NATIONAL INSTITUTE OF TECHNOLOGY
WARANGAL - 506 004 (Telangana State)

Faculty Development Programme (FDP)
On

Foundations of Cryptography

Jointly Sponsored by

Electronics & ICT Academy and Information Security Education Awareness (ISEA) Project-Phase II, Deity, Govt. of India

Organized by

Department of Computer Science and Engineering

(19th – 30th December 2016)

Preamble:

"Electronics & ICT Academy" is being set up at NIT Warangal with financial assistance from DeitY, MCIT, GoI. The jurisdiction of this academy is Telangana, Andhra Pradesh, Karnataka States and Puducherry, Andaman & Nicobar Islands and Goa UTs. This academy role is to offer faculty development programmes in standardized courses and emerging areas of Electronics, Information Communication Technologies; training & consultancy services for Industry; Curriculum development for Industry; CEP for working professionals; Advice and support for technical incubation and entrepreneurial activities.

Cryptography is a science that applies complex mathematics and logic to design strong encryption methods. Cryptography is also an art. Cryptography allows people to keep confidence in the electronic world. Encryption is the only way to protect our privacy and provide desired level of security. This art of Encryption Decryption lies in the cryptographic algorithms, which provide the locks and keys of this Information Age. Today's world is the age of universal electronic connectivity, our phone calls, e-mails, electronic devices, online electronic transaction passes through various electronic devices. The rapid increase of information transmitted electronically resulted to an increased reliance on cryptography. This leads to a rapid increase in the need of security services such as confidentiality, integrity, authentication etc. These security services are solely depends on cryptographic algorithms. These cryptographic algorithms in turn lie in the heart of Mathematics i.e. in Number Theory.

This faculty development programme (FDP) is designed to address the foundations of cryptography. The fundamental theory, practical aspects and research direction are the major topics to be covered in this programme.

Major Course Contents:

- Number Theory
- Abstract Algebra
- Integer factorization problem
- The discrete logarithm problem
- Primality test
- Perfect secrecy and computational secrecy
- Design and implementation of Stream and block ciphers
- One way Functions and Computationally hard problems
- Design and implementation of Public Key Cryptography
- Applications
- Design and Implementation of Elliptic Curve Cryptography
- Advanced Topics
- Research aspects and direction
- Hands on experience multi-precision integer tool (gmp), Number theory library (*NTL*) and SAGE (math library)

Faculty conducting this Programme:

The programme will be conducted by the faculty members from **NIT Warangal**. Eminent resource person in the concerned field from **DRDO/ISI/IITs/NITs/IIITs** are invited to deliver lectures in the programme. Speakers from **industries** are also expected to deliver as part of the course.

Eligibility:

The programme is open to the ***teachers of engineering colleges, MCA colleges and other allied disciplines*** in Telangana, Andhra Pradesh, Karnataka states and Puducherry, Andaman and Nicobar Islands, GoaUTs. Industry personnel working in the concerned/allied discipline can also attend.

Registration Fee Particulars:

- **Faculty from above mentioned states (Rs 3000/· Only)**
- **Faculty from ISEA Project-Phase II Participating Institutes (Rs 3000/· Only)**
- **Industry participants (Rs 9000/·Only)**
- **Research Scholars (Rs 3000/- Only)**
- **Faculty from states/UTs (other than above mentioned)**
  a) **Rs 12500/- Only (inclusive of boarding & lodging)**
  b) **Rs 6000/- Only (actual charges for lodging and boarding are extra)**

The participants need to send a crossed demand draft (DD) drawn in favour of "Director, NIT Warangal" and payable at SBH, NIT Warangal branch.

Accommodation:

All the selected participants will be provided FREE boarding & lodging in the institute guest house. No TA will be paid for the participants.

How to apply:

A filled in form of application in the prescribed format duly signed and sponsored by appropriate authorities (along with demand draft) should reach the coordinator by speed-post. It is also mandatory to send scanned application form and demand draft through e-mail to **rpadma@nitw.ac.in** or **r_padma3@rediffmail.com**. Selection will be intimated only through mail.

Selection Criteria:

Selection will be done based on ***first-cum-first-serve basis*** and the confirmed candidates will be notified immediately. The maximum number of participants will be **50 (fifty)**. Additionally 10 participants from industry are allowed to participate. The list of selected participants will be notified in the institute web site www.nitw.ac.in and also will be sent to their personal *e-mail* ids. In case a candidate is not selected, the demand draft will be sent back. A test will be conducted at the end of the course. Candidates will be issued certificates on successful completion of the course along with grade. Reservations are followed for selecting candidates as per GOI norms.

Important dates:

Last date for submission of application: 12.12.2016

Selection-list intimation/display before: 15.12.2016

Duration of Program: 19th – 30th December 2016

About the Institute, Department and Warangal:

National Institute of Technology (formerly Regional Engineering College), Warangal is the first among 17 RECs setup as joint venture of the Government of India and the state government. Over the years the college has established itself as a premier Institution imparting technical education of a very high standard leading to the B.Tech degrees in various branches of engineering and M.Tech. and Ph.D. programs in various specializations. The Department of Computer Science and Engineering (CSE) offers B.Tech course in CSE, M.Tech courses in CSE, Computer Science and Information Security (CSIS) and Master of Computer Applications (MCA). The Department has experienced faculty with good publications and well-established laboratories. The Department has liaison with reputed industries and R&D organizations like Microsoft, IBM, Oracle, Accenture, Infosys, TCS, EMC^2, C-DAC, Motorola, NIC, Sun Micro Systems, SPSS and tie up with IISc in certain areas. Department conducts various sponsored programmes throughout the year.

Warangal is known for its rich historical and cultural heritage. It is situated at a distance of 140Km. from Hyderabad. Warangal is well connected by rail and road. National Institute of Technology campus is 2 Km. away from Kazipet junction and 12Km. away from Warangal station.

Tentative Lecture Plan:

1. **Number Theory:** Divisibility, Congruence, Quadratic reciprocity and Quadratic forms, Algorithms in $\mathbb{Z}_n$ (2 Hrs.)
2. **Abstract Algebra:** Groups, Rings, Fields, Polynomial Rings, Vector Spaces, Finite Field, Extension Field, Arithmetic on Extension Field, Generators and elements of high order. (4 Hrs.)
3. **Integer factorization problem:** Trial Division, Pollard's rho factoring algorithm, Pollard's p-1 factoring algorithm, Elliptic curve factoring, Random square factoring methods, Quadratic Sieve factoring, Number Field sieve factoring, Factoring Polynomials over finite field, Irreducible polynomials over $\mathbb{Z}_p$. (4 Hrs.)
4. **The discrete logarithm problem:** Exhaustive search, Baby-step giant-step algorithm, Pollard's rho algorithm for logarithms, Pohlig-Hellman algorithm, Index-calculus algorithm, Discrete logarithm problem in subgroup of $\mathbb{Z}_p^*$. (4 Hrs.)
5. **Primality test:** Fermat's test, Solovay-Strassen test, Miller-Rabin Test, Testing Mersenne Number, Primality testing using the factorization of n-1, Jacobi sum test, Test using elliptic curves. (2 Hrs.)
6. **Perfect secrecy and computational secrecy.** (2 Hrs.)
7. **Design and implementation of Stream and block ciphers** (4 Hrs.)
8. **One way Functions and Computationally hard problems** (2 Hrs.)
9. **Design and implementation of Public Key Cryptography** (6 Hrs.)
10. **Applications:** MAC, digital signatures, Key Establishment protocols, Key management Techniques, Standards (NIST, FIPS etc.) (2 Hrs.)
11. **Design and Implementation of Elliptic Curve Cryptography** (4 Hrs.)
12. **Advanced Topics:** Introduction to Number field sieve and function field sieve, Lattice Based Cryptography, Light Weight cryptography (4 Hrs.)
13. **Research aspects and direction** (2 Hrs.)
14. **Hands on experience Multi-precision integer tool (gmp), Number theory library (*NTL*) and SAGE (math library)** (38 Hrs.)

FORMAT OF APPLICATION

Electronics and ICT Academy

Faculty Development Programme

On

Foundations of Cryptography

(19th– 30th December, 2016)

1. Name:
2. Gender: Male / Female
3. Designation:
4. Institution:
5. Email & Mobile Number:
6. DD No: Bank: Date:
7. Address for Correspondence
8. Educational Qualifications with specialization:
9. Subjects taught so far:
10. No. of refresher courses/workshops attended:
11. Experience (in years)
    Teaching:
    Research:
    Industry:
12. Accommodation required: YES / NO
13. Are you belong to SC/ST: YES / NO

Declaration

The information provided is true to the best of my knowledge. If selected, I agree to abide by the rules and regulations of the FDP and shall attend the course for the entire duration. I also undertake the responsibility to inform the Coordinator in case, I am unable to attend the course.

Place:
Date: Signature of the applicant

SPONSORSHIP CERTIFICATE

Dr/Mr/Ms.
……
……
…….....is an employee of our Institute/Organization and is hereby sponsored to participate in the FDP on ***Foundations of Cryptography*** sponsored by Electronics & ICT Academy during 19th – 30th December, 2016 at *Electronics & ICT Academy*, National Institute of Technology, Warangal.

Place:
Date:

Signature of Head of Institution
(With seal)

Address for correspondence

Post your application form with DD to

Dr. R. Padmavathy

Department of Computer Science & Engg.,
National Institute of Technology Warangal,
WARANGAL - 506 004, Telangana State, India.

Mail the scanned copies of filled-in and duly signed application form with DD to
rpadma@nitw.ac.in or
r_padma3@rediffmail.com

For more information visit:
http://nitw.ac.in/eict/

For any enquiry contact:
Mobile : 09440173819
Land line: 0870-2462738

Coordinators

Dr. R. Padmavathy and Dr. Ravichandra. Sadam

Organized by

Electronics & ICT Academy and

Department of Computer Science and Engineering

NATIONAL INSTITUTE OF TECHNOLOGY

WARANGAL - 506 004 (Telangana State)