A white paper with black text

Description automatically generated

Câu 1:

|  |  |
| --- | --- |
| Đối Xứng | Bất Đối Xứng |
| Độ An Toàn K Cao | Ngược Lại |
| Thuật Toán DES,Triple DES,AES | RSA |
| Một Khoá | Nhiều Khoá |
| Mã hoá, Giải Mã Đơn Giản | Phức Tạp |
| Hiệu suất nhanh,yêu cầu ít sức mạnh | Ngược Lại |
| Khoá ngắn hơn | Khoá Dài hơn |
| Độ phức tạp quản lý khoá cao | Độ phức tạp qlk thấp |
| Mã hoá nhiều dữ liệu | Mã hoá 1 lượng nhỏ dữ liệu |

Câu 2: RSA

P = 17, Q = 23 , E = 29

a.

N = p \* q = 17 \* 23 = 391

P(N) = (p-1)(q-1) = 16 \* 22 = 352

D = Mod 352

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| a | b | r | q | Y0 | Y1 | y |
| 352 | 29 | 4 | 12 | 0 | 1 | -12 |
| 29 | 4 | 1 | 7 | 1 | -12 | 85 |
| 4 | 1 | 0 |  |  |  |  |
|  |  |  |  |  |  |  |

* D = 85

Kp = (E,N) = (29,391)

Ks = (d,p,q) = (85,17,23)

b.

C = Mod N = Mod 391 = 166