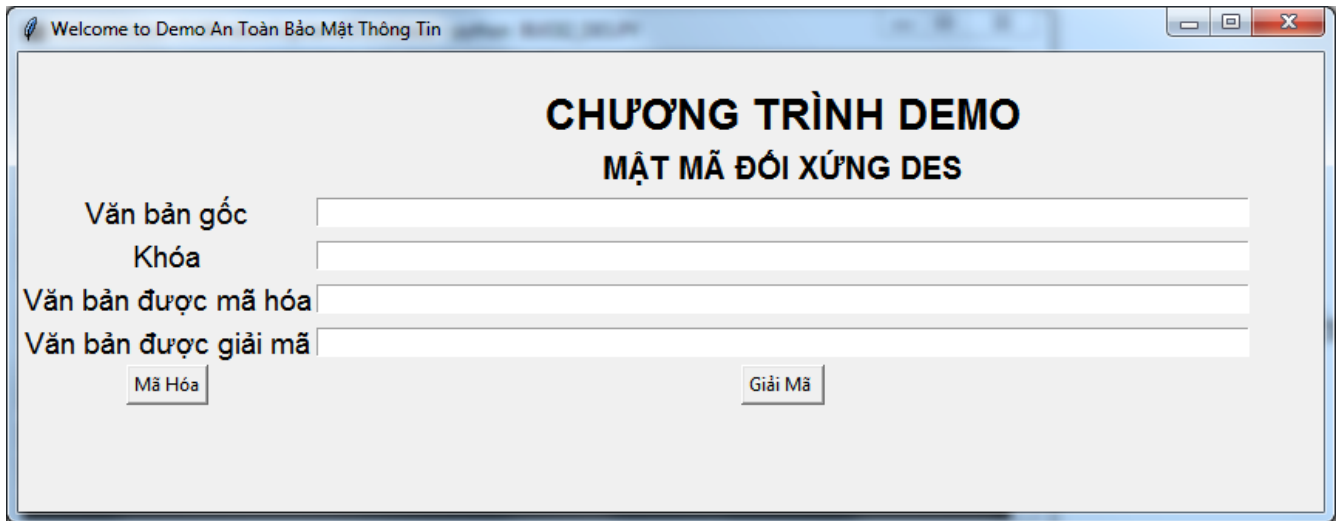


Hướng dẫn thực hành

1. Bài 1.

Bước 1. Hãy tạo giao diện như sau (học viên có thể sử dụng thư viện tkinter, Qt, Flask, ...)



Welcome to Demo An Toàn Bảo Mật Thông Tin

CHƯƠNG TRÌNH DEMO
MẬT MÃ ĐỐI XỨNG DES

Văn bản gốc

Khóa

Văn bản được mã hóa

Văn bản được giải mã

(Gợi ý; xem lại bài thực hành buổi 1)

Bước 2. Cài đặt sự kiện nhấn chuột cho nút Mã Hóa

Gợi ý:

```

from Crypto.Cipher import DES
import base64

def pad(s):
    #Them vao cuoi so con thieu cho du boi cua 8
    return s + (8 - len(s) % 8) * chr(8 - len(s) % 8)

def unpad(s):
    return s[:-ord(s[len(s)-1:])]

def mahoai_DES():
    txt = pad(plaintext.get()).encode("utf8")
    key = pad(keytxt.get()).encode("utf8")
    cipher = DES.new(key, DES.MODE_ECB)
    entxt = cipher.encrypt(txt)
    entxt = base64.b64encode(entxt)
    ciphertxt.delete(0,END)
    ciphertxt.insert(INSERT,entxt)

```

Ghi chú:

- Cần cài đặt thư viện pycryptodome (<https://pypi.org/project/pycryptodome/>) nếu sử dụng Python3.
- Hoặc thư viện pycrypto (<https://pypi.org/project/pycrypto/>) nếu sử dụng Python2. Trước đó cần cài Microsoft Visual C++ Compiler for Python 2.7 (<https://www.microsoft.com/en-gb/download/details.aspx?id=44266>)

Bước 3. Cài đặt sự kiện nhấn chuột cho nút Giải Mã

Gợi ý:

```

def giaima_DES():
    txt = ciphertxt.get()
    txt = base64.b64decode(txt)
    key = pad(keytxt.get()).encode("utf8")
    cipher = DES.new(key, DES.MODE_ECB)
    detxt = unpad(cipher.decrypt(txt))
    denctxt.delete(0, END)
    denctxt.insert(INSERT, detxt)

```

2. Bài 2.

Học viên viết 1 chương trình cho phép mã hóa và giải mã 1 tập tin txt. Học viên nộp bài (tập tin Python) trên hệ thống elcit. Buổi thực hành này được điểm danh bằng các bài nộp trên hệ thống elcit.

3. Bài 3.

Giả sử chúng ta nhận được các văn bản như sau.

	Văn bản gốc	Văn bản được mã hóa
1	The treasure is under the coconut tree	lIZg7tB/NvuG4MXsCDFUsRjvQrjw/UuUGzZw+QMMDF4nGjQCGzY0Uw==
2		LsmDvf9t1pLPn+NZ99+cVx+V1RO12/9KNqk9PLTe5uRii/aNc/X3tw==
3		5cdbWs00vXghkBLECplG8CINQ2Da5R/9KZ0bAKRs+bPvhwOwIt7Sh2ZZFtxHBAK9

Hãy tìm cách giải mã văn bản thứ hai và ba biết rằng tất cả các văn bản được mã hóa bằng giải thuật DES và sử dụng tên một quốc gia làm khóa (tất cả các văn bản đều được mã hóa cùng một khóa). Học viên nộp bài (tập tin Python) trên hệ thống elcit. Buổi thực hành này được điểm danh bằng các bài nộp trên hệ thống elcit (phải đủ tất cả các bài thực hành).

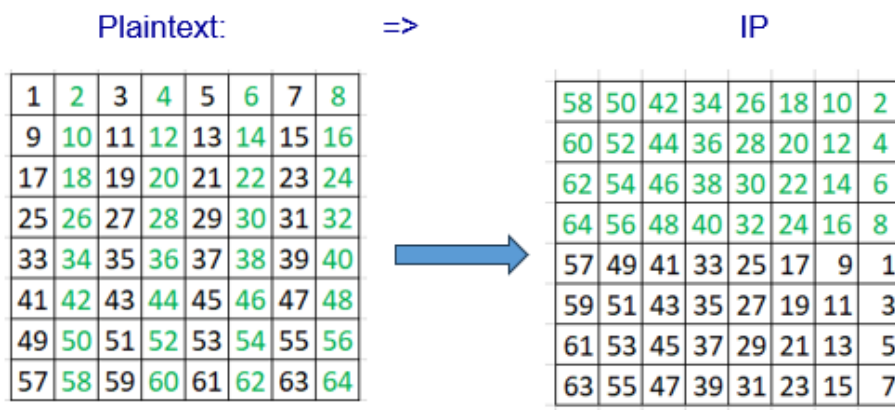
Danh sách các quốc gia:

<https://github.com/umpirsky/country-list/blob/master/data/en/country.csv>

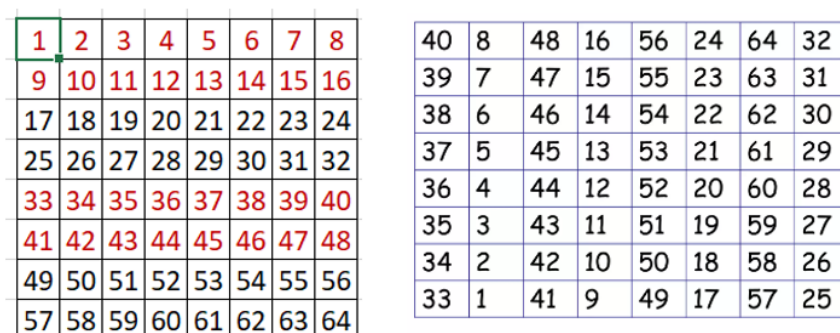
4. Bài 4. Không sử dụng thư viện mã hóa DES. Hãy viết chương trình mã hóa, và giải mã theo các bước của giải thuật: (Tham khảo quy trình trong slide bài giảng)

Gợi ý:

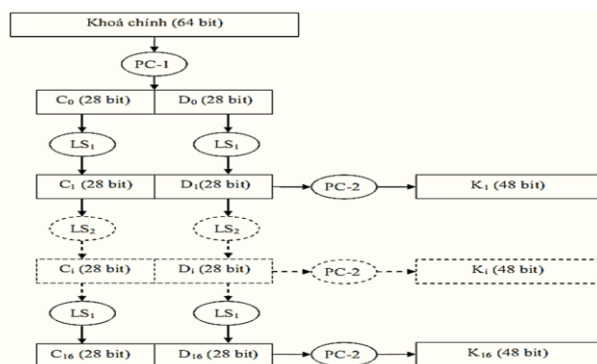
4.1 Viết hàm hoán vị đầu và cuối trong mật mã DES: **Encrypt_IP ()**



- và hàm **Decrypt_IP()**



4.2 Viết chương trình sinh khóa: **Generation_Key(key)** cho 16 vòng trong DES



- Sơ đồ gợi ý:

4.3 Viết các hàm trong mỗi 16 vòng