**A Magyar Tudomány Ünnepe**

**2017. november 3-30.**

**„Emberközpontú tudomány”**

|  |  |
| --- | --- |
| **A rendezvény címe** | Prof. Andrej Dujella előadása: Applications of Diophantine approximations algorithms in cryptanalysis of RSA |
| **A rendezvény típusa**  (pl. előadás, emlékülés, konferencia, kerekasztal-beszélgetés, könyvbemutató, kiállítás, szimpózium, tudományos ülés,  workshop stb.) | Előadás |
| **Tudományterület** | Informatika, Matematika |
| **A rendezvény időpontja** | 2017. november 24. 13.00 |
| **A rendezvény helyszíne** | Debreceni Egyetem Informatikai Kar, 4028 Debrecen, Kassai út 26. |
| **Szervező intézmény(ek)** | Debreceni Egyetem Informatikai Kar |
| **Kapcsolattartó**  (név, e-mail, telefon) | Dr. Cserhátiné Vecsei Ildikó  Dékáni Hivatalvezető  Informatikai Kar  tel: +36 (52) 512-900/75022   |  |  | | --- | --- | |  | [vecsei.ildiko@inf.unideb.hu](mailto:vecsei.ildiko@inf.unideb.hu) | |
| **A rendezvény honlapjának elérhetősége** |  |
| **Szinopszis, rövid összefoglaló**  (legfeljebb 1000 karakter) | To speed up the RSA decryption one may try to use small secret decryption exponent d. The choice of a small d is especially interesting when there is a large difference in computing power between two communicating devices. However, in 1990, Wiener showed that if d < n^(1/4), where n = pq is the modulus of the cryptosystem, then there exist a polynomial time attack on the RSA. He showed that d is the denominator of some convergent p\_m/q\_m of the continued fraction expansion of e/n, and therefore d can be computed efficiently from the public key (n,e). In this talk, we will discuss similar attacks on RSA and its variants which use results and algorithms from Diophantine approximations, such as Worley's extension of the classical Legendre's theorem on continued fractions and LLL-algorithm for computing short vectors in lattices. |
| **A rendezvény programterve**  (röviden ismertetve vagy  mellékletként csatolva) | Prof. Andrej Dujella előadása: Applications of Diophantine approximations algorithms in cryptanalysis of RSA  A Debreceni Egyetem Informatikai Kara ez évben Prof. Andrej Dujellat terjesztette fel a Doctor Honoris causa címre. A címmel járó oklevél ünnepélyes átadására 2017. november 25-én kerül sor, ezt megelőzően az Informatikai Kar lehetőséget ad a professzor úrnak tudományos előadás megtartására. Itt lehetősége lesz az oktatóknak, doktoranduszoknak és hallgatóknak betekintést nyerni a professzor úr munkásságába. |