Lý thuyết:

Form đề gồm 3 câu: hình thức thi viết 60p

Được sử dụng tài liệu

Câu 1: Giải mã, mã hóa Cho công thức dữ liệu trên đường truyền, vẽ sơ đồ hệ thống và giải thích.

Câu 2: Lý thuyết so sánh, mã hóa/giải mã bằng tay.

Câu 3: Lập trình mã hóa/giải mã hoặc cho một hệ thống đánh giá ưu nhược điểm của hệ thống.

Lý thuyết:

|  |  |
| --- | --- |
| E(K,?)  Mã hóa |  |
| D(K,?)  Giải mã |  |
| E(PRA, ?) |  |
| D(PUA, ?) |  |
| A || B |  |

Chú ý: Từ M qua mã hash được H(M) nhưng không thể tính ngược để thu được M từ H(M) .

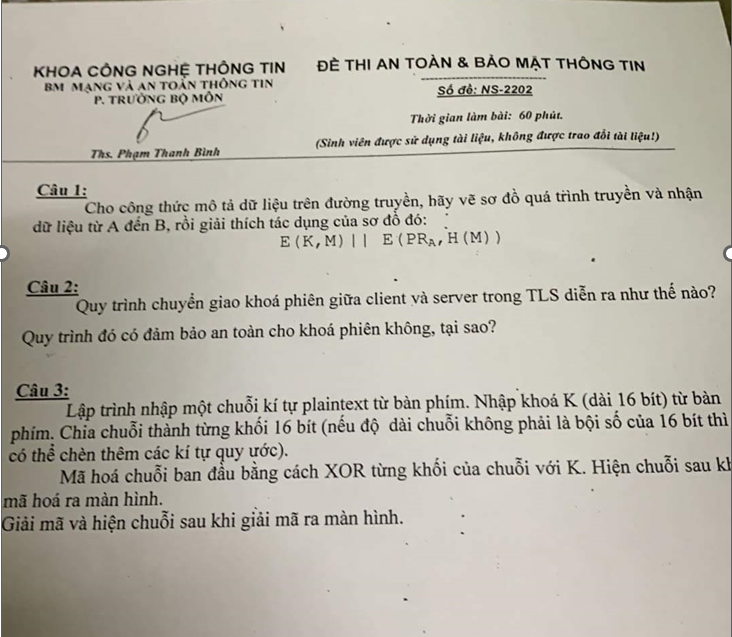
Ngoài ra còn có các ký hiêu khác: IDx : Định danh x, khi vẽ coi như 1 thông điệp (Tương tự như thông điệp M)

Tác dụng :

|  |  |
| --- | --- |
| Mật mã bất đối xứng | Khóa riêng (PRa): Khóa riêng của người gửi   * Xác thực nguồn gốc thông điệp   Khóa công khai người nhận (PUb)   * Bảo mật thông điệp trên đường truyền * Tốc độ chậm hơn mật mã đối xứng |
| Mật mã đối xứng | E(K): Có tác dụng bảo mật   * Tốc độ nhanh hơn mật mã bất đối xứng |
| Mã MAC | Sử dụng mật khóa K (C(K, ?),…)   * Mã chứng thực thông điệp |
| Mã Hash | H(…) |

Chữa đề:

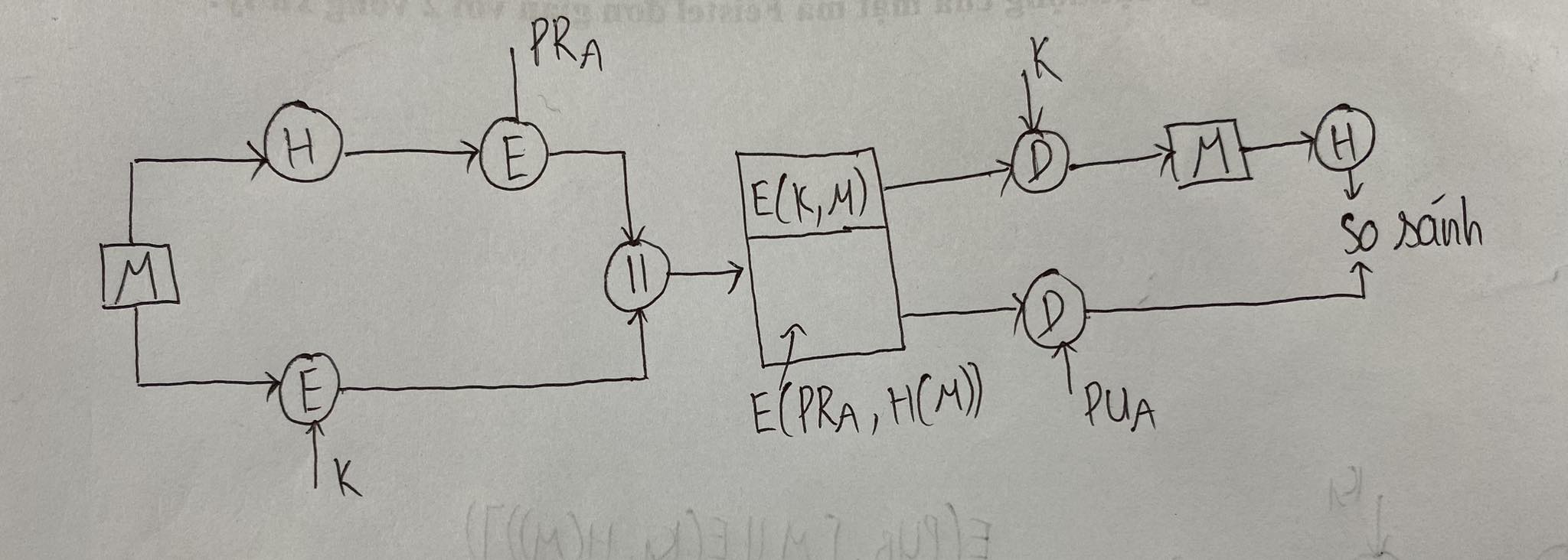
Đề 1:



Giải

Câu 1:

## E(K, M) || E(PRA, H( M))



**Bên gửi :**

* + - * A gửi B đoạn mã gồm 2 phần ghép với nhau:

Phần 1: Mã hóa thông điệp M với khóa K bởi hàm mã hóa E thu được E(K,M)

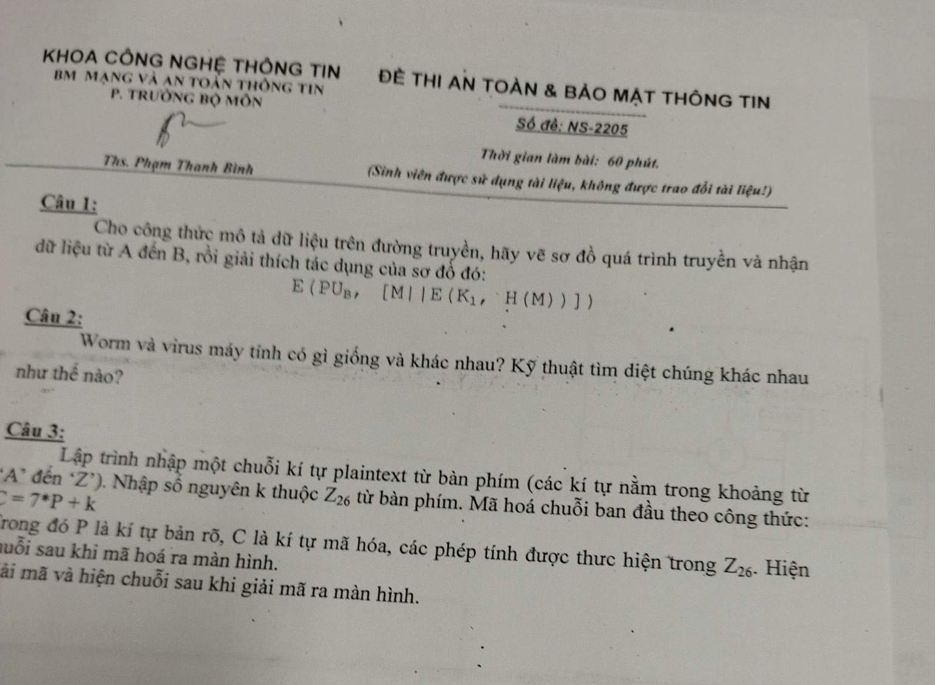
Phần 2: Mã hóa thông điệp M với hàm Hash thu được H(M) rồi đưa H(M) qua hàm mã hóa E với khóa riêng của người gửi thu được E(PRa, H(M))

**Bên nhận:**

* + - * B nhận được đoạn mã từ A:
        + Đưa hàm mã hóa E(K, M) đưa qua hàm giải mã D với khóa K được thông điệp M.
        + Mã hóa thông điệp M với hàm hash thu được H(M) (\*)
        + Đưa hàm mã hóa E(PRa, H(M)) qua hàm giải mã D với khóa công khai PUb thu được H(M) (\*\*)
        + So sánh hàm Hash (\*) thu được và hàm Hash (\*\*) trong đoạn mã để xác thực nội dung thông điệp có bị thay đổi trên đường truyền hay ko.

**Tác dụng:** Xác thực nội dung thông điệp có chính xác không, khóa E(K) có tác dụng bảo mật thông điệp, Khóa PRa: Xác thực nguồn gốc thông điệp.

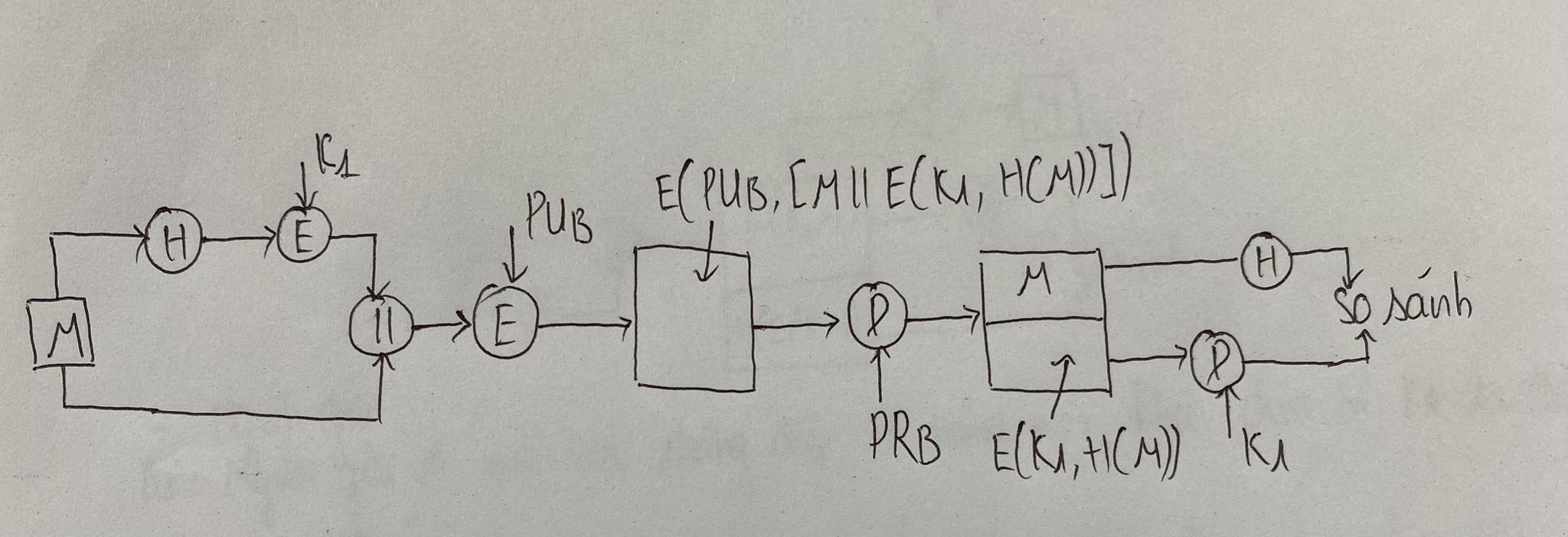
Đề 2:



Giải:

Câu 1:

## E(PUB, [M || E(K1, H(M))])



**Bên gửi :**

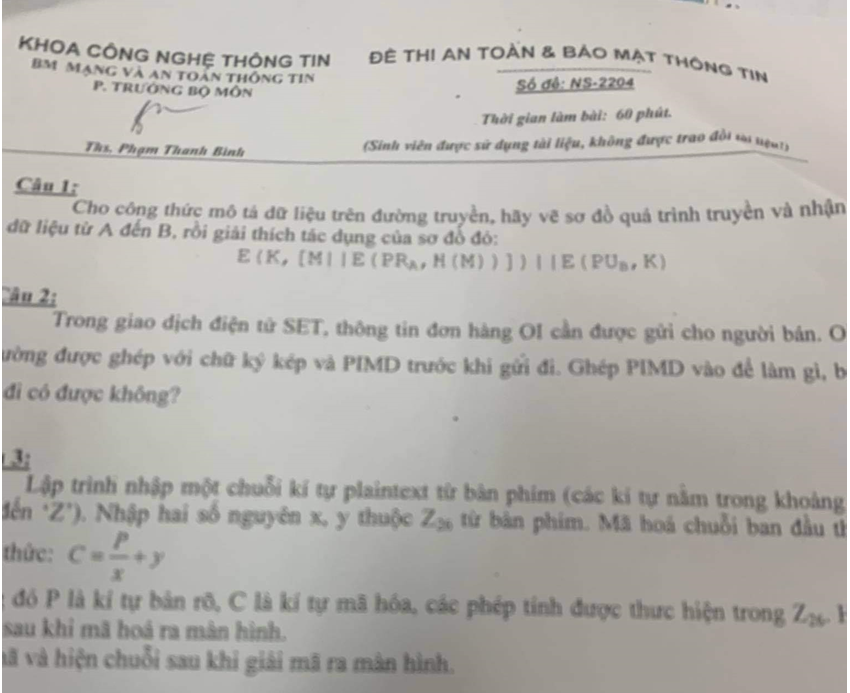
* + - * A gửi B đoạn mã
      * Phần 1: Mã hóa thông điệp M với hàm hash thu được H(M) , Mã hóa H(M) với khóa K1 bởi hàm mã hóa E thu được E(K1,H(M)), lấy E(K1,H(M)) ghép nối với thông điệp M được M|| E(K1,H(M)), đưa tất cả mã hóa với khóa công khai PUb bởi hàm mã hóa E thu được E(PUb, [M|| E(K1,H(M))])

**Bên nhận:**

* + - * B nhận được đoạn mã từ A:
      * Đưa hàm mã hóa E(PUb, [M|| E(K1,H(M))]) đưa qua hàm giải mã D với khóa PRb được thông điệp M|| E(K1,H(M))
        + Mã hóa thông điệp M với hàm hash thu được H(M) (\*)
        + Đưa hàm mã hóa E(K1,H(M)) qua hàm giải mã D với khóa K1 thu được H(M) (\*\*)
        + So sánh hàm Hash (\*) thu được và hàm Hash (\*\*) trong đoạn mã để xác thực nội dung thông điệp có bị thay đổi trên đường truyền hay ko.

**Tác dụng:** Xác thực nội dung thông điệp có chính xác không, PUb: Bảo mật thông điệp trên đường truyền, E(K): Có tác dụng bảo mật

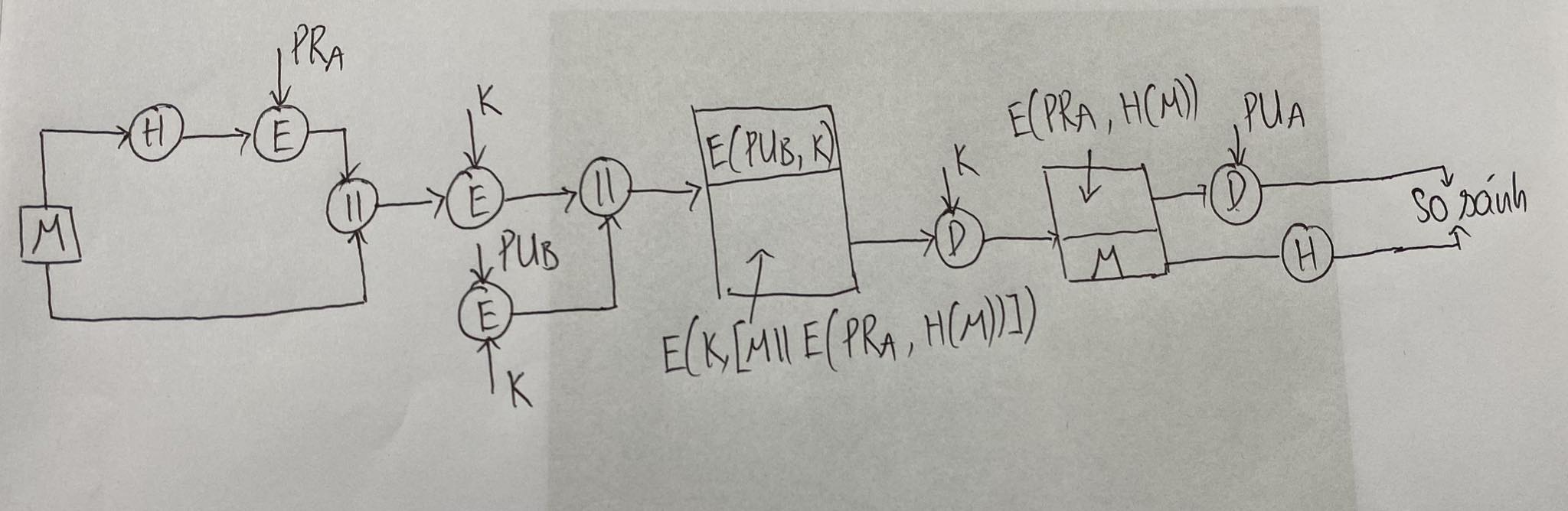
Đề 3:



Giải

Câu 1:

## E(K, [M || E(PRA, H(M)) ]) || E(PUB, K)



**Bên gửi :**

* + - * A gửi B đoạn mã gồm 2 phần ghép với nhau:

Phần 1: Mã hóa thông điệp M với hàm hash thu được H(M), Mã hóa H(M) với khóa PRa bởi hàm mã hóa E thu được E(PRa,H(M)), lấy mã thu được ghép nối với M ta được

M|| E(PRa,H(M)). Mã hóa M|| E(PRa,H(M)) với khóa K bởi hàm mã hóa E thu được E(K, M|| E(PRa,H(M)))

Phần 2: Khóa K đưa qua khóa PUb của hàm E thu được E(PUb, K))

**Bên nhận:**

* + - * B nhận được đoạn mã từ A:

+ Giải mã hàm E(K, M|| E(PRa,H(M))) qua hàm giải mã D với khóa K ta thu được M|| E(PRa,H(M))

+ Mã hóa thông điệp M với hàm hash thu được H(M) (\*)

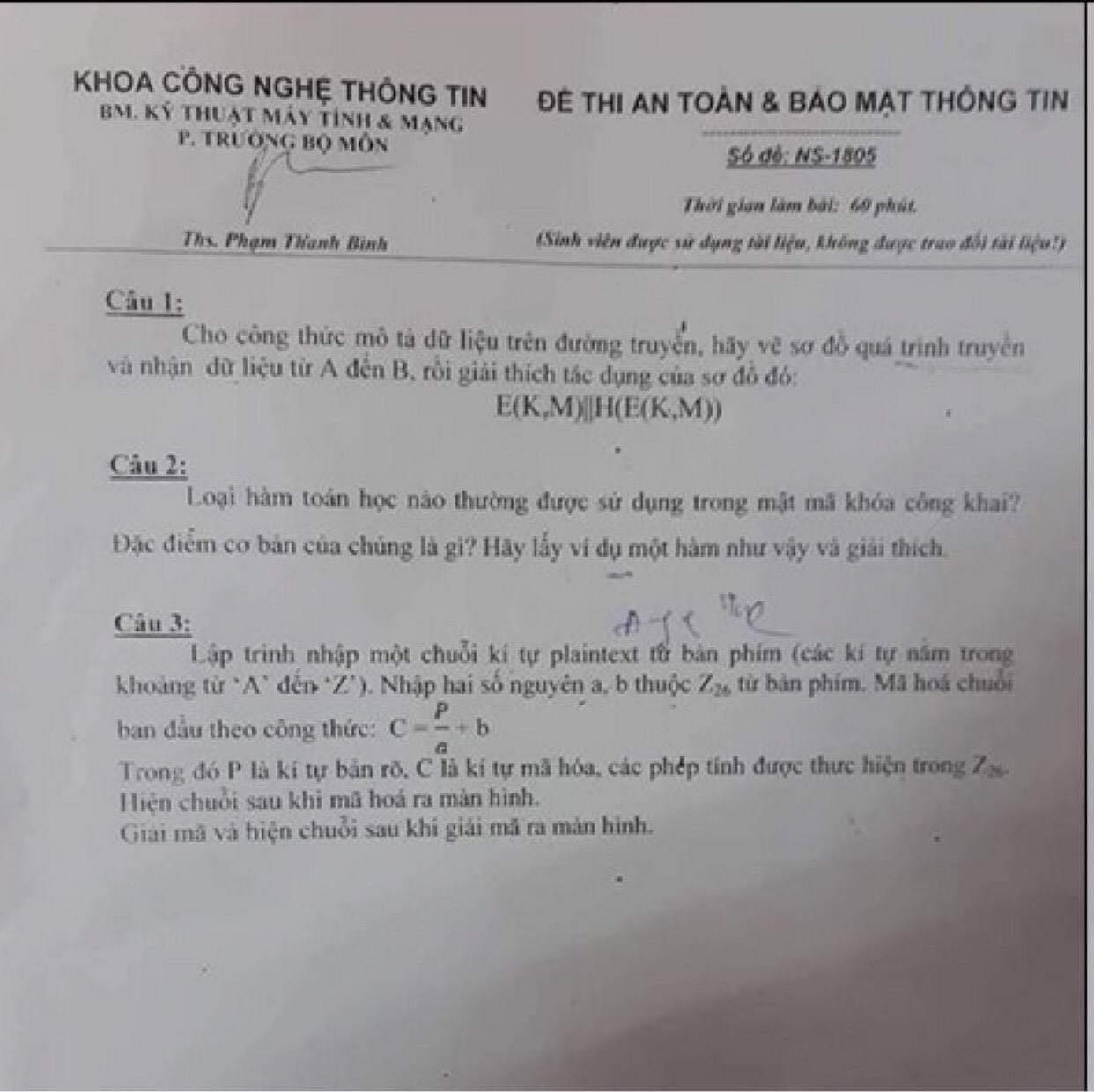
+ Giải mã hàm E(PRa,H(M)) qua hàm giải mã D với khóa công khai PUb thu được H(M) (\*\*)

* So sánh hàm Hash (\*) thu được và hàm Hash (\*\*) trong đoạn mã để xác thực nội dung thông điệp có bị thay đổi trên đường truyền hay ko.

**Tác dụng:** Xác thực nội dung thông điệp có chính xác không

Khóa PRa: Xác thực nguồn gốc thông điệp, khóa PUb: Bảo mật thông điệp trên đường truyền, E(K): Có tác dụng bảo mật, khóa PRb: xác thực nguồn gốc thông điệp.

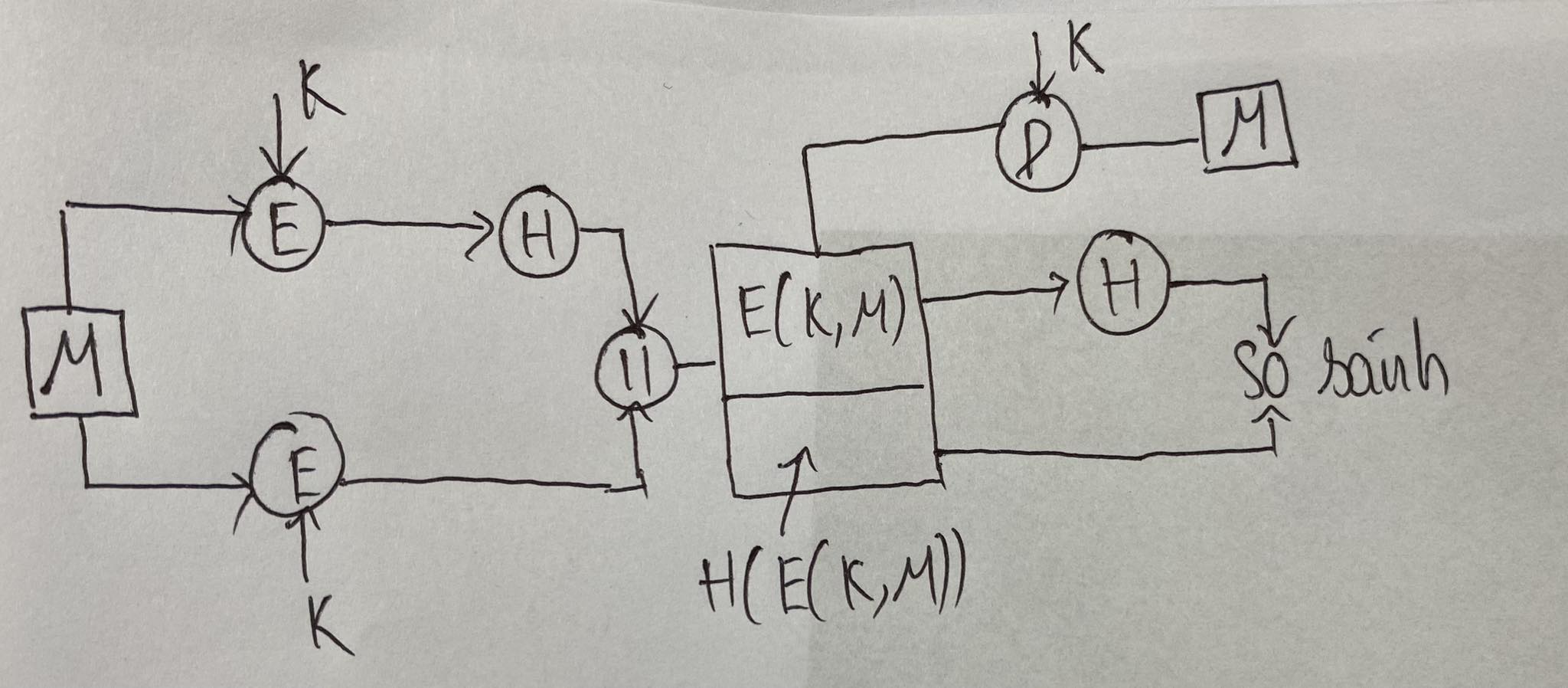
Đề 4:



Giải:

Câu 1:

## E(K,M) || H(E(K, M))



**Bên gửi :**

* + - * A gửi B đoạn mã gồm 2 phần ghép với nhau:

Phần 1: Mã hóa thông điệp M với khóa K bởi hàm mã hóa E thu được E(K,M)

Phần 2: Mã hóa thông điệp M với khóa K bởi hàm mã hóa E thu được E(K,M) rồi đưa toàn bộ E(K,M) qua hàm Hash thu được H(E(K,M))

**Bên nhận:**

* + - * B nhận được đoạn mã từ A:
        + Đưa hàm mã hóa E(K, M) đưa qua hàm hash thu được mã hask H(E(K, M)). So sánh hàm Hash thu được và hàm Hash trong đoạn mã để xác thực nội dung thông điệp có bị thay đổi trên đường truyền hay ko.

**Tác dụng:** Xác thực nội dung thông điệp có chính xác không

Khóa E(K): Có tác dụng bảo mật.

