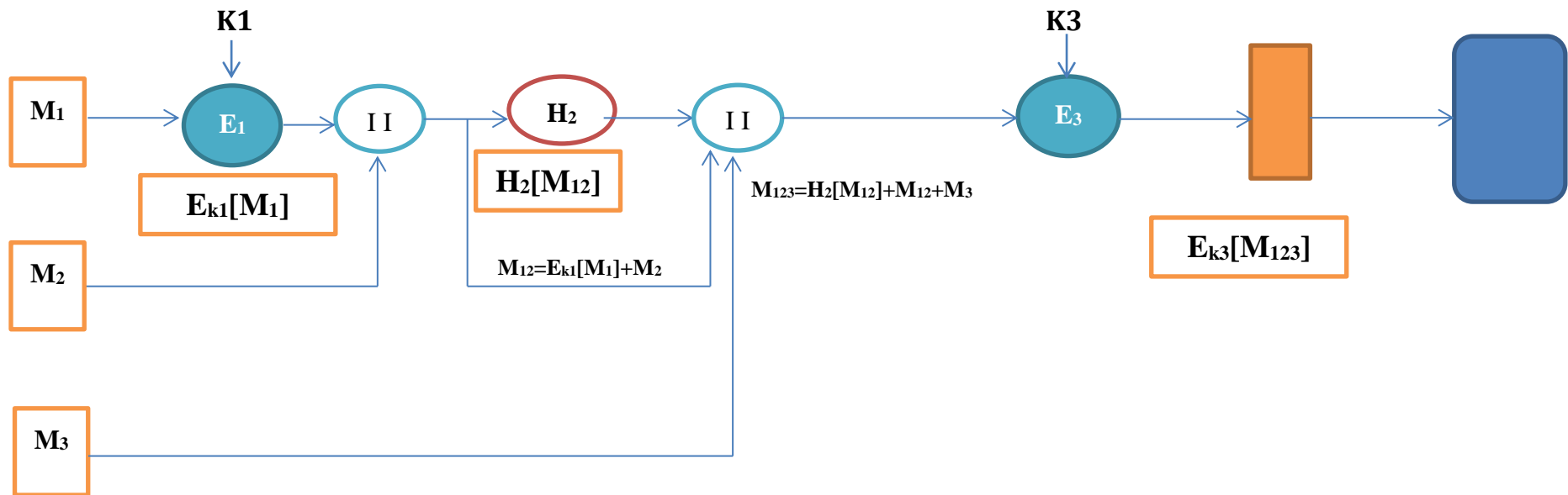




## MÃ ĐỀ THI



- Cho sơ đồ sau:

### 1. Mã Hóa

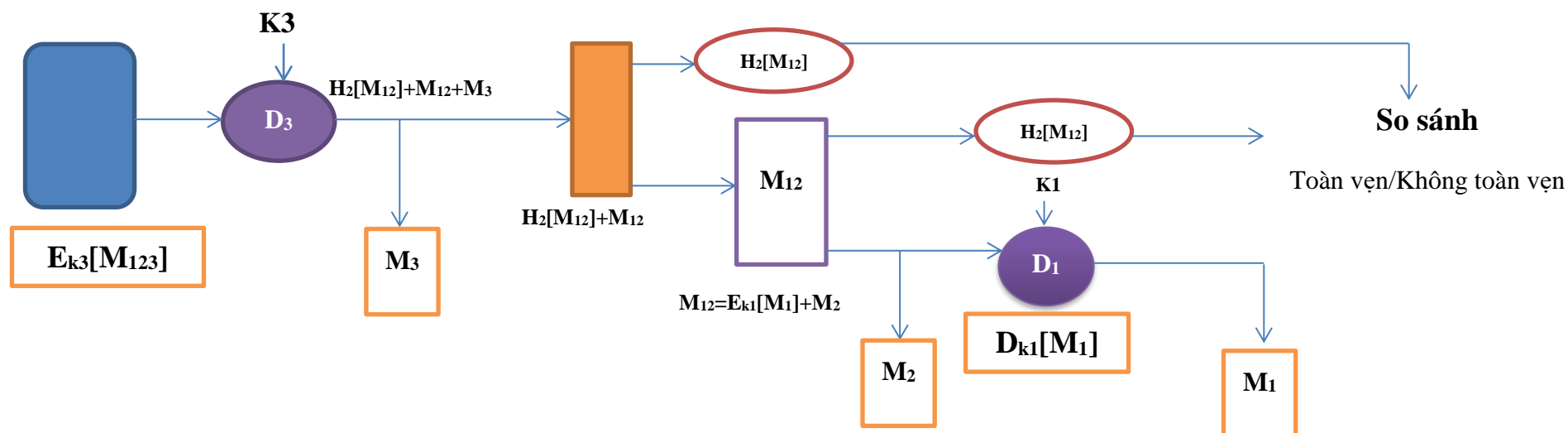


- Sơ đồ sử dụng 3 thuật toán ( $E_1, H_2, E_3$ ).

-  $M_1, M_2, M_3$ : Văn bản đầu vào.

-  $II$  : nối chuỗi,  $E$  : Mã hóa,  $H$  : Hàm băm,  : kết quả sau khi mã hóa/giải mã,  
  $D$  : giải 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	3DES
1	Vigenere	5	AES	9	DES
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. Trong đó:

- Số thứ nhất là thuật toán mã hóa E1
- Số thứ hai là hàm băm H2 ( nếu số chẵn là thuật toán MD5, số lẻ là thuật toán SHA)
- Số thứ ba là thuật toán mã hóa E3

Ví dụ 3 số cuối của MSSV là **018**, tra trong “ **Bảng các thuật toán**” ta có đề thi sau:

- Số “**0**”: Thuật toán mã hóa E1= Ceasar
- Số “**1**”: Hàm băm H2=SHA
- Số “**8**”: Thuật toán mã hóa E3=3DES

### Gợi ý

Xây dựng 2 form: 1 **FORM ENCRYPT** và 1 **FORM DECRYPT**

The screenshot shows a Windows-style application window titled "FORM ENCRYPT". The window has a light blue background and contains several input fields and buttons. The fields are labeled as follows:

- Message(M1):
- Key Encrypt (K1):
- Cipher (E1)=En(M1) với K1:
- Message (M2):
- Message(N1)=E1+M2:
- Message Hash (H2):
- Message (M3):
- Message (N2)=N1+H2+M3:
- Key Encrypt (K3):
- Cipher (E3)=En(N2) với K3:

Buttons are placed to the right of the input fields:

- "Mã hóa M1" is next to the "Cipher (E1)" field.
- "Nối chuỗi N1" is next to the "Message(N1)" field.
- "Băm chuỗi N1" is next to the "Message Hash (H2)" field.
- "Nối chuỗi N2" is next to the "Message (N2)" field.
- "Mã hóa N2" is next to the "Cipher (E3)" field.

The input fields for "Message (N2)" and "Cipher (E3)" are text boxes with a vertical scrollbar on the right side.

## FORM DECRYPT

Cipher (E3):

Mở File mã hóa E3

Key Encrypt (K3):

Decrypt (D3):

Giải mã E3

Message (M3):

Tách chuỗi D3 gồm: M3+H2+N1

Message (H2):

Message (N1):

Tách chuỗi N1 gồm: M2+E1

Message (M2):

Message (E1):

Key Encrypt (E1):

Message (M1):

Giải mã E1

Hash (H2'):

Băm chuỗi N1

Kiểm tra toàn vẹn



## FORM ENCRYPT

Message(M1):

Kiemtra

Key Encrypt (K1):

2

Cipher (E1)=En(M1) với K1:

MKGOVTC

Mã hóa M1

Message (M2):

Baomatthongtin

Message(N1)=E1+M2:

MKGOVTC-Baomatthongtin

Nội chuỗi N1

Message Hash (H2):

7DB9B706AA61B4AC8F6FCBFC0C2EFC

Băm chuỗi N1

Message (M3):

Made118

Message (N2)=N1+H2+M3:

A61B4AC8F6FCBFC0C2EFC-Made118

Nội chuỗi N2

Key Encrypt (K3):

baomatthongtinNguyenvanA

Cipher (E3)=En(N2) với K3:

KYXfzOOIAx3QGq+GSSlg+GaKyLsJL3R

Mã hóa N2

**. Hết**

Van ban toan ven