

## CURRICULUM DESCRIPTION / **FIŞA DISCIPLINEI**

### **1. Program information / Date despre program**

1.1 Higher education institution / <i>Instituția de învățământ superior</i>	West University of Timișoara / <i>Universitatea de Vest din Timișoara</i>
1.2 Faculty / Department / <i>Facultatea / Departamentul</i>	Mathematics and Informatics / <i>Matematică și Informatică</i>
1.3 Department / <i>Departamentul</i>	Informatics / <i>Informatică</i>
1.4 Study area / <i>Domeniul de studii</i>	Informatics / <i>Informatică</i>
1.5 Study cycle / <i>Ciclul de studii</i>	Masters / <i>Master</i>
1.6 Study program / Qualification / <i>Programul de studii / Calificarea</i>	Cybersecurity / Specialist in security-focused procedures and tools for information systems / <i>Securitate Cibernetică / Specialist în proceduri și instrumente de securitate a sistemelor informative</i>

### **2. Curriculum information / Date despre disciplină**

2.1 Name of class / <i>Denumirea disciplinei</i>	Cryptography and information security / Criptografie și securitatea informației						
2.2 Teacher for lecture / <i>Titularul activităților de curs</i>	Conf. dr. Ciprian Pungilă						
2.3 Teacher for laboratory / <i>Titularul activităților de seminar</i>	Conf. dr. Ciprian Pungilă						
2.4 Year of study / <i>Anul de studiu</i>	1	2.5 Semester / <i>Semestrul</i>	1	2.6 Evaluation type / <i>Tipul de evaluare</i>	E	2.7 Type of class / <i>Regimul disciplinei</i>	M

### **3. Estimated total time (hours per semester for didactic activities) / Timpul total estimat (ore pe semestru al activităților didactice)**

3.1 Hours per week / <i>Număr de ore pe săptămână</i>	4	of which / <i>din care:</i> 3.2 lecture / <i>curs</i>	2	3.3 seminary/laboratory / <i>seminar/laborator</i>	2
3.4 Hours in curriculum plan / <i>Total ore din planul de învățământ</i>	56	of which / <i>din care:</i> 3.5 lecture / <i>curs</i>	28	3.6 seminary/laboratory / <i>seminar/laborator</i>	28
Time distribution: / <i>Distribuția fondului de timp:</i>					hours / <i>ore</i>
Study time using the manual, lecture reading material, bibliography and notes / <i>Studiul după manual, suport de curs, bibliografie și notițe</i>					28

Suplimentary documentation inside a library, or online / on the field / <i>Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate / pe teren</i>	28
Seminary/laboratory preparation, homework, research paper, portfolios and essays / <i>Pregătire seminare / laboratoare, teme, referate, portofolii și eseuri</i>	28
Tutorship / <i>Tutoriat</i>	7
Exminations / <i>Examinări</i>	6
Other activities / <i>Alte activități</i>	
3.7 Total hours of individual study / <i>Total ore studiu individual</i>	<b>97</b>
3.8 Total hours per semester / <i>Total ore pe semestru</i>	<b>153</b>
3.9 Number of credits / <i>Numărul de credite</i>	<b>6</b>

#### 4. Preconditions (where applicable) / Precondiții (acolo unde este cazul)

4.1 for curriculum / <i>de curriculum</i>	<ul style="list-style-type: none"> <li>Operating Systems, Programming, Security and Cryptography / Sisteme de operare, Programare, Securitate și criptografie</li> </ul>
4.2 for competencies / <i>de competențe</i>	<ul style="list-style-type: none"> <li>Basic knowledge of computer usage / Cunoștințe de bază în utilizarea calculatorului</li> </ul>

#### 5. Conditions (where applicable) / Condiții (acolo unde este cazul)

5.1 for lecture development / <i>de desfășurare a cursului</i>	<p>Classroom properly equipped with: whiteboard, laptop/projector, computers, network, internet connection, appropriate software. Means for organizing online course activities: Google Classroom, Meet+Chat/Microsoft Teams, PowerPoint, Forms, virtual whiteboard, other specific software components for online activities / Sală de curs, dotată corespunzător: tablă, laptop/proiector, calculatoare, rețea, legătură internet, software adecvat.</p> <p>Mijloace pentru organizarea activităților de curs online: Google Classroom, Meet+Chat/Microsoft Teams, PowerPoint, Forms, tablă virtuală, alte componente software specifice activităților online.</p>
5.2 for seminary/laboratory development / <i>de desfășurare a seminarului / laboratorului</i>	<p>Laboratory classroom properly equipped with: whiteboard, laptop/projector, computers, network, internet connection, appropriate software. Means for organizing online course activities: Google Classroom, Meet+Chat/Microsoft Teams,</p>

	<p>PowerPoint, Forms, virtual whiteboard, other specific software components for online activities / Sală de laborator, dotată corespunzător: tablă, laptop/proiector, calculatoare, rețea, legătură internet, software adekvat.</p> <p>Mijloace pentru organizarea activităților de curs online: Google Classroom, Meet+Chat/Microsoft Teams, PowerPoint, Forms, tablă virtuală, alte componente software specifice activităților online.</p>
--	--

**6. Class objectives – expected learning results, contributed to by reading and passing of the class / Obiectivele disciplinei - rezultate așteptate ale învățării la formarea cărora contribuie parcurgerea și promovarea disciplinei**

<b>Knowledge / Cunoștințe</b>	<ul style="list-style-type: none"> <li>Understanding the mathematical foundations of cryptography and cryptographic analysis / Înțelegerea fundamentelor matematice ale criptografiei și analizei criptografice</li> <li>Knowledge and ability to apply methods of encryption and decryption / Cunoașterea și capacitatea de a aplica metodele de încriptare și decriptare</li> <li>Ability to apply hash functions and use digital certificates / Abilitatea de a aplica funcțiile de hash și utilizare a certificatelor digitale</li> </ul>
<b>Abilities / Abilități</b>	<ul style="list-style-type: none"> <li>Understanding the need to keep up with the latest developments and technologies in data transmission, storage, and protection / Înțelegerea necesității de a fi la curent cu ultimele noutăți și tehnologii de transmitere, stocare și protecție a datelor</li> <li>Understanding the need for secure communication in everyday life / Înțelegerea necesității comunicării securizate viața de zi cu zi</li> <li>Recognition of security threats and the need to implement measures to prevent and counter them / Recunoașterea amenințărilor de securitate și a necesității de a implementa măsuri de prevenire și contracarare a acestora</li> <li>Ability to decide on the opportunity to use a platform and a programming language in implementing a complex application / Capacitatea de a decide asupra oportunității utilizării unei platforme și unui limbaj de programare în implementarea unei aplicații complexe</li> <li>Knowledge and acquisition of advanced skills in using the main security concepts - hash functions, key sharing protocols, data encryption/decryption algorithms, digital signatures and certificates, public key infrastructure, data protection principles, as well as secure communication. / Cunoașterea și dobândirea abilităților avansate de utilizare a principalelor concepte de securitate – funcții de hash, protocoale de partajare a cheilor, algoritmi de încriptare/decriptare a datelor, semnăturile și certificatele digitale, infrastructura cheilor publice, principiile protecției datelor precum și comunicarea securizată</li> </ul>

<b>Responsability and autonomy / Responsabilitate și autonomie</b>	<ul style="list-style-type: none"> <li>• A good understanding of the mathematical foundations of cryptography and cryptographic analysis / O bună înțelegere a fundamentelor matematice ale criptografiei și analizei criptografice</li> <li>• Knowledge and application of the main methods of encrypting and decrypting messages as well as key sharing methods / Cunoașterea și aplicarea principalelor metode de încriptare și decriptare a mesajelor precum și metode de partajare a cheilor</li> <li>• Understanding the nature of security threats / Înțelegerea naturii amenințărilor de securitate</li> <li>• Ability to recognize and prevent security threats / Abilitatea de a recunoaște și a preveni amenințările de securitate</li> <li>• Ability to implement secure communication methods / Abilitatea de a implementa modalități de comunicare securizată</li> </ul>
--	--

## 7. Contents / Conținuturi

8.1 Lecture / Curs	Teaching methods / Metode de predare	Observations / Observații
Lecture 1 / Curs 1: Merkle's key exchange protocol Public-key encryption. Definition of security: IND-CPA. Overview of group theory and number theory.	Exercises, discussions and debates, modelling, projects, organized team-work / Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat	1 week – 2 hours / 1 săptămână – 2 ore
Lecture 2 / Curs 2: Discrete Log Assumption. Diffie-Hellman key exchange. Diffie-Hellman/El Gamal encryption	Exercises, discussions and debates, modelling, projects, organized team-work / Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat	1 week – 2 hours / 1 săptămână – 2 ore
Lecture 3 / Curs 3: Trapdoor functions. RSA, trapdoor permutations and another public-key cryptosystem. QRA, Goldwasser-Micali and Homomorphism.	Exercises, discussions and debates, modelling, projects, organized team-work / Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat	1 week – 2 hours / 1 săptămână – 2 ore
Lecture 4 / Curs 4: Digital Signatures: Definition. Lamport's One-time Signature Scheme.	Exercises, discussions and debates, modelling, projects, organized team-work / Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat	1 week – 2 hours / 1 săptămână – 2 ore
Lecture 5 / Curs 5: Collision-resistant hash functions. Many-time, stateful, signature schemes.	Exercises, discussions and debates, modelling, projects, organized team-work / Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat	1 week – 2 hours / 1 săptămână – 2 ore

Naor-Yung construction: stateless EUF-CMA-secure signature schemes.		
Lecture 6 / Curs 6: Instantiation of collision-resistant hash functions from discrete log. Direct construction of digital signatures from RSA. The hash-and-sign paradigm and the random oracle heuristic. Variants of digital signatures.	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore
Lecture 7 / Curs 7: Zero knowledge I, definitions and examples. Zero Knowledge Proofs for all of NP.	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore
Lecture 8 / Curs 8: Succinct (Zero Knowledge) Argument Systems. Tools: Merkle Trees, Probabilistically Checkable Proofs . Kilian's Protocol.	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore
Lecture 9 / Curs 9: Lattices, Learning with Errors (LWE). LWE-based Cryptography: Secret-key and Public-key Encryption, Collision-Resistant Hashing. Fully Homomorphic Encryption. A Construction of FHE from the LWE assumption.	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore
Lecture 10 / Curs 10: Fully Homomorphic Encryption continued: The Bootstrapping Theorem, and Circular Security. Open Problems in FHE Research.	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore
Lecture 11 / Curs 11: Oblivious Transfer. Private Information Retrieval.	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore

Lecture 12 / Curs 12: Secure Two-Party Computation. The Goldreich-Micali-Wigderson Protocol.	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore
Lecture 13 / Curs 13: Secret-Sharing. Secure Multiparty Computation.	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore
Lecture 14 / Curs 14: Program Obfuscation and Applications.	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore

Bibliography / Bibliografie :

Lecture 1 / Curs 1:

- [Lecture Notes on the Complexity of Some Problems in Number Theory](#) by Dana Angluin.
- [Probabilistic Encryption](#) by Shafi Goldwasser and Silvio Micali.
- [A Method for Obtaining Digital Signatures and Public-Key Cryptosystems](#) by R.L. Rivest, A. Shamir, and L. Adleman
- [New Directions in Cryptography](#) by Whitefield Diffie and Martin E. Hellman.
- [Secure Communications Over Insecure Channels](#) by Ralph C. Merkle
- [The Growth of Cryptography](#) by Ronald L. Rivest, at the 2011 Killian Lecture.

Lecture 2 / Curs 2

- [Generating Random Factored Numbers, Easily](#) by Adam Kalai.

Lecture 3 / Curs 3

- [Probabilistic Encryption by Shafi Goldwasser and Silvio Micali.](#)
- [A Minimalist Proof of the Law of Quadratic Reciprocity by Bogdan Veklych.](#)

Lecture 4 / Curs 4

- [Goldwasser-Micali-Rivest Signature Scheme](#) by Shafi Goldwasser, Silvio Micali, and Ron Rivest.
- [Two Remarks Concerning the Goldwasser-Micali-Rivest Signature Scheme](#) by Oded Goldreich
- [Universal One-way Hash Functions and their Cryptographic Applications](#) by Moni Naor and Moti Yung.

Lecture 5 / Curs 5

- [\*\*SPHINCS: Practical stateless hash-based signatures.\*\*](#) by Bernstein et al. (a modern version of the signature scheme from this lecture.)
- [\*\*Post-Quantum Cryptography\*\*](#) by NIST. See also: [\*\*SPHINCS+\*\*](#)

#### Lecture 6 / Curs 6

- [\*\*One-Way Functions are Necessary and Sufficient for Secure Signatures\*\*](#) by John Rompel.

#### Lecture 7 / Curs 7

- [\*\*The Knowledge Complexity of Interactive Proof Systems\*\*](#) by Shafi Goldwasser, Silvio Micali, and Charles Rackoff.

#### Lecture 8 / Curs 8

- [\*\*ZK for NP\*\*](#) by Oded Goldreich, Silvio Micali, and Avi Wigderson.

#### Lecture 9 / Curs 9

- [\*\*On Lattices, Learning with Errors, Random Linear Codes, and Cryptography\*\*](#) by Oded Regev.
- [\*\*Efficient Fully Homomorphic Encryption from \(Standard\) LWE\*\*](#) by Zvi Brakerski and Vinod Vaikuntanathan.
- [\*\*Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based\*\*](#) by Craig Gentry, Amit Sahai and Brent Waters.
- [\*\*Hardness of LWE on General Entropic Distributions\*\*](#) by Zvi Brakerski and Nico Döttling.
- [\*\*Homomorphic Encryption: from Private-Key to Public-Key\*\*](#) by Ron Rothblum.

#### Lecture 10-11 / Curs 10-11

- [\*\*How to Exchange and Generate Secrets\*\*](#) by Andrew Chi-Chih Yao
- [\*\*Private Information Retrieval\*\*](#) by Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan

#### Lecture 12 / Curs 12

- [\*\*Draft of A Chapter on General Protocols\*\*](#) from Volume 2 of Foundations of Cryptography, by Oded Goldreich
- [\*\*Bar-Ilan Winter School on MPC\*\*](#)

#### Lecture 13 / Curs 13

- [\*\*How To Play Any Mental Game\*\*](#) by Oded Goldreich, Silvio Micali, and Avi Wigderson
- [\*\*Extending Oblivious Transfers Efficiently\*\*](#) by Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank
- [\*\*Correlated Pseudorandomness and the Complexity of Private Computations\*\*](#) by Donald Beaver

- [\*\*Simplified VSS and Fast-track Multiparty Computations with Applications to Threshold Cryptography\*\*](#) by Rosario Gennaro, Michael O. Rabin, and Tal Rabin
- [\*\*Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation\*\*](#) by Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson
- [\*\*NIST Kick-Starts 'Threshold Cryptography' Development Effort\*\*](#)

#### Lecture 14 / Curs 14

- [\*\*On the \(Im\)possibility of Obfuscating programs,\*\*](#) Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang.
- [\*\*How to Use Indistinguishability Obfuscation: Deniable Encryption, and More,\*\*](#) Amit Sahai and Brent Waters.
- [\*\*Indistinguishability Obfuscation from Well-Founded Assumptions\*\*](#), Aayush Jain, Huijia Lin and Amit Sahai.

8.2 Seminary / laboratory / Seminar / laborator	Teaching methods / Metode de predare	Observations / Observații
Cipher text algorithms implementation.	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform / Notițe de laborator, informații teme laborator disponibile prin platforme specifice e-uvt.ro, comunicare prin platforma Google Classroom
Merkle's key exchange protocol Public-key encryption.	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform / Notițe de laborator, informații teme laborator disponibile prin platforme specifice e-uvt.ro, comunicare prin platforma Google Classroom
Diffie-Hellman key exchange. Diffie-Hellman/Elliptic Curve encryption	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele,</i>	2 weeks – 4 hours / 2 săptămâni – 4 ore Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through

	<i>lucrul în grup organizat</i>	the Google Classroom platform / Notițe de laborator, informații teme laborator disponibile prin platforme specifice e-uvt.ro, comunicare prin platforma Google Classroom
RSA implementation	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform / Notițe de laborator, informații teme laborator disponibile prin platforme specifice e-uvt.ro, comunicare prin platforma Google Classroom
Digital signatures implementation	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform / Notițe de laborator, informații teme laborator disponibile prin platforme specifice e-uvt.ro, comunicare prin platforma Google Classroom
Hash functions implementation	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform / Notițe de laborator, informații teme laborator disponibile prin platforme specifice e-uvt.ro, comunicare prin platforma Google Classroom
Merkle Trees implementation	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	1 week – 2 hours / 1 săptămână – 2 ore Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform

		/ Notițe de laborator, informații teme laborator disponibile prin platforme specifice e-uvt.ro, comunicare prin platforma Google Classroom
LWE-based Cryptography implementation	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	2 weeks – 4 hours / 2 săptămâni – 4 ore Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform / Notițe de laborator, informații teme laborator disponibile prin platforme specifice e-uvt.ro, comunicare prin platforma Google Classroom
Oblivious Transfer. Private Information Retrieval.	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	2 weeks – 4 hours / 2 săptămâni – 4 ore Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform / Notițe de laborator, informații teme laborator disponibile prin platforme specifice e-uvt.ro, comunicare prin platforma Google Classroom
Program Obfuscation	Exercises, discussions and debates, modelling, projects, organized team-work / <i>Exercițiile, discuțiile și dezbaterea, modelarea, proiectele, lucrul în grup organizat</i>	2 week – 4 hours / 2 săptămâni – 4 ore Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform / Notițe de laborator, informații teme laborator disponibile prin platforme specifice e-uvt.ro, comunicare prin platforma Google Classroom
<b>Bibliography / Bibliografie:</b>		<ul style="list-style-type: none"> <li>• <a href="#">New Directions in Cryptography</a> by Whitefield Diffie and Martin E. Hellman.</li> <li>• <a href="#">Secure Communications Over Insecure Channels</a> by Ralph C. Merkle</li> <li>• <a href="#">Universal One-way Hash Functions and their Cryptographic Applications</a> by Moni Naor and Moti Yung.</li> <li>• <a href="#">SPHINCS: Practical stateless hash-based signatures.</a> by Bernstein et al. (a modern version of the signature scheme from this lecture.)</li> </ul>

- [One-Way Functions are Necessary and Sufficient for Secure Signatures](#) by John Rompel.
- Real-World Cryptography, David Wong
- [Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based](#) by Craig Gentry, Amit Sahai and Brent Waters.
- [Hardness of LWE on General Entropic Distributions](#) by Zvika Brakerski and Nico Döttling.
- [Homomorphic Encryption: from Private-Key to Public-Key](#) by Ron Rothblum.
- [How to Exchange and Generate Secrets](#) by Andrew Chi-Chih Yao
- [On the \(Im\)possibility of Obfuscating programs](#), Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang.
- [How to Use Indistinguishability Obfuscation: Deniable Encryption, and More](#), Amit Sahai and Brent Waters.
- [Indistinguishability Obfuscation from Well-Founded Assumptions](#), Aayush Jain, Huijia Lin and Amit Sahai.

**8. Unification of class contents with the expectations of the representatives of the epistemic community, professional organisations and employers from the class's relevant field(s) of applicability / Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatorii reprezentativi din domeniul aferent programului**

Class contents corresponds to the curricula of other universities, from inside the country or from the European Union. The practical contents (laboratory works) correspond to the local labor market requirements. /

*Conținutul disciplinei corespunde curriculei din alte centre universitare, din țară sau Uniunea Europeană. Conținuturile practice (lucrări de laborator) corespund cerințelor de pe piața muncii locală.*

**9. Evaluation / Evaluare**

Activity type / Tip activitate	10.1 Evaluation criteria / Criterii de evaluare	10.2 Evaluation methods / Metode de evaluare	10.3 Weight in final grade / Pondere din nota finală
10.4 Lecture / Curs	<p>The evaluation takes into account the following categories of knowledge / Evaluarea are în vedere următoarele categorii de cunoștințe:</p> <ul style="list-style-type: none"> <li>• general knowledge, evaluated through a test consisting of multiple choice questions or basic definitions / cunoștințe generale, evaluate printr-un test cuprinzând întrebări cu variante multiple de răspuns sau definiții de bază</li> <li>• detailed knowledge, evaluated through a test focused on the key concepts</li> </ul>	<p>Written examination; active participation in class activities. / Examinare scrisă; participare activă la activitățile de curs.</p>	50%

	<p>taught / cunoștințe de detaliu, evaluate printr-un test cuprinzând întrebări orientate spre noțiunile cheie predate</p> <ul style="list-style-type: none"> <li>use of algorithms, evaluated through a test consisting of a set of problems based on the algorithms presented in class / utilizarea algoritmilor, evaluate printr-un test cuprinzând un set de probleme pe baza algoritmilor prezentați la curs</li> </ul>		
10.5 Seminary / laboratory / Seminar / laborator	Mandatory laboratory assignments / Temele de laborator obligatorii	Evaluation of assignments, additional activities; / Evaluarea temelor, activităților adiționale;	20%
	The projects cover parts of the material presented in the laboratory, under conditions similar to those of the laboratory examination / Proiectele acoperă părți ale materiei prezentate la laborator, în condiții similare examinării de laborator	Individual project, group project. / Proiect individual, proiect de grup.	30%
10.6 Minimum performance standards / Standard minim de performanță			
<b>Written examination / Examinare scrisă:</b> <ul style="list-style-type: none"> <li>To obtain a grade of 5, it is necessary to obtain a score higher than 60% for the general knowledge, as well as to demonstrate a minimum level of understanding and application of some of the algorithms presented in the course (at least 40%). / Pentru nota 5 este necesară obținerea unui punctaj superior (minim 60%) pentru cunoștințele generale, precum și dovedirea unui nivel minim de înțelegere și aplicare a unora dintre algoritmii prezentați la curs (minim 40%)</li> <li>To obtain a grade of 10, it is necessary to obtain a score higher than 90% for both general knowledge and detailed knowledge, as well as a good understanding of the presented algorithms. / Pentru nota 10 este necesară obținerea unui punctaj superior (minim 90%) pentru cunoștințele generale și cunoștințele de detaliu, precum și o bună înțelegere a algoritmilor prezentați</li> </ul>			

Date of completion /  
*Data completării*

Teacher for class /  
*Titular de disciplină*

Date of approval inside department /  
*Data avizării în departament*

Department director /  
*Director de departament*