СЕМИНАР
„АЛГЕБРА И ЛОГИКА”

Драги колеги,

Следващото заседание на семинара ще се проведе
на 2 март 2012 г. (петък) от 11:00 часа
в зала 578 на ИМИ – БАН.

Доклад на тема

КРИПТОСИСТЕМА С ОТКРИТ КЛЮЧ,

ОСНОВАНА

НА ПОЛУПРЪСТЕНИ ОТ ЕНДОМОРФИЗМИ

НА КРАЙНА ПОЛУРЕШЕТКА

ОТ СПЕЦИАЛЕН ВИД

ще изнесе Мариана Дурчева
от Техническия университет – София.

Поканват се всички желаещи.

От секция „Алгебра и логика” на ИМИ – БАН

http://www.math.bas.bg/algebra/seminarAiL/

==========

Резюме

Сигурността на редица криптосистеми с открит ключ (както протокола на Дифи – Хелман за обмен на ключове) се основава на задачата за дискретния логаритъм в циклични групи.

По-нататъшно развитие задачата за дискретния логаритъм получава при използване на действие на полугрупа на крайно множество.

Идеята се продължава в случая, когато комутативен полупръстен действа на матричен полупръстен с елементи от полупръстена от ендоморфизми на крайна полурешетка от специален вид.