
SECURITY (COMP0141): WHAT YOU HAVE



AUTHENTICATION

Authentication is:

What you know

text passwords

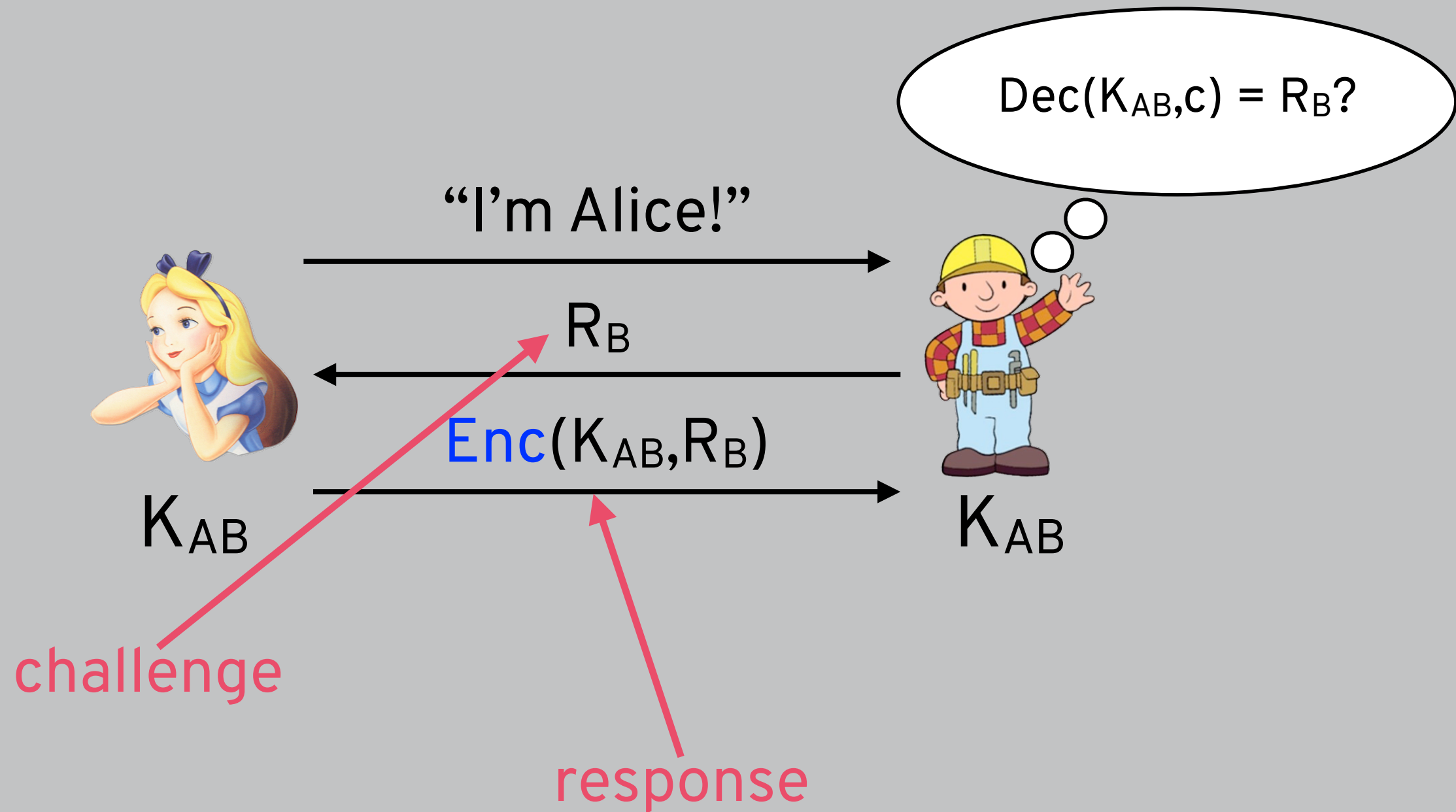
graphical passwords

personal details

What you have

What you are

CHALLENGE-RESPONSE



CHALLENGE-RESPONSE

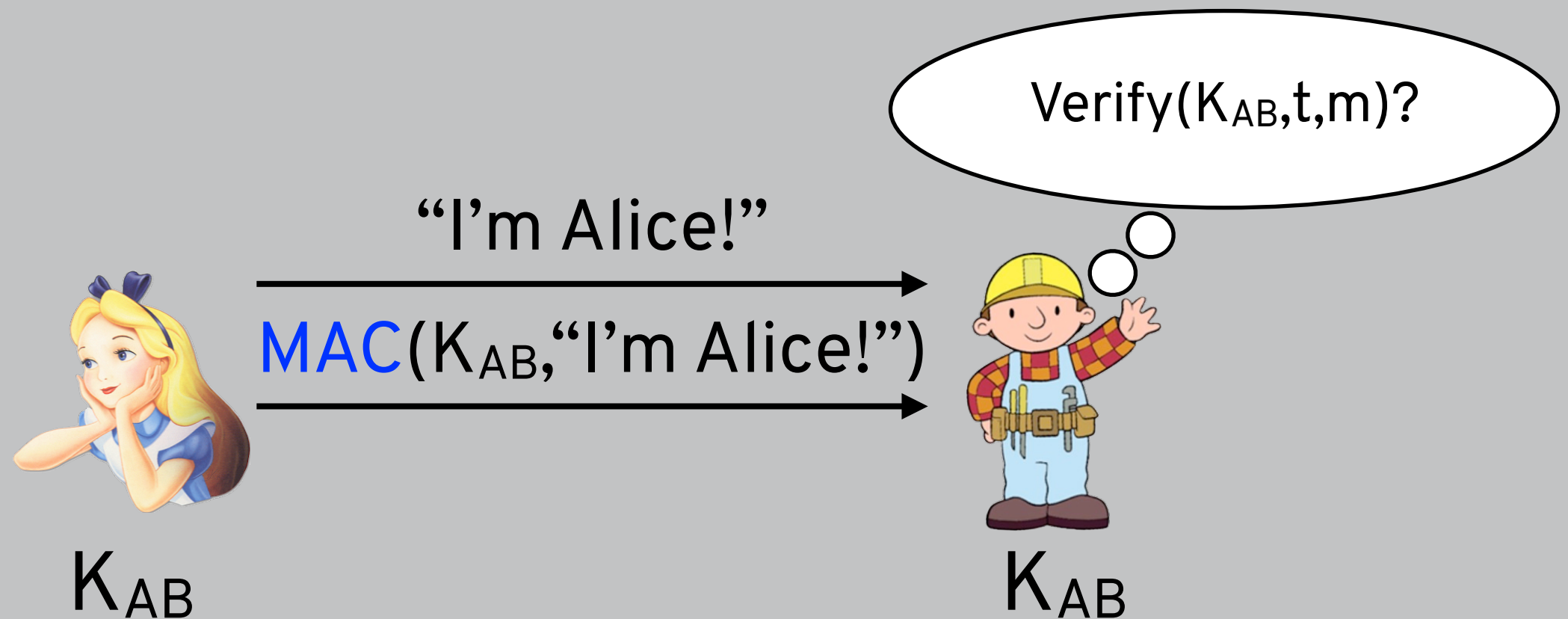
RFID: Radio Frequency Identification

?



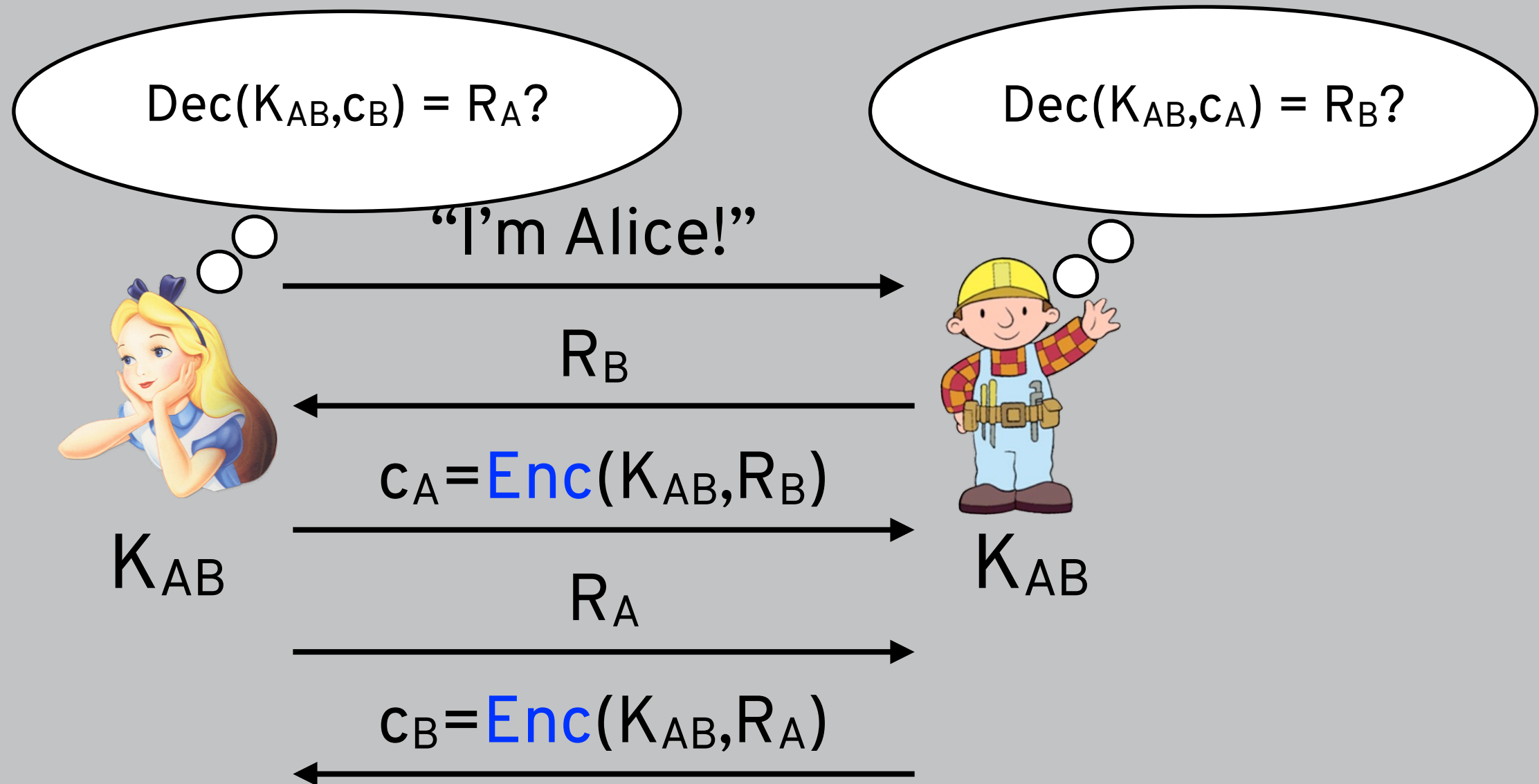
NFC: Near Field Communication

WHY NOT DO THIS?

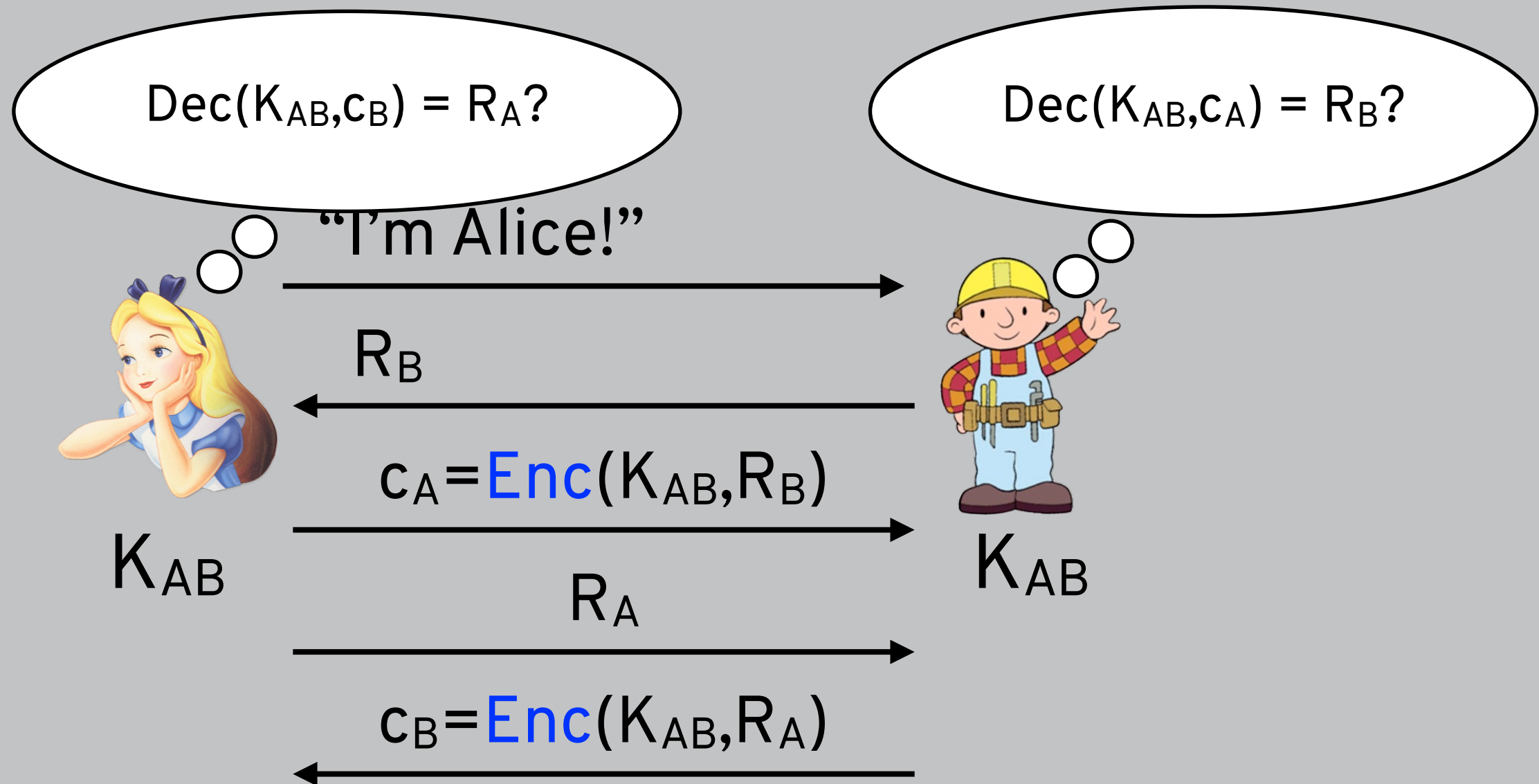


this doesn't work in really constrained environments!

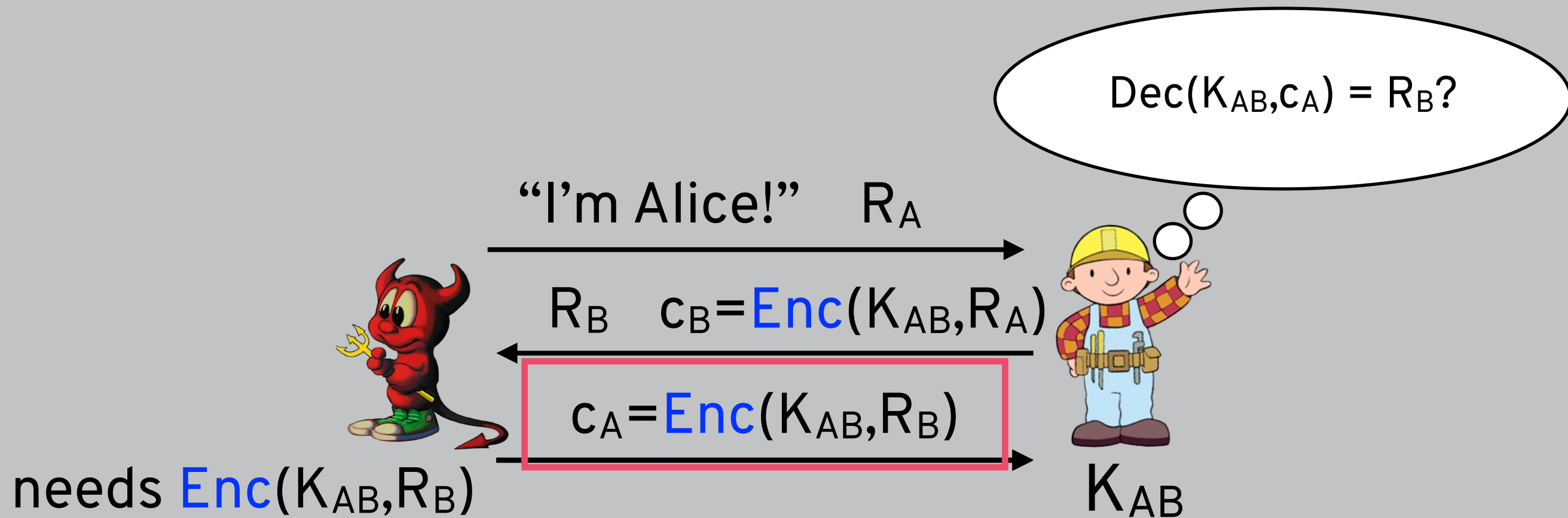
TWO-WAY CHALLENGE-RESPONSE



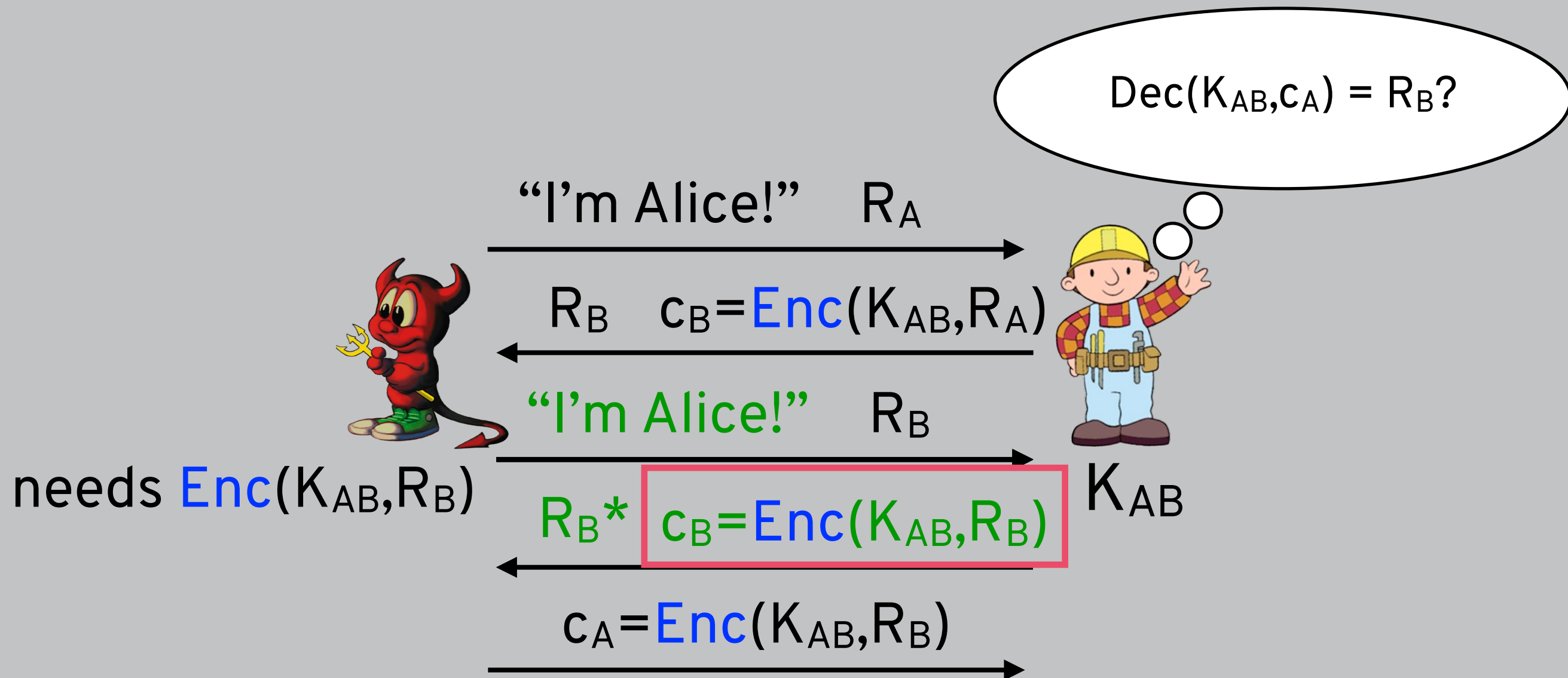
WHY NOT DO THIS?



WHY NOT DO THIS?

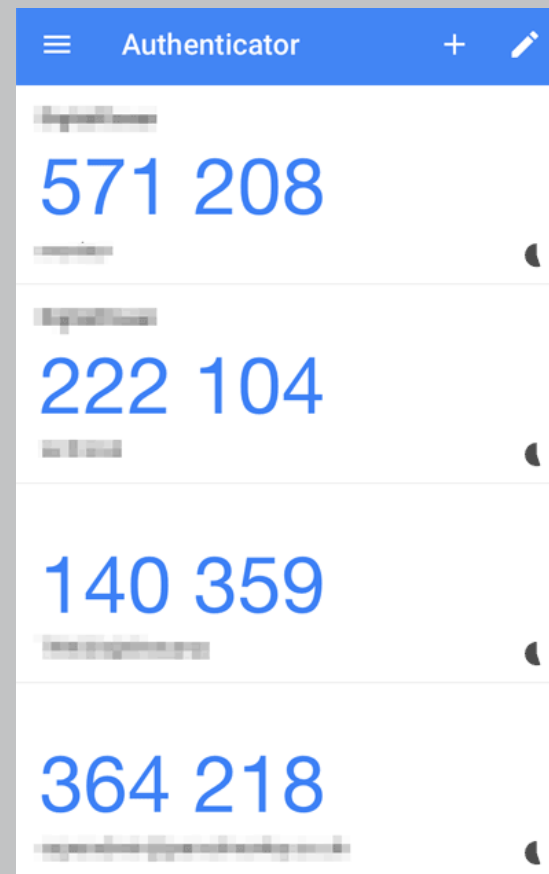


WHY NOT DO THIS?



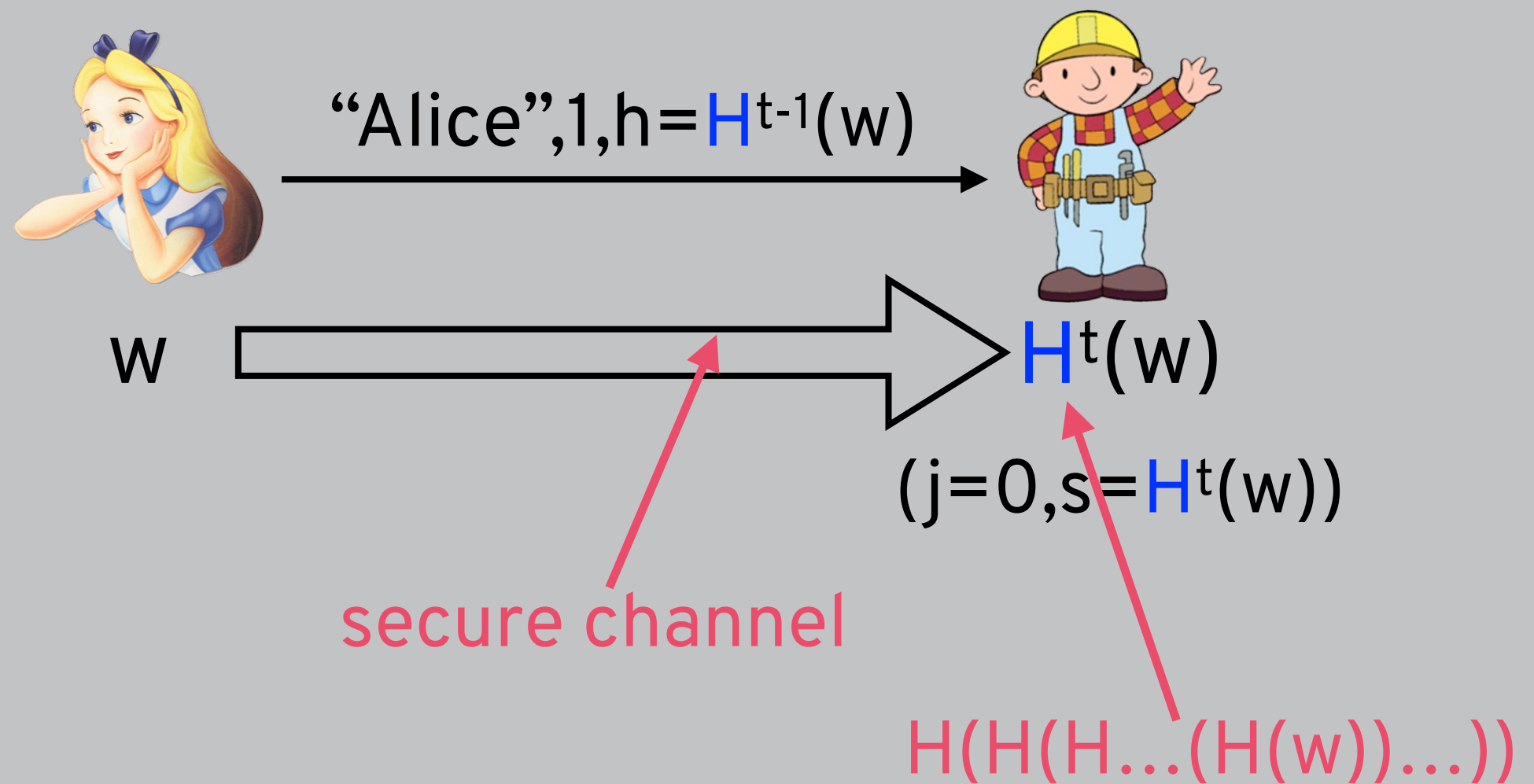
don't design your own crypto!
need to consider **all** possible attackers

ONE-TIME PASSWORDS

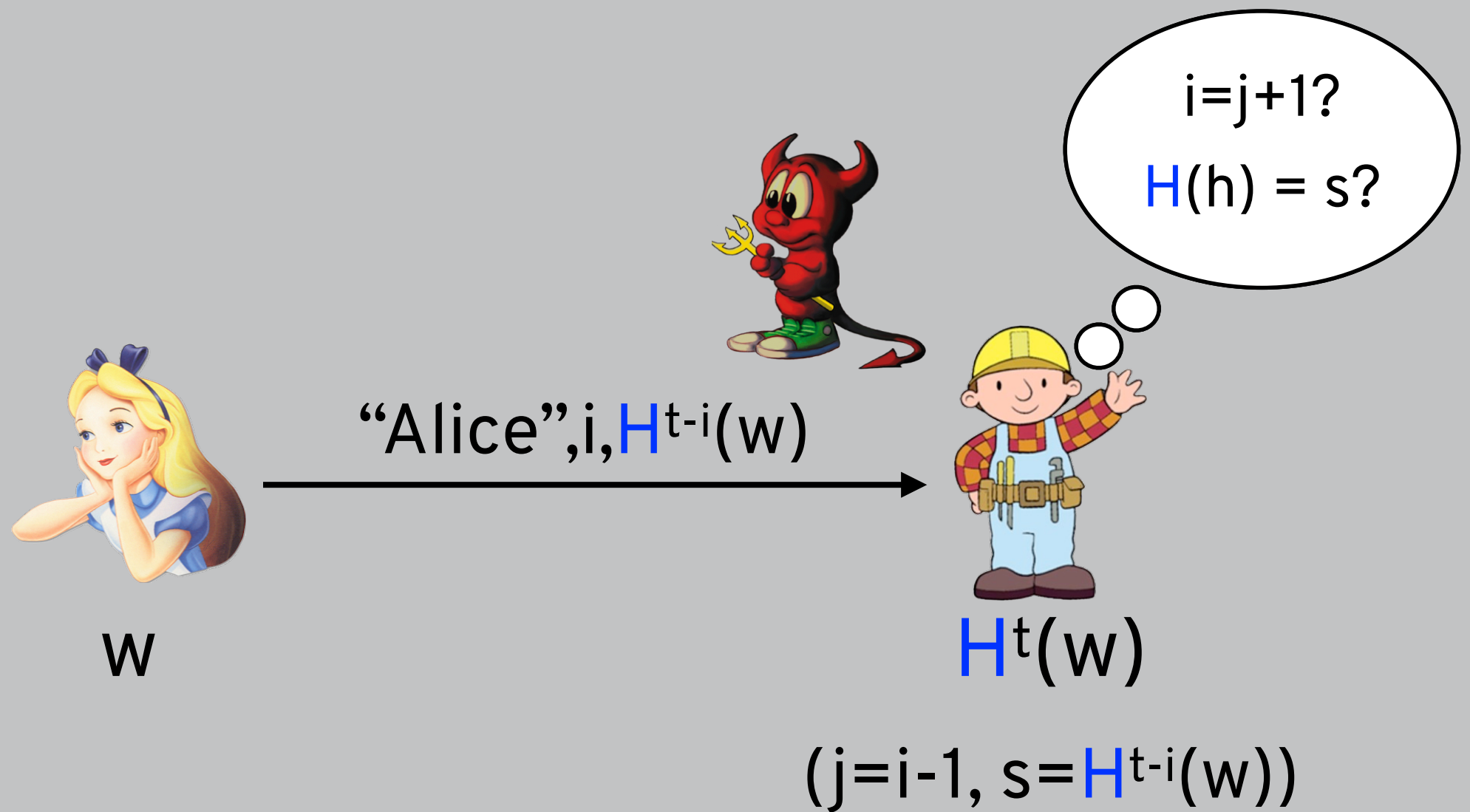


could be based on time (requires sync) or **math**

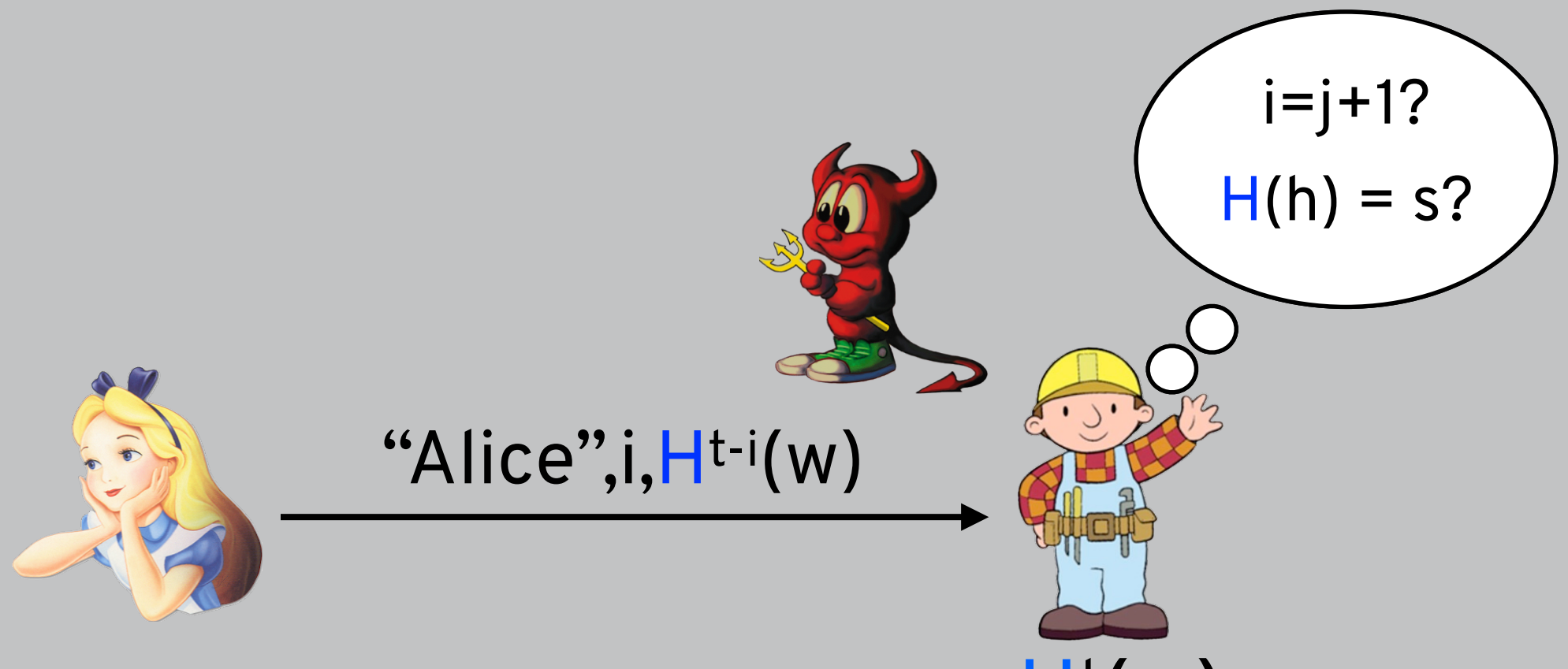
ONE-TIME PASSWORDS



ONE-TIME PASSWORDS



ONE-TIME PASSWORDS



pre-image resistance: given h , hard to find m such that $H(m) = h$

SECURE MESSAGING

	<u>Encrypted in transit?</u>	<u>Encrypted so the provider can't read it?</u>	<u>Can you verify contacts' identities?</u>	<u>Are past comms secure if your keys are stolen?</u>
FACEBOOK	yes	no		
IMESSAGE	yes	yes		
SIGNAL	yes	yes		
TELEGRAM	yes	no		
WHATSAPP	yes	yes		

what enables encryption is
keys stored on your device

SECURE MESSAGING

← Change number

✓ NEXT

← Change number

✓ DONE

SMS Verification

Changing your phone number will migrate your account info, groups and settings.

Before proceeding, please confirm that you are able to receive SMS or calls at your new number.

If you have both a new phone and a new number, first change your number on your old phone.

Please enter your old country code and phone number:

+ 1 1 234 567 8901

Please enter your new country code and phone number:

+ 1 1 234 567 8901

1 2 3 -

4 5 6 .

7 8 9 ✕

* # 0 + _ ✓

Waiting to automatically detect an SMS sent to

+1 1 234 567 8901

04:53

Please make sure you have a working SMS plan.

Sit back and relax. We'll notify you when we're done verifying.



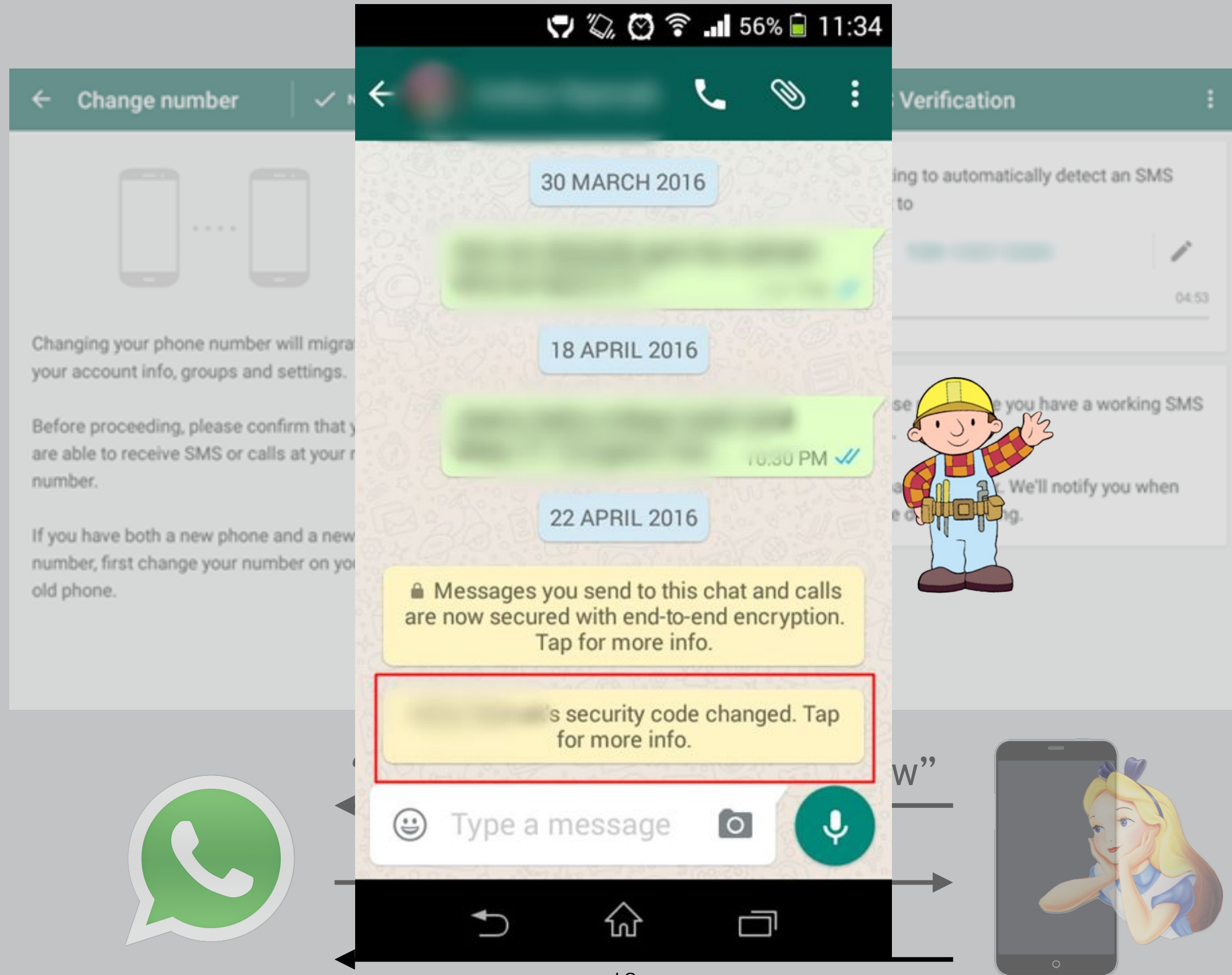
“I represent 07777 123456 now”

“prove it” (via SMS)

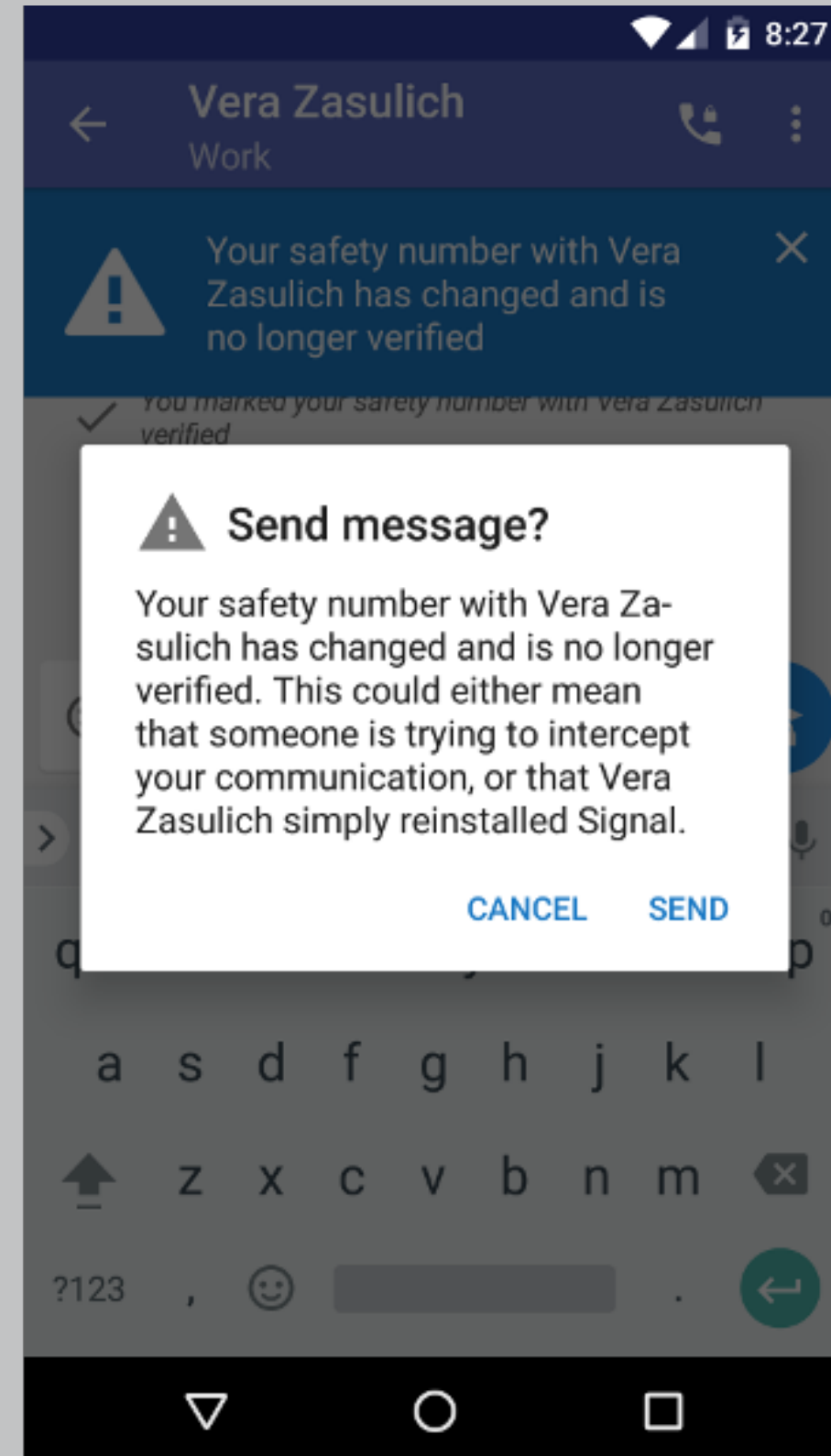
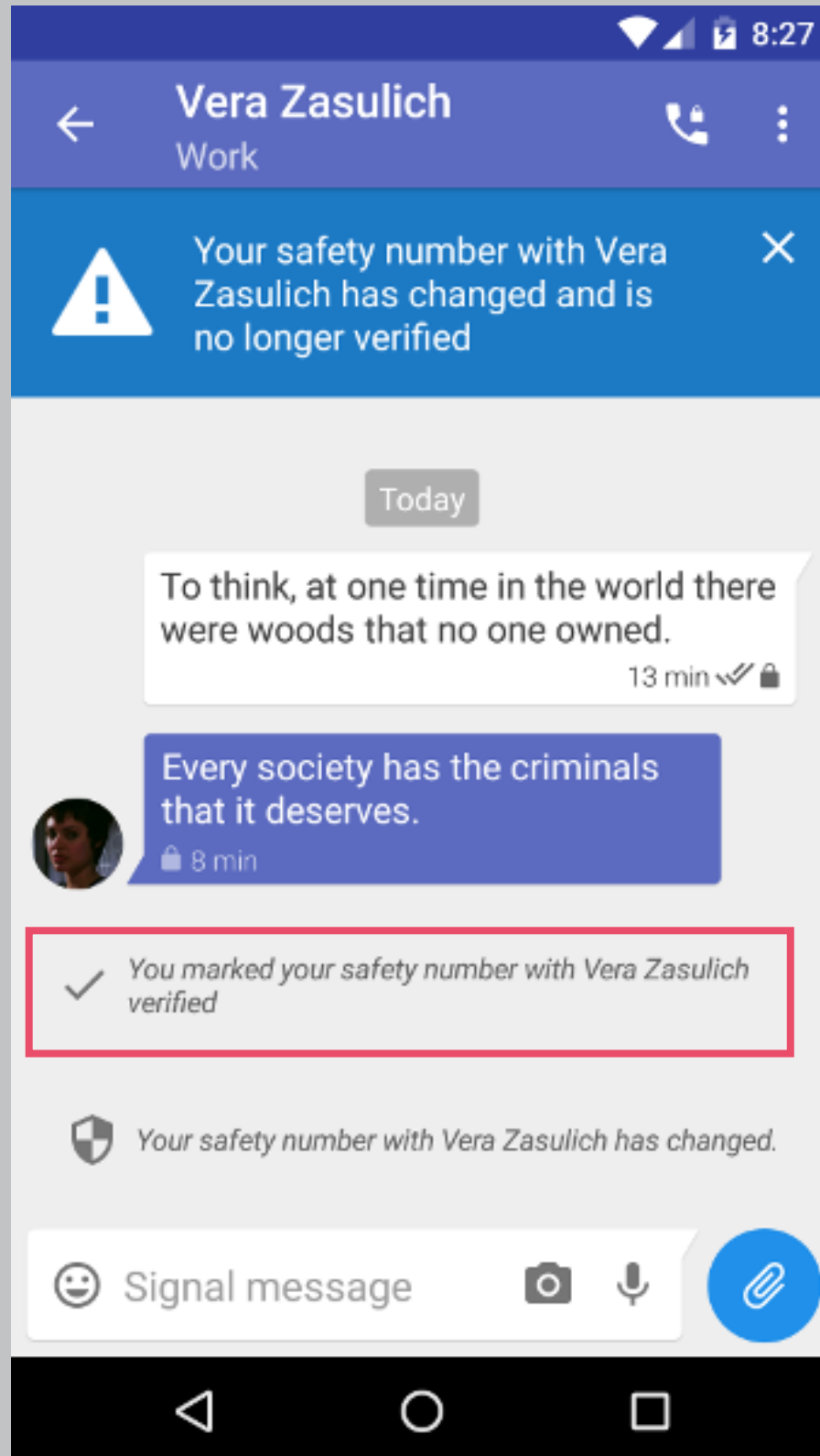
<verification code>



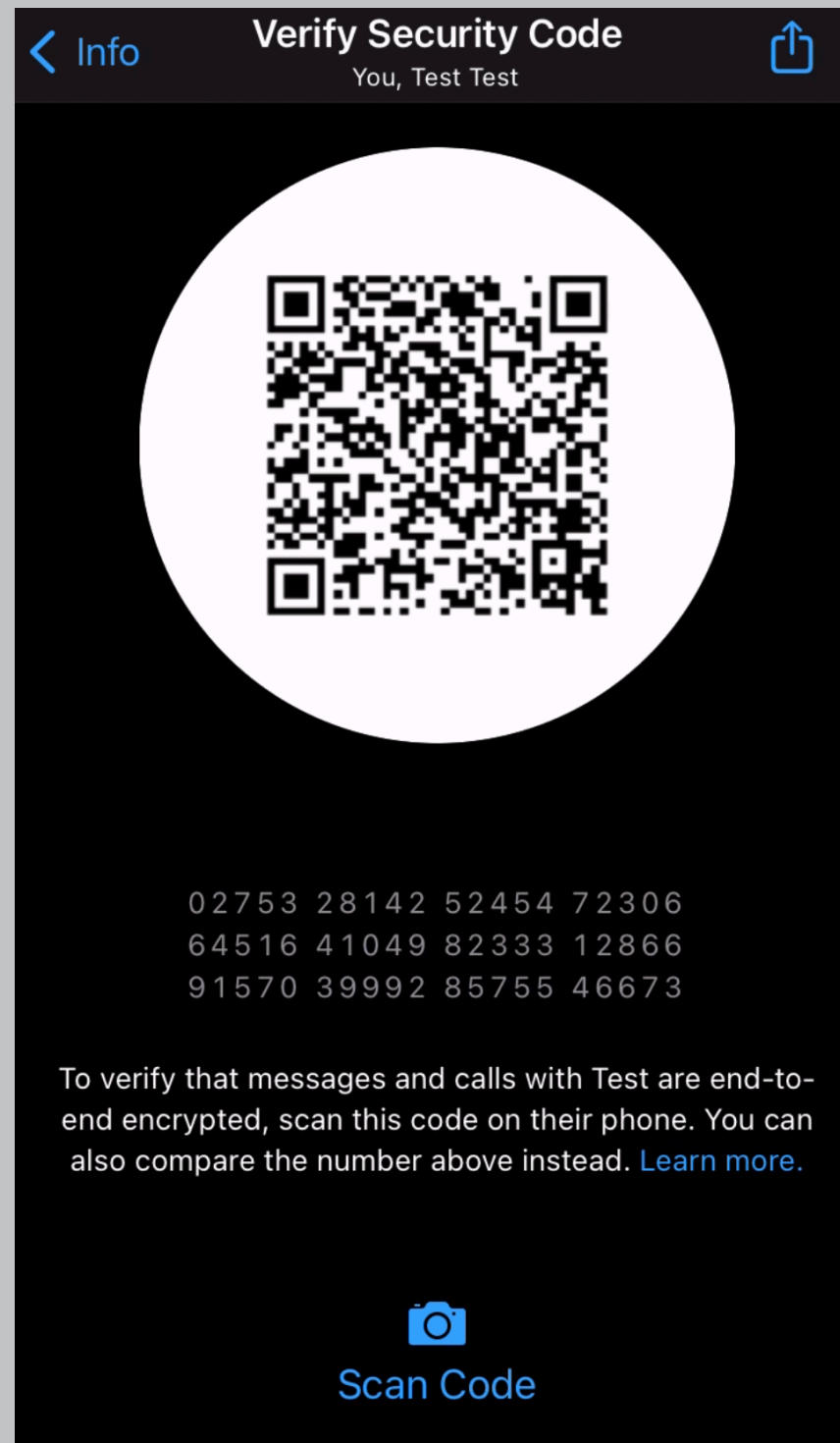
SECURE MESSAGING



SECURE MESSAGING



KEY VERIFICATION DEMO



SECURE MESSAGING

	<u>Encrypted in transit?</u>	<u>Encrypted so the provider can't read it?</u>	<u>Can you verify contacts' identities?</u>	<u>Are past comms secure if your keys are stolen?</u>
FACEBOOK	yes	no	no	
IMESSAGE	yes	yes	no	
SIGNAL	yes	yes	yes	
TELEGRAM	yes	no	no	
WHATSAPP	yes	yes	yes	

AUTHENTICATION

Authentication is:

What you know

text passwords

graphical passwords

personal details

What you have

RFID card

cryptographic tokens

What you are