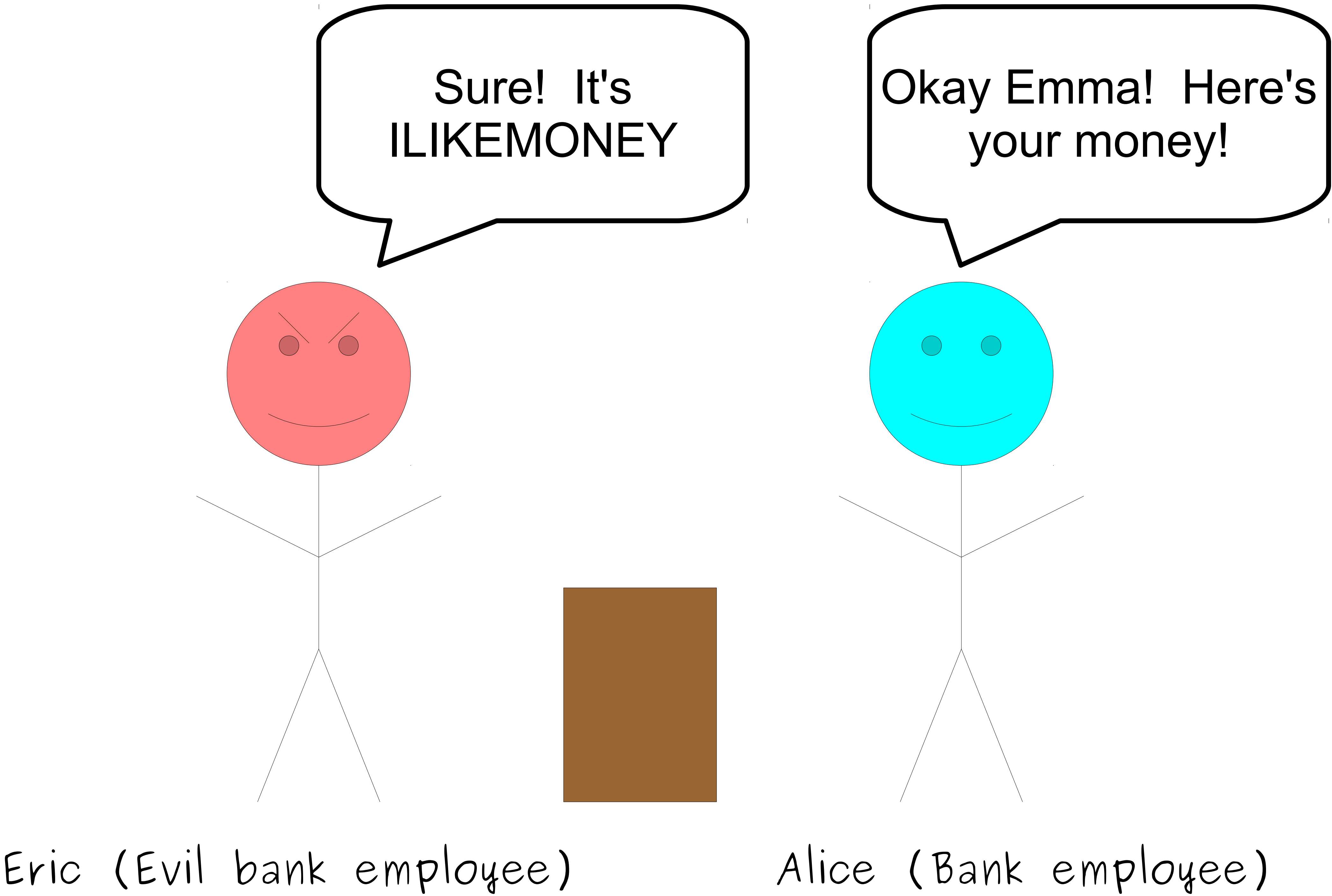
Fundamental Concerns in Passwords:

An Issue of Trust


Hi! I'm Emma! I'd like to withdraw money from my account!
Sure! But in order to prove that you're Emma, you need to give me your password!
Emma (Bank customer)
Eric (Evil bank employee)


Sure! It's ILIKEMONEY
Okay Emma! Here's your money!
Emma (Bank customer)
Eric (Evil bank employee)


Hi! I'm Emma! I'd like to withdraw money from my account!
Sure! But in order to prove that you're Emma, you need to give me your password!
Eric (Evil bank employee)
Alice (Bank employee)

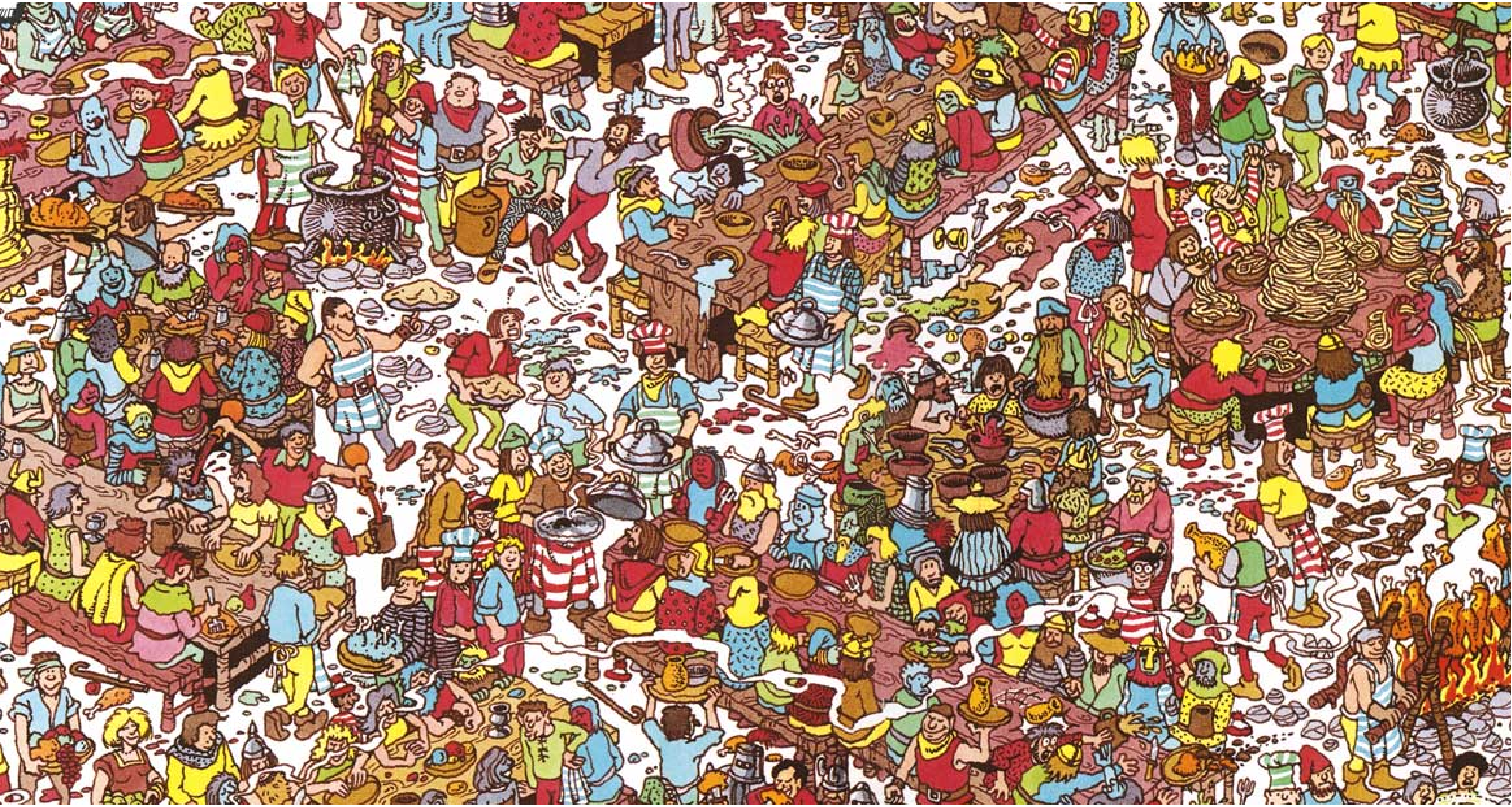

Sure! It's ILIKEMONEY
Okay Emma! Here's your money!
Eric (Evil bank employee)
Alice (Bank employee)

What is a Password?

Goal: Convince someone (the *verifier*) that you know a secret without revealing what that secret is.

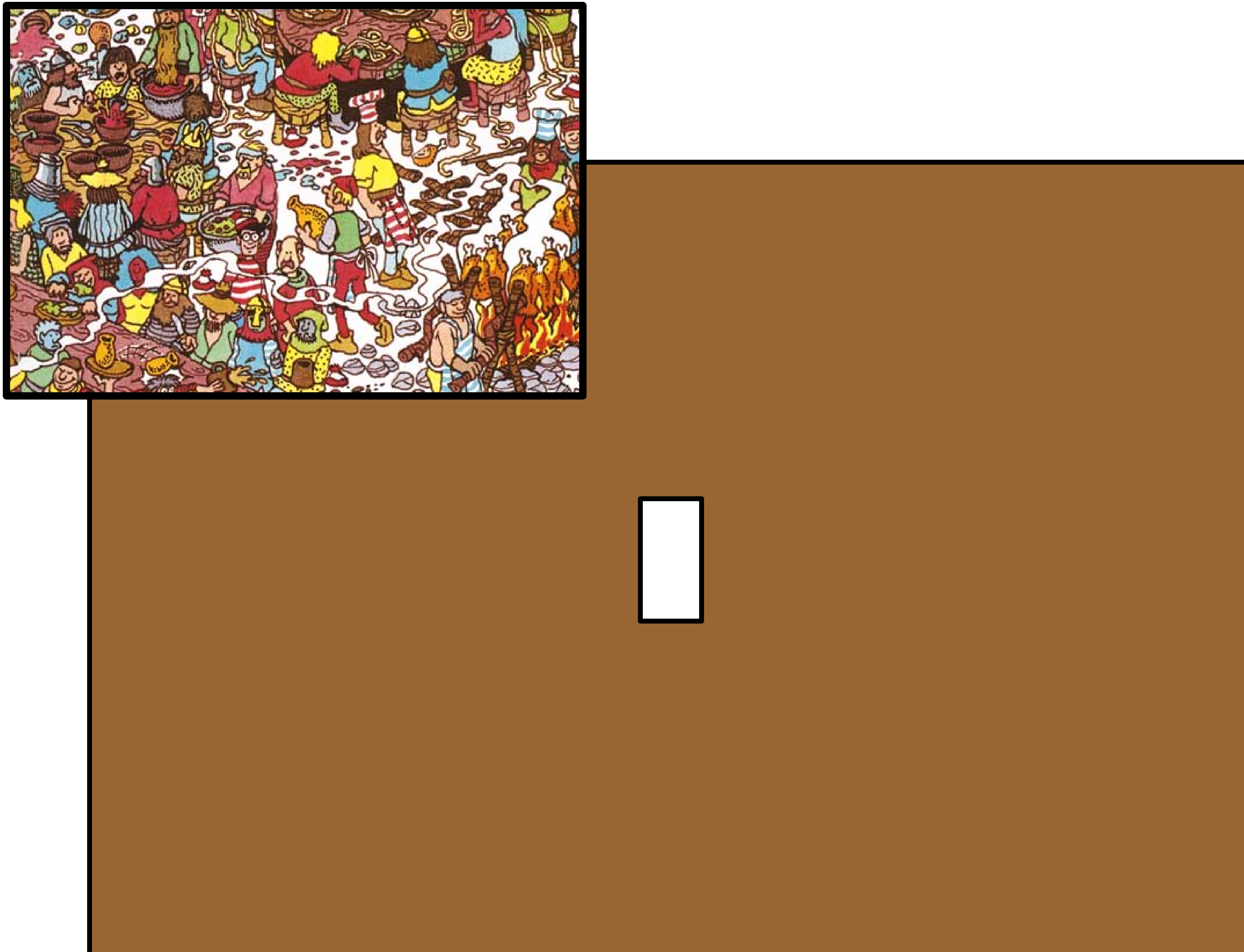
Where's Waldo?

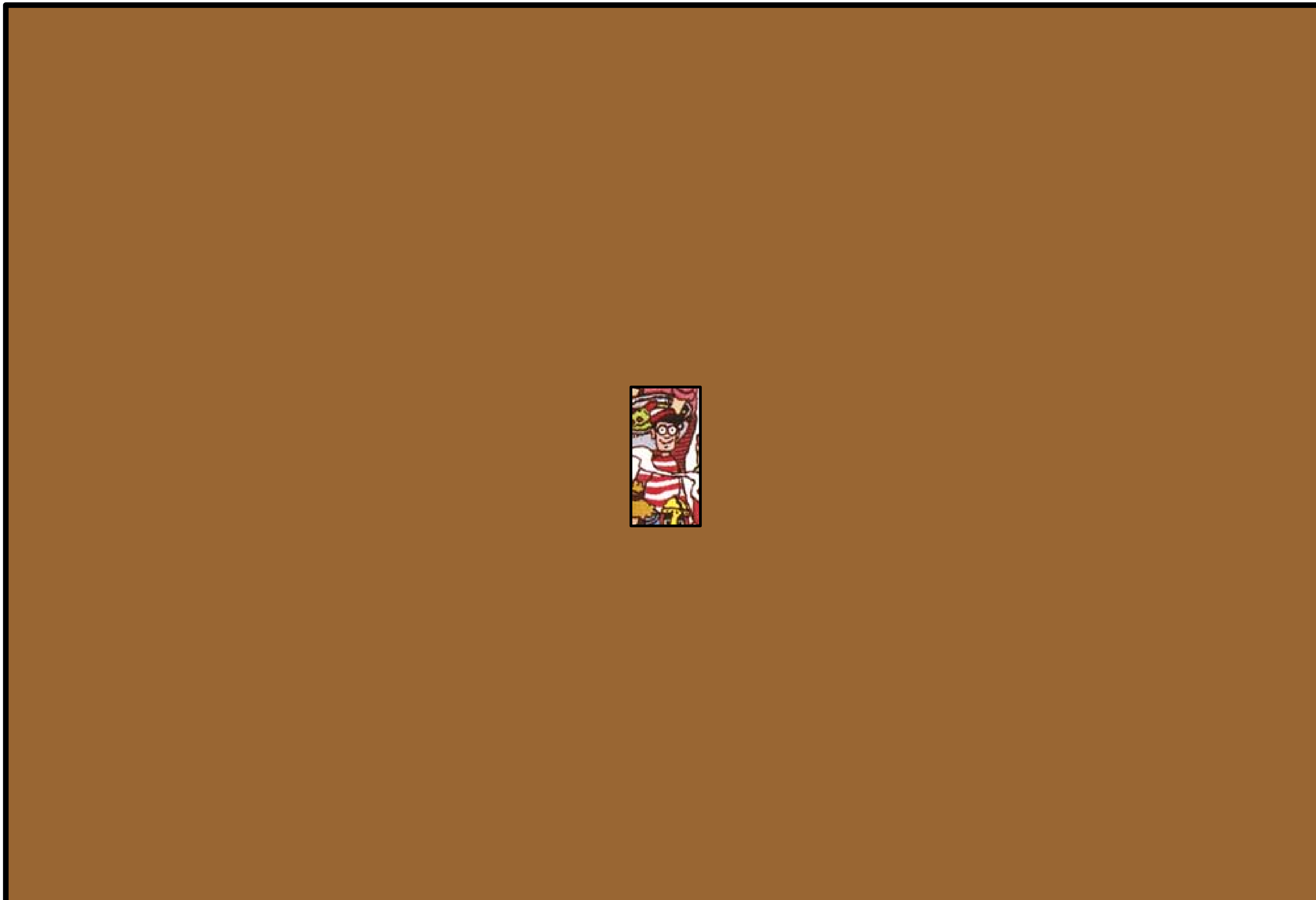
Where's Waldo?

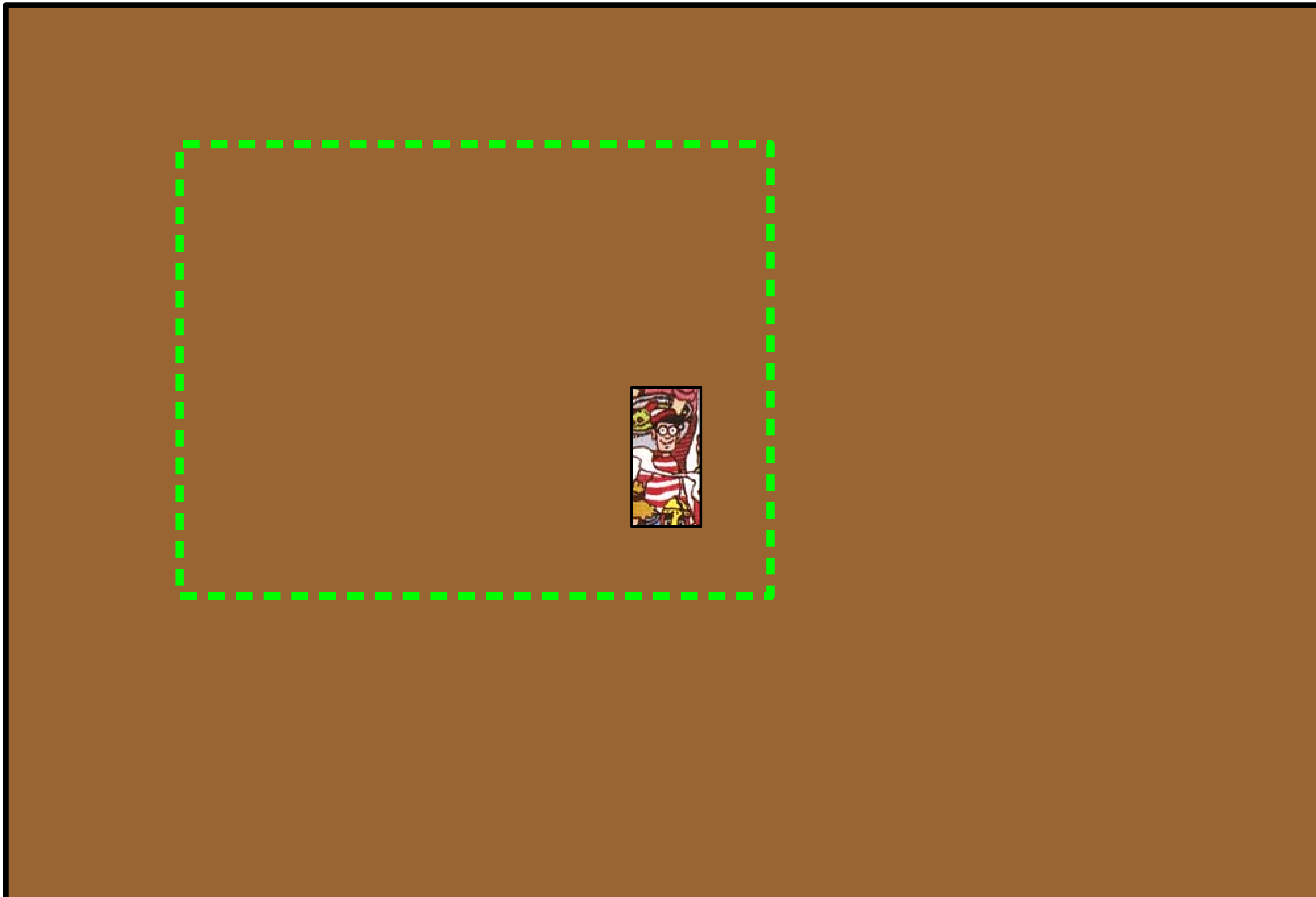


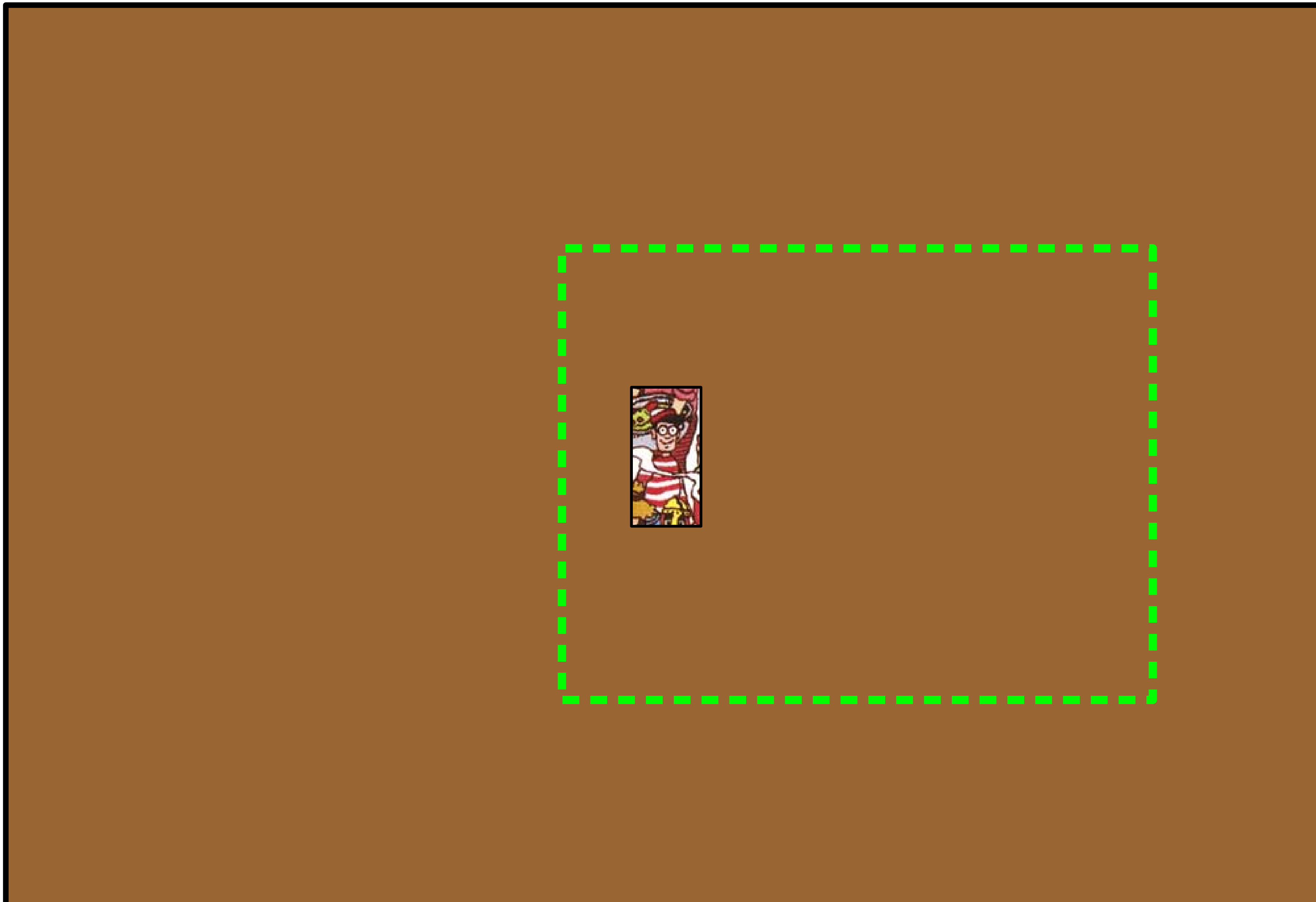
Source: http://www.findwaldo.com/maps/gluttons/gluttons_small.jpg

Could I convince you I know where Waldo is without revealing his position?









Applied Kid Cryptography
or
How To Convince Your Children You Are Not Cheating

MONI NAOR*   YAEL NAOR†   OMER REINGOLD‡

March, 1999

Abstract

In this note, we consider a real life cryptographic problem: how to convince people that you know where Waldo is without revealing information about his location. We propose and discuss methods of solving this problem.

Applied Kid Cryptography
or
How To Convince Your Children You Are Not Cheating

Moni Naor* Yael Naor† Omer Reingold‡

March, 1999

Abstract

In this note, we consider a real life cryptographic problem: how to convince people that you know where Waldo is without revealing information about his location. We propose and discuss methods of solving this problem.

Applied Kid Cryptography
or
How To Convince Your Children You Are Not Cheating

MONI NAOR[*] YAEL NAOR[†] OMER REINGOLD[‡]

March, 1999

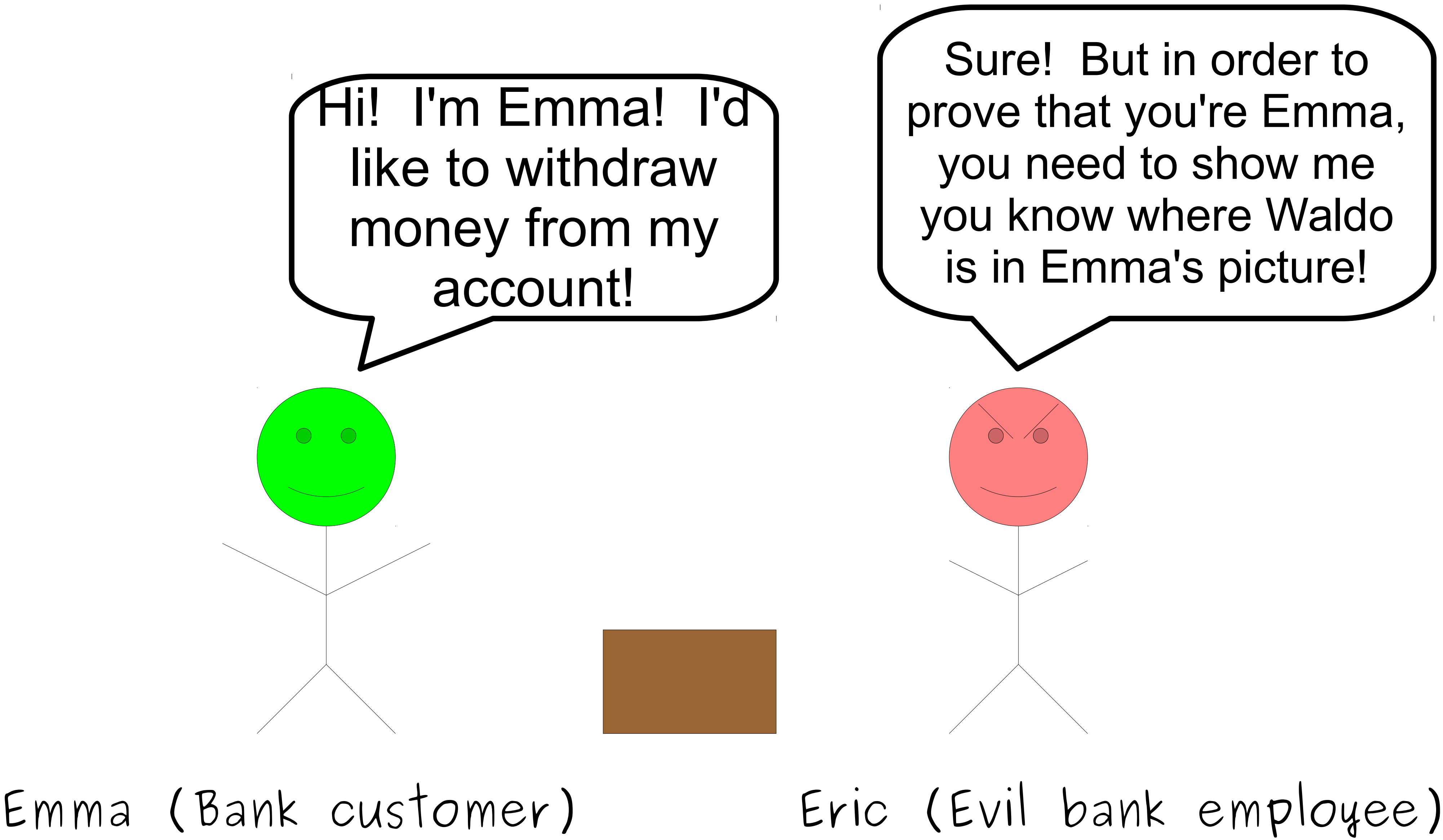
Abstr

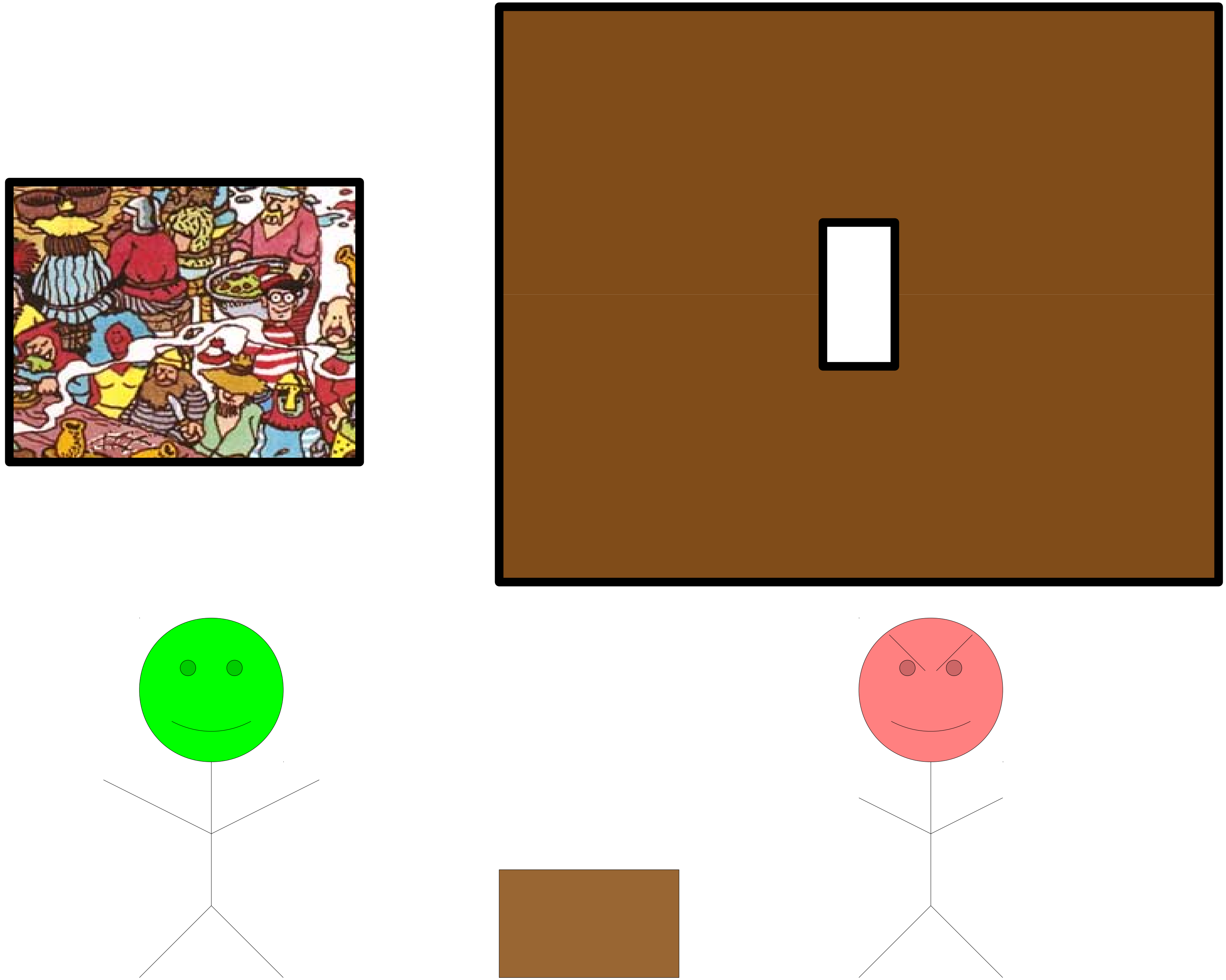
In this note, we consider a real life cryptograp
know where Waldo is without revealing informati
methods of solving this problem.

Zero-Knowledge Proofs

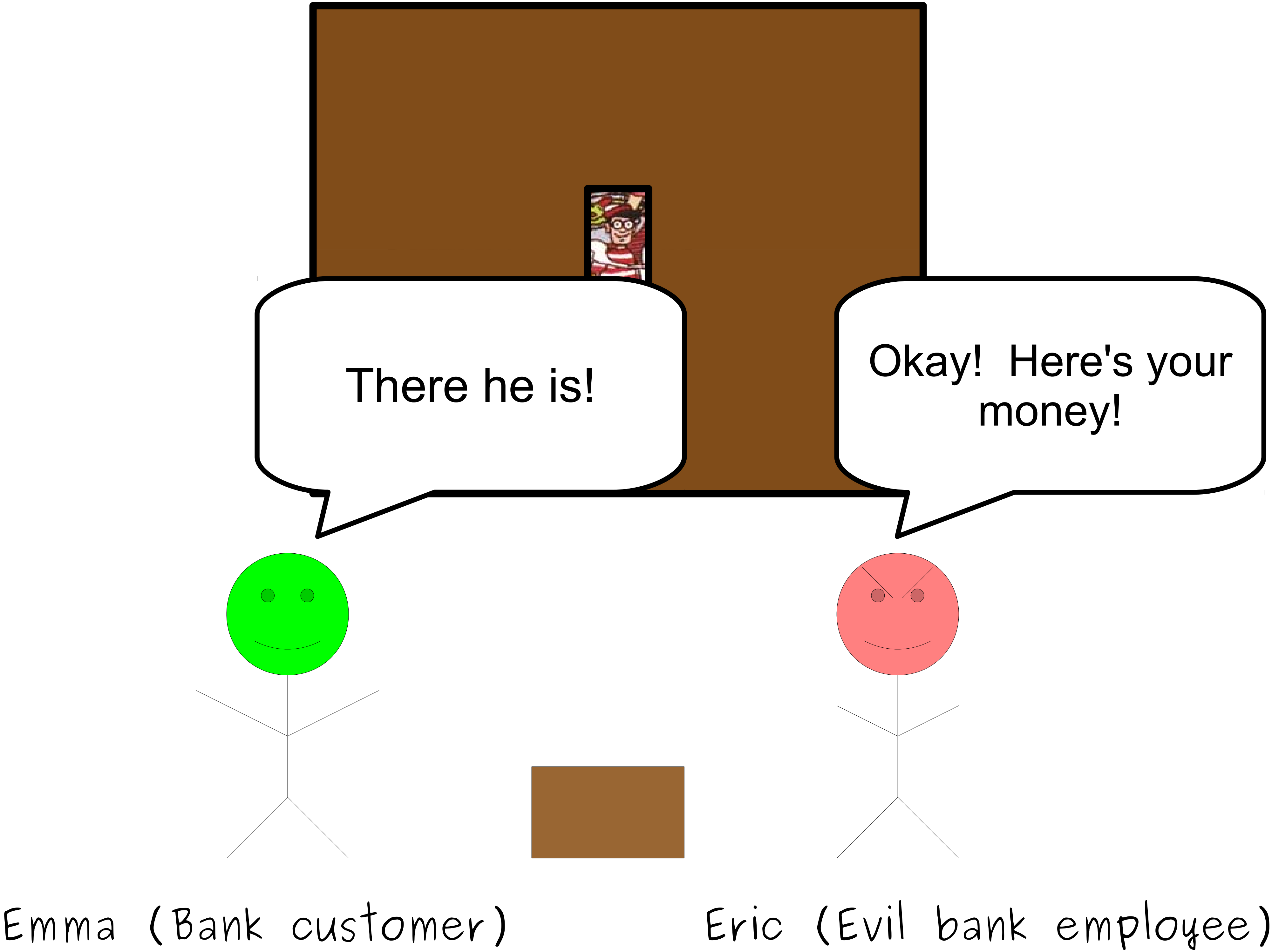
- A ***zero-knowledge proof*** (or ***ZKP***) is a system between a ***prover*** and a ***verifier***.
- The ***prover*** wants to convince the ***verifier*** that she knows a secret without revealing the secret to the verifier.
- Replaces passwords: can *prove* you are who you are to a *verifier,* who then cannot impersonate you.

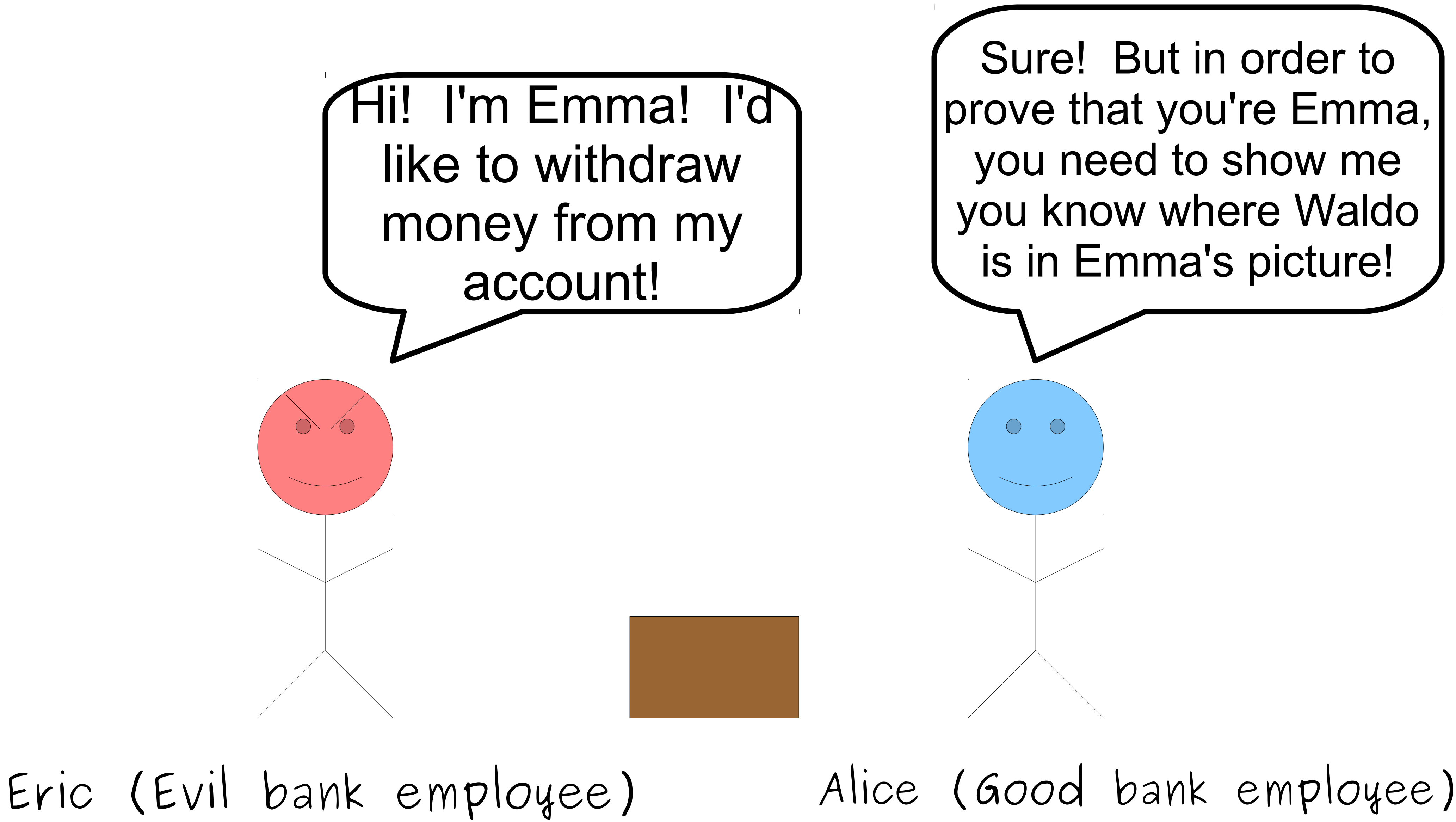
Database:
One Puzzle Per Person

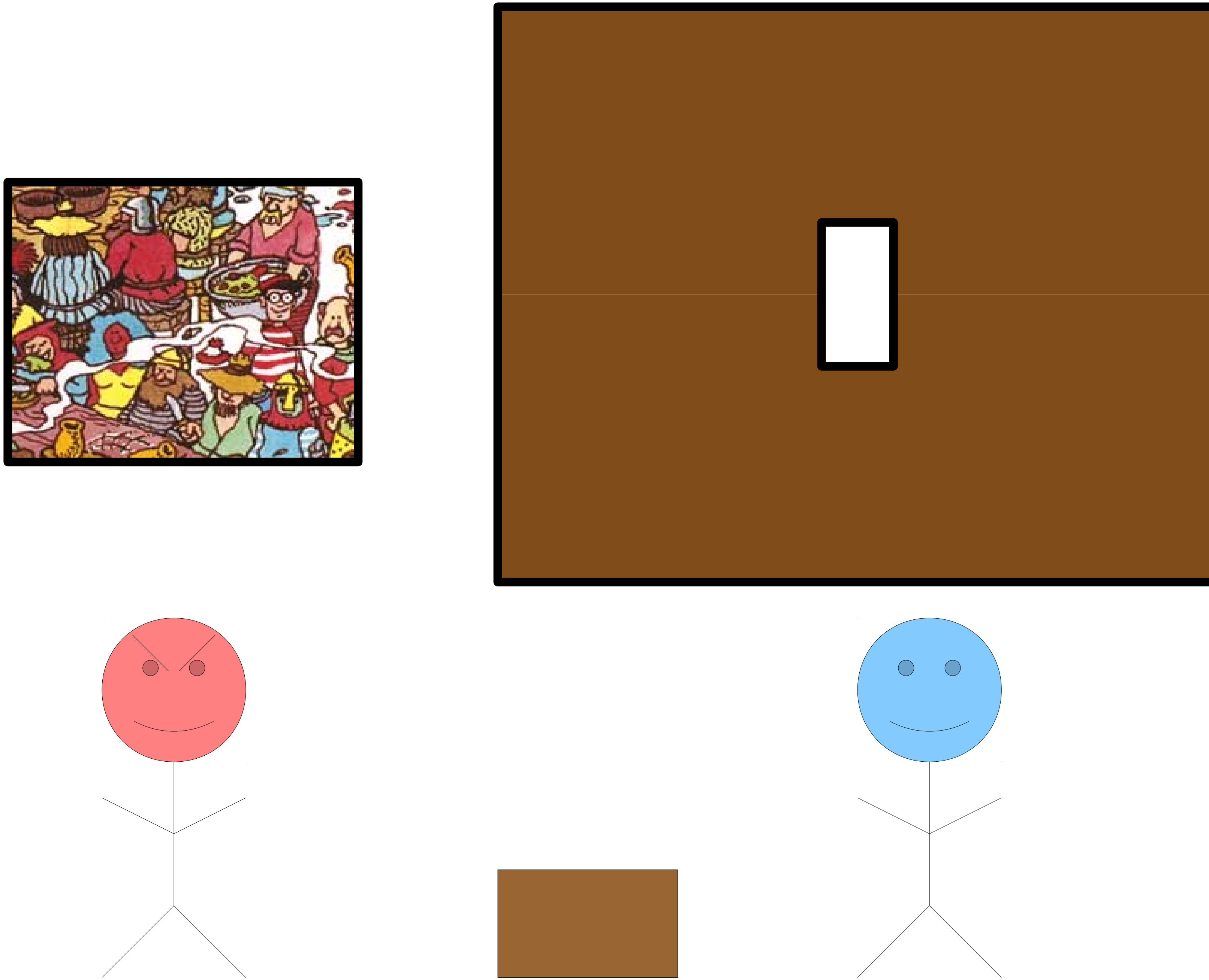

Hi! I'm Emma! I'd like to withdraw money from my account!
Sure! But in order to prove that you're Emma, you need to show me you know where Waldo is in Emma's picture!
Emma (Bank customer)
Eric (Evil bank employee)



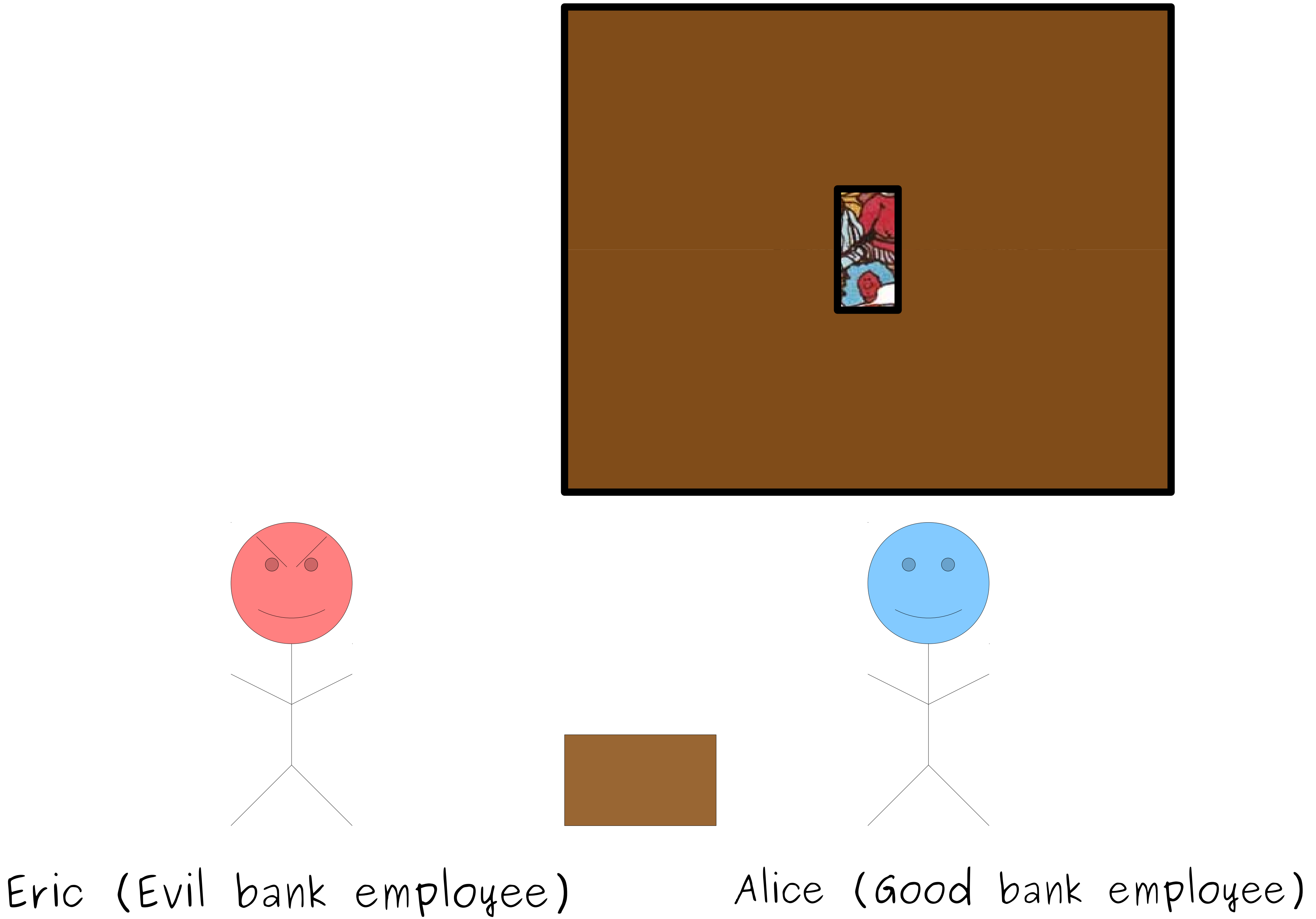
Emma (Bank customer) Eric (Evil bank employee)

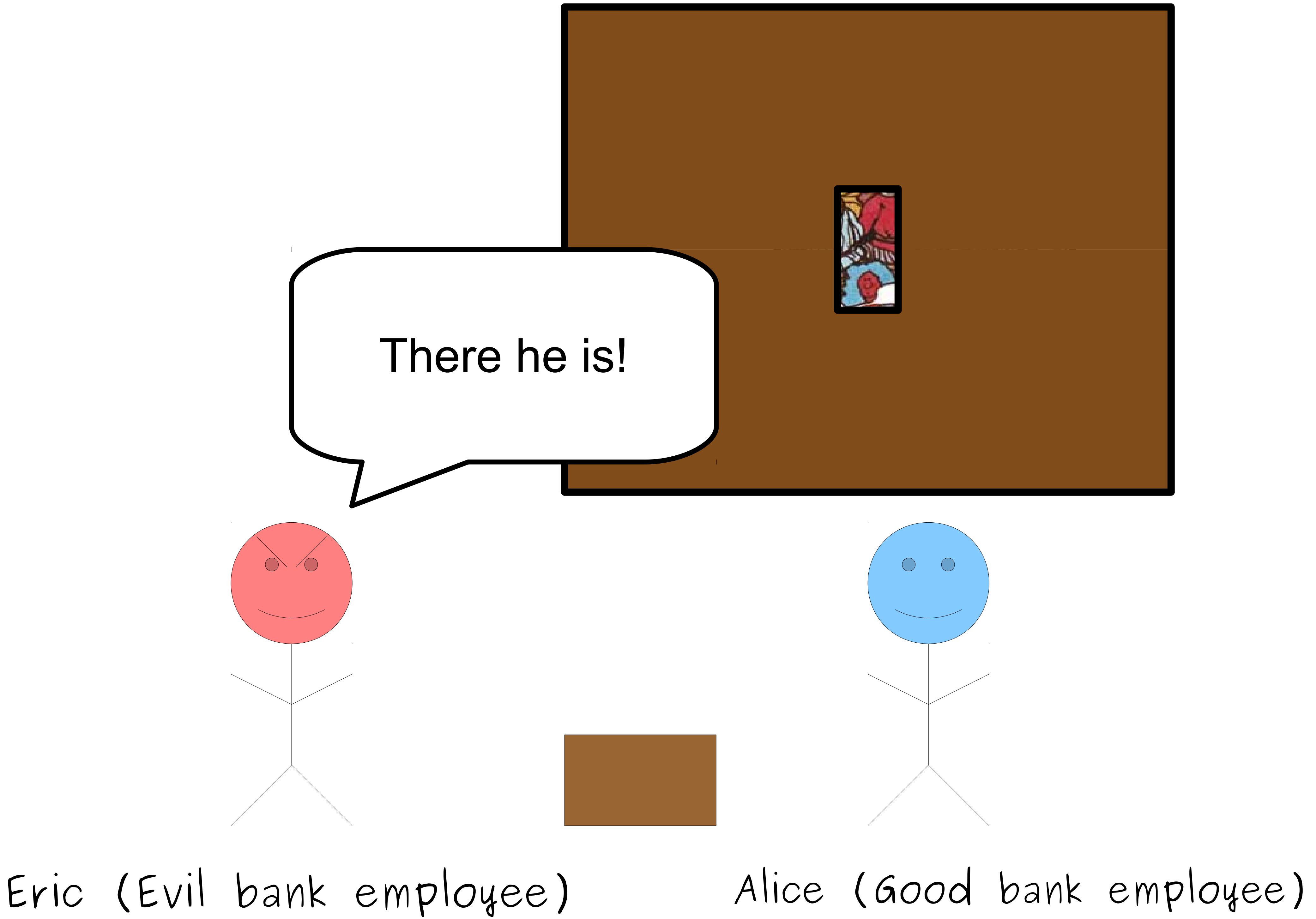

There he is!
Okay! Here's your money!
Emma (Bank customer)
Eric (Evil bank employee)

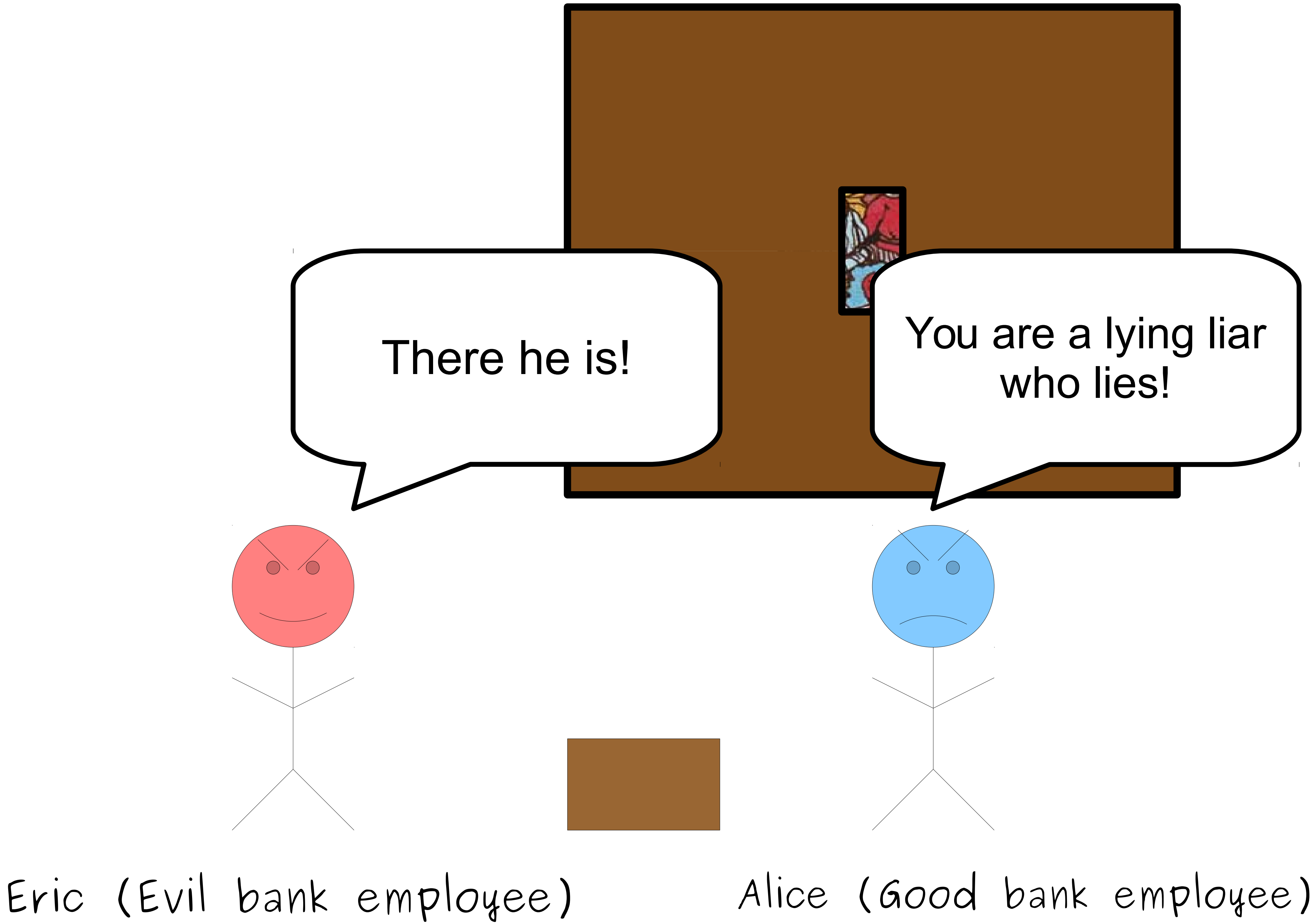

Hi! I'm Emma! I'd like to withdraw money from my account!
Sure! But in order to prove that you're Emma, you need to show me you know where Waldo is in Emma's picture!
Eric (Evil bank employee)
Alice (Good bank employee)



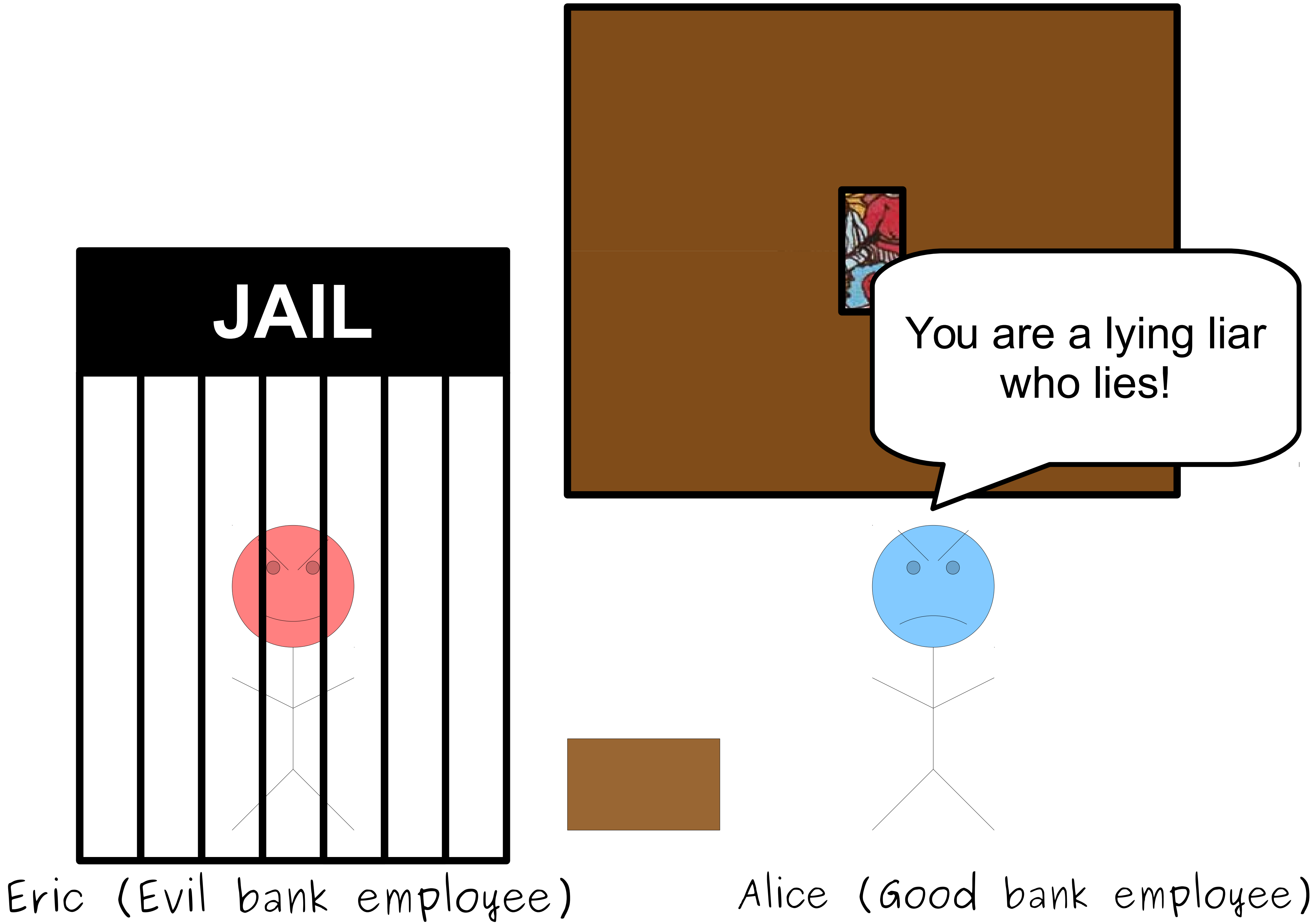
Eric (Evil bank employee) Alice (Good bank employee)

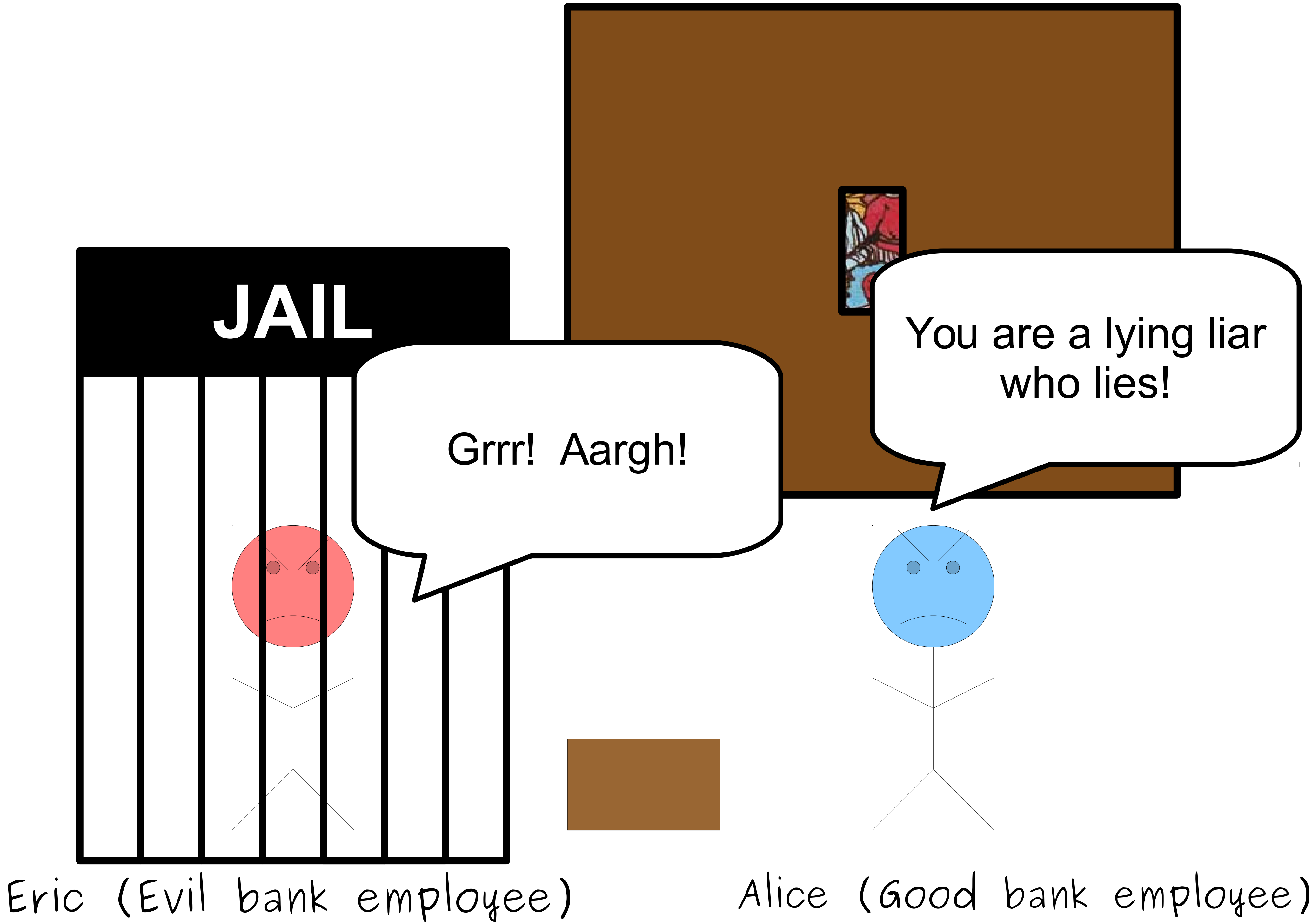

Eric (Evil bank employee)
Alice (Good bank employee)


There he is!
Eric (Evil bank employee)
Alice (Good bank employee)



There he is!
You are a lying liar who lies!
Eric (Evil bank employee)
Alice (Good bank employee)


JAIL
You are a lying liar who lies!
Eric (Evil bank employee)
Alice (Good bank employee)


JAIL
Grrr! Aargh!
You are a lying liar who lies!
Eric (Evil bank employee)
Alice (Good bank employee)

Zero-Knowledge Proofs in Practice

An Issue of Coercion

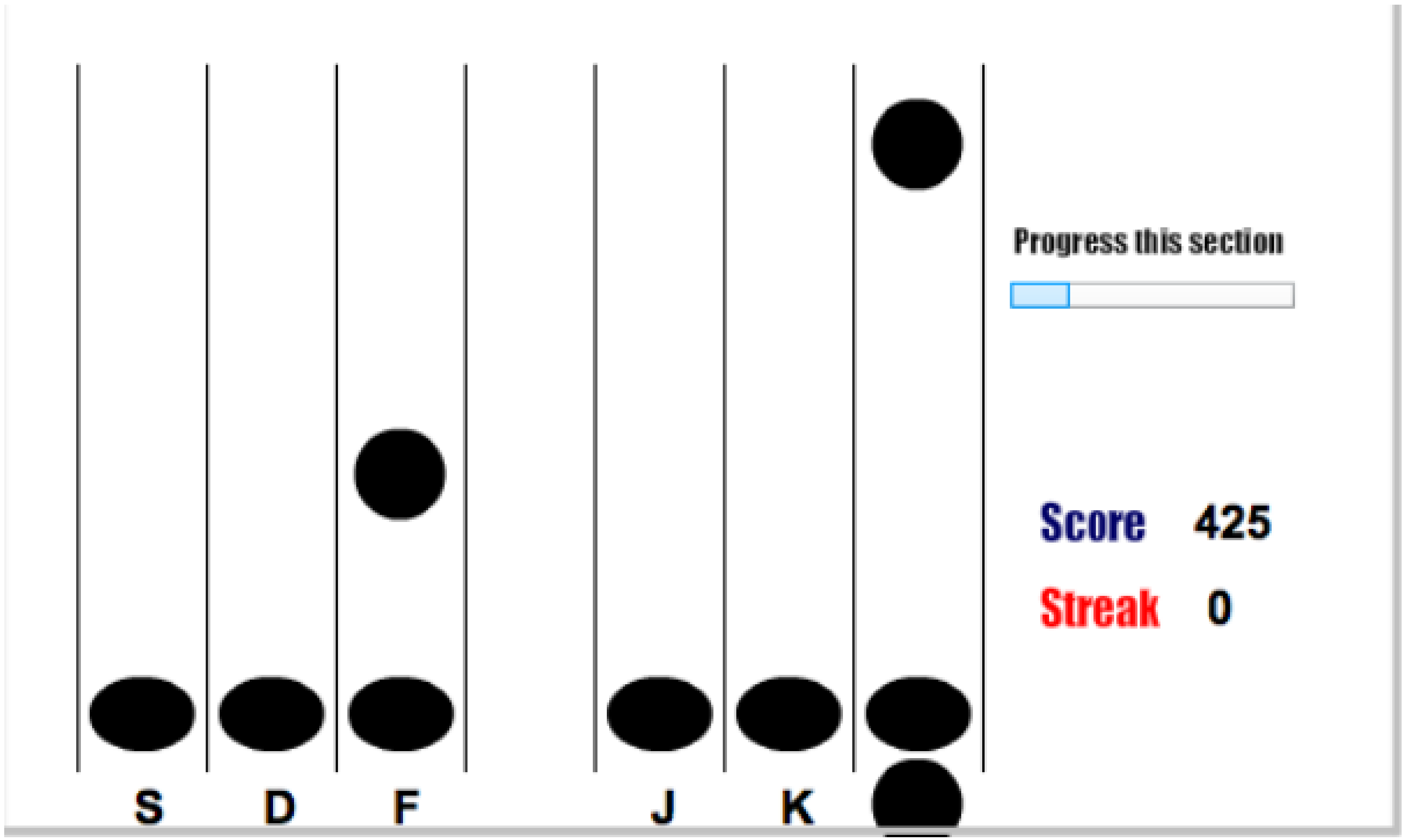


Figure 1: Screenshot of the SISL task in progress.

(This work was done in 2012)

Why This Matters

- Cryptography lies at the intersection of several fields:
    - ***Computer Science:*** How do you implement cryptography in software?
    - ***Mathematics*:** What mathematical properties ensure a system is safe?
    - ***Social Science:*** How do human social dynamics influence what to secure against?
    - ***Neuroscience:*** How does the brain form memories?
    - *And a lot more!*