

### EXPECTED RESOURCE PERSONS

The lectures will be delivered by eminent faculty from reputed Institutes like IITs, ISI, NITs etc.

### WHO CAN ATTEND

The programme is designed for the Faculty from AICTE approved Engineering colleges, Degree colleges, Research Scholars & PG students, and also for working professionals from industry and R & D organizations. Participants are invited to register by sending the duly filled **Registration Form** enclosed herewith.

### REGISTRATION FEE

Category of Participants	Registration Fee*	Registration Fee**
Faculty of Educational Institutions	Rs. 2,000/-	Rs. 500/-
Research Scholars & PG students	Rs. 2,000/-	Rs. 500/-
Participants from industry and R&D organizations	Rs. 5,000/-	--

\*includes accommodation, boarding and snacks

\*\* for Internal participants

The participants need to send crossed DD drawn in favor of "TEQIP III Funds", payable at SBI, NITW branch, Warangal. They can also pay the registration fee by online money transfer, the details of which are as follows:

Account Name	TEQIP III Funds
Account Number	37583198741
Bank	State Bank of India
Branch (Code 20149)	REC Warangal, NIT Campus
IFS Code	SBIN0020149

### IMPORTANT POINTS

- The number of delegates aimed for the programme is **limited to 20**. Therefore, the registration is based on the **first come first serve basis**.
- Mail the scanned copy of
  - 1) **completely filled registration form &**
  - 2) **DD/Online Payment Receipt to****ysr@nitw.ac.in cc to rsselva@nitw.ac.in**
- The hard copies of the completed registration form and DD/online-receipt should reach the Coordinators **on or before 10<sup>th</sup> Jan. 2019**.

Confirmation by e-mail on first come first serve basis

### ACCOMMODATION

The registered participants will be provided free boarding and lodging. No TA/DA will be paid.

## National Institute of Technology Warangal - 506 004 (T.S.)

A Five Day Workshop  
on

Cryptography & Coding Theory  
28<sup>th</sup> Jan. – 1<sup>st</sup> Feb. 2019

### REGISTRATION FORM

Name : \_\_\_\_\_

Designation : \_\_\_\_\_

Department : \_\_\_\_\_

Organization : \_\_\_\_\_

Mailing Address : \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Mobile : \_\_\_\_\_

Email : \_\_\_\_\_

### Registration Fee - DD/Online Transfer Details:

DD No.: \_\_\_\_\_

Online Transaction No.: \_\_\_\_\_

Amount: \_\_\_\_\_ Date: \_\_\_\_\_

Bank Name: \_\_\_\_\_

### Accommodation requirement:

Required  Not Required

Place:

Date: \_\_\_\_\_ **Signature of the Delegate**

I recommend the registration of the above person for attending the five day Workshop on **Cryptography and Coding Theory**.

Signature with seal  
Head of the forwarding Institute

## A Five Day Workshop on Cryptography & Coding Theory

28<sup>th</sup> Jan. - 1<sup>st</sup> Feb. 2019  
(Sponsored by TEQIP Phase-III)

On the eve of Diamond Jubilee Celebrations of  
NIT Warangal



### Coordinators

Dr. R. S. Selvaraj  
Dr. Y. Sreenivasa Rao



### Organized by

Department of Mathematics  
National Institute of Technology  
Warangal - 506 004 (T.S.)

## ABOUT THE INSTITUTE & WARANGAL

National Institute of Technology (formerly Regional Engineering College) Warangal, is in its Diamond Jubilee year, the first among RECs, setup in 1959. Over the years the institute has established itself as a premier institution imparting technical education of very high standard leading to B.Tech., M.Tech., M.Sc., MCA, MBA and Ph.D. programmes in various specializations. Having accorded the status of *Institute of National Importance*, the Institute currently has 13 departments and few advanced research centres in various disciplines of engineering, basic sciences and management, with nearly 100 laboratories organized in a unique pattern of functioning. Warangal city is known for its rich historical and cultural heritage. It is situated at a distance of 140 km from Hyderabad. Warangal is well connected by rail and road. NITW is about just 2 km away from Kazipet railway station and 12 km from Warangal Railway station.

## ABOUT THE DEPARTMENT

The Department of Mathematics is one of the reputed departments, which functions with 'excellence' as its motto. Started in the year 1959, along with the other engineering and science departments, it has steadily grown as a dynamic centre for academic and research activities. The Department offers Two 2-year (Four Semester) PG programmes namely: M.Sc (Applied Mathematics) and M.Sc. (Mathematics and Scientific Computing). Special emphasis is laid on imparting the concepts rigorously along with applications and computational aspects. The Department also offers PhD programme in Mathematics and has been recognized as QIP centre for Ph. D. in Mathematics. The department is recognized by MHRD as National Resource Centre (NRC) for conducting online courses in Mathematics under SWAYAM.

## WORKSHOP OBJECTIVE

In today's digital world, large amount of sensitive data is being transmitted over wired and wireless communication media. Cryptography deals with security, privacy and confidentiality of communication over insecure channels, whereas Coding theory is concerned with improving reliability of communication over noisy channels.

This workshop is intended to provide a theoretically sound foundation in cryptography and coding theory along with the state-of-the-art research challenges in the respective areas. After laying initial foundations on developing essential mathematical tools like computational aspects of number theory, finite fields, elliptic curves and arithmetic involved in them, the workshop will discuss on a wide range of basic cryptographic primitives with a focus on mathematical definitions of security, namely, provable security.

Moreover, this programme will also throw light on post-quantum cryptography including lattice-based and code-based. This in turn facilitates the participants to understand existing applications of coding and cryptography, and to develop new protocols and applications. It will also offer an opportunity to explore the current practices and challenges in emerging areas like IoT security and block-chain technology.

## CONTENTS TO BE COVERED

Computational Number Theory	Galois Fields & Elliptic Curves Arithmetic
Symmetric Key Cryptography (including DES, AES etc)	Public Key Cryptography, Elliptic Curve Cryptography
Secret Sharing Schemes	Provable Security
Digital Signature Schemes, Multiparty Computation	Functional Encryption including ID-based, Attributed-based
Error-correcting Codes including Goppa, GRS, Gabidulin Codes	Code-based Cryptosystems
Lattice-based Cryptosystems	IoT Security and Block-chain Technology

## PATRON

**Prof. N. V. Ramana Rao**  
Director, NITW

## FACULTY OF THE DEPARTMENT

Prof. D. Srinivasacharya, HOD  
Prof. Y. N. Reddy  
Prof. K. N. S. Kasi Viswanadham  
Prof. J.V. Ramana Murthy  
Prof. Debashis Dutta  
Dr. P. Muthu  
Dr. H. P. Rani  
Dr. A. Benerji Babu  
Dr. Kurmayya Tamminana  
Dr. J. Pranitha  
Dr. Ch. Ramreddy  
Dr. D. Bhargavi  
Dr. Satyanarayana Engu



## IMPORTANT DATES

- 1) Submission of scanned application through e-mail : **07-01-2019**
- 2) Application with DD should reach on or before : **10-01-2019**

## ADDRESS FOR CORRESPONDENCE

**Dr. R. S. Selvaraj & Dr. Y. Sreenivasa Rao**  
[rselva@nitw.ac.in](mailto:rselva@nitw.ac.in); [ysr@nitw.ac.in](mailto:ysr@nitw.ac.in)  
09908539330; 09494776866  
Department of Mathematics  
National Institute of Technology Warangal  
Warangal Urban – 506004, Telangana, India.