AGH UNIVERSITY OF SCIENCE AND TECHNOLOGY

Module name:	Securing Data Transmission: Cryptology, Watermarking and Steganography				
Academic year:	2019/2020	Code:	IETP-1-621-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:	6
Course homepage:	http://home.agh.edu.pl/~cholda/teaching/				
Responsible teacher:	dr hab. inż, prof. AGH Chołda Piotr (cholda@agh.edu.pl)				

Module summary

Presentation of fundamental concepts of cryptography applied in securing of 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: is able to			
M_K001	The student can critically and creatively approach the posed problem related to application of cryptography in the network environment. She/he is able to formulate a problem and analyse it on her/his own, solve the problem, as well as concisely explain the proposed solution to a broader public.	ETP1A_K04, ETP1A_K05, ETP1A_K01, ETP1A_K03	Execution of a project, Presentation, Project
Skills: he can			
M_U001	The student is able to learn on her/his own and use the scientific literature, draw conclusions and creatively solve challenging problems related to secure communications.	ETP1A_U03, ETP1A_U04, ETP1A_U05, ETP1A_U02, ETP1A_U06	Completion of laboratory classes, Execution of laboratory classes, Execution of a project, Report, Activity during classes, Presentation, Participation in a discussion, Project

M_U002	The student can convincingly formulate a current engineering or research problem to be solved with use of cryptography.	ETP1A_U03, ETP1A_U04, ETP1A_U05, ETP1A_U02, ETP1A_U06	Completion of laboratory classes, Execution of laboratory classes, Execution of a project, Report, Activity during classes, Participation in a discussion, Project
M_U003	Is able to effectively communicate in English in relatation to topics concering security and cryptography.	ETP1A_U05	Execution of laboratory classes, Project, Presentation
Knowledge: he knows and understands			
M_W001	The student knows mathematical foundations behind cryptographical, watermarking and steganographical concepts.	ETP1A_W01, ETP1A_W10	Completion of laboratory classes, Execution of a project, Report, Project, Activity during classes, Execution of laboratory classes, Presentation, Participation in a discussion
M_W002	The student is aware of basic methods used for securing communications.	ETP1A_W10	Completion of laboratory classes, Execution of a project, Report, Preparation and conduct of scientific research, Project, Activity during classes, Execution of laboratory classes, Presentation, Participation in a discussion

Number of hours for each form of classes

	Form of classes										
Suma	Lectures	Auditorium classes	Laboratory classes	Project classes	Conversation seminar	Seminar classes	Practical classes	Fieldwork classes	Workshops	Prace kontrolne i przejściowe	Lektorat
50	16	0	0	24	0	10	0	0	0	0	0

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	Prace kontrolne i przejściowe	Lektorat
Social competence: is able to												

M_K001	The student can critically and creatively approach the posed problem related to application of cryptography in the network environment. She/he is able to formulate a problem and analyse it on her/his own, solve the problem, as well as concisely explain the proposed solution to a broader public.	+	-	-	+	-	+	-	-	-	-	-
Skills: he can												
M_U001	The student is able to learn on her/his own and use the scientific literature, draw conclusions and creatively solve challenging problems related to secure communications.	+	-	-	+	-	+	-	-	-	-	-
M_U002	The student can convincingly formulate a current engineering or research problem to be solved with use of cryptography.	+	-	-	+	-	+	-	-	-	-	-
M_U003	Is able to effectively communicate in English in relatation to topics concering security and cryptography.	+	-	-	+	-	+	-	-	-	-	-
Knowledge: he knows and understands												
M_W001	The student knows mathematical foundations behind cryptographical, watermarking and steganographical concepts.	-	-	-	+	-	+	-	-	-	-	-
M_W002	The student is aware of basic methods used for securing communications.	-	-	-	+	-	+	-	-	-	-	-

Student workload (ECTS credits balance)

Student activity form	Student workload
Udział w zajęciach dydaktycznych/praktyka	50 h
Preparation for classes	10 h
przygotowanie projektu, prezentacji, pracy pisemnej, sprawozdania	15 h
Realization of independently performed tasks	15 h
Summary student workload	90 h
Module ECTS credits	3 ECTS

Additional information

Module content

Lectures

There are five lectures on fundamental aspects of cryptography.
The following problems are going to be covered during the lectures:
- Substitution and transposition ciphers.
- Affine ciphers.
- Perfect secrecy.
- Symmetric cryptography.
- DES. AES.
- Public-key encryption.
- Integer numbers and modular arithmetic (congruences). Factoring. Discrete logarithms.
- RSA.
- Cryptographic hash functions.
- Identification. Digital signatures.
- Public-key infrastructures.

There are eight lectures on fundamental aspects of cryptography, watermarking and steganography
The following problems are going to be covered during the lectures:
- Substitution and transposition ciphers.
- Affine ciphers.
- Perfect secrecy.
- Symmetric cryptography.
- DES. AES.
- Public-key encryption.
- Integer numbers and modular arithmetic (congruences). Factoring. Discrete logarithms.
- RSA.
- Cryptographic hash functions.
- Digital signatures. Public-key infrastructures.
- Digital watermarking.
- Steganography and steganalysis.
- Network steganography.

Project classes

The project is aimed at implementation of selected cryptographic methods
Implementation of a selected cryptographic method related to a standard proposed or used in contemporary telecommunications. Examples: implementation of IETF RFC 8032. After completing the implementation, it is necessary to prepare a short documentation to present the project to the classmates. The project is performed in small teams.

The project is aimed at implementation of selected cryptographic methods
Implementation of a selected cryptographic method related to a standard proposed or used in contemporary telecommunications. Examples: implementation of IETF RFC 8032. After finishing the implementation, it is necessary to prepare a short documentation to present the project to the classmates.

Seminar classes

The seminar is aimed at extending the selected topics
The participants are obliged to get to know some materials before the seminar meeting, and during the meeting the problems are discussed in open. The discussion is led by a group of the participants with the help of the prepared presentation.

The subset of the following topics is going to be covered at participants’ discretion:

machine learning in network security, biometry, steganography, cryptography based on elliptic curves, generation of prime numbers, secret sharing, quantum cryptography, post-quantum cryptography.

The seminar is aimed at extending the selected topics
The seminar work is based on one of the b-learning concepts, in this case the so-called mutual teaching. The participants are obliged to get to know some materials before the seminar meeting, and during the meeting the problems are discussed in open. The discussion is led by a group of the participants with the help of the prepared presentation.

The subset of the following topics is going to be covered at participants' discretion: machine learning in network security, biometry, watermarking, steganography, cryptography based on elliptic curves, generation of prime numbers, secret sharing, quantum cryptography, post-quantum cryptography.

Teaching methods and techniques:

Lectures: Treści prezentowane na wykładzie są przekazywane w formie prezentacji multimedialnej w połączeniu z klasycznym wykładem tablicowym wzbogaconymi o pokazy odnoszące się do prezentowanych zagadnień.
Project classes: Studenci wykonują zadany projekt samodzielnie, bez większej ingerencji prowadzącego. Ma to wykształcić poczucie odpowiedzialności za pracę w grupie oraz odpowiedzialności za podejmowane decyzje.
Seminar classes: Na zajęciach seminaryjnych podstawą jest prezentacja multimedialna oraz ustna prowadzona przez studentów. Kolejnym ważnym elementem kształcenia są odpowiedzi na powstałe pytania, a także dyskusja studentów nad prezentowanymi treściami.

Warunki i sposób zaliczenia poszczególnych form zajęć, w tym zasady zaliczeń poprawkowych, a także warunki dopuszczenia do egzaminu:

To obtain a positive final grade it is necessary to achieve the following credits:
- a positive grade for the seminar,
- a positive grade for the project.

Seminar
It is necessary to prepare a presentation (presentations) 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. 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:
- No more than 50% of absences at the seminar meetings are acceptable.
- The teacher must be provided a presentation on a selected topic at least two weeks prior to the meeting.
- The presentation should be prepared according to the suggestions of the teacher (e.g., use of LaTeX).
- If a student fails to conform to these rules, a revision test should be passed to obtain a positive grade.

Project
It is necessary to prepare the software implementing the assumed functionality, a short (up to 5 pages long) report, and present the project to the classmates.

Zasady udziału w poszczególnych zajęciach, ze wskazaniem, czy obecność studenta na zajęciach jest obowiązkowa:

Lectures:
– Attendance is mandatory: No
– Participation rules in classes: Studenci uczestniczą w zajęciach poznając kolejne treści nauczania zgodnie z syllabusem przedmiotu. Studenci winni na bieżąco zadawać pytania i wyjaśniać wątpliwości.

Rejestracja audiowizualna wykładu wymaga zgody prowadzącego.
Project classes:
– Attendance is mandatory: Yes
– Participation rules in classes: Studenci wykonują prace praktyczne mające na celu uzyskanie kompetencji zakładanych przez syllabus. Ocenie podlega sposób wykonania projektu oraz efekt końcowy.
Seminar classes:
– Attendance is mandatory: Yes
– Participation rules in classes: Studenci prezentują na forum grupy temat wskazany przez prowadzącego oraz uczestniczą w dyskusji nad tym tematem. Ocenie podlega zarówno wartość merytoryczna prezentacji, jak i tzw. kompetencje miękkie.

Method of calculating the final grade

The final grade is calculated as a mean of the grades for the seminar and the project. The lecture is treated as completed by all the student attending the course.

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.

Sposób i tryb wyrównywania zaległości powstałych wskutek nieobecności studenta na zajęciach:

If not present at seminar meetings, the student should work on her/his own to deal with the unattended topics.

Prerequisites and additional requirements

None.

Recommended literature and teaching resources

1. Johannes A. Buchmann, **Introduction to Cryptography**, Springer, 2004. The book can be downloaded by any AGH student from SpringerLink.

Scientific publications of module course instructors related to the topic of the module

None.

Additional information

Classes are conducted using innovative teaching methods developed during 2017-2019 in the POWR.03.04.00-00-D002/16 project, carried out by the Faculty of Computer Science, Electronics and Telecommunications under the Smart Growth Operational Programme 2014-2020.

The staff has improved communications skills, which have been developed during English language trainings in the POWR.03.04.00-00-D002/16 project, carried out by the Faculty of Computer Science, Electronics and Telecommunications under the Smart Growth Operational Programme 2014-2020.