Who am I?

Arnis Paršovs (arnis.parsovs@ut.ee)

MSc in Cyber Security
Tallinn University of Technology

PhD (Computer Science) from the University of Tartu

Applied Cyber Security Group: https://acs.cs.ut.ee/
Denizalp Kapisiz (denizalp.kapisiz@ut.ee)

MSc in Software Engineering
University of Tartu

Junior Lecturer of Software Security

Please contact him on all course-related matters!
Who are you?
This course

- Practical hands-on course, no math

Course timeline:

- [2022-08-27] 1: Randomness, PRNG, One-Time Pad, Stream Cipher
- [2022-09-03] 2: Abstract Syntax Notation One (ASN.1)
- [2022-09-10] 3: Hash functions and HMAC
- [2022-09-17] 4: Block ciphers (AES)
- [2022-09-24] 5: Public Key Cryptography (RSA)
- [2022-10-01] 6: Elliptic Curve Cryptography (ECC)
- [2022-10-08] 7: Public key certificates (X.509)
- [2022-10-15] 8: Revocation checking (CRL/OCSP)
- [2022-10-22] 9: Digital signatures (XAdES)
- [2022-10-29] 10: Smart cards (EstEID)
- [2022-11-05] 11: Smart cards (JavaCard)
- [2022-11-26] 14: The Onion Router (Tor)
- [2022-12-03] 15: Bitcoin
- [2022-12-09] Online exam

6 ECTS – 26*6=156 hours (10 hours weekly)
Grading

• Homework every week

• Homework assignments give maximum 70% of the final grade

• Deadlines are strict!
  • Homework deadline – Saturday 23:59:59
  • Late submissions get 50% penalty
  • Homework submitted later than 1 week after the deadline is not accepted!

• Exam gives another 30% of the final grade
  • Should be easy if you follow the lectures
Homework submissions

• Homework tasks must be implemented in Python 3
  • Test environment: Ubuntu 22.04, Python 10.x
  • Python packages from Ubuntu package repository (not pip)

• Create a private Bitbucket repository and grant me ‘read’ privileges:
  https://bitbucket.org/appcrypto/2022_fall/src/master/setup/

• Add your repository to the course grading page at
  https://cybersec.ee/appcrypto2022_fall/

• Homework templates will be published at the course repository:
  https://bitbucket.org/appcrypto/2022_fall/

• Feedback will be given using code comment feature

• Teaching assistance over e-mail not available
  • Practice session: Fridays 10:15-12:00, via Zoom
  • Slack channel

• Do not collaborate or look at the homework solutions of others!
Academic fraud

• It is academic fraud to collaborate with other people on work that is required to be completed individually.

• The homework tasks in this course are required to be completed individually!

• You can help your peers to learn by explaining general concepts, but don’t provide them implementation details or your own work!
  
  • If you don’t see the borders – work alone.

• Copying code samples from internet resources (e.g., stackoverflow.com) may be considered plagiarism:
  
  – the most basic building blocks may be OK
  – combination (composition) of building blocks is NOT OK
  • If you don’t see the borders – limit yourself to Python API documentation.