Cryptography and Network Security

About the course

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.

Course layout

Week 1: Introduction to cryptography, Classical Cryptosystem, Cryptanalysis on Substitution Cipher (Frequency Analysis), Play fair Cipher, Block Cipher.
Week 2: Data Encryption Standard (DES), DES (Contd.), Triple DES, Modes of Operation, Stream Cipher, Pseudorandom Sequence.
Week 3: LFSR based Stream Cipher, Mathematical background, Abstract algebra, Number Theory.
Week 4:Modular Inverse, Extended Euclid Algorithm, Fermat's Little Theorem, Eular Phi-Function, Eular's theorem, Quadratic Residue, Polynomial Arithmetic.
Week 5: Advanced Encryption Standard (AES), Introduction to Public Key Cryptosystem, Diffie-Hellman Key Exchange, Knapsack Cryptosystem, RSA Cryptosystem.
Week 6: More on RSA, Primarily Testing, ElGamal Cryptosystem, Elliptic Curve over the Reals, Elliptic curve Modulo a Prime.
Week 7: Generalised ElGamal Public Key Cryptosystem, Chinese Remainder Theorem, Rabin Cryptosystem, Legendre and Jacobi Symbol.
Week 8: Message Authentication, Digital Signature, Key Management, Key Exchange, Hash Function.
Week 9: Universal Hashing, Cryptographic Hash Function, Secure Hash Algorithm (SHA), Digital Signature Standard (DSS), More on Key Exchange Protocol.
Week 10: Cryptanalysis, Time-Memory Trade-off Attack, Differential Cryptanalysis, More on Differential Cryptanalysis, Linear Cryptanalysis.
Week 11: Cryptanalysis on Stream Cipher, Algebraic Attack, Implementation Attacks, side channel attack.
Week 12: Internetwork Security, SSL, PGP, Cloud Security, Introduction to Blockchain and Bitcoin.