
Lecture 14 – Course recap

TEK4500

04.12.2023

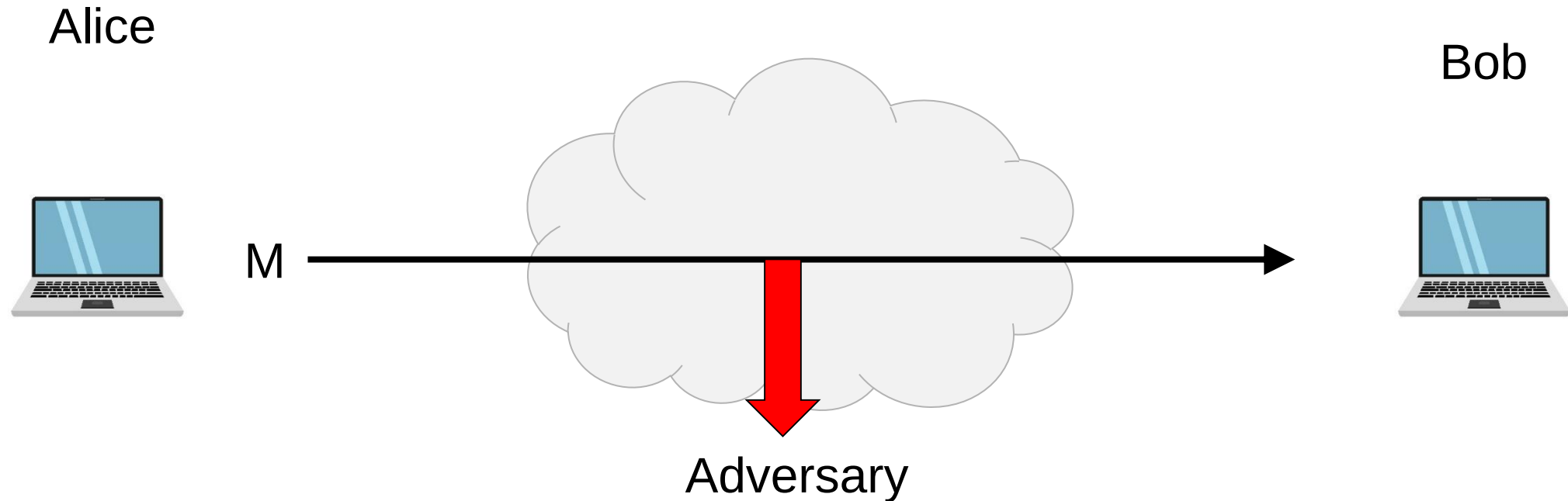
Håkon Jacobsen

hakon.jacobsen@its.uio.no

Agenda

- Recap of course
- Q&A
- Go through exam from 2023 and 2022 (offline)

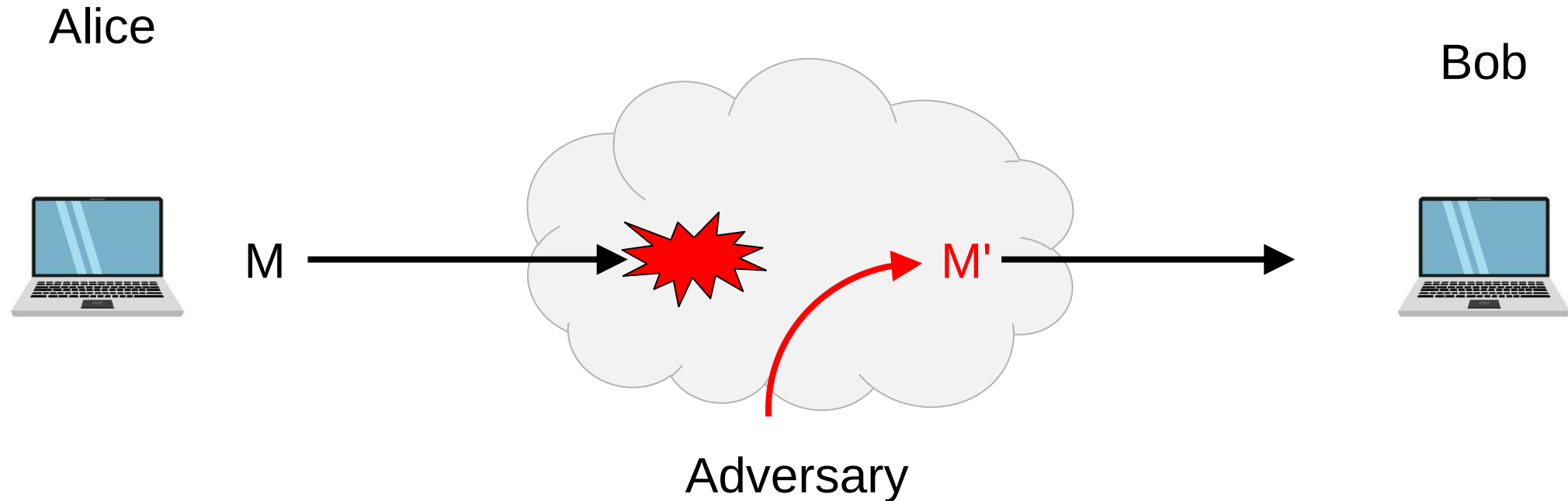
What is cryptography?



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

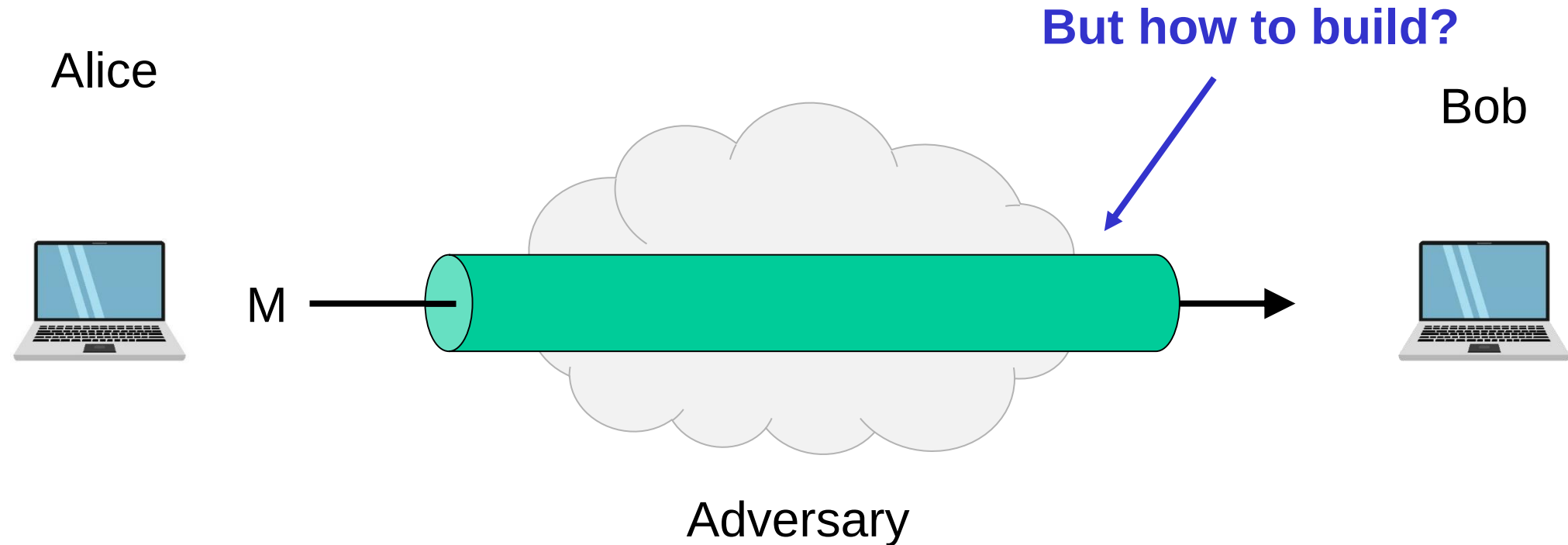
What is cryptography?



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

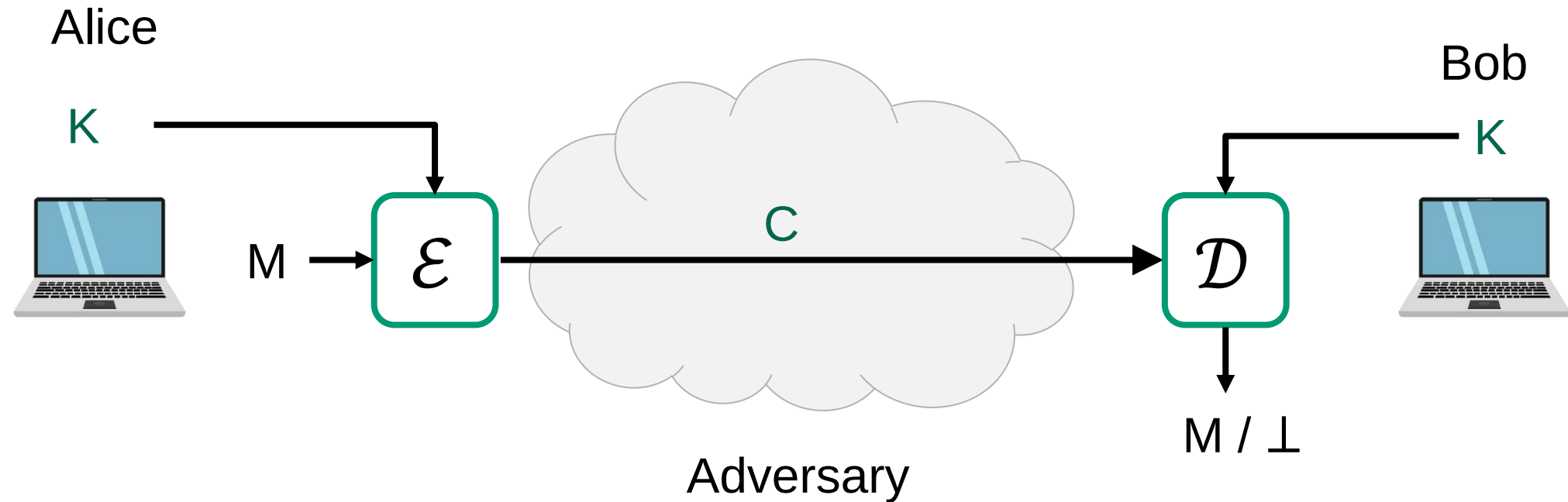
Ideal solution: secure channels



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

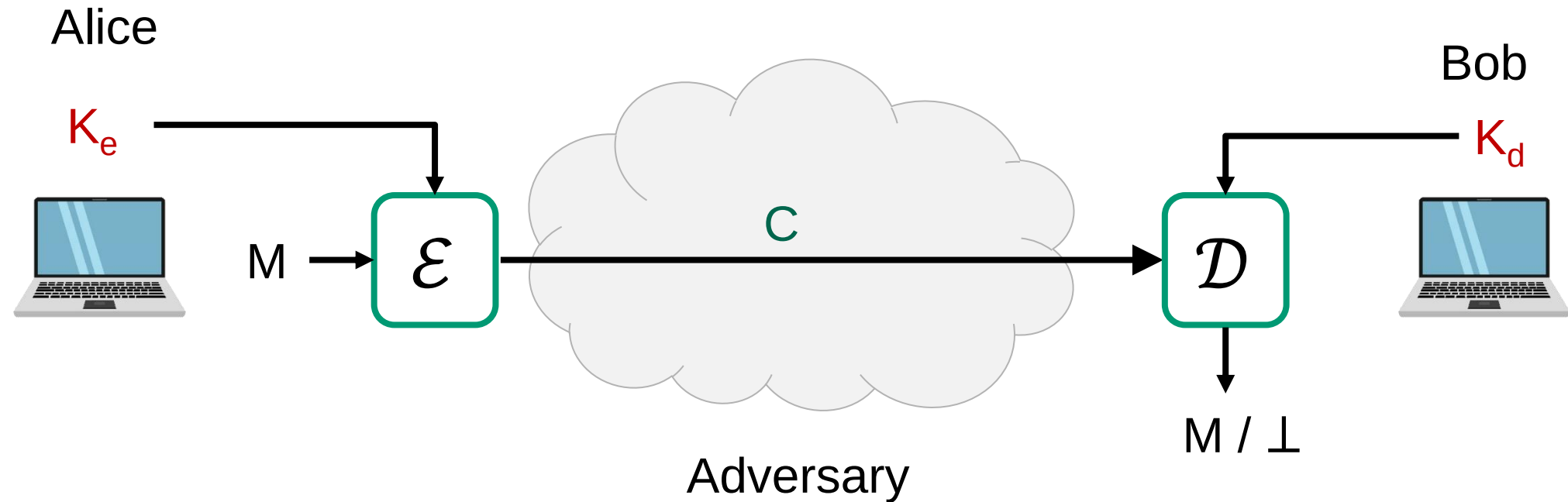


$\mathcal{E}$: encryption algorithm (public)

K : encryption / decryption key (secret)

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

Creating secure channels: encryption schemes



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

K_e : encryption key (public)

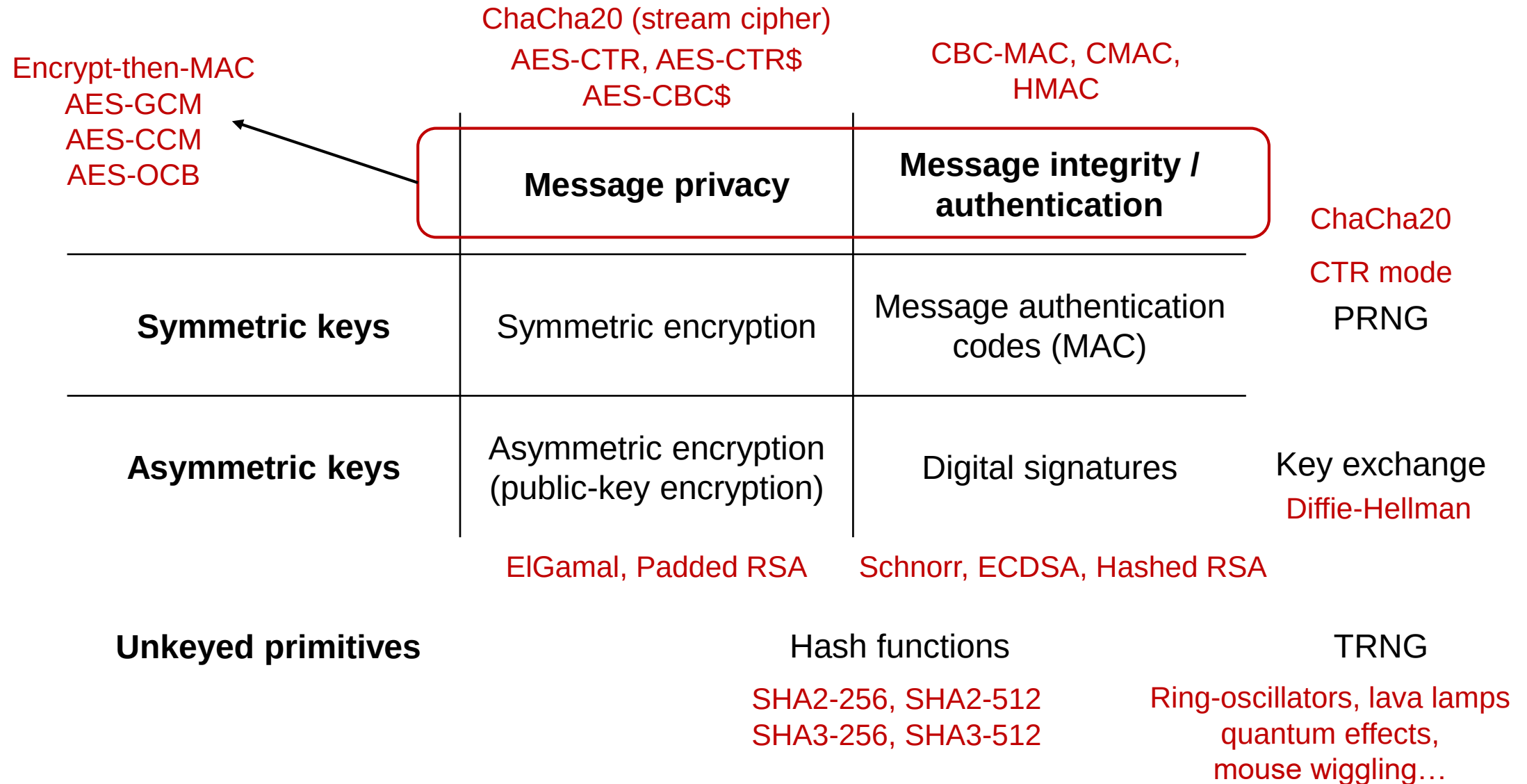
$\mathcal{D}$: decryption algorithm (public)

K_d : decryption key (secret)

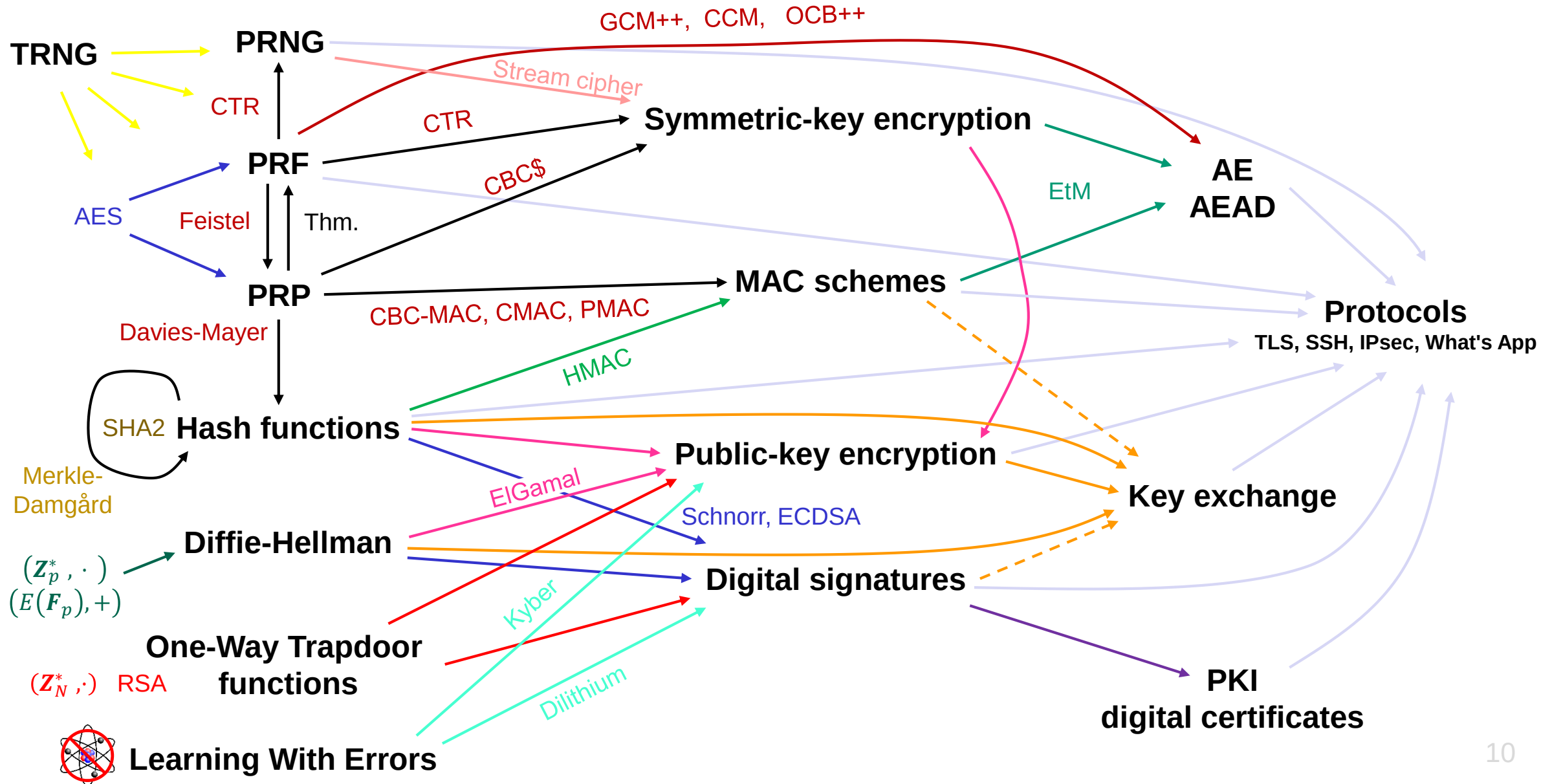
Basic goals of cryptography

	IND-CPA, IND-CCA	UF-CMA	
	Message privacy	Message integrity / authentication	
Symmetric keys	Symmetric encryption	Message authentication codes (MAC)	PRNG PRNG
Asymmetric keys	Asymmetric encryption (public-key encryption)	Digital signatures	Key exchange
	IND-CPA, IND-CCA	UF-CMA	
Unkeyed primitives		Hash functions	TRNG
		Collision resistance, one-wayness	Enough min-entropy

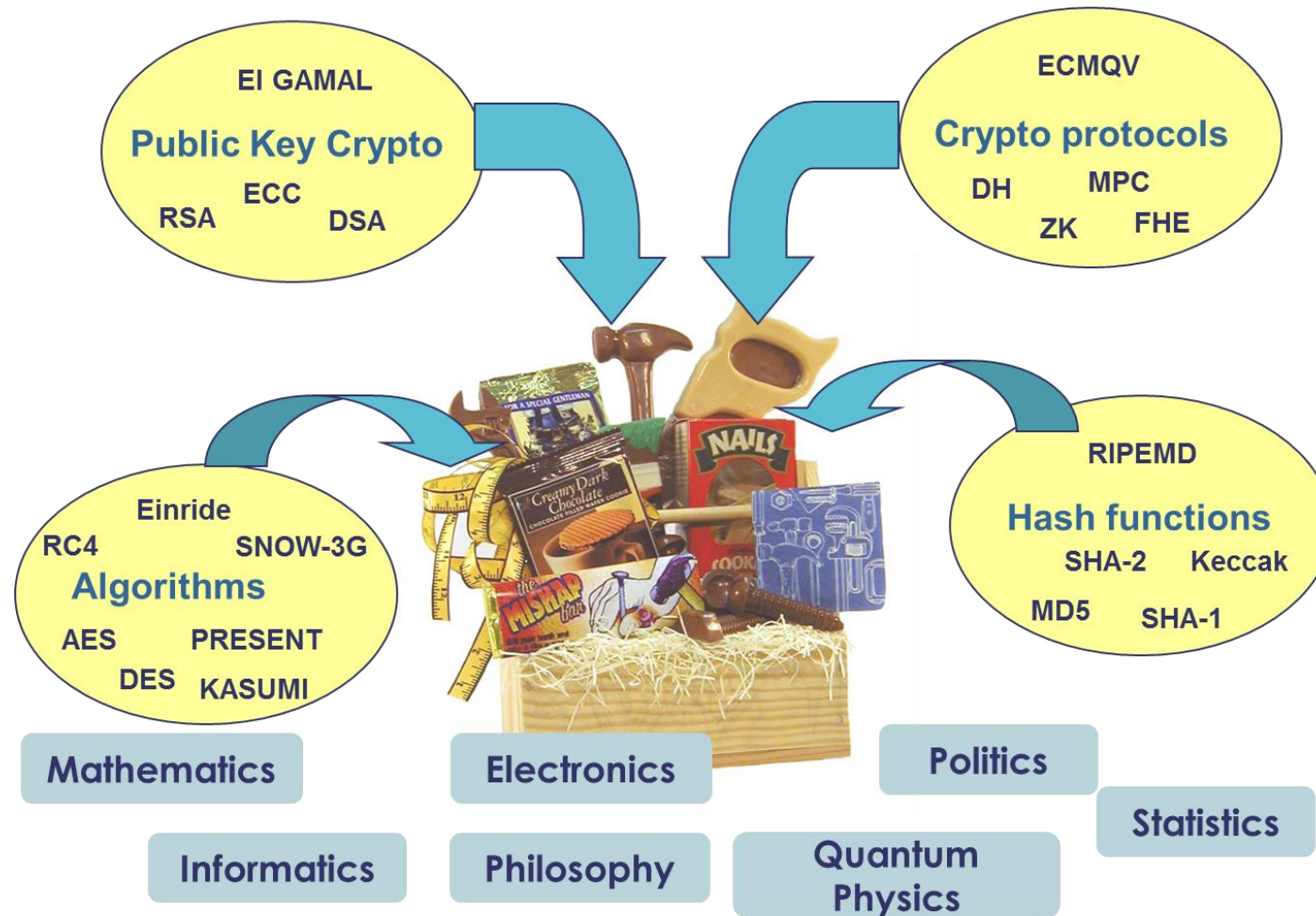
Basic goals of cryptography



Constructions and relations



The crypto toolbox



Exam

- Tuesday December 16, 15:00-19:00 (4 hours)
- Digital, on-campus (Silurveien 2, Sal 4D)
- Closed-book
- I will make a round approximately 2 hours into the exam for possible question
- <https://www.uio.no/studier/emner/matnat/its/TEK4500/h24/eksamen/index.html>

Course evaluation

- All students should have received a link to a course evaluation form by email
- Please submit your feedback to help improve the course!