MTH6115 CRYPTOGRAPHY
KEY OBJECTIVES

To obtain a pass in the examination, you should be able to answer questions on any of the following.

1. Basic ideas: cryptography and steganography; plaintext, ciphertext, key.
2. Substitution and other traditional ciphers.
3. Stream ciphers including Vigenère cipher, one-time pad, shift registers.
4. Statistical attack on ciphers; Shannon's theorem.
5. Public-key cryptography: basic principles including complexity issues; knapsack, RSA and El-Gamal ciphers.
6. Digital signatures and authentication; secret sharing.

The examination will range over all material covered during the lectures.