Lecture 15 – Course recap

TEK4500

06.12.2023

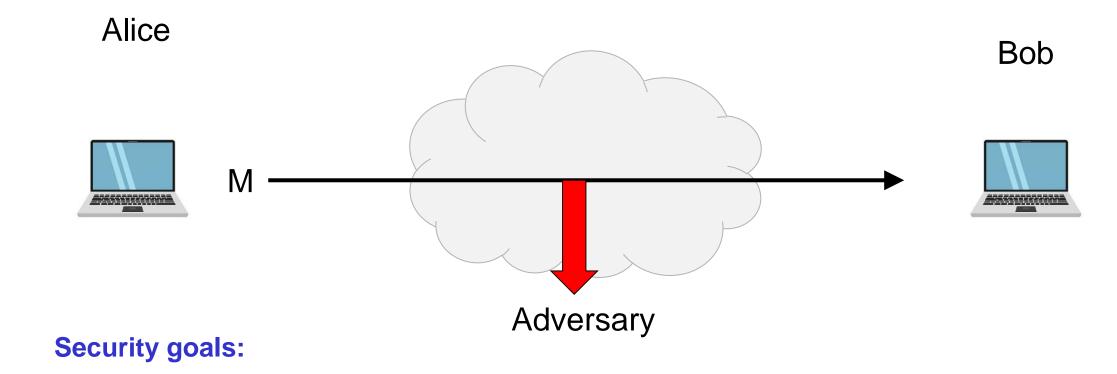
Håkon Jacobsen

hakon.jacobsen@its.uio.no

Agenda

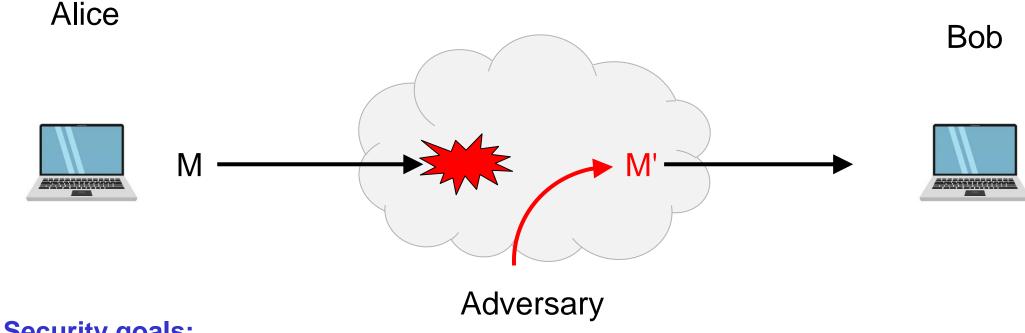
- Info on Heidelberg Laureate Forum by Hagen Echzell
- Recap of course
- Q&A
- Go through exam from 2022 (offline)

What is cryptography?



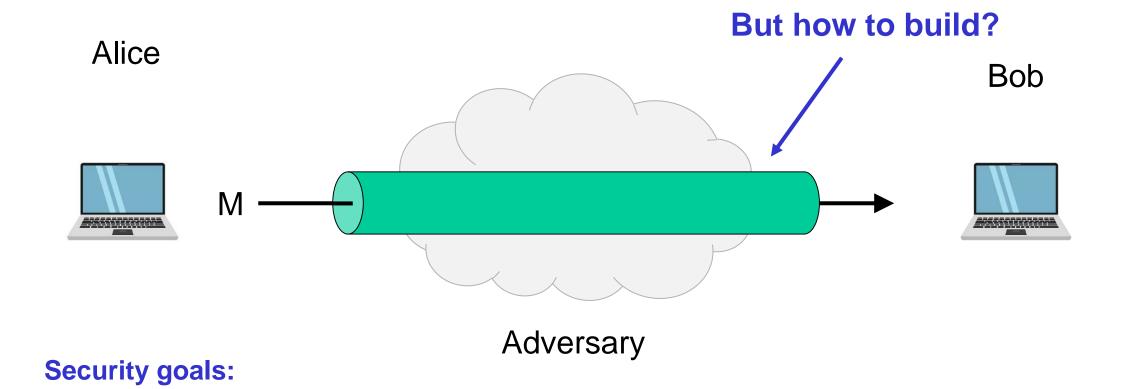
• Data privacy: adversary should not be able to read message M

What is cryptography?



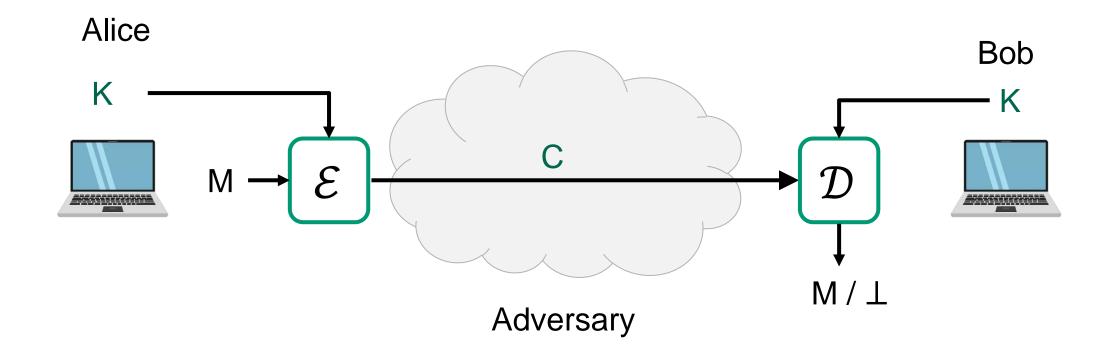
- **Security goals:**
- Data privacy: adversary should not be able to read message M
- Data integrity: adversary should not be able to modify message M
- Data authenticity: message M really originated from Alice

Ideal solution: secure channels



- 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

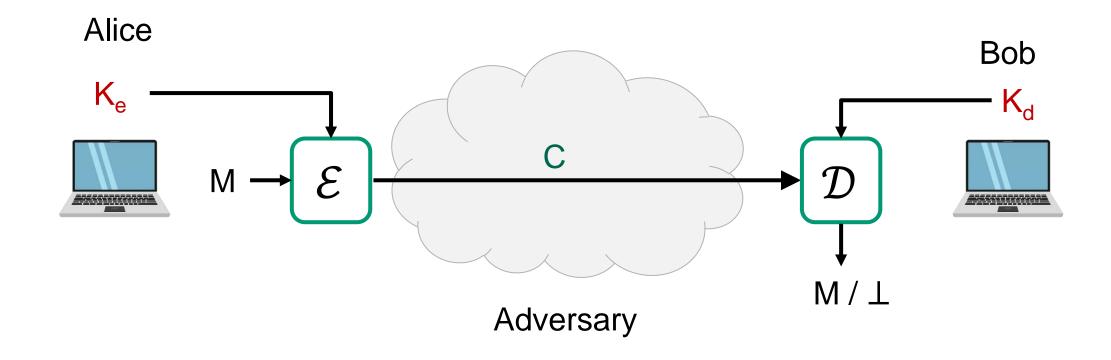


E: encryption algorithm (public)

K: encryption / decryption key (secret)

D: decryption algorithm (public)

Creating secure channels: encryption schemes



E: encryption algorithm (public)

1: decryption algorithm (public)

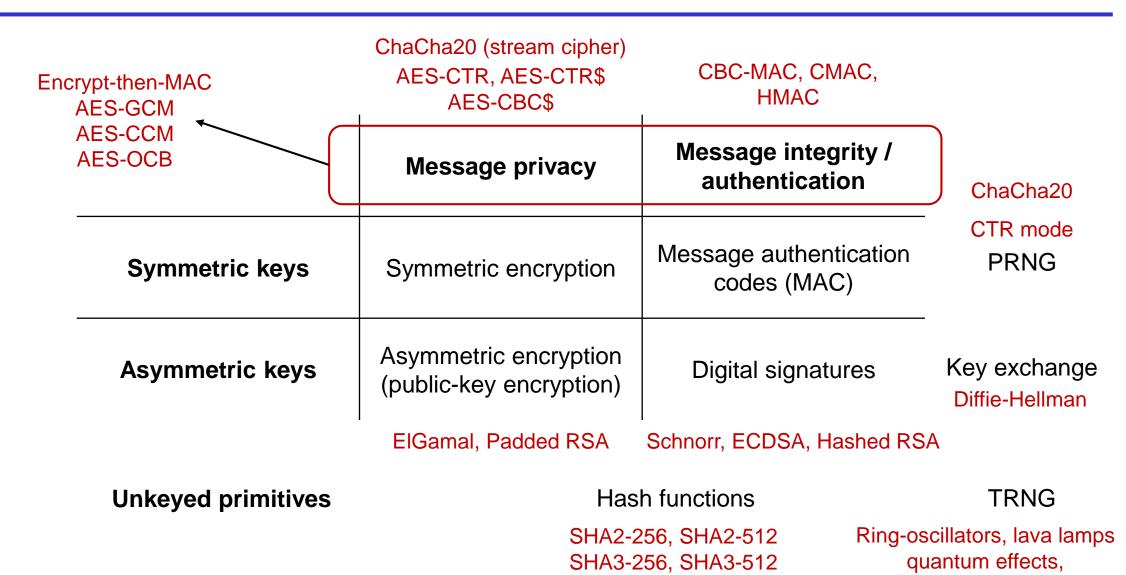
K_e: encryption key (public)

K_d: decryption key (secret)

Basic goals of cryptography

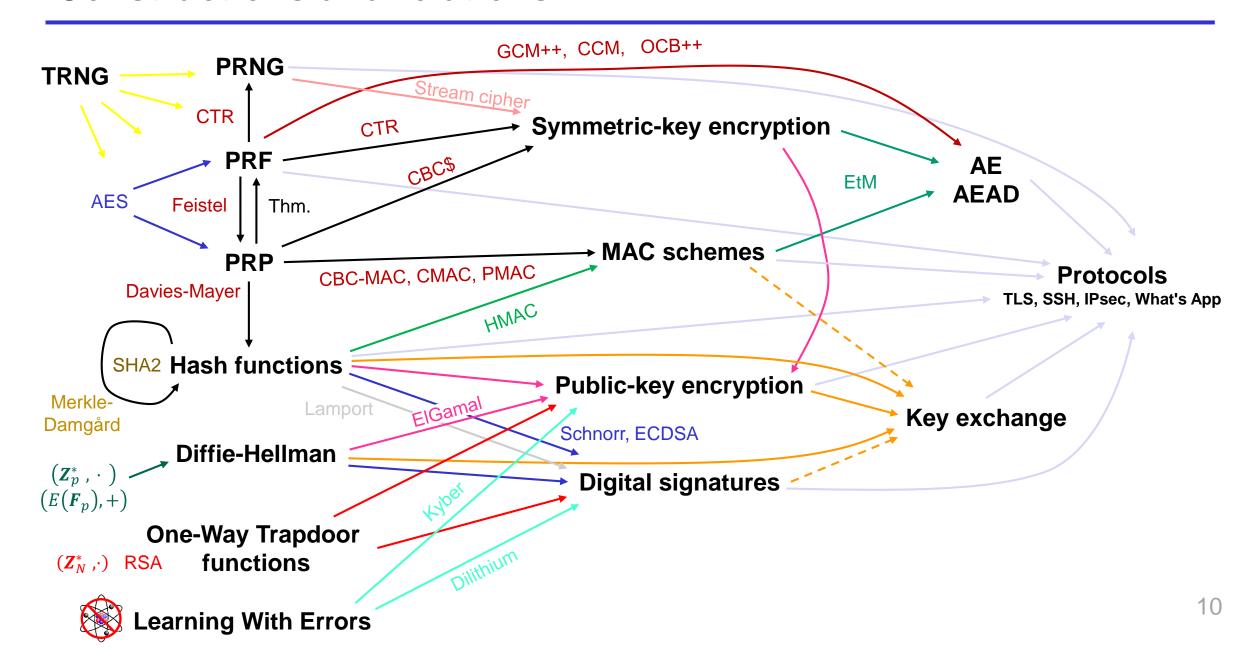
AEAD	IND-CPA, IND-CCA	UF-CMA	
	Message privacy	Message integrity / authentication	
Symmetric keys	Symmetric encryption	Message authentication codes (MAC)	PRNG PRNG
Asymmetric keys	Asymmetric encryption (public-key encryption)	Digital signatures	Key exchange
	IND-CPA, IND-CCA	UF-CMA	
Unkeyed primitives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

Basic goals of cryptography

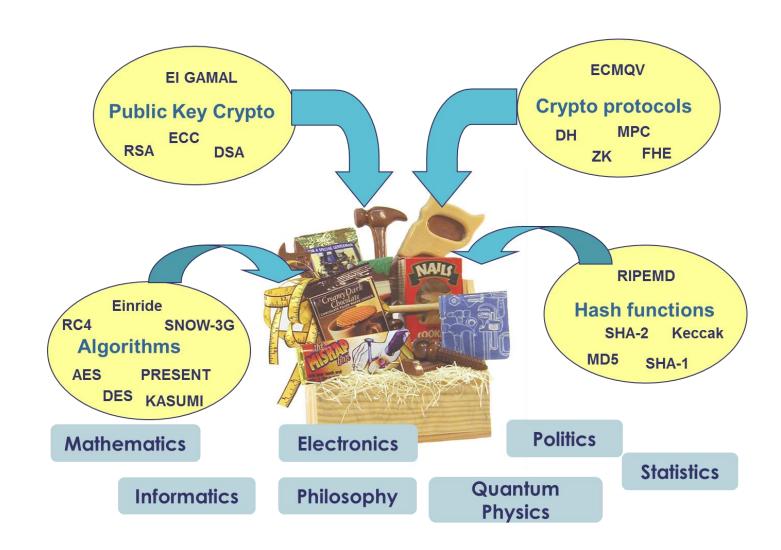


mouse wiggling...

Constructions and relations



The crypto toolbox



Exam

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