Syllabus

1. Program information

1.1. Institution	ACADEMY OF ECONOMIC STUDIES
1.2. Faculty	Economic Cybernetics, Statistics and Informatics
1.3. Departments	(Departament) INFORMATICA SI CIBERNETICA ECONOMICA
1.4. Field of study	Economic Informatics
1.5. Cycle studies	Master Studies
1.6. Education type	Full-time
1.7. Study program	IT&C Security
1.8. Language study	English
1.9. Academic year	2016-2017

2. Course information

2.1. Name	**Cryptography Basis**								
2.2. Code	**16.0241IF1.1-0001**								
2.3. Year of studies	**1**	2.4. Semester	**1**	2.5. Assessment type	**Exam**	2.6. Course type	**O**	2.7. Number of ECTS	**5**
2.8. Instructors									

3. Total estimated time

3.1. Number of weeks	14.00		
3.2. Number of hours per week	2.00	of which	
		C(C)	1.00
		S(S)	1.00
3.3. Total hours from curriculum	28.00	of which	
		C(C)	14.00
		S(S)	14.00
3.4. Total hours of study per semester (ECTS*25)	125.00		
3.5. Total hours of individual study	97.00		

Time distribution for individual study	
Study the textbook, course support, bibliography and notes	
Further reading in the library, on the online platforms and field	
Preparing seminars, labs, homework, portfolios and essays	
Tutoring	
Examinations	
Other activities	

4. Prerequisites

4.1. About curriculum	The course assumes no prior lectures from the curriculum
4.2. About skills	The course assumes prior knowledge on computer programming in C/C++

5. Requirements

C(C)	Course lectures take place in rooms with multimedia teaching equipment.
S(S)	Laboratories are held in rooms that have PCs with Internet access. The development environment used is Microsoft Visual Studio 2010 or 2012, Ubuntu within virtual machines with GCC, Java plus necessary tools.

6. Skills covered

	C1	Using the theories, principles and research methods in order to develop information security solutions in the use of complex IT&C systems.
	C1	Using the theories, principles and research methods in order to develop information security solutions in the use of complex IT&C systems.

7. Course objectives

7.1. General objective	The course provides a deeper understanding into cryptography, its application to network security, threats/vulnerabilities to networks and countermeasures.
7.2. Specific objectives	La sfârșitul cursului, studenții trebui să poată: - aprecia tehnicile de bază ale criptografiei şi modul în care acestea pot fi aplicate pentru a atinge diferite obiective de securitate; - să înțeleagă problemele legate de implementarea mecanismelor criptografice; - să implementeze un standard criptografic sau de securitate care sa fie adecvat soluției solicitate; - să înțeleagă avantajele şi dezavantajele metodelor criptografice existente; - să proiecteze şi să testeze soluții simple criptografice; - să evalueze protocoale criptografice existente din punct de vedere al securitatii şi al eficienței. - Apreciez modul în care tehnicile descrise sunt folosite în practică, într-o varietate de aplicații de securitate;

8. Course contents

8.1. C(C)		Teaching methods	Advices
1	Introduction to computer security. Basic concepts of cryptography. Vulnerabilities. Cryptographic systems. Security models.	Lectures with multimedia presentations and interaction with students	- Course materials are available on the student web-platform. - It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.
2	Mathematical concepts used in cryptography. XOR function, theorems, groups, algorithms, complexity, primes, factorization.	Lectures with multimedia presentations and interaction with students	- Course materials are available on the student web-platform. - It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.

3	Random and pseudo-random numbers. Psuedo-random generators: Linear congruential generator, Linear feedback shift register generator, ANSI X9.17, Blum Blum Shub Generator.	Lectures with multimedia presentations and interaction with students	- Course materials are available on the student web-platform. - It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.
4	Protocols	Lectures with multimedia presentations and interaction with students	- Course materials are available on the student web-platform. - It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.
5	One-way hash functions. General principles. MD4, MD5, SHA, SHA1 functions.	Lectures with multimedia presentations and interaction with students	- Course materials are available on the student web-platform. - It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.
6	Symetric encryption systems. History. Transposition and substitution ciphers. Mono and polyalphabetical systems. OTP ciphers. Encription machines. Block and stream encription systems (A5, SEAL, RC4). Feistel structures based systems (DES, 3DES, IDEA, RC6, MARS, SERPENT, TWOFISH).	Lectures with multimedia presentations and interaction with students	- Course materials are available on the student web-platform. - It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.
7	Encription methods: ECB, CBC, OFB, CFB.	Lectures with multimedia presentations and interaction with students	- Course materials are available on the student web-platform. - It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.
8	Complex symmetric ciphers: DES, AES.	Lectures with multimedia presentations and interaction with students	- Course materials are available on the student web-platform. - It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.
9	Multiple encryptions systems	Lectures with multimedia presentations and interaction with students	- Course materials are available on the student web-platform. - It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.

10	The security of symmetric encryption systems: generation, storage and distribution of keys.	Lectures with multimedia presentations and interaction with students	- Course materials are available on the student web-platform. - It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.
11	Public keys encription systems. General principles. RSA system. ElGamal system. Diffie – Hellman system. Merkle-Hellman system. Encription based on eliptic curves.	Lectures with multimedia presentations and interaction with students	- Course materials are available on the student web-platform. - It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.
12	Key-exchange algorithms	Lectures with multimedia presentations and interaction with students	- Course materials are available on the student web-platform. - It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.
13	Cryptanalysis. Attack methods: brute-force, dictionary, differential cryptanalysis, linear cryptanalysis, time and space agreement, meet-in-the-middle attack	Lectures with multimedia presentations and interaction with students	- Course materials are available on the student web-platform. - It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.

Bibliography

- Bruce Schneier, Applied cryptography, second edition :protocols, algorithms, and source code in C, John Wiley & Sons, New York, 1996, Statele Unite ale Americii
- William Stallings, Cryptography and Network Security Principles and Practices, 4th Edition, Prentice Hall, 2005, Statele Unite ale Americii
- A. Menezes, P. Oorschot, S. Vanstome, Handbook of Applied Cryptography, CRC Press, 1997, Statele Unite ale Americii
- Ion IVAN, Cristian TOMA , Informatics Security Handbook – 2nd Edition, ASE Publishing House, 2009, România

8.2. S(S)		Teaching methods	Advices
1	Exemplify basic concepts of cryptography. Vulnerabilities. Cryptographic models. Cryptographic systems.	Discussion based on proposed scenarios. Presenting examples / real situations.	Read textbooks available on the platform of support
2	Implementation in C/C++ of mathematical concepts used in cryptography. XOR method, raising power, Euclid's algorithm, factorization, prime number tests, exponential function, modlon n algebra.	Implementing the methods using programming language (C / C + +)	Using the course support to exemplify math concepts
3	Implementing a pseudo-random number generator.	Implementing/analyzing an C/C++ application using the integrated development environment.	It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.
4	Exemplification of protocols used in cryptography	Discussion based on proposed scenarios. Presenting examples / real situations.	Read textbooks available on the platform of support
5	Hash functions. MD5 and SHA1	Analysis and execution of C/C++	Read course support and check available C/C++ examples.
6	Symmetric encryption systems. Implementing transposition and substitution ciphers examples. Enigma simulation.	Analysis and execution of C/C++	Read course support and check available C/C++ examples.
7	Encription methods: ECB, CBC, OFB, CFB. Implementing a symmetric block cipher using the CBC mode.	Implementing the methods using programming language (C / C + +)	It is recommended that students study course materials and required textbooks to more easily interact with the teacher in the classroom.
8	Complex symmetric ciphers: DES, AES.	Analysis and execution of C/C++	Read course support and check available C/C++ examples.
9	Multiple encryptions systems: 3DES	Analysis and execution of C/C++	Read course support and check available C/C++ examples.
10	Public key encryption systems. General principles. The RSA, ElGamal. Examples.	Discussion based on proposed scenarios. Presenting examples / real situations.	Read textbooks available on the platform of support
11	Stream ciphers. Analysis of A5 and RC4. Implementing One Time Pad.	Analysis and execution of C/C++	Read course support and check available C/C++ examples.
12	Cryptanalysis. Examples.	Analysis and execution of C/C++. Using Cryptool.	Read course support and check available C/C++ examples.

Bibliography

- Bruce Schneier, Applied cryptography, second edition :protocols, algorithms, and source code in C, John Wiley & Sons, New York, 1996, Statele Unite ale Americii
- A. Menezes, P. Oorschot, S. Vanstome, Handbook of applied cryptography, CRC Press, 1997, Statele Unite ale Americii
- William Stallings, Cryptography and Network Security Principles and Practices, 4th Edition, Prentice Hall, 2005, Statele Unite ale Americii
- Ion IVAN, Cristian TOMA, Informatics Security Handbook – 2nd Edition, ASE Publishing House, 2009, România

9. Course contents corroboration with the demands of epistemic community representatives, professional associations and representative employers

The course is intendeed to:
- those who have a technical or management responsibility for implementing security and who need to be aware of cryptography and key management techniques.
- anyone who wishes to develop an understanding or appreciation of how cryptographic techniques can be used to solve a number of security problems.

Taking into account the best practices from IT&C field applied by big companies such as: Intel, Oracle, Microsoft, IBM, HP and professional consortiums such as: Apache, Red Hat, ISO/IEC.

10. Assessment

Activity	Assessment criteria	Assessment methods	Percentage in the final grade
10.1. S(S)	Ability to implement / analyze specific concepts of cryptography.	Applied and practical activities like labs/quizz tests/projects.	20.00
10.2. Final assessment	Gained knowledge	Final evaluation exam	80.00

10.3. Grading scale	Whole notes 1-10
10.4. Minimum performance standard	Mathematical background and know-how understanding of the main crytographic algorithms: types of cryptographic algorithms, SHA and MD5 for calculating the hash values, AES-Rijndael for symmetric-key cryptographic schemes and RSA for public key cryptography schemes. Basic concepts regarding cryptanalysis.

Completion date,
07/10/2016

Instructors,

Approval date of department

Director of department,