

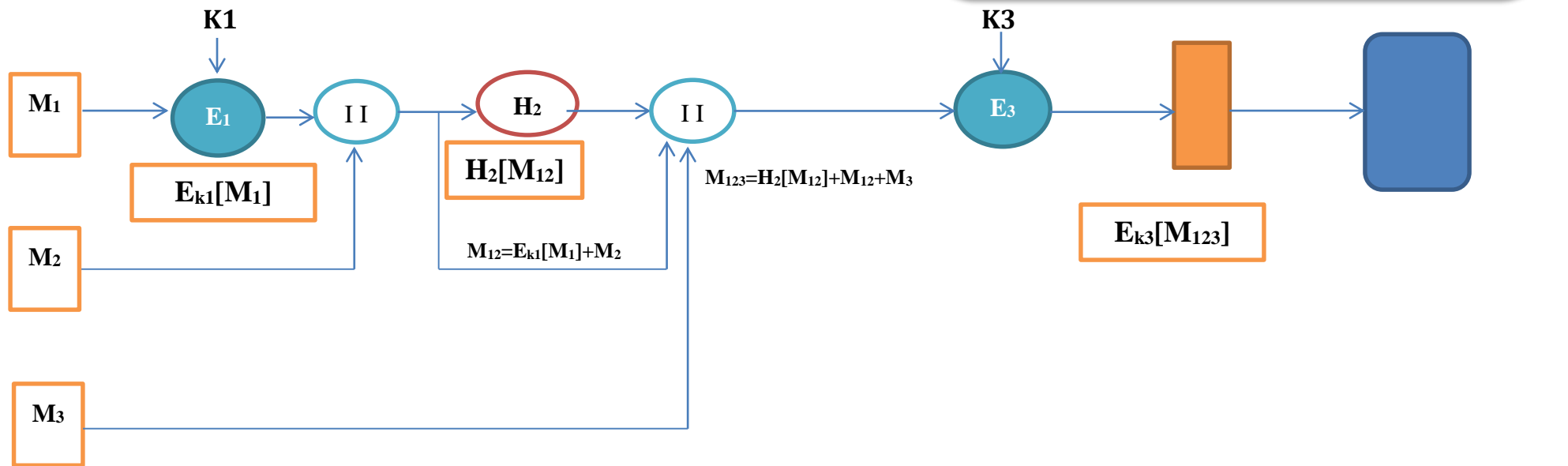


TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP HCM
KHOA CÔNG NGHỆ THÔNG TIN
Môn: Bảo mật thông tin

MÃ ĐỀ

- 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

Họ tên:

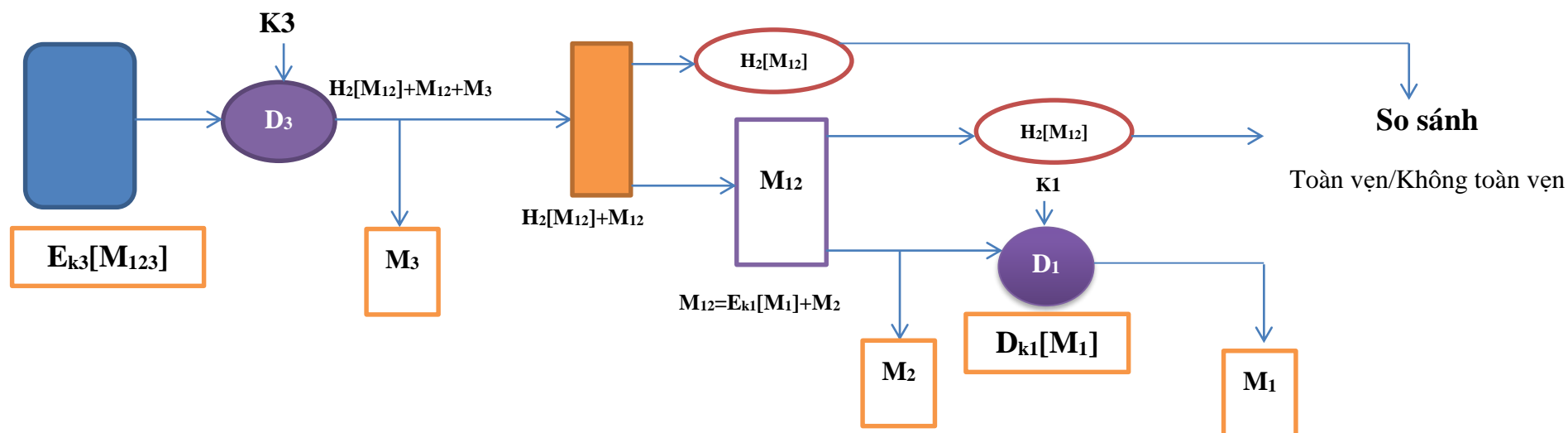
MSSV:

Mã đề:

- (E1):
- (H2):
- (E3):

Điểm:

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	Vigenere	4	PlayFair	8	Ceasar
1	RSA	5	3DES	9	DES
2	Transposition cipher	6	Rail Fence		
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 **815**, tra trong “ Bảng các thuật toán” ta có đề thi sau:

- Số “**8**”: Thuật toán mã hóa E1=Cesar
- Số “**1**”: Hàm băm H2=SHA
- Số “**5**”: Thuật toán mã hóa E3=3DES

Gợi ý

Xây dựng 2 form: 1 form gửi và 1 form nhận


The screenshot shows a Windows-style application window titled "FORM GUI". It contains several input fields and buttons arranged vertically. 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:

- Next to "Cipher (E1)=En(M1) với K1:" is a button labeled "Mã hóa M1".
- Next to "Message(N1)=E1+M2:" is a button labeled "Nối chuỗi N1".
- Next to "Message Hash (H2):" is a button labeled "Băm chuỗi N1".
- Next to "Message (N2)=N1+H2+M3:" is a button labeled "Nối chuỗi N2".
- Next to "Cipher (E3)=En(N2) với K3:" is a button labeled "Mã hóa N2".

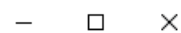
The input fields for "Message (N2)=N1+H2+M3:" and "Cipher (E3)=En(N2) với K3:" are text areas with horizontal scrollbars.

 — □ ×

FORM NHAN

Cipher (E3):	<input type="text"/>	Mở File mã hóa E3
Key Encrypt (K3):	<input type="text"/>	
Decrypt (D3):	<input type="text"/>	Giải mã E3
Message (M3):	<input type="text"/>	Tách chuỗi D3 gồm: M3+H2+N1
Message (H2):	<input type="text"/>	
Message (N1):	<input type="text"/>	Tách chuỗi N1 gồm: M2+E1
Message (M2):	<input type="text"/>	
Message (E1):	<input type="text"/>	Key Encrypt (E1): <input type="text"/>
Message (M1):	<input type="text"/>	Giải mã E1
Hash (H2'):	<input type="text"/>	Băm chuỗi N1

Kiểm tra toàn vẹn



FORM GUI

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

FORM NHAN

Cipher (E3):

zOOIAx3QGc+GSSlg+GaKyLsJL3R

Mở File mã hóa E3

Key Encrypt (K3):

baomatthongtinNguyenvanA

Decrypt (D3):

MKGOVTC-Baomatthongtin-E70D

Giải mã E3

Message (M3):

Made118

Tách chuỗi D3 gồm: M3+H2+N1

Message (H2):

9B706AA61B4AC8F6FCBFC0C2EFC

Message (N1):

MKGOVTC-Baomatthongtin

Tách chuỗi N1 gồm: M2+E1

Message (M2):

Baomatthongtin

Message (E1):

MKGOVTC

Key Encrypt (E1):

2

Giải mã E1

Message (M1):

KIEMTRA

Hash (H2'):

9B706AA61B4AC8F6FCBFC0C2EFC

Bấm chuỗi N1

Kiểm tra toàn vẹn

Message

i

Van ban toan ven

OK

Hết