

Registration Fee

- UG/PG Students –Rs 500/-
- Research Scholars –Rs 1000/-
- Faculty/Teaching Assistants –Rs 1500/-
- NITC Alumni –Rs 2000/-
- Professionals from the Industry –Rs 3000/-

(fee inclusive of taxes)

Registration:

For registration, fill the online Google form link given below with the scanned copy of the signed endorsement form and payment receipt and email the same to fomc2021@nitc.ac.in. The bank details are given below for online transfer:

- Account holder name: **DIRECTOR NIT CALICUT-CONTINUING EDUCATION PROGRAMME**
- Account No: **37618269594**
- IFSC: **SBIN0002207**
- Bank: **State Bank of India, NIT Calicut Campus**

Last date for registration and fee payment is **12th Nov 2021.**

Participants shall be notified by **14th Nov 2021.**

Google form link for registration is:
<https://forms.gle/i38uZcZfFE7tS39q9>

Resource Persons

Experts from Premier Academic Institutes and Industry:

Dr. Chester Rebeiro, CSE-IIT Madras
Dr. Gaurang Panchal, Technical Expert - Cyber Security at Siemens Technology India
Dr. Maria Francis, CSE-IIT Hyderabad
Dr. R. Padmavathy, CSE-NIT Warangal
Faculty Members from Cryptography and Security at CSE, NIT Calicut.

Who can apply?

Faculty members/research scholars, UG/PG students and professionals from industry, who are working / interested in the area of security and cryptography are motivated to apply.

Endorsement of the Head of the Institution/Department

Certified that Mr./Ms./ Dr.....
.....is a/
an faculty / UG student/PG student/ research scholar / employee of this Institution and is here by sponsored for the online continuing education programme on **Foundations of Modern Cryptography (FoMC-2021)** at NIT Calicut during **15th - 19th Nov 2021.** She / He will be permitted to attend the course, if selected.

Place :

Name & Signature of the

Date :

Sponsoring Authority

(seal of the institution)

Coordinators

Dr. Anil Pinapati, and Dr. Jimmy Jose
Department of Computer Science and Engineering
National Institute of Technology Calicut
NIT Campus PO, Calicut, Kerala-673601
India

Email : fomc2021@nitc.ac.in

Contact : +91 495-2286801

Online Continuing Education Programme (CEP)-2021

ON

Foundations of Modern Cryptography (FoMC-2021)

NOV 15 - 19, 2021



तमसो मा ज्योतिर्गमय

Organized by

Department of Computer Science
and Engineering

National Institute of Technology Calicut

History of the Department

The BTech programme in Computer Science and Engineering started in 1985 under the Department of Electrical Engineering. The Department of Computer Science and Engineering was formed in June 1997. The three-year MCA programme started in 1988. The two-year MTech programme in Computer Science and Engineering started in 1998. The two-year MTech programme in Computer Science and Engineering (Information Security) started in 2006. PhD programme started in 2002.

Vision and Mission

VISION: To be a Centre of Excellence in the Discipline of Computing.

MISSION: To develop human resource with sound knowledge- theory and practical - in the discipline of computing and the ability to apply the knowledge to the benefit of the society at large.

Profile of the Department

Department of Computer Science and Engineering offers Undergraduate and Postgraduate programs in Computer Science and Engineering, Master of Computer Applications program, and a Doctoral degree program. The fast changing scenario in Information Technology necessitates the Department to actively extend its research and development activities. The current research interests of the Department include major areas of research in Computer Science.

About the Institute

National Institute of Technology Calicut (NITC) is fully centrally funded by the Ministry of Education (formerly MHRD) and is governed by the NITSER Act 2007. The Institute has twelve departments, three schools and eight research centres. It offers eleven UG, and thirty PG programmes along with the PhD programme in various fields of Science, Engineering and Management. Faculty members in the various Departments have active collaborations with universities and elite institutions within and outside India for research and consultancy. For details visit our website www.nitc.ac.in

About Calicut

NITC is located about 22 kilometers north-east of Calicut City. Calicut or Kozhikode, is known as the city of spices. Calicut is a major knowledge hub of Kerala and is the hometown of institutions of national importance including NITC, IIMK, DOEACC, CWRDM. Calicut is connected by direct trains/road/air to all major cities in India. Kozhikode beach, Kappad beach, Kadalundy bird sanctuary, Tusharagiri Waterfalls, Pazhassiraja Museum, Tali Temple and Kuttichira Masjid are some of the local attractions. Kappad beach, a Blue Flag certified beach, is the place where the Portuguese explorer Vasco da Gama is believed to have landed in 1498.

Preamble

Nowadays, majority of our interactions happen online due to the pandemic. Cryptography allows people to keep confidence in the electronic world. The rapid increase of information transmitted electronically resulted in an increased reliance on cryptography. This leads to a rapid increase in the need of security services such as confidentiality, integrity, authentication and non-repudiation. These security services solely depend on cryptographic algorithms. In order to provide security to online communications, it is mandatory to learn the fundamental concepts of modern cryptography techniques.

This Faculty Development Programme (FDP) focuses on modern cryptography and provides insights into understanding cryptosystems better. The fundamental theory, practical aspects and research directions are the major topics to be covered in this programme. The topics are connected with **computer security** as well.

Major Course Contents:

- Basic concepts in Number Theory and Abstract Algebra
- RSA, Integer Factorization Problem (IFP)
- The Discrete Logarithm Problem (DLP)
- The evaluation of side-channel leakage
- Pseudo Randomness, Stream ciphers
- One-Way Functions
- Computationally hard problems
- Elliptic Curve Cryptography (ECC)
- Quantum Cryptography
- Applications of Cryptography
- Current Trends in Security: An Industry Perspective
- Hands on experience on Number Theory Library (NTL)