**Chengdu University of Technology Oxford Brookes College**

**Project Module (CHC 6096)**

**Weekly Report Sheet**

|  |  |
| --- | --- |
| STUDENT NAME: | Tony |
| STUDENT NUMBER: | 201918020429 |
| SUPERVISOR NAME: | Jakir Hossain |
| DATE: | 2022.4.1 |
| Briefly list all the main tasks you accomplished in the week.   1. Java language to achieve my improved ECC encryption algorithm programming. 2. ECC encryption algorithm of binary dot multiplication and ECC encryption algorithm of NAF dot multiplication are implemented by Java. 3. The results of the three algorithms under different keys are tested by programs. | |
| Briefly state all the challenges you encountered in the week.   1. It was very difficult to instantiate my own ECC improvement algorithm this week. Although I have clarified the logic, it is still a lot of trial and error to write and call the intermediate point multiplication. | |
| Briefly Plan out the agenda for next week.   1. I investigate the key relationship between RSA encryption algorithm and ECC encryption algorithm.   2. According to the corresponding relationship to design a comparative test, test under the same security of my own improved algorithm and RSA encryption algorithm compared with the computing power and encryption and decryption time. | |
| SUPERVISOR SIGNATURE: |  |