GUJARAT TECHNOLOGICAL UNIVERSITY

Report

of

Workshop on Cryptography

organized by

GTU PG Research Center of Cyber Security

on

13th February, 2016 at GTU PG School, BISAG

Coordinators:-Mr. Bhadreshsinh Gohil, bhadresh-wimc@gtu.edu.in
- Mr. Darshan Patel, ap_darshan@gtu.edu.in

With the visionary leadership of our Honorable Vice Chancellor, Dr. Akshai Aggrawal, PG research center of cyber security organized workshop in the core area of cyber security, Cryptography. Motivation behind conducting workshop is to broadcast knowledge and current research on cryptography and faculties, research scholars and students can further explore the field.

The workshop was initiated by Ms. Divya Sharma, Student of GTU PG SCHOOL by welcoming the guests and all participants and gave an introduction of the experts to all the participants. Shri Deval Mehta has completed B.E. (Electronics) from M.S. University, Baroda in 1989. He joined ISRO in 1989. He has done his Master Degree, M. Tech. (Satellite Communications) from United Nations CSSTE-AP (Centre for Space Science for Technology Education – Asia & Pacific) in 2002. He is the Head of Satellite Communication Technology Division in SAC, ISRO. He is Deputy Project Director for IRNSS (Indian Regional Navigation Satellite System) and responsible for design of encryption scheme for IRNSS. Another expert Ms. Bhanu Panjwani is responsible for design of encryption algorithm, their analysis and implementation for IRNSS.

First Session on fundamental was conducted by Mr. Deval Mehta, Head, Satellite Communication Technology Division, SAC, ISRO, and Ahmedabad. In the introduction he explained basic about cryptography, its objective, key terms such as cipher text, Plain text, encryption, confidentiality and integrity. After delivering introduction element at a very granular level, following technical topics were covered by him in detail:

- Public and Private Key Cryptosystem
- Fundamental Cryptographic Applications
- Popular Cipher Algorithms
- Data Encryption Standard
- SATCOM Application
- Comparison and Results
- SATNAV Application
- Preventing unauthorized interception of sensitive data
- Digital Signatures

In application part he briefed about functioning of IRNSS (Indian Regional Navigation Satellite System),IRNSS is an independent Navigation Satellite System providing services in the Indian Region and is being implemented by ISRO , in which he explained its design consideration, Encryption scheme used for IRNSS, the main elements of IRNSS ,its coverage and position accuracy. He said the special measures are required to ensure that RS signals are not spoofed intentionally or otherwise and to achieve this code encryption is proposed.

He also explained Popular Cipher Algorithms like:

- Shrinking Generator
- SNOW
- RSA
- El Gamel
- IDEA
- SHA
- Elliptic Curve Cryptography

Coordinators:-Mr. Bhadreshsinh Gohil, bhadresh-wimc@gtu.edu.in
- Mr. Darshan Patel, ap_darshan@gtu.edu.in

Second Session was conducted by Ms.Bhanu Panjwani. She covered AES (Advanced Encryption Standard) and ECC (Elliptical Curve Cryptography). Ms.Bhanu explained the history of an Advanced Encryption Standard (AES) and also gave the reason behind why AES is suitable for Space application that is its low memory requirement. Design part of AES includes: Sub Bytes, shift rows, mix column and add round key. Excluding sub Bytes, all three are linear operations. Very detailed mathematical explanation is given by her for:

- Cryptanalysis of AES
- Properties of AES S-Box(substitution box)
    - Strict Avalanche Criteria (SAC)
    - Differential uniformity
    - Linear probability
    - Algebraic degree
- Strict Avalanche Criteria
    - Two ways to test the SAC:
        -Analysis of the frequency of various hamming weight
        - Analysis of hamming weights according to the bit position
- Differential Uniformly
    - Differential cryptanalysis exploits the high probability of certain occurrences of plaintext differences and differences into the last round of the cipher.
- Linear approximation
    - Linear cryptanalysis tries to take advantage of high probability occurrences of linear expressions involving plaintext bits, "cipher text" and sub key bits.
- Interpolation Attacks

The Second concept covered by her was Elliptical Curve Cryptography (ECC) .She explained the need for ECC and said that, however, most of the public key cryptosystems rely on RSA for encryption and digital signature generation, but the computational load has already been increased because of larger key lengths. It was a need to find out the system which can be used in place of RSA with comparable security levels but with reduced key length and ECC was the right solution to this problem.

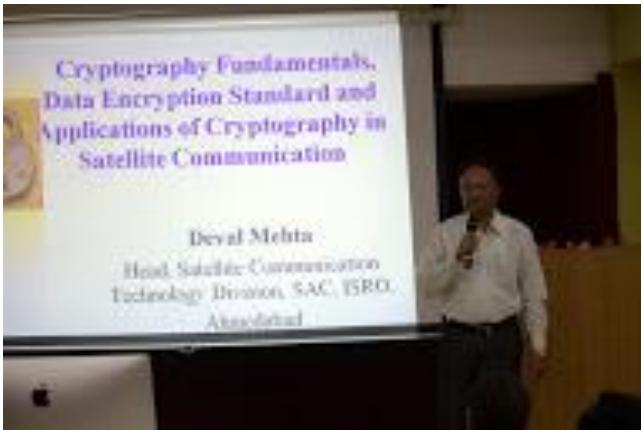
After explaining mathematics of ECC, she covered following topics of ECC:

- Elliptical Curve Discrete Logarithm Problem
- Projective Coordinate representation
- Double and Add Algorithm
- Delphi-Hellman Key exchange over EC

The entire session was very well delivered by Ms. Bhanu Panjawani. Seminar ended with the valuable support of participants and students of the GTU PG School.

Coordinators:-Mr. Bhadreshsinh Gohil, bhadresh-wimc@gtu.edu.in
- Mr. Darshan Patel, ap_darshan@gtu.edu.in

Workshop Photo Gallery



Expert seminar given by Mr. Deval Mehta

Expert seminar given by Ms. Bhanu Panjwani

Coordinators:-Mr. Bhadreshsinh Gohil, bhadresh-wimc@gtu.edu.in
- Mr. Darshan Patel, ap_darshan@gtu.edu.in