Lecture 15 – Course recap

TEK4500

26.11.2025

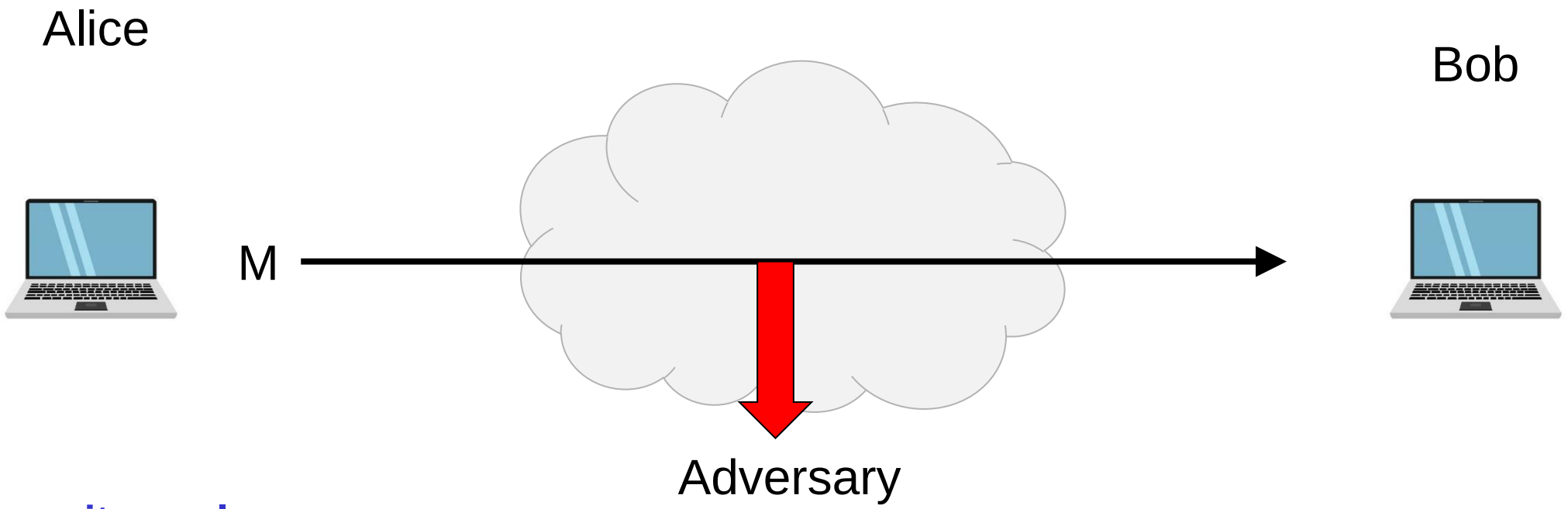
Håkon Jacobsen

hakon.jacobsen@its.uio.no

Agenda

- Recap of course
- Q&A
- Go through old exams

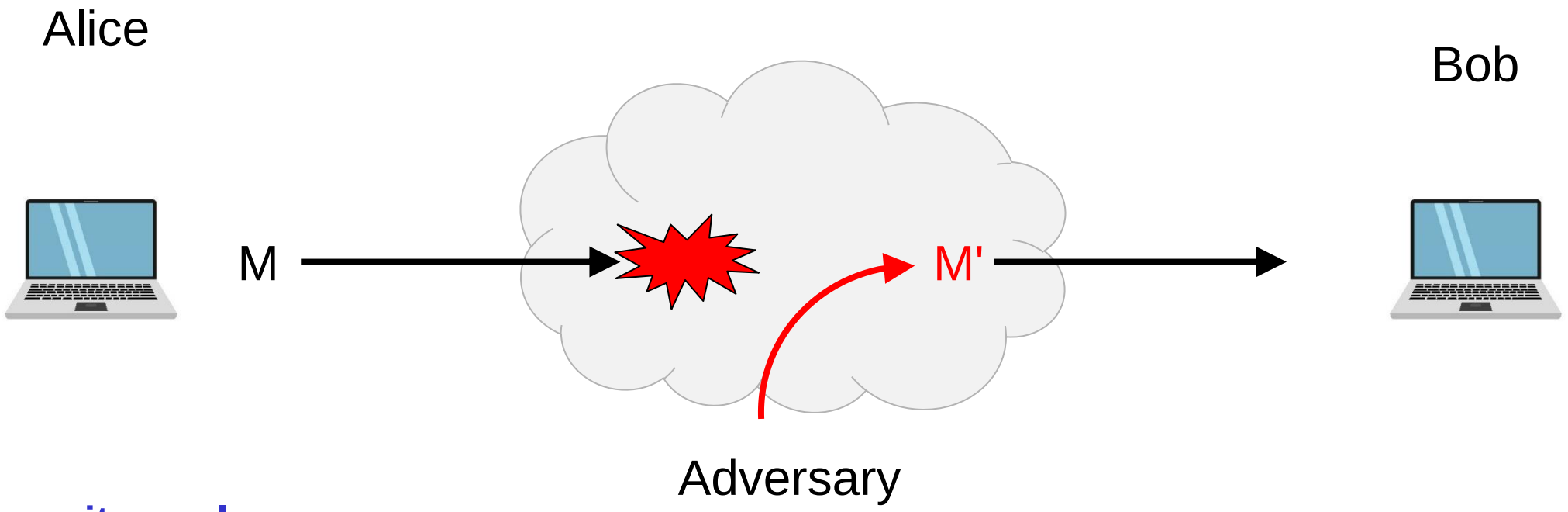
What is cryptography?



Security goals:

- **Data privacy:** adversary should not be able to *read* message M
- **Data integrity:** adversary should not be able to *modify* message M
- **Data authenticity:** message M really originated from Alice

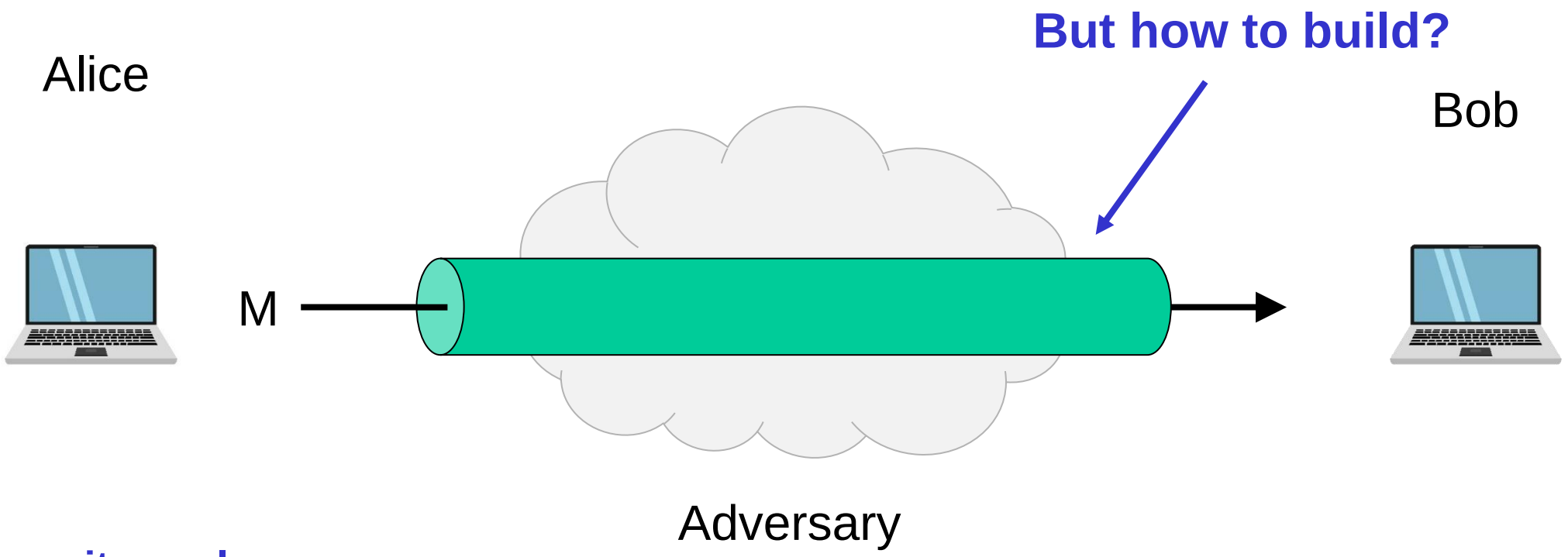
What is cryptography?



Security goals:

- **Data privacy:** adversary should not be able to *read* message M
- **Data integrity:** adversary should not be able to *modify* message M
- **Data authenticity:** message M really originated from Alice

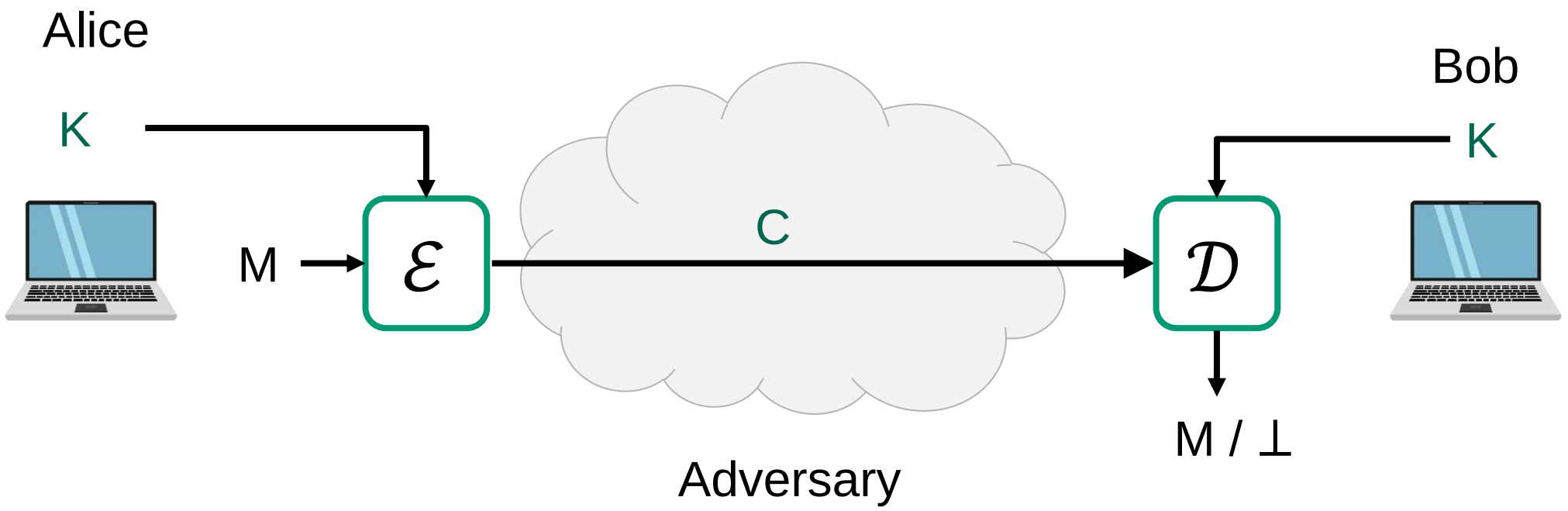
Ideal solution: secure channels



Security goals:

- **Data privacy:** adversary should not be able to *read* message M ✓
- **Data integrity:** adversary should not be able to *modify* message M ✓
- **Data authenticity:** message M really originated from Alice ✓

Creating secure channels: encryption schemes

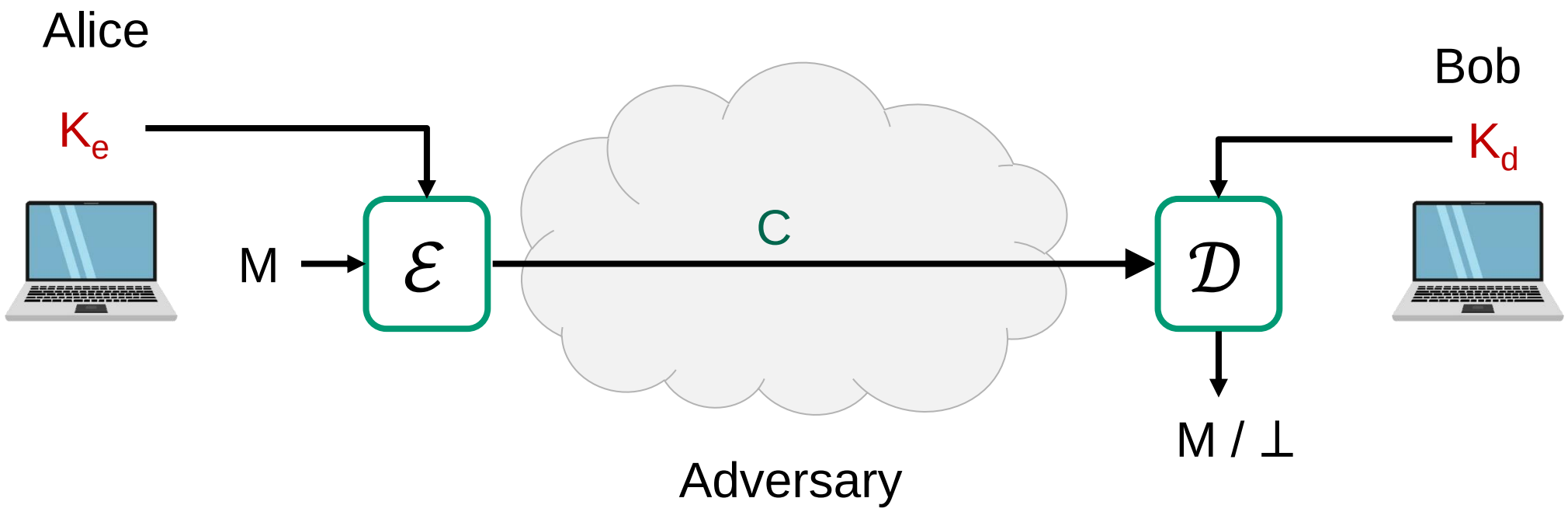


$\mathcal{E}$ **:** encryption algorithm (public)

K : encryption / decryption key (secret)

$\mathcal{D}$ **:** decryption algorithm (public)

Creating secure channels: encryption schemes



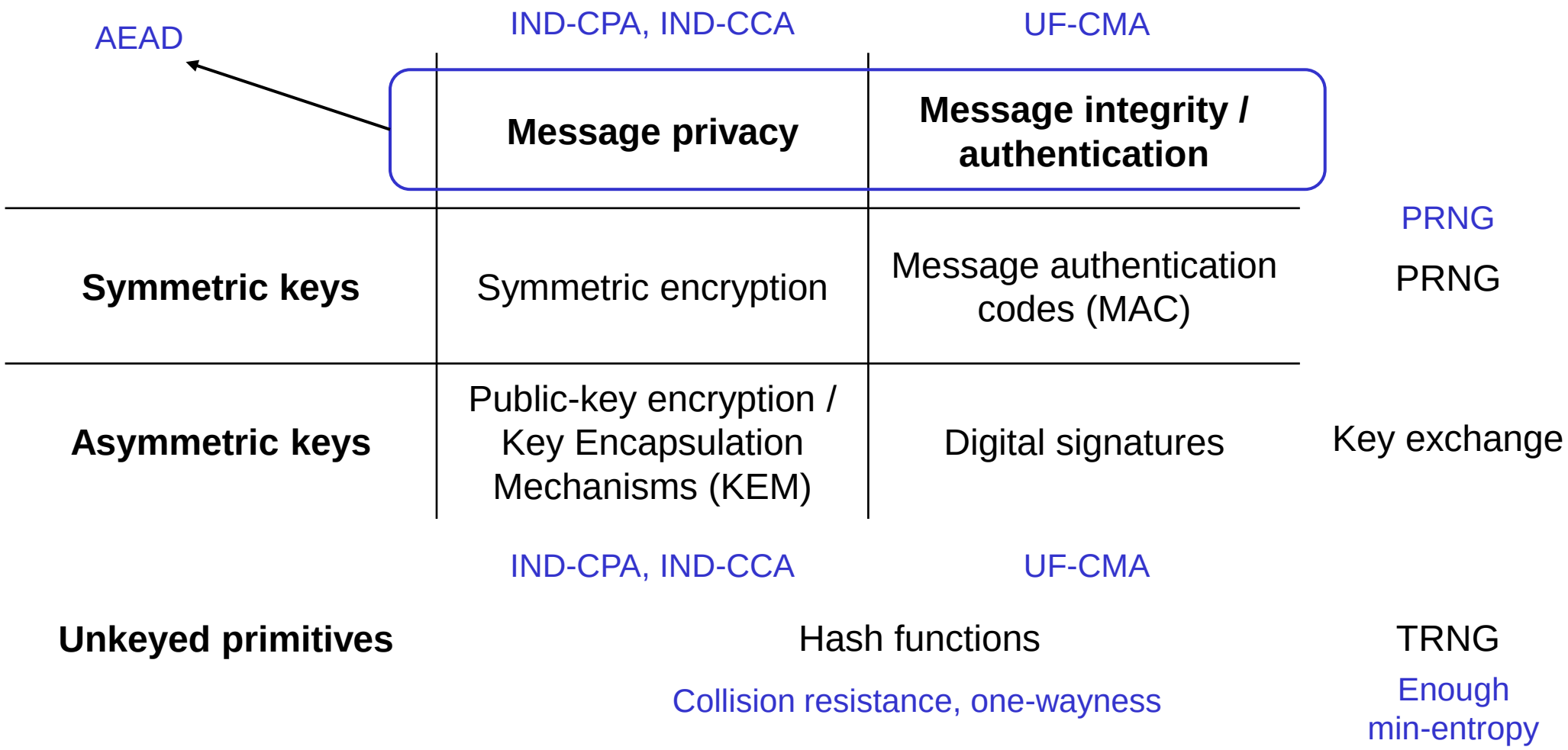
$\mathcal{E}$: encryption algorithm (public)

$\mathcal{D}$: decryption algorithm (public)

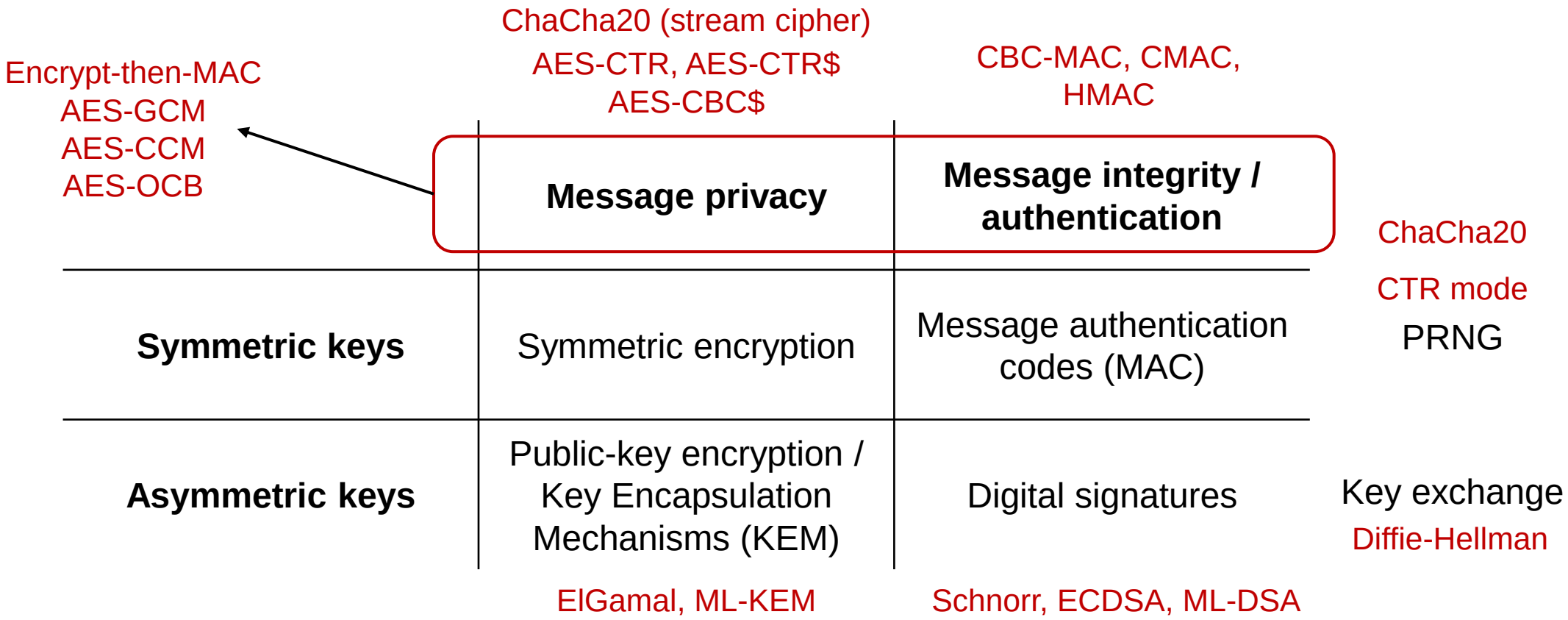
K_e : encryption key (public)

K_d : decryption key (secret)

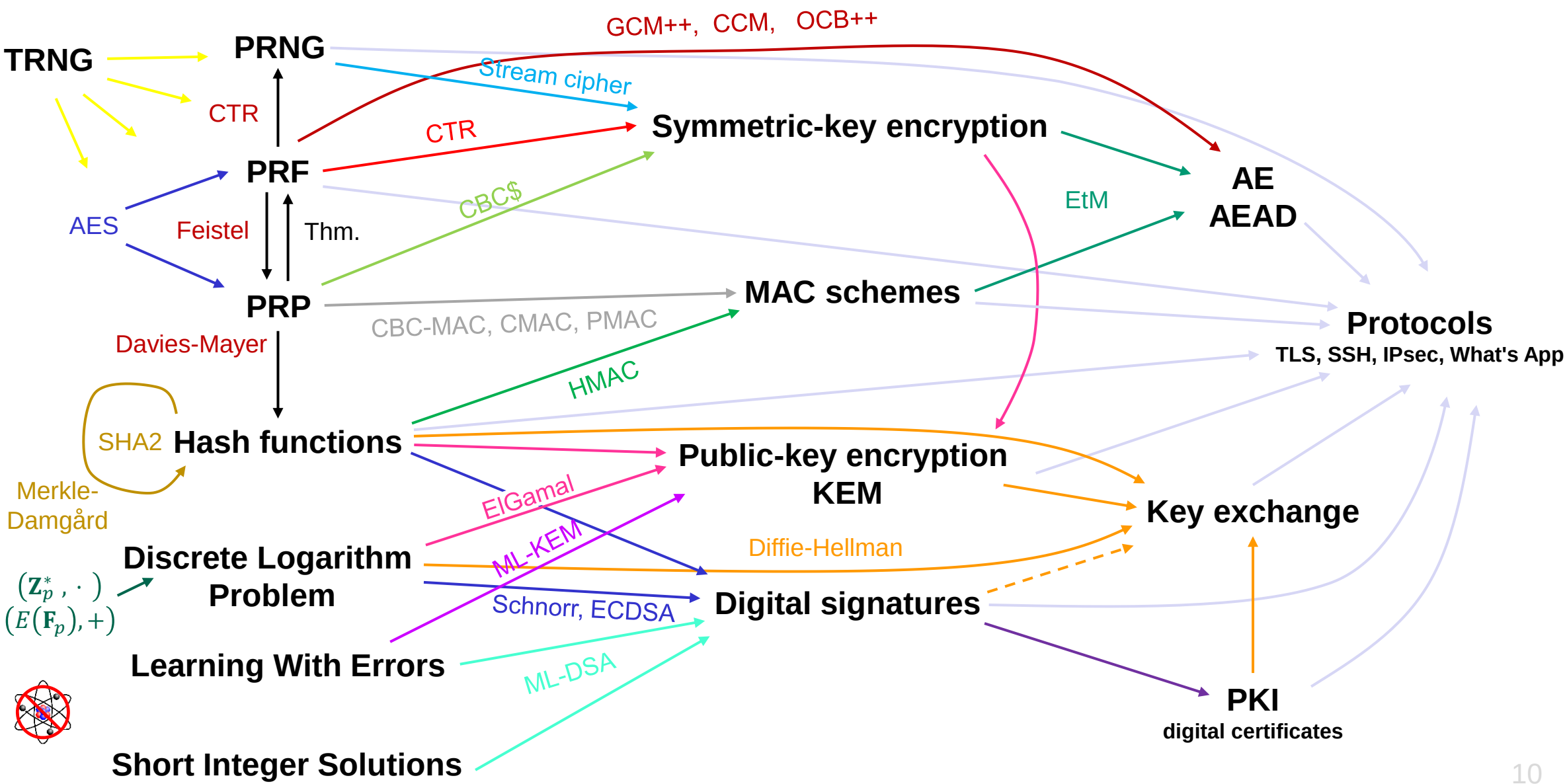
Basic goals of cryptography



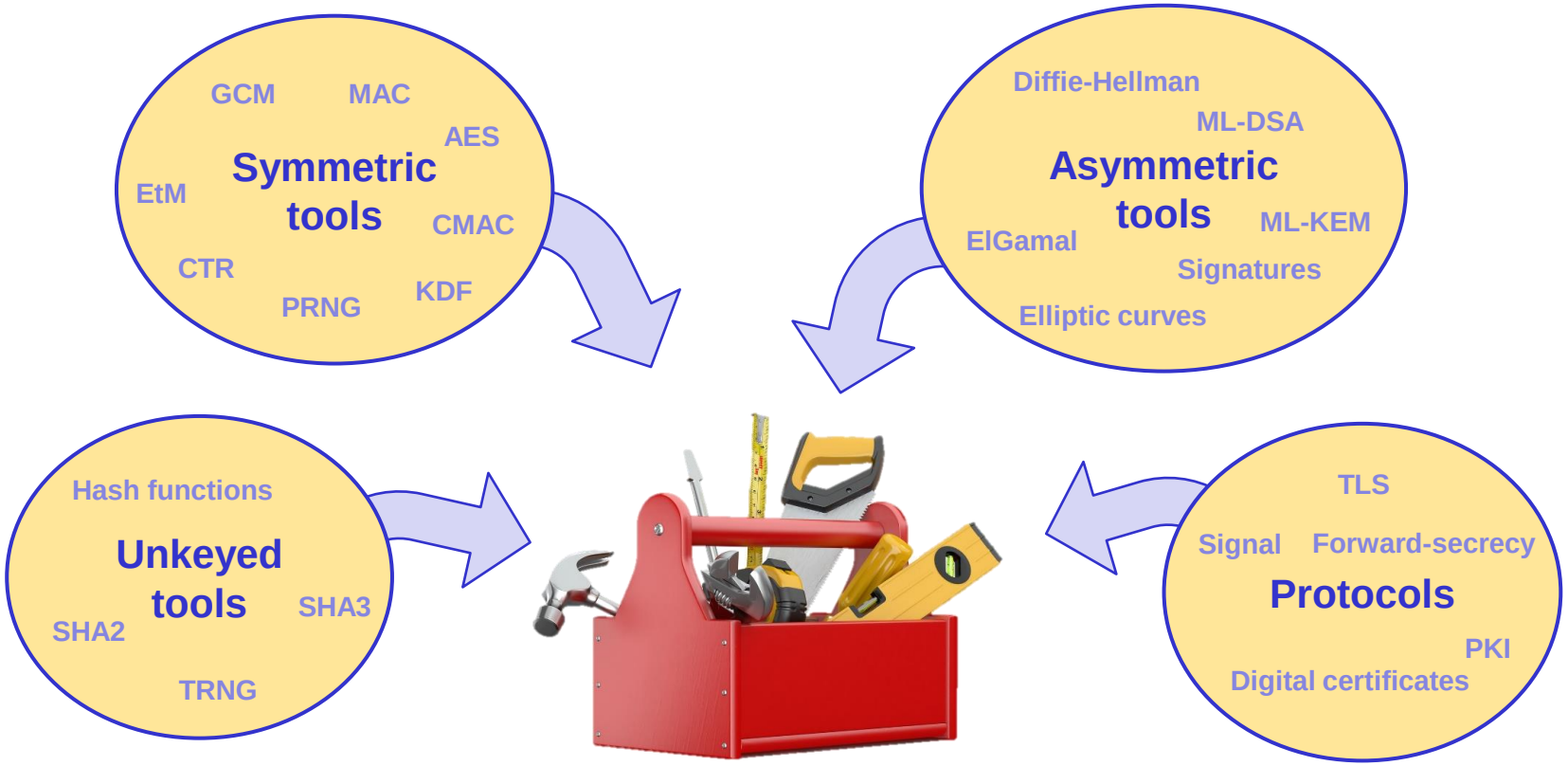
Basic goals of cryptography



Constructions and relations



The crypto toolbox



Mathematics | Electronics | Politics

Informatics | Philosophy | Physics

Exam

- Wednesday December 3, 09:00-13:00 (4 hours)
- Digital, on-campus (Silurveien 2, Sal 3C)
- Closed-book
- I will make a round approximately 2 hours into the exam for any possible questions
  - Make sure to look through all problems before you start answering in case you have questions for the some of the later problems
- https://www.uio.no/studier/emner/matnat/its/TEK4500/h25/eksamen/index.html