|  |  |  |  |
| --- | --- | --- | --- |
| STT | Bài | Input | Khóa |
|  | 1. ceasar | ALLWORKANDNOPLAYMA | 4 |
|  | 2. Vigenere\_lặp khóa | ALLWORKANDNOPLAYMA | WHENINRO |
|  | 3. Vigenere\_autokey | ALLWORKANDNOPLAYMA | SAVEFORA |
|  | 4. Mã chữ đơn | ALLWORKANDNOPLAYMA | LGRJOCFIKAHQYTEMNBWUVSDPXZ |
|  | 5. PlayFair | ALLWORKANDNOPLAYMA | NOROSEWI |
|  | 6. RailFence | ALLWORKANDNOPLAYMA | 4 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lũy thừa Modulo** | a | m | n |
|  | 479 | 871 | 6353 |
|  |  |  |  |
| Nghịch đảo | a | n | x |
|  | 823 | 3767 | 1483 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Hệ phương trình | Input |  |  |  |
|  | m1 = | 17 | a1 = | 13 |
|  | m2 = | 37 | a2 = | 10 |
|  | m3 = | 71 | a3 = | 30 |

|  |  |  |
| --- | --- | --- |
| Căn nguyên thủy |  |  |
|  | a | n |
|  | 15 | 397 |
|  | 11 | 331 |
|  | 5 | 463 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Logarit | a | b | n | k = logab(mod n) |
|  | 3 | 6 | 19 |  |
|  | 5 | 7 | 17 |  |
|  | 3 | 5 | 19 |  |
|  | 2 | 7 | 11 |  |

|  |  |  |
| --- | --- | --- |
| DES |  |  |
|  | M = | 40A78883D0E1D258 |
|  | K = | 089166C3FDDE9022 |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| AES |  |  |
| M | 79BD0FBD44684F2B5517876B99E20D62 |  |
| K | C977D97DB8DAA950B7E562675B163896 |  |
| C | C5EF962A4357DDC3CFBAD38DBE47B23F |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Differ - Helman | | | | | |
| Đề | 20 |  |  |  |  |
| q = | 6389 | phi(q) = |  |  |  |
| a = | 7 |  |  |  |  |
| xa = | 442 | ya = |  | kab = |  |
| xb = | 342 | yb = |  | kba = |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2. RSA.BT1 | | | | |
| đề | 1 |  |  |  |
| p = | 47 | n = |  |  |
| q = | 71 | f(n) = |  |  |
| e = | 61 | d = |  |  |
| M = | 59 | C1 = |  | An mã hóa gửi cho Ba, sử dụng khóa riêng |
|  |  | C2 = |  | Ba mã hóa gửi cho An, sử dụng khóa công khai |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. ElGamal |  |  |  |  |  |  |  |  |  |  |  |  |
| Đề | a | q | xA\_PR | M | k | yA | PUK | K | C1 | C2 | Bản mã | K^1 |
| 10 | 3 | 7433 | 341 | 403 | 872 |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. chukysoDSA | | | | | | | | | | | | | | | | | | | | | | |
| Đề | p | q | h | xA | k | H(M) | (p-1)/q | g | yA | g^k mod p | r | k^(-1) mod q | s | (r, s) | w | u1 | u2 | g^u1 mod p | y^u2 mod p | v | v = r' |
| 10 | 47 | 23 | 34 | 2 | 10 | 9 | 2 | 28 |  |  |  |  |  |  |  |  |  |  |  |  |  |