

#### ADVISORY COMMITTEE

Prof S.Ramachandram, Vice-Chancellor, OU  
Prof S.Sameen Fatima, Principal, UCE(A), OU  
Prof P. Premchand, Dean, Informatics, OU  
Prof P. Ramkumar, Dept of CSE, UCE, OU

#### CONVENORS

Dr. K. Veerabhadra Rao, Dept of CSE  
Prof. Venkat Dass Maredu, Dept of CSE

#### ORGANISING COMMITTEE

Mr. S. Ram Babu, Head, Dept of CSE  
Mr. S. Srinivas Rao, Dept of CSE  
Mr. L. K. Suresh Kumar, Dept of CSE  
Dr. K. Shyamala, Dept of CSE  
Mrs. P. V. Sudha, Dept of CSE  
Dr. V. B. Narasimha, Dept of CSE  
Mrs. B. Sujatha, Dept of CSE  
Mr. M. A. Hameed, Dept of CSE  
Mrs. E. Pragnavi, Dept of CSE  
Mrs. V. Sukanya, Dept of CSE  
Mr. K. Srinivasa Reddy, Dept of CSE  
Ms. K. Pranitha Kumari, Dept of CSE  
Mr. I. Govardhana Rao, Dept of CSE  
Mr. M. Thirupathi, Dept of CSE  
Ms. A. Gayathri, Dept of CSE  
Mr. K. Satyanarayana, Dept of CSE  
Mrs. S. Radha Rani, Dept of CSE  
Mr. M. Narender Reddy, Dept of CSE  
Mrs. K. Jaya, Dept of CSE  
Mrs. C. Vani, Dept of CSE

## “Cryptograpy & Its Applications”

INAUGURAL FUNCTION		Chief Guest: Prof. SAMEEN FATIMA, Principal, UCE, OU	
DAYS\TIME	19 <sup>TH</sup> DEC 1100 TO 1115	1530 TO 1700	AK
CV	20 <sup>TH</sup> DEC (MONDAY)	1515 TO 1530	VN
CV	20 <sup>TH</sup> DEC (TUESDAY)	1345 TO 1515	KS
VS	21 <sup>ST</sup> DEC (WEDNESDAY)	1345 TO 1515	KS
SR	22 <sup>ND</sup> DEC (THURSDAY)	1245 TO 1345	VN
KV	23 <sup>RD</sup> DEC (FRIDAY)	1115 TO 1245	LK
TEA BREAK		TEA BREAK	
LUNCH BREAK		LUNCH BREAK	

FOR INAUGURATION ALL PARTICIPANTS ARE REQUESTED TO BE SEATED IN HALL BY 9.10 A.M.

# A FIVE DAY WORKSHOP (In Commemoration of Sir Srinivasa Ramanujan) ON **CRYPTOGRAPHY & ITS APPLICATIONS**

FACULTY DEVELOPMENT PROGRAMME  
(FDP)  
19-23, DECEMBER, 2016

Venue

Sir Srinivasa Ramanujan Computing Hall  
DEPT. OF CSE, UCE, OU



Department of Computer Science and Engineering  
UNIVERSITY COLLEGE OF ENGINEERING (A)  
OSMANIA UNIVERSITY, HYDERABAD  
TELANGANA STATE

For Details Contact:

Prof. **VENKAT DASS MAREDU**

CONVENOR

Department of Computer Science and Engineering,  
Osmania University, Hyderabad.  
Mobile No : +91 9440488428  
Email : vmaredu@gmail.com

## THEME

Mathematics is the subject of pioneer for all the disciplines in human history. Computer Science is no exception for this kind of argument; even learned doyens are of the opinion that mathematics is also mother and fathom for Computer Science & Engineering. This course is being organised in honour of great mathematician and son of soil Sir Srinivasa Ramanujan whose birth day falls on 22<sup>nd</sup> December (ie., 22-12-1887). Hence on this historical occasion it is a great pleasure to meet distinguished resource persons drawn from academia and industry as well as scholars from cryptography fraternity. Enough emphasis is given to mathematics to improve the skills of research in the field of Cryptography. This programme covers different ciphering techniques using traditional and public key cryptography. We have also included the applications of cryptography in communications and especially in the Banking sector.



**(SR) Prof.S.Ramachandram, Vice-chancellor**  
security in cloud



**(VN) Dr. V.N Sastry (IDRBT)**  
Advanced applications of " Cryptography " in Banking industry



**(KS) Dr.K.Srinathan (IIITH)**  
**Blockcipher abstractions: PRPs and PRFs:** Pseudo Random Permutations (PRP); Pseudo Random Functions (PRF); security against chosen plaintext attacks (CPA); nonce-based CBC encryption and nonce-based counter mode, **Message integrity: definition and applications:** CBC-MAC and PMAC, **Collision resistant hashing** : Merkle-Damgard and Davies-Meyer. MACs from collision resistance. Case studies: SHA and HMAC.



**(AK) Dr. Ashok Kumar Das (IIITH)**  
Research issues in wireless sensor networks ,



**(CV) Dr. V. Ch. Venkaiah (HCU)**  
**History and Overview of Cryptography, One Time Pad and Stream Ciphers:** Perfect secrecy and the one time pad, semantic security and stream ciphers, **Block Cipher:** Case studies: Feistel networks, DES, 3DES and AES, Basic modes of operation(CBC and counter mode).

## SPEAKERS



**(YS) Dr.YV.Subba Rao(HCU)**  
**Algebra :** Group, Rings, Field, **Cryptography using arithmetic modulo primes :** vanilla key exchange (Diffie-Hellman), the CDH and discrete-log assumptions, **Public key encryption :** semantically secure ElGamal encryption; CCA security.



**(SD) Prof. R Sridevi (JNTUH)**  
**Digital signatures: definitions and applications,**  
How to sign using RSA.



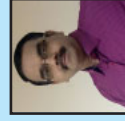
**(VS) Dr. V Srinivas (OU)**  
**Number Theory :** Fermat's and Euler's theorems, Testing for primality, Euclid's algorithms, prime and relatively prime numbers, modular arithmetic, the Chinese Remainder Theorems, Discrete logarithms,



**(KV) Dr.K.Veerabhadra Rao (OU)**  
**Attacks on block ciphers:** exhaustive search, time-space tradeoffs. Differential & linear cryptanalysis, meet in the middle, side channels



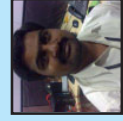
**(MV) Prof. Venkat Dass Maredu (OU)**  
Relations and Functions



**(LK) Prof. L.K. Suresh Kumar ( OU)**  
**Authenticated encryption: security against active attacks:** also: intro to session setup using a key distribution centre (KDC).



**(PV) Dr. PVS Anand (Dr. CR RAO)**  
Differential & linear cryptanalysis, meet in the middle, side channels.



**(KM) K Malliah Scientist - D (DRDO)**  
Security in cloud

## REGISTRATION FORM

A FIVE DAY WORKSHOP ON  
**(in commemoration of Sir Srinivasa Ramanujan)**  
**CRYPTOGRAPHY AND ITS APPLICATIONS**  
**19<sup>th</sup> - 23<sup>rd</sup> December 2016**

*Sponsored by:*  
**Technical Education Quality Improvement Programme**  
**(TEQIP Phase - II)**

Name : Prof/Dr/Mr/Mrs \_\_\_\_\_

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

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

Tel : \_\_\_\_\_ Fax : \_\_\_\_\_

Address for Communication : \_\_\_\_\_

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

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

Registration Fee : \_\_\_\_\_

D.D.No. \_\_\_\_\_ Dated : \_\_\_\_\_

Drawee Bank : \_\_\_\_\_

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

Place : \_\_\_\_\_

Please e-mail the registration form on or before 17th December 2016.

Signature

### REGISTRATION FEE DETAILS:

STUDENT	Rs. 2000/-
FACULTY	Rs. 3000/-
INDUSTRY	Rs. 5000/-

Last Date for Registration 17th December, 2016

Intake : 30 only, FCFS is followed