FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	**Universitatea Națională de Știință și Tehnologie POLITEHNICA București**
1.2 Facultatea	**Științe Aplicate**
1.3 Departamentul	Metode si Modele Matematice
1.4 Domeniul de studii universitare	Științe inginerești aplicate
1.5 Programul de studii universitare	Matematică și informatică aplicată în inginerie
1.6 Ciclul de studii universitare	Licență
1.7 Limba de predare	Română
1.8 Locația geografică de desfășurare a studiilor	București

2. Date despre disciplină

2.1 Denumirea disciplinei/ Course title (ro) (en)	Criptografie **Cryptography**						
2.2 Titularul/ii activităților de curs	Conf.dr.Petrescu-Nita Alina Claudia						
2.3 Titularul/ii activităților de seminar / laborator/proiect	Conf.dr.Petrescu-Nita Alina Claudia						
2.4 Anul de studiu	4	2.5 Semestrul/	I	2.6. Tipul de evaluare	E	2.7 Statutul disciplinei	Ob
2.8 Categoria formativă	DS	2.9 Codul disciplinei					

3. Timpul total (ore pe semestru al activităților didactice

3.1 Număr de ore pe săptămână	3	Din care: 3.2 curs	2	3.3 seminar/laborator/proiect	1
3.4 Total ore din planul de învățământ	42	Din care: 3.5 curs/	28	3.6 seminar/laborator/proiect	14

Distribuția fondului de timp:	ore
Studiul după manual, suport de curs, bibliografie și notițe Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii și eseuri	32
Tutorat	2
Examinări	4
Alte activități (dacă există):	0

3.7 Total ore studiu individual	**38**
3.8 Total ore pe semestru	**100**[1]

[1] *Se va calcula ținând cont că se acordă un credit pentru volumul de muncă care îi revine unui student cu frecvență la zi pentru a echivala 25 de ore de pregătire pentru dobândirea rezultatelor învățării.*

3.9 Numărul de credite	**4**[2]

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Nu este cazul
4.2 de rezultate ale învățării	Cunoștințe de bază de matematică (algebră, teoria numerelor, probabilități). Cunoștințe fundamentale de informatică și structuri de date. Abilități de programare într-un limbaj (C/C++/Java/Python). Noțiuni introductive despre rețele și sisteme de operare

5. Condiții necesare pentru desfășurarea optimă a activităților didactice (acolo unde este cazul)/

5.1 de desfășurare a cursului	Sală de curs dotată cu videoproiector.
5.2 de desfășurare a seminarului/laboratorului/ proiectului	Laborator dotat cu calculatoare prevăzute cu software specializat desfășurării aplicațiilor cryptool, matlab

6. Obiectiv general

Cursul își propune să ofere studenților cunoștințe fundamentale și aplicative privind principiile, metodele și tehnicile criptografiei moderne, necesare pentru înțelegerea și asigurarea securității informației în sisteme informatice și de comunicații. Se urmărește dezvoltarea capacității de a înțelege conceptele teoretice de bază, precum și de a aplica algoritmi și protocoale criptografice pentru protejarea datelor, autentificare și confidențialitate în diverse contexte tehnologice.

7. Rezultatele învățării

Cunoștințe	• explicarea principiilor fundamentale ale criptografiei clasice și moderne; • înțelegerea și diferențierea algoritmilor de criptare simetrică și asimetrică; • cunoașterea funcțiilor hash, a mecanismelor de semnătură digitală și a certificatelor digitale; • înțelegerea arhitecturii și a rolului protocoalelor criptografice în securizarea comunicațiilor și a datelor; • familiarizarea cu principalele atacuri și metode de evaluare a securității schemelor criptografice.

[2] Se va completa conform planului de învățământ.

Abilități	• aplicarea algoritmilor criptografici pentru asigurarea confidențialității, integrității și autenticității datelor; • implementarea și testarea protocoalelor criptografice în aplicații software și rețele de calculatoare; • utilizarea semnăturilor digitale și a mecanismelor de autentificare în scenarii practice; • analiza și compararea nivelului de securitate al diverselor soluții criptografice; • rezolvarea de probleme și studii de caz prin integrarea metodelor criptografice adecvate.
Responsabilitate și autonomie	• selectarea critică și justificată a soluțiilor criptografice potrivite în funcție de contextul tehnologic; • asumarea responsabilității privind protecția și securitatea informațiilor la nivel individual și organizațional; • respectarea normelor, standardelor și bunelor practici în domeniul securității informației; • capacitatea de a lucra independent în proiecte de securitate, dar și de a colabora eficient în echipe multidisciplinare; • dezvoltarea unei atitudini proactive față de identificarea riscurilor și aplicarea măsurilor de securitate.

8. Metode de predare

- **Prelegeri** pentru prezentarea conceptelor teoretice fundamentale și a algoritmilor criptografici;
- **Explicații și demonstrații** pe tablă și prin prezentări multimedia pentru ilustrarea metodelor și protocoalelor;
- **Studii de caz** privind aplicarea criptografiei în securitatea comunicațiilor și a sistemelor informatice;
- **Exerciții și aplicații practice** realizate în laborator, folosind limbaje de programare și instrumente software dedicate;
- **Învățare bazată pe proiect** pentru dezvoltarea și testarea unor soluții criptografice concrete;
- **Discuții interactive și dezbateri** pentru stimularea gândirii critice și a capacității de analiză;
- **Învățare individuală asistată** prin recomandarea de bibliografie și resurse online.
-

9. Conținuturi

CURS		
Capitolul	**Conținutul**	**Nr. ore**
I	1. Preliminarii 1.1. Grupuri 1.2. Corpuri finite . Extinderi Galois. 1.3. Elemente de Teoria Numerelor	**4**
II	Sisteme clasice de cifrare. Prezentarea algoritmilor de cifrare clasici, bazaţi pe substituţie şi transpoziţie: algoritmul lui Cezar, Cifrul afin, substituţii monoalfabetice,	**2**

	algoritmul lui Vigenere, algoritmul Playfair, algoritmul lui Hill, algoritmi de tip transpoziţie, Cifru *Polybius*, sisteme mixte.	
III	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;	**2**
IV	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;	**4**
V	Semnaturi digitale (RSA,Al Gamal, Standardul DSS)	**2**
	Total:	**14**

Bibliografie:

1. Alina Nita, R.Ursianu, Ana Nita, S. Balea ; Algebra liniara si Geometrie,Ed. Printech, Bucuresti, 2003
2. Atanasiu, Securitatea Informatiei, vol I (Criptografie), Ed. Infodata, Cluj, 2005
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. 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. 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. Gherghe, D.Popescu, Criptografie, Coduri, Algoritmi, Ed. Universitatea Bucuresti, 2005.
11. J.Hoffstein,J.Pipher, J.H.Silverman , An introduction to mathematical Cryptography , Springer Verlag, 2008
12. Zgureanu Aurelian – Note de Curs- Criptarea Și Securitatea Informaţiei, Chisinau 2013

LABORATOR/ SEMINAR/PROIECT		
Nr. crt.	**Conținutul**	**Nr. ore**
1.	Aplicaţii privind algoritmii de cifrare clasici: Cezar, Vigenere, Playfair, Hill, transpoziţii, sisteme mixte, Cifru *Polybius*	1

2.	Moduri de lucru ale unui cifru bloc (ECB, CBC, CFB, OFB);	1
3.	Criptografie asimetrică: exemplificarea computaţională a algoritmilor de tip rucsac, RSA, ElGamal, DSA.	3
4.	Criptografie asimetrică: EC (curbe eliptice), exemplificarea computaţională a algoritmilorMenezes-Vanstone, ECElGamal, ECDSA.	2
	Total:	**7**

Bibliografie:

1. Alina Nita, R.Ursianu, Ana Nita, S. Balea ; Algebra liniara si Geometrie,Ed. Printech, Bucuresti, 2003
2. A. Atanasiu, Securitatea Informatiei, vol I (Criptografie), Ed. Infodata, Cluj, 2005
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. C. Gherghe, D.Popescu, Criptografie, Coduri, Algoritmi, Ed. Universitatea Bucuresti, 2005.
11. J.Hoffstein,J.Pipher, J.H.Silverman , An introduction to mathematical Cryptography , Springer Verlag, 2008
12. www.cryptool.org
13. https://cryptopals.com/

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	cunoaşterea noţiunilor teoretice fundamentale; - cunoaşterea modului de aplicare a teoriei la probleme specifice; - analiza diferenţială a tehnicilor şi metodelor teoretice.	Examen parţial, cu posibilitate de degrevare a materiei, pondere 30%. Examen final, pondere 50%	80%
10.5 Seminar/laborator/proiect	cunoasterea aplicarii, pe exemple concrete a elementelor teoretice exemplificate in cadrul cursului.	Notare în timpul semestrului, teme de casă.	20%
10.6 Condiții de promovare			

• Îndeplinirea obligațiilor caracteristice activității de laborator: predarea de laborator realizat și susținerea acestuia; • Pentru promovarea disciplinei, studentul trebuie sa obțină cel puțin 50% din punctajul total.

Data completării	Titular de curs	Titular(ii) de aplicații
	Conf. dr. Petrescu-Nita Alina	
Data avizării în departament	Director de departament Lect Dr Alexandru Negrescu	
Data aprobării în Consiliul Facultății 26.09.2025	Decan Alina Claudia PETRESCU-NIȚĂ	