



Seminar Announcement

Speaker: Kerem KAŞKALOĞLU
(Atılım University)

Linear Feedback Shift Registers and Cryptography;

Stream ciphers are widely used in today's communication system such as Bluetooth and mobile cell phone networks as they do not require expensive hardware and they provide adequate security. In this talk, underlying mathematical tools for stream ciphers will be introduced, the theory of Linear Feedback Shift Registers (LFSR), a basic tool for most stream ciphers, will be considered. The properties that a key sequence of a stream cipher will be mentioned.

DATE: April 22, 2008

TIME: 15:45

PLACE: FEF 403 (Seminar Room)

All interested people are cordially invited. After the seminar, some cookies and soft drinks will be served.