Report on
National Workshop on Cryptology and Cyber Security (WCCS-2018), Mar 22-24, 2018
Prof. K. Raja Rajeswari, Director (R&D) and Program Chair
Dr. M. Bhanu Sridhar, Dr. K. Srinivasa Rao, Coordinators

The Departments of CSE &ECE in GVP College of Engineering for Women, Visakhapatnam have realised the importance of research in the field of Cryptology and Cyber Security and decided to conduct **A Three day National Workshop on Cryptology and Cyber Security (WCCS-2018)'**. This would suffice the Engineers, Mathematicians, and Researchers to get together, discuss, deduce and recommend useful ideas in the presence of experts and resource persons for finding a solution to the task of strengthening Cyber Security for the benefit of public to protect from cybercrimes and threats.The workshop is intended to provide opportunity for faculty members and research scholars for upgrading their knowledge in the area cyber security and cryptography. The **Cryptology Research Society of India (CRSI)** had kindly consented to fund the workshop and so did **Institution of Electronics and Telecommunication Engineers (IETE**)(partial funding). This program is beneficial for those who are involved in teaching and/or pursuing research in Cryptography and Network Security, Statistics and Applied Mathematics. This workshop covered some of the topics like Basics of Cryptology including notion of security, Block chain Technology, Introduction to Elliptic Curve Cryptology, Proxy-re-encryption, Cryptography from Channel Noise, Authentication Issues, Recent Strides in IT Security, Cryptography from Channel Noise and so on. The Resource persons are Prof. Bimal K. Roy, Former Director, ISI, Kolkata and General Secretary, CRSI, Prof. R. Balasubramanian, Former Director, IMSc, Chennai and President, CRSI, Prof. Shri Kant, Former Director, DRDO, Prof. C. Pandurangan, IIT Madras, Prof. Ganapati Panda, IIT Bhubaneswar, Dr. Y.V. Subba Rao, UoH, Dr. KannanSrinathan, IIIT Hyderabad, Prof. P. S. Avadhani, AUCE (A), Prof. M. S. Prasad Babu, AUCE (A), Prof. J. Madanmohan Ram, GVPCE (A) and Mr. P. Nagesh Gautham, Citi Bank, USA.The report summarizes key points from each of the eleven sessions of the workshop, which focused on Cryptology and Cyber Security, the specific challenges, needs and opportunities relating to the industries and academia.**Session 1: Some Problems in Cryptology by Prof. Bimal K. Roy(22-3-2018)**

The first session focused primarily on Cryptology basics, its ideas, and different problem solving methodologies. The covering of the topics by the Professor was very satisfactory and the delegates were eager to proceed deeper into Cryptology methods which looked exciting.

Session 2: Introduction to Elliptic Curve Cryptology by Prof. R. Balasubramanian (22-3-2018)

The Professor made the participants more involved in the session. The mathematicians also participated with a lot of interest to understand the narrowing gap between Applied Mathematics and Data Preserving through the Elliptic Curve Technology which fascinated all.

Session 3: BlockChain Technology by Dr. Y. V. Subba Rao, UoH (23-3-2018) In this session the speaker concentrated on the hottest topic these days: BlockChain Technology. Starting with linking blocks, the lecturer went through different transactions, gave a sample script, Merkle Tree etc. Some real-time topics were also explained to make the audience more satisfied about what is the future of the automation methodologies.

Session 4: Cryptography from Channel Noise by Dr. KannanSrinathan, IIIT, HYD(23-3-2018)

The resource person, starting from what is 'Crypto', took the participants through a detailed idea of cryptography, its types, methodologies and applications in the IT industry. Different examples were also provided and a fine discussion followed that made all the people realise that cryptography that conceals the data is the best option to preserve the privacy and security of data in transmission.

Session 5: Recent Strides in IT Security - Issues, Challenges - Some Techniques & Solutions by Prof. M. S. Prasad Babu, Vice-Principal, AUCE (A) (23-3-2018)

The Professor gave a broad idea of the network security issues, challenges, data security and classical algorithms before going deep into the crypto systems, mobile crypto issues and other latest topics. The session was very needful and the audience were taken through some other security applications also like IoT, ITS etc.

Session 6: Authentication Issues by Prof. P. S. Avadhani, Principal, AUCE (A)(23-3-2018)

Prof. Avadhani concentrated more upon security of the information and to whom the data must be available. Symmetric key encryption, public key encryption and other issues were reviewed, before the authentication issues were taken up. The methods of identification of a person like cards, bio-metrics, OTP and so on were touched and the recent issues that are unearthing there were also discussed. Some possible solutions were also suggested.

Session7: Cyber Security and SEED Labs by Mr. P. N.Gautham, CITI Bank USA (23-3-2018)

Mr.Gautham started off in a different approach to the issue of cyber security – an IT industry type approach – since he is a part of it. The developing and spreading of viruses and worms and the counter attacks needed were laid out nicely by the speaker before mentioning about new points like DDoS and Shell Shock.

Session 8: An Information Officer's Rendezvous with Cyber Security by Prof. J. Madanmohan Ram, GVPCE (A)(23-3-2018)

Prof. Madanmohan Ram is also from the IT industry and the audience were able to understand the requirements of the IT industry through the topics he mentioned. Cyber-attacks, cyber-crime statistics, relationships among security concepts with apt diagrams fascinated the participants in such a way that would surely mould their angle of approach to the network security concept and thus their students' also. Also, OWASP was briefly mentioned by the speaker.

Session 9 & 11:Crypt-Analysis of Symmentric Key Ciphers: Classical to Modern by Prof. Shri Kant, Director (R &D), Sharda University, Noida (24-3-2018)

Professor Shri Kant went back into the theoretical way of dealing with the cryptographic concepts using symmetric key cyber model, cryptanalytic scenario, classical and modern cyber, key cybers and so on. His detailed sessions (two) also touched Kerckhoff's Principles, cryptanalytic attacks and mono-alphabetic substitution topics that have ample amount of research hidden in them.

Session 10: Signature Scheme Without Forking-Lemma by Prof. C. Pandurangan, IIT Madras(24-3-2018)

The speaker of the session lay light in another angle of cryptography. Starting off with provable security issues, the Professor also went into the topics of tight and loose security reduction, in a mathematical way, to make the audience more involved by producing proofs for every point that he talked about. The solving methodology used for unearthing forgery issues was excellent and in the end to know that all this matter was from a student of his was more fascinating.

Session 11: Cyber Security and Cryptography Fundamentals and Applications by Prof. Ganapati Panda, IIT Bhubaneshwar(24-3-2018)

Prof. Panda reminded the audience that basics are the bricks by which the building of Cryptology and Cyber security has come up. Starting from the definition of 'Cyber', he went deep into every point concerned about security of data, how to preserve the data through cryptography and how to store the same in clouds. It was an apt end to the workshop through which the delegates refreshed their minds and got ideas for more research that is to be carried out in the concerned field.

We are happy to inform that most of the participants attended for the workshop are women that fulfilled our main aim: Taking the technical aspects to women participants.