Course content for MT3620/MT4620, Cipher Systems

Prerequisites:
MT1820 and some probability

Aims:
To introduce both symmetric key cipher systems and public key cryptography covering methods of obtaining the two objectives of privacy 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 structure of stream ciphers and block ciphers;
- know how to construct as well as have an appreciation of desirable properties of key stream generators, understand and manipulate the concept of perfect secrecy;
- understand the modes of operation of block ciphers and their properties;
- understand the concept of public key cryptography, including 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, including the Fiat-Shamir scheme;
- understand the problems of key management, be aware of key distribution techniques.
- MT4620: Demonstrate a breadth of understanding appropriate for an M-level course.

Course content:
Cipher systems: An introductory overview of the aims and types of ciphers. Methods and types of attack. Information theory. Statistical tests.
Stream ciphers: The one time pad. Pseudo-random key streams - properties and generation.
Block ciphers: Confusion and diffusion. Iterated ciphers - substitution/ permutation. The Feistal principle, DES, AES, Modes of operation.
Public key ciphers: Discussion of key management. Diffie-Hellman key exchange. One-way functions and trap-doors. RSA; ElGamal cryptosystem.
Authentication/Identification: Protocols. Challenge/response. MACs. Zero-knowledge protocols; Fiat-Shamir protocol.
Digital signatures: Digital signature methods. Hash functions. DSS. Certificates.