**Titulli i lëndës: Siguria e të dhënave**

|  |  |  |  |
| --- | --- | --- | --- |
| **Informatat themelore për lëndën** | | | |
| **Njësia akademike:** | Fakulteti i Shkencave Matemaike Natyrore (FSHMN), Departamenti i Matematikës | | |
| **Titulli i lëndës:** | Siguria e të dhënave | | |
| **Niveli:** | Bachelor (Programi Shkencë kompjuterike) | | |
| **Statusi i lëndës:** | Obligative | | |
| **Viti i studimeve:** | Viti i dytë / Semestri i katërt | | |
| **Numri i orëve në javë:** | 2+2 | | |
| **Kreditë ECTS:** | 6 | | |
| **Koha / Vendi:** | N/A, Departamenti i Matematikës | | |
| **Mësimdhënësi:** | Dr. Eliot Bytyçi | | |
| **Të dhënat kontaktuese:** | eliot.bytyci@uni-pr.edu | | |
|  | | | |
| **Përshkrimi i lëndës:** | Në këtë kurs temat përfshijnë hyrje teorike të kriptografisë, kriptosistemet me çelës simetrik, kriptosistemet me çelës asimetrik, funksionet njëkahëshe, nënshkrimet digjitale, skema sekrete dhe sfond matematikor të nevojshëm për t’i sqaruar ato. | | |
| **Qëllimet e lëndës:** | Do të mësojnë zbatimin e teorisë për sigurinë e të dhënave në botën në sistemet reale dhe abstrakte duke përfshirë edhe njohjen nga kërcënimet e mundshme të konfidencialitetit dhe integritetit. Do të mësojnë për algoritmat e thjeshtë të përdorur që nga koha e romakëve, algorimtat simetrik DES dhe AES, algoritmat asimetrik RSA, EL-Gamal, funksionet njëkahëshe SHA-1, SHA-2 dhe MD5 si dhe do të kuptojnë aspektet e llojllojshme dhe multidisiplinare në fushën e sigurisë së të dhënave. | | |
| **Rezultatet e pritshme të nxënies:** | Pas përfundimit të këtij kursi (lënde) studenti është i aftë që:   * të zotërojë njohuritë bazike për sigurinë e të dhënave, * të jetë në gjendje të elaborojë për pikat e forta dhe pikat e dobëta, si dhe kufizimet e teorive kryesore për sigurinë e të dhënave, * të vlerësojë trendet aktuale në sigurinë e të dhënave, * të kuptojë zhvillimin historik të sigurisë së të dhënave dhe çeshtjet që ndërlidhen me të, * të analizojë situata specifike dhe të propozojë zgjidhje adekuate për të garantuar sigurinë e sistemeve kompjuterike, * të kuptojë zbatimin e teorisë për sigurinë e të dhënave në botën në sistemet reale, * të jetë në gjendje t’i kuptojë aspektet e llojllojshme dhe multidisiplinare në fushën e sigurisë së të dhënave. | | |
|  | | | |
| **Ngarkesa e studentit (duhet të jetë në përputhje me Rezultatet e Nxënies të studentit)** | | | |
| **Aktiviteti** | **Orë mësimore** | **Ditë/Javë** | **Gjithsej** |
| Ligjëratat | 2 | 15 | 30 |
| Teori/Punë në laborator/Ushtrime | 2 | 15 | 30 |
| Punë praktike | - | - | - |
| Përgatitje për test intermediar | - | - | - |
| Konsultime me mësimdhënësin | - | - | - |
| Puna në terren | - | - | - |
| Testi, punimi seminarik | 1 | 5 | 5 |
| Detyrë shtëpie | 2 | 15 | 30 |
| Mësimi individual (në bibliotekë apo në shtëpi) | 2 | 15 | 30 |
| Përgatitja për provimin final | 1 | 15 | 15 |
| Koha e vlerësimit (testi, kuizi, provimi final) | 1 | 10 | 10 |
| Projektet, prezantimet, detyrat, etj. | - | - | - |
| Shto ndonjë aktivitet tjetër që nuk është në tabelë... | - | - | - |
| **Total** |  |  | **150** |
|  | | | |
| **Metodat e mësimdhënies:** | Kjo lëndë shpjegohet përmes ligjëratave, ushtrimeve teorike, ushtrimeve numerike, detyrave të shtëpisë dhe punimi seminarik (ku parashihet të realizohet me përcjellje të vazhdueshme të asistentit dhe ligjëruesit të lëndës). | | |
| **Metodat e vlerësimit:** | Detyrat: 30 pikë,  Seminari: 15 pikë,  Testi përfundimtar: 55 pikë.  Vlerësimi:   |  |  | | --- | --- | | **Pikët** | **Nota** | | **<50** | **5** | | **>=50 dhe <60** | **6** | | **>=60 dhe <70** | **7** | | **>-70 dhe <80** | **8** | | **>=80 dhe <90** | **9** | | **>=90** | **10** |   Pikët nga detyrat dhe punimi seminarik që janë arritur nga studenti gjatë vijimit të kursit do të vlejnë për çdo afat. Pra studenti i nënshtrohet gjithmonë provimit me maksimum 55 pikë. | | |
|  | | | |
| **Literatura primare:** | 1. Understanding Cryptography A Textbook for Students and Practitioners*,*Christof Paar, Jan Pelzl 2010 Springer | | |
| **Literatura shtesë:** | 1. Cryptography and Network Security - Principles and Practice, William Stallings, Pearson, 2011 | | |

|  |  |
| --- | --- |
| **Hartimi i planit mësimor** | |
| **Java** | **Titulli i ligjëratës** |
| ***Java 1:*** | Hyrje në sigurinë e të dhënave |
| ***Java 2:*** | Shifrimet rrjedhëse |
| ***Java 3*:** | DES |
| ***Java 4:*** | AES |
| ***Java 5:*** | Më shumë rreth shifrimeve me bllok |
| ***Java 6*:** | Vlerësimi i detyrës së parë |
| ***Java 7:*** | Kriptografia me çelës publik |
| ***Java 8:*** | Kriptosistemi RSA |
| ***Java 9:*** | Logaritmi diskret |
| ***Java 10:*** | ECC |
| ***Java 11*:** | Nënshkrimet shifrore |
| ***Java 12*:** | Hash funksionet |
| ***Java 13*:** | Vlerësimi i detyrës së dytë |
| ***Java 14*:** | MAC |
| ***Java 15*:** | Vlerësimi i punimit seminarik |

|  |
| --- |
| **Politikat akademike dhe Kodi i Sjelljes** |
| *Vijueshmëria e ligjëratave dhe ushtrimeve laboratorike është obligative.* |