FIȘA DISCIPLINEI

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea „Sapientia" din municipiul Cluj-Napoca
1.2. Facultatea/ DSPP	Facultatea de Științe Tehnice și Umaniste din Târgu Mureș
1.3. Domeniul de studii	Calculatoare și tehnologia informației
1.4. Ciclul de studii	Licență
1.5. Programul de studiu	Calculatoare
1.6. Calificarea	Inginer

2. Date despre disciplină

2.0. Departamentul				Matematică – Informatică			
2.1 Denumirea disciplinei				Criptografie și securitate informațională			
2.2 Titularul disciplinei / activităților de curs				Lector dr. Márton Gyöngyvér			
2.3 Titularul (ii) activităților de	seminar			-			
	laborator			Lector dr. Márton Gyöngyvér			
	proiect			-			
2.4 Anul de studiu	4	2.5 Semestrul	8	2.6. Tipul de evaluare	Ex	2.7 Regimul disciplinei	DI

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 seminar /laborator/ proiect	0 /2/ 0
3.4 Total ore din planul de învățământ	56	Din care: 3.5 curs	28	3.6 seminar / laborator / proiect	0 /28 /0

Distribuția fondului de timp:	ore
a) Studiul după manual, suport de curs, bibliografie și notițe	23
b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren	4
c) Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	14
d) Tutoriat	-
e) Examinări	3
f) Alte activități:	-

3.7 Total ore studiu individual	44
3.8 Total ore pe semestru	100
3.9 Numărul de credite	4

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	•
4.2 de competențe	•

5. Condiții (acolo unde este cazul)

5.1 De desfășurare a cursului	• Sală de curs cu tablă și videoproiector
5.2 De desfășurare a seminarului/laboratorului/proiectului	• Sală de laborator dotată corespunzător: calculatoare, rețea, legătură la Internet, videoproiector, tablă

6. Competențele specifice acumulate

Competențe profesionale	• C4. Îmbunătățirea performantelor sistemelor hardware, software si de comunicații • C4.1 Identificarea și descrierea elementelor definitorii ale performantelor sistemelor hardware, software și de comunicații • C4.2 Explicarea interacțiunii factorilor care determina performantele sistemelor hardware, software și de comunicații • C4.3 Aplicarea metodelor si principiilor de baza pentru creșterea performantelor sistemelor hardware, software și de comunicații • C4.4 Alegerea criteriilor si metodelor de evaluare a performantelor sistemelor hardware, software și de comunicații • C4.5 Dezvoltarea de soluții profesionale pentru sisteme hardware, software și de comunicații bazate pe creșterea performantelor
Competențe transversale	•

7. Obiectivele disciplinei (reieșind din grila competențelor acumulate)

7.1 Obiectivul general al disciplinei	• Cunoașterea conceptelor de bază și a principiilor ce fundamentează criptografia • Folosirea noțiunilor teoretice învățate în aplicații concrete. • Studenții vor fi capabili să dezvolte aplicații software pe baza noțiunilor matematice, criptografice învățate.
7.2 Obiectivele specifice	• Prezentarea noțiunilor teoretice și practice ale criptografiei, respectiv securitatea informației. • Prezentarea algoritmilor legate de criptografia clasica. Prezentarea algoritmilor legate de sistemele criptografice cu cheie privată, respectiv prezentarea securității acestor sisteme. Prezentarea sistemelor DES și AES. • Prezentarea noțiunilor matematice legate de sistemele criptografice cu cheie publica. Prezentarea diferenței dintre sistemele de criptare și noțiunea de semnătură digitală. Prezentarea sistemelor RSA, ElGamal DDS. Folosirea corectă a acestor sisteme, din punctul de vedere al securității. • Implementarea algoritmilor învățate într-un limbaj de programare: C, C++, #C, Java, Python sau PHP

8. Conținuturi

8.1 Curs	Metode de predare	Observații
Sisteme criptografice clasice: Caesar, Keyword Caesar, affin, Hill	Expunerea interactivă Dezbaterea Problematizarea	2 ore
Sisteme criptografice cu cheie privată • Sisteme criptografice de tip flux: OTP, RC4 • Sisteme criptografice de tip bloc: DES, AES • Securitatea sistemelor criptografice cu cheie privată	Expunerea interactivă Dezbaterea Problematizarea	8 ore
Coduri de autentificare a mesajelor (MAC) • definiție, securitate	Expunerea interactivă Dezbaterea	4 ore

Functii hash • Definiție, securitate • MD5, SHA, HMAC	Problematizarea	
Sisteme criptografice cu cheie publică. • Sistemul Diffie-Hellman • Sisteme de criptare cu cheie publică: RSA, Rabin, ElGamal, Blum-Goldwasser • Semnături digitale: RSA, ElGamal, ECC • Securitatea sistemelor criptografice cu cheie publică	Expunerea interactivă Dezbaterea Problematizarea	12 ore
Protocoale criptografice.	Expunerea interactivă Dezbaterea Problematizarea	2 ore

Bibliografie obligatorie

1. Pagina web al titularului de disciplina: https://ms.sapientia.ro/~mgyongyi/crypto.html

Bibliografie opțională

1. Bege A., Kása Z., Algoritmikus kombinatorika és számelmélet, Egyetemi Kiadó, Kolozsvár, 2006.
2. Buchmann J., Introduction to cryptography, Springer Verlag, 2002.
3. Buttyán L., Vajda I.: Kriptográfia és alkalmazásai, Typotex, Budapest, 2004.
4. Freud R., Gyarmati E., Számelmélet, Nemzeti Tankönyvkiadó, Budapest, 2000.
5. Cormen T.H., Leiserson C.E., Rivest R.L., Algoritmusok, Műszaki Könyvkiadó, Budapest, 2001.
6. Katz J., Lindell Y, Introduction to Modern Cryptography: Principles and Prtotocols, Second Edition, Chapman and Hall/CRC, 2014.
7. Márton Gy, Kriptográfiai alapismeretek, Scientia Kiadó, Kolozsvár, 2008.
8. Menezes J., van Oorschot P.C., Vanstone S.A., Handbook of Applied Cryptograph, CRC Press, Boca Raton, Florida, 1997.
9. Stinson D.R., Cryptography theory and practice, Third Edition, Chapman&Hall/CRC, 2016.

8.2 Seminar – nu este cazul	Metode de predare	Observații
8.3 Laborator		
Sisteme criptografice clasice: Caesar, Keyword Caesar, sistemul affin, Hill. Posibilități de decriptare. Implementări software.	Exerciții. Conversația euristică. Modelarea. Documentare pe web	6 ore
Sisteme criptografice de tip flux: OTP, RC4. Posibilități de decriptare. Implementare software.	Exerciții Problematizare Programare	4 ore
Sisteme criptografice de tip bloc: AES, CBC-AES, CTR-AES. Implementare software.	Exerciții Problematizare Programare	4 ore
Funcții hash. Programare.	Exerciții Problematizare Programare	2 ore
Sisteme de criptare cu cheie publica: Diffie-Hellman, RSA, Rabin, ElGamal, Blum-Goldwasser Implementări software.	Exerciții Problematizare Programare	6 ore
Semnături digitale: RSA, ElGamal. Implementare software.	Exerciții Problematizare Programare	4 ore
Test de evaluare a cunoștințelor		2 ore

Bibliografie

1. Márton Gy, Kriptográfiai alapismeretek, Scientia Kiadó, Kolozsvár, 2008.
2. Menezes J., van Oorschot P.C., Vanstone S.A., , Handbookof Applied Cryptograph, CRC Press, Boca Raton, Florida, 1997.
3. Stinson D.R., Cryptography theory and practice, Third Edition, Chapman&Hall/CRC, 2016.
4. Pagina web al titularului de disciplina: http://www.ms.sapientia.ro/~mgyongyi

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

- Conținutul disciplinei este în concordanță cu cerințele planului de învățământ, cu conținutul disciplinei predate la alte Universități din țară (Universitatea Tehnică din Cluj-Napoca, Universitatea Politehnică din Timișoara, Universitatea Transilvania din Brașov) și de peste hotare (Universitatea Tehnică și de Științe Economice din Budapesta)
- Aspecte de securitate a aplicațiilor în tehnologia informației au devenit importante în industrie, cursul pune accent pe înțelegerea metodelor care stau la baza soluțiilor de securitate în acest domeniu.

10. Evaluare

A. Condiții de îndeplinit pentru prezentarea la evaluare:

Efectuarea tuturor lucrărilor de laborator și promovarea testului de evaluare la laborator

B. Criterii, metode și ponderi în evaluare:

Tip activitate		10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs		înțelegerea problemei, abilitatea de a analiza funcționarea algoritmilor de criptare și decriptare	Evaluare scrisă	50%
10.5	Seminar	-	-	-
	Laborator	înțelegerea problemei, abilitatea de a dezvolta algoritmi de criptare și decriptare	Evaluare pe parcurs și testare a cunoștințelor prin test scris	50%
	Proiect	-	-	-

10.6 Standard minim de performanță
Cunoașterea elementelor fundamentale despre problematica securității IT și a metodelor de protecție a informației.

	Semnătura titularului disciplinei:	Semnătura titularului /rilor de aplicații:
	Lector dr. Márton Gyöngyvér	Lector dr. Márton Gyöngyvér
Data:	Semnătura directorului de departament:	Semnătura coordonatorului programului de studii:
16. 09. 2019	Conf. dr. ing. Kátai Zoltán	Ș.l.dr.ing. Szabó László Zsolt