

# Cryptography, Protocols and its Implementations

21 May – 02 June 2007

The Computer Science and Engineering department of National Institute of Technology Rourkela is organizing the short term course on "Cryptography, Protocols and its Implementations" during 21 May – 02 June 2007. The Sponsored Research and Industrial Consultancy (SRIC) Cell of NIT Rourkela is facilitating the assistant for the course.

## COURSE OUTLINE

- Mathematical Foundation
  - Congruence
  - Modular arithmetic
  - Chinese Remainder Theorem
  - Extended Euclid's Algorithm
  - Discrete Logarithm Problem
  - Miller-Rabin Test
  - Fermat Test
- Introduction to Cryptography
- Symmetric Cryptosystems
  - Simplified DES, DES, AES
- Public Key Cryptosystems
  - RSA,
  - Diffie-Hellman
  - ElGamal
  - DSA
  - ECC
- Protocols and Application
  - Blind Signature (RSA, ECC etc.)
  - Key Exchange Protocol
  - Electronic Voting
  - Digital Cash
- Implementations using Java/C

## INTENDED AUDIENCE

The course is designed primarily for scholars who would like to further their education in Cryptography. Professionals working in these fields, as well as Students of Electronics, Electrical and Computer Science & Engineering, Mathematics would find this course extremely useful and interesting.

## REGISTRATION AND FEE

The registration form may be downloaded from the website. Filled in registration form along with a demand draft of Rs. 3,000/- (Rupees Three Thousand Only) should be sent to The Coordinator at the address given below. The DD should favor "Continuing Education, NIT Rourkela" and should be payable at SBI, NIT Campus Branch Rourkela (Code: 2109).

## ACCOMODATION

Accommodation and food will be provided in Students' hostel of NIT Rourkela as per availability on payment basis. The cost would be approximately Rs.60/- per day.

## IMPORTANT DATES

Last date of receipt: (Completed application form with Draft)	10-May-2007
Commencement of Course	21-May-2007
Completion of Course	02-Jun-2007

## COORDINATORS

Prof. Banshidhar Majhi,  
Professor, CSE Dept. NIT Rourkela

## CORRESPONDENCE

Prof. Banshidhar Majhi, Coordinator, "CPI-2007",  
Dept. of CSE, NIT Rourkela,  
Rourkela – 769 008, Orissa, India

bmajhi@nitrkl.ac.in  
bm\_nitrkl@yahoo.com  
0661-246-2355  
09437221124



# Cryptography, Protocols and its Implementations

21 May-02 June 2007, Dept of CSE, NIT Rourkela

## Registration Form

Name:

---

Address:

---

---

e-mail:

---

Phone:

---

Accommodation

YES

NO

Registration Fee:

Rs. 3,000/-

Rupees Three Thousand Only

Demand Draft Number/Date/Bank:

---

---

Date

Signature

Number of seats for this course is limited and allocation would be strictly on first-come-first-serve basis. Fee for the course is to be paid in the form of demand draft favoring "Continuing Education, NIT Rourkela", payable at "Rourkela".

Amount

Rs. 3,000/-

To sign up for this course, fill up the registration form and send along with the required fee to the coordinator in the following address

Contact Details

Prof. Banshidhar Majhi, Co-coordinator CPI-2007,  
Dept of CSE, NIT Rourkela.  
Rourkela-769 008, Orissa, India

Ph-0661-246-2355, 9437221124,  
bmajhi@nitrkl.ac.in, bm\_nitrkl@yahoo.com

Last date of receiving application with DD is 10 May 2007

Accommodation and fooding can be arranged in institute hostel on payment basis (Approx Rs. 60/= per day)