**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: | 2022.3.10 |
| Briefly list all the main tasks you accomplished in the week.   1. RSA encryption algorithm is implemented in Java, which can encrypt plaintext and generate 1024 bit key to encrypt it. 2. A new model for mobile payment is designed, which has stronger security than the electronic payment model of the previous target article. The stronger is that customers and merchants are not directly connected and then transfer information to each other, but are connected through the payment gateway, and the message passing through the payment gateway will have better security. | |
| Briefly state all the challenges you encountered in the week.   1. I has not found a good ECC encryption algorithm can be well applied to the mobile payment system, because the mobile payment equipment such as mobile phone storage space, computing power are relatively low, so can not directly use the classical ECC encryption algorithm to achieve the encryption of plaintext. | |
| Briefly Plan out the agenda for next week.  1. Read more articles about ECC encryption algorithm improvement to find an ECC encryption algorithm suitable for mobile payment system  2. The classical ECC encryption algorithm is implemented in JAVA. | |
| SUPERVISOR SIGNATURE: |  |