GUJARAT TECHNOLOGICAL UNIVERSITY

Report

Of

Workshop on Cryptography

Organized by

GTU PG Research Center of Cyber Security

On

6th February, 2015 at GTU PG School, BISAG

Coordinators:-Mr. Bhadreshsinh Gohil, bhadresh-wimc@gtu.edu.in
- Mr. Darshan Patel, ap_darshan@gtu.edu.in
- Ms.Kinjal Dave, kjdave-itsns@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 disseminate knowledge and current research on cryptography and faculties, research scholars and students can explore in this field.

With the guidance of our research advisor, Dr. P. K. Srivastava, experts from SAC-ISRO were invited who had huge experience in the area of cryptography in ISRO. The workshop was initiated by Kinjal Dave by welcoming the guests and all participants and given an introduction of the experts to all participants. Dr. Dhaval Mehta, Head of Satellite Communication Technology division (SSTD) and director of Indian Regional Navigation Satellite System (IRNSS) project and is 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.

Dr. P. K. Srivastava delivered a keynote address and explained the significance of encryption in transferring the data and information by sharing various experiences. He suggested that one research group should be formed among faculties, research scholars and students who have participated in the workshop so that research can be scaled in the field of cryptography.

First Session on fundamental was taken 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
- Popular Cipher Algorithms
- Data Encryption Standard
- SATCOM Application
- Comparison and Results
- SATNAV Application

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.

Second Session was taken by Ms.Bhanu Panjwani. She covered AES (Advanced Encryption Standard) and ECC (Elliptical Curve Cryptography). Ms.Bhanu has 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:

Coordinators:-Mr. Bhadreshsinh Gohil, bhadresh-wimc@gtu.edu.in
- Mr. Darshan Patel, ap_darshan@gtu.edu.in
- Ms.Kinjal Dave, kjdave-itsns@gtu.edu.in

- 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

A 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.

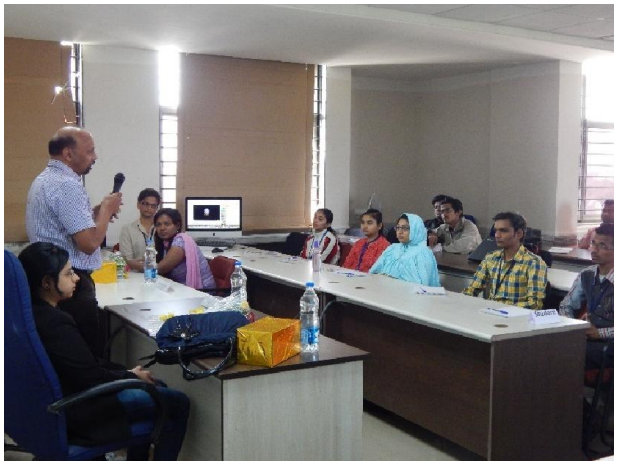
After explaining mathematics of ECC she covered following topics of ECC:

- 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. At the end of the day, Mr.Bhadreshsinh Gohil presented the vote of thanks to experts, participants and students of the GTU PG School of their valuable support.

Dr. P. K. Srivastava, research advisor, GTU is welcoming experts from SAC-ISRO

Coordinators:-Mr. Bhadreshsinh Gohil, bhadresh-wimc@gtu.edu.in
- Mr. Darshan Patel, ap_darshan@gtu.edu.in
- Ms.Kinjal Dave, kjdave-itsns@gtu.edu.in



Dr.P.K.Srivastava, research advisor, GTU is delivering keynote address

Mr.Deval Mehta is delivering session on fundamentals of cryptography

Ms. Bhanu Panjawani is delivering session on AES and ECC

Questions of participants were satisfactorily answered by the experts

Coordinators:-Mr. Bhadreshsinh Gohil, bhadresh-wimc@gtu.edu.in
- Mr. Darshan Patel, ap_darshan@gtu.edu.in
- Ms.Kinjal Dave, kjdave-itsns@gtu.edu.in