ITC8240: Cryptography

Lecturers/Instructors:

Ahto Buldas ahto dot buldas at taltech dot ee
Aleksandr Lenin aleksandr dot lenin at taltech dot ee

Course webpage:

https://courses.cs.ttu.ee/pages/ITC8240_Cryptography#Course_information

Topics

- Classical ciphers and their cryptanalysis
- Theory of unbreakable ciphers (Shannon’s theory and implications)
- Mini-course in Group Theory
- Public key cryptography (RSA, ElGamal, etc)
- Cryptographic protocols (key establishment, authentication, zero-knowledge proofs)
- Introduction to quantum computation and post-quantum cryptography

Grades

- 2 written tests
- 2-3 homeworks (before the written tests)
- grade = arithmetic mean of the grades of the written tests
- exams: like tests, possibility to improve the grades of both written tests (or just one of them)

Schedule

- **Lectures**: on Thursday 16:00-17:30 ICO-316 (start: Sep 10)
- **Practice hours**: on Friday 12:00-15:30 (start: Sep 11) remotely (Moodle’s virtual classroom)

Prerequisites

Students who:

- are **NOT** cyber security students specialized in crypto, **AND**
- must take this crypto course (ITC 8240)

must do the **math test** on **Friday, Sep 4 remotely (as homework)**:

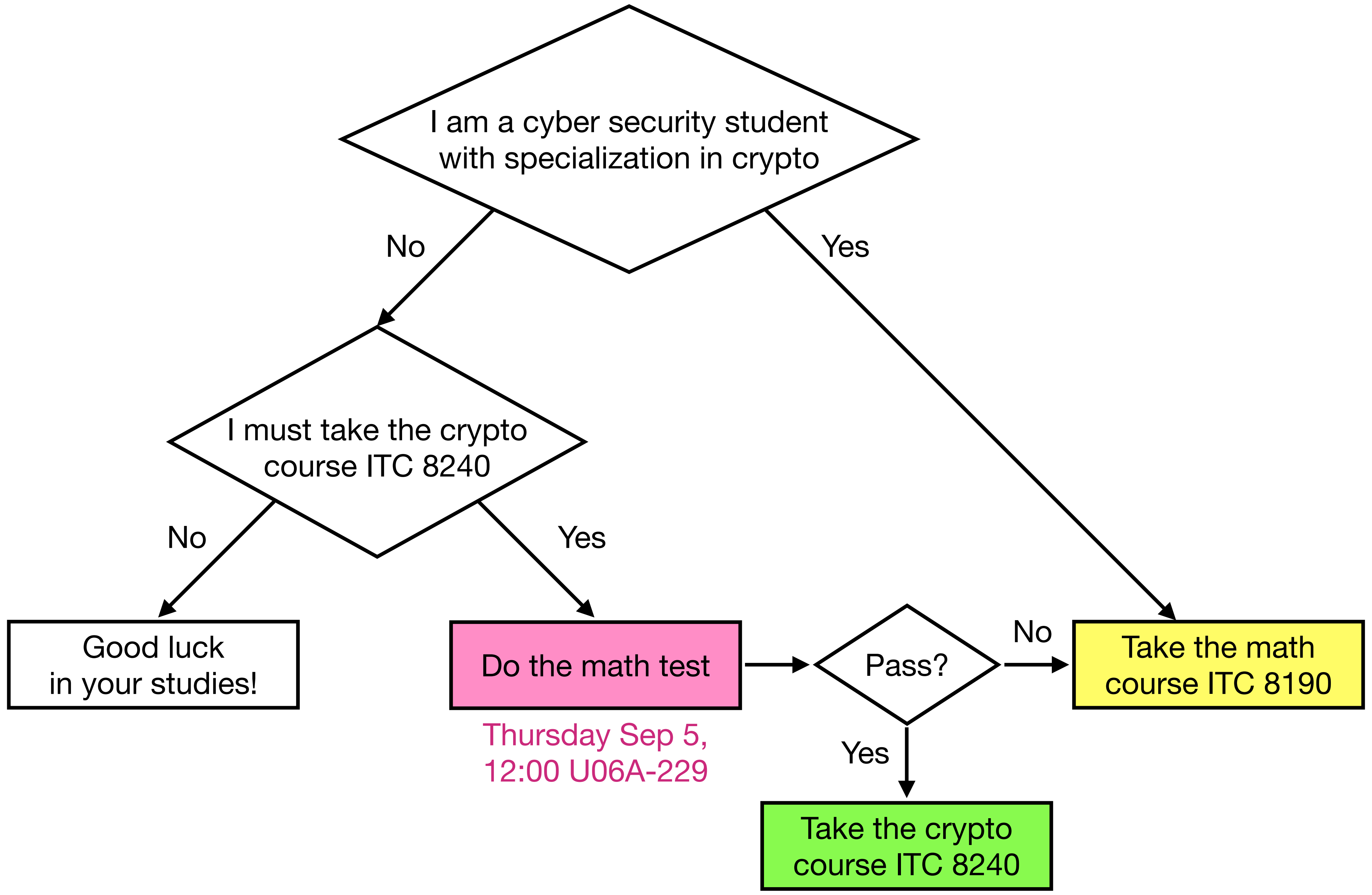
10:00— tests available at course webpage:

https://courses.cs.ttu.ee/pages/ITC8240_Cryptography#Course_information

16:00— last time to send solutions to:

aleksandr dot lenin at taltech dot ee

- passed: take the crypto course (ITC 8240)
- failed: take the math course (ITC 8190)



I am a cyber security student with specialization in crypto
No
Yes
I must take the crypto course ITC 8240
No
Yes
Good luck in your studies!
Do the math test
Pass?
No
Take the math course ITC 8190
Yes
Take the crypto course ITC 8240

Thursday Sep 5, 12:00 U06A-229