FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Ştiinţe
1.3 Departamentul	Matematică şi Informatică
1.4 Domeniul de studii	Informatică
1.5 Ciclul de studii	Licenţă
1.6 Programul de studii / Calificarea	**Informatică**
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	SINFL28.10

2. Date despre disciplină

2.1 Denumirea disciplinei	**Criptografie**						
2.2 Aria de conţinut							
2.3 Responsabil de curs	Conf. univ. dr. Ioana ZELINA						
2.4 Titularul activităţilor de seminar / laborator / proiect	Conf. univ. dr. Ioana ZELINA						
2.5 Anul de studiu	II	2.6 Semestrul	3	2.7 Tip de evaluare	sumativă	2.8 Regimul disciplinei	DS/DO

3. Timpul total estimat

3.1 Număr de ore pe săptămână	2	din care: 3.2 curs	1	3.3 seminar / laborator	1
3.4 Total ore din planul de învăţământ	28	din care: 3.5 curs	14	3.6 seminar / laborator	14
Distribuţia fondului de timp					ore
Studiul după manual, suport de curs, bibliografie şi notiţe					7
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					4
Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri					7
Tutoriat					2
Examinări					2
Alte activităţi.....					

3.7 Total ore studiu individual	22
3.8 Total ore pe semestru	50
3.9 Numărul de credite	2

4. **Precondiţii** (acolo unde este cazul)

4.1 de curriculum	Cunoaşterea unui limbaj de programare Algebra
4.2 de competenţe	Utilizarea sistemelor de calcul

5. **Condiţii** (acolo unde este cazul)

5.1. de desfăşurare a cursului	Studenții trebuie să aiba cont pe platforma kb.cunbm.utcluj.ro. Pentru a participa la cursurile online, studenții trebuie să dispună de sistem de calcul, camera si microfon.
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Termenul predării fiecărei lucrări de laborator este stabilit de titular în momentul enunţării temei. Pentru predarea cu întârziere a lucrărilor de laborator, lucrările vor fi depunctate cu 1 pct./zi de întârziere. Fiecare temă se notează cu punctaje între 1 şi 10, nota finală la laborator este media aritmetică a notelor. O lucrare nepredată se notează cu 0. Temele se încarcă pe platforma kb.cunbm.utcluj.ro. Pentru a participa la laboratoarele online studenții trebuie să dispună de sistem de calcul, camera si microfon.

6. Competenţele specifice accumulate

Competenţe profesionale	Prelucrarea matematica a datelor, analiza si interpretarea unor fenomene si interpretarea rezultatelor prelucrării datelor prin sisteme de criptare Analiza comparativă a rezultatelor obţinute prin utilizarea diverselor sisteme de criptare Elaborarea si analiza unor algoritmi pentru rezolvarea problemelor Identificarea notiunilor de baza folosite în constructia si specificarea algoritmilor de criptare a informaţiei şi a altor protocoale criptografice Explicarea etapelor care intervin în algoritmii criptografici
Competenţe transversale	**C1** Aplicarea regulilor de muncă organizată şi eficientă, a unor atitudini responsabile faţă de domeniul didactic-ştiinţific, pentru valorificarea creativă a propriului potenţial, cu respectarea principiilor şi a normelor de etică profesională **C3** Utilizarea unor metode şi tehnici eficiente de învăţare, informare, cercetare şi dezvoltare a capacităţilor de valorificare a cunoştinţelor, de adaptare la cerinţele unei societăţi dinamice și de comunicare în limba română şi într-o limbă de circulaţie internaţională

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

7.1 Obiectivul general al disciplinei	Insuşirea de către studenţi a noţiunilor, conceptelor şi exemplelor fundamentale din criptografie şi securitatea datelor Familiarizarea studenţilor cu tehnici de bază din criptografie şi criptanaliză Construcţia şi analiza unor algoritmi criptografici de bază
7.2 Obiectivele specifice	Studenţii vor fi capabili să : - explice funcţionarea principalilor algoritmi criptografici - utilizeze noţiuni şi rezultate de bază din aritmetică - calculeze cheile, mesajele în clar şi mesajele criptate în cadrul principalelor criptosisteme studiate

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
Noţiuni introductive. Securitatea informaţiei şi criptografia. Concepte şi noţiuni de bază.	Expunere	2
Sisteme simetrice de criptare. Cifruri de substituţie: monoalfabetice (Cezar, afin, Polybos), polialfabetice (Vigenere, Playfair, Homofonic). Criptanaliza sistemelor de criptare monoalfabetice şi polialfabetice.		2

Sisteme fluide de criptare. Sisteme sincronizabile şi auto-sincronizabile.		2
Sistemul de criptare DES. Modalităţi de atac.		2
Sistemul de criptare AES. Modalităţi de atac.		2
Criptare cu cheie publică.		2
Sistemul de criptare RSA		2
Bibliografie 1. Menezes, A., Oorschot, P., Vanstone, S., Handbook of Applied Cryptography, CRC Press, Florida, 1998 2. Christof Paar, Jan Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010 3. D. Stinton, Cryptography, Theory et Pratice, Second Edition, Chapman & Hall/CRC, 2002 4. Yan, Song Y., Number theory for computing, ed. a II-a, Springer Verlag, 2002 5. https://www.researchgate.net/profile/Adrian_Atanasiu/publication/308791446_Securitatea_Informatiei_vol_1_Criptografie/links/57f1f67608ae280dd0b2804e/Securitatea-Informatiei-vol-1-Criptografie.pdf		
8.2 Seminar / laborator / proiect	Metode de predare	Observaţii
Cifrurile Richelieu, Cezar, afin , Polybos, afin, Hill.	Exemple, probleme Exemple, implementare programe	2 ore
Cifrurile Vigenere, Playfair, Homofonic		2 ore
Sistemele Vernom, cu auto-cheie, RGA, RC4		2 ore
Sisteme de criptare înrudite de DES: 3DES, DES-X, IDEA		2 ore
Sisteme AES : RC6, Serpent, Twofish		2 ore
Comparaţie între criptare simetrică şi criptare cu cheie publică.		2 ore
Algoritmul Euclid extins. Teorema chineză a resturilor.		2 ore
Bibliografie 1. Menezes, A., Oorschot, P., Vanstone, S., Handbook of Applied Cryptography, CRC Press, Boca Raton, Florida, 1998 2. Christof Paar, Jan Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010 3. D. Stinton, Cryptography, Theory et Pratice, Second Edition, Chapman & Hall/CRC, 2002 4. Yan, Song Y., Number theory for computing, ed. a II-a, Springer Verlag, 2002 https://www.researchgate.net/profile/Adrian_Atanasiu/publication/308791446_Securitatea_Informatiei_vol_1_Criptografie/links/57f1f67608ae280dd0b2804e/Securitatea-Informatiei-vol-1-Criptografie.pdf		

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului

Tematica acestui curs este în concordanţă cu ceea ce este prevăzut în programul de studii la nivel licenţă al celor mai importante universităţi din ţară şi străinătate.

9. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Cunoaşterea principalelor aspecte teoretice prezentate la curs.	Examen scris sau online pe platformă	60%
10.5 Seminar/ Laborator	Capacitatea de a explica şi opera cu noţiunile prezentate la curs, cunoaşterea şi utilizarea sistemelor de criptare prezentate.	Verificare pe parcursul semestrului	40%
10.6 Standard minim de performanţă			
Cunoaşterea noţiunilor de bază legate de criptografie şi a sistemelor de bază. Obţinerea notei cel puţin 5 la examenul scris şi obţinerea mediei cel puţin 5 la lucrările de laborator.			

Examinarea online se face pe platforma kb.cunbm.utcluj.ro şi trebuie să fie onestă. Fiecare student va primi o parolă pentru participare la examen şi trebuie să aiba microfonul şi camera deschise pe durata desfăşurării examenului. Orice încercare de colaborare are ca şi consecintă nota 0 la examen.

Data completării	**Titulari**	**Titlu Prenume NUME**	**Semnătura**
15.09.2020	Curs	Conf. univ. dr. Ioana ZELINA	
	Aplicații	Conf. univ. dr. Ioana ZELINA	

Data avizării în Consiliul Departamentului 24.09.2020	Director Departament Prof.univ.dr. Vasile BERINDE
Data aprobării în Consiliul Facultății 25.09.2020	Decan Conferenţiar univ. dr. Monica Liliana MARIAN