19. Januar 2022

Theoretical and practical aspects of cryptography.

* Cryptographic primitives such as:

Stream ciphers

Block ciphers

Hash functions

* Cryptographic protocols used in practice for securing email communication, web transactions, etc.

**Symmetric Cryptography**

1. Classical ciphers

Caesar cipher

1. Stream ciphers
2. Block ciphers (DES, AES)
3. Differential cryptanalysis

*Cryptanalysis* means how to break a cipher.

1. Cryptographic Boolean functions

Used as building blocks for stream ciphers and block ciphers.

**Asymmetric cryptography**

1. RSA

When you connect your computer to a website with a public key

1. Key exchange protocols
2. Elliptic curves

Mathematical structure

**Derivatives**

1. Hash functions
2. Message authentication codes
3. Key management

**Cryptographic protocols(tentative plan)**

1. Authentication
2. Email security email security
3. IP security
4. Web security
5. System security

**Miscellaneous lectures**

1. Applied mathematics crash course (2 lectures)
2. Selected topics (2 lectures)

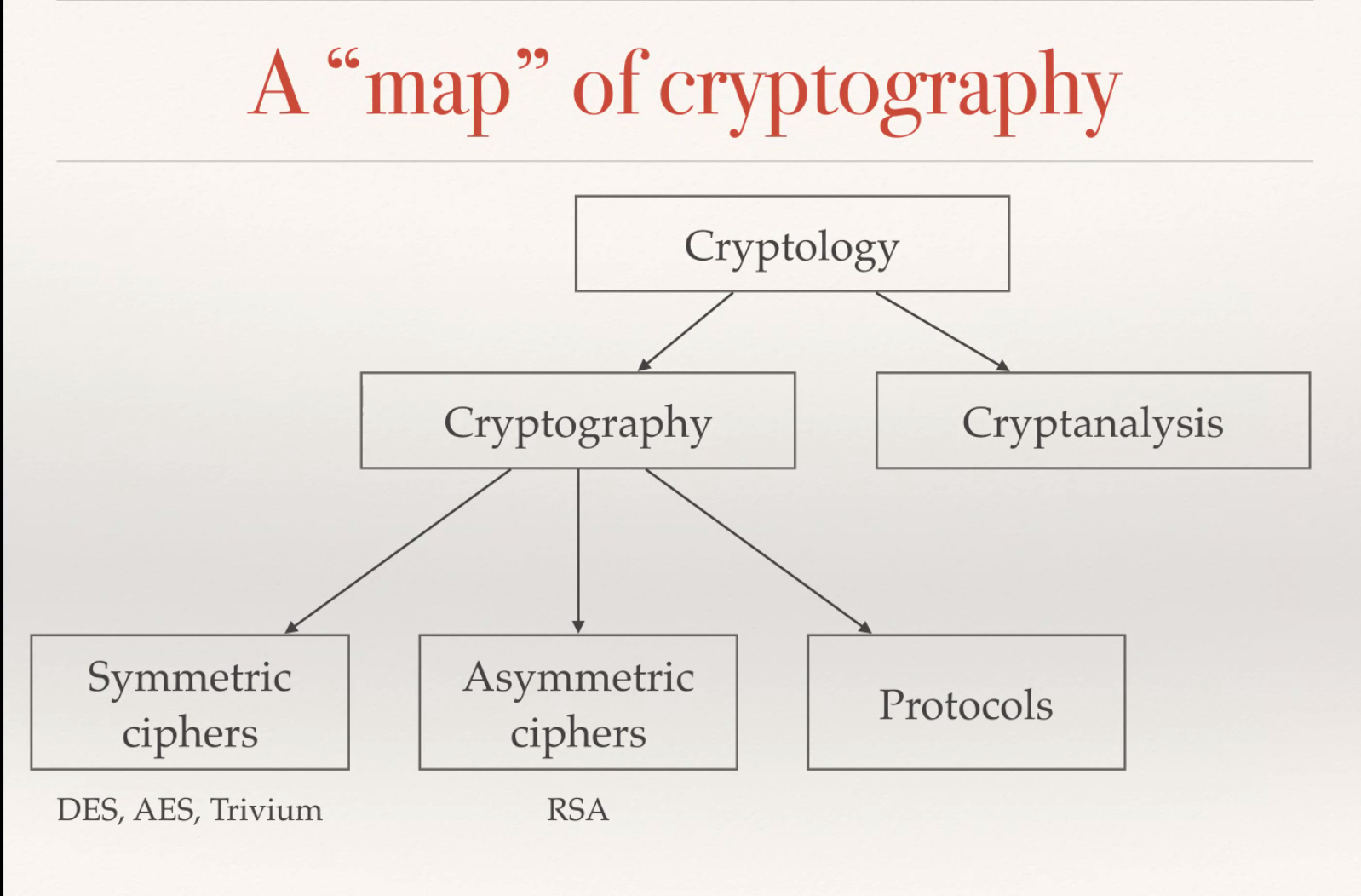
**Cryptography**

Confidentiality, integrity, authentication

Confidentiality: Guarantee privacy

Integrity: Guarantees the “safety” of the message. Message doesn’t get cut. Prevent date from getting modified by an unauthorized person.

Authentication: Guarantee the person communicating with is the one you are communicating with. Verify the identity of the other person



The goal of cryptanalysis is to “break” existing ciphers. The motivation behind it is not necessarily malicious. It can be used to test the security of the system.