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

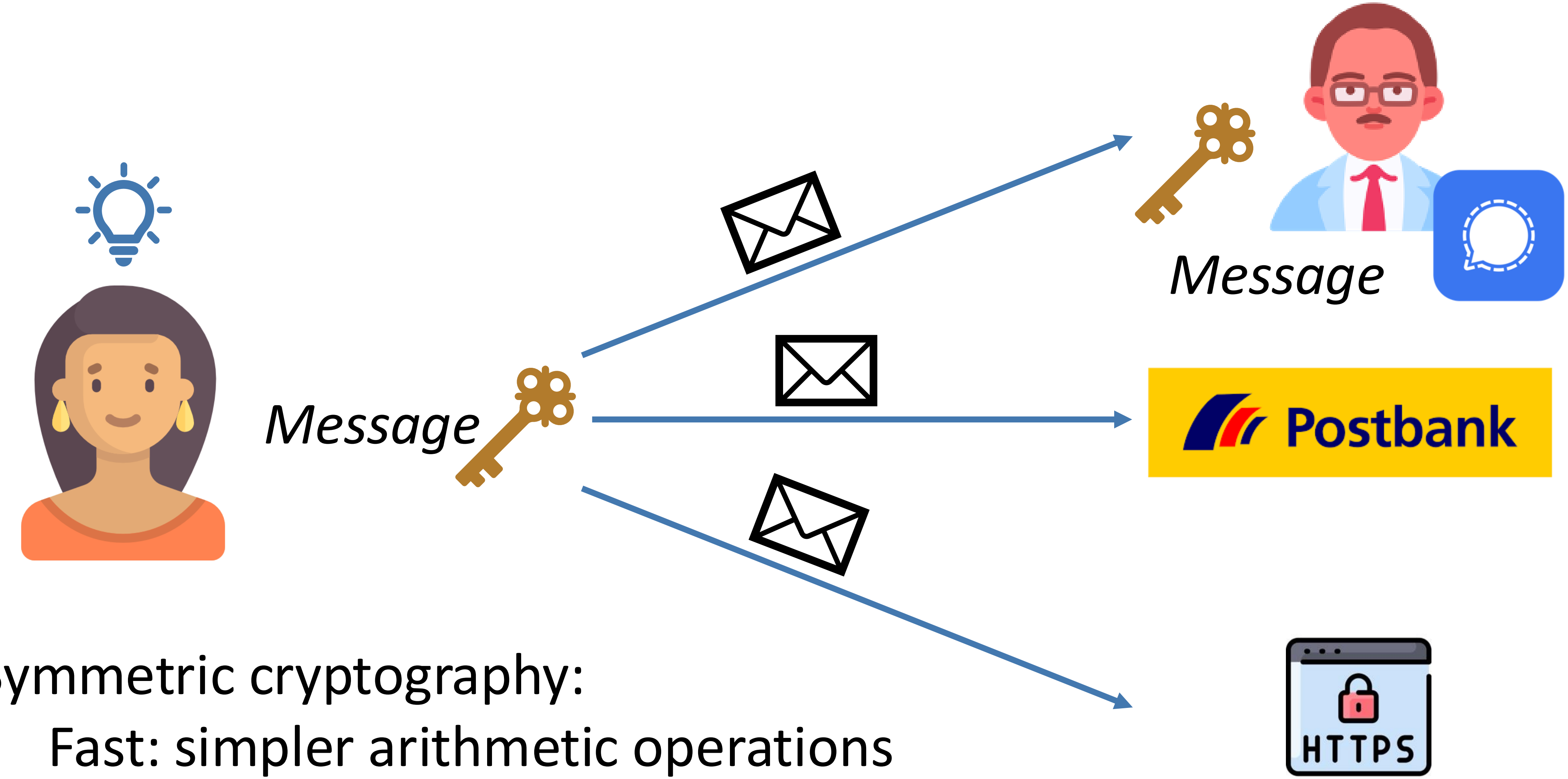
g^x **mod p**

3. Computational & Decisional Diffie-Hellman

4. Vulnerabilities

5. Mitigations and application

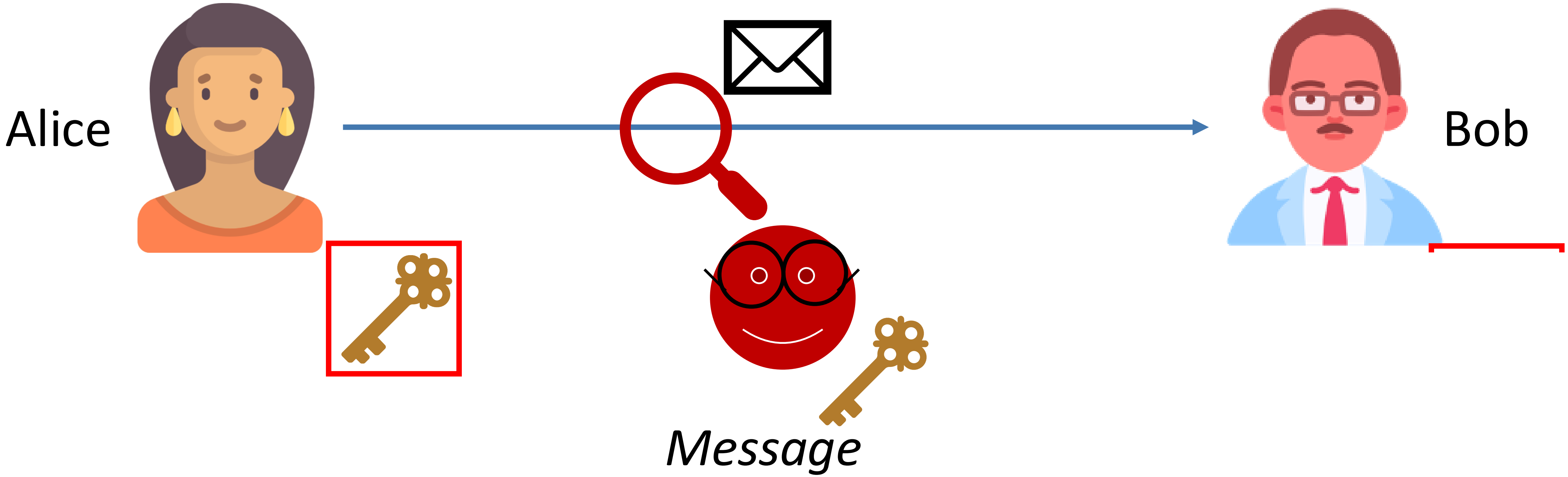
We all exchange encrypted messages



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 $\boldsymbol{p}$

Group has p elements;
p is prime

Cyclic group: There is a **primitive element/ generator** $\boldsymbol{g}$, such that

$$\forall m \in G \ \ \exists i \in \{0, \ldots p-1\}, \text{ such that, } m = \boldsymbol{g}^i.$$

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

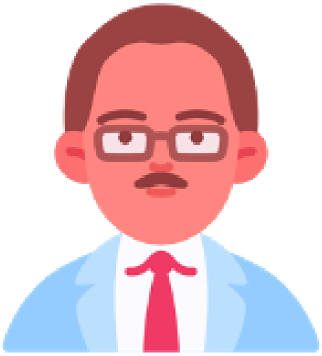
In Galois fields: non-zero elements form multiplicative group $GF(\boldsymbol{p})^*$:

e.g., $GF(11)^* = \{1,2, \ldots, 10\}$

→ Modular exponentiation!

Diffie-Hellman (DH) protocol for key exchange

$$p = 11, g = 2$$



$2^1 \equiv 2 \bmod 11$

$2^2 \equiv 4 \bmod 11$

$2^3 \equiv 8 \bmod 11$

$2^4 \equiv 16 \equiv 5 \bmod 11$

$2^5 \equiv 32 \equiv 10 \bmod 11$

$2^6 \equiv 64 \equiv 9 \bmod 11$

$2^7 \equiv 128 \equiv 7 \bmod 11$

$2^8 \equiv 256 \equiv 3 \bmod 11$

$2^9 \equiv 512 \equiv 6 \bmod 11$

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

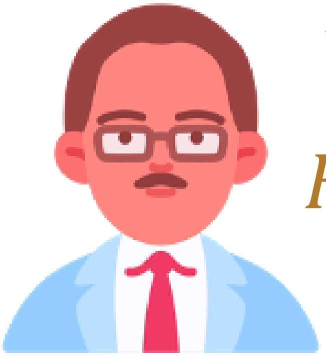
Diffie-Hellman (DH) protocol for key exchange

1

$K_{A,B}$

$a = 5$

$p = 11, g = 2$



1

$K_{A,B}$

$b = 8$

$A = g^a mod\ p$

$2^5 = 32 \equiv \mathbf{10}\ mod\ 11$

A **10**

$K_{A,B} = A^b mod\ p$

$10^8 \equiv \boxed{\mathbf{1}}\ mod\ 11$

$K_{A,B} = B^a mod\ p$

$3^5 = 243 \equiv \boxed{\mathbf{1}}\ mod\ 11$

B **3**

$\mathrm{B} = g^b mod\ p$

$2^8 = 256 \equiv \mathbf{3}\ mod\ 11$

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

Security requirements

1

$K_{A,B}$

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**

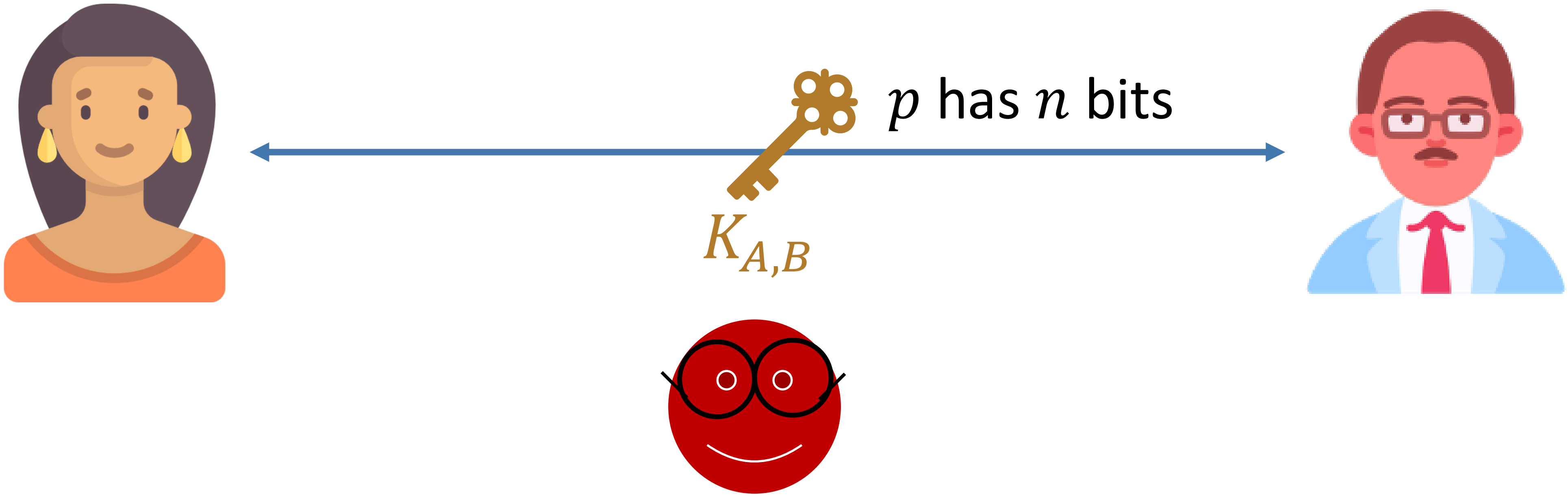
Given $g^x \bmod \mathrm{p}$, find x

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: $O\left(\sqrt{p}\right) \approx O\left(2^{n/2}\right)$
3) For some groups, we can have even more effective attacks

Today: 2048 bits, preferably larger!

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

$p = 11, g = 2$

a 

 b

$A = g^{a} \bmod p$ $\xrightarrow{A}$

Eve

e_A, e_B

$\tilde{A} = g^{e_B} \bmod p$ $\longrightarrow$ $\boxed{K_{B,E}} = \tilde{A}^{b} \bmod p$

$\boxed{K_{A,E}} = \tilde{B}^{a} \bmod p$ $\longleftarrow$ $\tilde{B} = g^{e_A} \bmod p$

$\xleftarrow{B}$ $B = g^{b} \bmod p$

$\boxed{K_{A,E}} = A^{e_A} \bmod p$

$\boxed{K_{B,E}} = B^{e_B} \bmod p$

Solution: station-to-station protocol (STS)

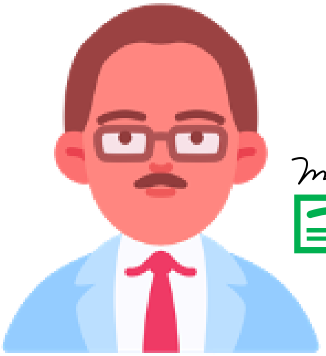
Problem: Standard Diffie-Hellman does not authenticate the participants!

K_{priv}^{A}

$\mathrm{K}_{\mathrm{pub}}^{\mathrm{A}}$

a

$p = 11, g = 2$



K_{priv}^{B}

$\mathrm{K}_{\mathrm{pub}}^{\mathrm{B}}$

b

$A = g^{a} mod\, p$

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

(A, Sig_A)

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

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

Transport Layer Security

...

Diffie-Hellman: Advantages and Disadvantages

Advantages

Secure key agreement over insecure channel

DLP

Based on well-studied mathematical hardness assumptions

TLS

Fast, scales well

Disadvantages

No authentication

p, g

Careful parameter selection

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

→ Elliptic curves

Lecture Materials