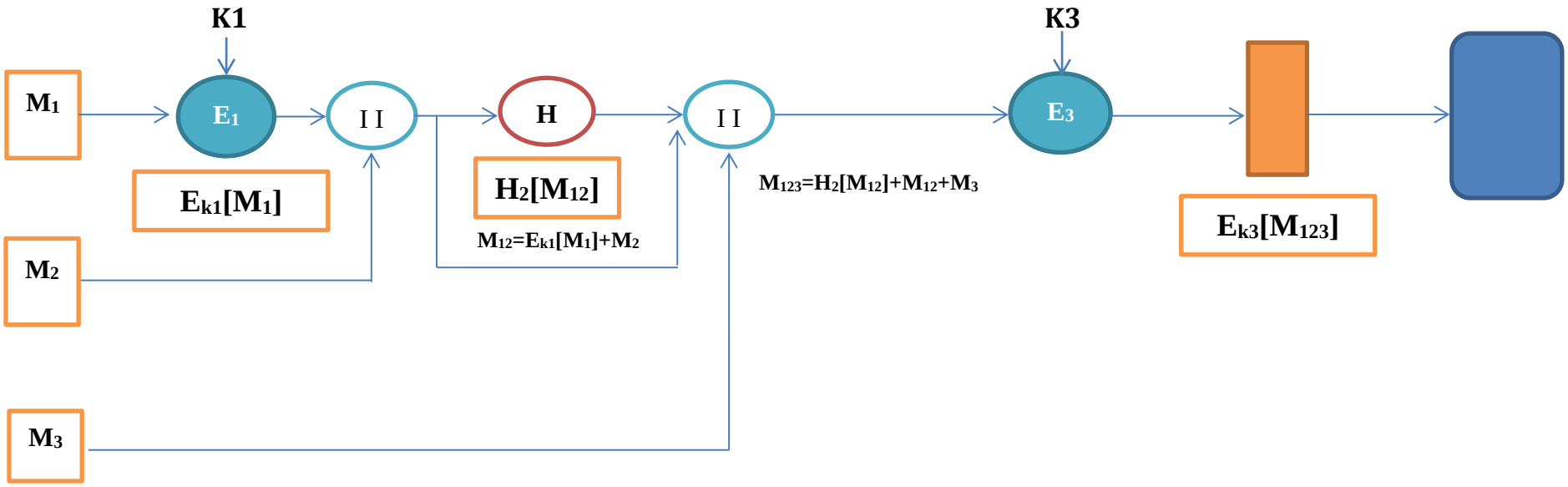
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP HCM
KHOA CÔNG NGHỆ THÔNG TIN
Môn: Bảo mật thông tin

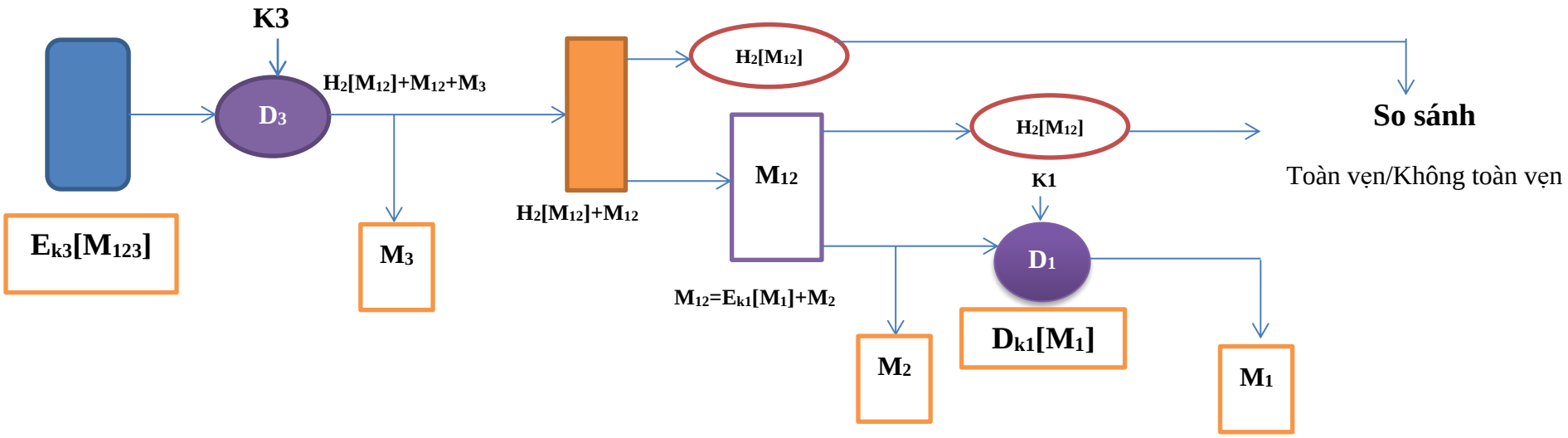
ĐỀ THI

❖ **Cho sơ đồ sau:**

1. **Mã Hóa**



2. Giải Mã



- 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 : 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	AES	**4**	Rail Fence	**8**	3DES
1	Vigenere	**5**	AES	**9**	Play Fair
2	3DES	**6**	DES		
3	RSA	**7**	Caesar		

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:

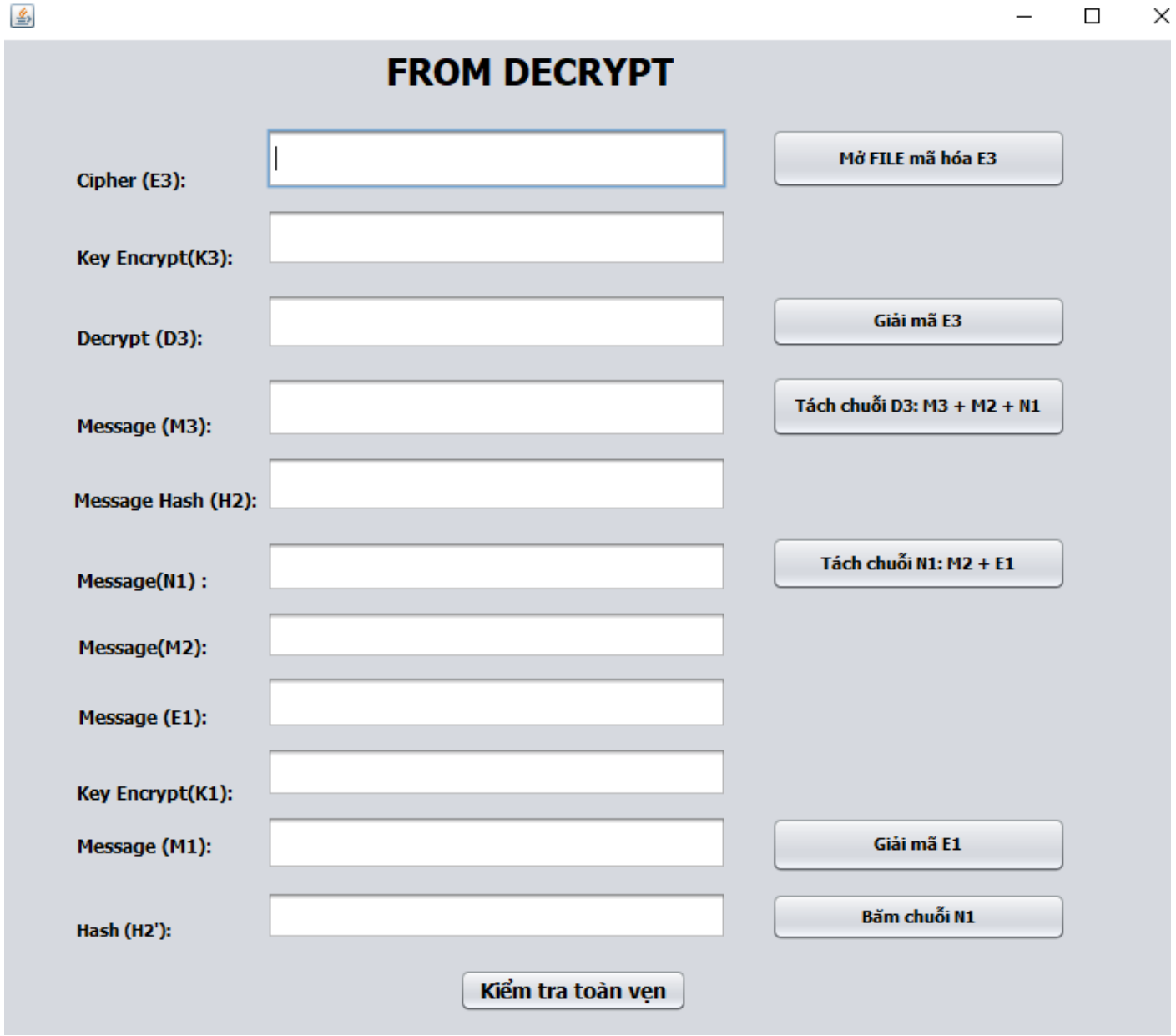
- Số thứ nhất là thuật toán mã hóa E1
- Số thứ hai là hàm băm H2 (nếu số chẵn là thuật toán SHA, số lẽ là thuật toán MD5)
- Số thứ ba là thuật toán mã hóa E3

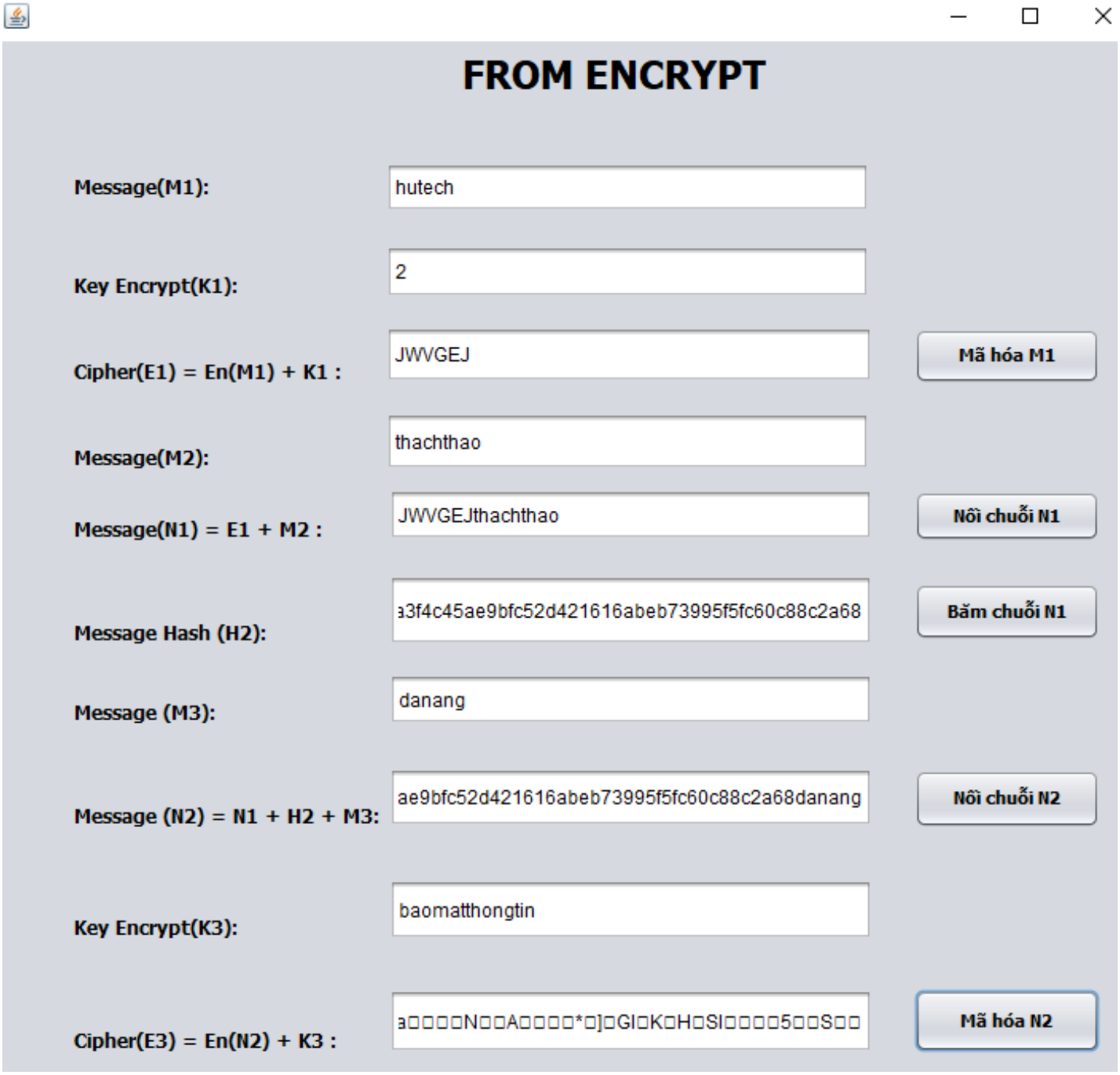
Ví dụ: 3 số cuối của MSSV là **706** , tra trong " **Bảng các thuật toán**" ta có đề thi sau:

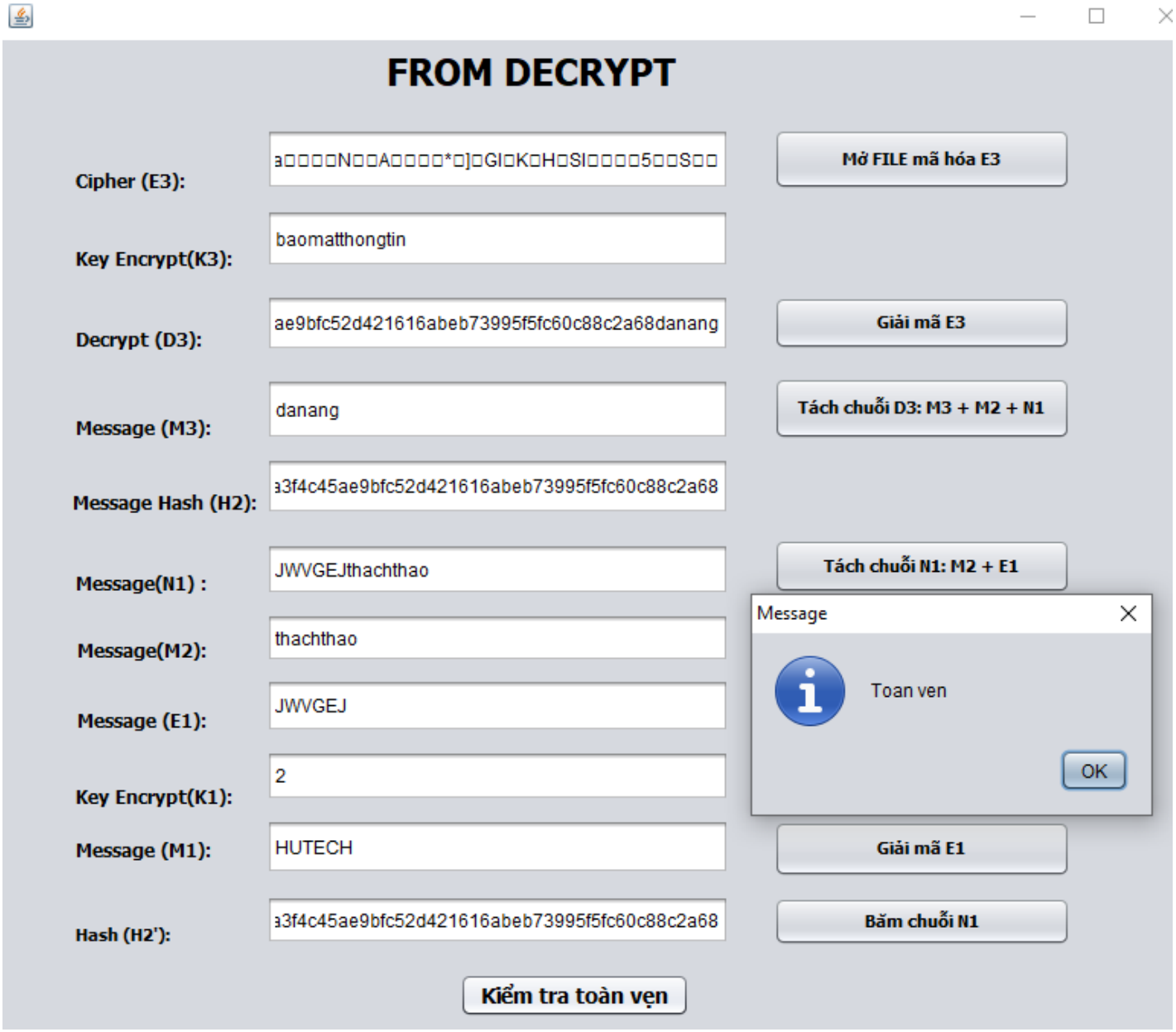
- Số "**7**": Thuật toán mã hóa E1 = Caesar
- Số **"0"**: Hàm băm H2 = SHA
- Số **"6"**: Thuật toán mã hóa E3 = DES

GỢI Ý

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


FROM DECRYPT
Cipher (E3):
Mở FILE mã hóa E3
Key Encrypt(K3):
Decrypt (D3):
Giải mã E3
Message (M3):
Tách chuỗi D3: M3 + M2 + N1
Message Hash (H2):
Message(N1) :
Tách chuỗi N1: M2 + E1
Message(M2):
Message (E1):
Key Encrypt(K1):
Message (M1):
Giải mã E1
Hash (H2'):
Băm chuỗi N1
Kiểm tra toàn vẹn


FROM ENCRYPT
Message(M1):
hutech
Key Encrypt(K1):
2
Cipher(E1) = En(M1) + K1 :
JWVGEJ
Mã hóa M1
Message(M2):
thachthao
Message(N1) = E1 + M2 :
JWVGEJthachthao
Nối chuỗi N1
Message Hash (H2):
a3f4c45ae9bfc52d421616abeb73995f5fc60c88c2a68
Băm chuỗi N1
Message (M3):
danang
Message (N2) = N1 + H2 + M3:
ae9bfc52d421616abeb73995f5fc60c88c2a68danang
Nối chuỗi N2
Key Encrypt(K3):
baomatthongtin
Cipher(E3) = En(N2) + K3 :
a□□□□N□□A□□□□*□]□GI□K□H□SI□□□□5□□S□□
Mã hóa N2


FROM DECRYPT
Cipher (E3):
a□□□□N□□A□□□□*□]□GI□K□H□SI□□□□5□□S□□
Mở FILE mã hóa E3
Key Encrypt(K3):
baomatthongtin
Decrypt (D3):
ae9bfc52d421616abeb73995f5fc60c88c2a68danang
Giải mã E3
Message (M3):
danang
Tách chuỗi D3: M3 + M2 + N1
Message Hash (H2):
a3f4c45ae9bfc52d421616abeb73995f5fc60c88c2a68
Message(N1) :
JWVGEJthachthao
Tách chuỗi N1: M2 + E1
Message(M2):
thachthao
Message
Toan ven
OK
Message (E1):
JWVGEJ
Key Encrypt(K1):
2
Message (M1):
HUTECH
Giải mã E1
Hash (H2'):
a3f4c45ae9bfc52d421616abeb73995f5fc60c88c2a68
Băm chuỗi N1
Kiểm tra toàn vẹn

..... Hết.....