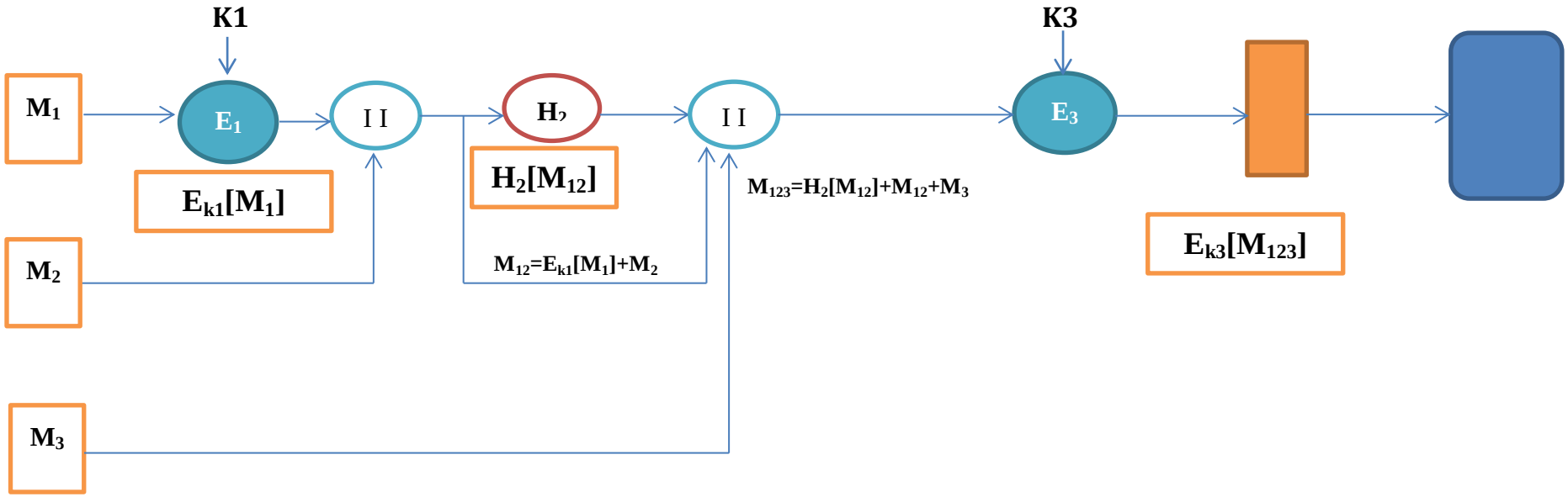
**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP HCM**
**KHOA CÔNG NGHỆ THÔNG TIN**
**Môn: Bảo mật thông tin**

# MÃ ĐỀ THI

- **Cho sơ đồ sau:**

## 1. Mã Hóa

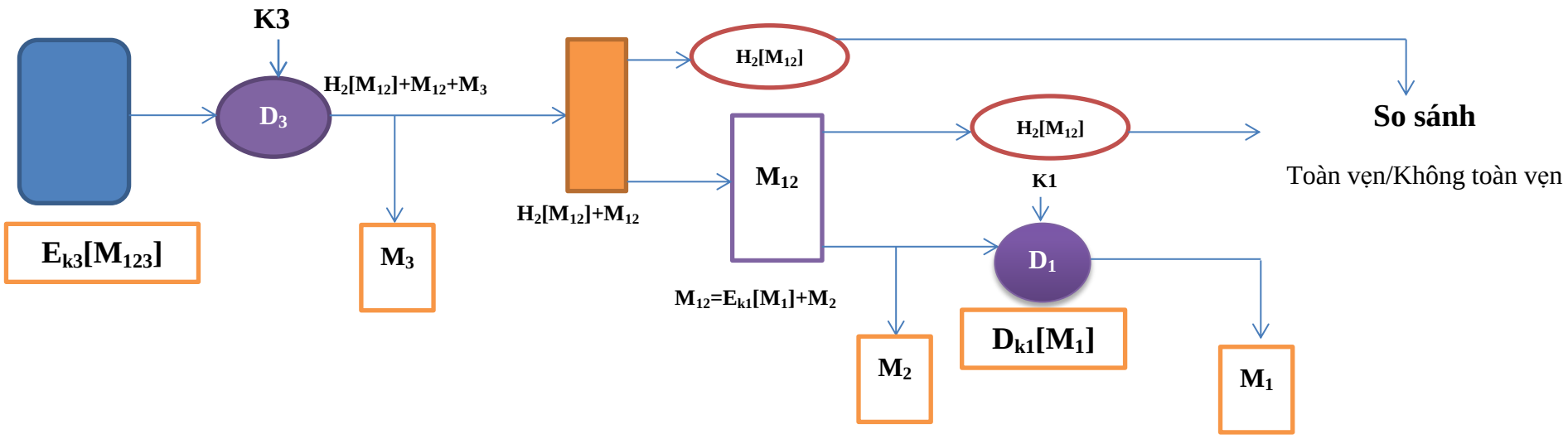



-Sơ đồ sử dụng 3 thuật toán ( $E_1$,$H_2$,$E_3$).

- $M_1$, $M_2$, $M_3$: Văn bản đầu vào.
- I I : nối chuỗi, E : Mã hóa, H : Hàm băm, : kết quả sau khi mã hóa/giải mã,

D : giãi mã

## 2. Giải Mã



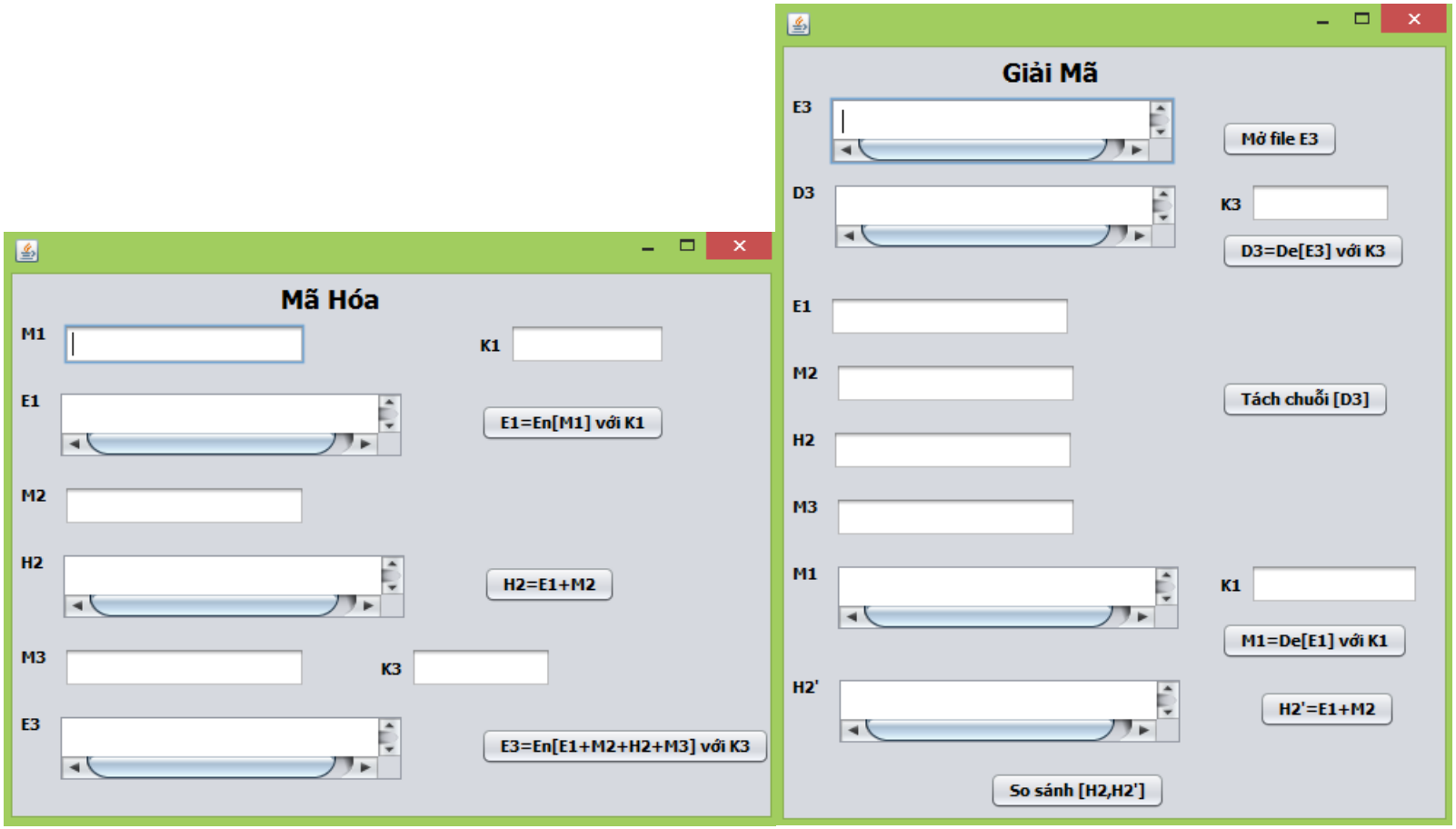

**Yêu cầu**: Anh/Chị hãy viết chương trình mô tả quá trình mã hóa và giải mã thực hiện cho sơ đồ.

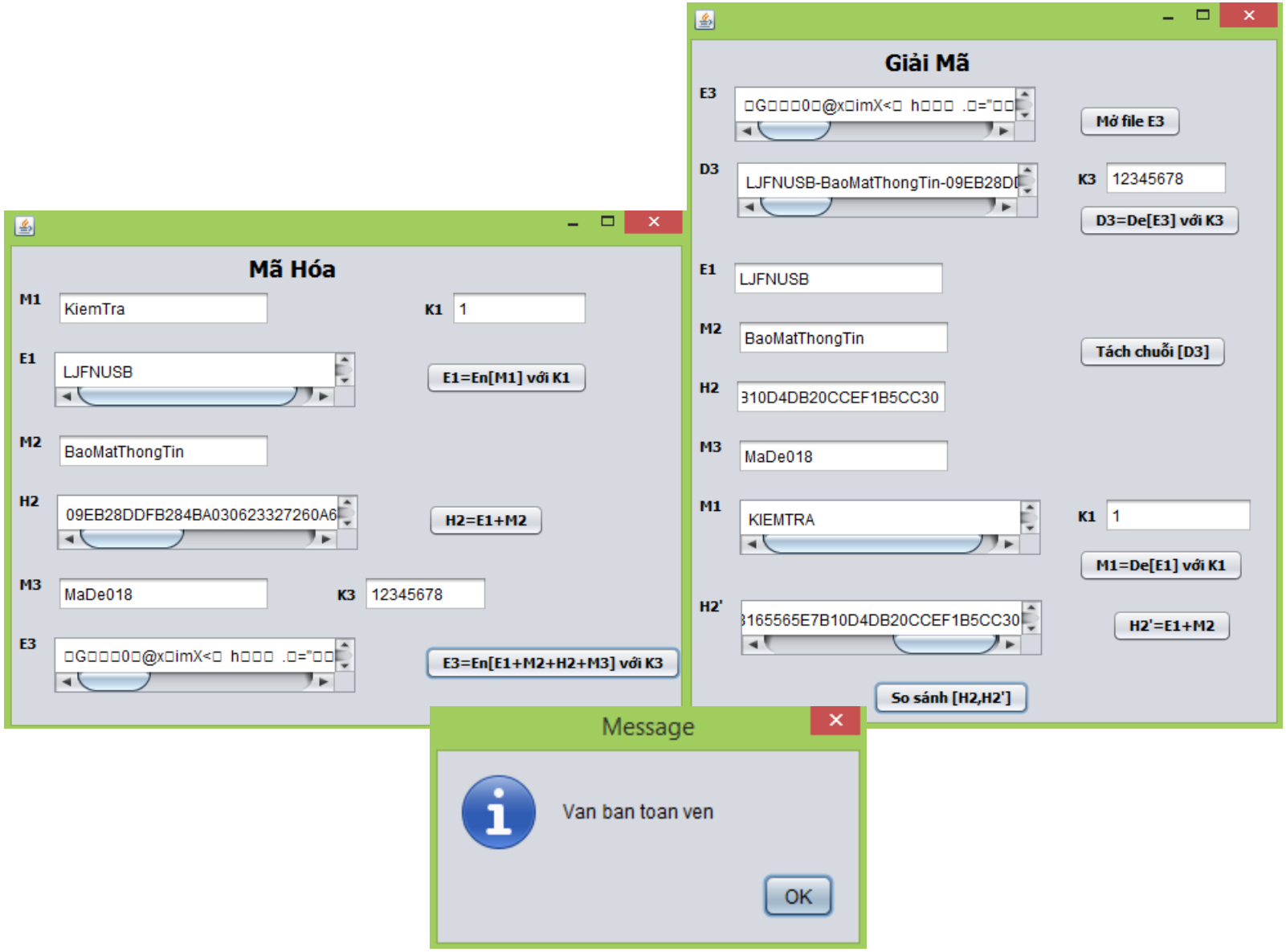
| Bảng các thuật toán | | | | | |
|---|---|---|---|---|---|
| **STT** | **Thuật toán** | **STT** | **Thuật toán** | **STT** | **Thuật toán** |
| **0** | Ceasar | **4** | 3DES | **8** | DES |
| **1** | Vigenere | **5** | AES | **9** | 3DES |
| **2** | Rail Fence | **6** | Vigenere | | |
| **3** | DES | **7** | AES | | |

**Lưu ý:** Dựa vào " ***3 số cuối của mã số sinh viên***" và tra "***Bảng các thuật toán***" để xác định đề thi. Số thứ nhất là thuật toán 1, số thứ hai là thuật toán số 2 ( số chẵn là thuật toán MD5, số lẽ là thuật toán SHA), số thứ ba là thuật toán 3. Ví dụ 3 số cuối của MSSV là **018**, tra trong " Bảng các thuật toán" ta có đề thi sau: Số **"0"** ta sử dụng Thuật toán Ceasar, số **"1"** ta sử dụng thuật toán SHA, số **"8"** ta sử dụng thuật toán DES.

# Gợi ý

Xây dựng 2 form:  1 form mã hóa và 1 form giải mã




Giải Mã
E3
□G□□□0□@x□imX<□ h□□□ .□="□□
Mở file E3
D3
LJFNUSB-BaoMatThongTin-09EB28DD
K3
12345678
D3=De[E3] với K3
E1
LJFNUSB
M2
BaoMatThongTin
Tách chuỗi [D3]
H2
310D4DB20CCEF1B5CC30
M3
MaDe018
M1
KIEMTRA
K1
1
M1=De[E1] với K1
H2'
3165565E7B10D4DB20CCEF1B5CC30
H2'=E1+M2
So sánh [H2,H2']
Mã Hóa
M1
KiemTra
K1
1
E1
LJFNUSB
E1=En[M1] với K1
M2
BaoMatThongTin
H2
09EB28DDFB284BA030623327260A6
H2=E1+M2
M3
MaDe018
K3
12345678
E3
□G□□□0□@x□imX<□ h□□□ .□="□□
E3=En[E1+M2+H2+M3] với K3
Message
Van ban toan ven
OK

..... Hết.....