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

(a) Basic ideas: cryptography and steganography; plaintext, ciphertext, key.

(b) Substitution and other traditional ciphers.

(c) Stream ciphers including Vigenère cipher, one-time pad, shift registers.

(d) Statistical attack on ciphers; Shannon’s theorem.

(e) Public-key cryptography: basic principles including complexity issues; knapsack, RSA and El-Gamal ciphers.

(f) Digital signatures and authentication; secret sharing.

The rubric on the examination paper 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 5 questions answered will be counted.

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