SREE VIDYANIKETHAN ENGINEERING COLLEGE
(AUTONOMOUS)
Sree Sainath Nagar, A. Rangampet – 517 102

Department of Computer Science and Systems Engineering
A Report on Three Day Faculty Development Programme
on
Cryptography: Foundations and New Directions in Research

The Department of Computer Science and Systems Engineering organized a 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.

Entrance banner at the venue *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 had explained the various cryptosystems and basics of cryptography. In the next

sessions **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 talks 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, Scientist, DRDO has delivering the keynote address.

The attentive audience of the session

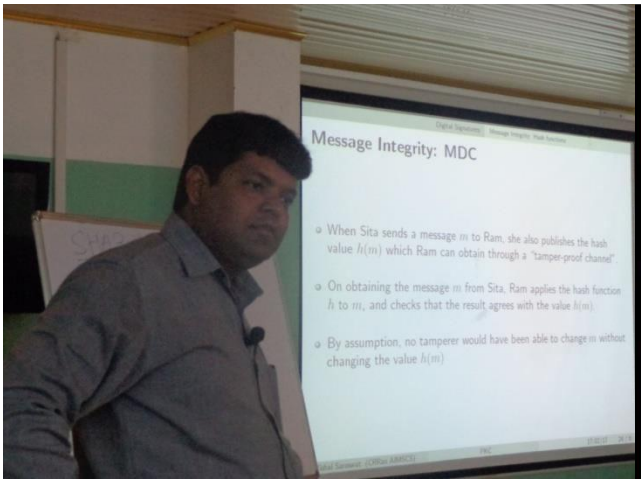
Dr. Sahadeo Padhye, Assistant Professor, MNNIT, Allahabad, delivered a talk on ***Public Key Cryptosystem***. In his lecture, the internals of Diffie-Hellman and RSA Cryptosystems were expounded upon.

In the first session on 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. In the next session **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"

The three day Faculty Development Programme came to successful end on 18th February, 2017. The participants appreciated the organizers for conducting the programme and they showed enthusiasm to attend many more programmes of such nature.