به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

رمزگشایی بلوک های سبک

Cryptanalysis of lightweight Ciphers

نداسادات رسولی

زمان: شنبه ۲۰ اردیبهشت ماه ۱۳۹۳ ساعت ۳ بعد از ظهر

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهارم، سالن ۴۰۴

Lightweight encryption denotes a class of cryptographic algorithms that are suitable for extremely resource constrained environments and offer a moderate security level.
Lightweight encryption algorithms can be divided into two classes: lightweight block ciphers and stream ciphers.
In this Section we focus on the cryptanalysis of lightweight encryption schemes .We introduce two block:
Ciphers C2 and Maya and start to cryptanalysis them.

شرکت در این جلسه برای تمامی دانشجویان علاقه مند آزاد است.

مشخصات سخنران:

ندا سادات رسولی

neda.asrasooli@yahoo.com

سوابق تحصیلی:

دانشجوی دوره دکتری ریاضیات محض گرایش جبر جابجایی مرکز تحصیلات تکمیلی در علوم پایه زنجان (در حال مطالعه برای امتحان جامع)

کارشناسی ارشد ریاضی محض -گرایش جبر جابجایی (عنوان پایان نامه : رشد خطی تجزیه اولیه ایده آل ها) (دانشگاه شهید بهشتی ۱۳۸۲-۱۳۸۵) (استاد راهنما : دکتر طوسی)

کارشناسی ریاضی محض (دانشگاه تهران ۱۳۷۷-۱۳۸۱)

دیپلم ریاضی (دبیرستان فرزانگان– سازمان ملی پرورش استعداد های درخشان)

جوایز و موفقیت های تحصیلی :

راهیابی پروژه " مقدمه ای بر نظریه گروه‌ها به مرحله نخست جشنواره خوارزمی " در سال ۱۳۷۵

قبولی در آزمون مرحله نخست المپیاد ریاضی دانش آموزی و راهیابی به مرحله دوم در سال ۱۳۷۵

قبولی در آزمون مرحله نخست المپیاد کامپیوتر دانش آموزی و راهیابی به مرحله دوم در سال ۱۳۷۵

کسب مقام برنز و مقام دوم تیمی در بیست و ششمین مسابقات ریاضی دانشجویی کشور (۱۳۸۱)

رتبه ۹۰ کنکور کارشناسی ارشد

مقالات:

۱. ارائه سمینار در دانشگاه تهران در موضوع قضیه دیریکله در تصاعد های حسابی
۲. ارائه سمینار در دانشگاه تهران در موضوع قضیه اجتناب از ایده آل های اول و تعمیم آن
۳. ارائه سمینار در دانشگاه شهید بهشتی در موضوع

Strongly adjacency-transitive graphs and uniquely shift-transitive graphs

۴. ارائه سمینار در دانشگاه شهید بهشتی در موضوع جبر های آفین

5. 31st Iranian Mathematics Conference, University of Tehran, Tehran Iran
6. Workshop and Conference on logic, Algebra and Arithmetic (18-22 Oct 2003) IPM, Tehran,Iran.
7. Workshop on Commutative Algebra and Related Topics (2004), IPM, Tehran, Iran
8. 6th Seminar on Commutative Algebra and Related Topics, 2009, IPM 20-Combinatorics 2009, IPM, Tehran, Iran