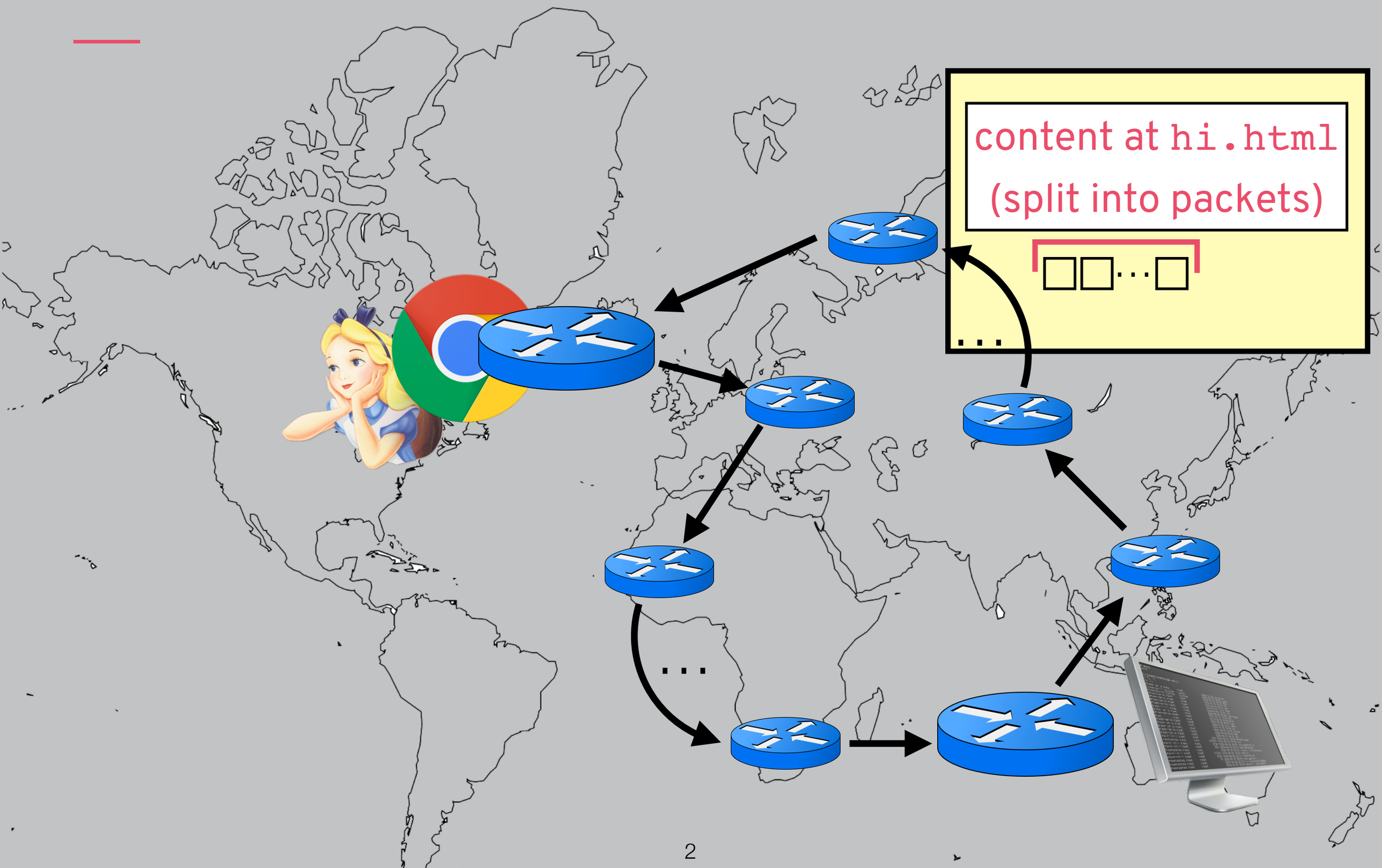
SECURITY (COMP0141):
ENCRYPTED WEB TRAFFIC

UCL

STEP 3: RECEIVE CONTENT



PACKETS

4-bit version	4-bit Header len	8-bit type of service	16-bit total length (in bytes)
16-bit identification		3-bit flags	13-bit fragment offset
8-bit time to live (TTL)	8-bit protocol	16-bit header checksum	
Bob's IP address			
Alice's IP address			
Options (if any)			
<Content at `hi.html` (part 1 of N)>			

as is, anyone can read your web traffic

STEP 3: RECEIVE CONTENT

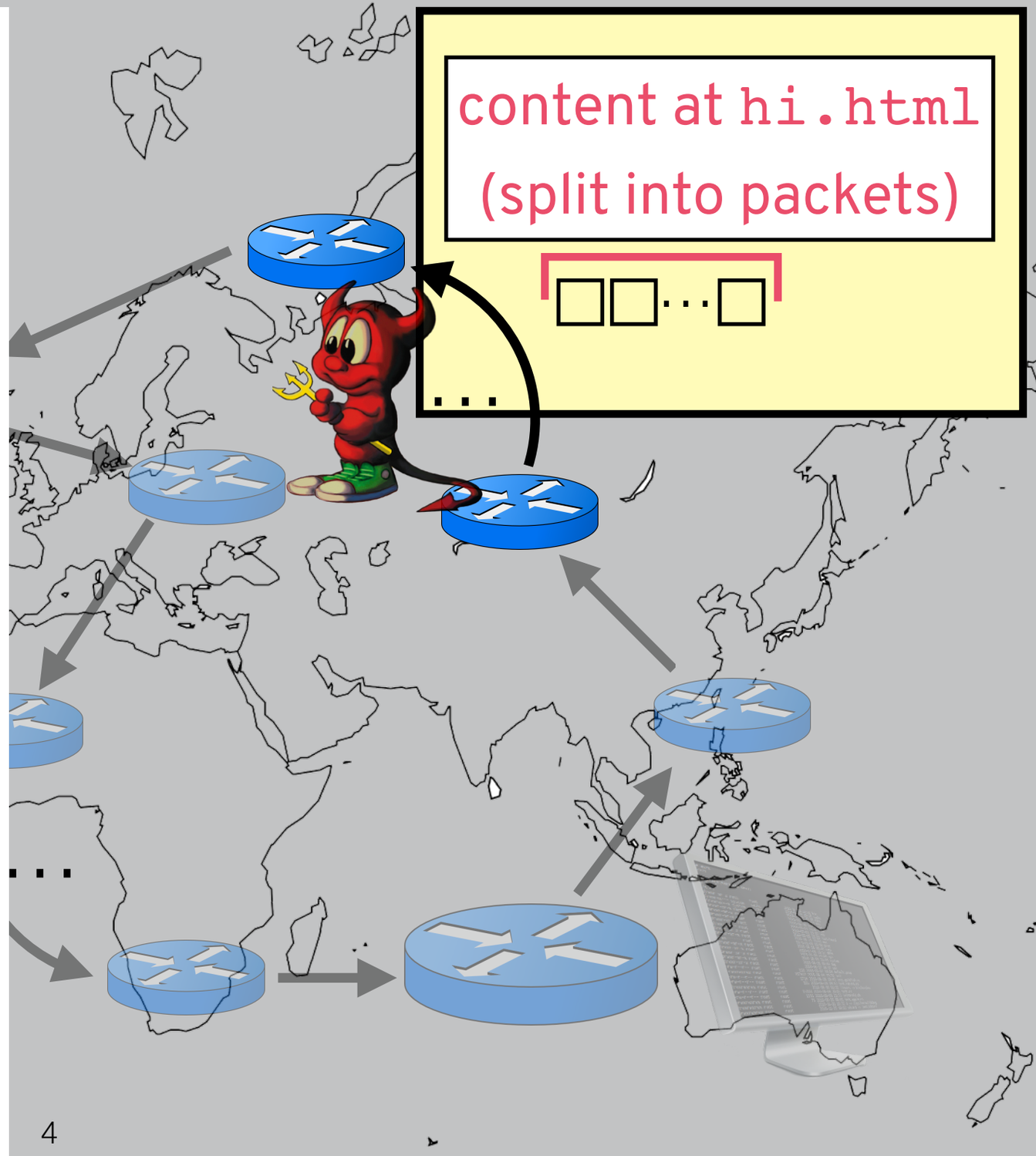
motivation?

nosy coffee shop neighbour

credential thief

government agency

capability?



SESSION KEYS

PKI
pk_u
⋮
pk_B

use expensive operation once (per session)…

…don't store keys…

pk_B

$c=Enc(pk_B,sk)$

$Dec(sk_B,c)$

pk_B

$(pk_B,sk_B) \leftarrow KeyGen(\ )$

session key sk

sk

…encrypt messages using cheap operations

ENCRYPTED WEB TRAFFIC

4-bit version	4-bit Header len	8-bit type of service	16-bit total length (in bytes)	
16-bit identification			3-bit flags	13-bit fragment offset
8-bit time to live (TTL)		8-bit protocol	16-bit header checksum	
Bob's IP address				
Alice's IP address				
Options (if any)				
Enc(sk,<Content at `hi.html` (part 1 of N)>**)**				

HYBRID ENCRYPTION

This general method is called **hybrid encryption**

To encrypt a long message m:

- Pick a random (symmetric) session key K
- Encrypt K with c_1 = PKE.Enc(pk,K)
- Encrypt m with c_2 = SKE.Enc(K,m)
- The ciphertext is c = (c_1,c_2)

To decrypt and recover m:

- Compute K = PKE.Dec(sk,c_1)
- Compute m = SKE.Dec(K,c_2)
- The ciphertext is c = (c_1,c_2)

LINGERING QUESTIONS

q: does encrypted web traffic still reveal IP addresses?

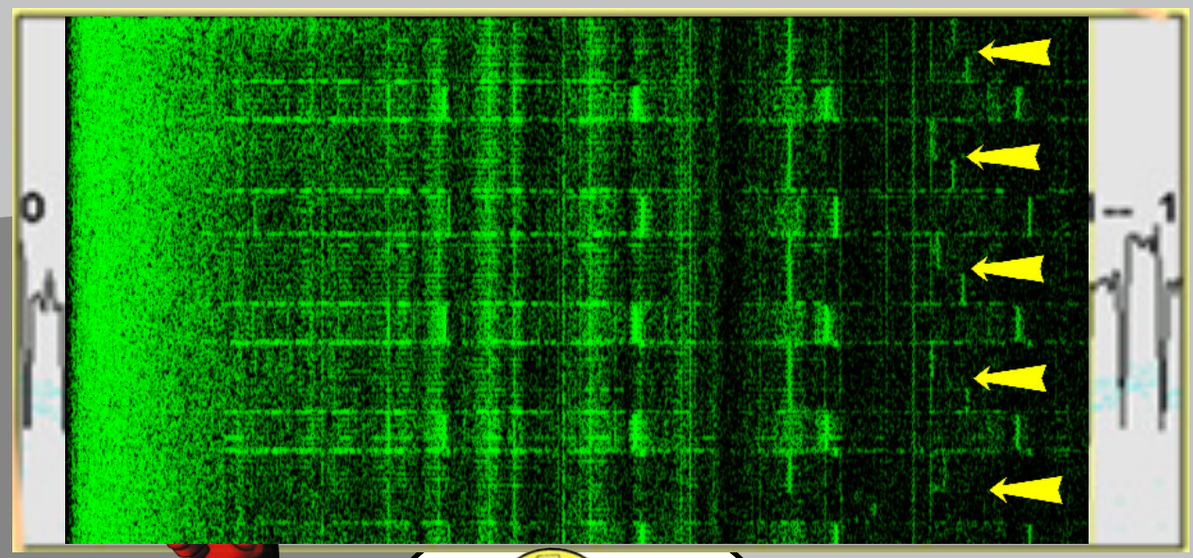
a: yes! to avoid this, use proxies or **onion routing** (e.g., Tor).

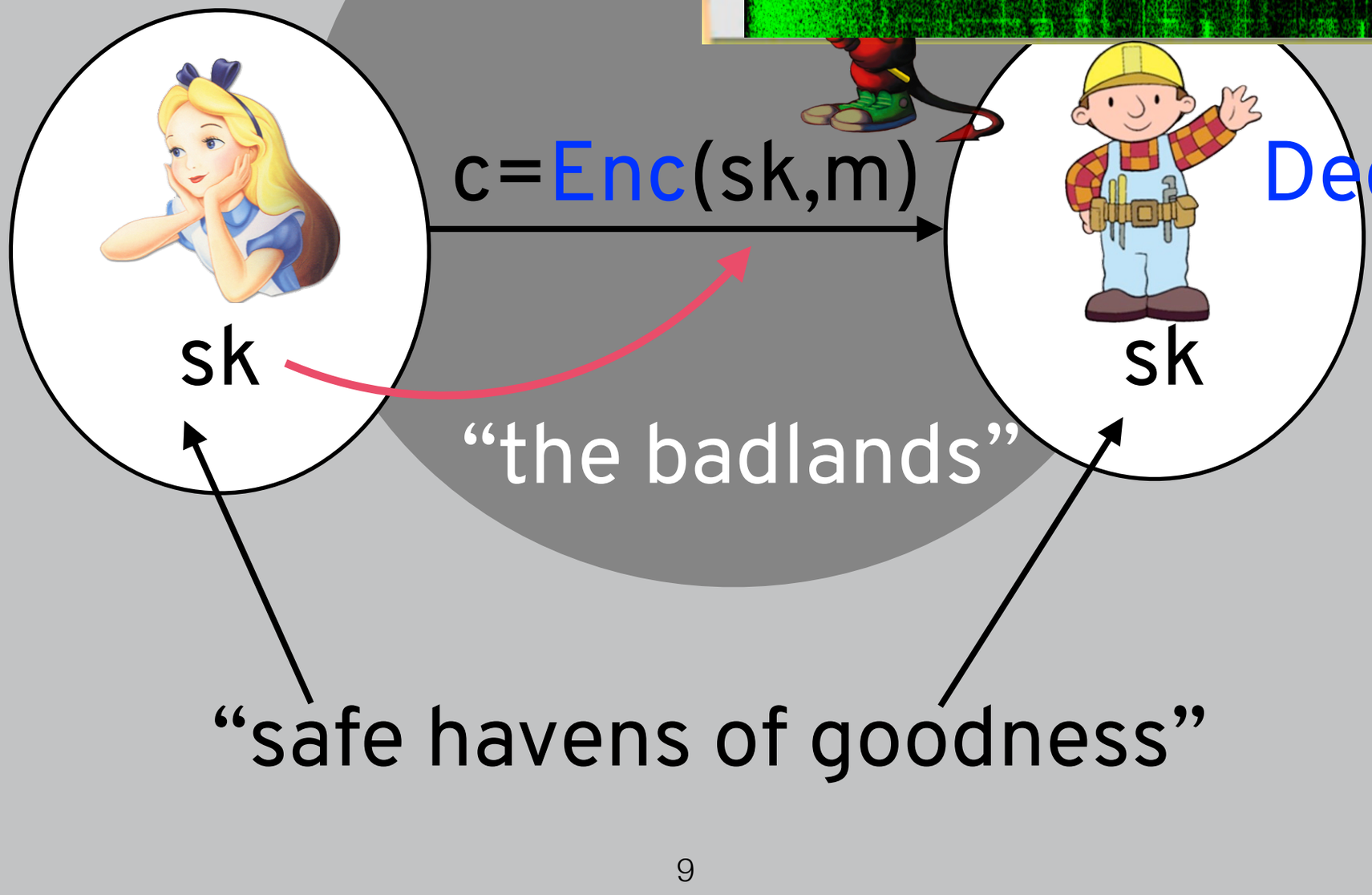
q: is communication channel the only attack surface?

a: no! **side channels** exploit weaknesses on either side.

SIDE CHANNELS

- timing
- power draw (DPA)
- acoustics





LINGERING QUESTIONS

q: does encrypted web traffic still reveal IP addresses?

a: yes! to avoid this, use proxies or **onion routing** (e.g., Tor).

q: is communication channel the only attack surface?

a: no! **side channels** exploit weaknesses on either side.

q: how does Alice actually know it's Bob?

a: stay tuned for next week!