Lecture 13 – Course recap

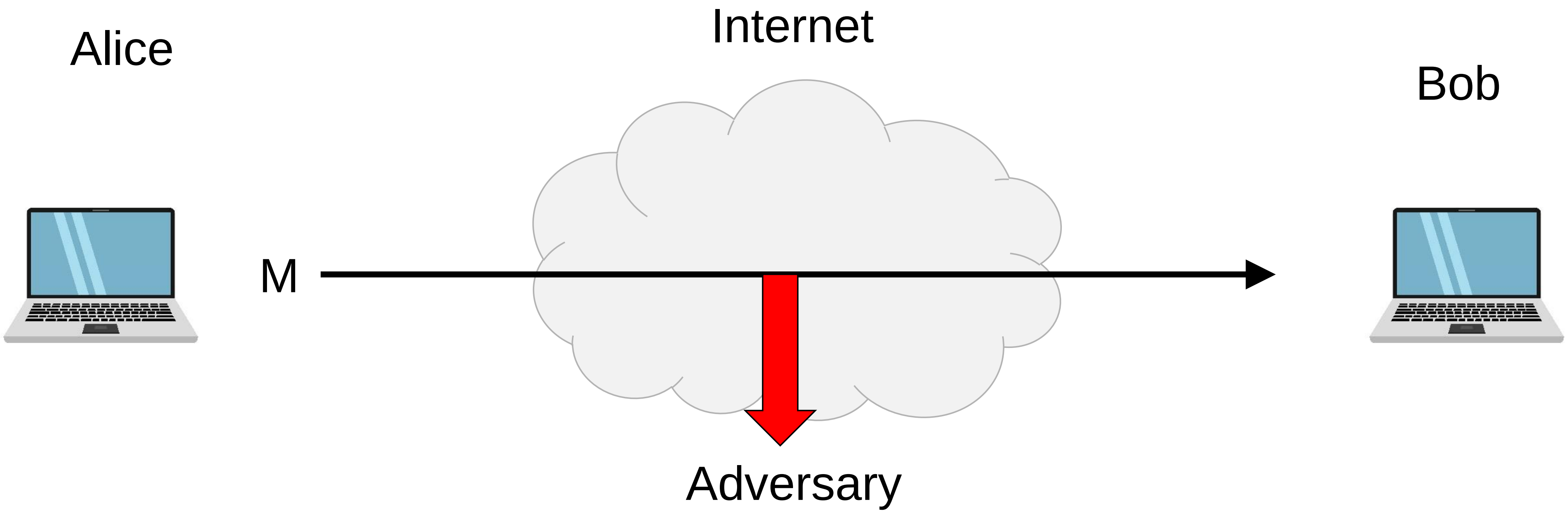
TEK4500

17.11.2020

Håkon Jacobsen

hakon.jacobsen@its.uio.no

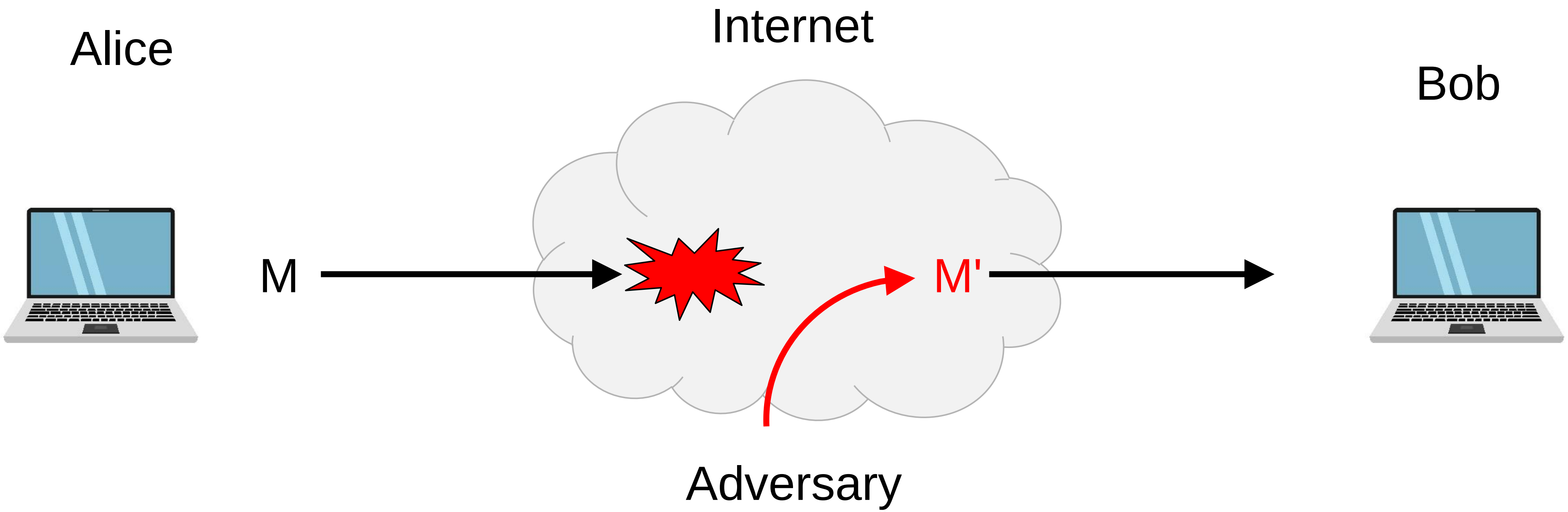
What is cryptography?



Security goals:

- **Data privacy:** adversary should not be able to read message M

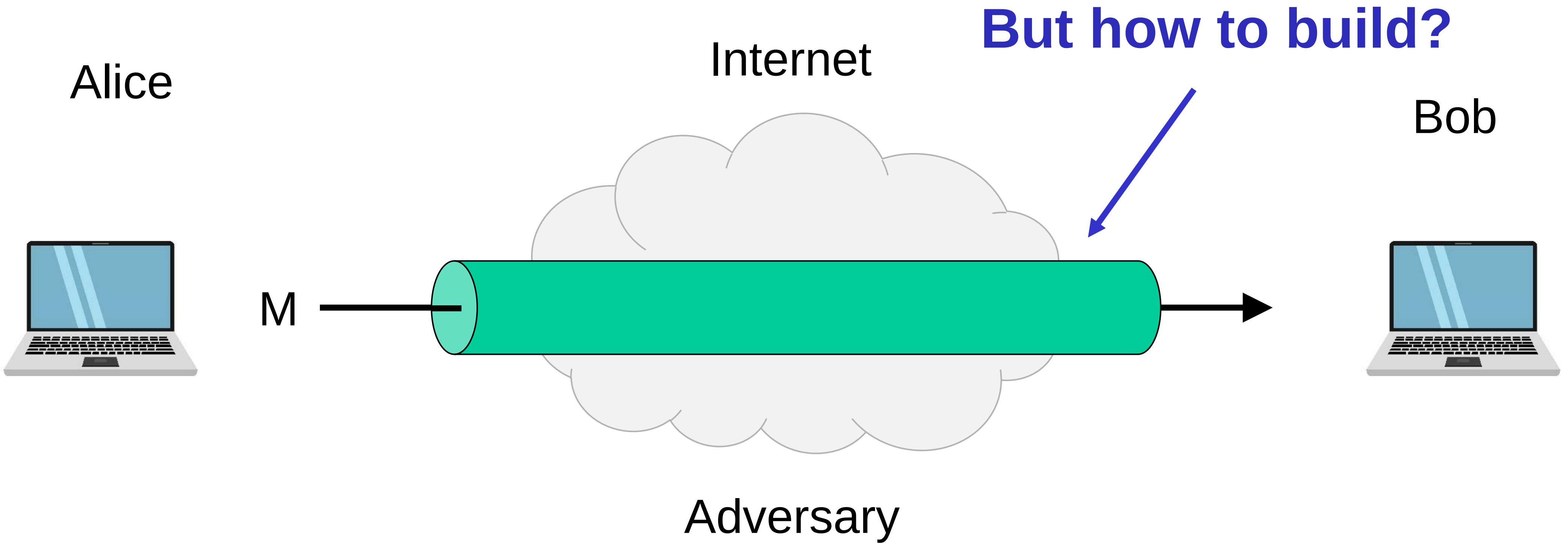
What is cryptography?



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



But how to build?

Alice

Internet

Bob

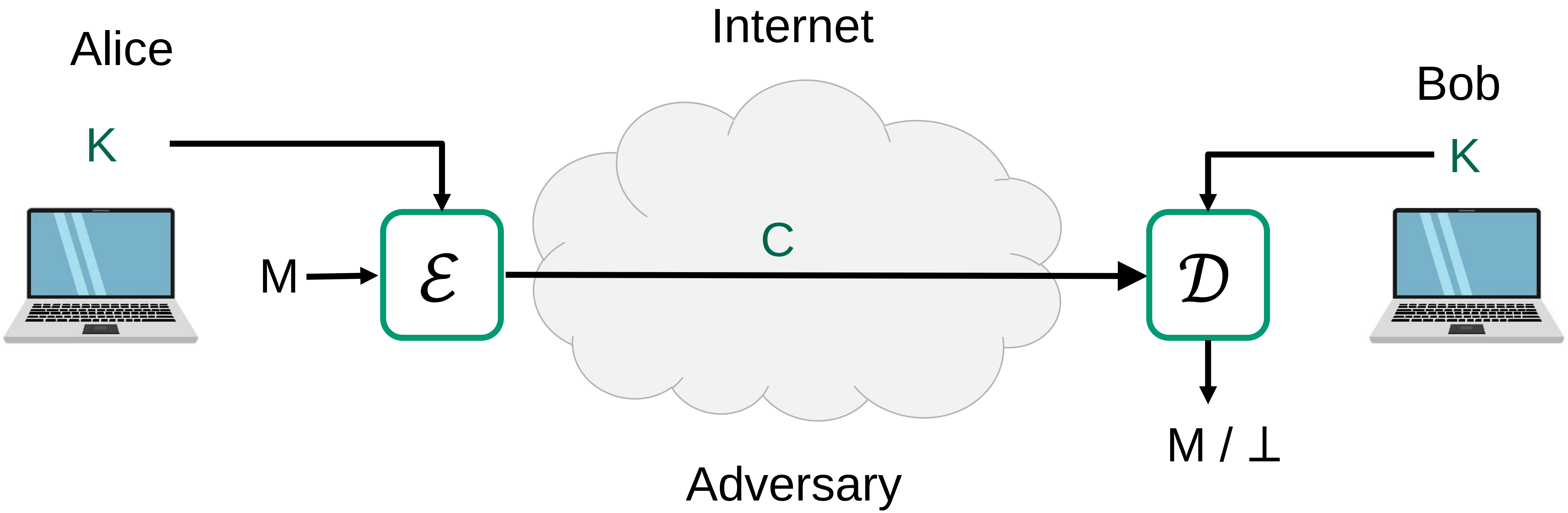
M

Adversary

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

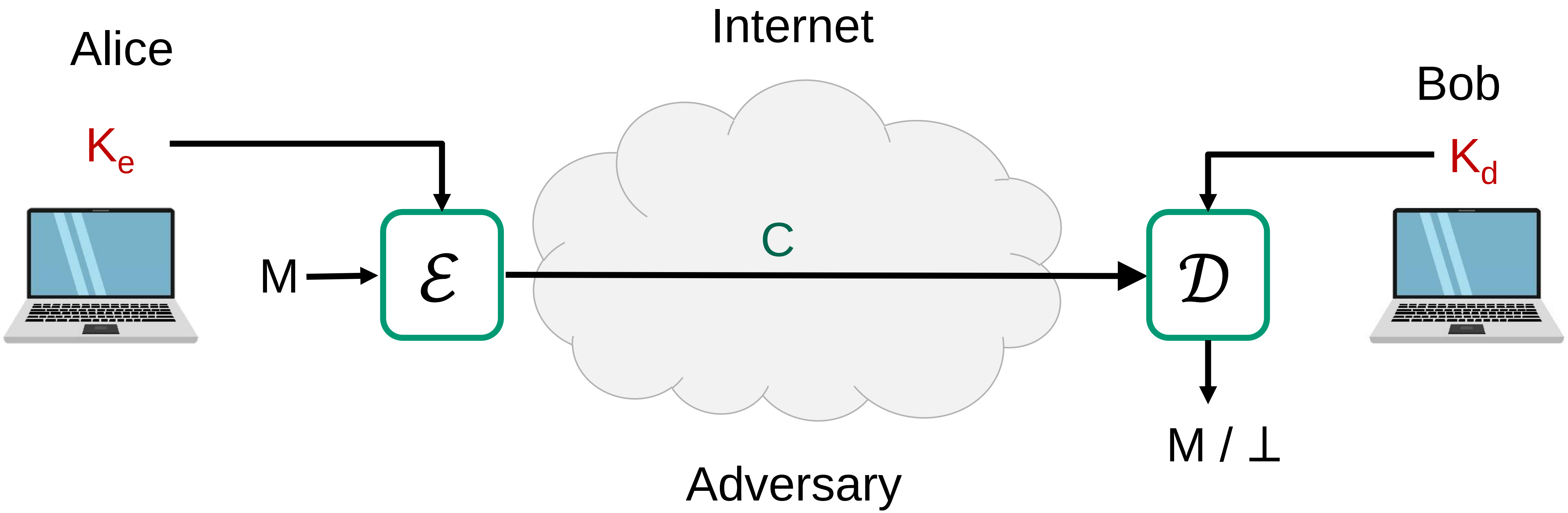


$\mathcal{E}$: encryption algorithm (public)

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

IND-CPA, IND$-CPA
IND-CCA

UF-CMA

AE

	Message privacy	**Message integrity / authentication**	
Symmetric keys	Symmetric encryption	Message authentication codes (MAC)	
Asymmetric keys	Asymmetric encryption (a.k.a. public-key encryption)	Digital signatures	(Key exchange)

IND-CPA, IND-CCA

UF-CMA

Unkeyed primitives

Hash functions

Collision resistance, one-wayness

Basic goals of cryptography

Encrypt-then-MAC
AES-GCM
AES-CCM
AES-OCB

AES-CTR, AES-CTR$
AES-CBC$

CBC-MAC, CMAC,
PRF

	Message privacy	Message integrity / authentication
Symmetric keys	Symmetric encryption	Message authentication codes (MAC)
Asymmetric keys	Asymmetric encryption (a.k.a. public-key encryption)	Digital signatures

Diffie-Hellman

(Key exchange)

ElGamal, Padded RSA

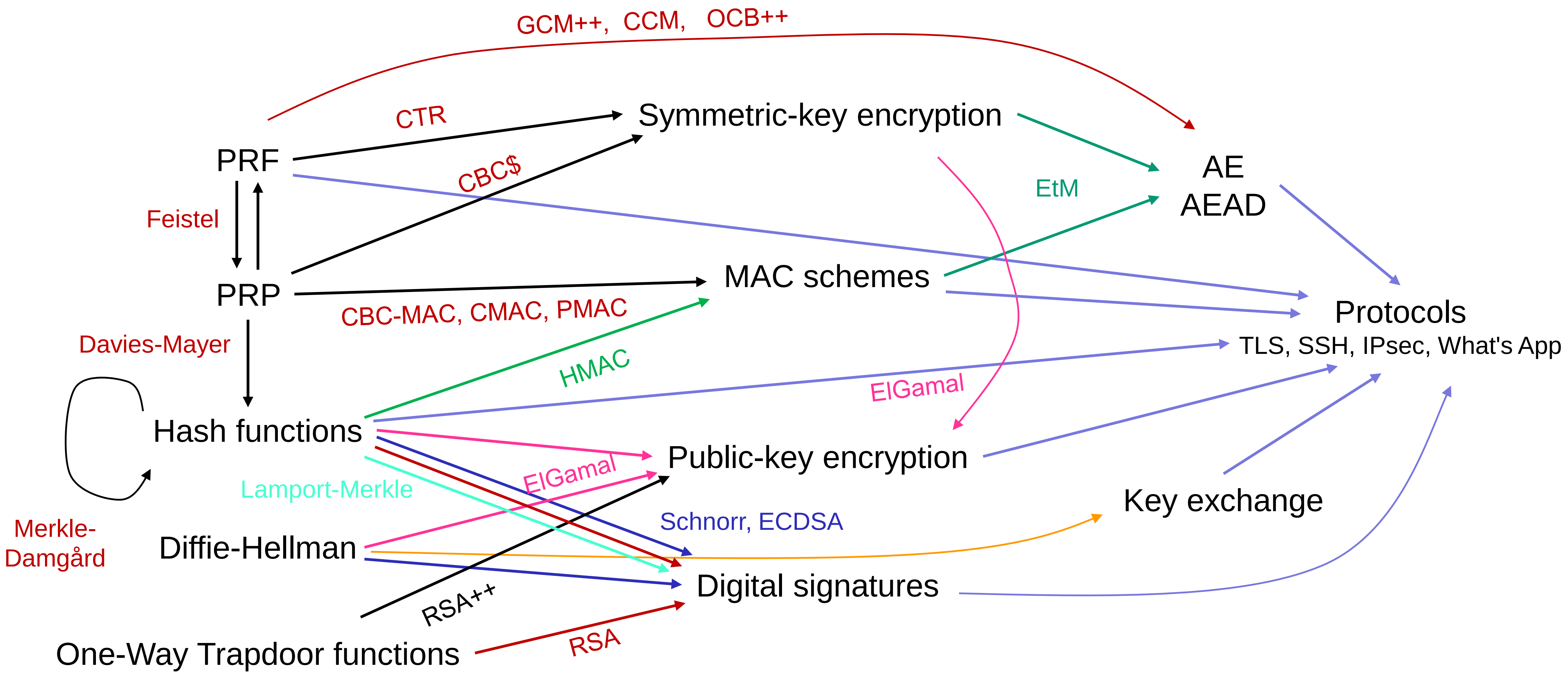
Schnorr, ECDSA, Hashed RSA

Unkeyed primitives

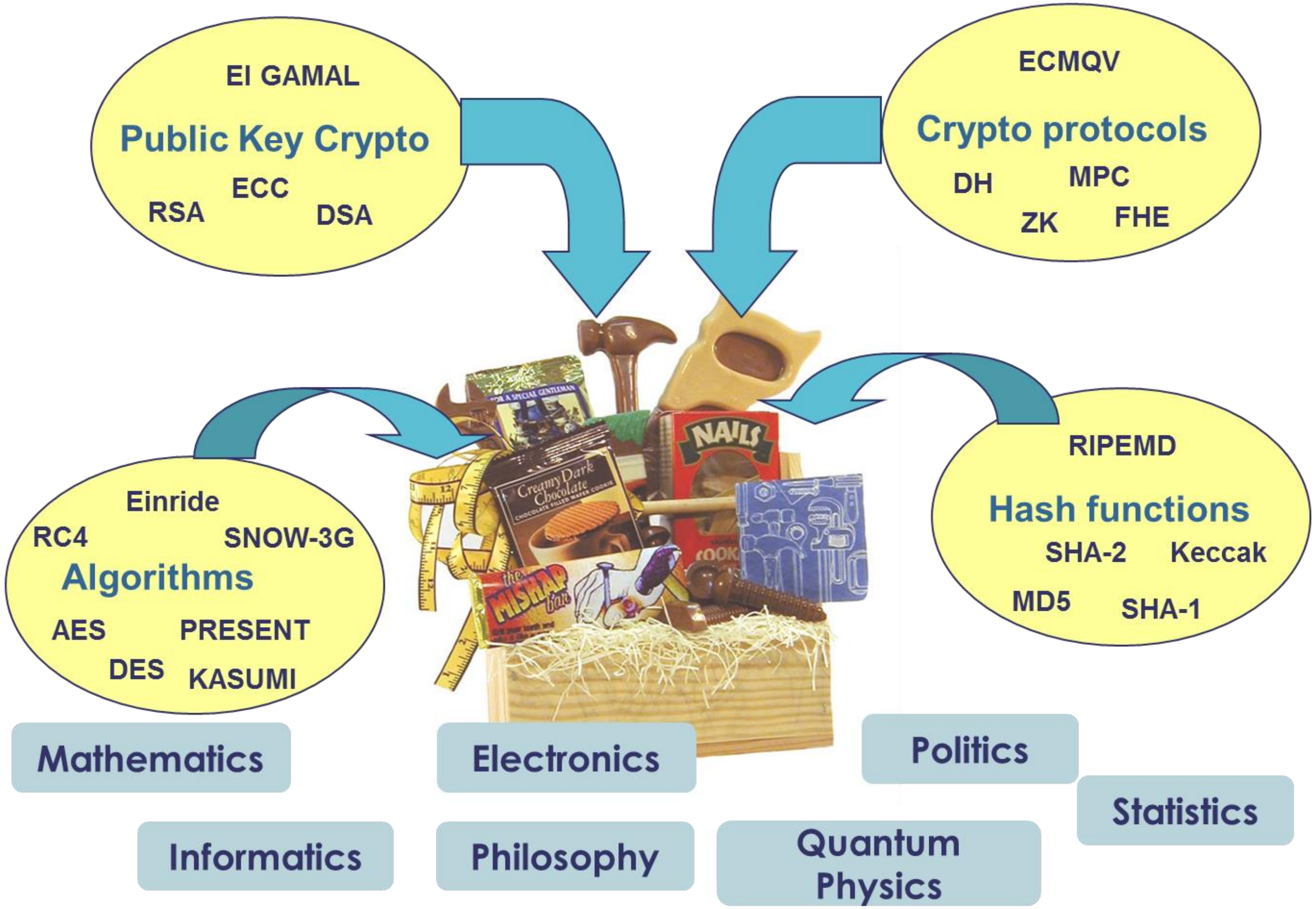
Hash functions

SHA2-256, SHA2-512
SHA3-256, SHA3-512

Constructions and relations



The crypto toolbox



El GAMAL

Public Key Crypto

ECC

RSA

DSA

ECMQV

Crypto protocols

DH

MPC

ZK

FHE

Einride

RC4

SNOW-3G

Algorithms

AES

PRESENT

DES

KASUMI

RIPEMD

Hash functions

SHA-2

Keccak

MD5

SHA-1

Mathematics

Electronics

Politics

Statistics

Informatics

Philosophy

Quantum Physics

Exam

- Digital home exam
- Wednesday November 25, 09:00-13:30 (4.5 hours)
- Format: single PDF file made available on Inspera and Canvas (similar to midterm)
- Answers are typed directly into Inspera (no PDF upload); will create forms that mirrors problems in exam PDF
- **NO collaboration** is allowed
  - Students may be picked out for conversations to prove ownership of answer
- I will be available on Zoom for questions (you can also send emails)