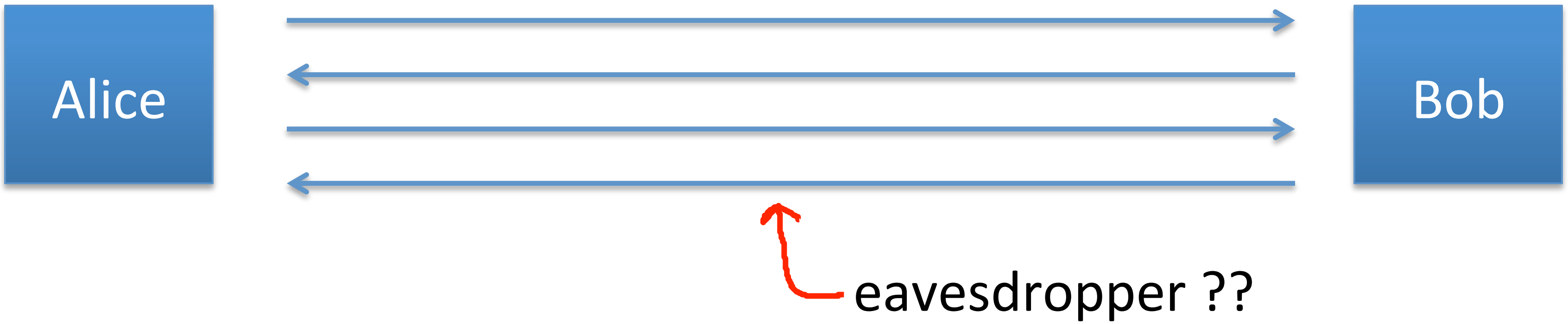
Basic key exchange

The Diffie-Hellman protocol

Key exchange without an online TTP?

Goal: Alice and Bob want shared secret, unknown to eavesdropper

- For now: security against eavesdropping only (no tampering)



Can this be done with an exponential gap?

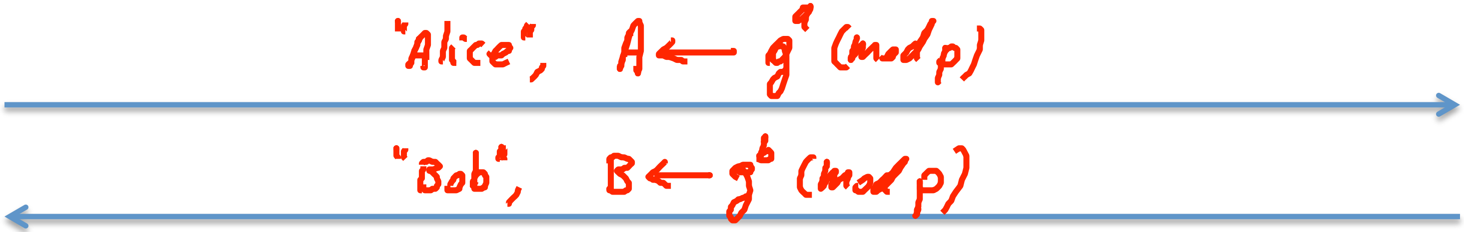
The Diffie-Hellman protocol (informally)

Fix a large prime p (e.g. 600 digits)

Fix an integer g in {1, …, p}

Alice **Bob**

choose random **a** in {1,…,p-1} choose random **b** in {1,…,p-1}



"Alice", $A \leftarrow g^a \pmod{p}$

"Bob", $B \leftarrow g^b \pmod{p}$

$$\mathbf{B^a} \pmod{p} = (g^b)^a = \mathbf{k_{AB} = g^{ab}} \pmod{p} = (g^a)^b = \mathbf{A^b} \pmod{p}$$

Security (much more on this later)

Eavesdropper sees: $p, g,$ $A=g^a \pmod p$, and $B=g^b \pmod p$

Can she compute $g^{ab} \pmod p$??

More generally: define $DH_g(g^a, g^b) = g^{ab} \pmod p$

How hard is the DH function mod p?

How hard is the DH function mod p?

Suppose prime p is n bits long.

Best known algorithm (GNFS): run time exp($\tilde{O}(\sqrt[3]{n})$)

cipher key size	modulus size	Elliptic Curve size
80 bits	1024 bits	160 bits
128 bits	3072 bits	256 bits
256 bits (AES)	**15360** bits	512 bits

As a result: slow transition away from (mod p) to elliptic curves

www.google.com

The identity of this website has been verified by Thawte SGC CA.

Certificate Information

Your connection to www.google.com is encrypted with 128-bit encryption.

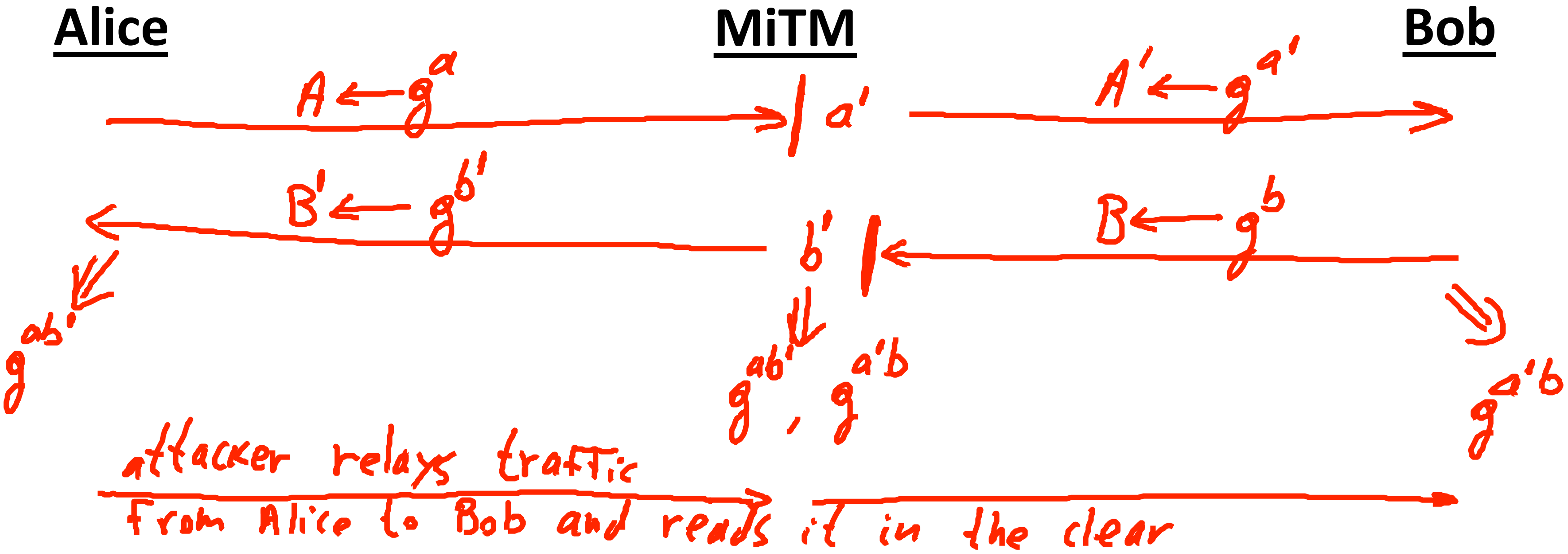
The connection uses TLS 1.0.

The connection is encrypted using RC4_128, with SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism.

Elliptic curve
Diffie-Hellman

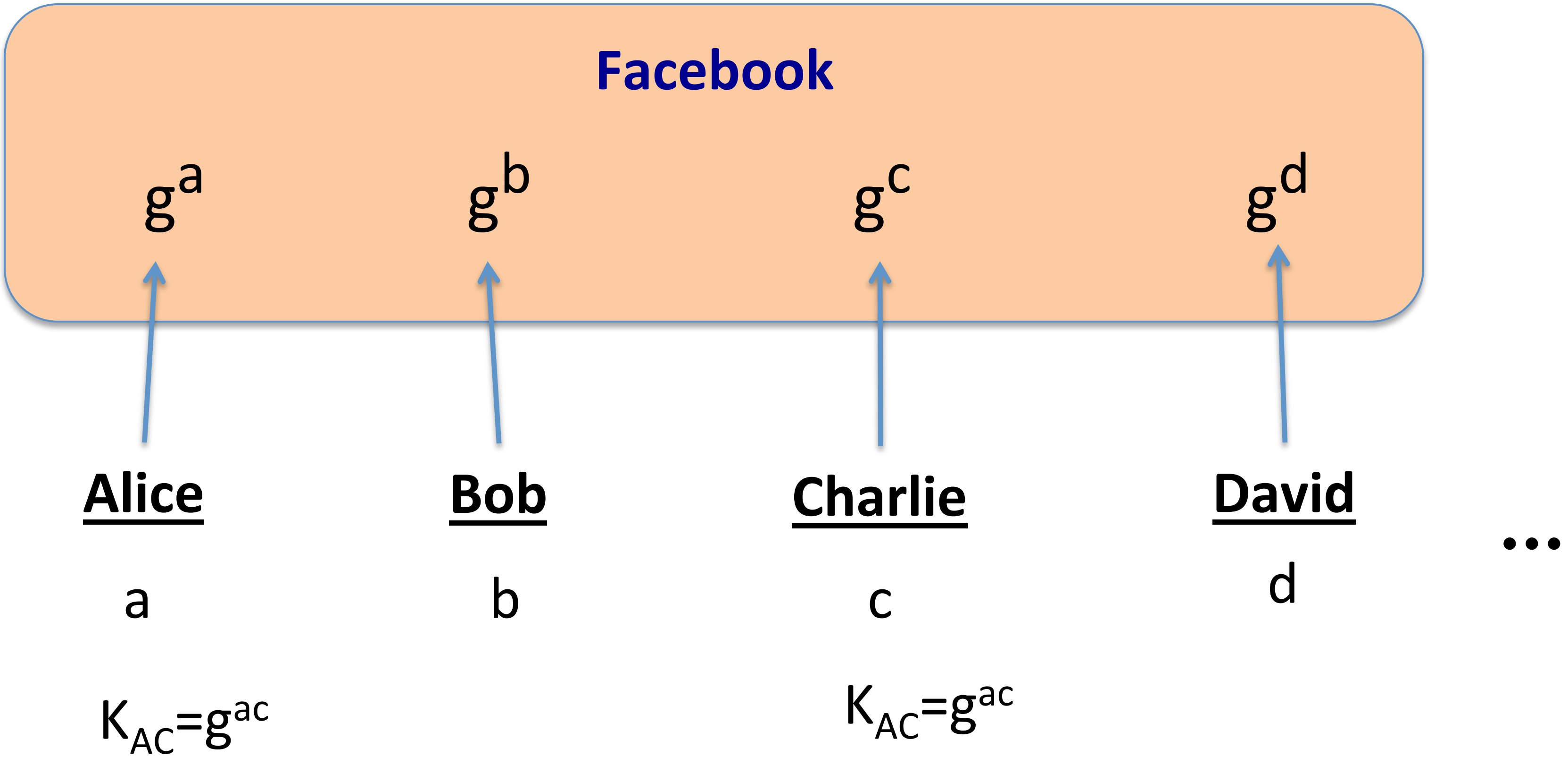
Insecure against man-in-the-middle

As described, the protocol is insecure against **active** attacks



attacker relays traffic from Alice to Bob and reads it in the clear

Another look at DH



Facebook

g^a g^b g^c g^d

Alice **Bob** **Charlie** **David** …

a b c d

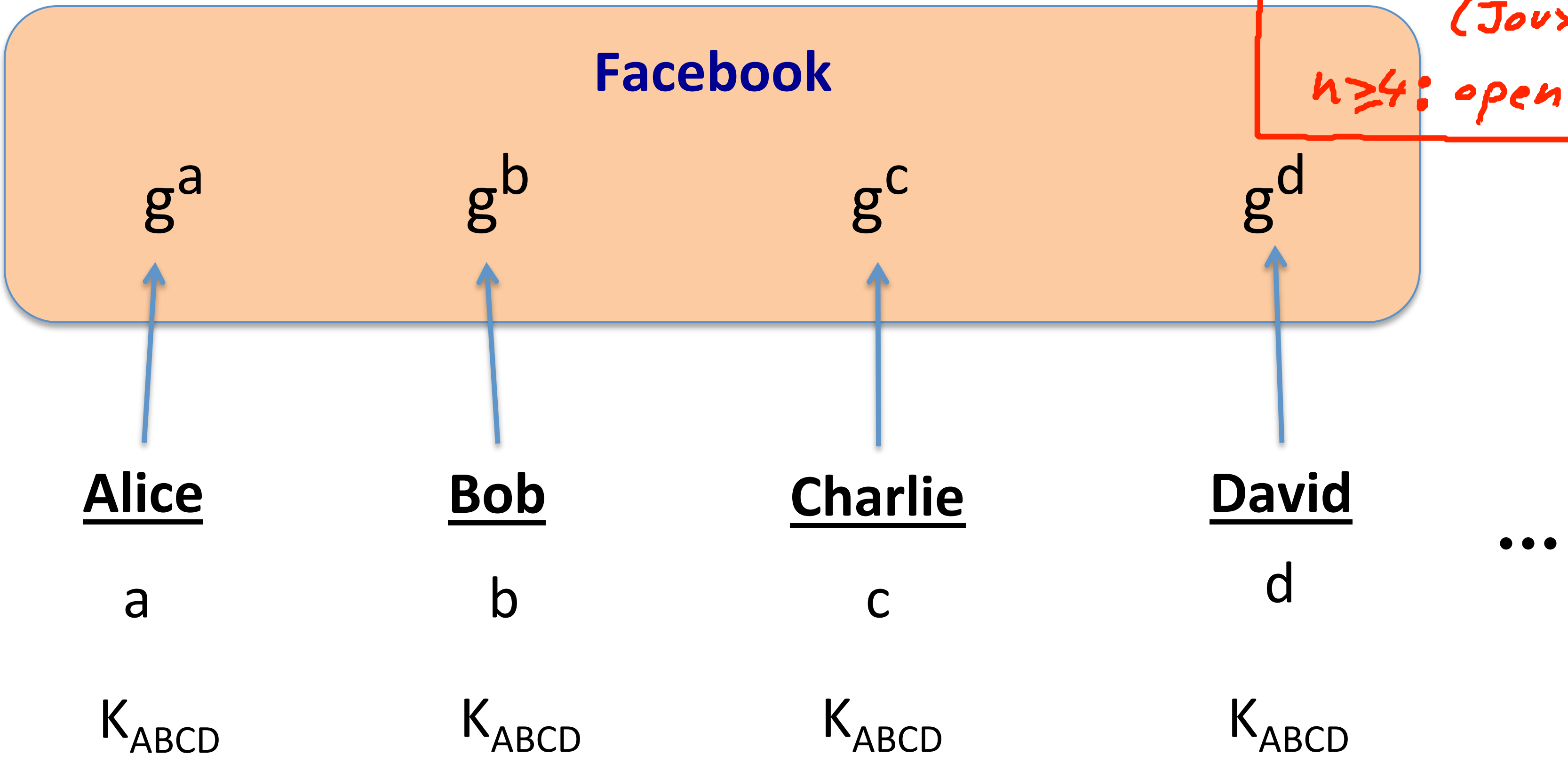
$K_{AC}=g^{ac}$ $K_{AC}=g^{ac}$

An open problem

n=2 : DH

n=3 : known (Joux)

n≥4: open



Facebook

g^a g^b g^c g^d

Alice **Bob** **Charlie** **David** …

a b c d

K_{ABCD} K_{ABCD} K_{ABCD} K_{ABCD}

End of Segment