



Cybersecurity 2025

part of Fabrizio d'Amore

6 of 9 ECTS

contents

1. **Cybersecurity, CNS and Web security and privacy** (long and partially sad story)
2. Part of d'Amore (6 ECTS) and part of Querzoni (3 ECTS)
3. Google classroom: **baomarw4**
 - slides (both in advance - tentatively - and in retrospect; they may slightly differ)
4. Website: <https://sites.google.com/diag.uniroma1.it/cybersecurity/>
 - Calendar
 - Textbook
 - Log
 - Classroom

contents (continued)

5. Homeworks
6. Exam
 - Mandatory written test
 - Oral exam optional (grade positive or negative)
 - Partial grade handling (Including people who for any reason have not been able to formalize official enrolment in the master's degree)
 - Reset: after September call
 - Final grade is $(2/3)(d'Amore)+(1/3)(Querzoni)$
7. Organization of the lectures
 - Only in presence
 - **Proposal:** 67.5min + 30min break + 67.5min (Thursday break might be shorter)
8. Master theses
 - Many and demanding

Syllabus 2024

- 1. Information security
 - only d'Amore
- 2. Symmetric encryption
- 3. Data integrity
- 4. Public key encryption
- 5. Digital signatures and PKI
- 6. CSPRNG (Cryptographically Secure Pseudo-Random Number Generators)
- 7. Authentication
- 8. Secret sharing
 - Tentatively 2025 like 2024
 - But Log 2025 is the official reference
- 9. Access control
- 10. Secure protocols (tls, ipsec, ssh)
- 11. Firewalls

information security

everything starts here

CIA requirements

other (non-secondary) requirements

what is a requirement?

safety vs. security