Elective course: Programming for security

About the course

Subject	Datalogi / Informatik
Activitytype	master course
Teaching language	English
Registration	Tilmelding sker via stads selvbetjening indenfor annonceret tilmeldingsperiode, som du kan se på Studieadministrationens hjemmeside Når du tilmelder dig kurset, skal du være opmærksom på, om der er sammenfald i tidspunktet for kursusafholdelse og eksamen med andre kurser, du har valgt. Uddannelsesplanlægningen tager udgangspunkt i, at det er muligt at gennemføre et anbefalet studieforløb uden overlap. Men omkring valgfrie elementer og studieplaner som går ud over de anbefalede studieforløb, kan der forekomme overlap, alt efter hvilke kurser du vælger. Registration through stads selvbetjeningwithin the announced registration period, as you can see on the Studyadministration homepage. When registering for courses, please be aware of the potential conflicts between courses or exam dates on courses. The planning of course activities at Roskilde University is based on the recommended study programs which do not overlap. However, if you choose optional courses and/or study plans that goes beyond the recommended study programs, an overlap of lectures or exam dates may occur depending on which courses you choose.
Detailed description of content	The aim of the course is for the students to acquire: • Knowledge of applied cryptography, including implementation of algorithms for symmetric and asymmetric encryption, cryptographic hashing, generation of signatures and certificates, and protocols for authentication. • Knowledge of challenges in applied cryptography, including initialization, randomization, padding, block chaining, and key generation and re-use. • Knowledge of challenges in security engineering, including patterns, architectures and testing. • Ability to organize and implement a small security-related software application. • Ability to evaluate trade-offs in a practical context, including choice of algorithms and protocols. Students will be working with programming in Java. JCA (Java Cryptographic Architecture) will be used to develop small and medium sized programs. Students will develop an application where security is a central design goal, for example an encrypted chat-service, a service that encrypts files on the harddisk, or a secure, distributed calendar. The exam is based on a written assignment. The written assignment is a Java program developed by the students, including documentation, that implements a service, chosen by the students, and which involves encryption or other cryptographic tools. It is required that students are familiar with programming. The level required corresponds to a bachelor's degree in computer science.
Expected work effort (ects-declaration)	The course will have a total workload of 135 hours with 40 hours of lectures and exercises, 70 hours of preparation over an 11 week course period and 25 hours for the exam and preparation before the course
Course material and reading list	Course material will be made available via the course Moodle page. The textbook for the course will be: David Hook and Jon Eaves. Java Cryptography: Tools and Techniques. 371 pages. Leanpub, 2010-2019. URL: leanpub.com/javacryptotoolsandtech.
Evaluation- and feedback forms	There will be feedback on exercises which are set during the course. An evaluation will take place at the end of the course.
Administration of exams	IMT Studyadministration (imt-studyadministration@ruc.dk)
The responsible course lecturer	Niels Jørgensen (nielsj@ruc.dk)

Type of examination	Individual oral examination based on a set assignment. The examination is conducted as a dialogue. During the examination, questions can be asked regarding the entire syllabus. The written product must be between 4,800 - 48,000 characters in length, including spaces. The size specifications include the cover, table of contents, bibliography, figures and other illustrations, but exclude any appendices. Time allowed for examination including time used for assessment 20 minutes. The assessment is an overall assessment of the written product(s) and a subsequent oral examination. Permitted support and preparation materials during the examination: All. Assessment: 7-point grading scale. Moderation: Internal co-assessor.
ECTS	5
Learning outcomes and assessment criteria	• Knowledge and understanding of a specific subject area in computer science • Knowledge and understanding of the area's techniques for designing and constructing software systems that meet specific requirements • Knowledge and understanding of the general principles behind the subject area's theory, methods and technological solutions. Skills in electing and applying appropriate methods and techniques from the subject area in order to analyse, design and construct reliable and user-friendly software systems • Competences in being able to work on computer science-related issues, both independently and in teams • Competences in being able to become proficient in new approaches to the subject area in a critical and systematic way and thereby independently take responsibility for one's own professional development.
Overall content	With an elective course, the student has the opportunity to specialise in a specific subject area where the student acquires knowledge, skills and competences in order to translate theories, methods and solutions ideas into their own practice in relation to software development. Examples of elective courses: Robotics, AI, internet technologies, programming language, parallel calculation, mobile computers, etc.The specific contents are listed on study.ruc.dk.
Prerequisites for participation	Currently no data from curriculum.
Prerequisites for participation in the exam	Currently no data from curriculum.
Teaching and working methods	Normal class instruction, i.e. a mix of lecturer presentations, student presentations and practical work on specific tasks. Lecture with exercises. Is stated in the description on study.ruc.dk.
Type of course	Elective course
Exam code(s)	Exam code(s) : U41387

Course days:

Hold: 1

Informatics: Programming for Security (PSec)

Time	10-02-2020 08:15 til 10-02-2020 12:00
Location	10.1-025 - teorirum (32)

Teacher Niels Jørgensen (nielsj@ruc.dk)

Informatics: Programming for Security (PSec)

Time 17-02-2020 08:15 til
17-02-2020 12:00

Location 10.1-025 - teorirum (32)

Teacher Niels Jørgensen (nielsj@ruc.dk)

Informatics: Programming for Security (PSec)

Time 24-02-2020 08:15 til
24-02-2020 12:00

Location 03.1-w01 - klyngerum 1 (30)

Teacher Niels Jørgensen (nielsj@ruc.dk)

Informatics: Programming for Security (PSec)

Time 02-03-2020 08:15 til
02-03-2020 12:00

Location 03.1-e23 - klyngerum 2 (30)

Teacher Niels Jørgensen (nielsj@ruc.dk)

Informatics: Programming for Security (PSec)

Time 09-03-2020 08:15 til
09-03-2020 12:00

Location 10.1-025 - teorirum (32)

Teacher Niels Jørgensen (nielsj@ruc.dk)

Informatics: Programming for Security (PSec)

Time 16-03-2020 08:15 til
16-03-2020 12:00

Location 10.1-025 - teorirum (32)

Teacher Niels Jørgensen (nielsj@ruc.dk)

Informatics: Programming for Security (PSec)

Time 23-03-2020 08:15 til
23-03-2020 12:00

Location 10.1-025 - teorirum (32)

Teacher Niels Jørgensen (nielsj@ruc.dk)

Informatics: Programming for Security (PSec)

Time	30-03-2020 08:15 til 30-03-2020 12:00
Location	10.1-025 - teorirum (32)
Teacher	Niels Jørgensen (nielsj@ruc.dk)

Informatics: Programming for Security (PSec)

Time	06-04-2020 08:15 til 06-04-2020 12:00
Location	10.1-025 - teorirum (32)
Teacher	Niels Jørgensen (nielsj@ruc.dk)

Informatics: Programming for Security (PSec)

Time	20-04-2020 08:15 til 20-04-2020 12:00
Location	10.1-025 - teorirum (32)
Teacher	Niels Jørgensen (nielsj@ruc.dk)

Informatics: Programming for Security (PSec) - Hand in

Time	28-04-2020 10:00 til 28-04-2020 10:00
Forberedelsesnorm	Ikke valgt
Forberedelsesnorm d-vip	Ikke valgt

Informatics: Programming for Security (PSec) - Oral exam

Time	16-06-2020 08:15 til 17-06-2020 18:00
Forberedelsesnorm	Ikke valgt
Forberedelsesnorm d-vip	Ikke valgt

Informatics: Programming for Security (PSec) - Reexam hand in

Time	11-08-2020 10:00 til 11-08-2020 10:00
Forberedelsesnorm	Ikke valgt
Forberedelsesnorm d-vip	Ikke valgt

Informatics: Programming for Security (PSec) - Oral reexam

Time	23-08-2020 08:15 til 23-08-2020 18:00
Forberedelsesnorm	Ikke valgt
Forberedelsesnorm d-vip	Ikke valgt