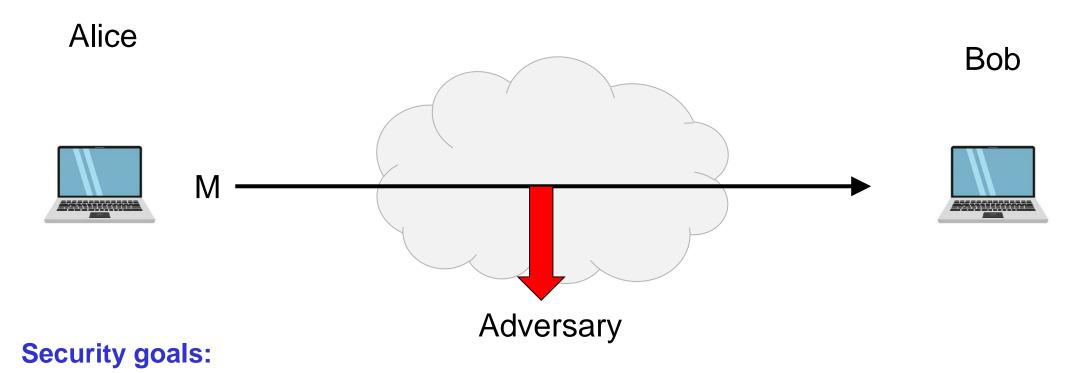
Lecture 14 – Course recap

TEK4500

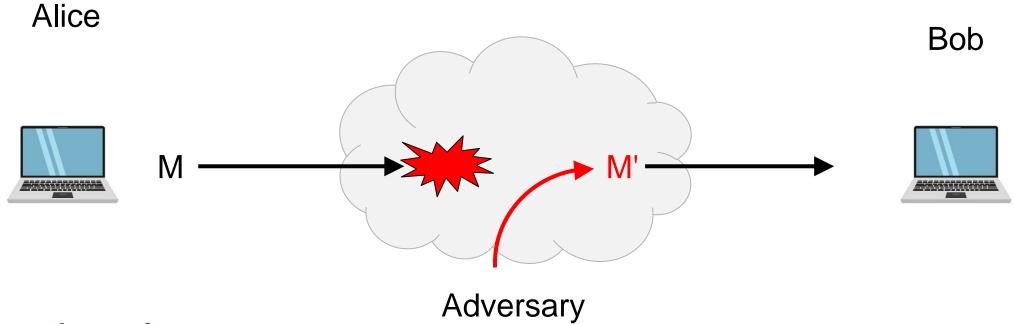
23.11.2022 Håkon Jacobsen <u>hakon.jacobsen@its.uio.no</u>

What is cryptography?



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

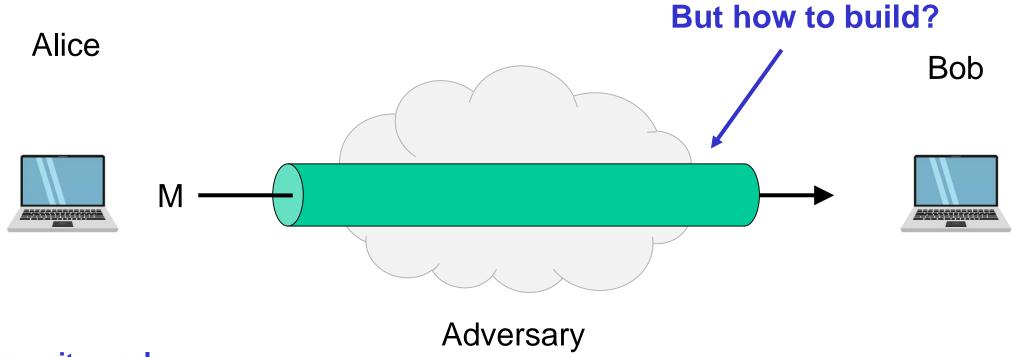
What is cryptography?



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

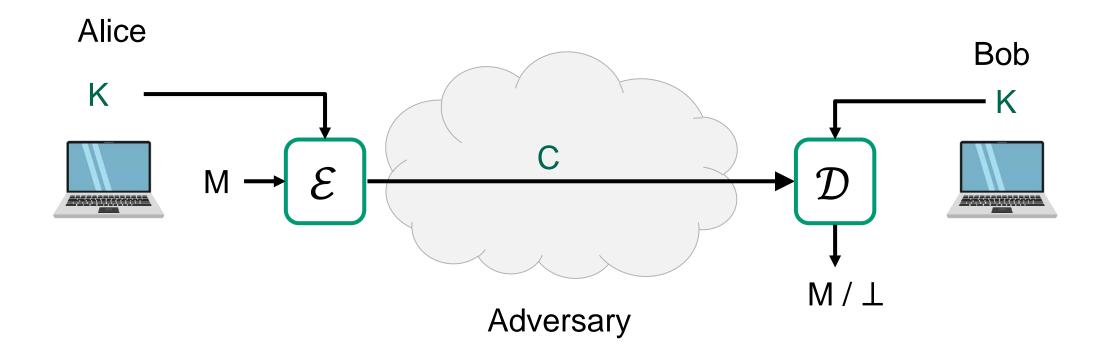
Ideal solution: secure channels



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

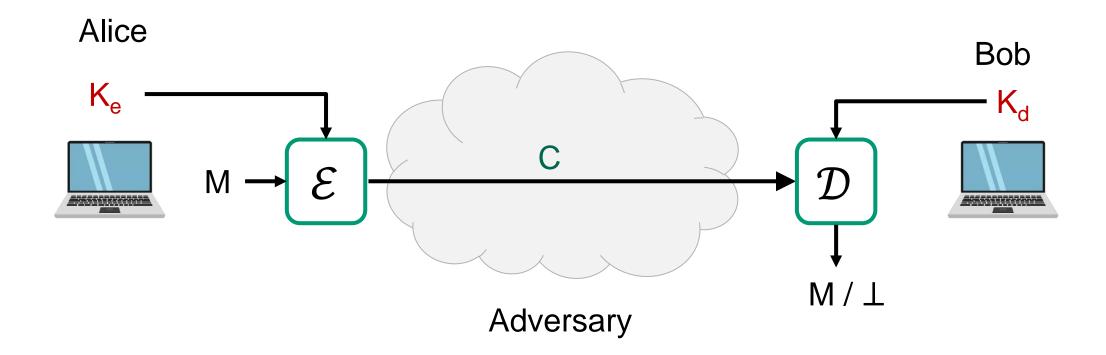


E : encryption algorithm (public)

K : encryption / decryption key (secret)

 \mathcal{D} : decryption algorithm (public)

Creating secure channels: encryption schemes



E : encryption algorithm (public)

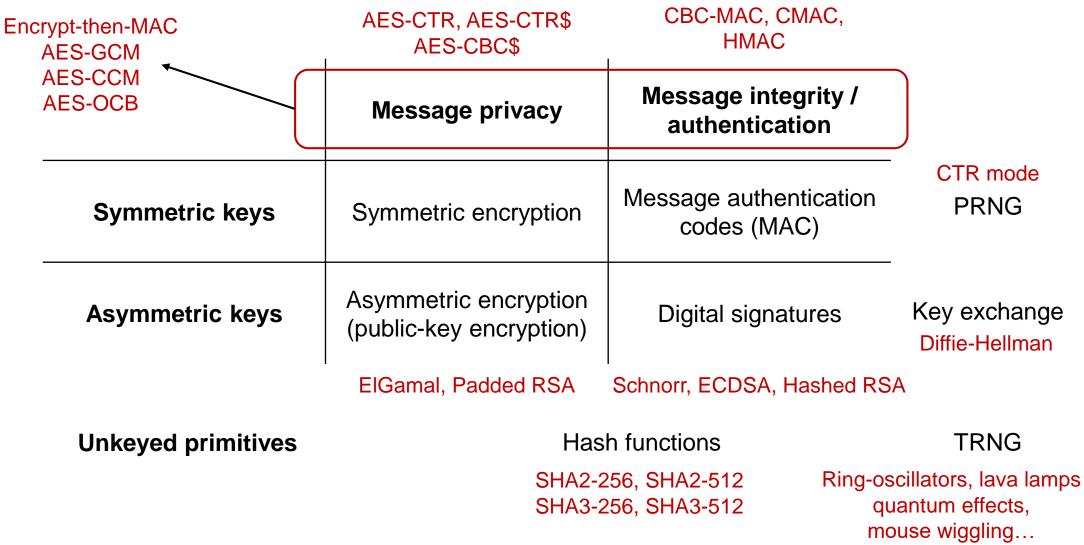
 \mathcal{D} : decryption algorithm (public)

- **K**_e : encryption key (public)
- K_d : decryption key (secret)

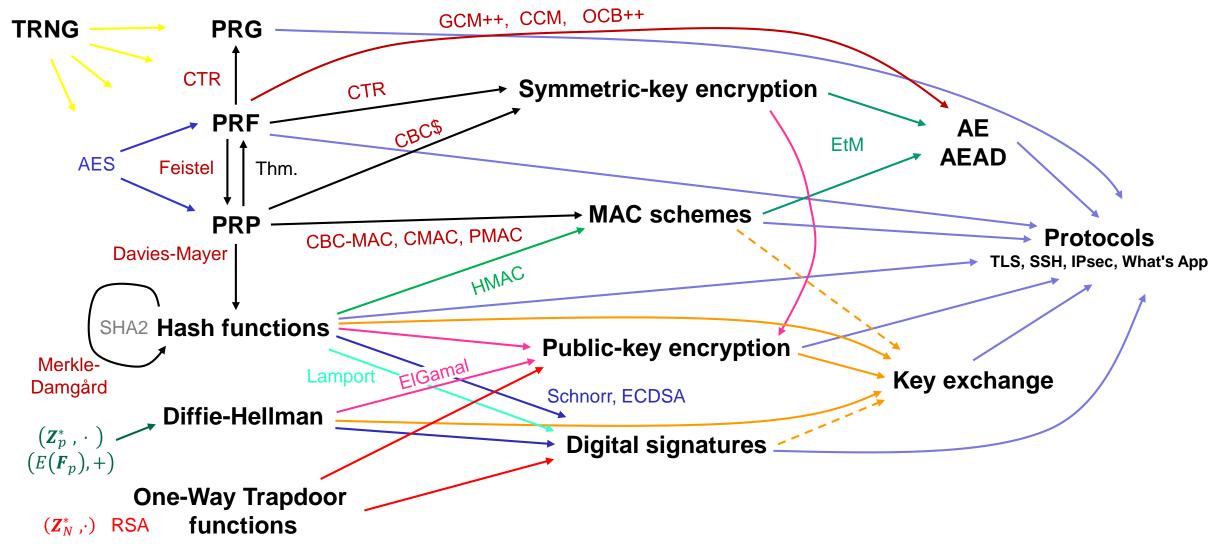
Basic goals of cryptography

AE 👞	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		TRNG
	Collision resistance, one-wayness		Enough min-entropy

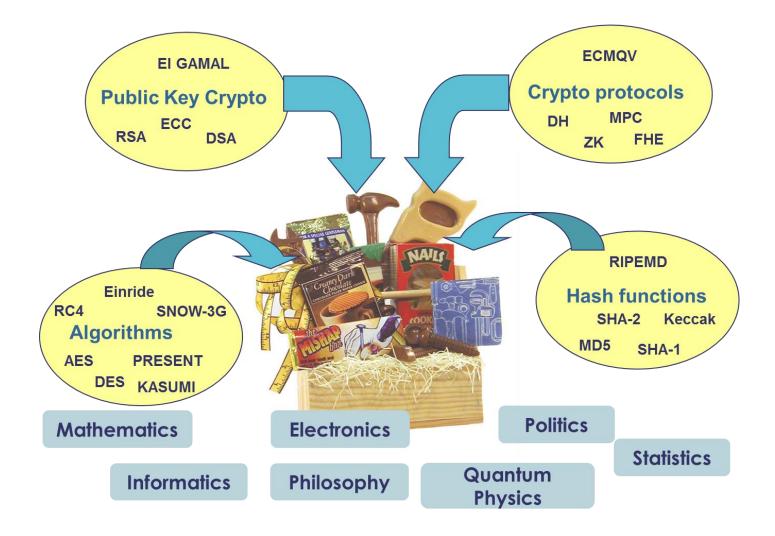
Basic goals of cryptography



Constructions and relations



The crypto toolbox



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