

Key agreement with Diffie-Hellman: Advantages, Disadvantages, Vulnerabilities

Dr. Franziska Boenisch
January 22nd, 2026

Outline for Today



1. Intuition into necessity of key exchange protocols



2. Diffie-Hellman protocol

$$g^x \bmod p$$

3. Computational & Decisional Diffie-Hellman

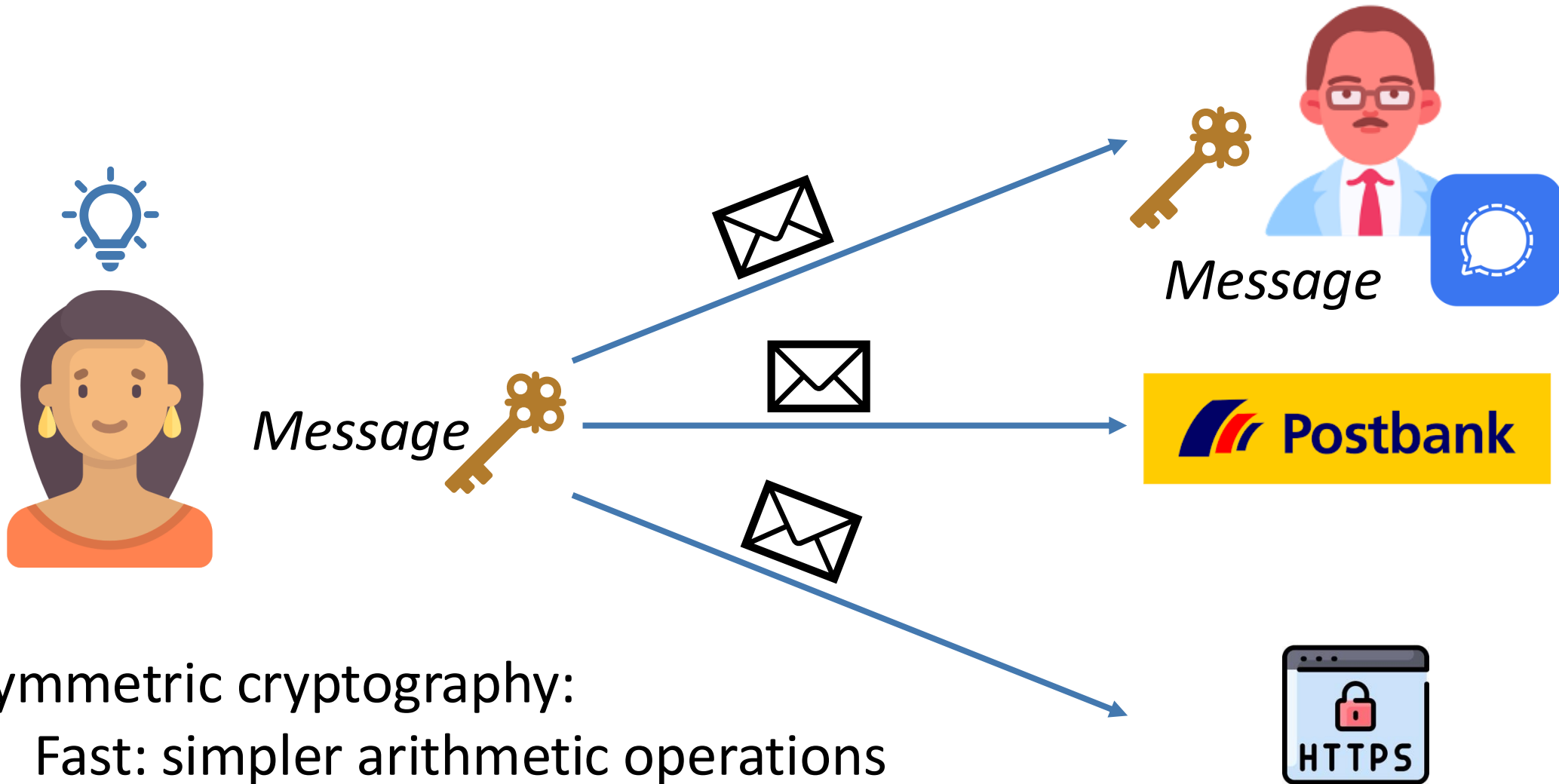


4. Vulnerabilities



5. Mitigations and application

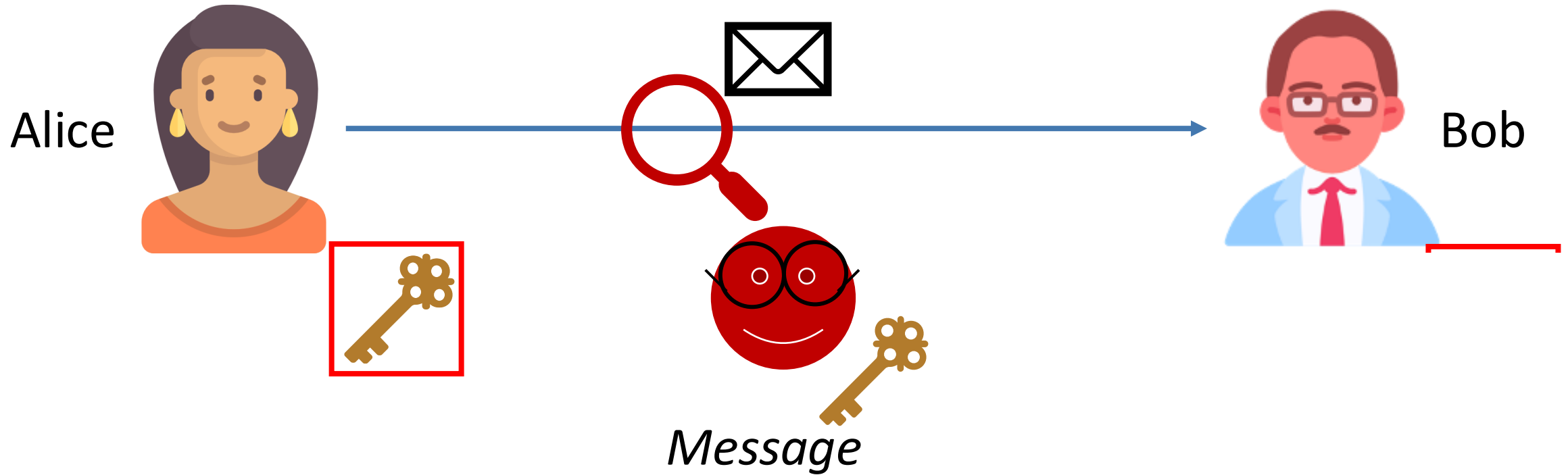
We all exchange encrypted messages



Symmetric cryptography:

- Fast: simpler arithmetic operations
- Efficient: lower (computational) costs

But how do we get the key?



We need a method to establish shared secret keys
over insecure communication channels!

→ **Diffie-Hellman**

Background: cyclic groups and generators


Group $\langle G, \cdot \rangle$: group of prime order p

Group has p elements;
 p is prime



Cyclic group: There is a **primitive element/ generator** g , such that
 $\forall m \in G \ \exists i \in \{0, \dots, p-1\}$, such that, $m = g^i$.

Every group element can be obtained by
repeatedly applying the group operation to g !



In Galois fields: non-zero elements form multiplicative group $GF(p)^*$:
e.g., $GF(11)^* = \{1, 2, \dots, 10\}$

→ Modular exponentiation!

Diffie-Hellman (DH) protocol for key exchange



$$p = 11, g = 2$$



$$2^1 \equiv 2 \pmod{11}$$

$$2^2 \equiv 4 \pmod{11}$$

$$2^3 \equiv 8 \pmod{11}$$

$$2^4 \equiv 16 \equiv 5 \pmod{11}$$

$$2^5 \equiv 32 \equiv 10 \pmod{11}$$

$$2^6 \equiv 64 \equiv 9 \pmod{11}$$

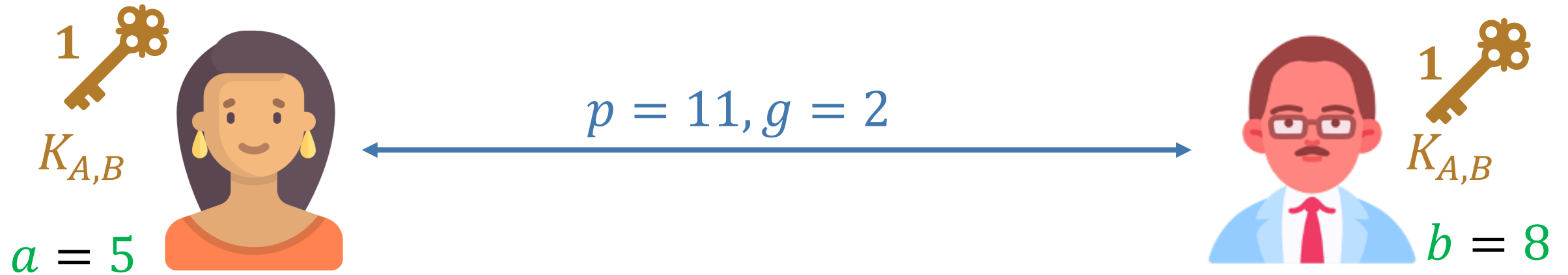
$$2^7 \equiv 128 \equiv 7 \pmod{11}$$

$$2^8 \equiv 256 \equiv 3 \pmod{11}$$

$$2^9 \equiv 512 \equiv 6 \pmod{11}$$

$$2^{10} \equiv 1024 \equiv 1 \pmod{11}$$

Diffie-Hellman (DH) protocol for key exchange



$$A = g^a \bmod p$$
$$2^5 = 32 \equiv 10 \bmod 11$$

A 10

$$K_{A,B} = A^b \bmod p$$
$$10^8 = \boxed{1} \bmod 11$$

$$K_{A,B} = B^a \bmod p$$
$$3^5 = 243 \equiv \boxed{1} \bmod 11$$

B 3

$$B = g^b \bmod p$$
$$2^8 = 256 \equiv 3 \bmod 11$$

$$B^a \bmod p = (g^b)^a \bmod p$$

Security requirements



Requirement 1: Attacker cannot compute the key

→ **Computational Diffie-Hellman Problem**

Given g, g^a, g^b , find g^{ab}

One obvious solution: Recover one of the secret exponents

→ **Discrete Logarithm Problem**

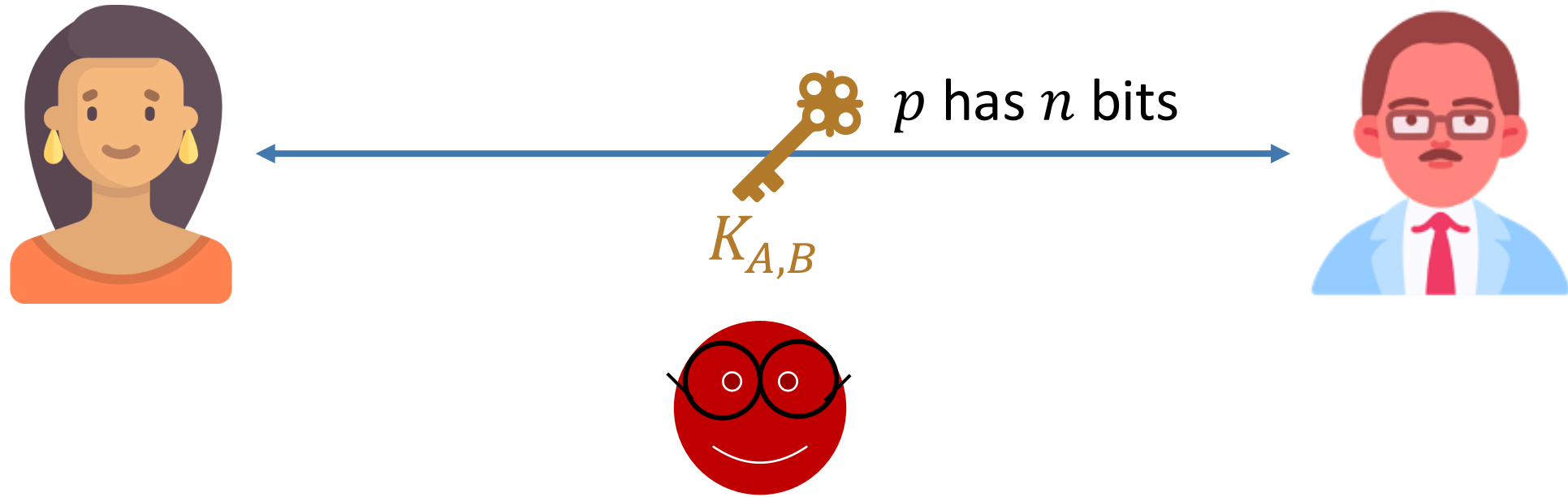
Given $g^x \bmod p$, find x

Requirement 2: Key looks random to the attacker

→ **Decisional Diffie-Hellman Problem**

Given g, g^a, g^b, g^c , decide if $c = ab$

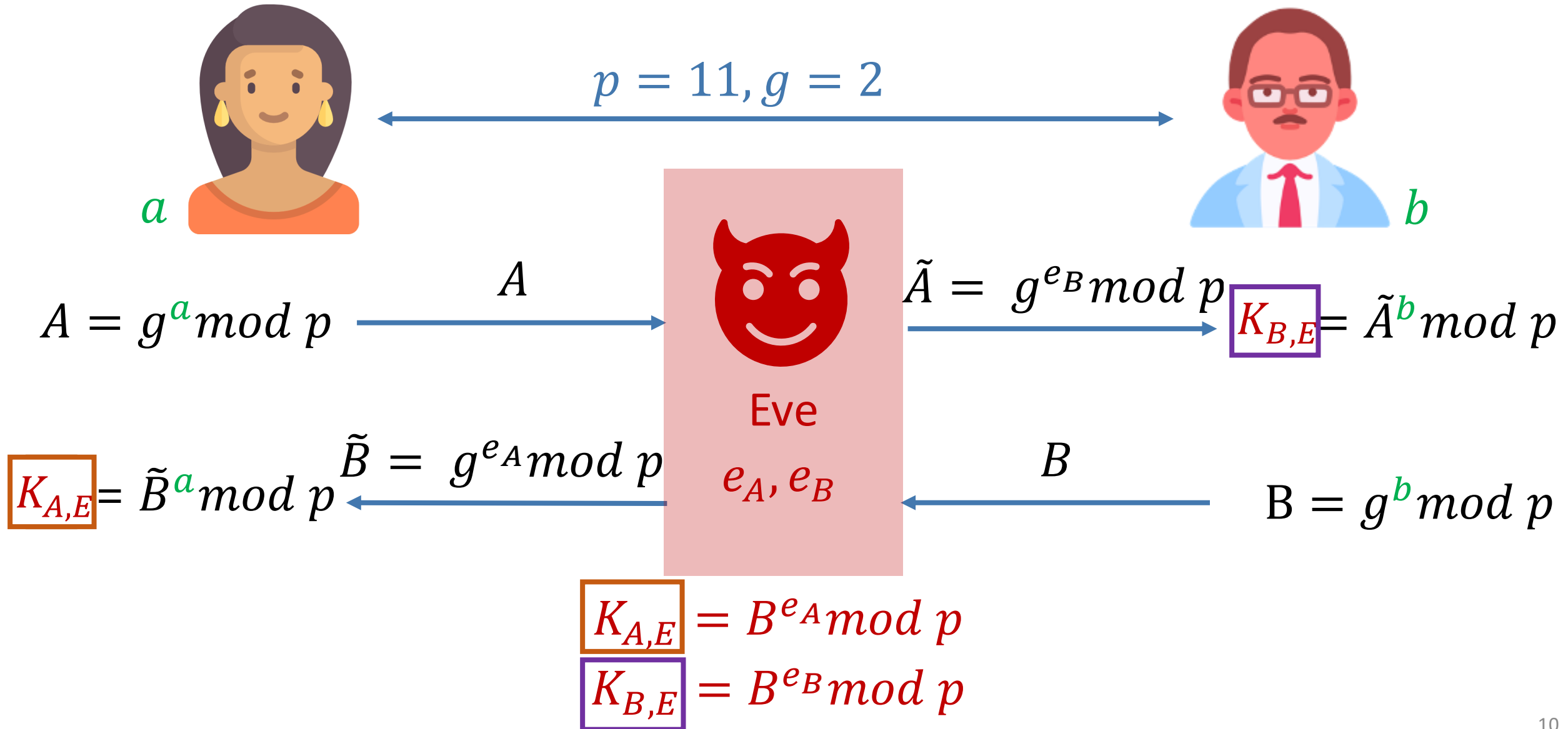
DH vulnerability: passive attacker



- 1) Brute force: $O(p) \approx O(2^n)$
- 2) Square root attacks: $O(\sqrt{p}) \approx O(2^{n/2})$
- 3) For some groups, we can have even more effective attacks

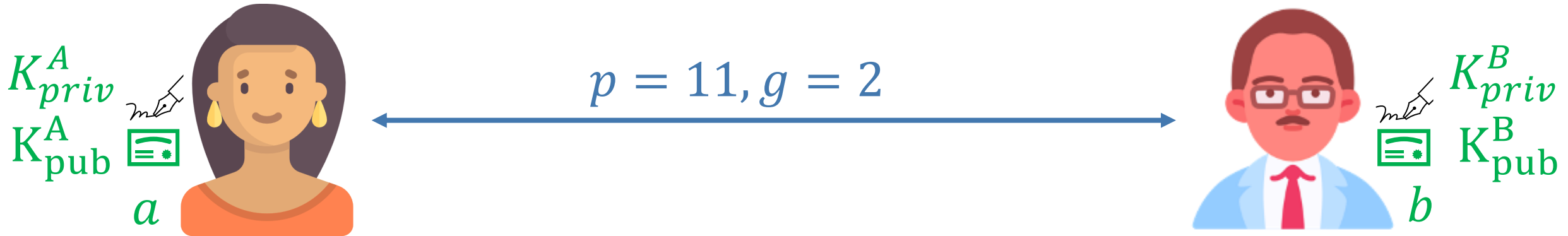
Today: 2048 bits, preferably larger!

Active attacker: man-in-the-middle (MITM)



Solution: station-to-station protocol (STS)

Problem: Standard Diffie-Hellman does not authenticate the participants!



$$A = g^a \bmod p$$

$$Sig_A = Sign(A, K_{priv}^A)$$

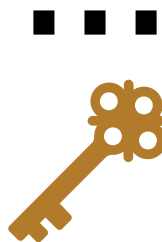
$$(A, Sig_A)$$

$$Verify(Sig_A, K_{pub}^A)$$

If successful: $K_{A,B} = A^b \bmod p$



Transport Layer Security



Diffie-Hellman: Advantages and Disadvantages

Advantages



Secure key

agreement over
insecure channel

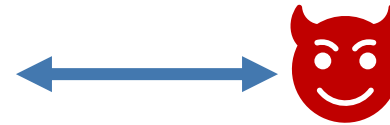
DLP

Based on well-studied
mathematical hardness
assumptions



Fast, scales well

Disadvantages



No authentication

p, g

Careful parameter
selection



Large key sizes
required over $GF(p)^*$

→ Elliptic curves

Lecture Materials

