MTAT.07.017
Applied Cryptography

Introduction

University of Tartu

Fall 2021
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/
Teaching Assistant

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?

- MSc (Computer Sci.) - 4
- PhD (Computer Sci.) - 3
- MSc (Software Eng.) - 3
- MSc (Cyber Sec.) - 2
- BSc (Computer Sci.) - 2
- PhD Chemistry - 1
- PhD (Computer Sci.) - 3
- MSc (Software Eng.) - 3
This course

- Learning by implementing, no proofs – just intuition

Course timeline:

- [2021-08-28] 1: Randomness, PRNG, One-Time Pad, Stream Cipher
- [2021-09-04] 2: Abstract Syntax Notation One (ASN.1)
- [2021-09-11] 3: Hash functions and HMAC
- [2021-09-18] 4: Block ciphers (AES)
- [2021-09-25] 5: Public Key Cryptography (RSA)
- [2021-10-02] 6: Elliptic Curve Cryptography (ECC)
- [2021-10-09] 7: Public key certificates (X.509)
- [2021-10-16] 8: Revocation checking (CRL/OCSP)
- [2021-10-23] 9: Digital signatures (XAdES)
- [2021-10-30] 10: Smart cards (EstEID)
- [2021-11-06] 11: Smart cards (JavaCard)
- [2021-12-04] 14: The Onion Router (Tor)
- [2021-12-11] 15: Bitcoin
- [2021-12-16] 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 20.04, Python 3.8.x
  • Python packages from Ubuntu package repository (not pip)

• Create a private Bitbucket repository and grant me ‘read’ privileges: https://bitbucket.org/appcrypto/2021_fall/src/master/setup/

• Add your repository to the course grading page at https://cybersec.ee/appcrypto2021_fall/

• Homework templates will be published at the course repository: https://bitbucket.org/appcrypto/2021_fall/

• Feedback will be given using code comment feature

• Teaching assistance over e-mail not available
  • Practice session: Thursdays 14:15-16:00, via Zoom

• Do not 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 and submitted individually.

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

• You can help your peers to learn by explaining concepts, but don’t provide them with answers 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.