**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: | 2022.3.18 |
| Briefly list all the main tasks you accomplished in the week.   1. ECC encryption algorithm is implemented in Java. 2. I read more papers about ECC encryption algorithm, and found some papers about the underlying operation design of ECC encryption algorithm, and found some clues to improve ECC encryption algorithm. | |
| Briefly state all the challenges you encountered in the week.   1. Papers related to the underlying logic of ECC encryption algorithm are very difficult to understand. There are many reciprocal operations and inverse operations involved in mathematical knowledge, and some even involve new mathematical design concepts. I feel that I need more time to understand them and then create my own improved ECC encryption algorithm based on them. | |
| Briefly Plan out the agenda for next week.  1. Understand several papers on the mathematical logic underlying elliptic curve cryptography.  2. This paper proposes an improved ECC encryption algorithm and expresses it by mathematical formula. | |
| SUPERVISOR SIGNATURE: |  |