**Titulli i lëndës: Teoria e kodimit dhe kriptografia**

|  |  |  |  |
| --- | --- | --- | --- |
| **Informatat themelore për lëndën** | | | |
| **Njësia akademike:** | Fakulteti i Shkencave Matemaike Natyrore (FSHMN), Departamenti i Matematikës | | |
| **Titulli i lëndës:** | Bazat e të dhënave | | |
| **Niveli:** | Bachelor (Programi Shkencë kompjuterike) | | |
| **Statusi i lëndës:** | Zgjedhore | | |
| **Viti i studimeve:** | Viti i tretë / Semestri i pestë | | |
| **Numri i orëve në javë:** | 2+2 | | |
| **Kreditë ECTS:** | 4 | | |
| **Koha / Vendi:** | N/A, Departamenti i Matematikës | | |
| **Mësimdhënësi:** | Msc. Artan Berisha | | |
| **Të dhënat kontaktuese:** | artan.berisha@uni-pr.edu | | |
|  | | | |
| **Përshkrimi i lëndës:** | Ky kurs përmban njohuri themelore të Kriptografisë dhe të kodeve për korrektimin (korigjimit) e gabimeve gjate transmetimit të të dhënave. Do të fillohet nga algoritma që janë përdorë nga koha e perandorisë Romake (Kodimi i Cezarit), pastaj transponimi afin i shifrave, kodimi matricor, algoritmi i Euklidit, sita e Eratostenit, algorimat me çelës simetrik (DES, AES), kodimi sipas Rabinit, algoritmat me çelës asimetrik (RSA, Pohling-Hellman, El-Gamal), funksionet njëkahëshe (SHA-1, SHA-2, MD5), nënshkrimet digjitale, kodimi sipas Huffman-it, kodi i Hamming-ut. | | |
| **Qëllimet e lëndës:** | Qëllimet themelore të këtij kursi janë njohuritë mbi kuptimet themelore të teorisë së kodimit dhe të kriptografisë: si p.sh. përdorimi i çelësave privat dhe publik, kriptoanalizë dhe teori të numrave, algoritmet DES dhe RSA si dhe kodeve për korrektimin (korigjimit) e gabimeve. | | |
| **Rezultatet e pritshme të nxënies:** | Pas përfundimit të këtij kursi (lënde) studenti është i aftë që:   * Që të ketë njohuri në fushën e teorisë së kodimit dhe të kriptografisë, * Të dijë për kodimin sipas Hammingut dhe Huffman-it, * Të dijë konceptet themelore mbi përdorimin e çelësave privat dhe publik * Të dijë për algoritmat simetrik (DES, AES) * Të dijë për algoritmat asimetrik (RSA, Pohling-Hellman, El-Gamal) | | |
|  | | | |
| **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 | 15 | 15 |
| Detyrë shtëpie | 1 | 15 | 15 |
| Mësimi individual (në bibliotekë apo në shtëpi) | 1 | 15 | 15 |
| Përgatitja për provimin final | - | - | - |
| Koha e vlerësimit (testi, kuizi, provimi final) | - | - | - |
| Projektet, prezantimet, detyrat, etj. | - | - | - |
| Shto ndonjë aktivitet tjetër që nuk është në tabelë... | - | - | - |
| **Total** |  |  | **105** |
|  | | | |
| **Metodat e mësimdhënies:** | Kjo lëndë shpjegohet përmes ligjëratave, ushtrimeve teorike, detyrave te shtëpisë (të cilat parashihen të realizohen me përcjellje të vazhdueshme të asistentit dhe ligjëruesit të lëndës), punimit seminarik dhe testit përfundimtar. | | |
| **Metodat e vlerësimit:** | Detyra e parë: 10 pikë,  Detyra e dytë: 10 pikë,  Detyra e tretë: 10 pikë,  Seminari: 15 pikë,  Testi përfundimtar: 55 pikë.  Kusht është që në testin përfundimtar studenti të arrijë së paku 27 pikë, pastaj mbledhen të gjitha pikët dhe kriteret për vlerësim janë si mëposhtë:   |  |  | | --- | --- | | **Pikët** | **Nota** | | **<50** | **5** | | **>=50 dhe <60** | **6** | | **>=60 dhe <70** | **7** | | **>-70 dhe <80** | **8** | | **>=80 dhe <90** | **9** | | **>=90** | **10** |   Pikët e detyrave dhe seminarit 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:** | * Christof Paar, Jan Pelzl, Understanding Cryptography, A Textbook for Students and Practitioners, Springer 2010, * Hamming, Richard: *Coding and Information Theory,* SecundEdition, Prentice Hall, 1986, * Jiri Adamek, Foundations of Coding: Theory and Applications of Error-Correcting Codes with an Introduction to Cryptography and Information Theory, Wiley 2011. | | |
| **Literatura shtesë:** | * 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*:** | Kriptografia me çelës publik |
| ***Java 7:*** | Kriptosistemi RSA |
| ***Java 8:*** | Logaritmi diskret |
| ***Java 9:*** | Nënshkrimet shifrore |
| ***Java 10:*** | Hash funksionet dhe MAC |
| ***Java 11*:** | Korrektimi i gabimeve të kodimit |
| ***Java 12*:** | Kodet lineare |
| ***Java 13:*** | Kodi i Hamming-ut |
| ***Java 14:*** | BCH kodet |
| ***Java 15:*** | Kodi I Huffman-it |

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