Centre for Continuing Education
(QIP Programme – Sponsored by AICTE)
Indian Institute of Science, Bengaluru – 560012, Karnataka, India
Ph: 080-22932491, 22932247 Fax: 080-23600911
E-mail: office.cce@iisc.ac.in, so.cce@iisc.ac.in
Website: http://cce.iisc.ac.in

****

QIP Short Term Course On FOUNDATIONS OF CRYPTOGRAPHY 23rd – 27th July 2018

Introduction

Cryptography is the science of secrets. It involves the study of mathematical techniques for securing digital information, systems and distributed computations against adversarial attacks. It has a significant relevance in our daily life, especially in the context of current digital society. Now a central topic within computer science, cryptography is a great enabler of information security

Course Objective

This course provides the basic paradigm and principles of modern cryptography. The focus of this course will be on definitions and constructions of various cryptographic objects. We will try to understand what security properties and desirable in such objects, how to formally define these properties, and how to design objects that satisfy the definitions. The aim is that at the end of this course, the participants are able to understand a significant portion of current cryptography research papers and standards. The topics covered in the course will be also useful for the participants who are willing to work on Network Security and Computer Security. In a nut-shell, this course will build the required foundation on top of which various complex and real-world cryptographic applications are built.

Course Contents

Course contents (for tentative 30 hrs. of contact): The course will be divided into following two major units, which will have several topics under them. The first unit deals with symmetric-key (a.k.a private-key) cryptography, while the second unit deals with asymmetric-key (a.k.a public-key) cryptography.

- Unit I: Classical cryptography, perfectly-secure encryption and limitations, computational-security, pseudo-randomness and private-key encryption, stream ciphers and block ciphers, message authentication, hash functions, theoretical constructions of pseudo-random objects, private-key management and public-key revolution.
- Unit II: Number theory and cryptographic-hardness assumptions, public-key encryption: overview and various schemes, digital signatures, random-oracle model.

Lectures

Lectures will be delivered by Institute faculty members.

Eligibility:

The course is meant for teachers of engineering colleges recognized by All India Council for Technical Education (AICTE) who send their applications through proper channel. There is no course fee for them. Selected teachers will be paid TA at actuals subject to the limit of Three tier AC train/bus fare by the shortest route from the place of work to Bengaluru and back. However, the maximum TA payable is Rs.3000/-. They will be provided with a daily allowance of Rs.500/- (for 5 days only) towards boarding and lodging as per QIP rules, and will be supplied with the course material. The lodging charges will be Rs.300/- per day. Local participants will be paid DA @ Rs.150/- per day for 5 days. The total numbers of seats are limited to 70 for applying on first come first serve basis and 35 candidates will be selected for the course.

In addition, non-sponsored AICTE approved college teachers and other self-support teachers, scientists from research labs, practicing engineers from industries and other interested are eligible. They should pay the fees online along with the application as under.

Fees	**Faculty: 10000+18% GST INR** **Industry Participants: 15000+18% GST INR** They will be entitled to participate in the course and receive the course material. Single room accommodation is available on the Institute campus at the Hoysala House. The participants have to request in advance along with the registration form for such accommodation. The lodging charges will be Rs.1000/- per day for self-support college teachers and Rs.1500+18%GST per day for Industry participants, subject to availability of accommodation.

For More Details Contact	Section Officer Centre for Continuing Education Indian Institute of Science Bengaluru – 560012 Ph: 080 - 2293 2055/ 2293 2491/ 2360 0911 Email: so.cce@iisc.ac.in, office.cce@iisc.ac.in

Apply online at:	http://iisc.online/qip/home.html

Co-ordinator

Dr. Arpita Patra
Dept. of CSA

Last Date to Apply:
02/04/2018

Intimation of Selection:
05/04/2018