|  |  |
| --- | --- |
| Óbudai EgyetemBánki Donát Gépész és Biztonságtechnikai Mérnöki Kar  | Biztonságtudományi és Kibervédelmi Intézet  |
| **Tantárgy címe és kódja:** | **Információbiztonság alapjai BBXIB13BNF**  | **Kreditérték:** | 4 |
| Nappali munkarend | 2 | tanév | 1 | félév  |
| **Szakok melyeken a tárgyat oktatják:** | **Biztonságtechnikai mérnök szak** |
| **Tantárgyfelelős oktató:** | Dr. habil. Kiss Gábor | **Oktatók:** | Dr. habil. Kiss Gábor |
| **Előtanulmányi feltételek (kóddal):** |  |
| **Heti óraszámok** |
| Előadás: | 2 | Tantermi gyak.:  | 0 | Laborgyakorlat:  | 2 | Konzultáció: |  |
| **Félévzárás módja:** | Évközi jegy |  (Válasszon) |
| ***Online konzultáció*** *(amennyiben szükséges):* | *… (BBB link)* |
| **Oktatási cél**: | *A tantárgy oktatásának célja, hogy a hallgatók megismerjék az információvédelem történelmi szakaszait és betekintést nyerjenek a múltban alkalmazott technikákba, világosan lássák azok sérülékenységét, biztonsági szintjét, hiányosságaikat, feltörési módjait. A laborfoglalkozásokon Python nyelven fejlesztjük ki az egyes szteganográfiai, kriptográfiai eljárásokat megvalósító programot. A félév sikeres teljesítése esetén a hallgatók könnyebben lesznek képesek a mai titkosítási eljárások, rendszerek működését elsajátítani a szakirányú képzésen.* |
| **Ütemezés**  |
| Oktatási hét | **Témakörök** |
| 1. | Szteganográfiai módszerek a múltban |
| 2. | Modern szteganográfia, adatrejtés TXT, DOCX fájlba |
| 3. | Modern szteganográfia, adatrejtés kép-, illetve zenefájlokba (LSB technika) |
| 4. | Kriptográfia, mint az adatvédelem új eszköze |
| 5. | Monoalfabetikus kódolási módszerek |
| 6. | Monoalfabetikus kódolás törése, arab kriptográfusok, gyakoriságelemzés |
| 7. | Nomenklatorok, homofónikus kód |
| 8. | Biliterális, polyliterális kódolás. |
| 9. | Vigenére kódolás és törése |
| 10. | Playfair kódolás, bifid, trifid kód, nihilista kódolás, négy négyzet kódolás |
| 11. | Jefferson-henger, ADFGVX kódolás |
| 12. | Enigma felépítése, működése, kódolásának törése I. Rejewski |
| 13. | Enigma kódolásának törése II. Alan Turing |
| 14. | Zh. |
|  |  |
|  | **Labor témakörei** |
| 1. | Karakterkódolási módok |
| 2. | Médiafájlok kezelés írás, olvasás, felülírás |
| 3. | Adatrejtés TXT fájlba |
| 4. | LSB technika lehetőségei, BMP, WAV fájl módosítása |
| 5. | Caesar kódolás és törése |
| 6. | Monoalfabetikus kódolás, gyakoriságtáblázat készítése |
| 7. | Homofónikus kódolás előkészítése |
| 8. | Biliterális kódoló készítése |
| 9. | Vigenére kódoló készítése |
| 10. | Vigenére kódolás visszafejtése |
| 11. | ADFGVX kódoló készítése |
| 12. | ADFGVX kódolás visszafejtése |
| 13. | Összefoglalás |
| 14. | Zh |
| **Félévközi követelmények**  |
| Zárthelyi dolgozat. | Beadandó feladat | Labormérés |
| száma | időpontok | száma | határidők | száma | időpontok |
| 2 db | félév elején egyeztetve | db |  | db |  |
| **Az értékelés, a lebonyolítás, a pótlás módja, a jegy kialakításának szempontjai** *Értékelés: Az aláírás megszerzésének feltétele az évközi zárthelyik legalább elégséges szintre való teljesítése.**Elégséges>40%**Közepes>55%**Jó>70%**Jeles>85%**Zárthelyi dolgozatíráskor, ill. vizsgán a meg nem engedett segédeszközök (puska, mobiltelefon, stb.) használata, ill. arra tett kísérlet, továbbá bármilyen információcserére tett kísérlet az érintett hallgató(k) letiltását vonja maga után.**A szorgalmi időszak utolsó hetében lehetőség van a sikertelen, illetve igazoltan (pl. betegség) mulasztott zh-k pótlására.**Az évközi jegy/aláírás szorgalmi időszakon túli pótlásának módja: HKR 47. §**Hiányzás szabályozása: HKR 46. §**Valamennyi, jelen dokumentumban nem szabályozott, kérdésben az Óbudai Egyetem Hallgatói Követelményrendszere, valamint Tanulmányi Ügyrendjének rendelkezései az irányadók.* |

|  |  |
| --- | --- |
| **Letiltva bejegyzést kap:** | Aki eléri, illetve meghaladja a megengedett hiányzások számát, illetve egyik zárthelyi dolgozatot sem írta meg és nem igazolta megfelelően a hiányzását (pl. betegség esetén orvosi naplószámot tartalmazó igazolással). |
| **Kötelező irodalom:** | Előadás jegyzet |
| **Ajánlott irodalom:**  | Simon Singh: Kódkönyv - A rejtjelezés és rejtjelfejtés története , ISBN: 9789635307982, 2007Johannes Ernesti, Peter Kaiser: Python 3: The Comprehensive Guide to Hands-On Python Programming, ISBN: 978-1493223022, 2022 |
| **A tárgy minőségbiztosítási módszerei:** |  |

Kelt: Budapest, 2023. 06. 15.

Szöveg beírásához kattintson vagy koppintson ide.

………………………………………………………

Dr. habil. Kiss Gábor