FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Transilvania din Braşov
1.2 Facultatea	Inginerie Electrică şi Ştiinţa Calculatoarelor
1.3 Departamentul	Automatică şi Tehnologia Informaţiei
1.4 Domeniul de studii	Calculatoare şi Tehnologia Informaţiei
1.5 Ciclul de studii[1)]	Licenţă
1.6 Programul de studii/ Calificarea	Tehnologia Informaţiei

2. Date despre disciplină

2.1 Denumirea disciplinei	**Securitatea sistemelor informatice** (cod TI0703)							
2.2 Titularul activităţilor de curs				Dr.fiz. dr.ing. Valentin GHIŞA				
2.3 Titularul activităţilor de seminar/laborator				Dr.ing. Cornelia RÂŞNOVEANU				
2.4 Anul de studiu	4	2.5 Semestrul	7	2.6 Tipul de evaluare	E	2.7 Regimul disciplinei	Conţinut[2)]	DD
							Obligativitate[3)]	DI

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

3.1 Număr de ore pe săptămână	**4**	din care: 3.2 curs	**2**	3.3 seminar/laborator/proiect	**0/2/1**
3.4 Total ore din planul de învăţământ	70	din care: 3.5 curs	28	3.6 seminar/laborator/ proiect	0/28/14

Distribuţia fondului de timp	ore
Studiul după manual, suport de curs, bibliografie şi notiţe	20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	12
Pregătire seminarii/ laboratoare/ proiecte, teme, referate, portofolii şi eseuri	20
Tutoriat	24
Examinări	4
Alte activităţi.	0

3.7 Total ore studiu individual	80
3.8 Total ore pe semestru	150
3.9 Numărul de credite[4)]	6

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	• Parcurgerea cursurilor: *Matematici speciale, Arhitectura sistemelor de calcul.*
4.2 de competenţe	• C1. Operarea cu fundamente ştiinţifice, inginereşti şi ale informaticii; • C2. Proiectarea componentelor hardware, software şi de comunicaţii.

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului	• videoproiector • note de curs • bibliografia recomandată
5.2 de desfăşurare a seminarului/ laboratorului/ proiectului	• videoproiector • programe specializate • îndrumar de laborator • bibliografia recomandată

6. Competenţe specifice acumulate

Competenţe profesionale	• C5 Întreţinerea şi exploatarea sistemelor hardware, software şi de comunicaţii • C5.3 Utilizarea unor principii şi metode de bază pentru asigurarea securităţii, siguranţei şi uşurinţei în exploatare a sistemelor hardware, software şi de comunicaţii
Competenţe transversale	• Nu este cazul.

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

7.1 Obiectivul general al disciplinei	• Disciplina Securitatea Sistemelor Informatice îşi propune să creeze în rândul studenţilor abilităţi teoretice şi aplicative pentru studiul metodelor matematice şi a implementărilor tehnice legate de securizarea informaţiei. Disciplina conduce la obţinerea de soluţii capabile să asigure confidenţialitatea, autentificarea şi păstrarea integrităţii datelor transmise prin diferite căi speciale de comunicaţie.
7.2 Obiectivele specifice	• Utilizarea unor principii şi metode de bază pentru asigurarea securităţii şi siguranţei în exploatare a sistemelor hardware, software şi de comunicaţii. • Însuşirea conceptelor şi pricipiilor fundamentale în criptologie. • Cunoaşterea principalelor criptosisteme cu cheie privată, sistemele DES şi AES cu variantele lor îmbunătăţite şi actualizate. • Analiza şi studiul celor mai cunoscute criptosisteme cu cheie publică şi modalităţile de criptanaliză a acestora. • Identificarea şi aplicarea modelelor matematice necesare în realizarea algoritmilor de criptare şi decriptare.

8. Conţinuturi

8.1 Curs	Metode de predare	Număr de ore	Observaţii
1. Noţiuni introductive. Concepte şi noţiuni de bază. 1.1 Securitatea informaţiei şi criptografia 1.2 Bazele teoretice ale sistemelor secrete. 1.3 Bazele matematice ale sistemelor de secretizare.	problematizare explicaţie prelegere clasică demonstraţie conversaţie	2 ore	
2. Criptosisteme simetrice. 2.1 Cifruri de permutare. 2.2 Cifruri de substituţie. Sistemul de criptare afin. 2.3 Criptanaliza criptosistemelor monoalfabetice. 2.4 Sisteme de criptare polialfabetice. 2.5 Sistemul Playfair.	problematizare explicaţie demonstraţie conversaţie studii de caz	2 ore	
3. Sistemul Vigenere. Criptanaliza sistemelor polialfabetice. 3.1 Metoda indexului de coincidenţe. 3.2 Testul Kasiski.	problematizare explicaţie prelegere clasică demonstraţie	2 ore	
4. Sisteme de criptare fluide. 4.1 Sisteme sincronizabile. Sistemul Vernam. 4.2 Sisteme autosincronizabile. Regiştrii liniari cu feedback. 4.3 Criptarea cu auto-cheie. Autentificarea prin MAC.	problematizare explicaţie demonstraţie conversaţie	2 ore	
5. Succesiuni pseudoaleatoare în secretizarea informaţiei. 5.1 Conceptul de aleatorism. Teste de aleatorism. 5.2 Scheme liniare şi neliniare pentru generarea pseudoaleatoare.	problematizare explicaţie prelegere clasică demonstraţie	2 ore	
6. Sistemul de criptare DES. 6.1 Consideraţii generale. Descrierea sistemului DES. 6.2 Moduri de utilizare a DES. Modulele S-box. 6.3 Variante de criptosisteme DES.	problematizare explicaţie prelegere clasică conversaţie studii de caz	2 ore	
7. Criptanaliza sistemului DES. 7.1 Compromisul spaţiu-timp al unui atac. 7.2 Atacul meet-in-the-middle. 7.3 Criptanaliza diferenţială. Criptanaliza liniară.	problematizare explicaţie demonstraţie conversaţie studii de caz	2 ore	
8. Criptosistemul AES. 8.1 Prezentarea sistemelor concurente AES. 8.2 Sistemul de criptare Rijndael. 8.3 Prelucrarea şi extinderea cheii de criptare. 8.4 Proiectarea AES. Avantajele AES.	problematizare explicaţie prelegere clasică demonstraţie conversaţie	2 ore	
9. Criptarea cu cheie publică. 9.1 Funcţii neinversabile. 9.2 Trapa secretă. 9.3 Securitatea criptosistemelor asimetrice. 9.4 Comparaţia între criptarea simetrică şi cea cu cheie publică.	problematizare explicaţie prelegere clasică demonstraţie conversaţie studii de caz	2 ore	

10. Criptosistemul RSA. 10.1 Descrierea sistemului RSA. 10.2 Implementarea sistemului RSA. 10.3 Teste de primalitate probabiliste. Algoritmul Miller-Rabin.	problematizare explicaţie prelegere clasică demonstraţie	2 ore	
11. Securitatea sistemului RSA. 11.1 Algoritmi – oracol. Factorizarea modulului. 11.2 Atacul lui Wiener. Metoda Pollard. 11.3 Algoritmul Dixon. Criptosistemul Rabin. 12. Criptosistemul El Gamal.	problematizare explicaţie demonstraţie conversaţie studii de caz	2 ore	
12.1 Descrierea algoritmului de criptare. 12.2 Calculul logaritmului discret. 12.3 Generalizarea sistemului El Gamal.	problematizare explicaţie demonstraţie cstudii de caz	2 ore	
13. Criptarea prin curbe eliptice. 13.1 Criptosistemul Menezes – Vanstone 13.2 Criptosistemul Williams. 13.3 Criptosistemul McEliece. Codul Goppa.	problematizare explicaţie prelegere clasică demonstraţie studii de caz	2 ore	
14. Criptanaliza cifrurilor cu chei publice. 14.1 Viteza algoritmilor asimetrici. Standardul PKCS. 14.2 Atac de tip eroare hardware. 14.3 Infrastructura cheilor publice PKI. 14.4 Criptosisteme hibride.	problematizare explicaţie demonstraţie conversaţie studii de caz	2 ore	

Bibliografie
1. Buşneag, D., Boboc, F., Piciu, D., *Aritmetică şi teoria numerelor*, Ed. Universitaria, Craiova, 1999.
2. Song, Y., *Number theory for computing*, ed. a II-a, Springer-Verlag, 2002.
3. Simion, E., Oprişan, G., *Elemente de cercetări operaţionale şi criptologie*, Ed. Polotehnica Press, 2003.
4. Stallings, W., *Crytography and network security: Principles and practice*, Prentice Hall, second ed., 1999.
5. Dan, C., *Algoritmi în teoria numerelor*, Ed. Universitaria, Craiova, 2005.
6. Koblitz, D.,E., *A course in number theory and Cryptography*, ed. a II-a, Springer-Verlag, Berlin, 1994..
7. Scripcariu, I., Bogdan, I., Nicolaescu,.L., *Securitatea sistemelor de comunicaţii*, Ed. Venus, Iaşi, 2008.

8.2 Laborator	Metode de predare-învăţare	Număr de ore	Observaţii
1. Prezentare noţiuni teoretice generale despre reţelele de comunicaţii, tipuri de reţele de comunicaţii, modelarea reţelelor de comunicaţii.	conversaţie demonstraţie experiment individual experiment în grupuri mici studii de caz prezentări de referate evaluare	2 ore	
2. Referat tematic – Securitatea Sistemelor Informatice.		2 ore	
3. Prezentarea sistemelor de numeraţie. Metode de conversie în baze de numeraţie.		2 ore	
4. Structura adreselor IP. Clase de IP. Subreţele.		2 ore	
5. Crearea/Configurarea simulată a unei reţele de calculatoare de complexitate medie (2 routere, 2 switch-uri, 6 terminale). Utilizarea aplicaţiei CISCO Packet-Tracer.		2 ore	
6. Principii ale securităţii reţelelor (metode de securitate).		2 ore	
7. Protocoale şi servere de securitate.		2 ore	
8. Criptarea ca metodă de securitate a informaţiilor. Cifrul lui Hill (implementare practică criptare/decriptare).		2 ore	
9. Cifrul lui Vernam (implementare practică criptare/decriptare). Exemple de metode proprii de criptare (implementare practică criptare/decriptare).		2 ore	
10. Steganografia ca metodă de securitate a informaţiilor. Aplicaţii practice. Utilizarea aplicaţiei OurSecret.		2 ore	
11. Tehnici de securitate (firewall, sisteme de detecţie a intruşilor, reţele private virtuale).		2 ore	
12. Echipamente de secretizare a semnalului vocal TRC/DSP.		2 ore	
13. Echipamente de secretizare de grup: TCE/ Cryptolex.		2 ore	
14. Evaluare sumativă.		2 ore	

Bibliografie:
1. Stallings, W., Brown, L., *Cryptography and Network Security*, Idaho Institute of Technology, US, 2006;
2. Scripcariu, I., Bogdan, I., Nicolaescu,.L., *Securitatea sistemelor de comunicaţii*, Ed. Venus, Iaşi, 2008;
3. Welschenbach, M., *Cryptography in C and C ++*, Apress, 2001;
4. Schneier, B., *Applied crytography*, Adison-Wesley, 1998;
5. Povros, N., Honeyman, P., *Detecting Steganographic Content on the Internet*, Tech. Report, Univ. of Michigan, 2002.

8.3 Proiect	Metode de predare-învăţare	Număr de ore	Observaţii
Temele de proiect se refera la urmatoarele subiecte: - Ransomware - Virusi de tip troieni - Virusi de tip vierme - DNS poisoning - Spyware si malware - Tehnici de SQL injection - Tehnici de cross site scripting (XSS) - Spam - Atacuri de tip Denial of Service - Root-kit-uri - Boot-kit-uri - Vulenrabilitati in hardware	problematizare studiu individual studii de caz referate evaluare	14 ore	

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţilor epistemice, asociaţilor profesionale şi angajatori reprezentativi din domeniul aferent programului

Disciplina, prin aria sa aplicativă, aparţine domeniului de *Asigurare a securităţii, siguranţei şi uşurinţei în exploatare* şi pune la dispoziţie cunoştinţele necesare analizei, proiectării, testării şi implementării sistemelor de criptare şi securizare a transferului de date între diferite entităţi informaţionale. Fişa disciplinei respectă recomandările Societăţii Române de Automatică şi Informatică Tehnică – SRAIT.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3Pondere din nota finală
10.4 Curs	Claritatea şi coerenţa expunerii subiectelor propuse; Gradul de acoperire a problematicii cerute de subiecte; Redarea semnificaţiei şi corectitudinea matematică a relaţiilor de calcul; Asimilarea corectă a demonstraţiilor conceptelor cursului; Utilizarea corectă a conceptelor şi noţiunilor specifice cursului; Capacitatea şi claritatea exemplificării.	Evaluare prin examen oral: – rezolvare de aplicaţii; biletele conţin 1 subiect; ponderea în nota finală 30%; – test de cunoştinţe teoretice; biletele conţin 14 subiecte; ponderea în nota finală 20%. Pentru fiecare subiect se comunică baremul de notare studenţilor odată cu preluarea subiectelor;	60%
10.5 Laborator	Aplicarea metodelor specifice de rezolvare pentru problema dată; Utilizarea corectă a algoritmilor proprii tematicii abordate; Utilizarea corectă şi fluentă a termenilor specifici; Corectitudinea calculului analitic şi numeric; Corectitudinea interpretării rezultatelor; Aplicarea metodelor specifice de rezolvare pentru problema dată; Utilizarea corectă a algoritmilor proprii tematicii abordate; Corectitudinea calculului analitic şi numeric; Capacitatea de exemplificare; Interpretarea rezultatelor.	Evaluare pe parcurs; Evaluare prin probă practică – colocviu de laborator (A/R).	20%
10.5 Proiect	Acuratetea informatiilor prezentate Indeplinirea tuturor cerintelor	Evaluare pe parcurs; Evaluare prin probă practică	20%

10.6 Standard minim de performanţă

- Accederea la examen este condiţionată de: efectuarea integrală a lucrărilor de laborator, promovarea colocviului de laborator, precum şi prezentarea aplicaţiilor în ultima săptămână a semestrului.
- Media la examen se calculează numai în situaţia în care nota obţinută la proba teoretică şi nota obţinută la proba practică (conform baremurilor specificate), precum şi nota de la laborator, sunt de minim 5.
- Cunoaşterea şi aplicarea independentă a principalilor algoritmi de criptare/criptanaliză studiaţi, în scopul secretizării

comunicaţiilor de date în reţele.

Data completării 10.11.2016	Semnătura titularului de curs Dr.fiz. dr.ing. Valentin GHIȘA	Semnătura titularului de seminar/ laborator/ proiect Dr.ing. Cornelia RÂȘNOVEANU .....
Data avizării în departament 11.11.2016	Semnătura directorului de departament Prof dr.ing. Sorin-Aurel MORARU	

Notă:

1) Ciclul de studii - *se alege una din variantele:* Licenţă/ Master/ Doctorat;

2) Regimul disciplinei (conţinut) - *pentru nivelul de licenţă se alege una din variantele:* **DF** (disciplină fundamentală)/ **DD** (disciplină din domeniu)/ **DS** (disciplină de specialitate)/ **DC** (disciplină complementară);

3) Regimul disciplinei (obligativitate) - *se alege una din variantele:* **DI** (disciplină obligatorie)/ **DO** (disciplină opţională)/ **DFac** (disciplină facultativă);

4) Un credit este echivalent cu 25 – 30 de ore de studiu (activităţi didactice şi studiu individual).