**DANH SÁCH BÀI THỰC HÀNH MMUD 2022**

|  |  |  |
| --- | --- | --- |
| **Tên bài** | **Yêu cầu** | **Ghi chú** |
| Bài 1. Cài đặt hệ mật AES với các chế độ hoạt động theo chuẩn | - Cài đặt được thuật toán mã hóa AES  - Kết hợp các chế độ hoạt động CBC, ECB, CFB, OFB, CTR để mã hóa file |  |
| Bài 2. Cài đặt hệ mật RSA với các chế độ hoạt động theo chuẩn PKCS | Cài đặt hệ mật RSA tuân theo chuẩn PKCS#1 OAEP (RSA) |  |
| Bài 3. Cài đặt hệ mật mã ECC | Cài đặt triển khai hệ mật mã trên đường cong Elipptic ECC |  |