A white paper with black text

Description automatically generated

Câu 1

A diagram of a key system

Description automatically generated

Câu 2:

N = p \* q = 31 \* 47 = 1457

P(N) = (p-1)(q-1) = 30 \* 46 = 1380

D = Mod P(N) = Mod 1380 = 893

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| A | B | R | Q | Y0 | Y1 | y |
| 1380 | 17 | 3 | 81 | 0 | 1 | -81 |
| 17 | 3 | 2 | 5 | 1 | -81 | 406 |
| 3 | 2 | 1 | 1 | -81 | 406 | -487 |
| 2 | 1 | 0 |  |  |  |  |

Kp = (N,e) = (1457,17)

Ks = (d,p,q) = (893,31,47)

b)

C = Mod N = Mod 1457 = 1160

Công thức giải mã:

M = Mod N

ĐỀ KHÔNG YÊU CẦU LÀM PHẦN NÀY, ĐÂY LÀ BONUS:

= Mod 1457 = 55