**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: | 2022.4.8 |
| Briefly list all the main tasks you accomplished in the week.   1. The relationship of key length between ECC and RSA is investigated. 2. The code that can command the two algorithms to switch the length of the generated key is written in JAVA, and the computing power of the two algorithms is compared under the key length of 160(ECC)-1024(RSA),192(ECC)-1536(RSA), and then the encryption and decryption time of the two algorithms is tested under the same security. It is concluded that my improved ECC encryption algorithm has better computing power and encryption and decryption efficiency than RSA in the resource-constrained environment. | |
| Briefly state all the challenges you encountered in the week.   1. It took a lot of time to select the curves suggested by NIST and the Federal Information Processing Standard (FIPS) because finding the correspondence required searching them. | |
| Briefly Plan out the agenda for next week.   1. According to the comparison data of the tested algorithms, tables and graphs are drawn to show readers intuitively. 2. The mobile electronic payment model based on improved ECC encryption algorithm designed by myself is compared with other similar models. | |
| SUPERVISOR SIGNATURE: |  |