AGH UNIVERSITY OF SCIENCE AND TECHNOLOGY

Module name: Selected Topics in Cryptography

Academic year: 2014/2015 Code: IET-1-706-s ECTS credits: 3

Faculty of: Computer Science, Electronics and Telecommunications

Field of study: Electronics and Telecommunications Specialty: —

Study level: First-cycle studies Form and type of study: Full-time studies

Lecture language: English Profile of education: Academic (A) Semester: 7

Course homepage: http://home.agh.edu.pl/~cholda/teaching/

Responsible teacher: dr hab. inż, prof. AGH Chołda Piotr (cholda@agh.edu.pl)

Academic teachers: dr hab. inż, prof. AGH Chołda Piotr (cholda@agh.edu.pl)

Module summary

Presentation of classical and recent problems of cryptography applied in computer and communication networks.

Description of learning outcomes for module

MLO code	Student after module completion has the knowledge/ knows how to/is able to	Connections with FLO	Method of learning outcomes verification (form of completion)
Social competence			
M_K001	The student can critically and creatively approach the posed problem in cryptography. She/he is able to formulate a problem and analyse it on her/his own, as well as concisely explain the proposed solution to a broader public.	ET1A_K03, ET1A_K05, ET1A_K06, ET1A_K01	Presentation, Project, Report, Execution of a project, Involvement in teamwork
Skills			
M_U001	The student can convincingly formulate a current engineering or research problem to be solved in cryptography.	ET1A_U24, ET1A_U22, ET1A_U23	Presentation, Participation in a discussion, Project, Report, Execution of a project
M_U002	The student is able to learn on her/his own and use the scientific literature, draw conclusions and creatively solve challenging problems in cryptography.	ET1A_U03, ET1A_U02, ET1A_U06, ET1A_U01, ET1A_U07, ET1A_U04, ET1A_U05	Presentation, Participation in a discussion, Project, Report, Execution of a project

Knowledge			
M_W001	The student is aware of current industrial and research trends in cryptography.	ET1A_W18	Presentation, Participation in a discussion, Project, Report, Execution of a project
M_W002	The student knows notions and methods related to the contemporary problems of cryptography.	ET1A_W18, ET1A_W01	Presentation, Participation in a discussion, Project, Report, Execution of a project

FLO matrix in relation to forms of classes

MLO code	Student after module completion has the knowledge/ knows how to/is able to	Form of classes										
		Lectures	Auditorium classes	Laboratory classes	Project classes	Conversation seminar	Seminar classes	Practical classes	Fieldwork classes	Workshops	Others	E-learning
Social competence												
M_K001	The student can critically and creatively approach the posed problem in cryptography. She/he is able to formulate a problem and analyse it on her/his own, as well as concisely explain the proposed solution to a broader public.	-	-	-	+	-	-	-	-	-	-	-
Skills												
M_U001	The student can convincingly formulate a current engineering or research problem to be solved in cryptography.	-	-	-	+	+	-	-	-	-	-	-
M_U002	The student is able to learn on her/his own and use the scientific literature, draw conclusions and creatively solve challenging problems in cryptography.	-	-	-	+	+	-	-	-	-	-	-
Knowledge												
M_W001	The student is aware of current industrial and research trends in cryptography.	-	-	-	+	+	-	-	-	-	-	-
M_W002	The student knows notions and methods related to the contemporary problems of cryptography.	-	-	-	+	+	-	-	-	-	-	-

Module content

Project classes

The project is aimed at software implementation of a selected cryptographic method
Implementation of a selected cryptographic method or a related problem (e.g., hash function, random numbers generation) and study of its performance. After implementation is finished, it is necessary to provide a short report on the studies and present the results to the classmates.

Conversation seminar

The presentation of the material is given in the conversatory manner
The participants are obliged to get to know some materials before the class meeting, and during the meeting the problems are discussed. The discussion is led by one of the participants with the help of the prepared presentation.
The subset of the following topics is going to be covered at participants' discretion:
1. Primality testing.
2. Integer factorization and the related cryptographic methods.
3. Discrete logarithms and the related cryptographic methods.
4. Secret-key cryptography.
5. Elliptic curve based cryptography.
6. Selected methods of cryptanalysis.
7. Post-quantum cryptography.

Method of calculating the final grade

To obtain a positive final grade for the course the following requirements should be met:
- a positive grade for the conversatory,
- a positive grade for the project.

The final grade is calculated as the mean value of the grades for the conversatory and the project.
To obtain a positive grade for the conversatory, it is necessary to prepare a presentation on a selected topic and lead a discussion on it. The number of presentations is related to the fair share of all the participants and the number of meetings (e.g., one presentation per person). The grade is found as the maximum of m and n, where m is the grade proposed by the teacher and n is the median of the grades proposed by other participants of the course. Additionally: (1) No more than three absences (with no excuse) at the conversatory meetings are acceptable. (2) The teacher must be provided a presentation at least a week prior to the meeting. (3) The presentation should be prepared according to the suggestions of the teacher. Failing to meet these conditions, is related to necessity to pass a test covering the discussed topics.
To obtain a positive grade for the project it is necessary to design and implement either random number generation solution or an effective hash function. A report and public presentation of results are also required.
If any grade is determined based on achieved scores, the grading scale of §13, pt. 1 of the Study Regulations is applied. If any grade is determined on the basis of the weighted average of other grades, the thresholds defined in §27, pt. 4 of the Study Regulations are applied.

Prerequisites and additional requirements

None.

Recommended literature and teaching resources

1. Song Y. Yan, **Computational Number Theory and Modern Cryptography**, Higher Education Press, 2013.
2. Lynn M. Batten, **Public Key Cryptography**, Wiley-IEEE Press, 2013.

Scientific publications of module course instructors related to the topic of the module
None.

Additional information
None.

Student workload (ECTS credits balance)

Student activity form	Student workload
Participation in conversation seminars	30 h
Preparation for classes	10 h
Preparation of a report, presentation, written work, etc.	10 h
Completion of a project	15 h
Participation in project classes	10 h
Summary student workload	75 h
Module ECTS credits	3 ECTS