T-79.5501
Cryptology

Lecture 7 (Nov 1, 2005):

- Announcements
- RSA

OPTIMI Mathematical Cafe Tomorrow

http://optimi.tky.fi/pub.php

MATHEMATICAL CAFÉ

D-salissa

Keskiviikkona 2.11. klo 17.15

Yleisön viihdyttämisestä vastaavat:

* Kaisa Nyberg: Matemaatikkona Nokialla
* Lasse Leskelä: Milloin satunnaiskävelijä unohtaa lähtöpisteensä?
* Juhani Pitkäranta: Insinöörit vastaan matemaatikot: Elementti-menetelmän esihistoriasta

Tarjolla myös virvokkeita ja sokeroituja toruksia.

Jatkot JMT 3A:n kattosaunalla välittömästi tilaisuuden jälkeen.

Jatkoilla tasokkaat tarjoilut ja saunomismahdollisuus.

Room Change

- Exercise Group 2 (Fridays) changed: new room T3

RSA Public Key Cryptosystem

Stinson:

Section 5.1 Public key Cryptography

Section 5.3 RSA

Section 5.4 Quadratic residues, Jacobi Symbol

Sanastoa:

public key = julkinen avain

trapdoor = salaovi, salaluukku

one-way function = yksisuuntainen funktio

quadratic residue = neliönjäännös

quadratic non-residue = neliön epäjäännös