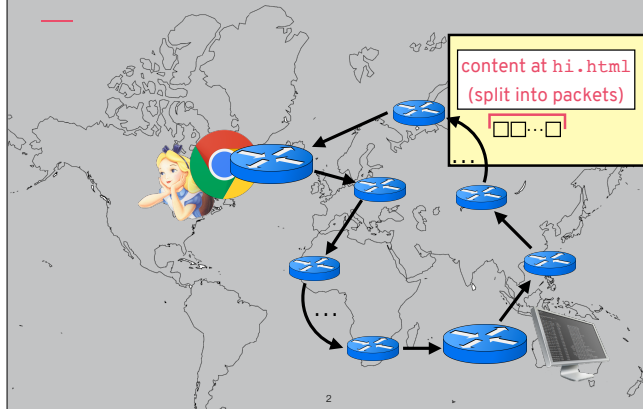


SECURITY (COMP0141): ENCRYPTED WEB TRAFFIC



STEP 3: RECEIVE CONTENT



Remember from last week that packets are sent all around the internet

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



3

If we don't encrypt them, anyone can read them

STEP 3: RECEIVE CONTENT

motivation?

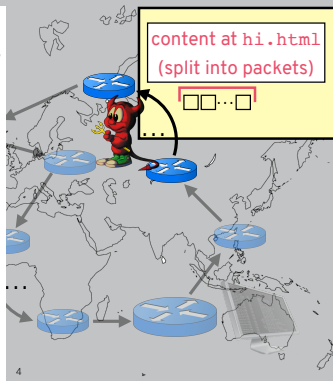
nosy coffee shop neighbour
credential thief
government agency

capability?



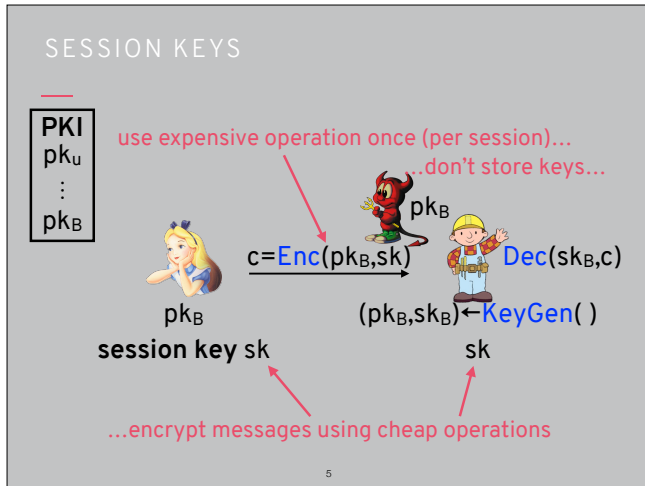
content at hi.html
(split into packets)

...

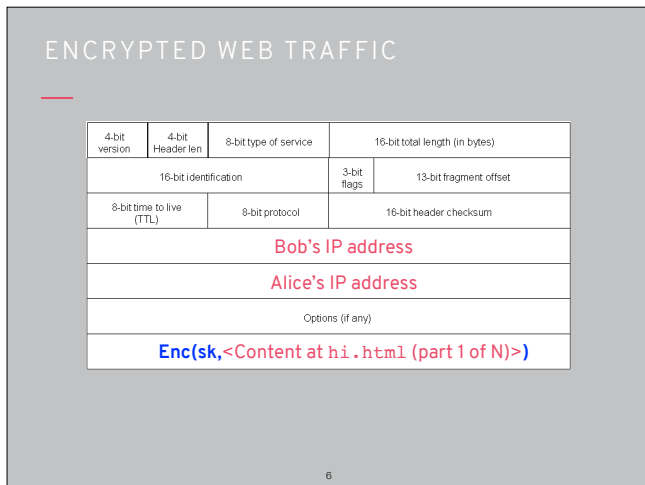


4

Going back to threat model, there are obvious motivations ranging from curiosity to state-level attacks, and there are a lot of tools that make this easy so don't need specialist capabilities



In practice, we combine the advantages of both by using public-key encryption once to establish a shared session key



The session key is then used to encrypt all our packets, and at the end of the session it is discarded

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 $c_1 = \text{PKE.Enc}(pk, K)$
- Encrypt m with $c_2 = \text{SKE.Enc}(K, m)$
- The ciphertext is $c = (c_1, c_2)$

To decrypt and recover m :

- Compute $K = \text{PKE.Dec}(sk, c_1)$
- Compute $m = \text{SKE.Dec}(K, c_2)$
- The ciphertext is $c = (c_1, c_2)$

7

On the Internet we do this for multiple messages in a given session, but it can even be beneficial for single long messages as well. The overall cryptographic primitive this exemplifies is called hybrid encryption

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?

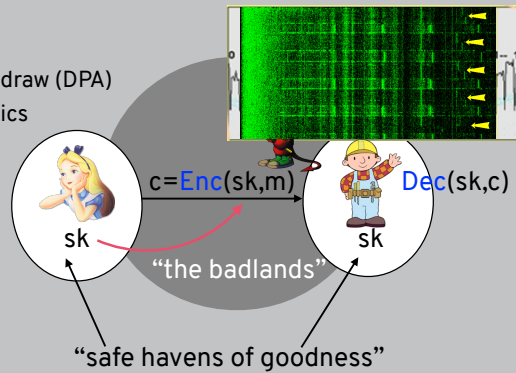
a: no! **side channels** exploit weaknesses on either side.

8

We'll see Tor later on, remember that packet is an envelope and a letter and we haven't yet hidden the address information

SIDE CHANNELS

- timing
- power draw (DPA)
- acoustics



Side channels are prevalent and demonstrate that the communication channel isn't the only thing that can be attacked (again, need to consider attacker capabilities)

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!

We still don't know who we're talking to though, this will be addressed with integrity next time