10. The reimbursement of travel expenses is limited to a maximum Rs. 3,000/-. We request you to inform us if you require reimbursement of travel expenses.

Yes | No

Date :

Signature of applicant

Note :

1. This application form should reach the QIP Office latest by **02.11.2017.**
2. We will not entertain applications without sponsorship certificate.
3. Please note that 100% attendance is compulsory for the course.

SPONSORSHIP CERTIFICATE

This applicant is permitted to participate in the above programme if selected. Further, I have personally talked to the applicant and he/she is confident of attending the course in case admission is offered to him/her.

This is to certify that this institute is recognized by AICTE.

Date :

Signature
Sponsoring Authority
(Principal / Director)

SEAL

OBJECTIVES OF THE COURSE:

Cryptology is employed to communicate securely, authenticate messages and sign digitally. This QIP course "Introduction to Cryptology" is designed for both computer science and mathematics teachers interested in the basics of the subject. This course touches upon the most important ideas and techniques of the present day cryptology. An introduction to quantum computation and quantum cryptography is also included as a new element. All the pre-requisite topics are revised during the lectures making this course self-contained and accessible to a wider audience.

COURSE CONTENTS:

Day 1: **Classical Cryptography**: L1 : Introduction, Caesar cipher.
L2 : Modular arithmetic. The shift Cipher.
L3 : The affine cipher, The Vigenere cipher.
L4 : Information Theory Introduction.
L5 : Perfect secrecy, Entropy.

Day 2: **Block Cipher**:
L6 : Introduction.
L7 : Substitution Permutation Network. 30 min.
L8 : S-box theory.
L9 : Vector Boolean functions.
L10: Linear and differential attack on block ciphers.

Day 3: **Public Key Cryptography**:
L11: Introduction, Required number theory results.
L12 : Extended Euclidean Algorithm.
L13 : Description of RSA.
L14: Chinese Remainder theorem and Quadratic Residues.
L15: RSA key generation primality testing. Miller and Rabin algorithm.

Day 4 : **Cryptographic Hash Functions**:
L16: What is a cryptographic hash function? The random oracle model.
L17: Preimage resistance, second preimage resistance.
L18 : Birthday paradox.
L19 : Collision resistance.
L20: Iterated hash functions, The Merkal Damgard construction.

Day 5: **Quantum Cryptography**:
L21: Introduction toQuantum Computing 1.
L22 : Introduction to Quantum Computing 2.
L23 : Properties of Quantum Gates.
L24 : Deutsch – Jozsa Algorithm.
L25 : BB84 Quantum Key exchange protocol.

COURSE COORDINATOR(S):

Dr. Sugata Gangopadhyay
Associate Professor
Deptt. of Computer Sc. & Engg.
IIT Roorkee
Tel.: 01332 – 285582
Email: sugatfma@iitr.ac.in

Dr. Aditi Gangopadhyay
Associate Professor
Deptt. of Mathematics
IIT Roorkee
Tel.: 01332 – 285829
Email: aditifma@iitr.ac.in

AICTE SPONSORED
SHORT TERM COURSE

INTRODUCTION TO CRYPTOLOGY

Organized by

Department of Computer Science & Engineering
and
Mathematics
Indian Institute of Technology Roorkee
ROORKEE - 247667

04.12.2017 to 08.12.2017

QUALITY IMPROVEMENT PROGRAMME CENTRE
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE - 247 667 (Uttarakhand)

Phone : (01332) 285241, 284341
Fax : (01332) 286691, 273560
Email : qip@iitr.ernet.in

General Information

The Indian Institute of Technology Roorkee is organizing a course on "**Introduction to Cryptology" from 04.12.2017 to 08.12.2017.**The course is open to teachers from AICTE-recognized engineering colleges.

Limited seats are available in this course. Merit will be taken into consideration while selecting candidates. The application on the enclosed form, duly signed by the sponsoring authority, should reach the QIP Office latest by **02.11.2017.** The candidate will be informed of his / her selection in advance.

Candidates admitted will be provided free hospitality. The boarding and lodging arrangements for all the participants will be made in the institute Guest House on twin sharing basis. Participants who are not availing this facility will not be entitled to any rebate. Family accommodation is not available on campus. However, personal arrangements in city hotels can be made at own's expense.

Applications on the attached form with due sponsorship should be sent to the address given below. In case sponsorship takes time, one can send an advance photo copy, so as to reach before the due date by email. However, no candidate will be admitted without due sponsorship.

About Roorkee

Roorkee is located at the foothills of the Himalayas in Uttarakhand State. The Railway Station is on the main line of Northern Railways with direct links to Delhi, Mumbai, Calcutta, Amritsar, Jodhpur and Ganganagar. It is also within easy reach from Delhi by road (180 km), and is located on Delhi - Haridwar and Delhi - Dehradun bus routes. Roorkee is ideally located near several tourist destinations, including Dehradun (70 km), Mussoorie (100 km), Haridwar (32 km), and Rishikesh (52 km).

List of Short Term Courses during 2017 – 2018

Sl. No.	Name of Course Coordinator	Department	Course Title	Duration
1.	Prof. Zillur Rahman Prof. Rajat Agarwal Prof. Vinay Sharma	Management Studies	Social Media Marketing	May 22 – 26, 2017
2.	Prof. Madhu Jain Prof. Kusum Deep	Mathematics	Stochastic Modeling and Optimal Control of Engineering Systems	May 22 – 26, 2017
3.	Prof. K.S. Suresh Prof. G.P. Chaudhari	Metallurgical and Materials Engineering	Advanced Techniques in Microstructural Characterization	May 29 – June 02, 2017
4.	Prof. Pradeep Kumar Prof. Akshay Dvivedi	Mechanical and Industrial Engineering	Quality Management: Issues, Tools and Techniques	May 29 – June 09, 2017 **(Two Week)**
5.	Prof. Indra Vir Singh Prof. B.K. Mishra	Mechanical & Industrial Engineering	Finite Element Methods for Engineering Applications	June 12 – 16, 2017
6.	Prof.Jaydev Debas Prof. Sanjeev Kumar	Applied Sciences and Engg. and Mathematics	Research Skills and Methods in Computational sciences with Engineering Applications	June 12 – 16, 2017
7.	Prof. V. Devadas Prof. E. Fernandez	Architecture & Planning and Electrical Engg.	Urban Dynamics and Planning Techniques	June 26 – 30, 2017
8.	Prof. Manoj Tripathy Prof. Yogesh Vijay Hote	Electrical Engineering	New Trends in Power System Protection and Control Techniques	June 26 – 30, 2017
9.	Prof. Smita Jha Prof. A.J. Mishra	Humanities and Social Sciences	Significance of Literary Theories in Humanities and Social Sciences	July 03 – 07, 2017
10.	Prof. Sujata Kar Prof. Ramesh Anbanandam	Management Studies	Econometrics with Application of 'R' Programming	July 03 – 07, 2017
11.	Prof. Sonalisa Ray Prof. Mohd. Ashraf Iqbal	Civil Engineering	Recent Advances in Fracture and Fatigue	July 10 – 14, 2017
12.	Prof. D.B. Karunakar Prof. D.K. Dwivedi	Mechanical & Industrial Engineering	Enhancing Yield in Metal Casting Industry	July 10 – 14, 2017
13.	Prof. Ram Sateesh Pasupuleti Prof. Uttam Kumar Roy	Architecture and Planning	Architecture and Planning Pedagogy in the Digital age	July 17 – 21, 2017
14.	Prof. Ashok K. Ahuja Prof. Pramod K. Gupta	Civil Engineering	Wind Resistant Design of Structures	July 17 – 21, 2017
15.	Prof. Sugata Gangopadhyay Prof. Aditi Gangopadhyay	Computer Science & Engineering and Mathematics	Introduction to Cryptology	Dec. 4-8, 2017
16.	Prof. Vivek K. Malik Prof. Tulika Maitra	Physics	Novel Quantum Electronic Materials: Theoretical and Experimental Approach	Dec. 18-22, 2017
17.	Prof. K.L. Yadav Prof. Monojit Bag	Physics	Critical Raw materials Management for Green Energy and Sustainability	**To be announced later**

Application Form for
Short Term Course (STC)
on
"Introduction to Cryptology"
Duration: 04.12.2017 to 08.12.2017

(You may get the form enlarged by xeroxing on A4 Size paper or download Application Form from website: www.iitr.ac.in for submission of your application)

After Completion, Please Mail to:
Dr. Bhupendra K. Gandhi
Professor & Coordinator
Q.I.P. Centre, I.I.T. Roorkee
ROORKEE – 247667 (Uttarakhand)
Phone : (01332) 285241 & 284341
Fax : (01332) 286691, 273560
Email : qip@iitr.ac.in, qip.iitr@gmail.com

Affix
Passport Size
Photograph

1. Name: Ms./Mr./Dr.
(In block letters)

2. Designation:

3. Age (years):

4a. Residential address with pin code, telephone no., mobile

Tel: Mobile:

4b. Complete official mailing address:
(Including name of state and pin code number)

Email**:**
Phone (Off.) Fax**:**

4c. Name of the Institute where employed:

4d. Name of the Department:

5. Academic qualification (degree onwards) (Attach Brief CV):

6. Specialization:

7. Teaching experience in years:

8. Subjects taught related to this STC

9. No. of STCs attended so far

At Roorkee ..... At other places .....Total .....