CRYPTOGRAPHY AND NETWORK SECURITY

PROF. SOURAV MUKHOPADHYAY

Department of Computer Science and Engineering

IIT Kharagpur

INDUSTRIES APPLICABLE TO : Stratign FZE, Dubai(UAE), SAG, DRDO, ISRO, WESEE, NTRO.

COURSE OUTLINE :

The aim of this course is to introduce the student to the areas of cryptography and cryptanalysis. This course develops a basic understanding of the algorithms used to protect users online and to understand some of the design choices behind these algorithms. Our aim is to develop a workable knowledge of the mathematics used in cryptology in this course. The course emphasizes to give a basic understanding of previous attacks on cryptosystems with the aim of preventing future attacks. A wide variety of basic cryptographic primitives will be discussed along with recent developments in some advanced topics like identity-based encryption, attribute-based encryption, functional encryption, two-party/multi-party computation, bitcoin and crypto-currency and postquantum cryptography. The cryptanalysis part will help us understanding challenges for cybersecurity that includes network security, data security, mobile security, cloud security and endpoint security.

ABOUT INSTRUCTOR :

Prof. Sourav Mukhopadhyay is an Associate Professor, Department of Mathematics at Indian Institute of Technology Kharagpur. He has completed his B.Sc (Honours in Mathematics) in1997 from University of Calcutta, India. He has done M.Stat (in statistics) and M.Tech (in computer science) from Indian Statistical Institute, India, in 1999 and 2001 respectively. He worked with Cryptology Research Group at Indian Statistical Institute as a PhD student and received his Ph.D. degree in Computer Science from there in 2007.

COURSE PLAN :

Week 1: Introduction to cryptography, Classical Cryptosystem, Block Cipher.

Week 2: Data Encryption Standard (DES), Triple DES, Modes of Operation, Stream Cipher.

Week 3: LFSR based Stream Cipher, Mathematical background, Abstract algebra, Number Theory.

Week 4: Modular Inverse, Extended Euclid Algorithm, Fermats Little Theorem, Euler Phi-Function, Eulers theorem.

Week 5: Advanced Encryption Standard (AES), Introduction to Public Key Cryptosystem, Diffie-Hellman Key Exchange

Week 6: Primarily Testing, ElGamal Cryptosystem, Elliptic Curve over the Reals, Elliptic curve Modulo a Prime.

Week 7: Generalized ElGamal Public Key Cryptosystem, Rabin Cryptosystem.

Week 8: Message Authentication, Digital Signature, Key Management, Key Exchange, Hash Function.

Week 9: Cryptographic Hash Function, Secure Hash Algorithm (SHA), Digital Signature Standard (DSS).

Week 10: Cryptanalysis, Time-Memory Trade-off Attack, Differential and Linear Cryptanalysis.

Week 11: Cryptanalysis on Stream Cipher, Modern Stream Ciphers, Shamirs secret sharing and BE, Identity-based Encryption (IBE)

Week 12: Side-channel attack, The Secure Sockets Layer (SSL), Pretty Good Privacy (PGP), Introduction to Quantum Cryptography