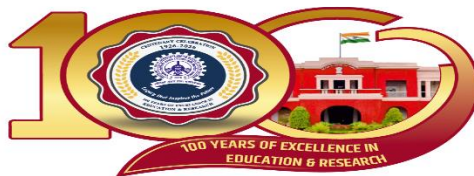इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
सत्यमेव जयते

IIT (ISM)
DHANBAD
1926-2026
LEGACY THAT INSPIRES THE FUTURE.

100 YEARS OF EXCELLENCE IN
EDUCATION & RESEARCH

ISEA

Short Term Course
On

Cryptography & Cryptology: Securing the Digital World

10-14 December 2024

Organized by

Department of Computer Science and Engineering
Indian Institute of Technology (Indian School of Mines) Dhanbad-826004, Jharkhand, India

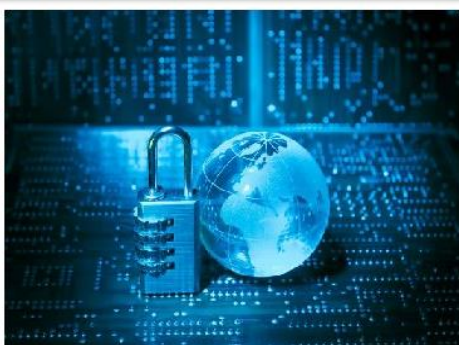Sponsored by MeitY, Govt. of India

Under ISEA Project (Phase -III)

Registration Deadline

09 December 2024

Registration: No Registration Fee

(Only Limited Number of Seats are available.)

Interested participants are requested to submit an Application Form

https://faas.isea.app/formview/CCSDW

Importance and Scope

In the current IT age, we are benefiting from advancements in efficient computation, communication, entertainment, e-marketing, social networking, and more. People across the globe collaborate seamlessly, overcoming geographical barriers to innovate and create new solutions. However, security risks have emerged as a significant concern, growing rapidly in multiple dimensions. Without adequate security measures, none of these IT benefits can be fully realized. For instance, transmitting sensitive messages or images through open channels like the Internet requires confidentiality, which is achieved using cryptographic techniques. Similarly, the authentication and integrity of messages are equally critical to prevent unauthorized access and tampering. Cryptography addresses these needs by providing robust methods for secure communication. Cryptology, encompassing cryptography and cryptanalysis, plays an even broader role. It not only develops tools to secure information but also analyzes and counters vulnerabilities in existing systems. This field is essential for protecting data in diverse applications, including financial transactions, secure messaging, military communications, and emerging technologies like blockchain and quantum computing.

This short-term course introduces the fundamental mathematical concepts necessary for understanding and developing cryptographic techniques, highlighting the indispensable role of cryptology in securing the digital world.

Course Outline

- Introduction to Information Security
- Mathematics of Cryptography
- Modern Symmetric-Key Ciphers and Their Cryptanalysis
- Asymmetric-Key Cryptography and Their Cryptanalysis
- Digital Signature
- Key Management
- Cryptographic Hash Function and Blockchain
- Quantum Resistant Cryptography
- Image/Video Security

Course Instructors

Faculty members from Department of Computer Science and Engineering, IIT (ISM) Dhanbad will conduct this course.

Date and Venue

December 10-14, 2024 at Dept. of CSE, IIT (ISM), Dhanbad.

Target Participants and Eligibility Criteria

The target participants include both internal and external faculty members, scientists, industry professionals, research scholars, and M.Tech/B.Tech students.

About Location

IIT(ISM) Dhanbad is well connected by rail and road. The institute is located at a distance of about 3 KMs from Dhanbad Railway Station in Jharkhand State.

Contact Details

Prof. Arup Kumar Pal, Coordinator,
Dept. of Computer Science & Engineering
Indian Institute of Technology (Indian School of Mines), Dhanbad, Jharkhand-826004
Phone: 9471191835 and Email: arupkrpal@iitism.ac.in