Blekinge Institute of Technology
Department of Computer Science

Revision: 1
Reg.no: BTH-4.1.14-0472-2022

COURSE SYLLABUS

Tillämpad kryptografi
Applied Cryptography
5 credits (5 högskolepoäng)

Course code: DV2616
Main field of study: Computer Science, Software Engineering
Disciplinary domain: Technology
Education level: Second cycle
Specialization: A1N - Second cycle, has only first cycle course/s as entry requirements

Language of instruction: English
Applies from: 2022-08-29
Approved: 2022-03-01

1. Decision
This course is established by Dean 2021-11-10. The course syllabus is approved by Head of Department of Computer Science 2022-03-01 and applies from 2022-08-29.

2. Entry requirements
Admission to the course requires at least 120 credits, of which at least 90 credits in a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by,for example, a work certificate from an employer).

3. Objective and content

3.1 Objective
The main objective of this course is for students to learn how to use cryptographic algorithms and protocols to protect data in transit and at rest from unwanted interference. Participants in this course will gain knowledge that helps them enhance the security of applications and services that are used and/or developed in their organization.

3.2 Content
The students will be introduced to fundamental security mechanisms such as encryption, digital signature, integrity, authentication and authorization. Furthermore, the course will include showcases of how these fundamental mechanisms can be combined to implement industry standard security services such as IP security (IPsec) and secure web communication (TLS/SSL).
The course comprises the following:

- Introduction to cryptography
- Quick review of programming languages used in the course
- Using programming frameworks to implement security mechanisms/services
- Distribution and management of encryption keys with digital certificates
- Fundamentals of IP security (IPsec)
- Fundamentals of web communication (TLS/SSL)
- Security for cloud-based storage

4. Learning outcomes
The following learning outcomes are examined in the course:

4.1 Knowledge and understanding
On completion of the course, the student will be able to:
- Explain the type of threats that can be mitigated by applied cryptography and the types that cryptography cannot address
- Explain how fundamental security mechanisms and services work

4.2 Competence and skills
On completion of the course, the student will be able to:

- Implement fundamental security mechanisms using security frameworks introduced during the course
- Manage encryption keys and digital certificates
- Be able to configure and operate a Linux-based IPsec virtual private network (VPN)
- Be able to trace and diagnose IPsec and TLS/SSL connection establishment

4.3 Judgement and approach

On completion of the course, the student will be able to:

- Determine the pros and cons of specific security frameworks based on their feature list
- Determine the security mechanisms required for implementing a specific security service.

5. Learning activities

The teaching is organised around online lectures, pre-recorded videos, together with written material, literature, and research literature. Throughout the course, communication, feedback, and discussions with teachers and fellow participants will take place through email and the course's online learning platform.

6. Assessment and grading

Modes of examinations of the course

Code	Module	Credits	Grade
2230	Written assignment	5 credits	GU

The course will be graded G Pass, UX Fail, supplementation required, U Fail.

The information before a course occasion states the assessment criteria and make explicit in which modes of examination that the learning outcomes are assessed.

An examiner can, after consulting the Disability Advisor at BTH, decide on a customized examination form for a student with a long-term disability to be provided with an examination equivalent to one given to a student who is not disabled.

7. Course evaluation

The course evaluation should be carried out in line with BTH:s course evaluation template and process.

8. Restrictions regarding degree

The course can form part of a degree but not together with another course the content of which completely or partly corresponds with the contents of this course.

9. Course literature and other materials of instruction

The teaching is organised around online lectures, pre-recorded videos, together with written material, literature, and research literature. Throughout the course, communication, feedback, and discussions with teachers and fellow participants will take place through email and the course's online learning platform.