

**FIȘA DISCIPLINEI****1. Date despre program**

1.1 Instituția de învățământ superior	Universitatea “Alexandru Ioan Cuza” din Iași
1.2 Facultatea	Facultatea de Informatică
1.3 Departamentul	Informatică
1.4 Domeniul de studii	Informatică
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Securitatea Informatiei/Master in informatica

2. Date despre disciplină

2.1 Denumirea disciplinei		Tehnisi si Metode de Criptanaliza					
2.2 Titularul activităților de curs		Dr. Simion Emil					
2.3 Titularul activităților de seminar		Dr. Simion Emil					
2.4 An de studiu	I	2.5 Semestru	1	2.6 Tip de evaluare	E	2.7 Regimul disciplinei*	OB

* *OB – Obligatoriu / OP – Opțional*

3. Timpul total estimat (ore pe semestru și activități didactice)

3.1 Număr de ore pe săptămână	4	din care: 3.2 curs	2	3.3 seminar/laborator	2
3.4 Total ore din planul de învățământ	56	din care: 3.5 curs	28	3.6 seminar/laborator	28
Distribuția fondului de timp					ore
Studiu după manual, suport de curs, bibliografie și altele					14
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					14
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					28
Tutoriat					-
Examinări					4
Alte activități					-
3.7 Total ore studiu individual					56
3.8 Total ore pe semestru					114
3.9 Număr de credite					5

4. Precondiții (dacă este cazul)

4.1 De curriculum	-
4.2 De competențe	-



5. Condiții (dacă este cazul)

5.1 De desfășurare a cursului	Este recomandată prezența la curs
5.2 De desfășurare a seminarului	Prezența la seminar

6. Competențe specifice acumulate

Competențe profesionale	C1. Expunerea unor tehnici și metode de criptanaliză specifice criptografiei clasice, precum și criptografiei moderne (simetrice și asimetrice) C2. Aplicarea conceptelor asimilate în domeniul securității informației
Competențe transversale	CT1. Eficientizarea activităților desfășurate în cadrul organizat, prin aplicarea regulilor academice de muncă riguroasă și creativă CT2. Utilizarea optimă a surselor informaționale și a resurselor de comunicare din domeniu CT3. Exprimarea unei atitudini responsabile față de înțelegerea rolului domeniului în informatică CT4. Valorificarea eficace a potențialului științific însușit în domeniu

7. Obiectivele disciplinei (din grila competențelor specifice acumulate)

7.1 Obiectivul general	Cursul introduce studenților o tematică majoră în domeniul criptologiei și anumite tehnici și metode specifice de criptanaliză.
7.2 Obiectivele specifice	La finalizarea cu succes a acestei discipline, studenții vor fi capabili să: <ul style="list-style-type: none">▪ Utilizeze corespunzător concepte de criptanaliză;▪ Înțeleagă corespunzător, la nivel ridicat, securitatea sistemelor informatice.



8. Conținut

8.1	Curs	Metode de predare	Observații (ore și referințe bibliografice)
1.	Prezentarea tehnicilor de analiza statistica (conceptul de test statistic bazat pe intervale de incredere, reguli de decizie, exemple: NIST SP 800-22)	Expunere si demonstratii realizate la tabla	8
2.	Criptanaliza sistemelor clasice	Expunere si demonstratii realizate la tabla	2
3.	Criptanaliza sistemelor de cifrare si semnare electronica asimetrice (RSA, ElGamal si ElGamal pe curbe eliptice)	Expunere si demonstratii realizate la tabla	4
4.	Criptanaliza sistemelor de cifrare simetrice (studiu de caza AES, tipuri de atacuri asupra modurilor de operare, generatoare pseudoaleatoare)	Expunere si demonstratii realizate la tabla	4
5.	Criptanaliza functiilor hash	Expunere si demonstratii realizate la tabla	4
6.	Criptanaliza protocoalelor criptografice (studii de caz SSL, SSH si IPSEC)	Expunere si demonstratii realizate la tabla	6

Bibliografie

Referințe principale:

- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography, CRC Press, third printing, 1997
- Friedman, William F, Military Cryptanalysis, Part I-IV
- Christopher Swenson, Modern cryptanalysis: Techniques for Advanced Code Breaking, ISBN 978-0-470-13593-8, Wiley, 2008

Referințe suplimentare:

- E. Simion, Criptanaliza. Tehnici si Metode Matematice, Ed. Univ. Buc, 2004, ISBN 973575975-6.



8.2	Seminar	Metode de predare	Observații (ore și referințe bibliografice)
1.	Prezentarea tehnicilor de analiza statistica (conceptul de test statistic bazat pe intervale de incredere, reguli de decizie, exemple: NIST SP 800-22)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	8
2.	Criptanaliza sistemelor clasice	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
3.	Criptanaliza sistemelor de cifrare si semnare electronica asimetrice (RSA, ElGamal si ElGamal pe curbe eliptice)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	4
4.	Criptanaliza sistemelor de cifrare simetrice (studiu de caza AES, tipuri de atacuri asupra modurilor de operare, generatoare pseudoaleatoare)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	4
5.	Criptanaliza functiilor hash	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	4
6.	Criptanaliza protocoalelor criptografice (studii de caz SSL, SSH si IPSEC)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	6

Bibliografie

Referințe principale:

- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography, CRC Press, third printing, 1997
- Friedman, William F, Military Cryptanalysis, Part I-IV
- Christopher Swenson, Modern cryptanalysis: Techniques for Advanced Code Breaking, ISBN 978-0-470-13593-8, Wiley, 2008

Referințe suplimentare:

- E. Simion, Criptanaliza. Tehnici si Metode Matematice, Ed. Univ. Buc, 2004, ISBN 973575975-6.

**9. Coroborarea conținutului disciplinei cu așteptările reprezentanților comunității, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului**

Cursul este corelat cu asteptarile moderne in securitatea informatiei (de exemplu, Amazon si-a format recent echipe de securitatea informatiei, multi dintre fostii studenti ai masterului de securitatea informatiei fiind membri ai acestor echipe).

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în nota finală (%)
10.4 Curs	Cunoasterea conceptelor si a rezultatelor fundamentale in domeniu; Abilitatea de aplicare a lor	Test scris	50%
10.5 Seminar/ Laborator	Cunoasterea conceptelor si a rezultatelor fundamentale in domeniu; Abilitatea de aplicare a lor	Exercitii realizate in clasa de fiecare student, precum si evaluarea de implementari	50%
10.6 Standard minim de performanță			
Minim nota 5 atat la testul scris cat si la activitatea de seminar/laborator			

Data completării

Titular de curs
Dr. Simion EmilTitular de seminar
Dr. Simion Emil

Data avizării în departament

Director de departament