FOUNDATIONS OF CRYPTOGRAPHY

PROF. ASHISH CHOUDHURY
Department of Computer Science
IIIT Bangalore

PRE-REQUISITES : There are no pre-requisites for this course. However it is expected that the students who are interested to take this course have had some exposure to a basic course on discrete mathematics, algorithms, or theory of computation.Having said that, I ensure that a significant effort will be made from my side to simplify the overall presentation of the course and make it easily accessible.

INTENDED AUDIENCE : Computer Science and Mathematics students

INDUSTRIES APPLICABLE TO : The course will be relevant for any IT related company

COURSE OUTLINE :

The course provides the basic paradigm and principles of modern cryptography. The focus of this course will be on definitions and constructions of various cryptographic objects. We will try to understand what security properties are desirable in such objects, how to formally define these properties, and how to design objects that satisfy the definitions. The aim is that at the end of this course, the students are able to understand a significant portion of current cryptography research papers and standards.

ABOUT INSTRUCTOR :

Prof. Ashish Choudhury is currently an Assistant Professor at IIIT Bangalore. He did his MS and PhD in Computer science from IIT Madras, followed by postdoc at ISI Kolkata and University of Bristol. His research work is focused on the foundation of cryptographic protocols for real-world problems. His current projects aim to design efficient protocols in the asynchronous network model which can be realized in practice. In general he is interested in secure distributed computing and all areas of theoretical computer science.

COURSE PLAN :

Week 1: Course Overview, Symmetric-key Encryption, Historical Ciphers, Perfect Security and Its Limitations

Week 2: Computational Security, Semantic Security and Pseudorandom Generators (PRGs)

Week 3: Stream Ciphers, Provably-secure Instantiation of PRG, Practical Instantiation of PRG, CPA-security and Pseudo-random Functions (PRFs)

Week 4: CPA-Secure Ciphers from PRF, Modes of Operations of Block Ciphers, Theoretical Constructions of Block Ciphers and Practical Constructions of Block Ciphers

Week 5: DES, AES and Message Authentication Codes (MAC)

Week 6: Information-theoretic Secure MAC, Cryptographic Hash Functions, Ideal-Cipher Model, Davies-Meyer construction and Merkle-Damgård Paradigm

Week 7: Birthday Attacks on Cryptographic Hash Functions, Applications of Hash Functions, Random Oracle Model and Authenticated Encryption

Week 8: Generic Constructions of Authenticated Encryption Schemes, Key-exchange Problem, One-way Trapdoor Functions and Cyclic Groups

Week 9: Discrete-Logarithm Problem, Computational Diffie-Hellman Problem, Decisional Diffie-Hellman Problem, Elliptic-Curve Based Cryptography and Public-Key Encryption

Week 10: El Gamal Encryption Scheme, RSA Assumption, RSA Public-key Cryptosystem, KEM-DEM Paradigm and CCA-security in the Public-key Domain

Week 11: CCA-secure Public-key Hybrid Ciphers Based on Diffie-Hellman Problems and RSA-assumption, Digital Signatures, RSA Signatures and Schnorr Identification Scheme

Week 12: Schnorr Signature, Overview of TLS/SSL, Number Theory, Interactive Protocols and Farewell