REGISTRATION FORM

Faculty Development Programme
on
Cryptanalysis : Tools and Techniques
4th - 8th December 2017

Full Name :
Designation :
Organization:.....
.....
Qualification:.....
Specialization:.....
Mailing Address:.....
.....
.....
Pin Code:.....Phone(M).....
(O).....Email:.....
Aadhar No:.....

Accommodation required ? Yes /NO

DETAILS OF REGISTRATION FEE

Name of Bank & Branch_____

DD No:_____Dt_____

For Rs._____ in favour of "**Director,**

NITK, Surathkal " payable at Surathkal, is enclosed.

Date:_____ Signature of Participant

The applicant will be permitted to participate in this

Workshop, if selected.

SIGNATURE AND STAMP OF THE SPONSORING AUTHORITY

(Please post your completely filled registration form along with DD)

REGISTRATION

Faculty of Academic Institutes/Industries	Rs.2000/-
Students / Research Scholars	Rs.1000/-

For registration duly filled Registration from along with Demand Draft drawn in favour of **Director NITK, Surathkal** should be sent in advance to the Course Coordinators through Email or in original through registered post. The confirmation would be sent through Email. The registration fee includes course materials, certificate, working lunch and tea.

ACCOMMODATION

Limited accommodation is available in the Guest House/Hostels of the NITK, Surathkal for outstation participants on the nominal chargeable basis with an advance request and on a first come first serve basis. The participant will not be paid any TA/DA.

IMPORTANT DATES

Last Date to Register : 27th November , 2017
Acceptance Notification: 1st December , 2017

ADDRESS FOR CORRESPONDENCE :

Dr.Alwyn Roshan Pais , Coordinator
Department of Computer Science & Engineering
National Institute of Technology - Karnataka
Surathkal , P.O. Srinivasnagar,
Mangalore - 575 025.
E-Mail : alwyn.pais@gmail.com
Web : http://isea.nitk.ac.in

Venue: Dept. of CSE, NITK, Surathkal

Faculty Development Programme
on
Cryptanalysis : Tools and Techniques
4th - 8th December 2017

Organized By

Department of Computer Science & Engineering, National Institute of Technology Karnataka Surathkal, P.O. Srinivasnagar Mangalore - 575 025 Website: http://isea.nitk.ac.in

Resource Center
for

Information Security Education and Awareness Project(ISEA),Phase-II

Course Coordinators

Dr.Alwyn Roshan Pais
&
Dr.P.Santhi Thilagam
Dept, of CSE ,NITK, SURATHKAL

ABOUT NITK SURATHKAL

National Institute of Technology Karnataka, Surathkal has established itself as one of the top technological institutions in India & is declared as an Institute of National Importance under the NIT Act 2007. Since its inception in 1960 as the Karnataka Regional Engineering College (KREC), the institute is considered as a premier center engaged in imparting quality Technological education and providing support to research and development activities. The institute has a long tradition of research for several decades in both traditional and modern areas of engineering and science.

ABOUT CSE DEPARTMENT

Department of Computer Science and Engineering, established in the year 1986 has strong International reputation for its excellence in education and research. It has a rich history and an outstanding record of contributions to the ever growing field of Computer Science & Engineering. The Department offers B.Tech, M.Tech, M.Tech (By Research), M.Tech (Information Security) and Ph.D. in Computer Science & Engineering Discipline. The Department has also established a Information Security research Lab from various R&D fundings received from various Government agencies. The Department is also accredited by NBA. For more information on the Department of Computer Science and Engineering at National Institute of Technology Karnataka, Surathkal, please visit: http://cse.nitk.ac.in

TARGET AUDIENCE

The Program is targeted towards postgraduates, researchers, scholars, faculty members from academic institutes, industry professionals & consultants.

OBJECTIVES OF THE FDP

The major objective of the FDP is to study the major topics in cryptanalysis. In involves a variety of ways to break, fix/repair and to measure/evaluate the security of cryptographic primitives. It will also involve understanding the maths , the security design principles, the internal structure and important properties of major cryptosystems. A study of major computational hard problems in cryptography (symmetric and public key) will also be provided. Step by step analysis of mathematical/algebraic/statistical attacks, methods and algorithms in cryptanalysis using different tools will be studied.

THE MAJOR CONTENTS OF THE PROGRAMME ARE :

* Introduction to Cryptanalysis
* Computational Complexity
* Secret Parameters and keys
* Tools for Symmetric cryptanalysis
* Tools for asymmetric cryptanalysis.

METHODOLOGY

In addition to classroom lectures, the programme includes discussions, hands-on sessions, assignments.

ORGANIZING COMMITTEE

PATRON

Prof. Karanam Uma Maheshwar Rao,
Director NITK Surathkal.

CO-ORDINATORS

Dr.Alwyn Roshan Pais (NITK-Surathkal)
Dr.Santhi Thilagam (NITK-Surathkal)

RESOURCE PERSONS

1.Dr.Bimal K. Roy, ISI-Kolkatta
2.Dr.KannanSrinathan, IIIT-Hyderabad
3.Dr. B. B. Amberker, NIT-Warangal
4.Dr. B. R. Purushothama, NIT-Goa
5.Dr. Ashok Kumar Das, IIIT-Hyderabad
6.Dr.SanthiThilagam(NITK-Surathkal)
7.Dr.AlwynRoshanPais (NITK-Surathkal)

ELEGIBILITY

This FDP is open to UG & PG Students, Research Scholars, Faculty Members and Industry Professionals. Registration is based on First Come First Served basis.