Course content for MT5462, Advanced Cipher Systems

Prerequisites:
UG courses in linear algebra and probability

Aims:
To introduce and study the mathematical and security properties of both symmetric key cipher systems and public key cryptography, covering methods for obtaining confidentiality and authentication.

Learning outcomes:
On completion of the course the student should be able to:
Understand the concepts of secure communications and cipher systems;
Understand and use statistical information and the concept of entropy in the cryptanalysis of cipher systems;
Understand the main properties of Boolean functions, and their applications and use in cryptographic algorithms;
Understand the structure of stream ciphers and block ciphers;
Know how to construct as well as have an appreciation of desirable properties of keystream generators, and understand and manipulate the concept of perfect secrecy;
Understand the main mathematical and statistical properties of Feedback Shift Registers, and of FSR-based stream ciphers;
Understand the modes of operation of block ciphers and their properties;
Understand the main design principles and cryptographic techniques of modern symmetric cryptography algorithms;
Understand the concept of public key cryptography, including the details of the RSA and ElGamal cryptosystems, both in the description of the schemes and in their cryptanalysis;
Understand the concepts of authentication, identification and signature, be familiar with techniques that provide these, including one-way functions, hash functions and interactive protocols and the Fiat-Shamir scheme;
Understand the problems of key management, and be aware of key distribution techniques.

Course content:
Cipher systems: An introductory overview of the aims and types of ciphers. Methods and types of attack. Information theory. Boolean functions. Statistical tests.
Stream ciphers: The one-time pad. Pseudo-random key streams – properties and generation. Mathematical and statistical properties of feedback shift registers. Berlekamp-Massey algorithm. Design principles and cryptanalytic techniques of modern stream ciphers.
Block ciphers: Confusion and diffusion. Iterated block ciphers – substitution/ permutation. SP-networks. The Feistel principle. DES, AES. Modes of operation. Linear and differentiable cryptanalysis, and related cryptographic techniques.
Public key ciphers: Discussion of key management. Diffie-Hellman key exchange. One-way functions and trapdoors. RSA, ElGamal cryptosystem.
Authentication/identification: Protocols. Challenge/response. MACs. Zero-knowledge protocols; Fiat-Shamir protocol.

Digital signatures: Digital signature methods. Hash functions – design and analysis techniques. DSS. Digital certificates.