

---

# Lecture 14 – Course recap

**TEK4500**

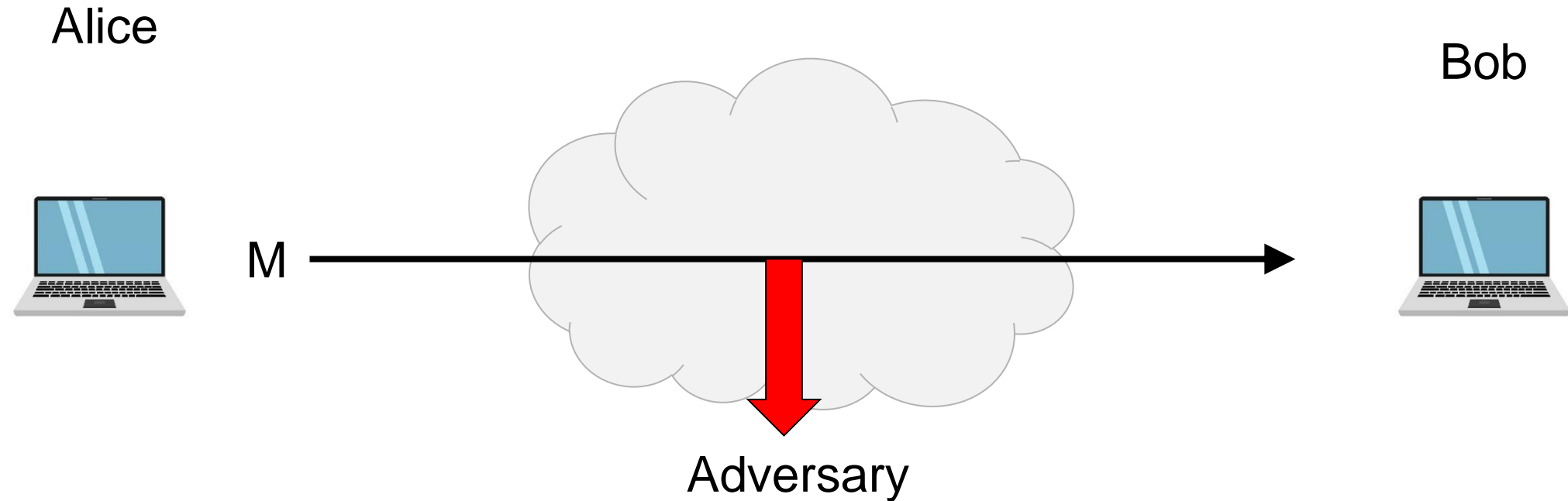
23.11.2022

Håkon Jacobsen

[hakon.jacobsen@its.uio.no](mailto:hakon.jacobsen@its.uio.no)

# What is cryptography?

---

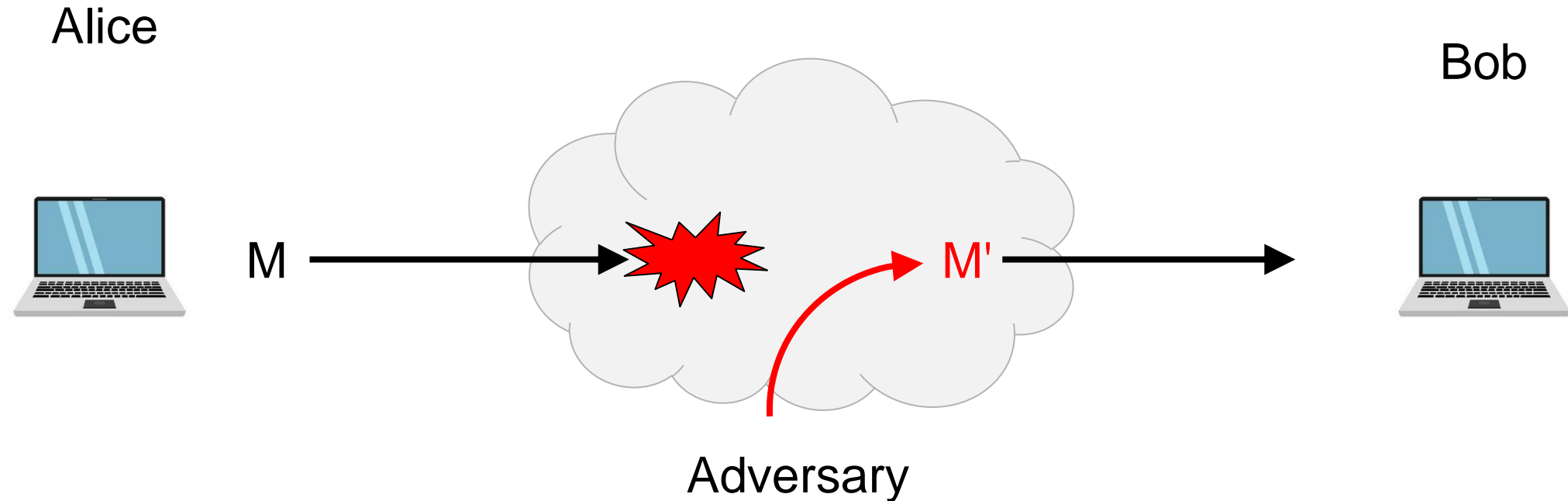


## Security goals:

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

# What is cryptography?

---

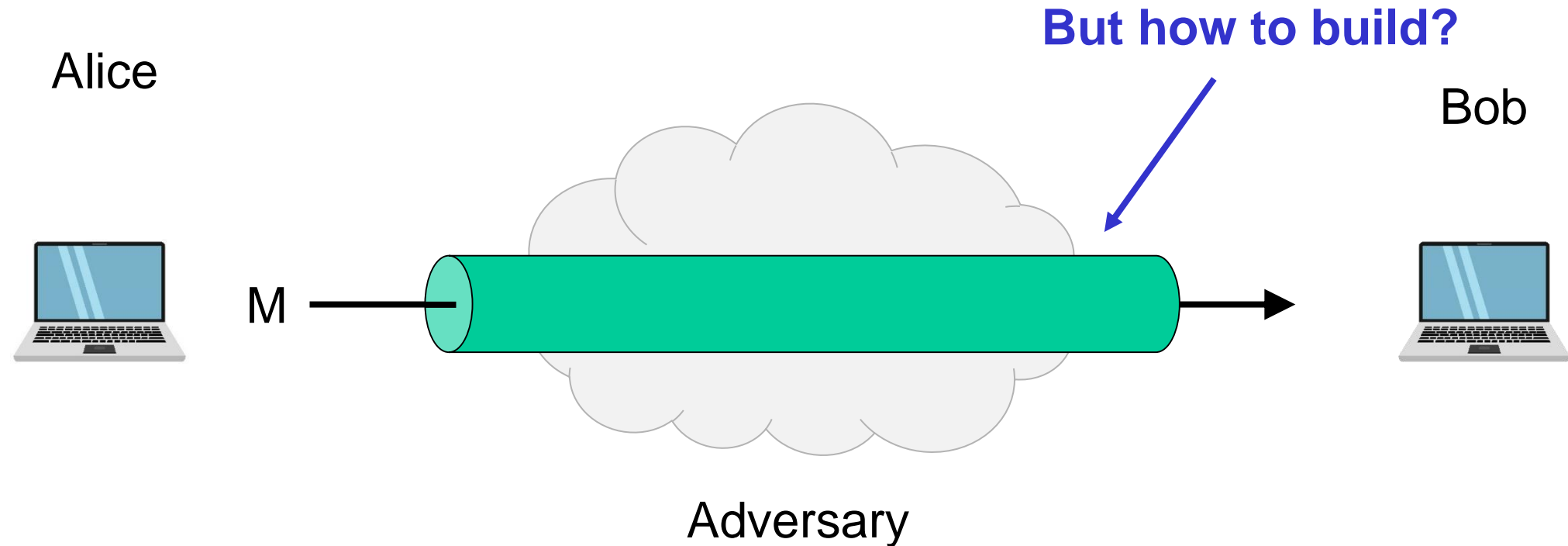


## Security goals:

- **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

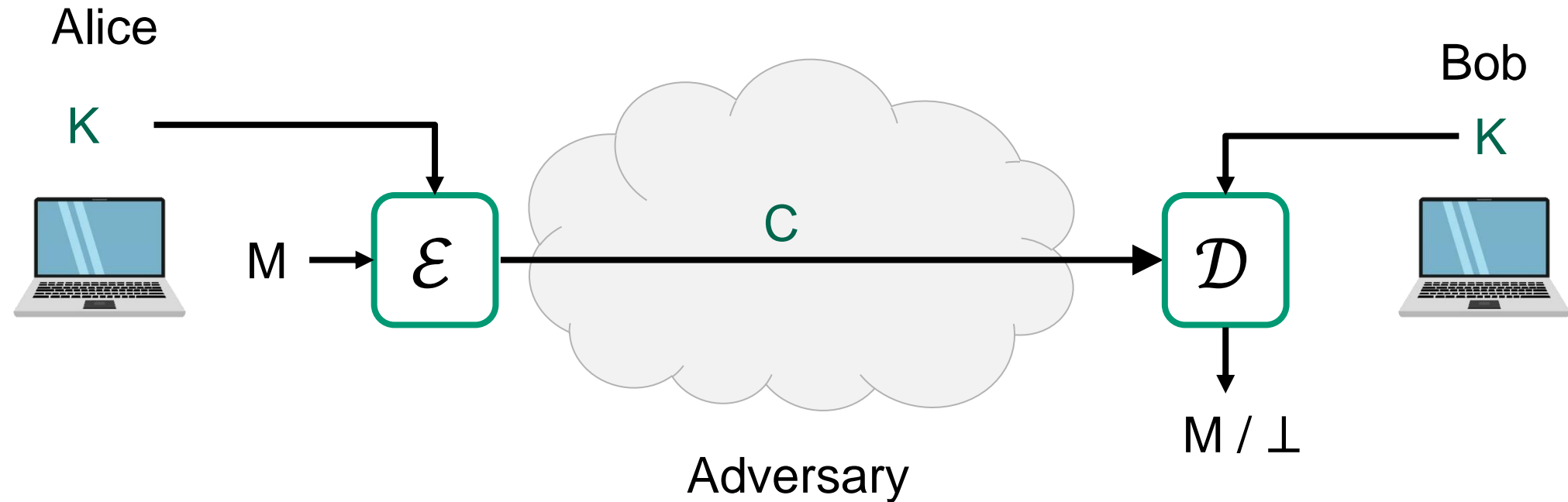
---



## 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

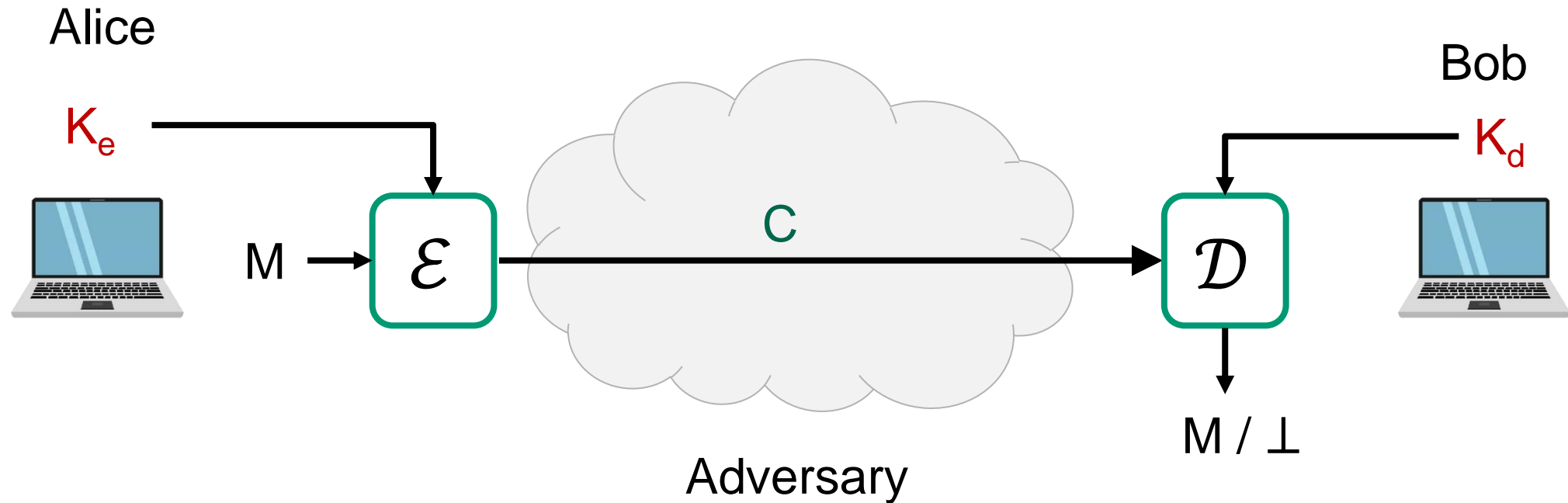


$\mathcal{E}$  : encryption algorithm (public)

$K$  : encryption / decryption key (secret)

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

# Creating secure channels: encryption schemes



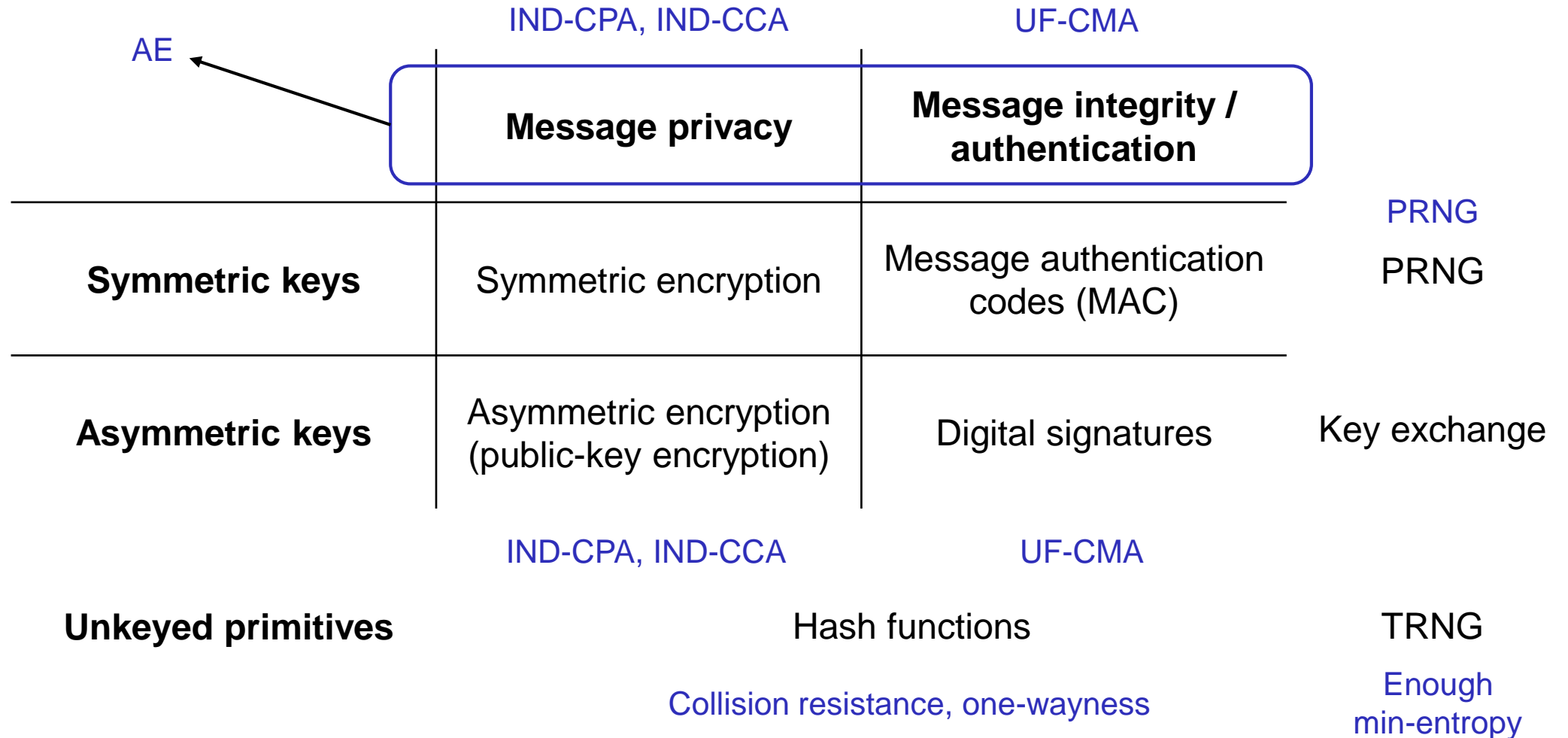
$\mathcal{E}$  : encryption algorithm (public)

$K_e$  : encryption key (public)

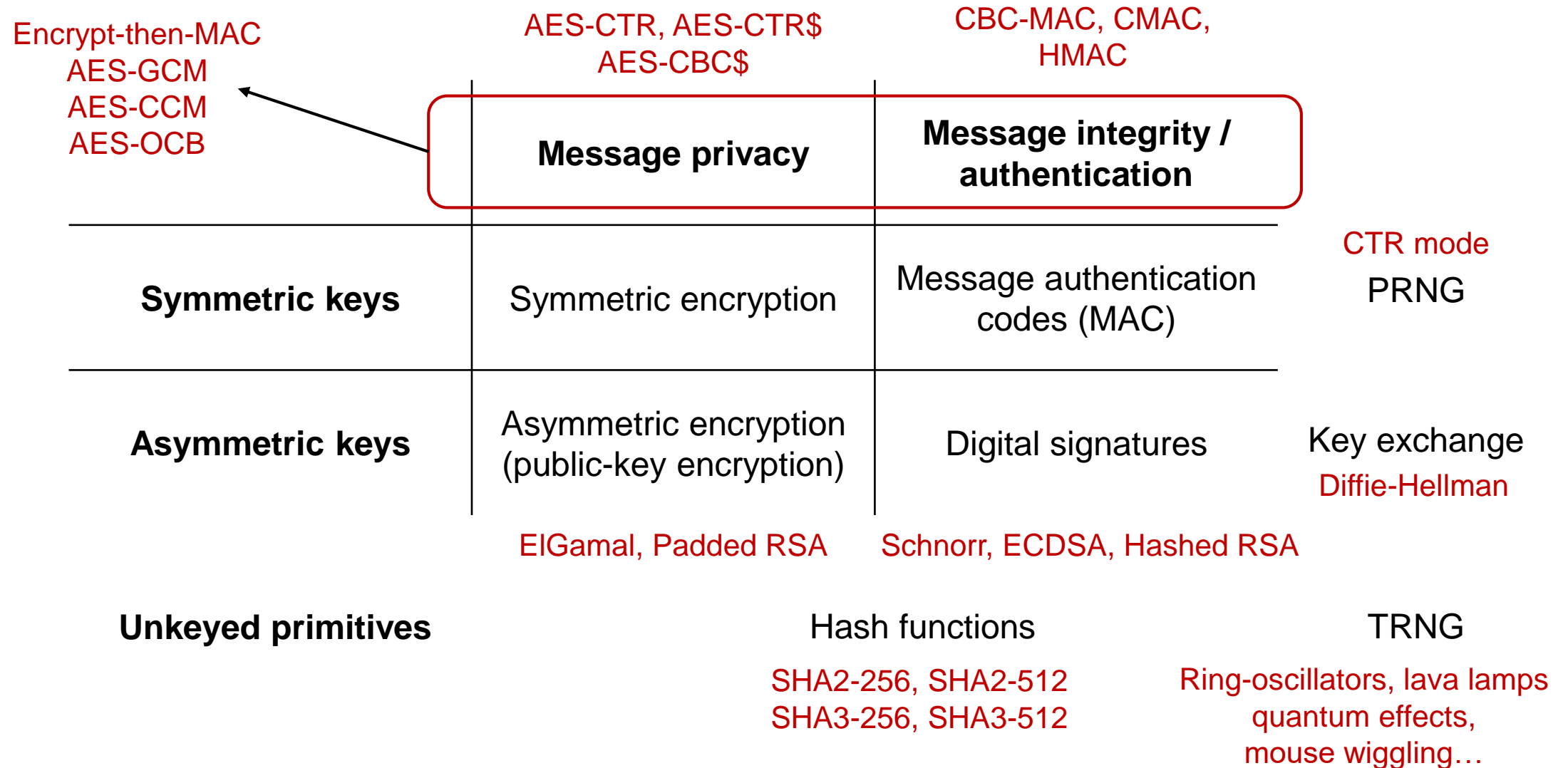
$\mathcal{D}$  : decryption algorithm (public)

$K_d$  : decryption key (secret)

# Basic goals of cryptography

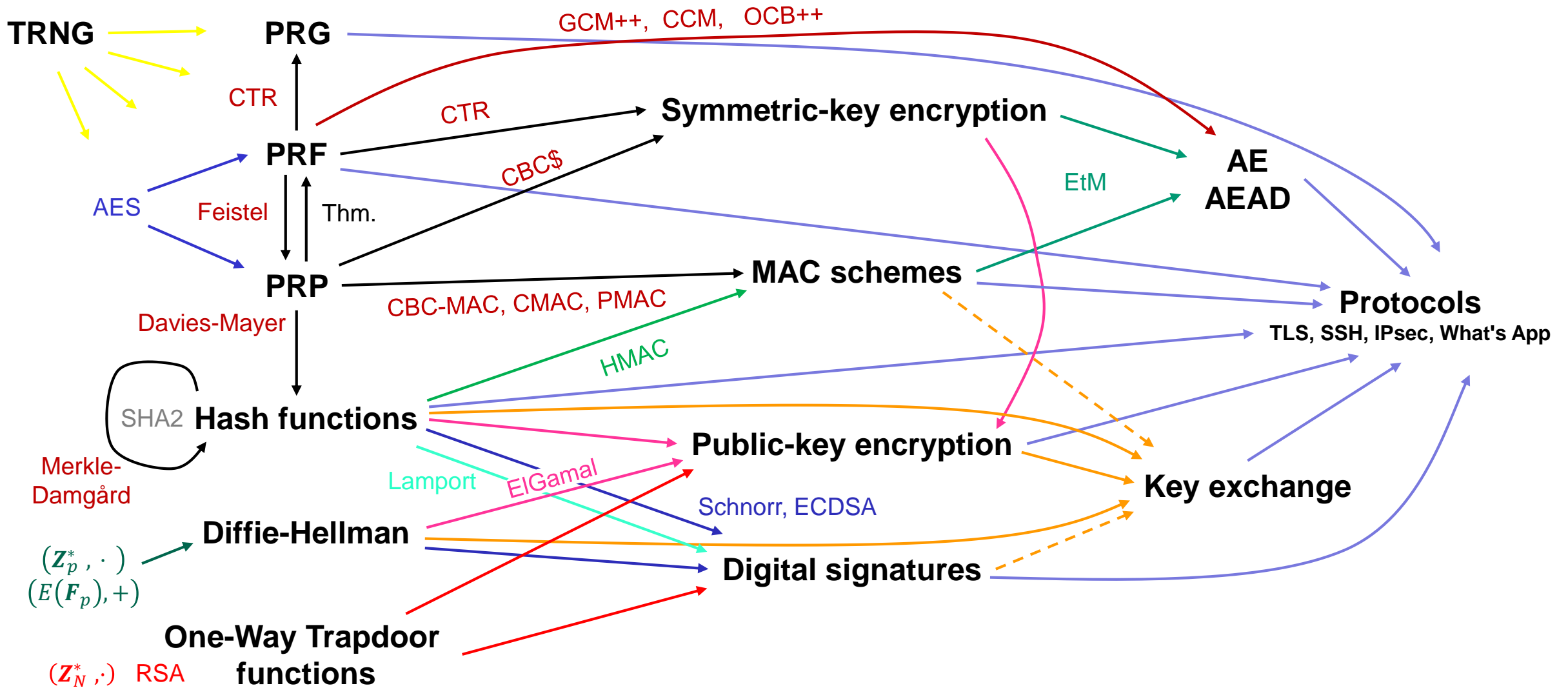


# Basic goals of cryptography

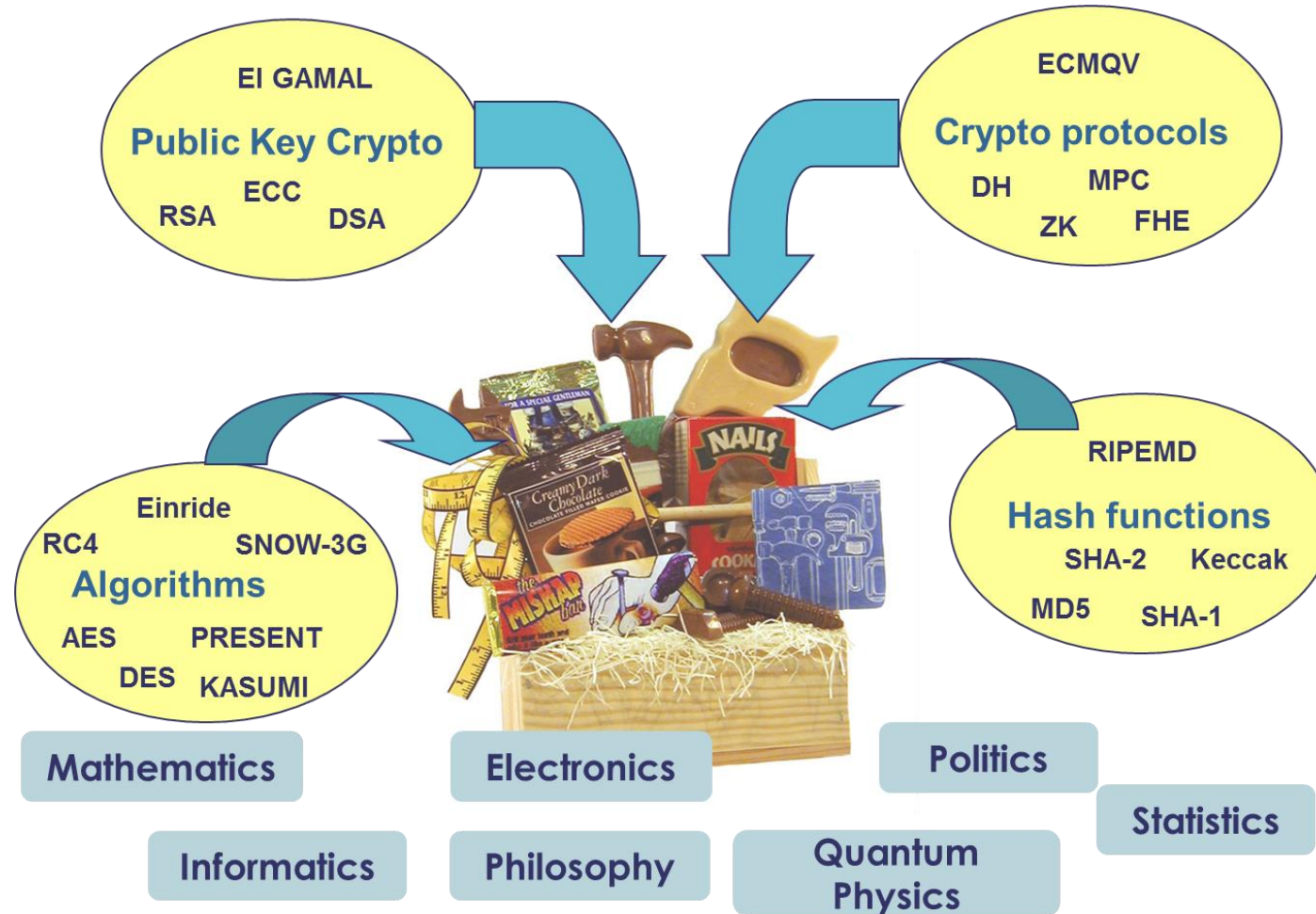




# Constructions and relations



# The crypto toolbox



# Exam

---

- Tuesday December 06, 15:00-19:00 (4 hours)
- Digital, on-campus (Silurveien 2, Sal 3B+3D)
- Closed-book