Department of Information Engineering and Mathematics

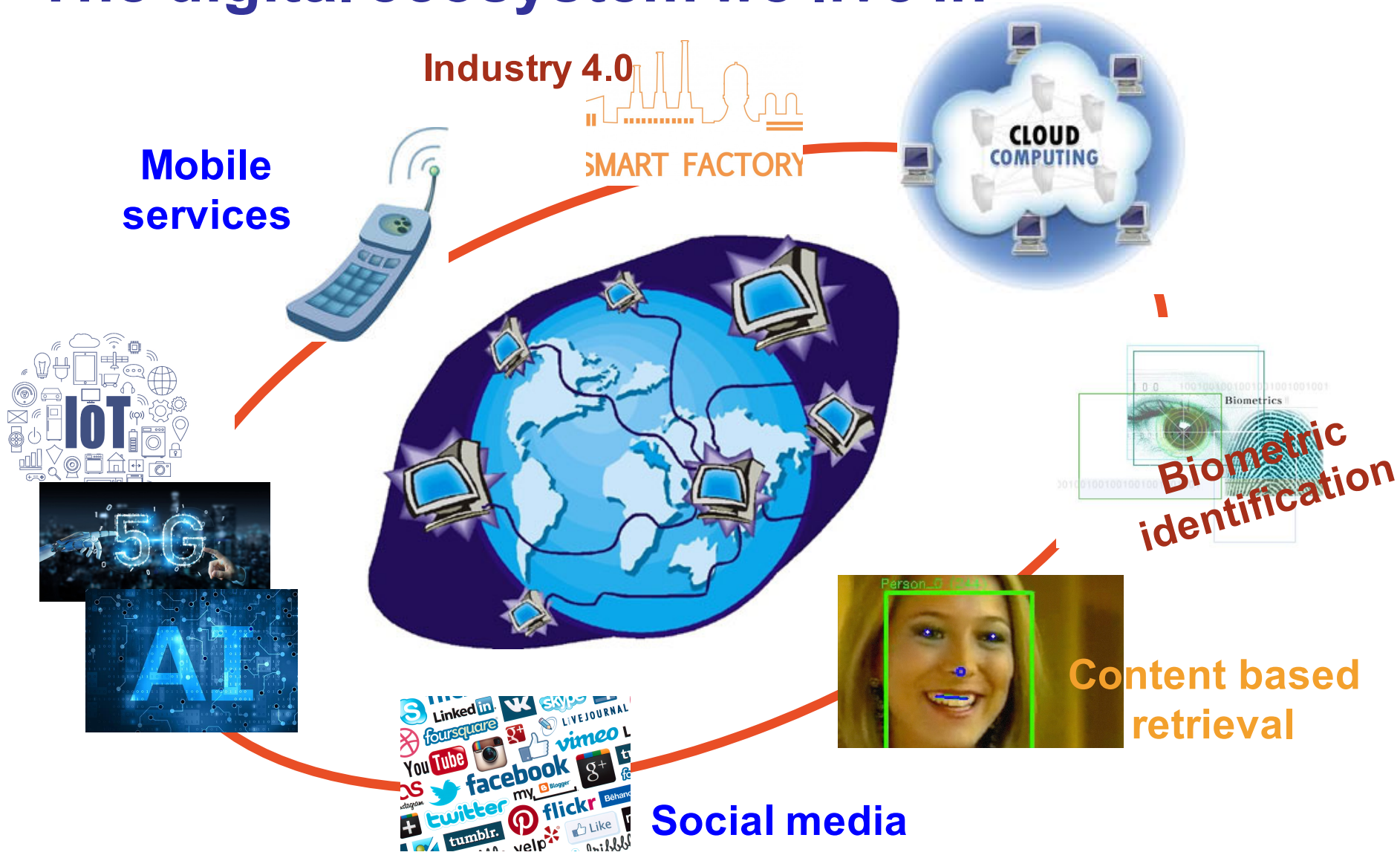
a.a. 2018-2019

Cybersecurity

Mauro Barni

University of Siena

The digital ecosystem we live in



The digital ecosystem we live in

Industry 4.0

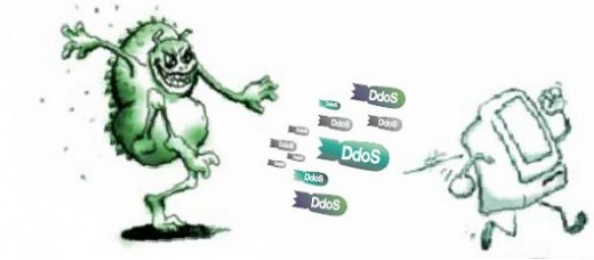
An interconnected digital paradise

-tric
dentification

Content based retrieval

Social media

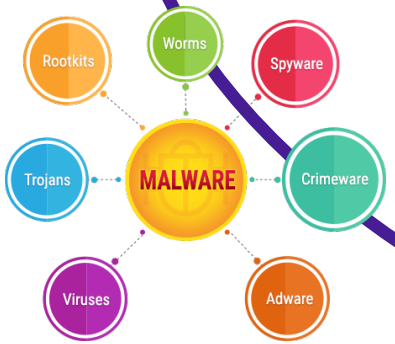
The digital ecosystem we live in



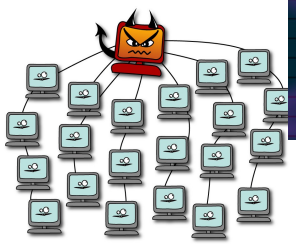
Denial of Service attacks

SPAM

Identity theft



Botnets



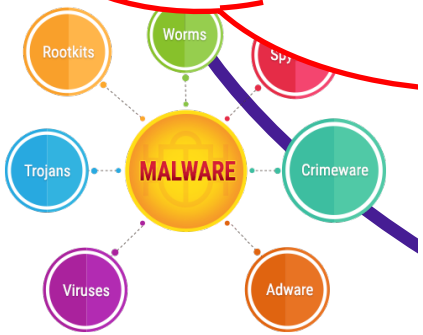
Fake news and fake media

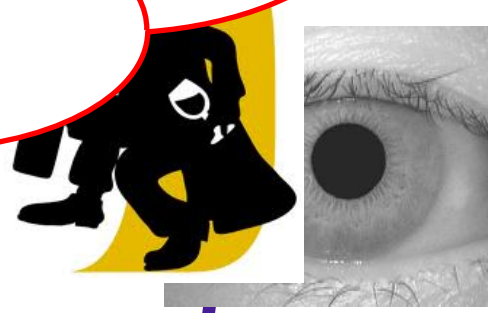
The digital ecosystem we live in

D

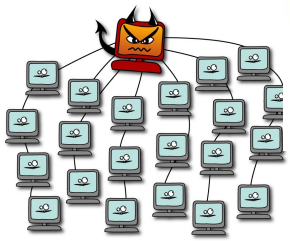
Or a battlefield ?

tity
ft





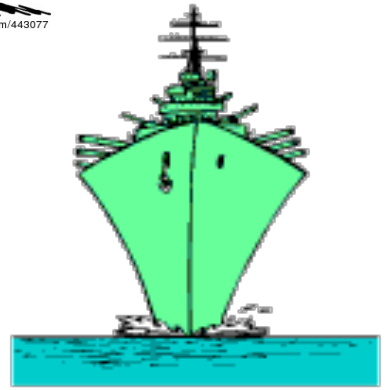
Botnets



media

To the rescue

- Classical Secure-oriented technology
  - Cryptography
  - Applied cryptography
  - Privacy protection
  - System security
  - Biometrics
  - Network-monitoring
  - Intrusion detection and prevention
  - Anonymisation

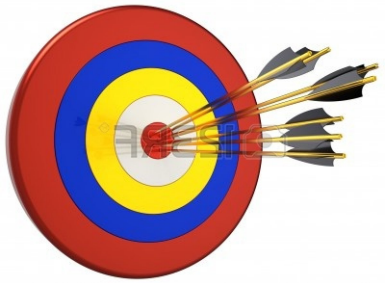


To the rescue (unconventional)

- Differential privacy (also in media)
- Adversarial AI
- Waterrmarking
- Social network forensics
- Multimedia forensics
  - Source identification
  - Integrity verification
- Awareness raising
- New legislation (see GDPR)

All together forming a new discipline referred to as CYBERSECURITY

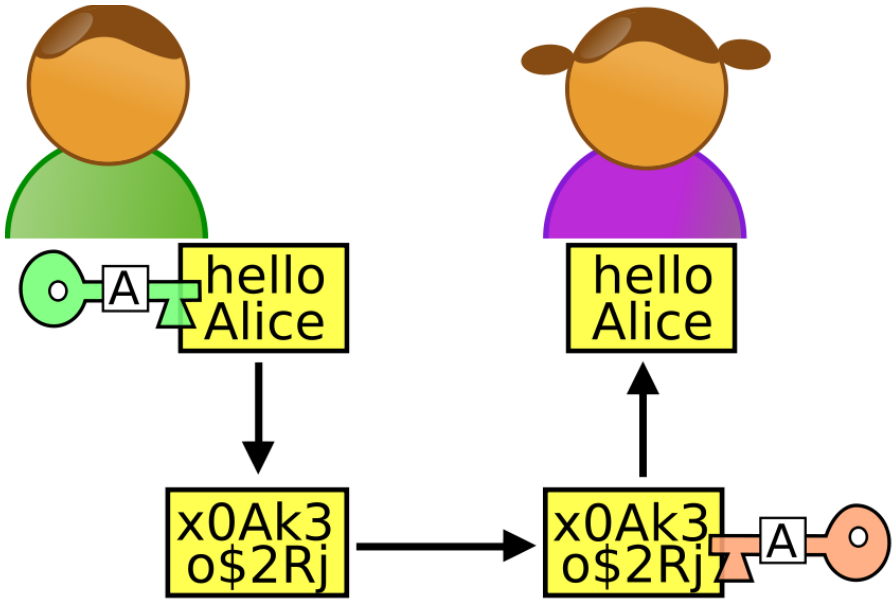
The goal(s) of the course (tentative)

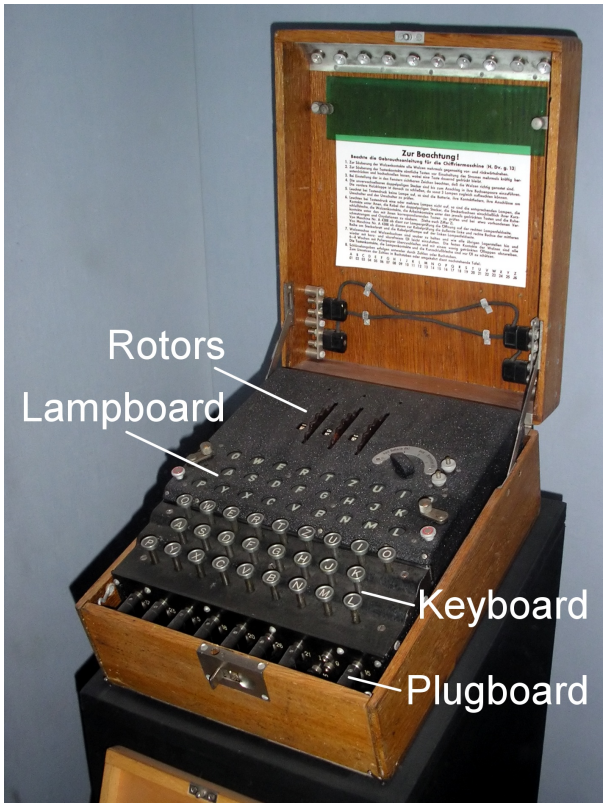


- Overall view of Cybersecurity
- Introduction to basic cryptographic notions
- Beyond crypto
  - user authentication, access control, malware diffusion, DoS …
- Network and wireless network security
  - (hands on)
- Media security
  - data hiding, media forensics, adversarial AI
- Couple theory with practice
  - Lab activity

Cryptography

- The art (nowadays the science) of message obfuscation ...
- and much much more



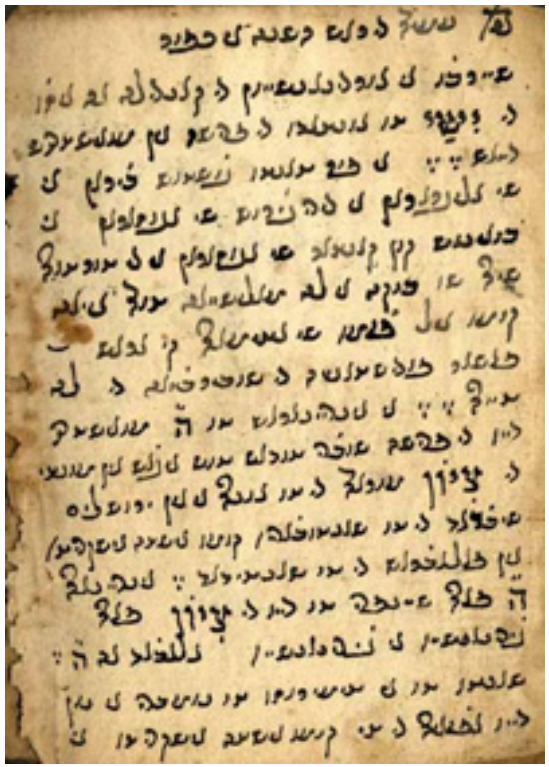


A history as old as the humankind

- **Non-standard hieroglyphs**, 1900 BC
- They were used to hide the meaning of engravings outside graves

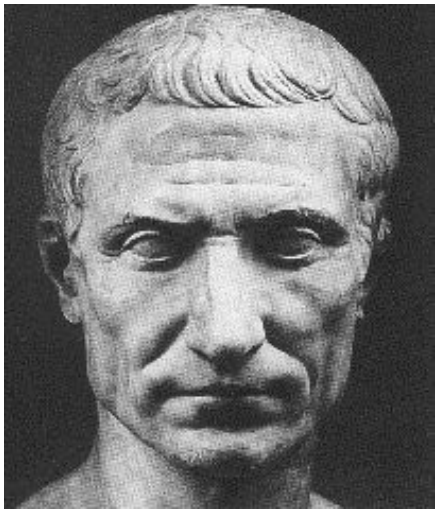
A history as old as the humankind

- **Atbash cipher** (600 BC)
- Used to hide names and places in Jeremiah's book
- Replace first letter of the alphabet with the last, the second with the second-to-the-last and so on
- The name derives from the fact that A -> tav, B -> shin, yielding: ATBSh - ATBASH



A history as old as the humankind

- **Ceasar' cipher**
- According to Svetonio, Ceasar used this cipher to obfuscate military messages:
  - *si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset; quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet. .*
  - Svetonio, *De vita caesarum* 56



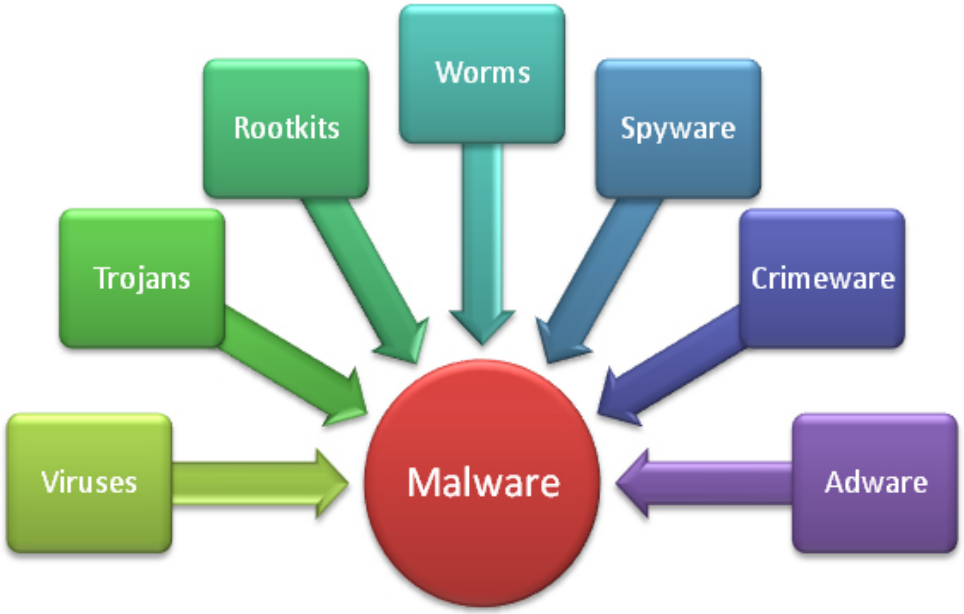
Cryptography in cybersec course

- Basic notions and definitions
- Symmetric cryptography
- Asymmetric cryptography
- Cryptanalysis
- Beyond obfuscation:
  - Authentication
  - Digital signatures
  - Hashes
  - Pseudo-random number generators

Beyond crypto

- User authentication
  - something you know
  - something you possess
  - something you are, something you do
    - biometric-based authentication
- Access control
  - definition and implementation of a proper policy to grant or deny access to a digital asset

Beyond crypto



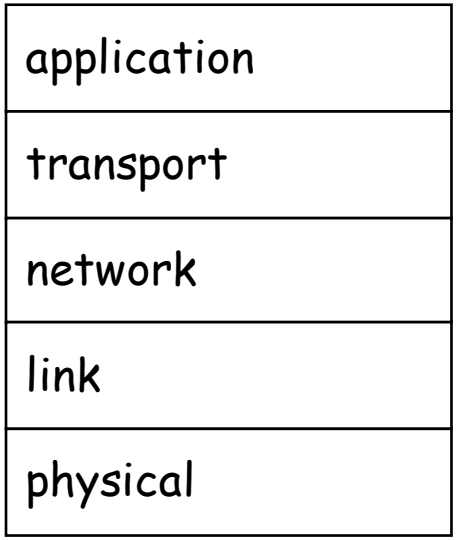
- Malware classification
  - propagation mechanism
    - viruses
    - worms
    - trojans
  - payload
    - corruption
    - theft
    - botnets
- Defenses
  - detection, identification removal

Beyond crypto

- Denial of Service attacks
  - Exhaustion of: bandwidth, system resources, application resources
  - Single source vs distributed DoS attacks
  - Countermeasures
- Intrusion detection
  - host-based ID, network-based ID, hybrid ID
  - honeypots
- Intrusion prevention
  - firewalls

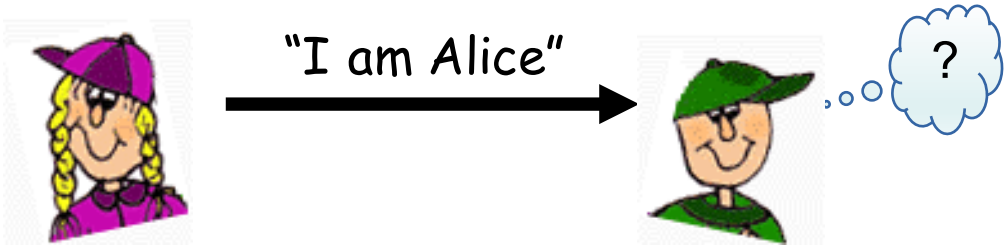
Network security (hands on approach)

- Lab experience led by Prof. Alessandro Andreadis
- Security mechanisms applied at different protocol layers
  - Security at Application layer
  - Security at Transport layer
  - Security at Network layer
  - Security at Link layer



Application Layer Security

- How to achieve end point authentication
  - Goal: Bob wants Alice to "prove" her identity to him

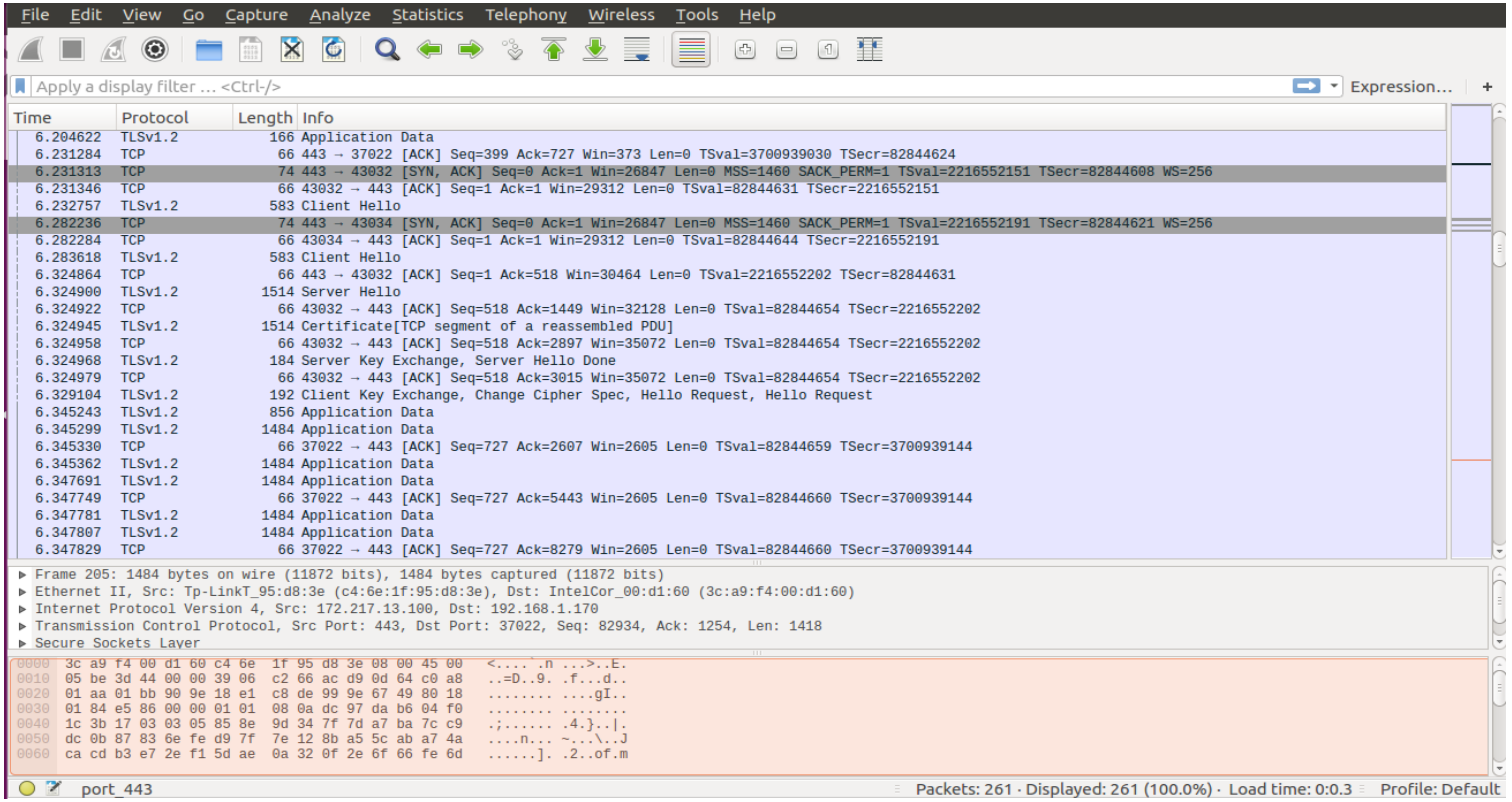


  - Attacks and countermeasures

- How to secure an application: example of combined symmetric and asymmetric criptography
  - Securing e-mails and files

Traffic analyzer and packet sniffing

- Wireshark network protocol analyzer
  - Basics on how to inspect packets
  - Malicious usage and packet sniffing



Transport Layer Security

- Securing TCP connections
  - Most applications run over TCP (http, ftp, facebook…). How does SSL/TLS secure them?

Link Layer Security

- Wireless LANs (WiFi) security: you can better protect your WiFi if you know how to hack it !!!
  - Basics on WEP, WPA, WPA2 and 802.11i
  - How to hack a WiFi: monitoring, attacking, testing and cracking

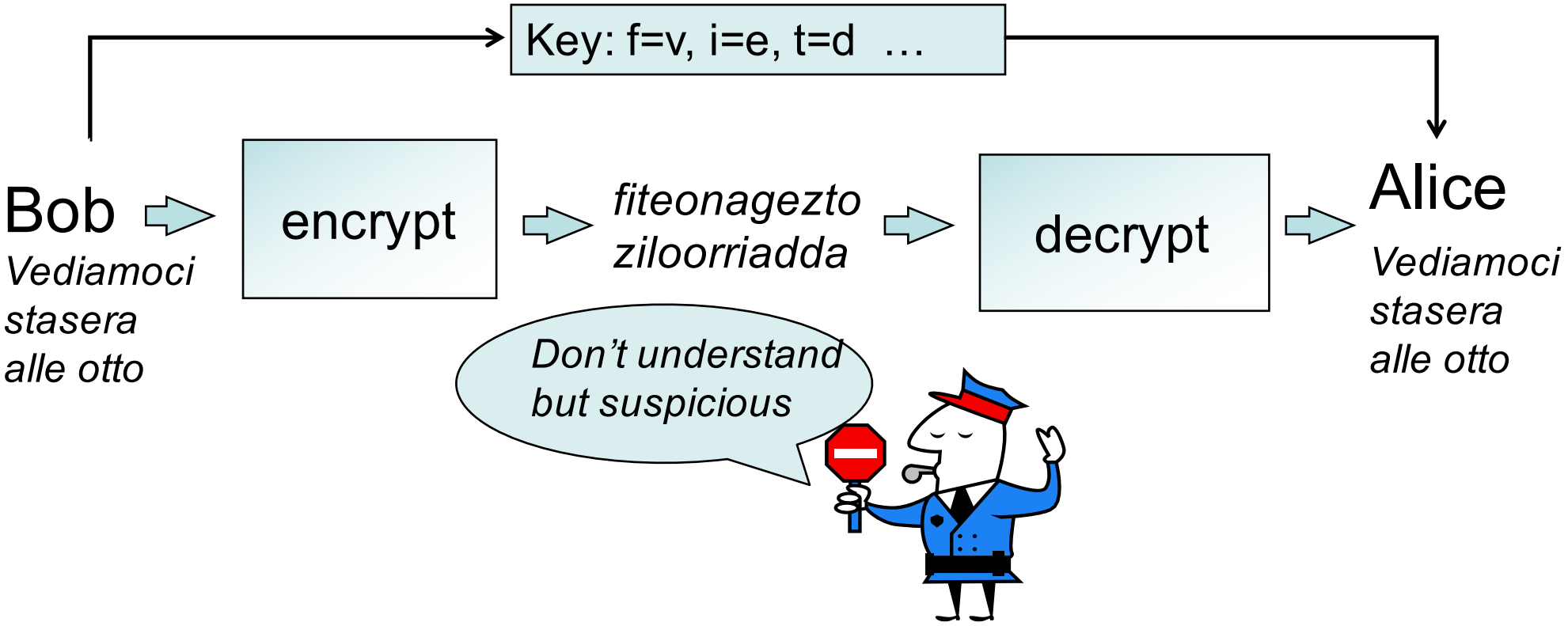
Less conventional yet very hot topics

Steganography

Steganography is the art-science of communicating hiding the existence of the communication

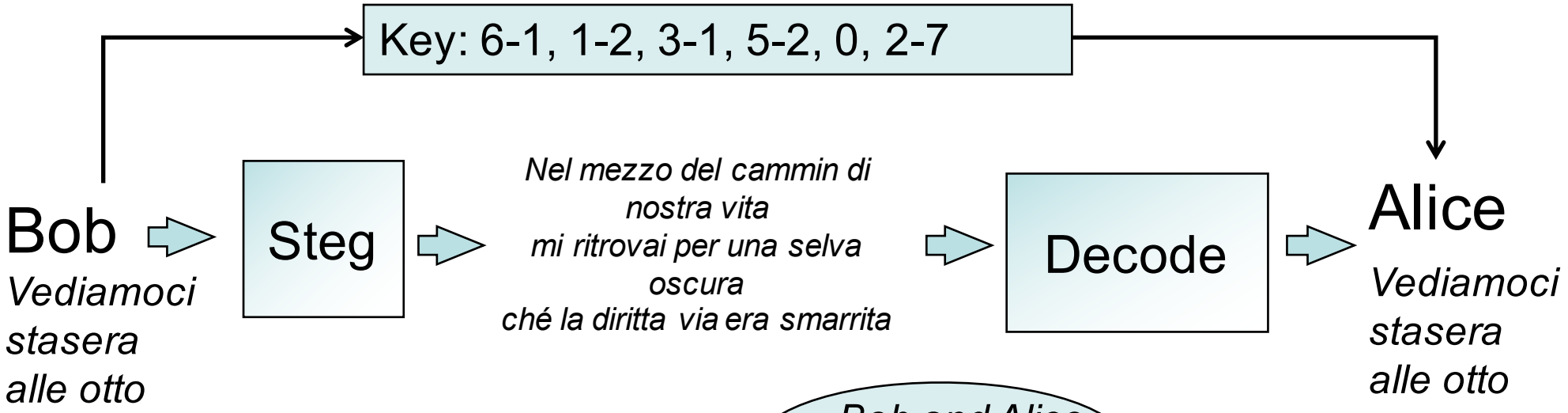
In contrast to cryptography, where the enemy is allowed to intercept and modify messages without being able to violate the security ensured by a cryptosystem, the goal of steganography is *to hide messages inside other harmless messages in a way that does not allow any enemy to even detect the presence of a second secret message*

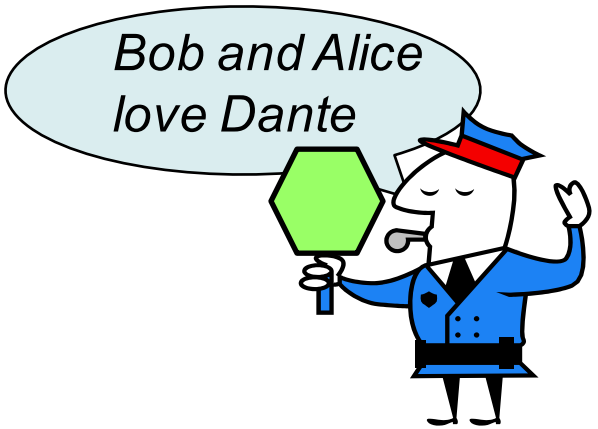
Cryptography



In some cases the very existence of a message is enough to raise a suspect

Steganography





Steganography hides the very presence of the message into an innocuous host

In a more flexible way

"My friend Bob: Until yesterday I was using binoculars for stargazing. Today I decided to try my new telescope. The galaxies in Leo and Ursa Major were unbelievable! Next, I plan to check out some nebulas and then prepare to take a few snapshots of the new comet. Although I am satisfied with the telescope, I think I need to purchase light pollution filters to block the xenon lights from a nearby highway to improve the quality of my pictures. Cheers, Alice."

Take initial letters:
mfbuyiwubfstidttmnttgilaumwuniptcosnatpttafsotncaiaswttitintplpftbtxlfan htitqompca

Filter with p = 3.141592653689793…-> buubdlupnpsspx

Take the preeceding letter in the alphabet: ATTACK TOMORROW

Steganography in CS course

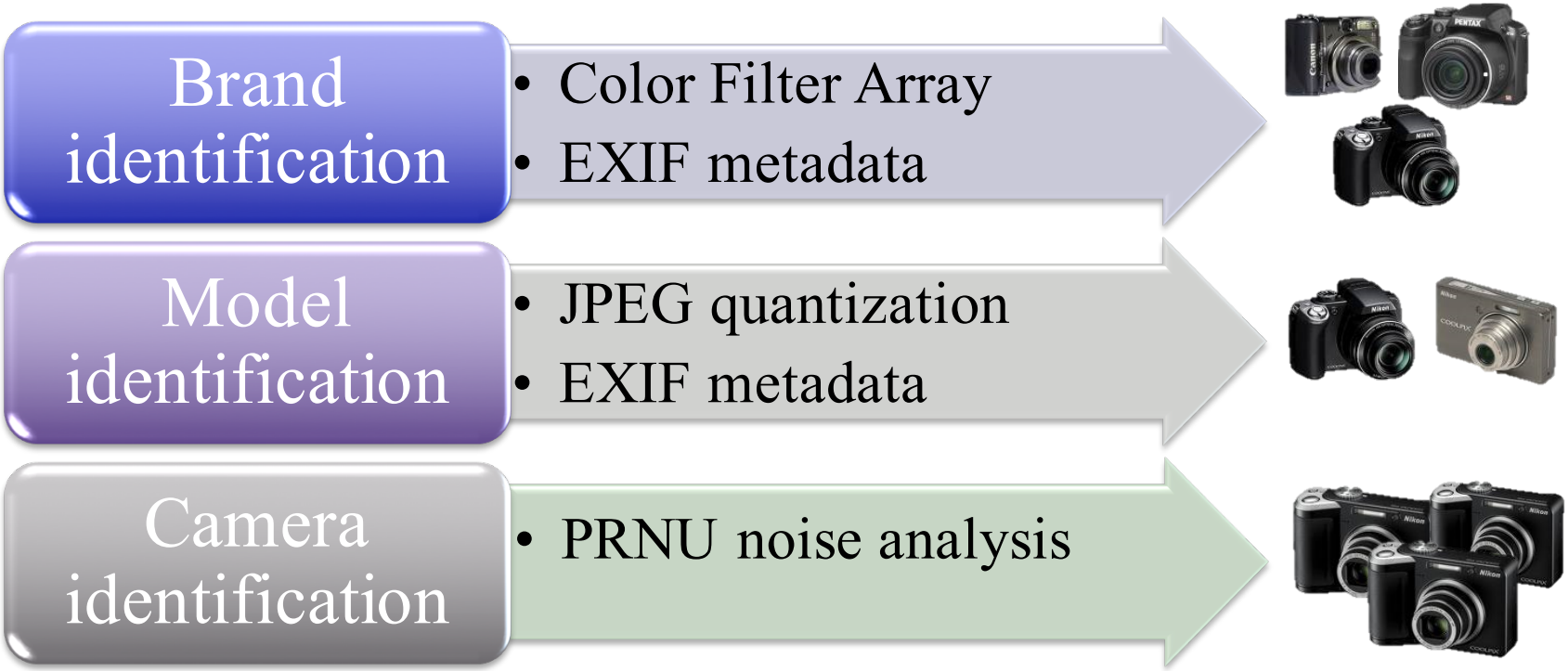
- Basic notions and definitions
- A review of steganographic algorithms
- Steganalysis

Multimedia forensics

- Multimedia forensics gathers information on the history of images, video and audio contents
- Each manipulation leaves peculiar traces that can be exploited to detect its presence
- Provides solutions for:
  - Identifying the source of the media
  - Deciding on the integrity of the media

Source identification

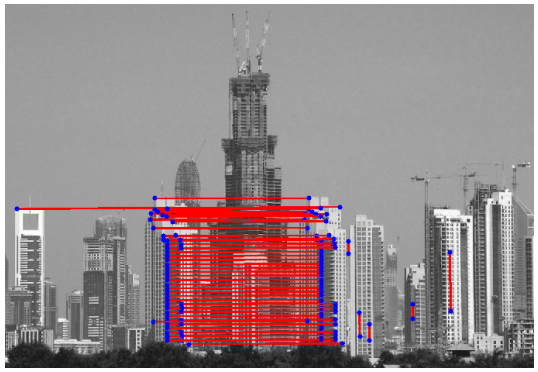
- Recover information on the device that originated the media content (e.g. image)



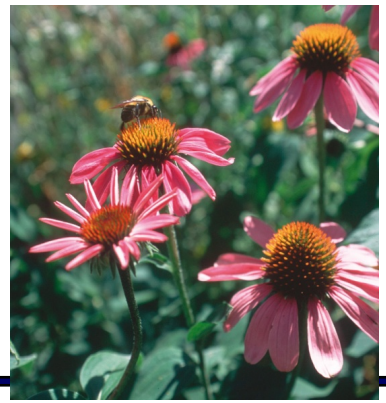
Integrity verification

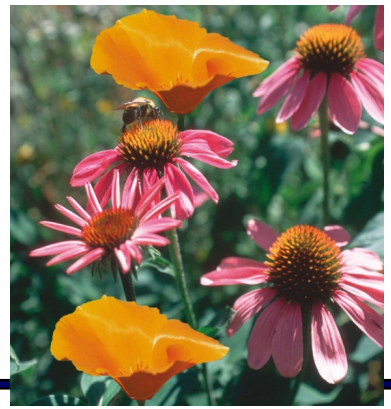
- Determine whether a media (or a part of it) has undergone some processing
  - “innocent” editing tools to improve quality
  - “malicious” manipulations to alter the semantic message
- Look for edited contents

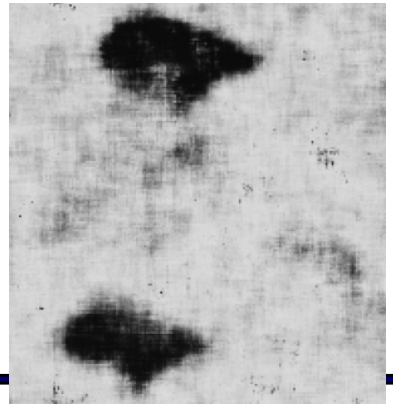
- **Copy-move**: a portion of an image is copied and pasted into the same image



- **Image splicing**: a portion of an image is copied and pasted into another image







Multimedia forensics in CS course

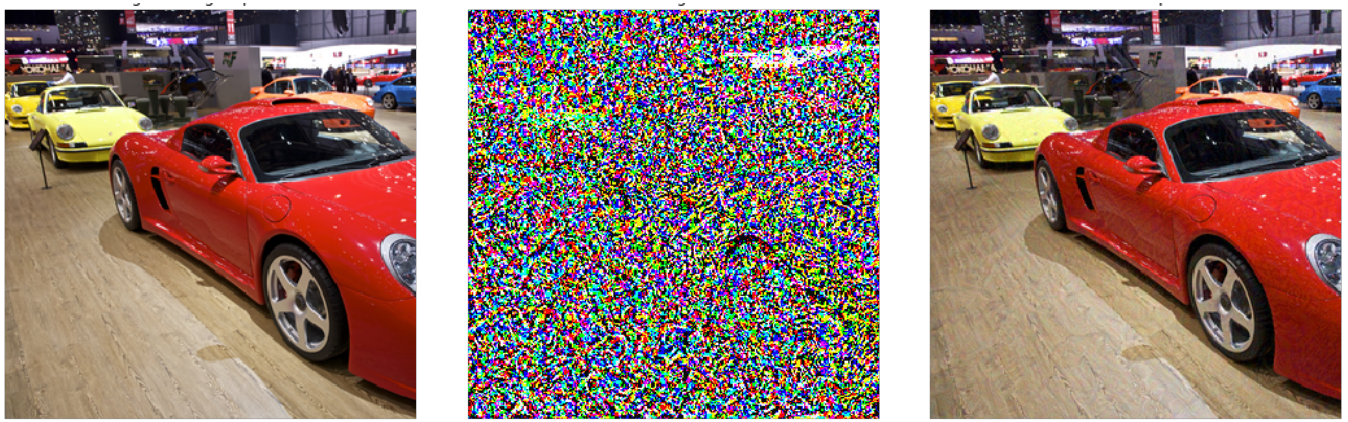
- Basic notions and definitions
- Source identification (PRNU)
- Examples of manipulation/tampering detection
- Focus on images

Machine Learning and Security

- The use of ML techniques (noticeably DL) for security applications has been rapidly increasing
  - Malware detection, Multimedia forensics, Biometric-based authentication, Traffic analysis, Steganalysis, Network intrusion detection, Detection of DoS, Data mining for intelligence applications, Cyberphysical security …
- Little attention has been given to the security of machine learning
  - Yet fooling a ML system turns out to be an easy task

Striking examples

Magnified noise



Classified as a *toaster*

Classified as a *Gibbon*

Striking examples: one pixel attack

Striking examples: not only digital

Security OF Machine Learning

Machine Learning FOR security → **Security OF Machine Learning**

Adversarial machine learning in CS course

- Security is not robustness
- Attacker's perspective
- Defender's perspective
- A joint game-theoretic point of view

Course organization

- Timetable
  - Monday 11.00 – 13.00 (meaning: 11.15– 12.45)
  - Tuesday and Thursday 14.00 – 16.00 (meaning: 14.15 – 15.45)
- Laboratory
  - Network and wireless network security
  - Prof. Alessandro Anedradis, 2-3 weeks in May
- Textbooks
  - Computer Security: principles and practices, 4-th edition. W. Stallings, L. Brown, Pearson
  - Slides: http://clem.dii.unisi.it/~vipp/index.php/teaching/33-multimediasecurity
- Exam: oral exam including discussion on lab activity
- Office hours: Friday afternoon from 14.30 to 16.30
- E-mail: barni@dii.unisi.it

With a not-so-little help from my friends

VIPP group (http://clem.dii.unisi.it/~vipp/)

- 1 Professor
- 1 Adjunct professor (A. Andreadis)
- 2 Post doc researchers
- 1 visiting professor
- 1 PhD student
- 2 visiting phD student

I hope you will enjoy the course