FIȘA DISCIPLINEI

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea de Vest din Timişoara
1.2. Facultatea	Matematică și Informatică
1.3. Departamentul	Informatică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	licență
1.6. Programul de studii / calificarea*	Informatică / *Administrator baze de date - 252101; Administrator de retea de calculatoare - 252301; Analist - 251201; Asistent de cercetare în informatica - 214918; Asistent de cercetare în matematica-informatica - 212024; Profesor în învatamântul gimnazial - 233002; Programator - 251202; Proiectant sisteme informatice - 251101*

2. Date despre disciplină

2.1. Denumirea disciplinei			Securitate și Criptografie				
2.2. Titularul activităților de curs			V.Iordan				
2.3. Titularul activităților de seminar			M. Gaianu				
2.4. Anul de studii	3	2.5. Semestrul	2	2.6. Tipul de evaluare	C	2.7. Regimul disciplinei	DO

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

3.1. Număr de ore pe săptămână	3	din care: 3.2 curs	3	3.3. seminar/laborator	1
3.4. Total ore din planul de învățământ	42	din care: 3.5 curs	28	3.6. seminar/laborator	14

Distribuția fondului de timp*	**ore**
Studiu după manual, suport de curs, bibliografie și notițe	21
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate	14
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	35
Examinări	6
Tutorat	4

3.7. Total ore studiu individual	80
3.8. Total ore pe semestru	122
3.9. Număr de credite	5

4. Precondiții (acolo unde e cazul)

4.1. de curriculum	SO, Programare
4.2. de competențe	Cunoştinţe de bază în utilizarea calculatorului

5. Condiții (acolo unde e cazul)

5.1. de desfășurare a cursului	
5.2. de desfășurare a seminarului/laboratorului	Mediul de dezvoltare Eclipse

6. Competențe specifice acumulate

Competențe profesionale	Însușirea conceptelor de bază în securitatea rețelelor şi criptografie Dezvoltarea abilităţilor de proiectare a algoritmilor de criptare în vederea realizării unei retele securizate
Competențe transversale	Îmbunătăţirea abilităţilor în utilizarea calculatoarelor şi în administrarea rețelelor de calculatoare

7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

7.1. Obiectivul general al disciplinei	Însușirea conceptelor şi problematicii securității retelelor de calculatoare prin utilizarea algoritmilor de criptare
7.2. Obiectivele specifice	Însușirea algoritmilor de criptare simetrici Însușirea algoritmilor de criptare asimetrici Cunoașterea mecanismelor de generare a cheilor publice/private și a modului de administrare a acestora Principiile de bază ale securității rețelelor

8. Conţinuturi*

8.1. Curs	Metode de predare	Observații
1. Concepte de securitate şi criptografie.	Prelegere însoţită de materiale în format electronic (PDF)	
2. Clasificarea metodelor de criptare. Criptografie clasică şi tendinţe actuale în criptografie şi analiza criptografică	Prelegere însoţită de materiale în format electronic (PDF)	
3-4-5 Criptarea convenţională clasică. Modelul criptării convenţionale Algoritmi de criptare clasici (Codul lui Caesar, Roata alfabetică, Tabele Viginere, Tabela Porta, Codificări matrice, Codificări Bifid, Codificări cu transpoziție, Codul Playfair, Codul Hill)	Prelegere însoţită de materiale în format electronic (PDF)	
6. Algoritmi moderni de criptare Principiile codurilor bloc. Structura codului Feistel	Prelegere însoţită de materiale în format electronic (PDF)	
7-8 Algoritmii: DES, Triplu DES, IDEA, RC5, AES	Prelegere însoţită de materiale în format electronic (PDF)	
9. Criptarea cu chei publice. Algoritmul RSA. Algoritmul Diffie-Hellman	Prelegere însoţită de materiale în format electronic (PDF)	

10. Funcţii hash, semnături digitale.	Prelegere însoţită de materiale în format electronic (PDF)	
11. Administrarea cheilor	Prelegere însoţită de materiale în format electronic (PDF)	
12-13 Tehnici de atac şi apărare în era internetului.	Prelegere însoţită de materiale în format electronic (PDF)	
14. Colocviu -Test		

Bibliografie

1. Nicolae Constantinescu. Criptografie. Ed. Acdemiei Române, 2009
2. Lars Klander - Anti Hacker. Ghidul securităţii reţelelor de calculatoare"- Editura All Educational, 1998
3. Victor V. Patriciu, Ion Bica, Monica Pietroşanu-Ene, Costel Cristea – Securitatea Informatică în Unix şi Internet, Ed. Tehnică, 1998
4. Harold F. Tipton, Micki Krause – Information Security Management Handbook, Auerbach Publications, CRC Press LLc, 2000
5. Matt Curtin - Introduction to Network Security, 1997, http://www.interhack.net/pubs/network-security.pdf
6. Jonathan Knudsen - Java Cryptography, Editura O'Reilly, 1998

8.2. Seminar/laborator	Metode de predare/ invățare	Observații
1. Implementarea de algoritmi de criptare clasici	Expunere. Exemplificare interactivă.	Studentii vor lucra individual sau grupati cate doi pentru realizarea exemplelor de laborator. Pentru temele primite la finalul laboratorului ei vor lucra individual, urmand a le prezenta in cadrul laboratorului imediat urmator.
2. Implementarea de algoritmi de criptare simetrici	Expunere. Exemplificare interactivă.	
3. Implementarea algoritmilor de criptare/decriptare de tip cifruri de substituţie polialfabetice: Cifrul lui Vigenere, Cifrul lui Trithemius	Expunere. Exemplificare interactivă.	
4. AES, algoritmul Rijndael, operaţii algebrice	Expunere. Exemplificare interactivă.	
5. Exemple de implementări pentru algoritmul RSA	Expunere. Exemplificare interactivă.	
6. Implementare algoritmi pentru generarea cheilor publice	Expunere. Exemplificare interactivă.	
7. Prezentare proiect.		

Bibliografie

1. Jonathan Knudsen - Java Cryptography, Editura O'Reilly, 1998

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

Dezvoltarea abilităţilor de exploatare a reţelelor de calculatoare pentru potenţiali utilizatori. Piaţa muncii locală, naţională sau europeană este în permanentă căutare de absolvenţi cu bune cunoştinţe în proiectarea unor rețele sigure

10. Evaluare*

Tip de activitate	10.1. Criterii de evaluare**	10.2. Metode de evaluare***	10.3. Pondere din nota finală
10.4. Curs	Lucrare scrisă – test grila si descriptiva- la care se evaluează cunoştinţele teoretice dobândite din tematica cursului şi a laboratorului. Cerinte minime pentru nota 5: Cunoaşterea elementelor fundamentale de teorie. Cerinte pentru nota 10: Cunoaşterea tuturor elementelor de teorie predate la curs şi la laborator. Realizarea tuturor temelor de laborator.	Examen scris	40%
	Activitate laborator: întocmirea unui proiect dintr-o listă pusă la dispoziţia studenţilor (implementarea a 3 algoritmi de criptare dintre care cel puțin unul cu cheie publică	Probă practică pe calculator	40%
10.5. Seminar/laborator	Temele de laborator obligatorii (algoritmi de criptare/decriptare)		20%
10.6. Standard minim de performanţă			
Obţinerea notei minime 5(cinci) atât la evaluarea teoretică (curs) cât şi la cea practică (laborator)			

Data completării Semnătura titularului de curs Semnătura titularului de seminar

27.02.2017

Semnătura directorului de departament
Conf.dr. Victoria Iordan