SYLLABUS / FIȘA DISCIPLINEI

1. Information on the study programme / Date despre programul de studii

1.1. Institution / Instituția de învățământ superior	Universitatea de Vest din Timișoara
1.2. Faculty / Facultatea	Matematică și Informatică
1.3. Department / Departamentul	Computer Science (Informatică)
1.4. Study program field	Computer Science (Informatică)
1.5. Study cycle/ Ciclul de studii	Bachelor / licență
1.6. Study programme / Programul de studii / calificarea*	Computer Science / Informatică în limba engleză - *Analyst / Analist - 251201; Research assistant in computer science / Asistent de cercetare în informatica - 214918; Teacher in secondary schools / Profesor în învatamântul gimnazial - 233002; Programmer / Programator - 251202; Software systems designers / Proiectant sisteme informatice - 251101*

2. Information on the course / Date despre disciplină

2.1. Title of the course / Denumirea disciplinei	Security and Criptography						
2.2. Teacher in charge of the course / Titularul activităților de curs	Stelian Mihalas						
2.3. Teacher in charge of the seminar / Titularul activităților de seminar	Stelian Mihalas						
2.4. Study year / Anul de studii	3	2.5. Semester / Semestrul	2	2.6. Examination type / Tipul de evaluare: E(xam)/C(olloquim)	C	2.7. Course type / Regimul disciplinei: M(andatory)/ E(lective)/ F(acultative)	DO

3. Estimated study time (number of hours per semester) /Timpul total estimat (ore pe semestru al activităților didactice)

3.1. Attendance hours per week / Număr de ore pe săptămână	3	out of which din care: 3.2 lecture/ curs	2	3.3. seminar/laborator	1
3.4. Attendance hours per semester / Total ore din planul de învățământ	42	out of which: 3.5 lecture / curs	28	3.6. seminar/laborator	14

Distribution of the allocated amount of time / Distribuția fondului de timp*	**hours/ ore**
Individual study /Studiu după manual, suport de curs, bibliografie și notițe	14
Supplementary documentation at library or using electronic repositories / Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate	7
Preparing for laboratories, homework, reports etc. /Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	28
Exams / Examinări	7
Tutoring / Tutorat	14

3.7. Total number of hours of individual study / Total ore	70

studiu individual	
3.8. Total number of hours per semester / Total ore pe semestru	112
3.9. Number of credits (ECTS) / Număr de credite	5

4. Prerequisites (if it is the case) / Precondiții (acolo unde e cazul)

4.1. curriculum / de curriculum	Programming I
4.2. skills / de competențe	

5. Requirements (if it is the case) / Condiții (acolo unde e cazul)

5.1. for the lecture / de desfășurare a cursului	Lecture room with a video-projector
5.2. for the seminar, laboratory / de desfășurare a seminarului/laboratorului	C development environment installed on the workstations, internet connection

6. Acquired skills / Competențe specifice acumulate

Professional skills / Competențe profesionale	• Understanding the mathematical foundations of cryptography and cryptanalysis • The knowledge and the capacity of applying information encryption and decryption methods • Basic understanding of statistical methods used in cryptanalysis • Ability of applying hash functions to guarantee the integrity of a file or of a message • Ability to use digital certificates in the authentication process and in secure communication • Recognizing the importance of data backup, protection and integrity preservation • Skills in identifying, preventing and blocking internet specific threats – viruses, trojans, phishing, spoofing
Transversal skills / Competențe transversale	• Ability to use the Visual Studio IDE for application development • Realizing the importance of personal data protection in general • Understanding the necessity of secure communication in day to day life • Recognizing the general internet threats and implementing mesures to prevent them

7. Objectives of the course / Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

7.1. General objective / Obiectivul general al disciplinei	Getting to know and use cryptographic and security concepts – hash functions, key exchange protocols, encryption and decryption algorithms, digital signatures, public key certificates and infrastructure, data protection principles, secure communication, internet threats prevention.
7.2. Specfic objectives / Obiectivele specifice	*Knowledge objectives (KO)*: (1) Good understanding of the mathematical foundations of cryptography; (2) Knowing the main encryption and decryption algorithms and the key exchange protocols (3) Understanding the nature of security threats *Ability objectives (AO)*: (1) Ability to implement secure communication (2)

	Ability to recognize and prevent threats *Skills wise objectives (SO)*: (1) Implementation of basic data protection, backup and restoration; (2) Ability to use antivirus and other threat prevention and removal software

8. Content / Conținuturi*

8.1. Lecture / Curs	**Teaching strategies / Metode de predare**	**Remarks, details / Observații**
01 - Cryptography and cryptanalysis	Lecture, class discussion, informal debate	
02 - Classical cryptography, Diffie-Hellman algorithm	Lecture, class discussion, student presentation, questioning	
03 - Hash functions - MD5, SHA-1, SHA-4	Student presentations, questioning, informal discussion	
04 - DES, AES, specifications and algorithms	Student presentations, questioning, informal discussion	
05 - Elements of number theory, the RSA algorithm	Lecture on number theory, Student presentation, questioning, informal discussion	
06 - DSS, specification and implementation	Student presentations, questioning, informal discussion	
07 - The SSL protocol, Secure Shell	Student presentations, questioning, informal discussion	
08 - Data security, Network security	Student presentations, questioning, informal discussion	
09 - Traffic analyzers, Passwords	Student presentations, questioning, informal discussion	
10 - Torrents, the hide and seek game	Student presentations, questioning, informal discussion	
11 - Viruses, examples, protection	Student presentations, questioning, informal discussion	
12 - Trojans, examples, protection	Student presentations, questioning, informal discussion	
13 - Software exploits, Internet threats	Student presentations, questioning, informal discussion	
14 – Security Proxies	Lecturer presentation, justification, critical discussion	

Recommended bibliography / Bibliografie

1. Course notes - http://web.info.uvt.ro/~smihalas/cry_sec/book/crysec.pdf
2. FIPS 180-2 - csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
3. FIPS 46-3 - csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
4. FIPS 186 - www.itl.nist.gov/fipspubs/fip186.htm
5. FIPS 197 - csrc.nist.gov/publications/fips/fips197/fips-197.pdf
6. Lynn Margaret Batten - Public Key Cryptography Applications and Attacks - John Wiley and Sons, Inc, New Jersey, 2013.
7. A. Atanasiu: Securitatea informatiei, vol 1, (2) , Editura InfoData, Cluj 2007 (2009)
8. Douglas Crawford - Proxies vs. VPN – What's the difference? - https://www.bestvpn.com/blog/4085/proxies-vs-vpn-whats-the-difference/
9. Buchmann J., Karatsiolis E. - Introduction to Public Key Infrastructures – Springer Verlag, 2013

8.2. Seminar, lab / Seminar, laborator	Teaching/learning strategies / Metode de predare/ invățare	Remarks, details / Observații
1 - Projects setup and specification, bit level operations	Development environment setup, operations detailed with examples, discussion	
2 - SHA-1 algorithm details, functions	Implementation skeleton provided, main functions detailed according to their specs	
3 - Project SHA-1 submitted	Students present project, examination on details knowledge	
4 - AES, the Rijndael algorithm, algebraic operations	Standard context presentation, mathematical principles presented, discussion	
5 - Functions used in the Rijndael algorithm, encryption phase	Implementation skeleton provided, main functions detailed according to their specs	
6 - Inverse functions, decryption phase	Inversion functions and decryption detailed	
7 - Project AES (Rijndael) submitted	Students present project, examination on details knowledge	

Recommended bibliography / Bibliografie:

1. SHA-1 specification - FIPS 180.2 - csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
2. AES specification - FIPS 197 - csrc.nist.gov/publications/fips/fips197/fips-197.pdf

9. Correlations between the content of the course and the requirements of the IT field / Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului

Course content is typical for teaching Security and Cryptography in colleges at undergraduate level. Ubiquity of security issues and data protection concerns make skilled professionals in this area in high demand.

10. Evaluation / Evaluare*

Activity / Tip de activitate	10.1. Evaluation criteria / Criterii de evaluare**	10.2. Evaluation methods / Metode de evaluare***	10.3. Weight in the final mark / Pondere din nota finală
10.4. Lecture / Curs	Knowledge levels in all course areas, quality of course presentations	Colloquium in written form or course presentation	50%
10.5. Seminar/ lab	Proper implementation, knowledge	Project execution, questioning	20%
	Proper implementation, knowledge	Project execution, questioning	30%
10.6. Minimal knowledge for passing / Standard minim de performanță			
Acquiring a passing grade as a combination of the colloquium and lab projects.			

Date/ Data completării
1.10.2016

Signature (lecture) /
Semnătura titularului de curs

Signature (seminar)
Semnătura titularului de seminar

Signature (director of the department)
Semnătura directorului de departament
Conf.dr. Victoria Iordan