A white background with black text

Description automatically generated

Câu 1:

* Chức năng : là một tập hợp các phần cứng , phần mềm , nhân lực , chính sách và các thủ tục để tạo , quản lý , phân phối, sử dụng , lưu trữ và thu hồi các chứng chỉ số
* Thành phần:

+CA: cơ quan cấp và kiểm tra chứng chỉ số

+RA: bộ phận kiểm tra thông tin nhận dạng của nd theo yêu cầu của CA

+VA: cơ quan xác nhận thông tin nhận dạng của nd thay mặt CA

+CD: Nơi lưu danh mục và lập chỉ số các khóa

+ Hệ thống quan lý chứng chỉ

+Chính sách về chứng chỉ

Câu 2:

a)

N = p \* q = 31 \* 43 = 1333

P(N) = (p-1)(q-1) = 30 \* 42 = 1260

d = Mod P(N) = Mod 1260

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| A | B | R | Q | Y0 | Y1 | Y |
| 1260 | 19 | 6 | 66 | 0 | 1 | -66 |
| 19 | 6 | 1 | 3 | 1 | -66 | 199 |
| 6 | 1 | 0 |  |  |  |  |

d = 199

Kp = (N,e) = (1333,19)

Ks = (d,p,q) = (199,31,43)

b)

C = mod N = Mod 1333 = 1009

CTGM:

M = mod N

BONUS GIẢI MÃ

= Mod 1333 = 55