FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	**Universitatea Babeș-Bolyai din Cluj-Napoca**
1.2 Facultatea	**Facultatea de Matematică și Informatică**
1.3 Departamentul	**Departamentul de Matematică și Informatică al Liniei Maghiare**
1.4 Domeniul de studii	**Calculatoare și tehnologia informației**
1.5 Ciclul de studii	**Licență**
1.6 Programul de studiu / Calificarea	**Informatică (în limba maghiară)**

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)			**Introducere în criptografie** Introduction to cryptography				
2.2 Titularul activităților de curs			Lect. dr. Șuteu-Szöllősi Ștefan Lucian				
2.3 Titularul activităților de laborator			Lect. dr. Șuteu-Szöllősi Ștefan Lucian				
2.4 Anul de studiu	3	2.5 Semestrul	5	2.6. Tipul de evaluare	Colocviu	2.7 Regimul disciplinei	Opțional
2.8 Codul disciplinei	**MLM5085**						

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1 Număr de ore pe săptămână	4	Din care: 3.2 curs	2	3.3 laborator	2
3.4 Total ore din planul de învățământ	56	Din care: 3.5 curs	28	3.6 laborator	28
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe					14
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					15
Pregătire laboratoare, teme, referate, portofolii și eseuri					14
Tutorat					14
Examinări					4
Alte activități: proiect					8
3.7 Total ore studiu individual	69				
3.8 Total ore pe semestru	125				
3.9 Numărul de credite	4				

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	• Nu e cazul
4.2 de competențe	• Cunoștințe de bază de algebră, teoria numerelor, programare

5. Condiții (acolo unde este cazul)

5.1 De desfășurare a cursului	• Videoproiector
5.2 De desfășurare a seminarului/laboratorului	• Videoproiector

6. Competențele specifice acumulate

Competențe profesionale	• C1.5 Dezvoltarea de unități de program și elaborarea documentațiilor aferente • C3.2 Descrierea de concepte, teorii și modele folosite în domeniul de aplicare • C3.3 Utilizarea modelelor și instrumentelor informatice și matematice pentru rezolvarea problemelor specifice domeniului de aplicare • C3.5 Elaborarea componentelor informatice ale unor proiecte interdisciplinare
Competențe transversale	• CT2 Desfășurarea eficientă a activităților organizate într-un grup interdisciplinar și dezvoltarea capacităților empatice de comunicare interpersonală, de relaționare și colaborare cu grupuri diverse • CT3 Utilizarea unor metode și tehnici eficiente de învățare, informare, cercetare și dezvoltare a capacităților de valorificare a cunoștințelor, de adaptare la cerințele unei societăți dinamice și de comunicare în limba română și într-o limbă de circulație internațională

7. Obiectivele disciplinei (reieșind din grila competențelor acumulate)

7.1 Obiectivul general al disciplinei	• Prezentarea, analiza siguranței și implementarea diferitelor sisteme criptografice (de la cele clasice la cele cu cheie publică) și a diferitelor protocoale criptografice (funcții hash, semnătura digitala, TLS, cripto-valute). Înțelegerea cadrului matematic asociat și al principiilor de construcție ale acestor sisteme.
7.2 Obiectivele specifice	• Scopul laboratoarelor este implementarea și utilizarea specifică a sistemelor criptografice de mai sus, îmbunătățind astfel și abilitățile de programare.

8. Conținuturi

8.1 Curs	Metode didactice	Observații
1. Noțiuni criptografice de bază. Sistemul CAESAR și variantele lui	Prelegere, demonstrație, exemple	[1], capitolul 1,2.1.1
2. Sisteme matriceale (Vigenere, Playfair)	Prelegere, demonstrație, exemple	[1], capitolul 2.1.2
3. Codebook, sisteme de transpoziție, aparate de criptare	Prelegere, demonstrație, exemple	[1], capitolul 2.1.3,4,5,6
4. One time pad, generarea numerelor pseudo-aleatoare	Prelegere, demonstrație, exemple	[1], capitolul 2.2.1
5. Noțiuni din teoria complexității. Corpuri finite	Prelegere, demonstrație, exemple	[1], Appendix
6. Sisteme Feistel 1 (DES, AES)	Prelegere, demonstrație, exemple	[1], capitolul 2.2.2
7. Sisteme Feistel 2 (criptanaliză diferențială)	Prelegere, demonstrație, exemple	[6]
8. Funcții one-way și trapdoor. Sisteme cu cheie publică Knapsack	Prelegere, demonstrație, exemple	[1], capitolul 3, 3.1
9. Cifrul RSA	Prelegere, demonstrație, exemple	[1], capitolul 3.2
10. Sisteme bazate pe logaritmare discretă	Prelegere, demonstrație, exemple	[1], capitolul 3.3,4
11. Funcții hash	Prelegere, demonstrație, exemple	[1], capitolul 4
12. Protocoale criptografice 1 (semnătura digitală, autentificare)	Prelegere, demonstrație, exemple	[1], capitolul 5,6
13. Protocoale criptografice 2 (TLS)	Prelegere, demonstrație, exemple	[1], capitolul 5,6
14. Bazele criptografice ale criptovalutei Bitcoin. Structura unui blockchain	Prelegere, demonstrație, exemple	[7]

Bibliografie

[1] Szántó Cs., Șuteu Szöllősi I.: *Kriptográfia*, Presa Universitară Clujeană, 2009.
[2] Koblitz N.: *A Course in Number Theory and Cryptography* (Second Edition), Springer, 1994.
[3] Salomaa A.: *Public-Key Cryptography* (Second Edition), Springer, 2000.
[4] Crivei S., Marcus A., Sacarea Ch., Szántó Cs.: *Computational algebra with applications to coding theory and cryptography*, EFES, 2006.
[5] Heiko Knospe: *A Course in Cryptography*, AMS Pure and Applied Undergraduate Texts, 2019
[6] https://www.ukma.edu.ua/~yubod/teach/coding/crypto/diffanalysis.pdf
[7] Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf, 2009

8.2 Laborator	Metode didactice	Observații
1. Folosirea sistemelor de version control (Git) în programare. Programare în Python	Prelegere, exemple	[1], [2], [3]
2. Implementarea sistemelor criptografice clasice (sistemul CAESAR și variantele lui, sisteme matriceale, sisteme de transpoziție, etc.) în Python	Prelegere, exemple, implementare	[4], [5]
3. Criptanaliza sistemelor criptografice clasice	Exemple, exerciții, implementare	[6]
4. Algoritmi pentru generarea numerelor pseudo-aleatoare. Implementarea cifrelor de flux în Python. Aplicații (comunicare securizată între programe)	Prelegere, implementare	[7]
5. Infrastructuri cu chei publice (PKI). Implementare/simulare în Python	Prelegere, exemple, implementare	
6. SSL/TLS în practică. Implementare în Java (OpenSSL, java.security). Aplicații (generarea și verificarea certificatelor, comunicare securizată client-server, etc.)	Prelegere, implementare	[8]
7. Securizarea serverelor web. Bune practici de securitate	Prelegere, exemple, exerciții	[9]

Bibliografie

[1] https://try.github.io/
[2] https://www.atlassian.com/git/tutorials
[3] https://www.vogella.com/tutorials/Git/article.html
[4] PEP 8 – Style Guide for Python Code, https://peps.python.org/pep-0008/
[5] PEP 20 – The Zen of Python, https://peps.python.org/pep-0020/
[6] https://www.cryptool.org
[7] NIST - National Institute of Standards and Technology, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf
[8] Oracle, *Package java.security*, https://docs.oracle.com/javase/8/docs/api/java/security/package-summary.html
[9] The Open Worldwide Application Security Project (OWASP), https://owasp.org

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

- Conținutul cursului coincide cu cel tradițional al unui curs de criptografie predat la universitățile majore din învățământul universitar.
- Diferitele implementări criptografice testează și dezvoltă în mod semnificativ abilitățile de programare.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Capacitatea de aplicare a noțiunilor teoretice	Examen scris și oral (dacă este cazul)	50%
10.5 Laborator	Abilitatea de a implementa și de a analiza sistemele criptografice	Probleme concrete de implementare și analiză	50%
10.6 Standard minim de performantă			
Nota de trecere este 5 (care trebuie obținută atât la examenul scris cât și la laborator)			

Data completării	Semnătura titularului de curs	Semnătura titularului de laborator
12.03.2024	Lect. dr. Șuteu-Szöllősi Ștefan L.	Lect. dr. Șuteu-Szöllősi Ștefan L.

Data avizării în departament	Semnătura directorului de departament
14.03.2024	Conf. dr. András Szilárd