A. GENERAL INFORMATION
   A1. Supervisor(s): Dr. Aqil Azmi
   A2. Project Title: Elliptic Curve Cryptography (ECC)
   A3. Number of Students: 2

B. PROJECT ABSTRACT
RSA is widely used for encryption in products and standards that use the public-key cryptography. To retain a reasonable security level, the bit length for secure RSA has increased over recent years resulting in a heavy processing load on applications using RSA. This is not good news for many e-commerce sites. Recently a competing system began to challenge RSA: elliptic curve cryptography (ECC). The main attraction of ECC is that it is able to offer comparable security with a far smaller bit size and this translates to a reduced processing overhead.

C. REQUIREMENTS (both hardware and software)
   (i) IBM PC or compatible

D. PROJECT PHASES
   Phase I: Going through the mathematical background for ECC.
   Phase II: Implementation.

E. SCHEDULING OF PHASES
   Semester 1: Phase I
   Semester 2: Phase II