

Selected Areas in Cryptology

Monika Trimoska

Selected Areas in Cryptology - Part 1
Spring, 2024

TU/e

General info

▶ Lecturers:

- Bart Mennink, Radboud University <b.mennink@cs.ru.nl>
- Monika Trimoska, Eindhoven University of Technology <m.trimoska@tue.nl>

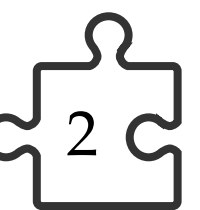
▶ Every **Thursday, 10:00 - 12:45** (Week 6-21)

▶ Location: Utrecht, room **BBG 005**

▶ Evaluation

- Exam (written or oral): **June 13, 2024**.
- Retake: **July 4, 2024**.
- The assignments are **not** included in the grade, but feedback will be given if submitted.

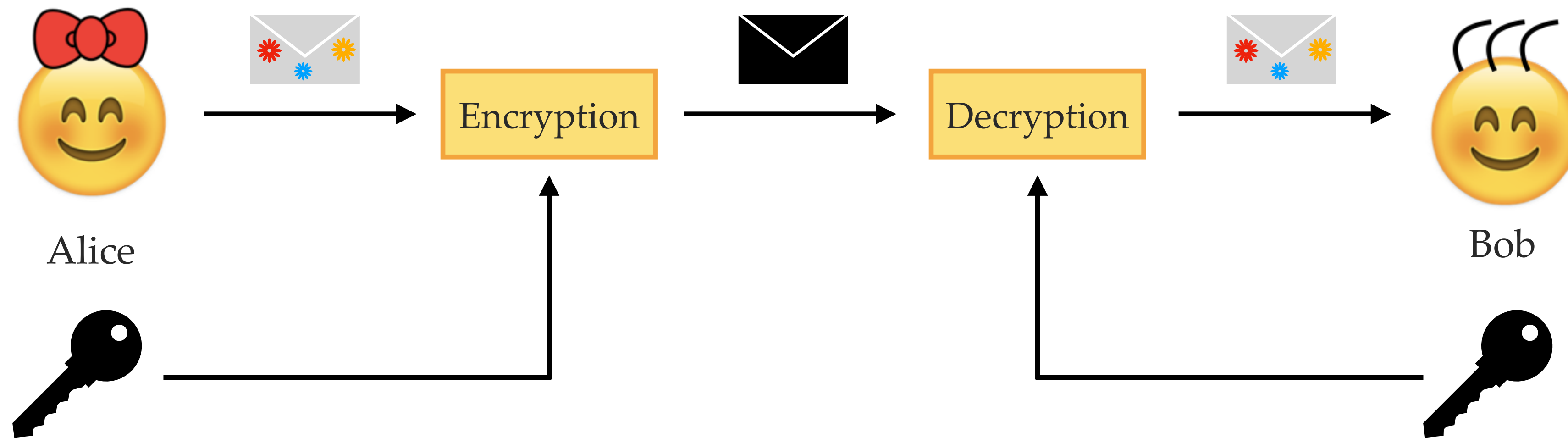
▶ Recordings: <https://vimeo.com/showcase/10950327> ; Password: t7i8



Cryptology 101



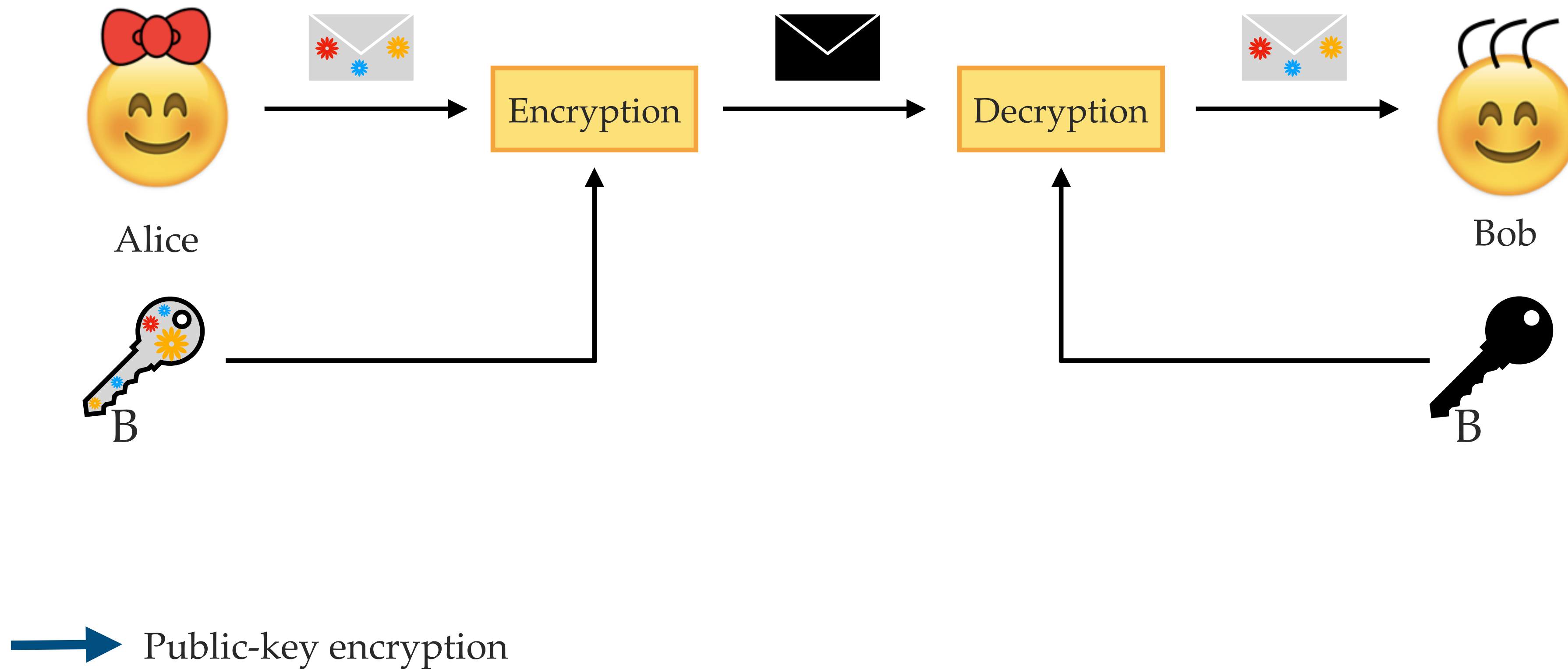
(Secret-key) Cryptography



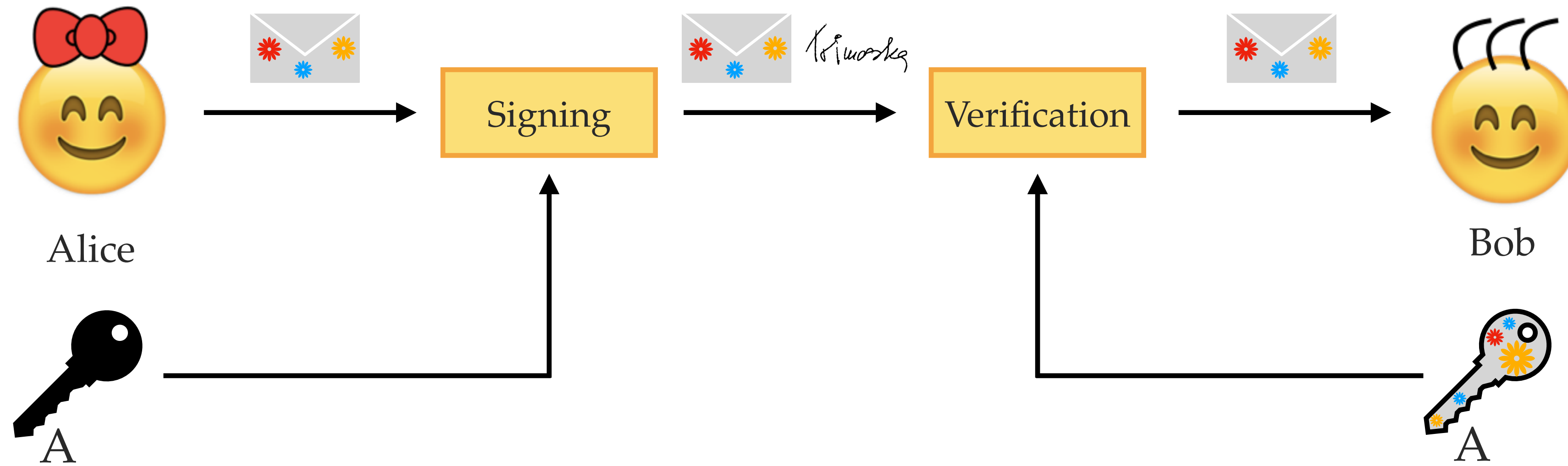
Example. (Caesar cipher) Shift all letters in the message by $s = 4$ positions down the alphabet.

Everything is public information, except for the secret key!

Public-key cryptography



Public-key cryptography

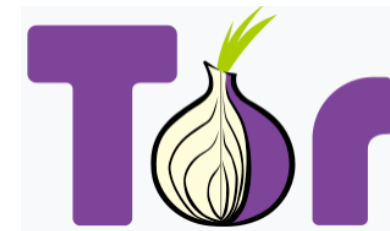


➡ Digital signature scheme

Security and privacy tools

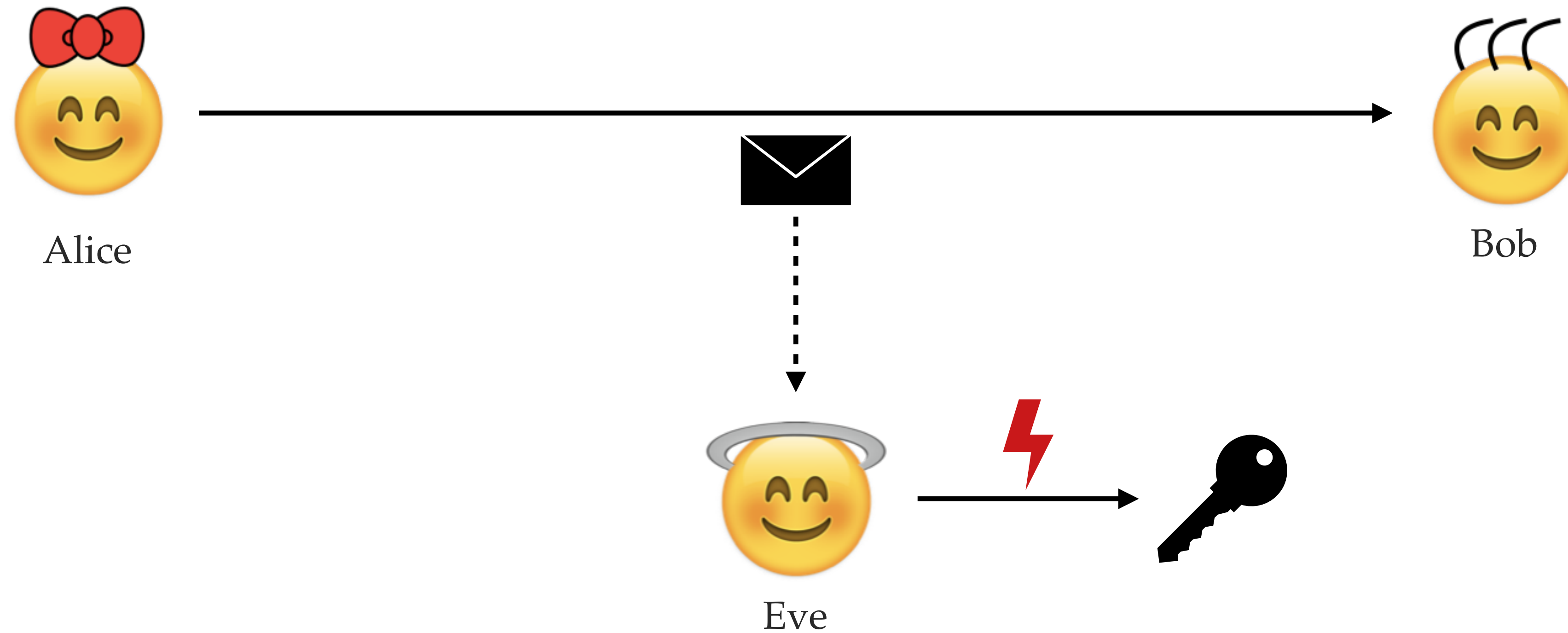
<https://prism-break.org/en/>

<https://www.privacytools.io/>



➔ Privacy as a right

Cryptanalysis



Goal of cryptanalysis in academia

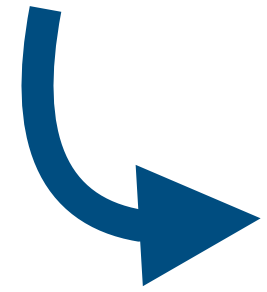
- Ensure that the cryptosystems are secure, before the deployment in real-world applications.
- Determine minimum key length requirements.

Example: NIST security levels	
I	2^{128}
III	2^{192}
V	2^{256}

Post-quantum cryptography



Post-quantum cryptography



Implemented on a classical, but resistant to attacks on a quantum computer.

- **Shor's** quantum algorithm: solves integer **factorisation** and **discrete logarithms** in abelian groups in **polynomial** time.
 - ▶ All* currently deployed public-key cryptosystems would be broken by an adversary in possession of a large **quantum** computer.
 - ▶ All public-key cryptosystems need to be **replaced**.
 - ▶ If the public-key cryptography component is broken, the entire infrastructure is broken because the **handshake** is compromised.
- **Grover's** quantum algorithm: quadratic speedup of exhaustive search.
 - ▶ Impact on symmetric cryptography (as a rule of thumb): double the key sizes.

Computationally hard problems

Travelling salesman
problem

Isomorphism of polynomials
problem

Boolean satisfiability
problem

Graph colouring
problem

Syndrome decoding
problem

MQ (multivariate quadratic)
problem

Integer factorisation
problem

Code equivalence
problem

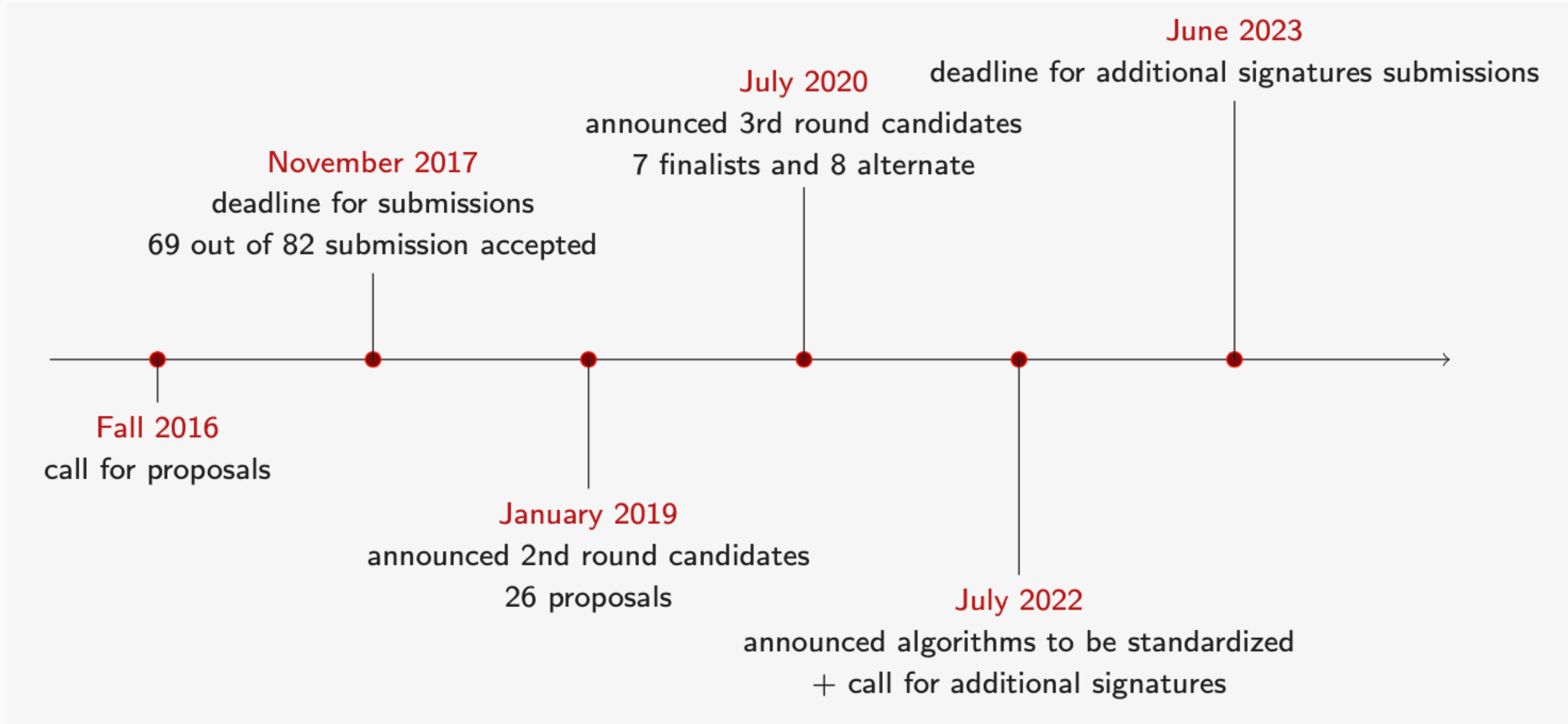
Isogeny path
problem

Discrete log
problem

Standardisation efforts

- National Institute of Standards and Technology (NIST), United States
- Information security, cybersecurity and privacy protection: ISO/IEC WD
- Internet Research Task Force (IRTF): RFC 8391
- Chinese Association for Cryptologic Research (CACR), China
- Korean Post-Quantum Cryptography Competition (KpqC), South Korea
- ...

NIST standardisation timeline



More signatures

Standardization of Additional Digital Signature Schemes

Post-Quantum Cryptography: Digital Signature Schemes



Standardization of Additional Digital Signature Schemes

[Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process](#) (PDF)

Closed June 1, 2023

NIST announced that the PQC standardization process is continuing with a fourth round, with the following KEMs still under consideration: BIKE, Classic McEliece, HQC, and SIKE. However, there are no remaining digital signature candidates under consideration. As such, NIST is calling for additional digital signature proposals to be considered in the PQC standardization process.

NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices. For certain applications, such as certificate transparency, NIST may also be interested in signature schemes that have short signatures and fast verification. NIST is open to receiving additional submissions based on structured lattices, but is intent on diversifying the post-quantum signature standards. As such, any structured lattice-based signature proposal would need to significantly outperform CRYSTALS-Dilithium and FALCON in relevant applications and/or ensure substantial additional security properties to be considered for standardization.

PROJECT LINKS

[Overview](#)

[News & Updates](#)

ADDITIONAL PAGES

[Standardization of Additional Digital Signature Schemes](#)

[Call for Proposals](#)

[Example Files](#)

[Workshops and Timeline](#)

[Round 1 Additional Signatures](#)

[Email List \(PQC Forum\)](#)

[PQC Standardization: Main Project](#)

CONTACTS

NIST announced 40 valid submissions divided in 7 categories:

- Code-based
- Isogeny-based
- Lattice-based
- MPC-in-the-Head
- Multivariate
- Symmetric-based
- Other

Course plan : part 1

- ▶ Algebraic cryptanalysis: MQ solving
- ▶ Multivariate cryptography: trapdoor constructions; UOV
- ▶ Code-based cryptography I: equivalence problems; the Fiat-Shamir construction
- ▶ Code-based cryptography II: information set decoding; the MPC-in-the-Head construction
- ▶ Lattice-based cryptography: Dilithium (subject to change)
- ▶ Isogeny-based cryptography: SQISign (subject to change)
- ▶ Hash-based cryptography: stateless signatures; SPHINCS+

Tutorials

- ▶ The tutorial session in week i is dedicated to answering your questions from assignment $(i - 1)$.
- ▶ Some of the exercises are about experimenting with the mathematical objects that are studied via a computer algebra system. You can submit those for feedback in either [SageMath](#) or [Magma](#), according to your preference.