

MTH6115

Cryptography

Learning Outcomes

Winter/Spring 2010

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 the material covered in lectures.

The parts of the rubric on (and information about) the examination paper you will need to know will be as follows:

You may attempt as many questions as you wish and all questions carry equal marks. Except for the award of a bare pass, only the best FOUR questions answered will be counted. There are SIX questions on this paper.

Calculators are NOT permitted in this examination. The unauthorised use of a calculator constitutes an examination offence.