Europass Önéletrajz

Személyi adatok

Vezetéknév / Utónév(ek)	**Dr HUSZTI Andrea**
Telefonszám(ok)	+36 52 512900 Mobil:
E-mail(ek)	huszti.andrea@inf.unideb.hu
Állampolgárság	magyar
Neme	nő

Betölteni kívánt munkakör / foglalkozási terület

Tudományos kutató

Szakmai tapasztalat

Időtartam	2016– egyetemi docens, Debreceni Egyetem Informatikai Kar, Számítógéptudományi tanszék 2009–2016 adjunktus, Debreceni Egyetem Informatikai Kar, Számítógéptudományi tanszék 2007–2009: egyetemi tanársegéd, Debreceni Egyetem Informatikai Kar, Számítógéptudományi tanszék előadások, gyakorlatok tartása magyar és angol nyelven, számos hallgatói szakdolgozat, diplomamunka, valamint doktori értekezés témavezetése, tudományos kutatás kriptográfiai protokollok témakörben, több kutatási projektben kutatóként való részvétel, nemzetközi szakmai kapcsolatok kialakítása
Foglalkozás / beosztás	egyetemi docens
Főbb tevékenységek és feladatkörök	oktatás, kutatás
A munkáltató neve és címe	Debreceni Egyetem, Informatikai Kar, Számítógéptudományi tanszék
Tevékenység típusa, ágazat	Felsőoktatás

Tanulmányok

Időtartam

2015: Habilitációs oklevél az informatikai tudományok területén,
Debreceni Egyetem

2009: PhD oklevél a műszaki tudományok területén az informatikai tudományokban,
Debreceni Egyetem

2002: Electronic Commerce Certificate,
Maharishi University of Management, Iowa, USA

1999: Okleveles informatika szakos tanár,
Kossuth Lajos Tudományegyetem (később Debreceni Egyetem)

1998: Okleveles matematika és ábrázoló geometria szakos tanár,
Kossuth Lajos Tudományegyetem (később Debreceni Egyetem)

Egyéni készségek és kompetenciák

Anyanyelv(ek) **magyar**

Egyéb nyelv(ek)
Önértékelés
Európai szint (*)

	Szövegértés			Beszéd			Írás	
	Hallás utáni értés		Olvasás	Társalgás		Folyamatos beszéd		
angol	C2	Mesterfokú nyelvhasználó	C2 Mesterfokú nyelvhasználó	C2	Mesterfokú nyelvhasználó	C2 Mesterfokú nyelvhasználó	C2	Mesterfokú nyelvhasználó
orosz	B1	Önálló nyelvhasználó	B1 Önálló nyelvhasználó	B1	Önálló nyelvhasználó	B1 Önálló nyelvhasználó	B1	Önálló nyelvhasználó

(*) Közös Európai Referenciakeret (KER) szintjei

Társas készségek és kompetenciák

Jól tudok csapatban dolgozni,
Több kutatási projektben is részt vettem kutatócsoporti tagként, illetve számos több szerzős tudományos cikkem készült

Szervezési készségek és kompetenciák

Jó szervezőképesség,
Több hazai és nemzetközi konferencia, valamint szakmai rendezvény szervezésében is részt vettem

Járművezetői engedély(ek) B

Kiegészítő információk

Kutatási terület:

Kriptográfia protokollok tervezése és elemzése
Több eredményem született felhasználó hitelesítés felhőkörnyezetben, e-szavazás, e-vizsgáztatás, e-közvélemény kutatás, e-fizetés témakörében. A biztonságos protokollok tervezésén túl, azok biztonsági elemzését is elvégzem bizonyítható biztonsági és kalkulus alapú modellekben.

Díjak, kitüntetések

2013. Debreceni Egyetem Informatikai Karának díja
2007. Debreceni Egyetem TEK kiváló hallgatója díj
2007. Debreceni Egyetem Universitas Alapítvány díja

Pályázati részvétel

2013 - 2017 Kutató
Számelméleti kutatások
OTKA pályázat (NK104208)
Debreceni Egyetem, Informatikai Kar
2012 - 2014 Kutató
Jövő Internet kutatások az elmélettől az alkalmazásig
TÁMOP pályázat (TÁMOP-4.2.2.C-11/1/KONV-2012-0001)
Debreceni Egyetem, Informatikai Kar
2010 - 2012 Kutató
Kriptográfiai algoritmusok és protokollok
TÁMOP pályázat (TÁMOP-4.2.1/B-09/1/KONV-2010-0007)
Debreceni Egyetem Kutatóegyetemi pályázat
2009 - 2012 Kutató
Diofantikus számelmélet és alkalmazásai
OTKA pályázat (K75566)
Debreceni Egyetem, TTK, Matematikai Intézet
2008 -2011 Kutató

Magyar Tudományos Akadémia által támogatott számelméleti kutatócsoport
2008 - 2011 Kutató
Hiteles és anonim vizsgajavítási rendszer
K+F+I GOP pályázat (GOP-1.1.2-07/1-2008-0001)
Debreceni Egyetem, Informatikai Kar és
NetLock Kft

Nemzetközi kapcsolatok

2009 – 2011 Számelmélet és kriptográfia
Horvát-magyar TÉT pályázat
2009 - 2010 Matematikai módszerek a kriptográfiában
Magyar-osztrák TéT pályázat
2009 - 2010
Magyar - Mexico TéT pályázat
2008 – 2009
Magyar - Japán TéT pályázat
2006 – 2007 Aktion Osterreich-Ungarn"
OMAA pályázat
2005 – 2007 Számelmélet és kriptográfia
Horvát-magyar TÉT pályázat

Konferencia szervezés

2014 Programbizottság tagja
Central European Conference on Cryptology
Budapest, Hungary
2011 Szervező bizottság tagja
Central European Conference on Cryptology
Debrecen, Hungary

Meghívott előadások

2014 Bilinear Pairings and their applications,
NIMS Number Theory and Cryptography Conference, Daejeon, Korea
2014 Bilineáris párosítások és alkalmazásai,
ELTE Formális eszközök az informatikában című szeminárium, Budapest, Magyarország
2014 Bilineáris párosítások és alkalmazása
Sapientia Erdélyi Magyar Tudományegyetem Kiss Elemér Szakkollégium, Marosvásárhely, Románia
2012 Secure Electronic Applications
Interdisciplinary Centre for Security, Reliability and Trust, Luxembourg, Luxembourg
2012 Biztonságos e-alkalmazások
"A nagyság átka: nagyméretű hálózatok, adatok és szoftverek problémái" című MTA tudományos ülésszak, Budapest, Hungary
2012 Kriptográfiai protokollokkal kapcsolatos biztonsági elvárások vizsgálata
BJMT Alkalmazott Matematikai Konferencia, Győr, Hungary
2010 Experiment-based definitions for electronic exam systems
Central European Conference on Cryptography, Bedlewo, Poland

Válogatott előadás lista

A Simple Authentication Scheme for Clouds
IEEE Conference on Communications and Network Security (CNS), Workshop on Security and Privacy in the Cloud (SPC)
2016, Philadelphia, USA

Anonymous Multi-Vendor Micropayment Scheme based on Bilinear Maps
International Conference on Information Society, I-Society
2014, London, United Kingdom

Multi-Vendor PayWord with Payment Approval
International Conference on Security & Management, SAM
2013, Las Vegas, USA

Payment Approval for PayWord
The 13th International Workshop on Information Security Applications, WISA
2012, Jeju Island, Korea

European eID Interoperability Conference
2012, Beil, Switzerland

Secure Universal Protocol for E-Assessment
Computational and Mathematical Methods in Science and Engineering
2011, Benidorm, Spain

Secure Electronic Elections

2008, Nihon University, Tokyo, Japan

Válogatott publikációk

1. Andrea Huszti; Norbert Oláh, A simple authentication scheme for clouds, 2016 IEEE Conference on Communications and Network Security (CNS), IEEE, (2016), pp. 565–569.
2. A.Huszti, Z. Kovács, Bilinear Pairing-based Hybrid Mixnet with Anonymity Revocation, Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP), Scitepress, (2015), pp.238–245.
3. A. Huszti, Anonymous Multi-Vendor Micropayment Scheme based on Bilinear Maps, In: International Conference on Information Society (i-Society 2014). IEEE, (2014), pp. 27-32.
4. A. Huszti, Multi-Vendor PayWord with Payment Approval, In: Kevin Diami, Hamid R Arabnia (szerk.), Proceedings of the 2013 International Conference on Security and Management. Las Vegas: CSREA Press, (2013). pp. 265-271.
5. László Aszalós, Andrea Huszti, Payment approval for PayWord, In: D H Lee, M Yung (szerk.), Information Security Applications, LECTURE NOTES IN COMPUTER SCIENCE 7690. Springer-Verlag, (2012), pp. 161-176.
6. A. Huszti, A Homomorphic Encryption-Based Secure Electronic Voting Scheme, PUBLICATIONES MATHEMATICAE DEBRECEN 79:(3.-4.), (2011), pp. 479-496.
7. A. Huszti, A Pethő, A secure electronic exam system, PUBLICATIONES MATHEMATICAE DEBRECEN 77:(3-4), (2010), pp. 299-312.
8. A. Huszti, A Secure Electronic Voting Scheme, PERIODICA POLYTECHNICA-ELECTRICAL ENGINEERING 51:(3-4), (2007), pp. 141-146.
9. A. Huszti, K. Scheicher, P. Surer, J M Thuswaldner, Three-dimensional symmetric shift radix systems, ACTA ARITHMETICA 129: (2007), pp. 147-166.
10. Pethő A, Brunotte H, Huszti A, Bases of canonical number systems in quartic algebraic number fields, JOURNAL DE THEORIE DES NOMBRES DE BORDEAUX 18:, (2006), pp. 537-557.