Course content for MT5466, Public Key Cryptography

Prerequisites:
MT5462

Aims:
To introduce some of the mathematical ideas essential for an understanding of public key cryptography, such as discrete logarithms, lattices and elliptic curves;
To introduce several important public key cryptosystems, such as RSA, Rabin, ElGamal Encryption, Schnorr signatures;
To discuss modern notions of security and attack models for public key cryptosystems.

Learning outcomes:
- be familiar with the RSA and Rabin cryptosystems, the hard problems on which their security relies and certain attacks on them;
- have a basic knowledge of finite fields and elliptic curves over finite fields, and the discrete logarithm problem in these groups;
- be familiar with cryptosystems based on discrete logarithms, and some algorithms for solving the discrete logarithm problem;
- know the definition of a lattice and be familiar with the LLL algorithm and some applications of lattices in cryptography and cryptanalysis;
- be able to define security notions and attack models relevant for modern theoretical cryptography, such as indistinguishability and adaptive chosen ciphertext attack;
- be able to critically analyse cryptosystems;

Course content:
Background: Integers modulon; Chinese remainder theorem; finite fields; fast exponentiation; public key cryptography and security; complexity theory.
RSA/Rabin: Key generation; implementation; encryption and signatures; OAEP; the RSA problem and relationship with factoring; square roots modulo a prime; Hastad attack; Wiener attack.
Discrete logarithms: Diffie-Hellman; ElGamal encryption; Schnorr signatures; Diffie-Hellman problem and decision Diffie-Hellman; methods to solve discrete logarithms such as baby-step-giant-step, Pollard rho and lambda, index calculus.
Lattices: Definition of a lattice; GGH cryptosystem; LLL algorithm; lattice attacks on knapsack cryptosystems and variants of RSA.
Elliptic curves: Group law; Hasse bound; group structure; point counting; ECC protocols; Maurer equivalence of DH and DL.