

Óbudai Egyetem			
Alba Regia Egyetemi Központ			
Tantárgy neve és kódja: Az informatikai biztonság alapjai NRKIB0SSND		Kreditérték: 4	
Nappali tagozat 2016/2017. tanév		2. félév	
Szakok, melyeken a tárgyat oktatják: felsőfokú mérnökinformatikus asszisztens			
Tantárgyfelelős oktató:	Dr. Póser Valéria PhD	Oktatók:	Lukács Balázs
Előtanulmányi feltételek: (kóddal)			
Heti óraszámok:	Előadás: 2	Tantermi gyak.: 0	Konzultáció: 0
Számonkérés módja (s,v,f):		Írásbeli vizsgák átlaga, nem egyértelműség esetén szóbeli vizsga	
A tananyag			
<p><i>Oktatási cél:</i> Az információ fogalomköre, továbbítása és tárolása és ezek során az információt fenyegető sérülések, támadások, valamint betekintés az információ-védelem módszereibe.</p> <p>A hallgatók gyakorlati felkészítése e problémakör identifikációjára és a még kezelhető módszerek elsajátítására Cél a gyakorlati módszerek elméleti alapjainak a megtanítása is.</p>			
Előadások			Óraszám
1. hét	Az információ és fogalomköre. Az informatikai biztonság tárgya, eszközei, módszerei.		2
2. hét	Az informatikai biztonság összetevői, aspektusai		2
3. hét	Az informatikai biztonság alapmodelljei		2
4. hét	Biztonsági rendszerek tervezése, alapfogalmak A rendszer elemei, a védelem tervezése, eszköztára, módszerei A megbízható informatikai rendszer funkciói Állandó fenyegetettség és védekezés		2
5.hét	Védelmi szabványok		2
6. hét	1. Zárthelyi dolgozat		2
7. és 8. hét	Kriptográfia, szükségessége, eredete, fejlődése Kriptográfia célja, eszközei napjainkban		4
9. és 10. hét	A kriptográfia elemei, kriptogenerációk, protokollok. A kriptográfia 2. generációja, asszimétrikus titkosítás		4
11. hét	Kriptográfiai technikák és a szimmetrikus titkosítás		2
12. hét	Kulcsmenedzsment, Alkalmazások, kriptográfia szolgáltatásai		2
13. hét	2. Zárthelyi dolgozat		
14. hét	Pótlások		2
Összesen:			28 ó.e.a.

Félévközi követelmények	
AZ ELŐADÁSOK LÁTOGATÁSA KÖTELEZŐ!	
Előadások:	
2 db nagy zárthelyi van betervezve. A féléves jegy a 2 zárthelyi dolgozat érdemjegyének számtani átlaga. Az elégséges szint a maximálisan elérhető pontérték 50%-a. Nem egyértelműség esetén, szóbeli vizsga eredménye dönti el a féléves jegyet. Pótlás: Utolsó alkalmat az elmaradások pótlására, szóbeli vizsgákra tartjuk fenn.	
A pótlás módja:	Írásbeli és szóbeli vizsga előadások. Lásd mint fent!
Aláírás feltétele:	Az előadások rendszeres látogatása és az előadásokkal kapcsolatos számonkérés félévközi eredménye (vagy a pótlása) eléri el a 50%-ot.
A vizsga módja (írásbeli, szóbeli, teszt, stb):	Írásbeli, 50 % az elégséges szint, nem egyértelműség esetén szóbeli vizsga.
Kötelező irodalom	
Kötelező: Az egyetem e-learning rendszerébe (folyamatosan) e tárgyhoz feltöltött valamennyi elektronikus tananyag (mind az előadások prezentációi, mind az elektronikus jegyzetek) rendszeres, előadástól-előadásra való figyelése, elolvasása és megtanulása.	
Ajánlott irodalom	
Virasztó Tamás: Titkosítás és adatretjtés, NetAcademia Kft. 2004t, ISBN 963 214 253 5	
Dr. Berta István Zsolt: Nagy e-szignó könyv, Microsec Kft. 2011, ISBN 978 963 08 1168 2 (Ez a könyv és egyes részei is internetről is letölthetők.)	
Niels Ferguson & Bruce Schneier: Practical Cryptography, Wiley Publishing Inc. 2003. ISBN 0-471-22357-3 (Paperback) NAGYON JÓ!	
Nagy Sándor: Elektronikus leveleink védelme, Computerbooks, 2005	
Himansu Dwivedi: SSH a gyakorlatban, Kiskapu, 2004	
Tom Thomas: Hálózati biztonság, Panem Kft. 2005	
Buttyán Levente-Vajda István :Kriptográfia és alkalmazásai, Typotex Kiadó, 2004	
Opcionális szakirodalmat és linkeket találhat e tárgy e-learning webkikötőjén is.	

Székesfehérvár, 2017. február 1.

.....
Lukács Balázs