Requirements / Goals / Attributes / ...

CIA Triad

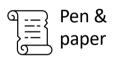
Confidentiality

Integrity

Availability

Authentication

Non-repudiation





Terminology

Cryptology Cryptography **Cryptanalysis Cryptogram**

Attack (§ 6) **Adversary** Corrupted / **Malicious Party**

Defences **Mitigations Countermeasures**



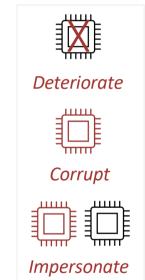
Security



Electronical computation

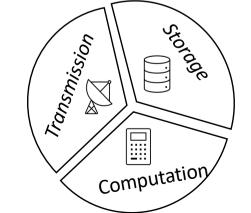


Quantum computation



Mechanical computation

Attacks		
Passive	vs.	Active
Outsider	>	Insider



Secure all!



Alice



Bob

Charlie



Daisy



Oscar / Eve