HRVATSKA AKADEMIJA ZNANOSTI I UMJETNOSTI

CROATIAN ACADEMY OF SCIENCES AND ARTS

HRVATSKA AKADEMIJA ZNANOSTI I UMJETNOSTI

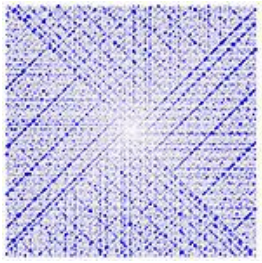
ima čast pozvati Vas na predavanje koje će održati

akademik ANDREJ DUJELLA

TEORIJA BROJEVA I KRIPTOGRAFIJA

u četvrtak, 29. svibnja 2014. u 18 sati

u dvorani Knjižnice Hrvatske akademije znanosti i umjetnosti
Zagreb, Strossmayerov trg 14



Uvodna riječ

akademik Velimir Neidhardt, potpredsjednik
Hrvatske akademije znanosti i umjetnosti

Ljudi su od davnina željeli sigurno komunicirati, ali bili su svjesni da njihove poruke često putuju nesigurnim komunikacijskim kanalima. Iako su se kroz stoljeća načini prenošenja poruka uvelike promijenili, osnovni problem je ostao isti, a to je kako onemogućiti onoga tko može nadzirati kanal, kojim se prenosi poruka, da dozna njezin sadržaj. Načinima rješavanja ovog problema bavi se znanstvena disciplina koja se naziva **kriptografija**.

Metode, koje su se najčešće tijekom povijesti koristile za šifriranje poruka, bile su zamjena (supstitucija) i premještanje (transpozicija) osnovnih elemenata teksta (slova, blokova slova, bitova). Kombinaciju ovih dviju metoda susrećemo i danas u modernijim simetričnim kriptosustavima. Asimetrični kriptosustavi ili kriptosustavi s javnim ključem pojavili su se tek 70-tih godina 20. stoljeća. Kod njih se za šifriranje koriste funkcije koje su "jednosmjerne" (one se računaju lako, ali njihov inverz vrlo teško). To znači da funkcija za šifriranje može biti javna, dok samo funkcija za dešifriranje mora biti tajna. U konstrukciji jednosmjernih funkcija koriste se "teški" matematički problemi, koji uglavnom potječu iz algoritamske teorije brojeva, kao što su faktorizacija velikih prirodnih brojeva, te logaritmiranje u nekim konačnim grupama (glavni primjeri su multiplikativna grupa konačnog polja te grupa točaka na eliptičkoj krivulji nad konačnim poljem).

U ovom predavanju, prikazat ćemo neke klasične i neke moderne metode za šifriranje. Pokušat ćemo objasniti pojmove i algoritme iz teorije brojeva koji su relevantni za realizaciju kriptosustava s javnim ključem.

Najljepše Vam zahvaljujemo na sudjelovanju!

Zrinski trg 11, 10000 Zagreb, Hrvatska Tel.: (01) 489 51 11 – Telefax: (01) 481 99 79