Lecture 1

# Course Information

## Assignments

* Become available at 10:00 on Wednesday (week n)
* You can ask for advice in tutorials in week n and n+1
* Hand-in deadline: Monday 17:00 in week n+2
* Grades become available by Monday of week n+3

## Other info

* Lecture notes contain information that is not needed for the course, but they give more information regarding the slides.

# Start of the actual lecture

## Administrative details

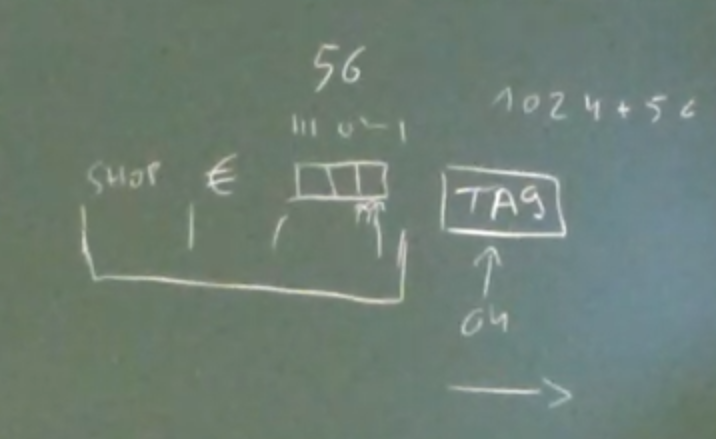
The classical security services

* **Confidentiality** AKA **data privacy**: the assurance that data cannot be viewed by an unauthorised party
* **Data integrity**: the assurance that data has not been modified in an unauthorized party
* **Data origin authentication**: the assurance that a given entity was the original source of received data
* **Entity authentication**: the assurance that a given entity is who they claim to be
* **Non-repudiation**: the assurance that a person cannot deny a previous commitment

### Non-repudiation

* Often used as an argument for public crypto.
* Argued in front of an arbiter or a judge.
* The cryptographic material provides evidence.
* A legal concept, not really a property of a cryptographic system.
* Lawyers may use any security hole in their favor.

### MAC function

* Many people believe that encryption protects integrity, it does **not**.
* In general, this is not true, in some cases it does.
* It protects confidentiality, but not integrity.
* An adversary can modify a bit.
  + Example: Payment device and bank
  + Field 1: Shop
  + Field 2: Euro
  + Field 3: A binary encoded number
    - A bitstring that represents a number.
    - It represents 56 euros
  + The bank will transfer the amount from the bank to your account.
  + Bit flipping adds 1024 to the amount, so it becomes 56 + 1024 instead.
  + So, they add a tag at the end to make sure that the bits in front of the tag are valid. 

### TODO