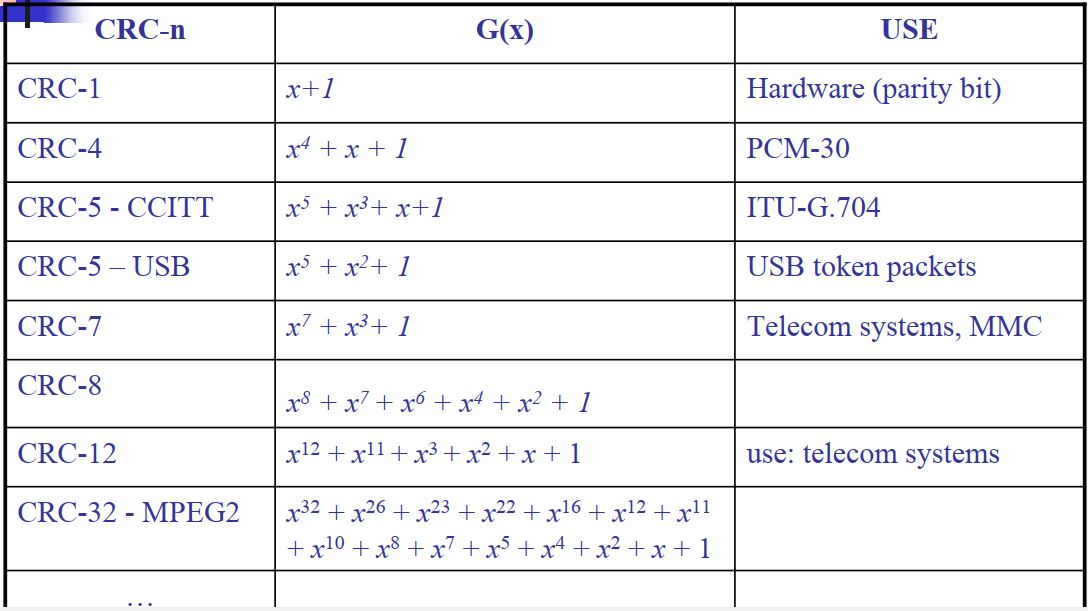
**Dạng bài tập chứng thực điện tử - AT16D**

# **Dạng 1: Kiểm tra dư thừa vòng – CRC (Cyclic Redundancy Check) của một chuỗi số nhị phân**

Cách xác định CRC-n: Các bước thực hiện

* + - Biểu diễn chuỗi bit thành đa thức nhị phân
    - Nhân với thu được
    - Chia cho đa thức sinh của CRC-n
    - Thu được và phần dư sao cho:

* Phần dư là CRC-n
* Đa thức sinh G(x) sẽ là như sau:



Ví dụ: Tìm CRC-1 của chuỗi số nhị phân sau: 1101 0010 1010 1010

* CRC-1 => n=1
* Đa thức sinh G(x) = x+1
* Biểu diễn chuỗi số thành đa thức nhị phân
* Thực hiện phép chia nhị phân 𝑀(𝑥). cho 𝐺(𝑥) thu được:
* 𝑄(𝑥) =
* 𝑅(𝑥)= 0
* CRC-1 = 0

**Bài tập vận dụng:**

1. Tìm CRC-7 của 1101 0010 1010 1010
2. Tìm CRC-7 của 1011 0010 0110 1110

# **Dạng 2: Xây dựng đường dẫn chứng thực dựa trên mô hình kiến trúc PKI**

Kiến thức:

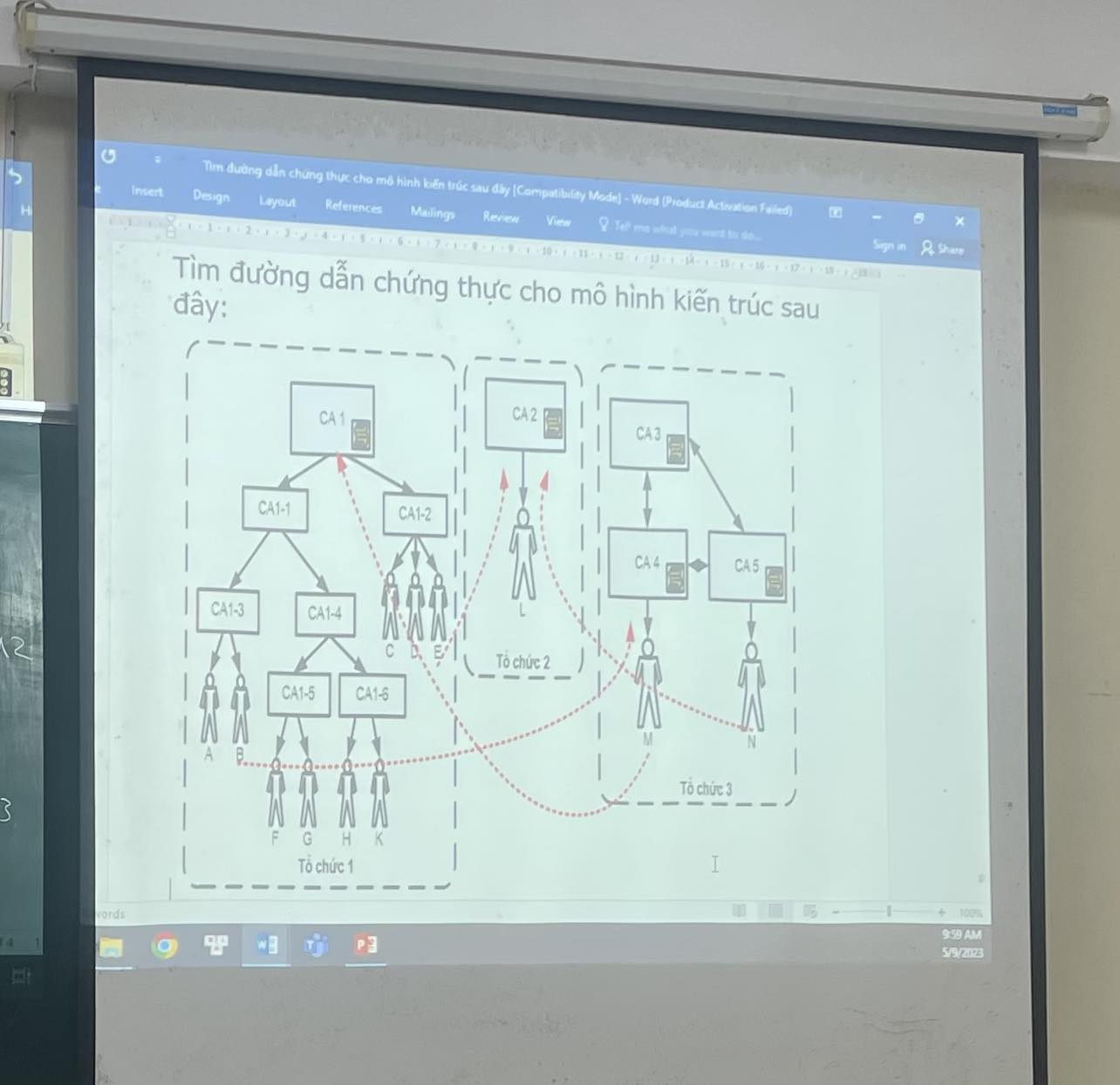
Mũi tên nét liền: CA cấp phép chứng thực số cho người dùng

Mũi tên nét đứt: Người dùng tin cậy CA

Mũi tên hai chiều: ngang hàng với nhau

Ví dụ: Xây dựng đường dẫn chứng thực từ:

1. M đến A, L
2. N đến B, E, D, L, M



1. DSach CA tin cậy của M là: CA4, CA3, CA5, CA1 (người dùng tin cậy, xin cấp phép từ CA1)

Danh sách CA tin cậy của A: CA1

Danh sách CA tin cậy của L: CA2

Từ M đến A: [CA1 🡪 CA(1-1)] : [CA(1-1) 🡪 CA(1-3)] : [CA(1-3) 🡪 A]

Từ M đến L: không có đường dẫn

1. Danh sách CA tin cậy của N: CA3, CA4, CA5, CA2

Của B: CA1, CA4, CA5, CA3

Của E: CA1, CA2

Của D: CA1

Của L: CA2

Của M câu a)

Từ N đến B: [CA5 🡪 CA3] : [CA3 🡪 CA4] : [CA4 🡪 B]

Hoặc: [CA5 🡪 CA4] : [CA4 🡪 B]

Từ N đến E: [CA2 🡪 E]

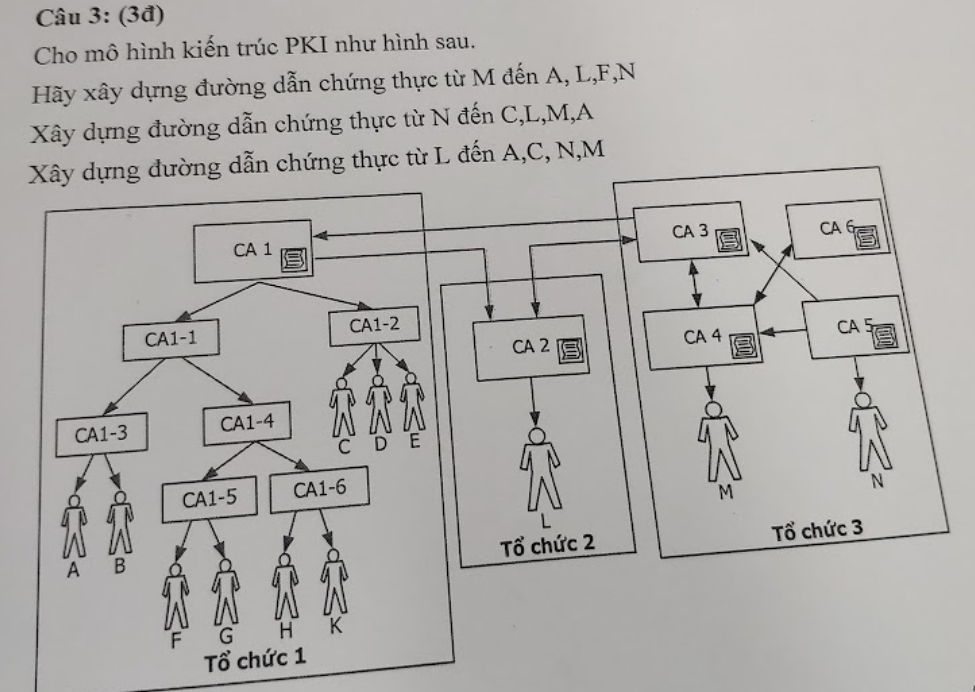
Từ N đến D: không có đường dẫn

Từ N đến L: [CA2 🡪 L]

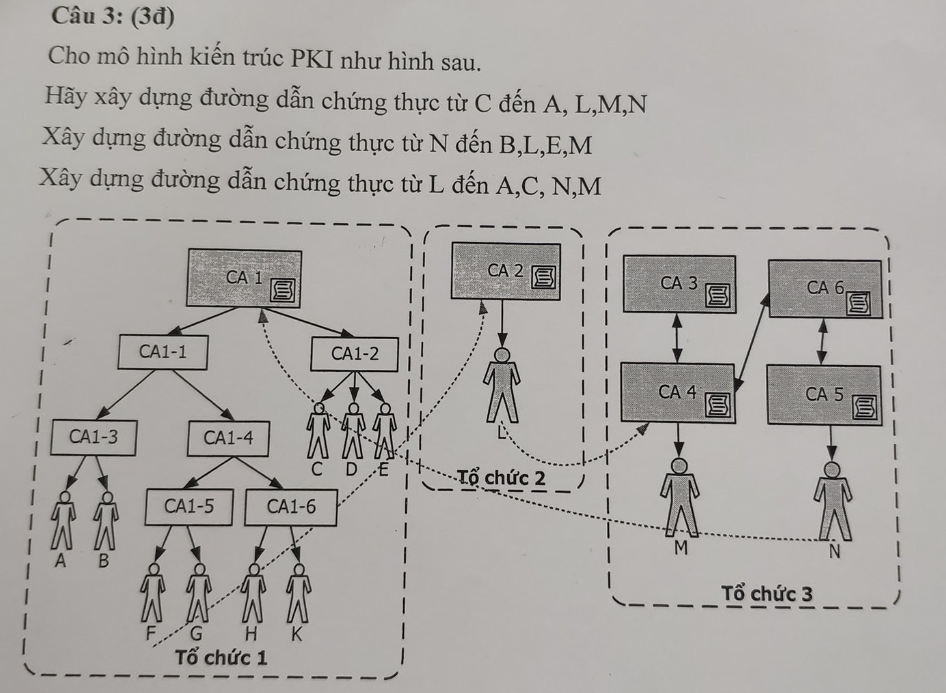
Từ N đến M: tương tự từ N đến B

**Bài tập vận dụng:**

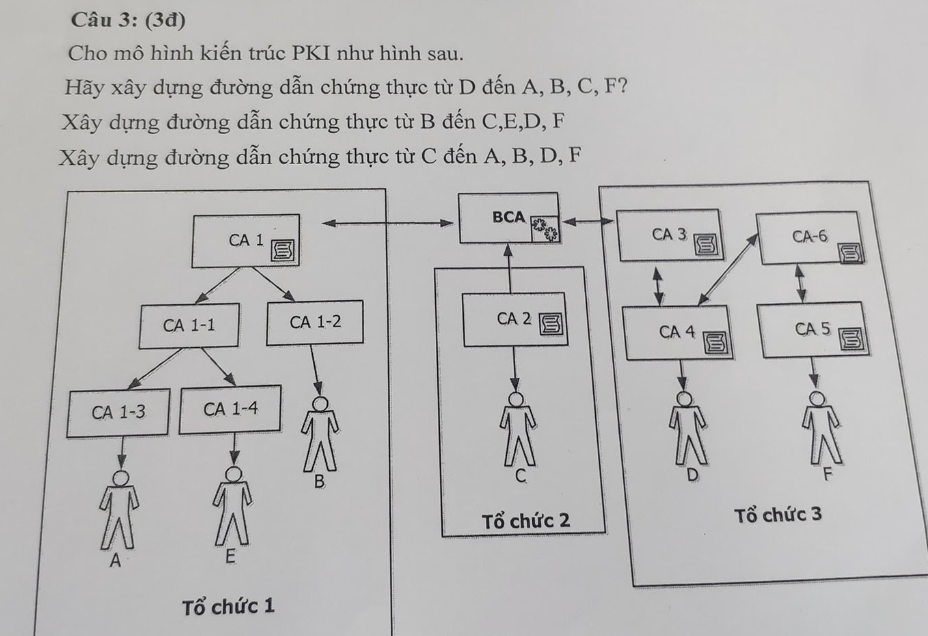
Đề 3:



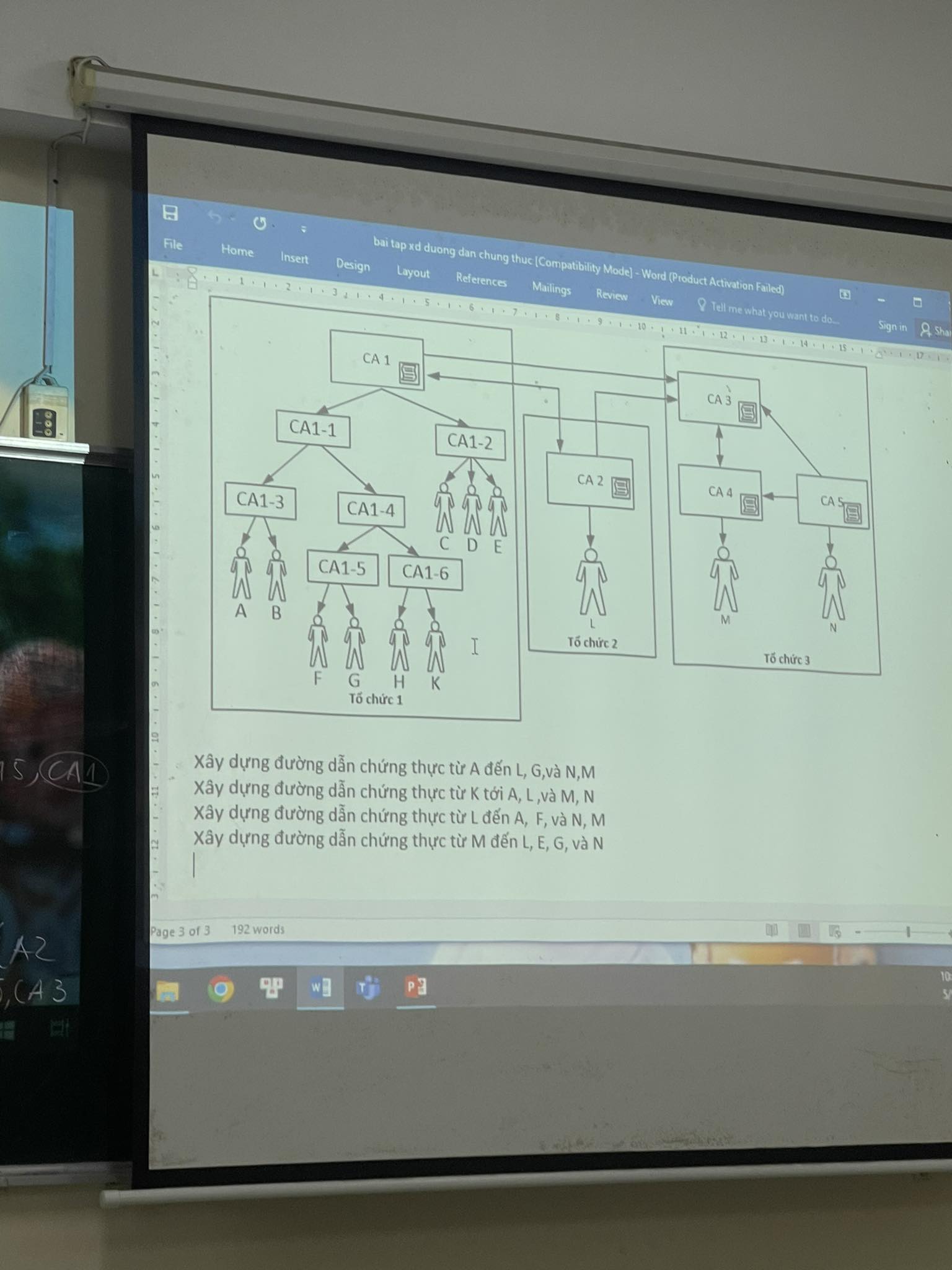
Đề 2:

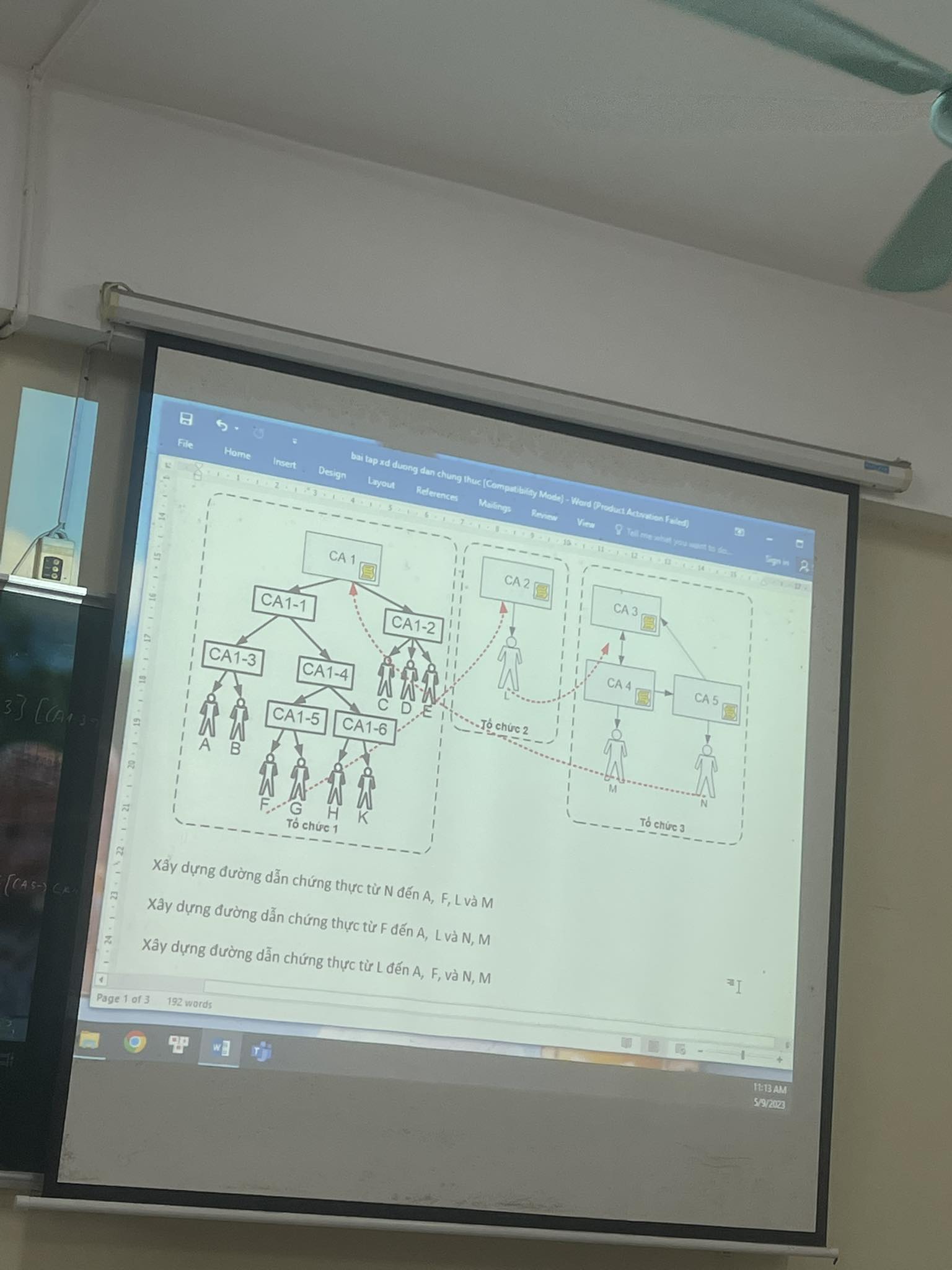


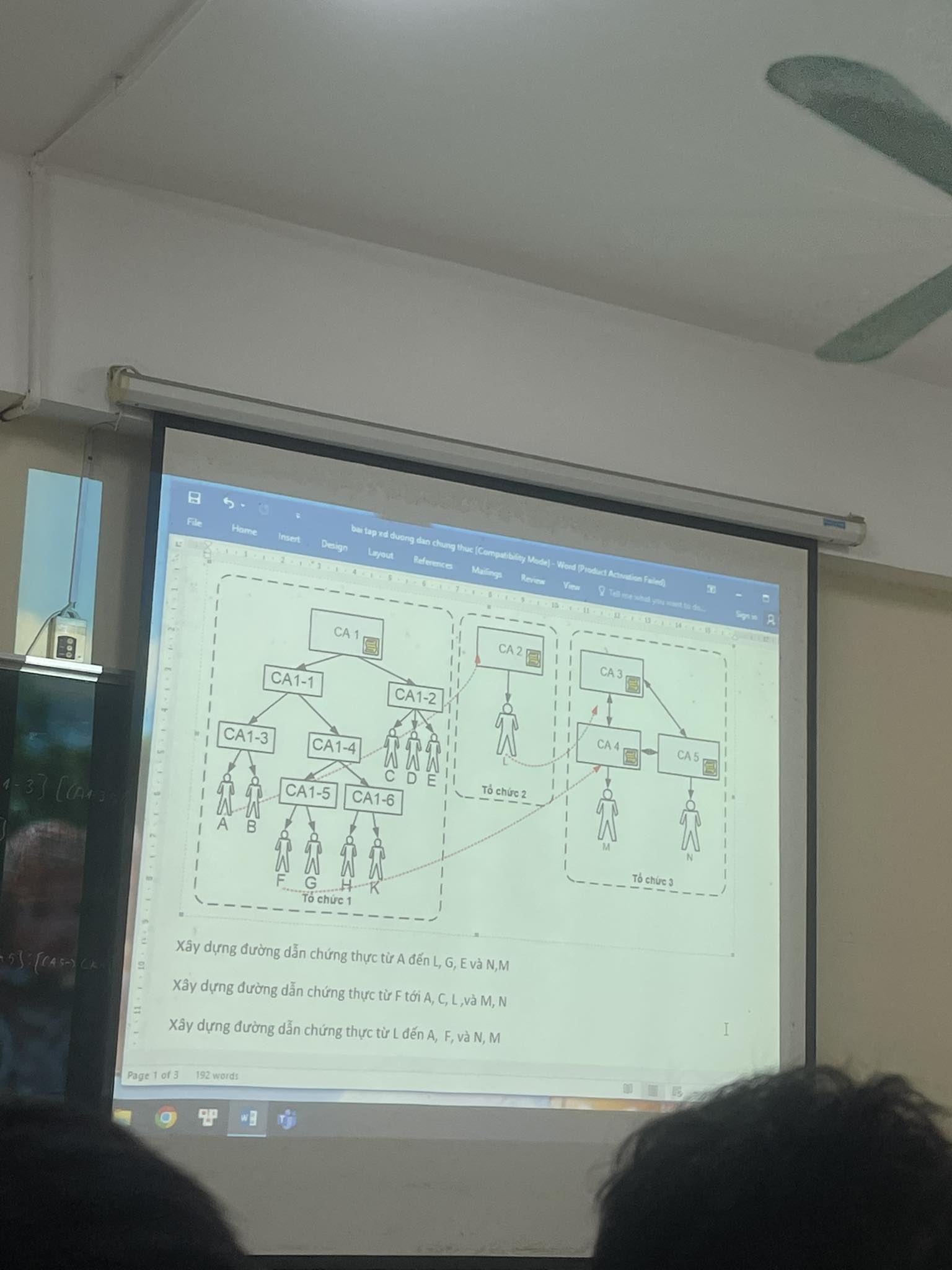
Đề 1:

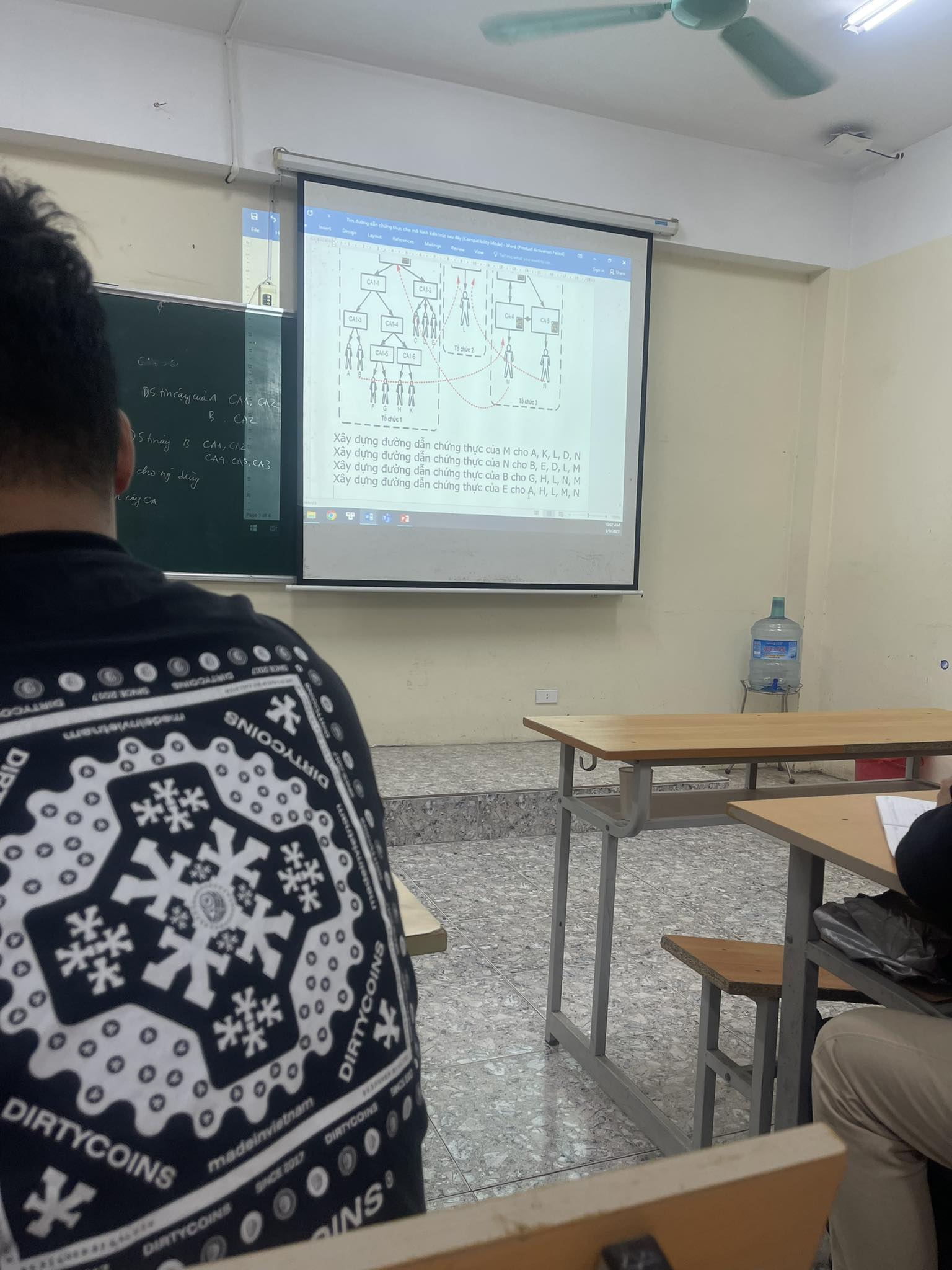


Một số bài tập khác:









# **Dạng 3: Tạo và kiểm tra chữ ký số**

***Kiến thức:***

*Chữ ký số RSA*: m là bản tin cần ký

• Tạo chữ ký số: S = = mod n

• Kiểm tra chữ ký số: (m, S) ↔ đúng nếu m = mod n

*Thuật toán RSA:* Chọn p và q, tính n = p ∗ q

• φ(n) = (p – 1) (q – 1) là 1 số chẵn

• Chọn khóa e sao cho gcd(e, φ(n)) = 1

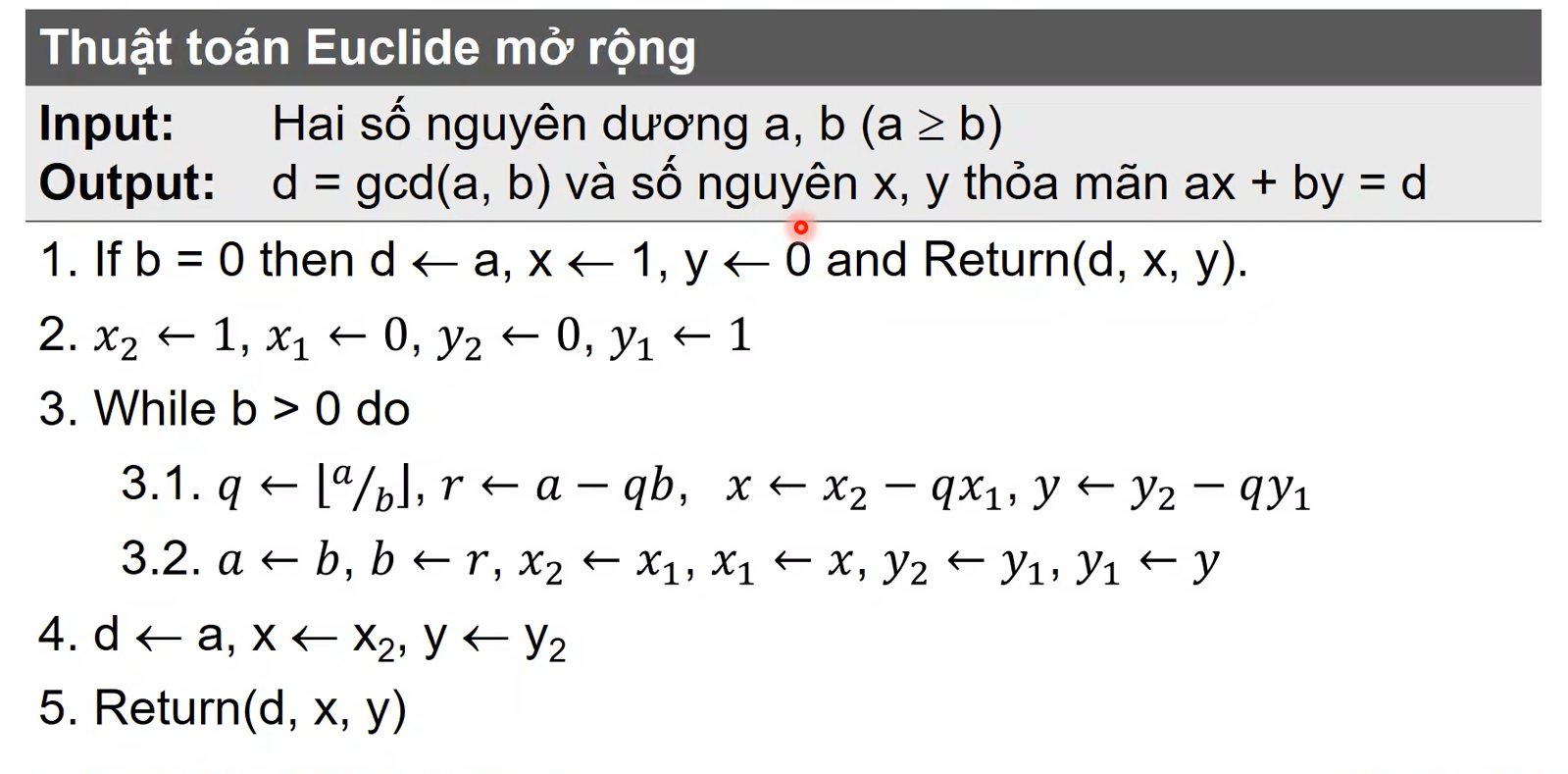
• Chọn khóa d sao cho d = mod φ(n) (dùng euclide mở rộng)

(e, n) là khóa công khai và d là khóa bí mật

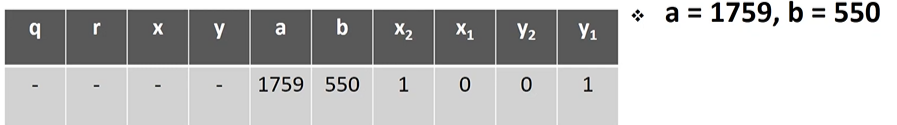
• Mã hóa: C = mod n (dùng nhân bình phương có lặp)

• Giải mã: M = mod n

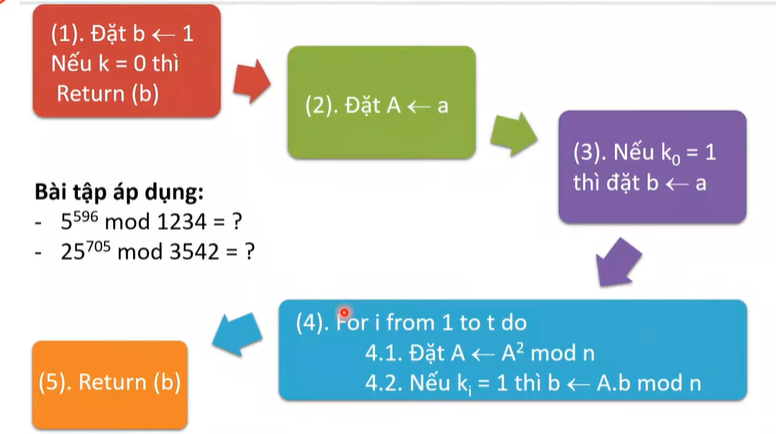
*Thuật toán Euclide mở rộng:*



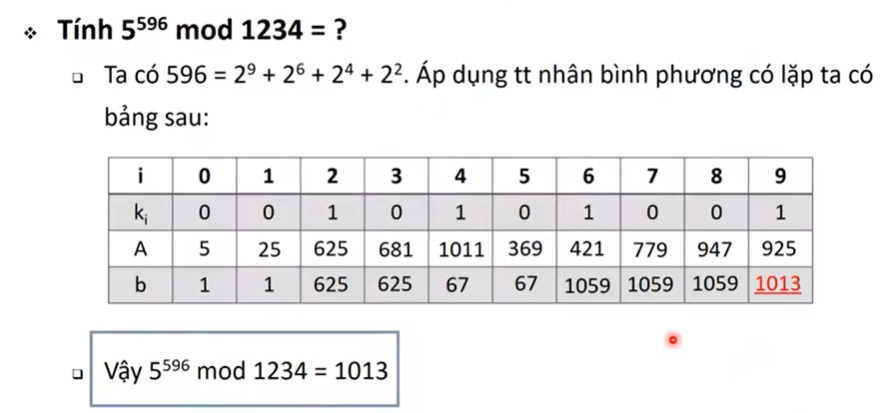
Ví dụ: Kẻ bảng tính



*Thuật toán nhân bình phương có lặp:*



Ví dụ:



**Bài tập:** Cho p = 61, q = 53, m = 42, chọn e = 17

1. Thực hiện mã và giải mã m
2. Thực hiện ký và kiểm tra chữ ký trên m

**Giải:**

1. Tính n = p.q = 3233

φ(n) = (p – 1) (q – 1) = 60.52 = 3120

d =

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| q | r | x | y | a | b |  |  |  |  |
|  |  |  |  | 3120 | 17 | 1 | 0 | 0 | 1 |
| 183 | 9 | 1 | -183 | 17 | 9 | 0 | 1 | 1 | -183 |
| 1 | 8 | -1 | 184 | 9 | 8 | 1 | -1 | -183 | 184 |
| 1 | 1 | 2 | -367 | 8 | 1 | -1 | 2 | 184 | -367 |
| 8 | 0 | -17 | 3120 | 1 | 0 | 2 | -17 | -367 | 3120 |

=>d = => d = -367 mod 3120 = 2753

***Mã hóa:*** C = mod n = (áp dụng bình phương lặp để tính)

***Giải mã****:* M = mod n = (tương tự)

1. Tạo chữ ký số và kiểm tra

***Tạo chữ ký số:*** S = = mod n =

Ta có

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| k | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| A | 42 | 1764 | 1550 | 381 | 2909 | 1520 | 2038 | 2272 | 2116 | 2984 | 574 | 2943 |
| B | 42 | 42 | 42 | 42 | 42 | 42 | 1538 | 2696 | 2696 | 1160 | 1160 | 3065 |

sẽ lần lượt lấy mod n

Ví dụ:

Nếu bit bắt đầu k = 0 thì b = 1 (bài này bit k đầu tiên là 1)

Nếu bit = 0 thì B giữ nguyên: nên B vẫn giữ nguyên là 42

Nếu bit thì B = b.A mod n: nên

=>S = 3065 là chữ ký số tạo được

***Kiểm tra chữ ký số:*** (m, S) ↔ đúng nếu m = mod n

Tính mod n = ( áp dụng bình phương có lặp) tính ra so sánh kết quả vs m nếu = thì hợp lệ, nếu không suy ra chữ ký số không hợp lệ