SECURITY (COMP0141):

WHAT YOU HAVE

UCL

AUTHENTICATION

Authentication is:

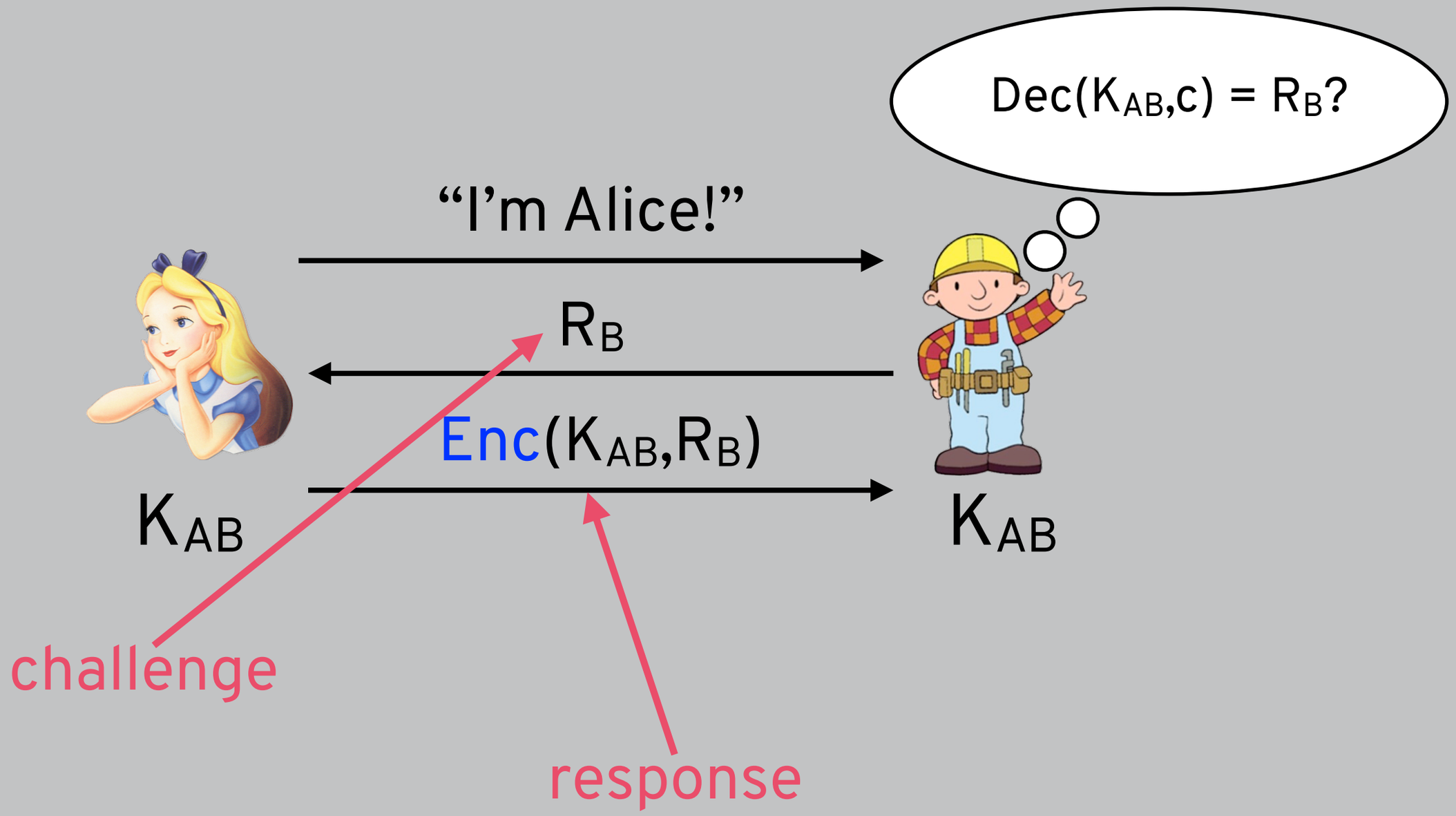
What you know

text passwords graphical passwords personal details

What you have

What you are

CHALLENGE-RESPONSE



CHALLENGE-RESPONSE

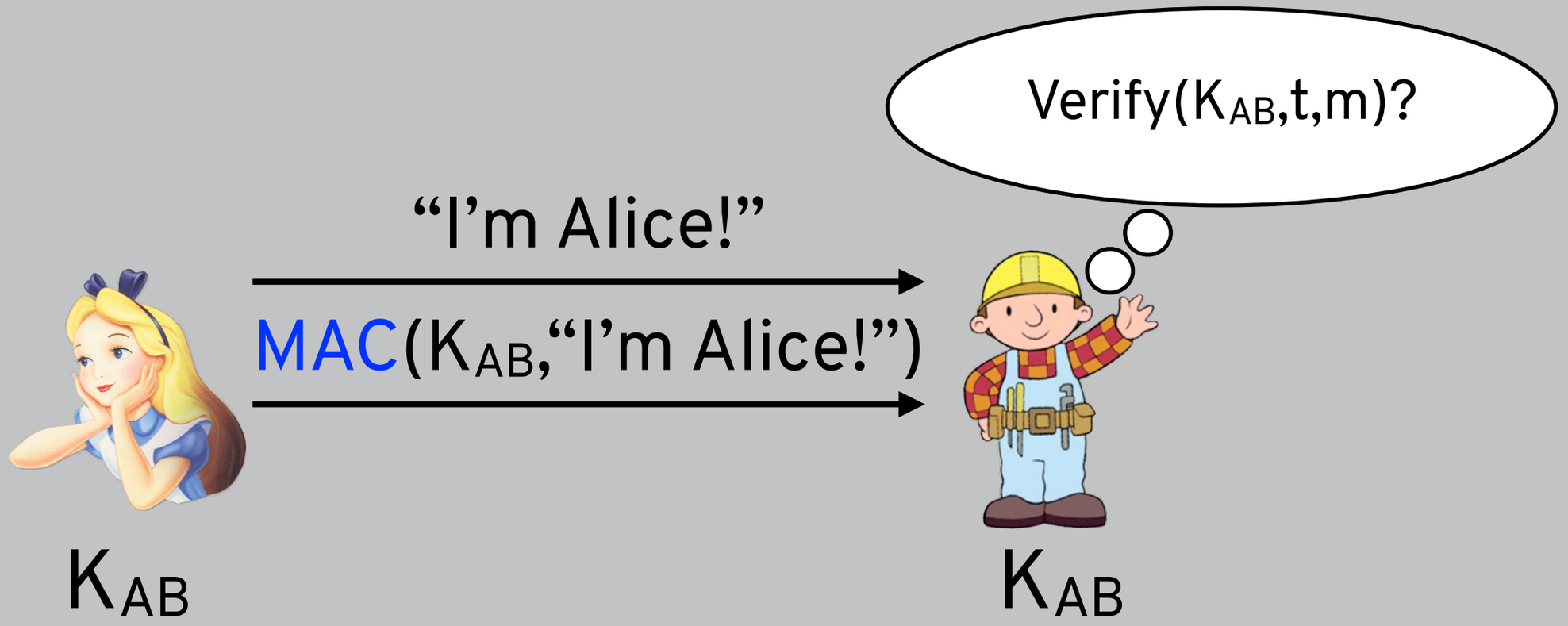
RFID: Radio Frequency IDentification

?

challénge

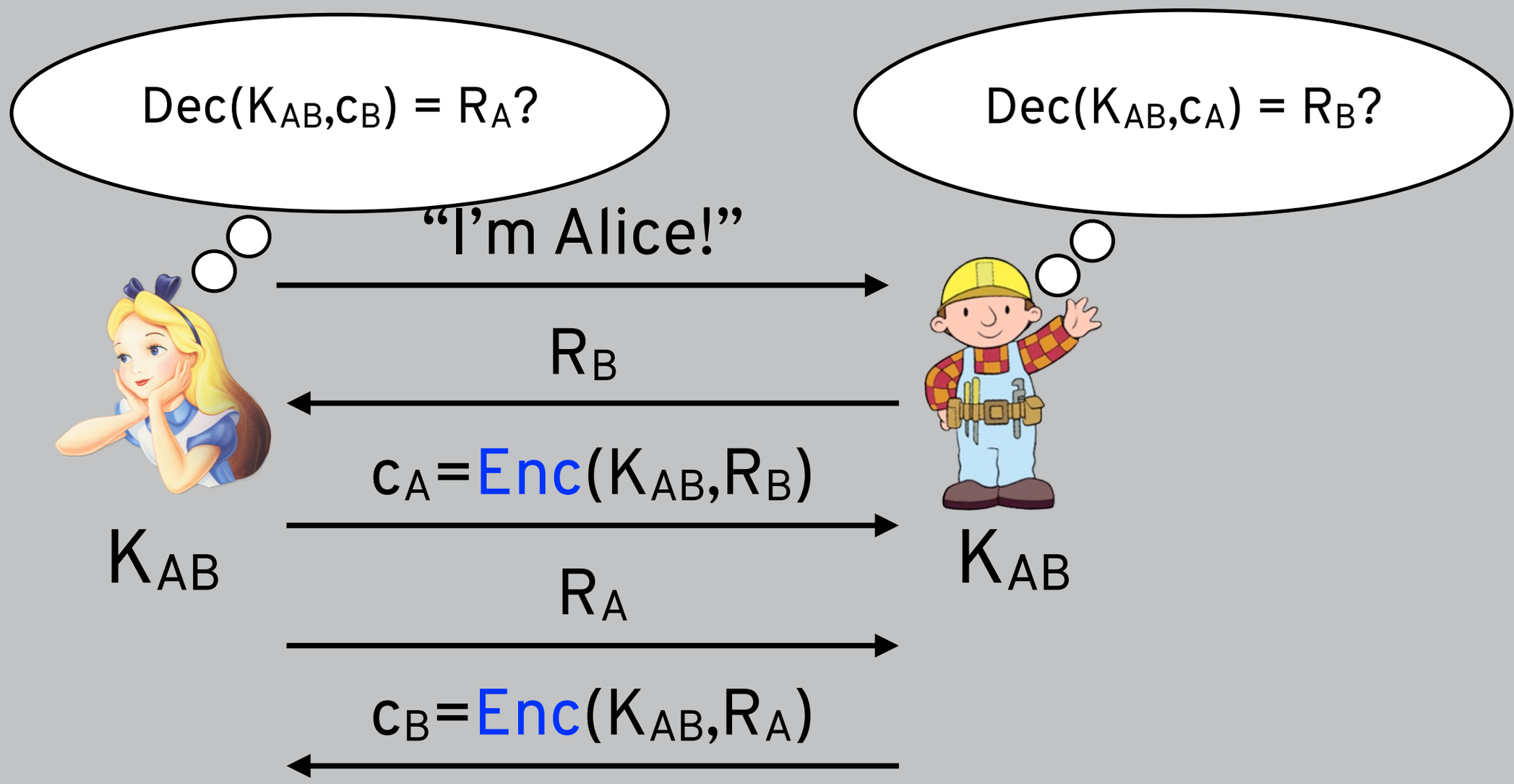
NFC: Near Field Communication

WHY NOT DO THIS?

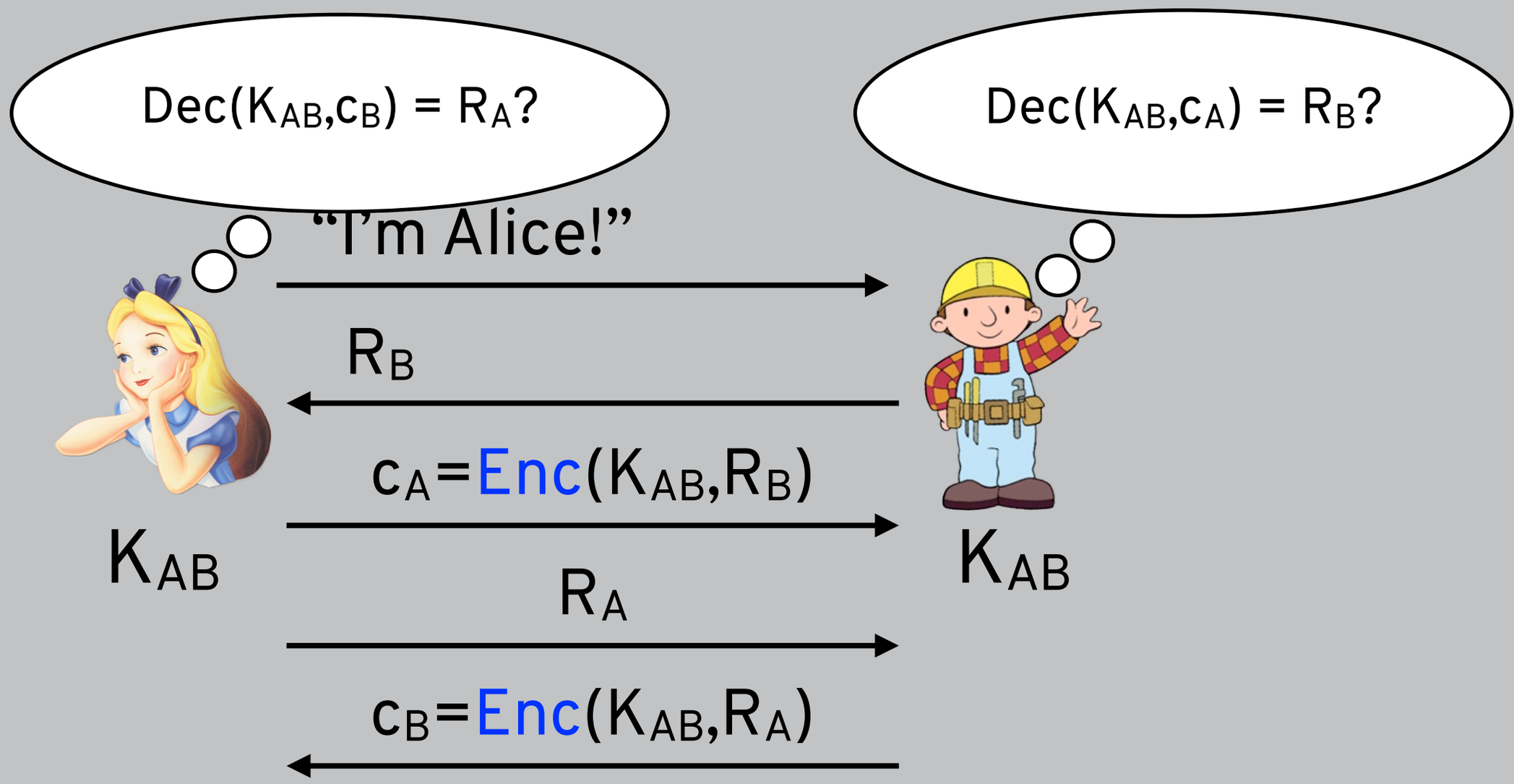


this doesn't work in really constrained environments!

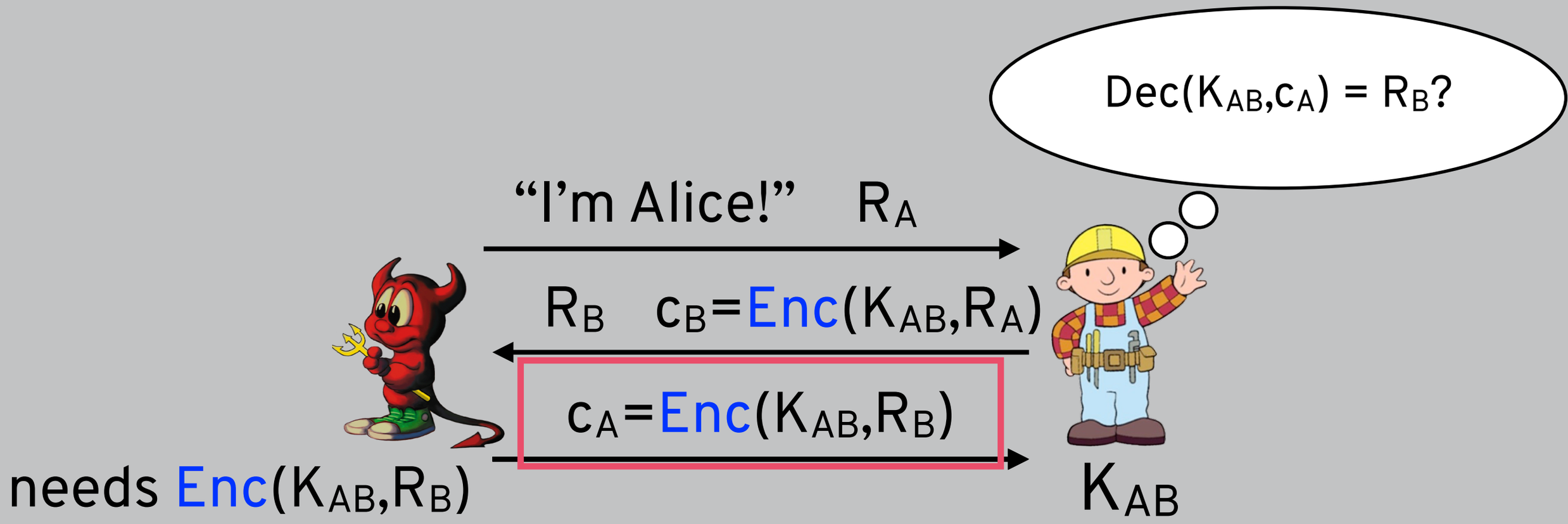
TWO-WAY CHALLENGE-RESPONSE



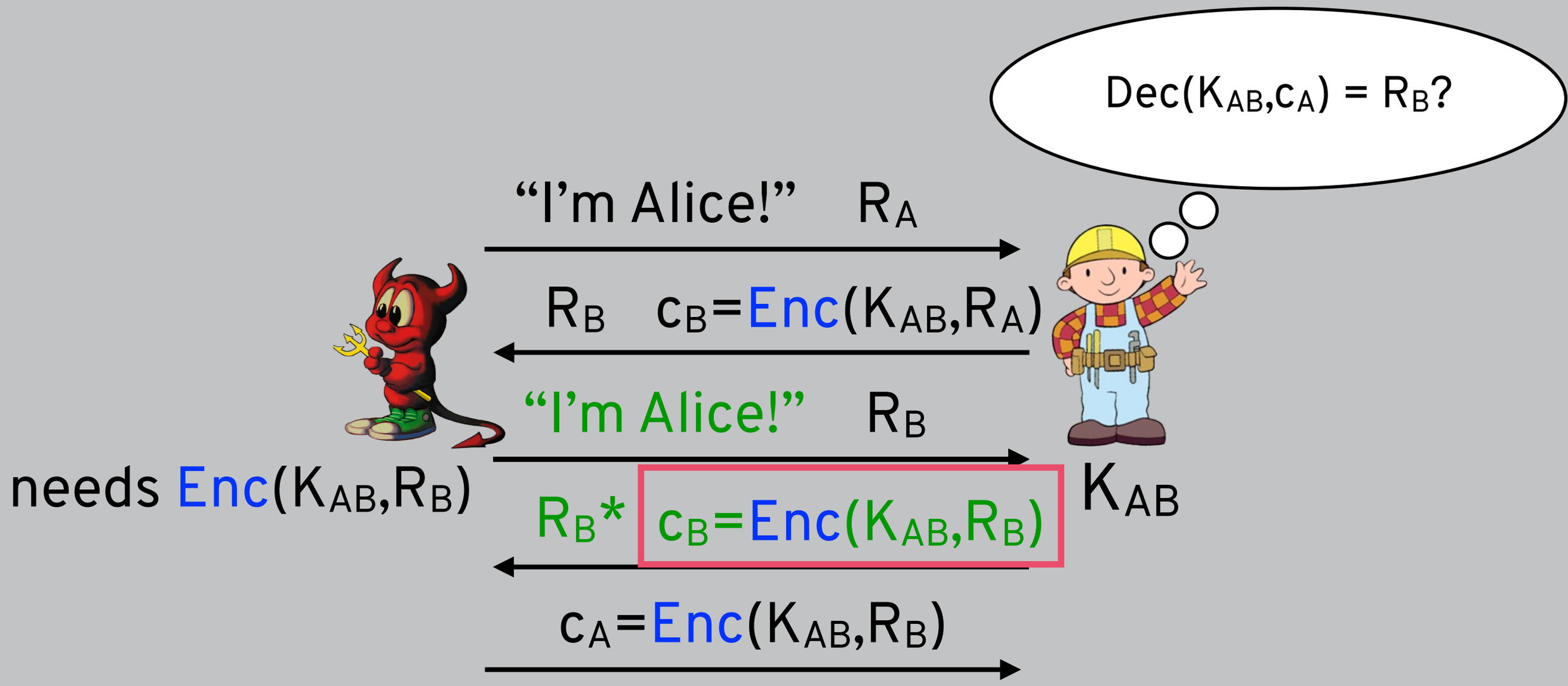
WHY NOT DO THIS?



WHY NOT DO THIS?

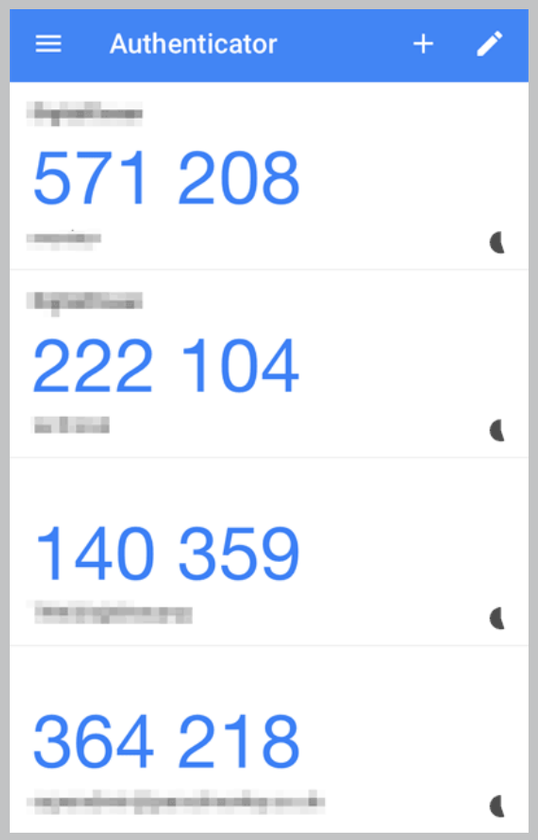


WHY NOT DO THIS?



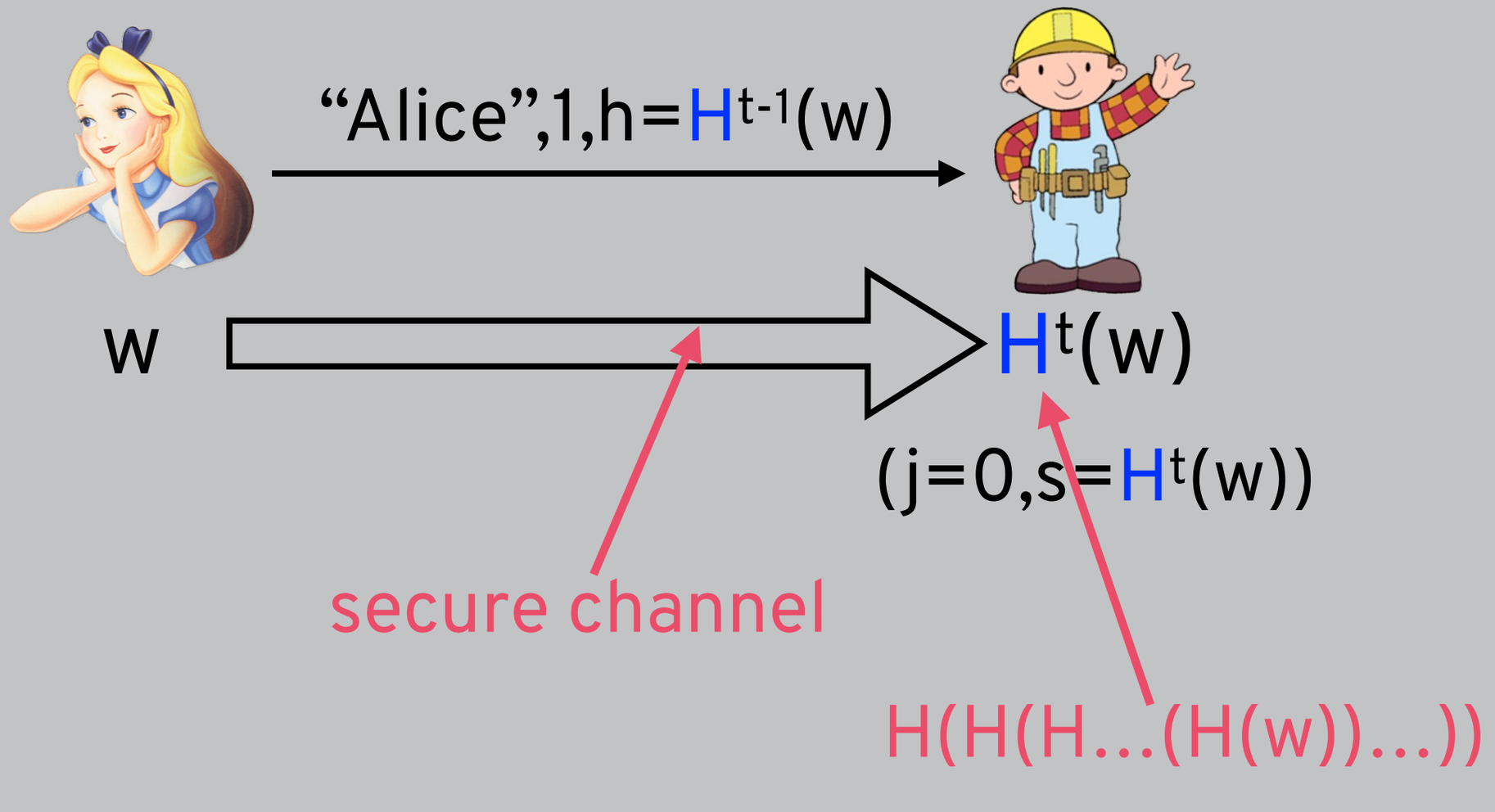
don't design your own crypto!
need to consider **all** possible attackers

ONE-TIME PASSWORDS



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

ONE-TIME PASSWORDS



ONE-TIME PASSWORDS

w

“Alice”,i,$H^{t-i}(w)$

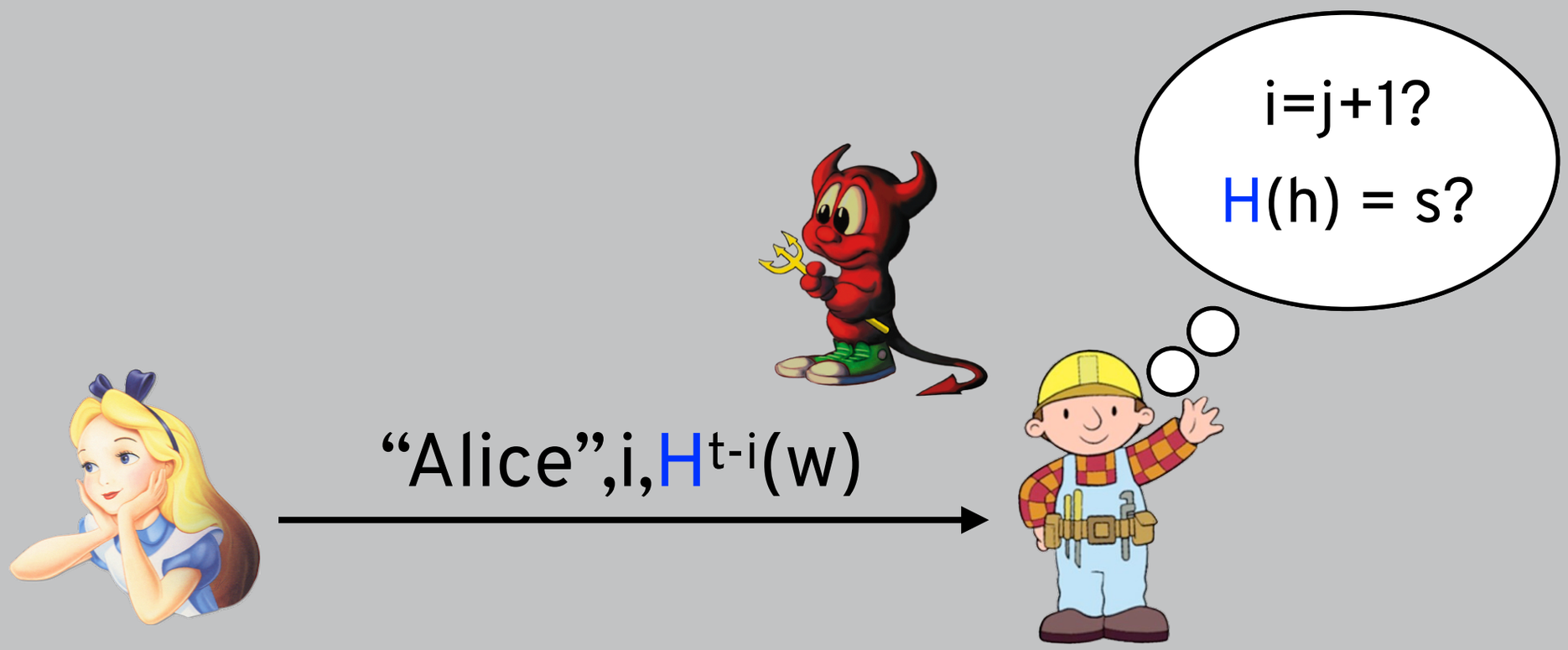
$H^t(w)$

i=j+1?

H(h) = s?

($j=i-1$, $s=H^{t-i}(w)$)

ONE-TIME PASSWORDS



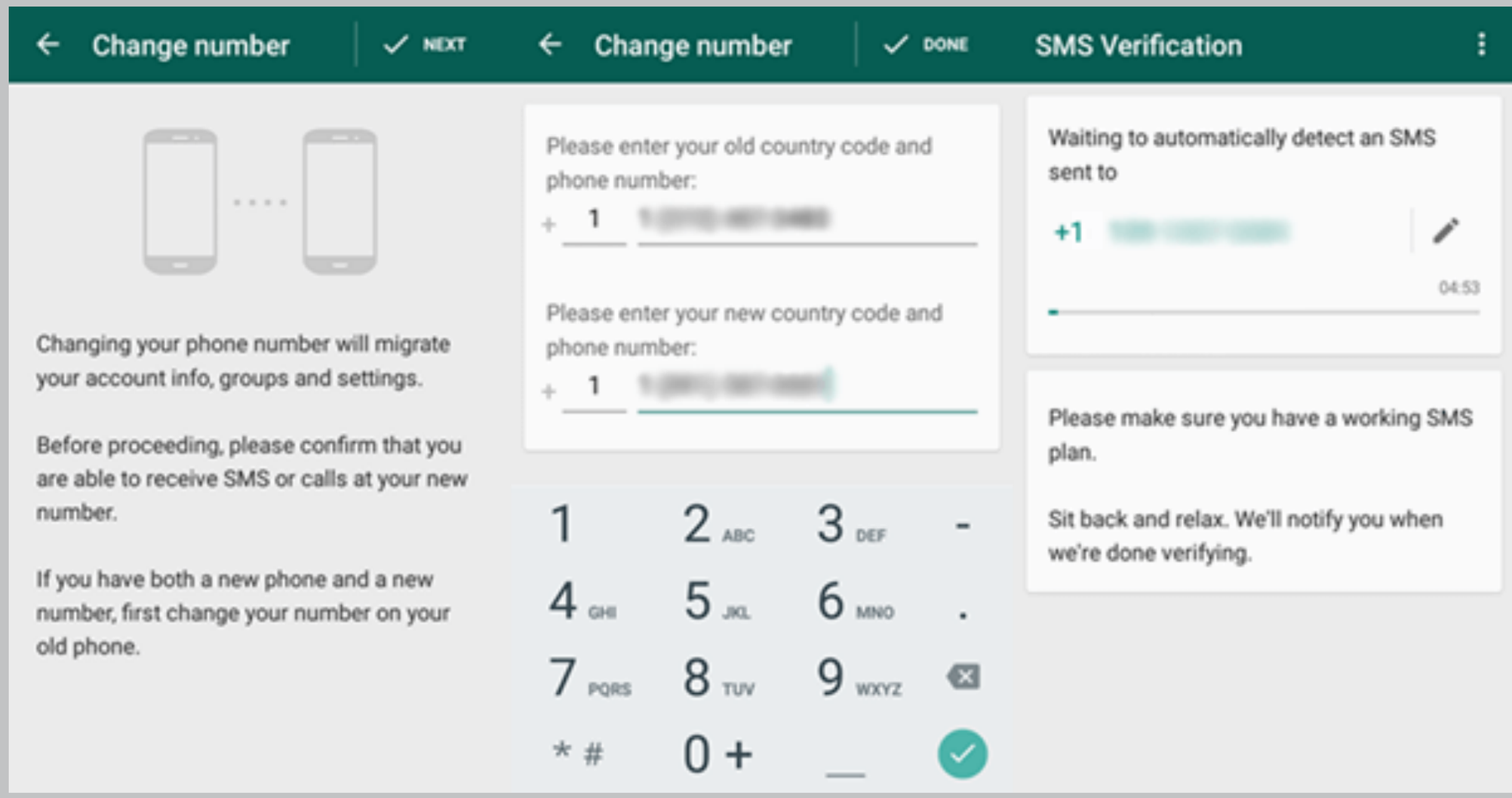
pre-image resistance: given h, hard to find m such that H(m) = h

SECURE MESSAGING

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?
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

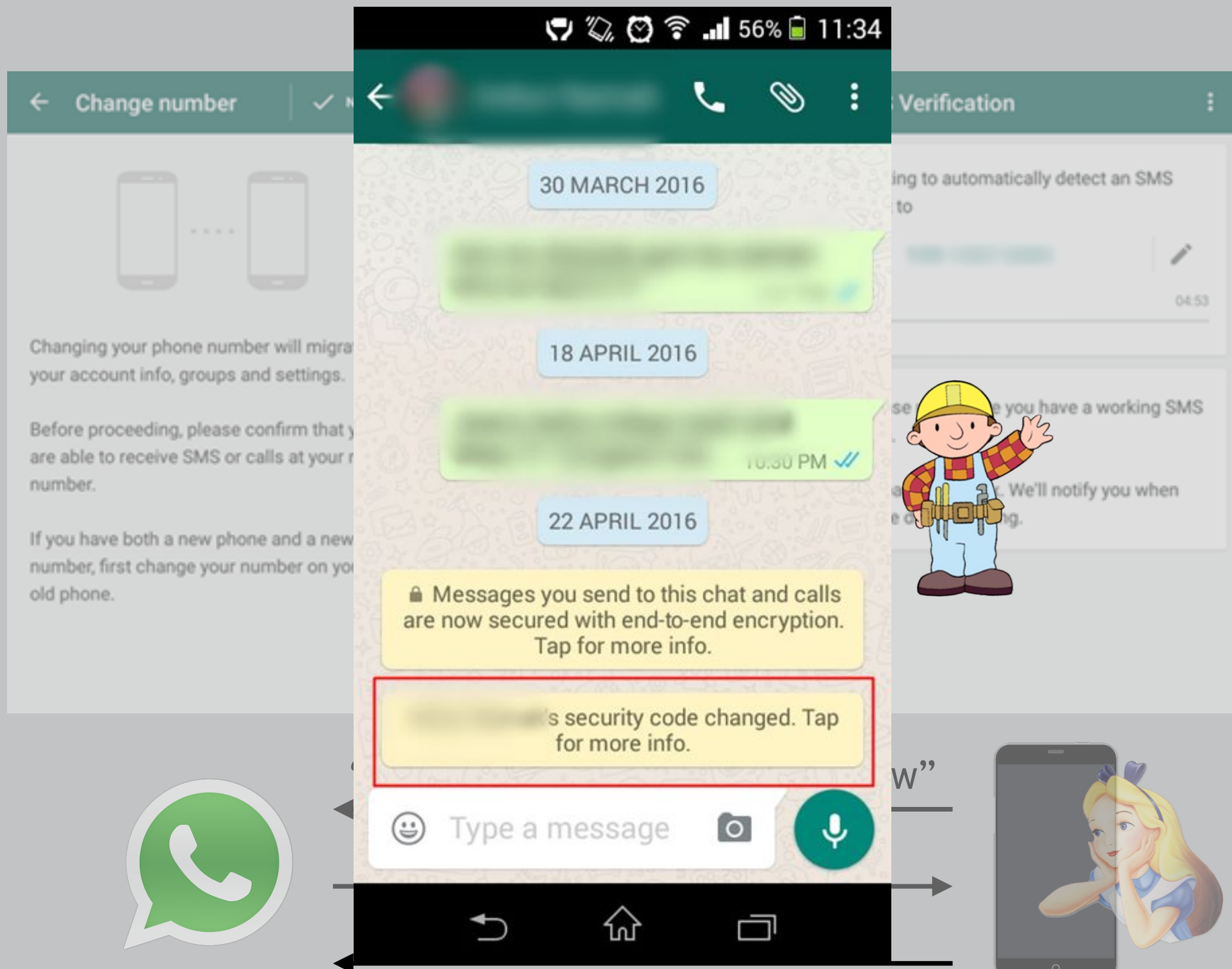


"I represent 07777 123456 now"

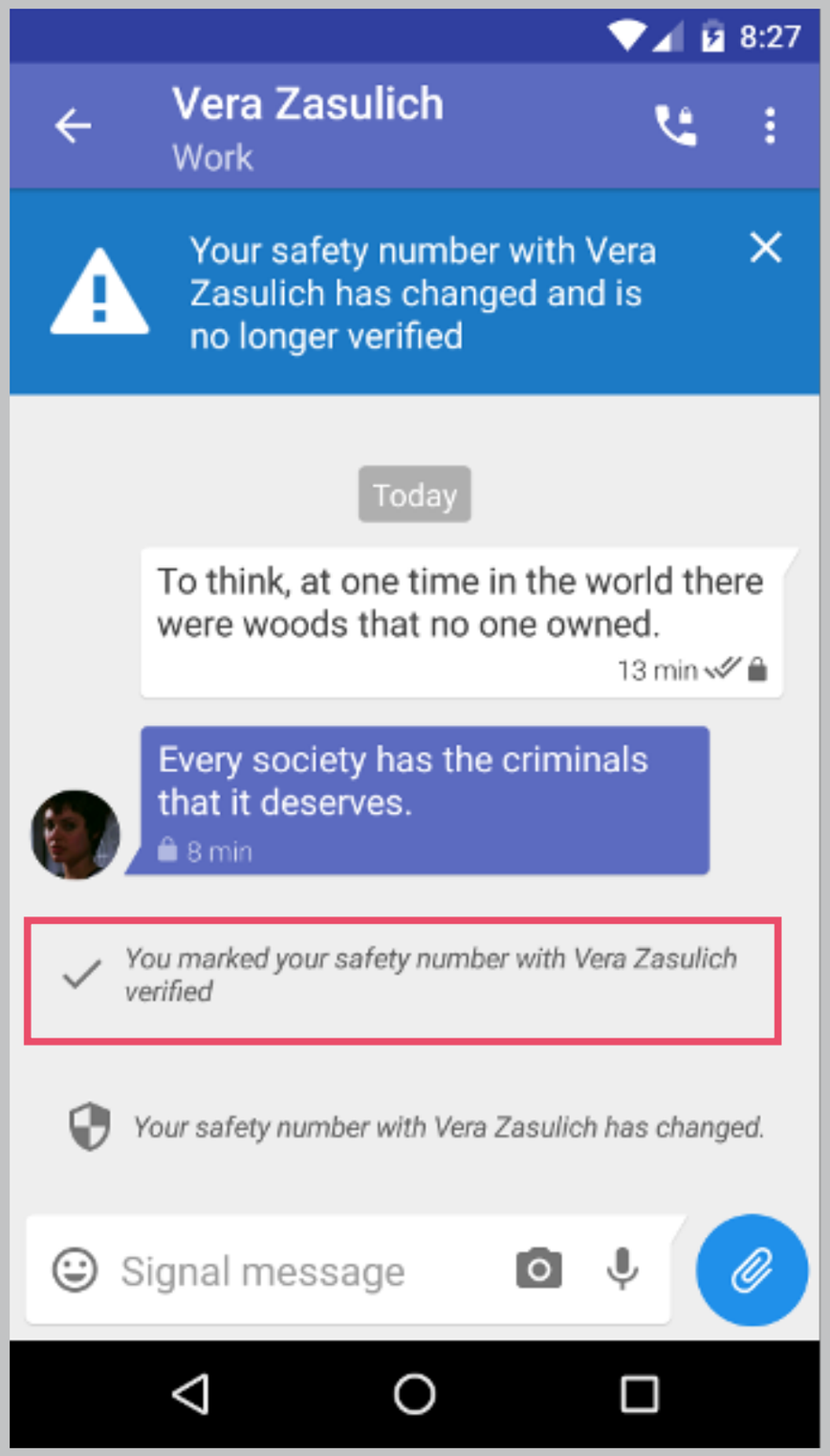
"prove it" (via SMS)

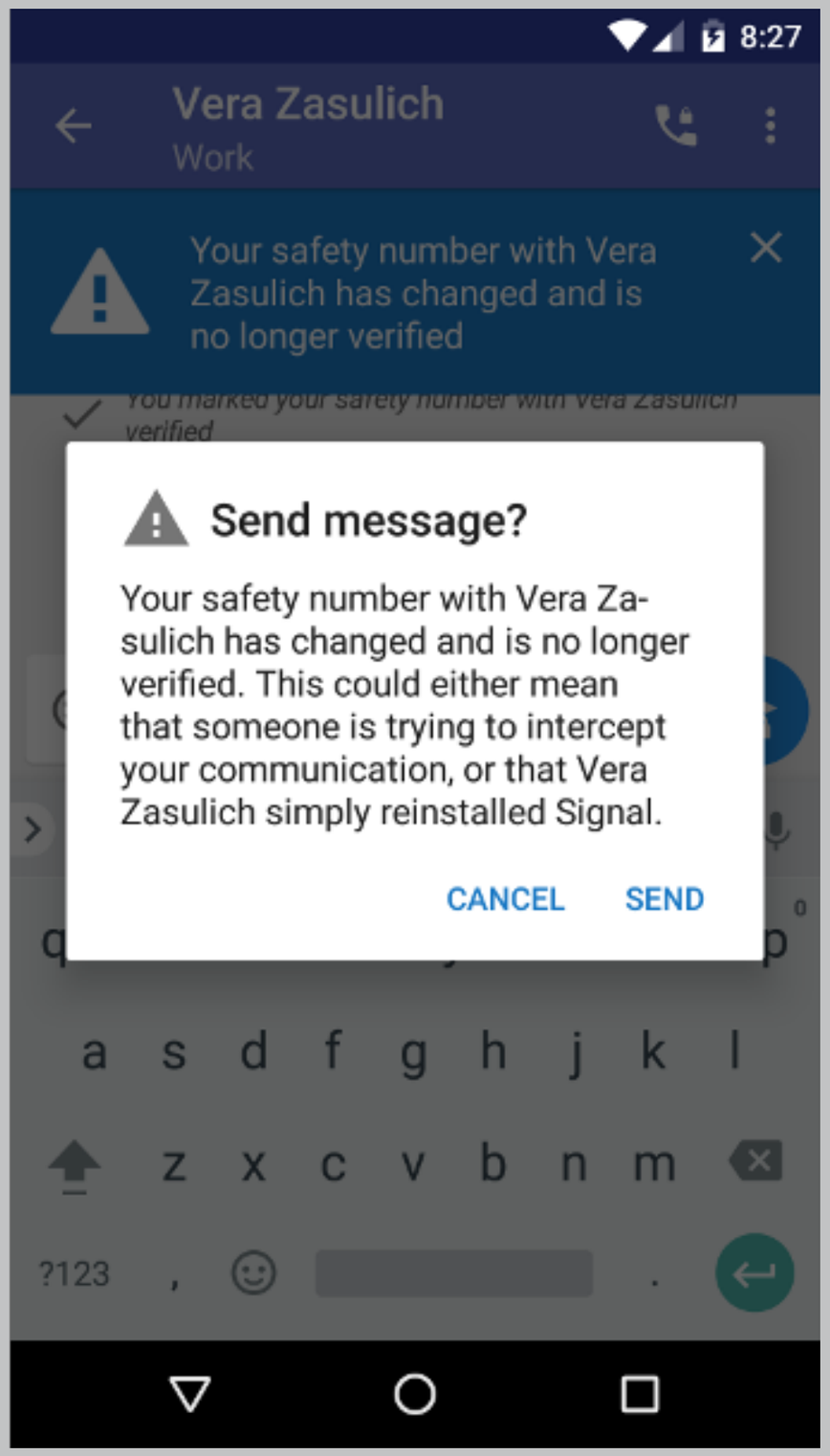
<verification code>

SECURE MESSAGING

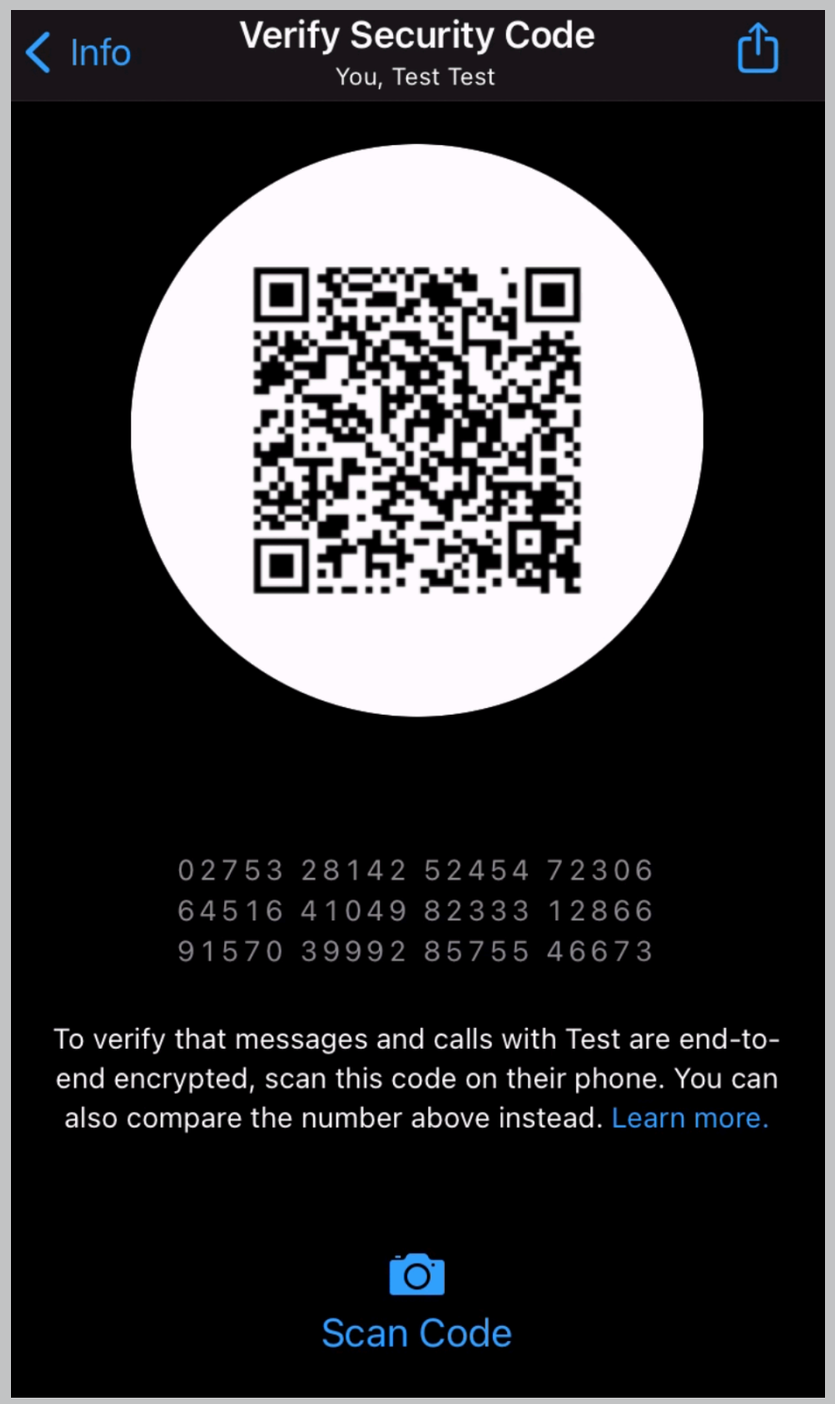


SECURE MESSAGING





KEY VERIFICATION DEMO



SECURE MESSAGING

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?
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