Universitatea POLITEHNICA din Bucureşti
Facultatea de Stiinte Aplicate

FISA DISCIPLINEI
CRIPTOGRAFIE COMPUTATIONALA (C.C.)

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea POLITEHNICA din Bucureşti
1.2 Facultatea	Facultatea de Stiinte Aplicate
1.3 Departamentul	Departamentul de Metode si Modele Matematice
1.4 Domeniul de studii	Stiinte Ingineresti Aplicate
1.5 Ciclul de studii	MASTER
1.6 Programul de studii/Calificarea	TCSI/ specialist SIG/IT COD.COR 252901

2. Date despre disciplină

2.1 Denumirea disciplinei				CRIPTOGRAFIE COMPUTATIONALA (C.C.)			
2.2 Titularul activităţilor de curs				lector dr. Emil Simion			
2.3 Titularul activităţilor de seminar				lector dr. Emil Simion			
2.4 Anul de studiu	I	2.5 Semestrul	I	2.6 Tipul de evaluare	Examen	2.7 Regimul disciplinei	Obligatoriu

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

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

Distribuţia fondului de timp	ore
Studiul după manual, suport de curs, bibliografie şi notițe	30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate	5
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	10
Tutoriat	0
Examinări	3
Alte activităţi	0

3.7 Total ore studiu individual	34
3.9 Total ore pe semestru	104
3. 10 Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Nu este cazul
4.2 de competenţe	Nu este cazul

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului	Nu este cazul
5.2 de desfăşurare a seminarului	Prezenţa obligatorie la seminarii

6. Competenţe specifice acumulate

Competenţe profesionale	- Dezvoltarea capacităţii de a folosi în domeniul cercetării informatice cunoştinţe de matematică modernă; - Dezvoltarea abilităţilor de folosire a sistemelor de operare UNIX şi

	LINUX; - Dezvoltarea capacităţii de a proiecta şi administra reţele de calculatoare; - Dezvoltarea capacităţii de a proteja serverele de atacurile informatice si de a asigura un trafic informaţional securizat; - Dezvoltarea capacităţii de lucru în echipă; - Dezvoltarea capacităţii de cercetare ştiinţifică; - Aplicarea, în situaţii tipice, a metodelor de proiectare a algoritmilor si protocoalelor criptografice *(criptografia)*, precum si a metodelor de evaluare a acestora *(criptanaliza)*.
Competenţe transversale	Comportarea onorabilă, responsabilă, etică, în spiritul legii pentru a asigura reputaţia profesiei.

7. Obiectivele disciplinei (reieşind din grila de competenţe specifice acumulate)

7.1 Obiectivul general al disciplinei	Aplicarea, în situaţii tipice, a metodelor de proiectarea a algoritmilor si protocoalelor criptografice (criptografia), precum si a metodelor de evaluare a acestora (criptanaliza).
4.2 Obiective specifice	**1. Cunoştinţe teoretice - Cunoaştere şi înţelegere:** Prezentarea tehnicilor şi metodelor criptografice utilizate în protecţia informaţiei în format electronic. Cunoaşterea principiilor şi metodelor de proiectare a mecanismelor criptografice. **2. Deprinderi dobândite - Explicare şi interpretare:** Formarea deprinderilor necesare proiectării, implementării şi evaluării tehnicilor criptografice. Identificarea problemelor specifice implementării algoritmilor criptografici în module criptografice (hardware/software). **3. Abilităţi dobândite - Instrumental-aplicative:** Utilizarea instrumentelor de analiză şi testare a mecanismelor criptografice. Implementarea algoritmilor criptografici în diverse soluţii de protecţie a informaţiei. **4. Atitudinale:** Capacitatea de lucru în echipă pentru rezolvarea unor probleme practice. Responsabilitate şi corectitudine în activităţile desfăşurate.

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
1. Sisteme clasice de cifrare. Prezentarea algoritmilor de cifrare clasici, bazaţi pe substituţie şi transpoziţie: algoritmul lui Cezar, substituţii monoalfabetice, algoritmul lui Vigenere, algoritmul Playfair, algoritmul lui Hill, algoritmi de tip transpoziţie, sisteme mixte.	Predarea se bazează pe folosirea videoproiectorului (acoperind	2 ore

2. Sisteme simetrice de cifrare. Sisteme de cifrare de tip bloc: ➢ Prezentarea conceptului de cifrare bloc; ➢ Moduri de lucru ale unui cifru bloc (ECB, CBC, CFB, OFB); ➢ Algoritmul Rijndael (standardul AES FIPS 197, rezultate recente). Sisteme de cifrare de tip flux: ➢ Criterii de proiectare a algoritmilor de tip flux; ➢ Registre de deplasare liniare. Perioada şi complexitatea; Studiu de caz: algoritmii Geffe, Beth-Piper şi A5 (GSM).	funcţia de comunicare şi demonstrativă); metodele de comunicare orală utilizată sunt metoda expozitivă şi metoda problematizării, utilizate frontal. Materialele de curs sunt: notele şi prezentările de curs, culegeri de probleme propuse (teoretice şi cu rezolvare pe calculator). Toate materialele sunt disponibile în format electronic, prin situl cursului.	6 ore
3. Elemente de criptanaliză. Modele de securitate; Categorii de atacuri: ➢ atac cu text clar cunoscut; ➢ complexitatea atacului brut; ➢ compromisul spaţiu timp; ➢ atacul meet in the middle; ➢ criptanaliza liniară; criptanaliza diferenţială.		2 ore
4. Generatoare (pseudo)aleatoare utilizate în criptografie. Conceptul de test statistic. Suita de teste statistice NIST SP 800-22. Prezentarea conceptelor: True random number generators, PUFs (physical(ly) unclonable functions).		2 ore
5. Funcţii de dispersie criptografică. Prezentarea conceptului de funcţie hash. Principii (tipuri de coliziuni, birthday paradox) şi criterii de proiectare.		2 ore
6. Semnătura electronică. Formularea principiilor de proiectare a algoritmilor utilizaţi în procesul de semnare electronică. Precizări cu privire la: watermarks, fingerprints.		2 ore

7. Cripografia asimetrică. Caracteristicile unui sistem de cifrare asimetric. Prezentarea categoriilor de algoritmi asimetrici: ➢ Algoritmi de tip rucsac; ➢ Algoritmi asimetrici bazaţi pe problema factorizării: RSA. Condiţii de utilizare pentru cifrare/semnare corectă; ➢ Algoritmi asimetrici bazaţi pe problema logaritmului discret. Algoritmul ElGamal. Algoritmul DSA. Curbe eliptice: ➢ Prezentarea conceptului de curbă eliptică; ➢ Algoritmul EC-ElGamal, algoritmul Menezes- Vanstone; ECDSA.		6 ore
8. Protocoale criptografice. Prezentarea categorilor de protocoale criptografice: ➢ Scheme de partajare a secretelor: Brickell, Shamir; ➢ Protocoale de autemtificare mutuală; ➢ Protocoale de vot electronic; Protocolale de management a cheilor: Blum, Diffie – Hellman, Kerberos.		4 ore
9. Managementul cheilor criptografice. Principii şi coduri de bune practici în implementarea managementului cheilor criptografice.		2 ore

Bibliografie

1. M. Andraşiu, D. Naccache, E. Simion, Gh. Simion, *Operational research, Probability and Cryptology. Applications*, Military Technical Academy, 2011, ISBN 978-973-640-208-1.
2. Pooya Farshim, E. Simion, *Innovative Security Solutions for Information Technology and Communications*, Springer Verlag, LNCS 10543, 2017, ISBN: 978-3-319-69283-8, DOI: 10.1007/978-3-319-69284-5.
3. A.J. Menezes, P. Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1999.
4. D. Naccache, E. Simion ş.a, *Criptografie şi Securitatea Informaţiei. Aplicaţii*, MATRIXROM, 2011.
5. B. Schneier, *Applied Criptography*, Second Edition, John Wiley & Sons, 1996.
6. E. Simion, V. Preda şi A. Popescu, *Criptanaliza. Rezultate şi Tehnici Matematice*, Ed. Univ. Buc., ISBN 973575975-6, 2004.
7. D. Stinton, *Cryptography, Theory and Practice*, Chapman &Hall/CRC, Third Edition, 2006.
8. W. Stalings, *Cryptography and Network Security: Principles and Practice (6th Edition)*- 6th Edition, 2013.
9. FIPS 140-2, *Security Requirements for Cryptographic Modules*, 2001.
10. National Institute of Standards and Technologies, SP 800-22, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, 2010.

11. www.cryptool.org
12. https://cryptopals.com/

8.2 Laborator	Metode de predare	Observaţii
1. Unelte de analiză criptografică: CrypTool.	Predarea se bazează pe folosirea videoproiectorului (acoperind funcţia de comunicare şi demonstrativă); metoda de comunicare orală utilizată este metoda problematizării,utilizate frontal. Materialele didactice sunt postate pe platforma educaţională a UPB.	2 ore
2. Aplicaţii privind algoritmii de cifrare clasici: Cezar, Vigenere, Playfair, Hill, transpoziţii, sisteme mixte.		2 ore
3. Exemplificarea funcţiilor criptografice utilizate de algoritmul RIJNDAEL.		2 ore
4. Criptografie asimetrică: exemplificarea computaţională a algoritmilor de tip rucsac, RSA, ElGamal, DSA.		4 ore
5. Criptografie asimetrică: EC (curbe eliptice), exemplificarea computaţională a algoritmilor Menezes-Vanstone, ECElGamal, ECDSA.		4 ore
6. Utilitare de analiză statistică utilizate în criptologie: SP 800-22.		2 ore
7. Standarde criptografice: PKCS.		2 ore
8. Infrastructuri cu chei publice (PKI).		2 ore
9. Elemente privind evaluarea modulelor criptografice. Prezentarea standardelor FIPS 140-2 (ISO 19790).		2 ore
10. Securitatea poştei electronice. Studiu de caz: Pretty Good Privacy.		2 ore
11. Analiza implementării protocoalelor criptografice. Studiu de caz: Protocolul OpenSSL.		2 ore
12. Standardizarea NIST privind primitivele criptografice (Cryptographic ToolKit).		2 ore

Bibliografie

1. M. Andraşiu, D. Naccache, E. Simion, Gh. Simion, *Operational research, Probability and Cryptology. Applications*, Military Technical Academy, 2011, ISBN 978-973-640-208-1.
2. A.J. Menezes, P. Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1999.
3. D. Naccache, E. Simion ş.a, *Criptografie şi Securitatea Informaţiei. Aplicaţii*, MATRIXROM, 2011.
4. E. Simion, V. Preda şi A. Popescu, *Criptanaliza. Rezultate şi Tehnici Matematice*, Ed. Univ. Buc., ISBN 973575975-6, 2004.
5. D. Stinton, *Cryptography, Theory and Practice*, Chapman &Hall/CRC, Third Edition, 2006.
6. W. Stalings, *Cryptography and Network Security: Principles and Practice (6th Edition)*- 6th Edition, 2013.
7. FIPS 140-2, *Security Requirements for Cryptographic Modules*, 2001.
8. National Institute of Standards and Technologies, SP 800-22, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, 2010.
9. www.cryptool.org
10. https://cryptopals.com/

8.3 Seminar	Metode de predare	Observaţii
Seminarul urmareste indreaproape continutul laboratorului abordeaza componenta teoretica a notiunilor necesare abordarii aplicative.	Predarea se bazează pe folosirea videoproiectorului (acoperind funcţia de comunicare şi demonstrativă); metoda de comunicare orală utilizată este metoda problematizării,utilizate frontal. Materialele didactice sunt postate pe platforma educaţională a UPB.	14 ore

Bibliografie

1. M. Andraşiu, D. Naccache, E. Simion, Gh. Simion, *Operational research, Probability and Cryptology. Applications*, Military Technical Academy, 2011, ISBN 978-973-640-208-1.
2. A.J. Menezes, P. Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1999.
3. D. Naccache, E. Simion ş.a, *Criptografie şi Securitatea Informaţiei. Aplicaţii*, MATRIXROM, 2011.
4. E. Simion, V. Preda şi A. Popescu, *Criptanaliza. Rezultate şi Tehnici Matematice*, Ed. Univ. Buc., ISBN 973575975-6, 2004.
5. D. Stinton, *Cryptography, Theory and Practice*, Chapman &Hall/CRC, Third Edition, 2006.
6. W. Stalings, *Cryptography and Network Security: Principles and Practice (6th Edition)*- 6th Edition, 2013.
7. FIPS 140-2, *Security Requirements for Cryptographic Modules*, 2001.
8. National Institute of Standards and Technologies, SP 800-22, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, 2010.
9. www.cryptool.org

https://cryptopals.com/

9. Coroborarea conţinuturilor disciplinei cu asteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale si angajatori reprezentativi din domeniul aferent programului

Intrând progresiv în era informaţiei, societăţile industrializate se găsesc în faţa unui paradox: pe de o parte, puterea şi influenţa Europei şi a Americii de Nord au crescut semnificativ, în principal datorită măiestriei modalităţilor prin care se controlează fluxurile de informaţii, precum şi valorii crescute a datelor procesate. Pe de altă parte, după cum au demonstrat-o deja criza Wikileaks, viermele Stuxnet, sau virusul WannaCry, apar noi ameninţări şi vulnerabilităţi care fac ca dependenţa noastră de sistemele informaţionale să fie crucială. De aceea, dezvoltarea atacurilor cibernetice, precum şi disponibilitatea online a instrumentelor utilizate în activitatea de piraterie conduce la obiective strategice importante şi cultivă necesitatea de a pregăti experţi pentru acest domeniu. Mediul în care trăim se schimbă în ritm alert, această evoluţie fiind rezultatul progresului în domeniul tehnologiilor informaţionale, precum şi al matematicii. **Cursul are ca obiectiv dobindirea competentelor necesare conceperii, implementarii si evaluarii primitivelor criptografice utilizate in sistemele de protectie a informatiei in format electronic**.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în nota finală
10.4 Curs	-cunoaşterea noţiunilor teoretice fundamentale; - cunoaşterea modului de	Examen parţial, cu posibilitate de degrevare a materiei, pondere 33%.	66%

	aplicare a teoriei la probleme specifice; - analiza diferenţială a tehnicilor şi metodelor teoretice.	Examen final, pondere 33%	
10.5 Laborator/Seminar	- cunoasterea aplicarii, pe exemple concrete a elementelor teoretice exemplificate in cadrul cursului.	Notare în timpul semestrului, teme de casă.	33%
10.6 Standard minim de performanţă			
Cunoaşterea noţiunilor teoretice de bază prezentate la curs şi rezolvarea unor probleme tip.			

Data completării
01.09.2018

Semnătura titularului de curs
lector dr. Emil Simion

Semnătura titularului de aplicaţii
lector dr. Emil Simion

Data avizării în departament
.....

Semnătura sefului de department
prof. dr. Mircea Olteanu

Responsabil program master
lector dr. Emil Simion