# SREE VIDYANIKETHAN ENGINEERING COLLEGE

(AUTONOMOUS)

Sree Sainath Nagar, Tirupati - 517102

## DEPARTMENT OF COMPUTER SCIENCE AND SYSTEMS ENGINEERING

### A Three Day Faculty Development Program on

### "Cryptography: Foundations and New Directions in Research"

The Department of Computer Science and Systems Engineering organized a Three Day Faculty Development Programme on**"Cryptography: Foundations and New Directions in Research",** during 16th-18th February, 2017 under TEQIP–II.

This FDP mainly focused on Advances in Cryptography, Public Key Cryptosystems, Block Chain Technology, Applications of Public Key Cryptosystems, Post Quantum Cryptography and Randomness. The members of faculty from different colleges across the nation attended the FDP.

*Dignitaries at the inauguration of the FDP*

**Shri. Girish Mishra** Scientist-D, SAG, DRDO, New Delhi; **Dr. Sahadeo Padhye**, Assistant Professor, MNNIT, Allahabad; **Dr. Vishal Saraswat**, Assistant Professor, **C.R.Rao**, AIMSCS, Hyderabad; **Dr. P.V.S Anand,** Associate Professor, **C.R.Rao,** AIMSCS, Hyderabad were the resource persons of the FDP.

**Shri. Girish Mishra,** Scientist-D from DRDO delivered the keynote address on "Cryptology: Security Everywhere" on 16th February 2017. In his lecture, he explained the various cryptosystems and basics of cryptography. In the next Session, **Dr. M Naresh Babu**, Associate Professor, Department of CSSE, Sree Vidyanikethan Engineering College enlightened the audience on Secret Sharing Schemes, Cryptanalysis of Reduced Round DES and Lightweight Crypto- systems. In his talk he demonstrated how a secret can be revealed through t-1 shares by using SMT solver. He explained various light weight cryptosystems- salsa, LEA - useful for constrained devices like RFID card, sensor networks etc.


***Shri. Girish Mishra,*** *DRDO delivering the keynote address*

*Audience during keynote Address*

Sahadeo Padhye, Assistant Professor, MNNIT, Allahabad, delivered a talk on Public Key Cryptosystem. In his lecture, the internals of Diffie-Hellman and RSA Cryptosystems were expounded upon.

During the second day, "Block Chain Technology (BITCOIN)" was explicated by Shri Girish Mishra. In his lecture, he explained the recent technologies in Cryptography which can succour virtual cash transactions. In the second session, Dr. Sahadeo Padhye delivered a talk on Public Key Cryptosystem, explaining the internals of ElGamal and Knapsack cryptosystems.

***Dr. Sahadeo Padhye,*** *delivering a talk on Public Key Cryptosystem*

***Dr. P.V.S Anand's*** *session on application for Cryptanalysis.*

Dr.Vishal Saraswat, Assistant Professor, C. R. Rao, AIMSCS, presented a talk on "Public Key Cryptosystems and its Application". The last session of the second day was handled by Dr. P.V.S Anand, Associate Professor, C. R. Rao, AIMSCS, Hyderabad, who elucidated the internals of SMT Solver and the usage of "SMT Solver as an Application for Cryptanalysis".

***Dr.Vishal Saraswat,*** *presentation on Public Key Cryptosystems and its Application*

*The participants listening ardently*

On the third day, Dr. Vishal Saraswat delivered a talk on "Post Quantum Cryptology". He illustrated the new theories to build the new cryptosytems to withstand the Quantum Computers. Later, Dr. Sahadeo Padhye delivered a talk on "Digital Signatures", demonstrating the different signature mechanisms. He also provided enlightenment on Security Analysis. The final session was by Dr. P.V.S Anand on "Randomness". He explained how random number generators are used in the Cryptology.

*The participants of the three day FDP on "Cryptography: Foundations and New Directions in Research"*

40 Faculty participated and gained knowledge on Cryptography: Foundations and New Directions in Research.

The Several outcomes are as follows:

- Gain knowledge on basic principles of applied cryptography, including classical cryptography, modern secret key and public key cryptography.
- Identify Research Problems in the area of Cryptography.
- Participants can acquire skills in Cryptanalytic attacks.
- Understanding security (attacks and defenses) in complex real life systems and the role of keys, cryptographic algorithms and protocols.
- Hands-on Experience-Attacks on existing Ciphers viz DES, SHA-1 etc..
- Learn basic techniques to protect data in computer and communication environments against several different varieties of fraud.