

…………………………………………………………………………………………………………………………………………………………

**BSc Shkenca Kompjuterike dhe Inxhinieri**

**Sillabus**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lënda** | Hyrje në Sigurinë e të Dhënave | | | |
| Llojj | Semestri | ECTS | Kodi |
| OBLIGATIVE (O) | 4 |  |  |
| **Ligjeruesi i lëndës** | Blerton Abazi  Besnik Qehaja | | | |
| **Qëllimet dhe Objektivat** | Qëllimi i këtij kursi është të japë konceptet themelore të kriptografisë dhe të njoftojë me studentët sistemet kriptografike klasike private. Kursi shërben gjithashtu si një hyrje për studentët të cilët janë të interesuar të bindin hulumtimet në kriptografi. Pas marrjes së kursit, studentët duhet të kenë një pasqyrë të disa prej kriptosistemev klasike, të cilat janë në përdorim. | | | |
| **Rezultatet e pritshme** | Deri në përfundimin e këtij kursi, studentët duhet të jenë në gjendje të njohin:  Kuptimi themelor i mjeteve të sigurisë së të dhënave të tilla si mekanizmat e kontrollit të qasjes, mjetet e autentikimit dhe konstruktet kriptografike.   * Përcaktojnë nivelet e mbrojtjes dhe reagimit ndaj incidenteve të sigurisë * Hartojnë një sistemi të qëndrueshëm dhe të arsyeshëm të sigurisë së informacionit, me karakteristika të përshtatshme të zbulimit dhe raportimit të ndërhyrjeve * Identifikon spektrin e aktiviteteve të sigurisë, metodave, metodologjive dhe procedurave * Kryen inspektimin dhe mbrojtjen e pasurive të informacionit * Zbulon dhe reagoni ndaj kërcënimeve ndaj pasurive të informacionit * Shqyrton procedurat para dhe pas incidentit * Siguron përgjigje teknike dhe menaxheriale * Prezanton një pasqyrë të planifikimit të sigurisë së informacionit dhe funksioneve të personelit | | | |
| **Përmbajtja** | **Plani javor** | | | **Java** |
| Një Përmbledhje dhe Hyrje në Sigurinë e Informacionit | | | 1 |
| Kriptografi klasike | | | 2 |
| Kritposistemeve Simetrike, llojet e sulmeve | | | 3 |
| Blloku Ciphers | | | 4 |
| Funksionet Hash | | | 5 |
| Arti i sigurimit të Integritetit të të Dhënave, Algoritmeve Hash dhe Nënshkrimit Dixhital | | | 6 |
| Kontrolli i Qasjes | | | 7 |
| Kundërmasat për të siguruar disponueshmërinë | | | 8 |
| Masat përçarëse të sigurisë së sigurisë së të dhënave | | | 9 |
| Malware dhe Kodi i keq | | | 10 |
| Domains cybersecurity | | | 11 |
| Domains cybersecurity | | | 12 |
| Prezantimet | | | 13 |
| Konsultime | | | 14 |
|  | | |  |
| Provimi perfundimtar | | | 15 |
| **Metodat e mësimdhënies** | **Aktiviteti** | | | **Pesha (%)** |
| 1. Ligjerata | | | 60% |
| 1. Projekti Seminar | | | 20% |
| 1. Vizita studimore | | | 10% |
| 1. Mysafir nga Industria | | | 10% |
|  | | |  |
| **Metodat e vlerësimit** | **Aktiviteti i vlerësimit** | **Numri** | **Java** | **Pesha (%)** |
| 1. Vijueshmeria ne ligjerata |  |  | 10% |
| 1. Prezantimet e Projekteve |  |  | 20% |
| 1. Provim përfundimtar |  |  | 60% |
| 1. Kuizet | 3 | 4,8,12 | 10% |
|  |  |  |  |
| **Burimet dhe mjetet e konretizimit** | **Mjetet** | | | **Numri** |
| 1. Klase (e.g) | | |  |
| 1. Laborator (e.g) | | |  |
| 1. Moodle | | |  |
| 1. Projektor | | |  |
| **Ngarkesa dhe aktivitetet** | **Lloji i aktivitetit** | | **Orë javore** | **Ngarkesa total** |
| 1. Ligjerata | | 2 | 24 |
| 1. Seminare | | 0 | 0 |
| 1. Laborator | | 0 | 0 |
| 1. Praktike ne industry | | 2 | 4 |
| 1. Mesim I pavarur | | 4 | 90 |
| 1. Provime | | 2 | 4 |
| **Literatura/Referencat** | Text Book   1. W. Stallings, “Cryptography and Network Security”, Fourth Edition Prentice Hall 2. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996. http://www.cacr.math.uwaterloo.ca/hac/ 3. Douglas Stinson, "Cryptography: Theory and Practice", CRC Press, 2002. 4. Jonathan Katz & Yehuda Lindell "Introduction to Modern Cryptography". 5. https://www.crcpress.com/Introduction-to-Modern-Cryptography-Second-Edition/Katz-Lindell/9781466570269   Reference Book   1. Kaufman, Perlman, and Speciner, “Network Security: Private Communication in a Public World”, Second Edition, Prentice Hall PTR, 2002, ISBN 0130460192. 2. B. Schneier, “Applied Cryptography” ,2nd edition, John Wiley and Sons, Inc, New York, 1996. 3. Neal Koblitz, "A Course in Number Theory and Crytography", Graduate Text in Mathematics, Springer Verlag, 1987. 4. Johannes Buchmann, "Introduction to Cryptography", Springer-Verlag, New York, 2001. | | | |
| **Kontakti** | Blerton Abazi [blerton.abazi@ubt-uni.net](mailto:blerton.abazi@ubt-uni.net)  Besnik Qehaja besnik.qehaja@ubt-uni.net | | | |