SZEMINÁRIUM

Az ELTE TTK Valószínűségelméleti és Statisztika Tanszékének szemináriumán 2014. március 21-én, pénteken 10 órakor

Szabó István (ELTE TTK Valószínűségelméleti és Statisztika Tanszék)

A kriptográfia és a matematika kapcsolata

címmel tart előadást.

Az előadás helye: ELTE lágymányosi campus, déli épület (1117 Budapest, Pázmány Péter s. 1/C), 3-316.

Kivonat:

A kriptográfiai (titkosírási) algoritmusok biztonságának elemzése nagyon sok matematikai terület eredményeit használja fel (pl. statisztika, információelmélet, számelmélet, algebra, algoritmuselmélet, bonyolultságelmélet, véges geometria), de a hatás kölcsönös, a kriptográfia által felvetett problémák több területen jelentős matematikai kutatásokat, eredményeket indukáltak.

Rövid áttekintést adok a gyakorlati alkalmazások által inspirált néhány kiemelt kutatási területről, elsősorban a számelméleti alapú RSA titkosító algoritmus, valamint a digitális aláírások biztonságáról. Az előadásban szerepel jó néhány matematikailag is érdekes, egészen meglepő következtetés is.