Kari Tanácsi elfogadás: Szám/dátum

TANTÁRGYI ADATLAP

1. Tanulmányi program adatai

1.1. Intézmény	Sapientia Erdélyi Magyar Tudományegyetem
1.2. Kar/Tanárképző Intézet	Műszaki és Humántudományok
1.3. Képzési szint	alapképzés
1.4. Képzési ág	informatika/számítástechnika és információtechnológia
1.5. Tanulmányi program	Informatika/Számítástechnika
1.6. Képzettség	informatikus/villamosmérnök

2. Tantárgy adatai

2.1. Tantárgy címe		Kriptográfia és információbiztonság					
2.2. Tantárgy kreditszáma				2.3. Tantárgy Neptun kódja		MBEI0231	
2.4. Tanszék		Matematika – Informatika					
2.5. Tantárgyfelelős		dr. Márton Gyöngyvér, lektor					
2.6. Szeminárium/ gyakorlat/terv felelőse		dr. Márton Gyöngyvér, lektor					
2.7. Év	3	2.8. Félév	6	2.9. Tantárgy típusa (kötelező, opcionális, fakultatív)		2.10. Követelmény (vizsga, kollokvium, folyamatos számonkérés)	
2.11. Heti óraszám	4	Melyből: Előadás	2	Szeminárium	2	Gyakorlat/terv	

3. Előfeltételek (esetenként)

3.1. Tantervi	
3.2. Kompetencia	

4. Tantárgy célkitűzései

4.1. Tantárgy általános célkitűzése	1. A kriptográfia alapelveinek, a kriptográfiai primitíveknek a megismerése. 2. Az elméleti ismeretek gyakorlati alkalmazásokban való hasznosítása. 3. A diák gondolkodásának oly módon való alakítása, hogy a későbbiek során fel tudja használni a tanult matematikai és kriptográfiai ismereteket.

5. Tartalom

5.1. Előadás (téma)	Óraszám
Bevezető fogalmak. Klasszikus kriptográfiai rendszerek: Caesar, Keyword Caesar, affin, Hill	2 óra
Biztonságértelmezések. Titkos kulcsú (szimmetrikus) rendszerek: alapfogalmak. Folyamrejtjelező rendszerek: OTP, RC4, LFSR, ChaCha20. A rendszerek biztonsága.	4 óra
Titkos kulcsú (szimmetrikus) rendszerek: Blokkrejtjelező rendszerek: DES, TEA, AES. A rendszerek biztonsága. Blokktitkosítási módok: ECB, CBC, CTR	4 óra
Hash függvények: értelmezés, biztonság. Az SHA függvénycsalád. Üzenethitelesítő kódokok (MAC): értelmezés, biztonság. HMAC, CMAC. Hitelesített titkosítás: GCM mód, Poly1305.	2 óra

Publikus kulcsú (aszimmetrikus) rendszerek: bevezető fogalmak. Matematikai modellek. Matematikai feltételezések. A Diffie-Hellman kulcscsere. Biztonságproblémák.	2 óra
Publikus kulcsú (aszimmetrikus) rendszerek: RSA, RSA-OAEP. A rendszerek biztonsága.	2 óra
Publikus kulcsú (aszimmetrikus) rendszerek: Rabin, SAEP, ElGamal, Blum-Goldwasser. A rendszerek biztonsága.	2 óra
Digitális aláírások: RSA-PSS, ElGamal, DSA.	2 óra
Elliptikus görbéken alapuló kriptográfia. Biztonságproblémák.	4 óra
Kriptográfiai protokollok: TLS/SSL, Noise, Signal, PGP, HTTPS	2 óra
Ismétlés	2 óra

Szakirodalom/Bibliográfia

1. Dan Boneh, Victor Shoup. A Graduate Course in Applied Cryptography. 2023: http://toc.cryptobook.us/
2. Buchmann J., Introduction to cryptography, 2nd edition. Springer Verlag, 2004.
3. Buttyán L., Vajda I.: Kriptográfia és alkalmazásai, Typotex eKiadó, Budapest, 2012.
4. Freud R., Gyarmati E., Számelmélet, Nemzeti Tankönyvkiadó, Budapest, 2006.
5. Márton Gy, Kriptográfiai alapismeretek, Scientia Kiadó, Kolozsvár, 2008.
6. Menezes J., van Oorschot P.C., Vanstone S.A., , Handbook of Applied Cryptograph, CRC Press, Boca Raton, Florida, 1997.
7. Stinson D.R., Cryptography theory and practice, 4th Edition, Chapman&Hall/CRC, 2018.
8. David Wong, Real-World Cryptography. Manning. 2021,
9. Az oktató weboldala: http://www.ms.sapientia.ro/~mgyongyi

5.2. Terv/laboratóriumi gyakorlat /szeminárium	Óraszám
Klasszikus kriptográfiai rendszerek feltörési lehetőségei	2 óra
Folyamrejtjelező rendszerek: OTP, RC4, LFSR, A5/1 feltörési lehetőségek, implementációk, kriptográfiai könyvtárcsomagok	4 óra
Blokkrejtjelező rendszerek: AES, 3DES. Implementációval kapcsolatos kérdések	2 óra
Hash függvények	2 óra
Nyilvános kulcsú titkosító rendszerek: Diffie-Hellman.	2 óra
Nyilvános kulcsú titkosító rendszerek: RSA, RSA-OAEP.	2 óra
Nyilvános kulcsú titkosító rendszerek: Rabin, SAEP, ElGamal, Blum-Goldwasser.	2 óra
Elliptikus görbéken alapuló kriptográfia.	4 óra
Digitális aláírások: RSA, ElGamal.	2 óra
Feladatok bemutatása	6 óra

Szakirodalom/Bibliográfia

1. Dan Boneh, Victor Shoup. A Graduate Course in Applied Cryptography. 2023: http://toc.cryptobook.us/
2. Buchmann J., Introduction to cryptography, 2nd edition. Springer Verlag, 2004.
3. Buttyán L., Vajda I.: Kriptográfia és alkalmazásai, Typotex eKiadó, Budapest, 2012.
4. Freud R., Gyarmati E., Számelmélet, Nemzeti Tankönyvkiadó, Budapest, 2006.
5. Márton Gy, Kriptográfiai alapismeretek, Scientia Kiadó, Kolozsvár, 2008.
6. Menezes J., van Oorschot P.C., Vanstone S.A., , Handbook of Applied Cryptograph, CRC Press, Boca Raton, Florida, 1997.
7. Stinson D.R., Cryptography theory and practice, 4th Edition, Chapman&Hall/CRC, 2018.
8. David Wong, Real-World Cryptography. Manning. 2021,
9. Az oktató weboldala: http://www.ms.sapientia.ro/~mgyongyi

6. Felmérés

Tevékenység típusa	6.1. Felmérési kritériumok	6.2. Felmérési módszerek	6.3. Aránya a végső jegyből

6.4. Előadás			Projekt, tudományos dolgozat bemutatás	100%
6.5.	Szeminárium			
	Gyakorlat		Feladatbemutatás és plusz pontok	50%
	Terv			
6.6. Minimális teljesítmény elvárás				
A kriptográfia és információbiztonság alapfogalmainak az elsajátítása és gyakorlati alkalmazása. A minimális jegy 5 (öt).				

Dátum	Előadás felelősének aláírása	Gyakorlati órák felelősének aláírása
2024.01.09.	dr. Márton Gyöngyvér	dr. Márton Gyöngyvér

Tanszéki láttamozás dátuma	Tanszékvezető aláírása