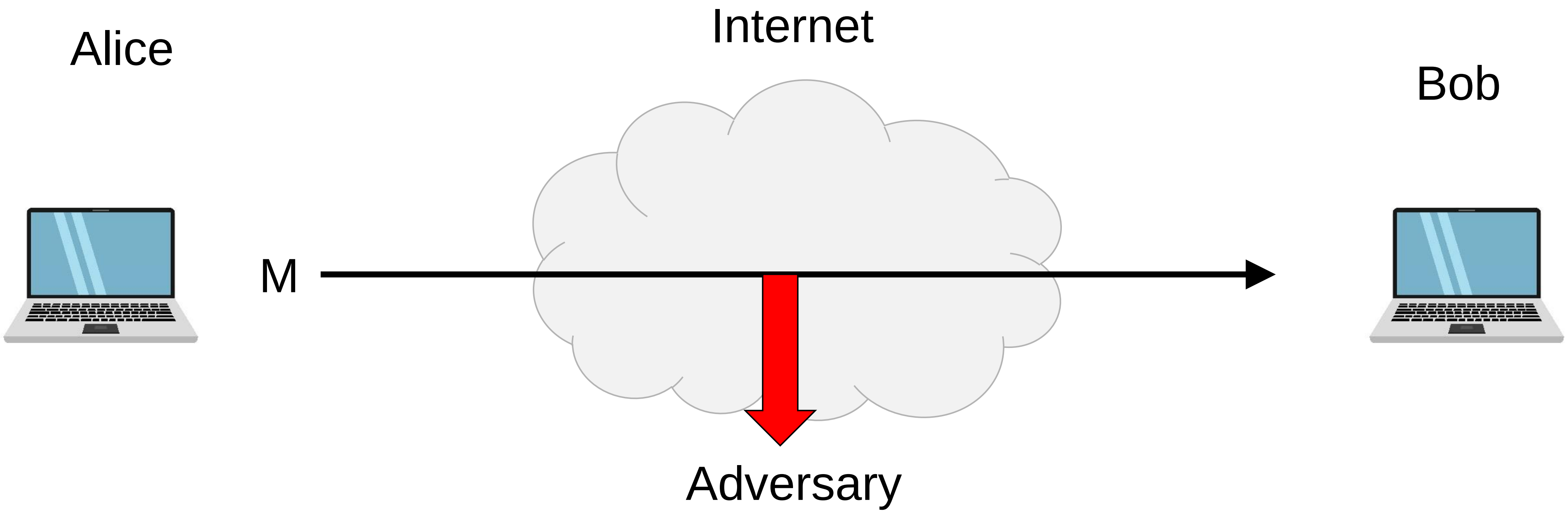
Lecture 14 – Course recap

TEK4500

24.11.2021

Håkon Jacobsen
hakon.jacobsen@its.uio.no

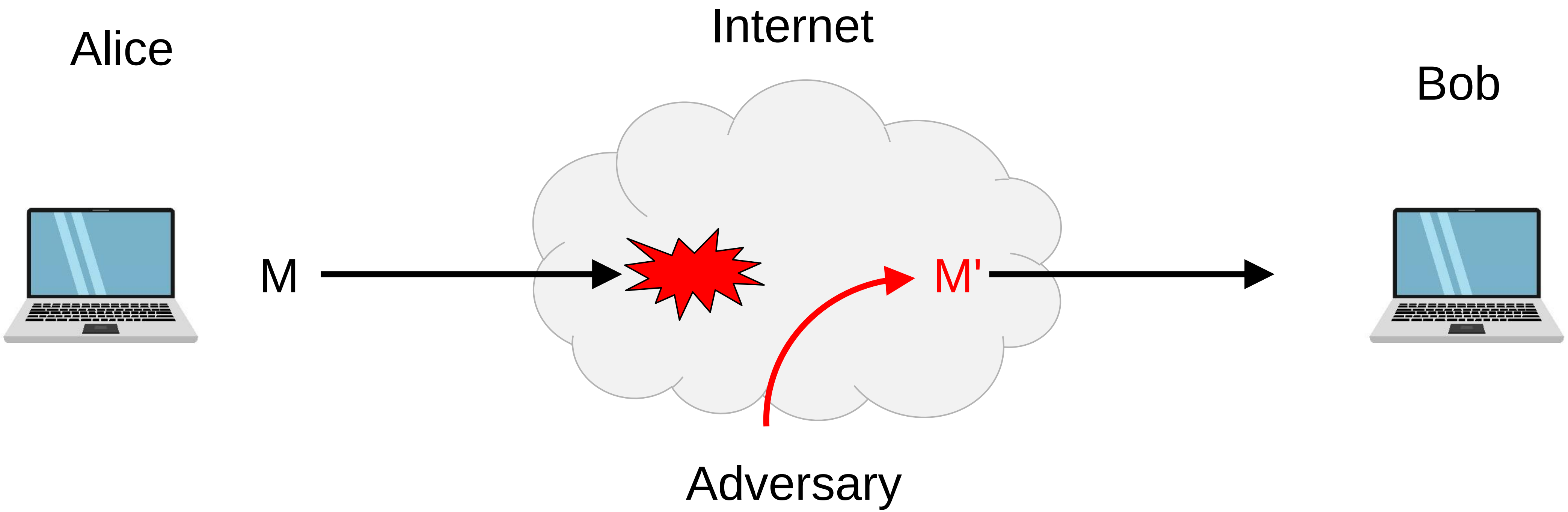
What is cryptography?



Security goals:

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

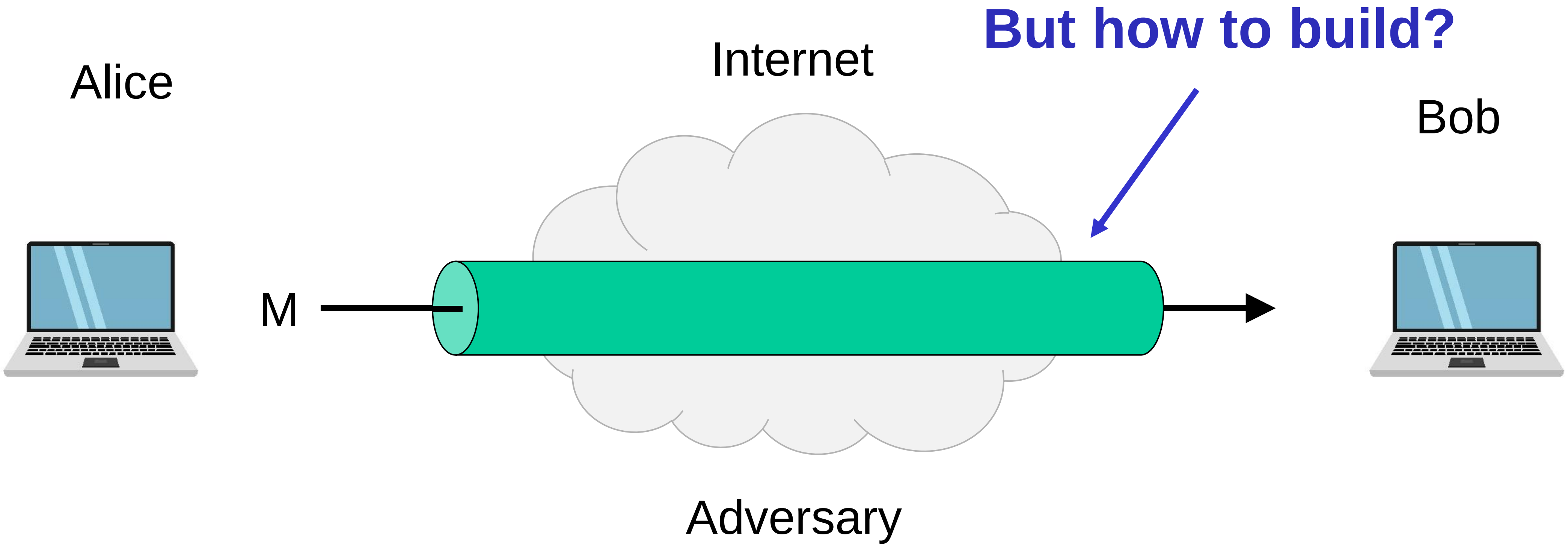
What is cryptography?



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

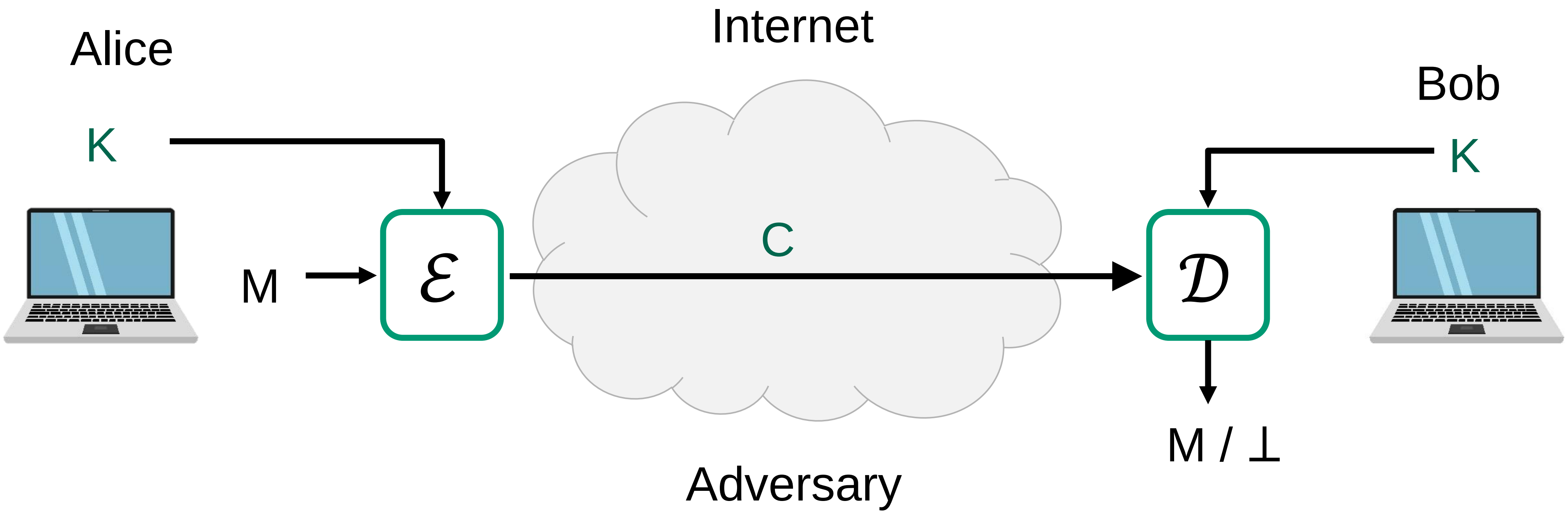


But how to build?

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

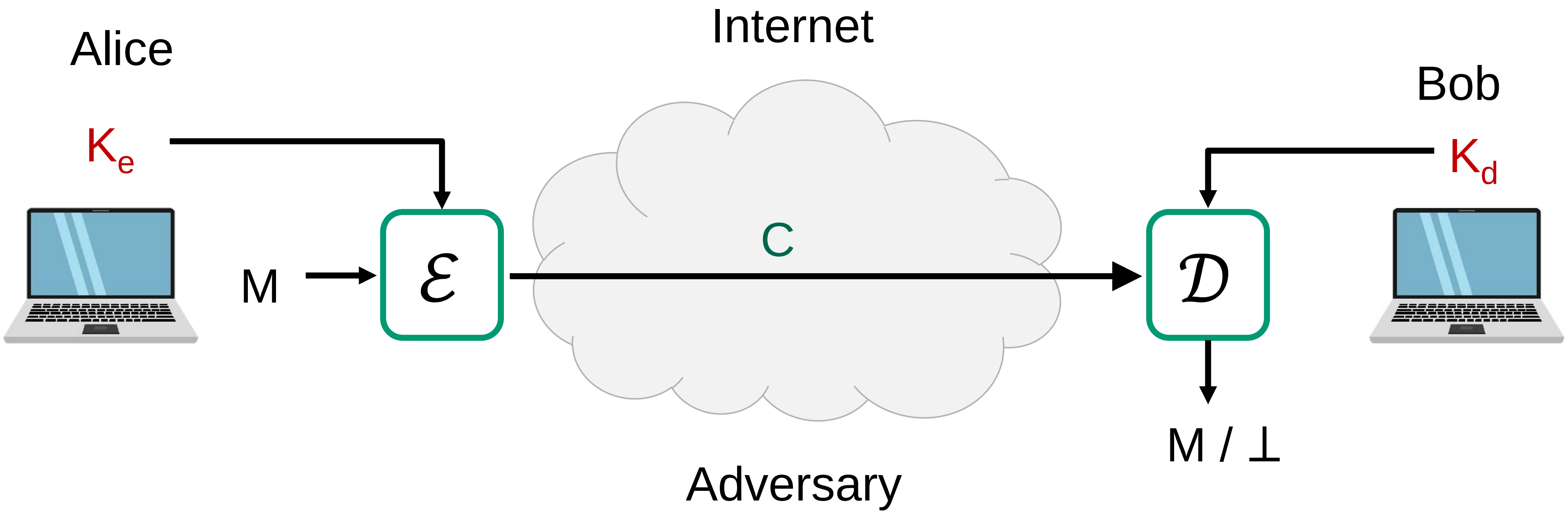


$\mathcal{E}$: encryption algorithm (public)

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-CCA UF-CMA

AE

	Message privacy	Message integrity / authentication	Enough min-entropy
Symmetric keys	Symmetric encryption	Message authentication codes (MAC)	True random generators Pseudrandom generators PRG
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,
HMAC

	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

ElGamal, Padded RSA

Schnorr, ECDSA, Hashed RSA

Ring-oscillators,
lava lamps,
quantum effects, ...

True random generators

CTR mode

Pseudrandom generators

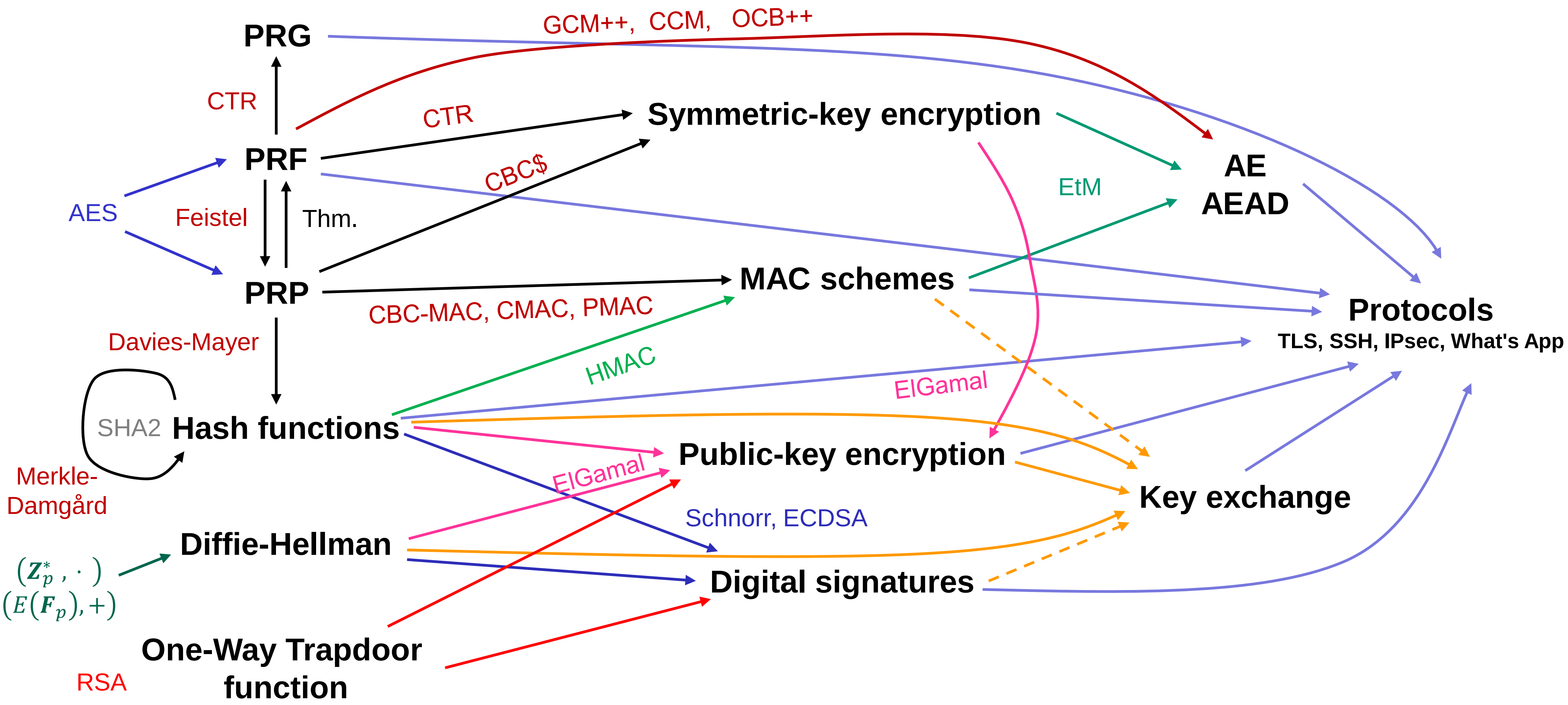
Key exchange

Diffie-Hellman

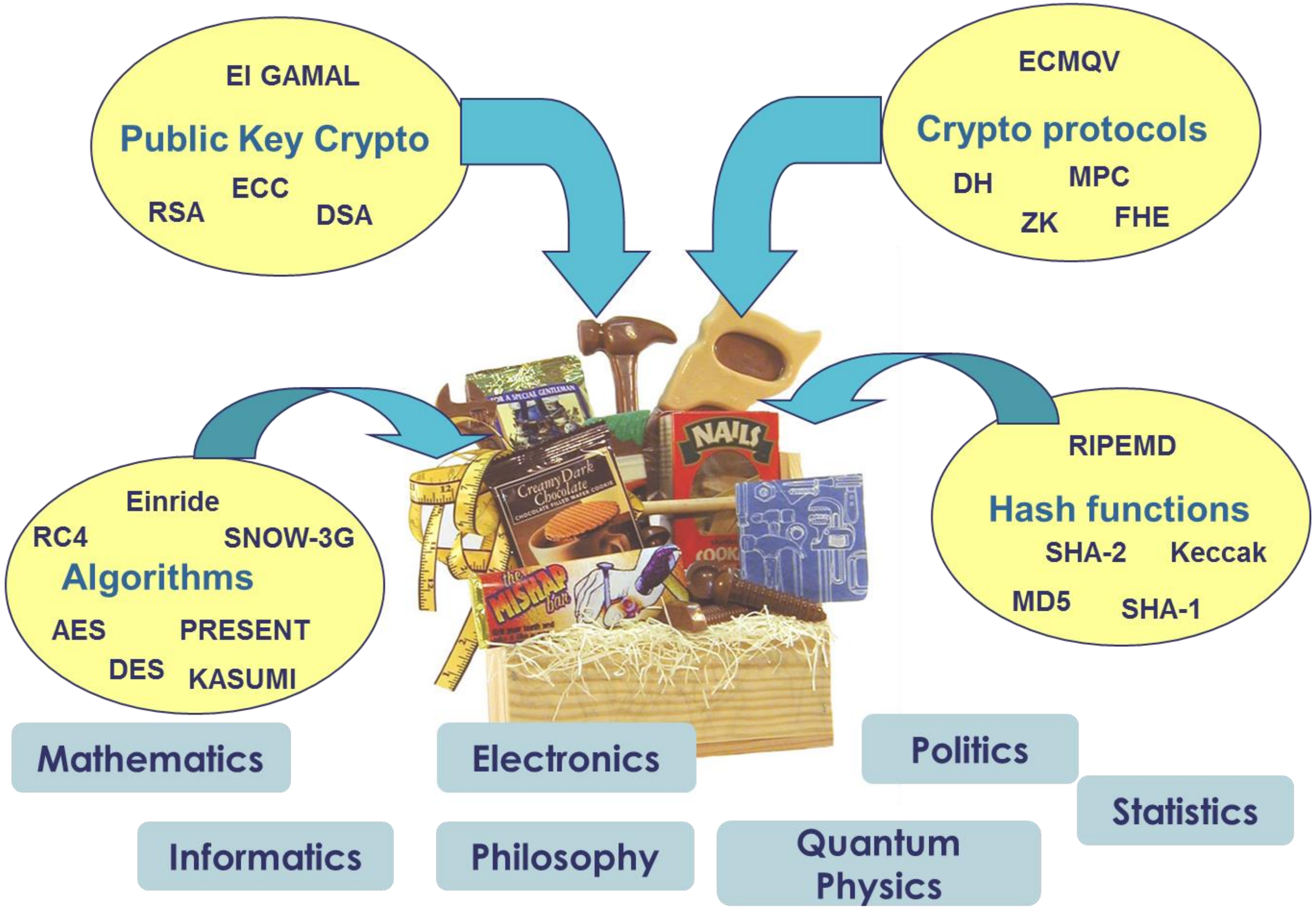
Unkeyed primitives Hash functions

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

Constructions and relations



The crypto toolbox



Exam

- Wednesday December 08, 15:00-19:00 (4 hours)

- Digital on-campus exam

- Closed-book exam