

Marking Guide for RSA and ECC implementation

1. RSA:

- a. To get a C students have to implement RSA digital signature, Miller-Rabin test, and follow all the other requirements such as pseudo code, design of the program and discuss the limitations of the implementation.
- b. To get a D student have to complete a. and write their random generator function, functions to compute e and d using gcd and Euclid's algorithm.
- c. To get a HD, students have to complete a. and b. and to discuss all the limitations of their program, especially the probability that p and q are prime numbers; what if they are not prime numbers; what security issues resulted from those limitations.

2. ECC: (for ECC students are not required to implement digital signature to get a HD – bonus mark is given if you can implement it).

- a. To get a C students have to implement ECC with embedding message algorithm, and follow all the other requirements such as pseudo code, design of the program and discuss the limitations of the implementation.
- b. To get a D student have to complete a. and implement efficient operations of points on the curve.
- c. To get a HD, students have to complete a. and b. and to discuss all the limitations of their program and what security issues resulted from those limitations