|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Óbudai EgyetemBánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar | | | | | | | Biztonságtudományi és Kibervédelmi Intézet | | | |
| **Tantárgy címe és kódja:** **Elektronikus információbiztonsági ismeretek BBXEB13BNF Kreditérték: 4**Nappali tagozat 2. tanév 1 . félév | | | | | | | | | | |
| Szakok melyeken a tárgyat oktatják: **Kibermérnök szak** | | | | | | | | | | |
| Tantárgyfelelős oktató: | | | **Dr. Kiss Gábor** | | | Oktatók: | | | **Dr. Kiss Gábor** | |
| Előtanulmányi feltételek (kóddal) | | | | |  | | | | | |
| Heti óraszámok: | Előadás: 2 | | | Tantermi gyak.: | | | | Laborgyakorlat: 2 | | Konzultáció: |
| Félévzárás módja:  (követelmény) | **Évközi jegy** | | | | | | | | | |
| **A tananyag** | | | | | | | | | | |
| **Oktatási cél:**A tárgy oktatásának célja, hogy a hallgatók megismerjék az elektronikus rendszerek működését, biztonságukat érintő veszélyforrásokat. A különböző adatvédelmi technikák, kriptográfiai lehetőségek felhasználási területét, módját, valamint feltörési technikákat.  A napjainkban használt szimmetrikus kódoló algoritmusok működése. Aszimmetrikus kódolás menete. Hibrid titkosítás, HTTPS, tanúsítványkezelés.  Titkosított fájlrendszerek használata, PGP működése, használata.  HASH függvények működése, felhasználási területeik.  Esettanulmányok. | | | | | | | | | | |
| Ütemezés: | | | | | | | | | | |
| Oktatási hét  (konzultáció) | | Témakör | | | | | | | | |
| 1. | | Szimmetrikus kódolások I. (DES) | | | | | | | | |
| 2. | | Szimmetrikus kódolások II. (AES) | | | | | | | | |
| 3. | | Diffie-Hellman kulcscsere | | | | | | | | |
| 4. | | Asszimetrikus kódolasok I. (RSA) | | | | | | | | |
| 5. | | Asszimetrikus kódolasok II:(Elliptikus görbék) | | | | | | | | |
| 6. | | PGP, titkosított levélküldés, titkosított fájlrendszer | | | | | | | | |
| 7. | | 1. Zh. | | | | | | | | |
| 8. | | Vírusok, vírusvédelem | | | | | | | | |
| 9. | | Hibrid titkosítás, HTTPS protokoll | | | | | | | | |
| 10. | | VPN | | | | | | | | |
| 11. | | Egyirányú függvények és alkalmazási területeik | | | | | | | | |
| 12. | | Jelszavak biztonsága, sózás. | | | | | | | | |
| 13. | | Social Engineering technikák, a Social Engineering eredményének felhasználása. | | | | | | | | |
| 14. | | 2. Zh. | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Labor témakörei** | | | | | | | | |
| 1. | | MS Office adatvédelmi lehetőségei, biztonsági szintje | | | | | | | | |
| 2. | | Adattitkosítási lehetőségek háttértárolón | | | | | | | | |
| 3. | | Információtitkosítás Pythonban I. | | | | | | | | |
| 4. | | Információtitkosítás Pythonban II. | | | | | | | | |
| 5. | | Információtitkosítás Pythonban III. | | | | | | | | |
| 6. | | Információtitkosítás Pythonban IV. | | | | | | | | |
| 7. | | Információtitkosítás Pythonban V. | | | | | | | | |
| 8. | | Jelszógenerálás Pythonban | | | | | | | | |
| 9. | | Szivárványtábla generálás Pythonban | | | | | | | | |
| 10. | | Módosított szivárványtábla generálás Pythonban | | | | | | | | |
| 11. | | Titkosított fájlrendszer | | | | | | | | |
| 12. | | Titkosított hálózati adatforgalmazás (VPN) | | | | | | | | |
| 13. | | Titkosított e-mail küldés | | | | | | | | |
| 14. | | Zh. | | | | | | | | |
| **Félévközi követelmények**  *(feladat, zh. dolgozat, esszé, stb)* | | | | | | | | | | |
| Oktatási hét  (konzultáció) | | Zárthelyik (részbeszámolók, stb.) | | | | | | | | |
|  | | 2 db. zárthelyi az előadások és 2 db. zárthelyi a labor anyagából | | | | | | | | |
| *Az értékelés, a lebonyolítás, a pótlás módja, a jegy kialakításának szempontjai* | | | | | | | | | | |
| *Értékelés: Az évközijegy 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. | | | | | | | | | | |
| **A félévzárás módja** *(vizsga módja: írásbeli, szóbeli, teszt, stb.)* | | | | | | | | | | |
| |  |  | | --- | --- | | **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 jegyezet | | | | | | | | | | |
| **Ajánlott irodalom:** | | | | | | | | | | |
|  | | | | | | | | | | |
| **Egyéb segédletek:** | | | | | | | | | | |
|  | | | | | | | | | | |
| **A tárgy minőségbiztosítási módszerei:** | | | | | | | | | | |

Kelt: Budapest, 2024. 06. 06.

………………………………

tantárgyfelelős

Dr. habil. Kiss Gábor