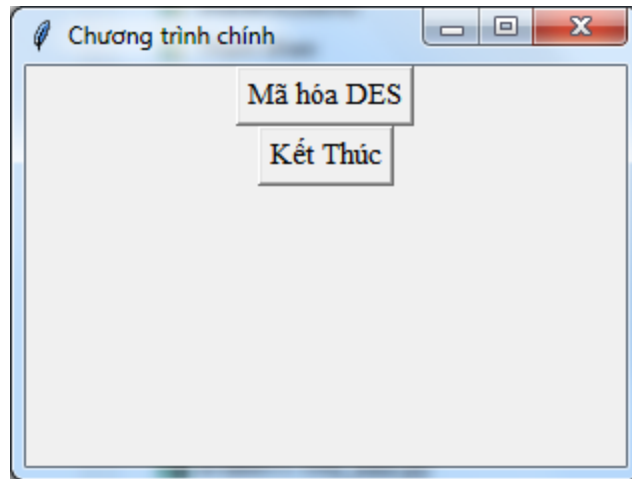


BUỔI 5: ÔN TẬP

Bước 1. Hãy tạo chương trình có giao diện đồ họa như hình 1. Khi nhấn vào nút "Mã hóa DES", phần mềm sẽ hiển thị chương trình mã hóa DES như hình 2. Khi nhấn vào nút "Kết thúc", phần mềm sẽ thoát.



Hình 1 - Giao diện chương trình chính

Gợi ý code

```
# -*- coding: utf8 -*-
from tkinter import *
import tkinter as tk
from Crypto.Cipher import DES
import base64

class MainWindow(tk.Frame):
    def __init__(self, parent):
        self.parent = parent
        tk.Frame.__init__(self)

        self.mahoa_DES = Button(text="Mã hóa DES",
                                font=("Times New Roman", 11),
                                command=self.des)
        self.mahoa_DES.pack()

        self.thoat = Button(text="Kết Thúc",
                              font=("Times New Roman", 11),
                              command=quit)
        self.thoat.pack()

    def des(self):
        MAHOA_DES(self)

def main():
```

```

window = tk.Tk()
window.title("Chương trình chính")
window.geometry('300x200')
MainWindow(window)
window.mainloop()
main()

```

Bước 2. Cài đặt sự kiện cho nút "Mã hóa DES". Khi nhấn chuột vào nút này, phần mềm sẽ hiển thị chương trình mã hóa DES như hình 2.



Hình 2 - chương trình mã hóa DES

Gợi ý code

```

def pad(s):
    #Thêm vào cuối số còn thiếu cho đủ bội của 8
    return s + (8 - len(s) % 8) * chr(8 - len(s) % 8)
def unpad(s):
    return s[:-ord(s[len(s)-1:])]

class MAHOA_DES(tk.Toplevel):
    def __init__(self, parent):
        self.parent = parent
        Toplevel.__init__(self)
        self.title("Chương trình mã hóa đối xứng")
        self.geometry('800x600')

        self.lbl = Label(self,
                        text="CHƯƠNG TRÌNH DEMO",
                        font=("Arial Bold", 20))

```

```

self.lb1.grid(column=1, row=1)

self.lb2 = Label(self,
    text="MẬT MÃ ĐỔI XỨNG DES",
    font=("Arial Bold", 15))
self.lb2.grid(column=1, row=2)

self.plainlb3 = Label(self,
    text="Văn bản gốc",font=("Arial", 14))
self.plainlb3.grid(column=0, row=4)
self.plaintxt = Entry(self,width=100)
self.plaintxt.grid(column=1, row=4)

self.lb4 = Label(self, text="Khóa",font=("Arial", 14))
self.lb4.grid(column=0, row=5)
self.keytxt = Entry(self,width=100)
self.keytxt.grid(column=1, row=5)

self.lb5 = Label(self,
    text="Văn bản được mã hóa",font=("Arial", 14))
self.lb5.grid(column=0, row=6)
self.ciphertxt = Entry(self,width=100)
self.ciphertxt.grid(column=1, row=6)

self.lb6 = Label(self,
    text="Văn bản được giải mã",font=("Arial", 14))
self.lb6.grid(column=0, row=7)
self.denctxt = Entry(self,width=100)
self.denctxt.grid(column=1, row=7)

self.btn_enc = Button(self, text="Mã Hóa",
    command=self.mahoa_DES)
self.btn_enc.grid(column=1, row=9)
self.btn_dec = Button(self, text="Giải Mã ",
    command=self.giaima_DES)
self.btn_dec.grid(column=1, row=10)
self.thoat = Button(self,text="Quay về màn hình chính",
    command=self.destroy)
self.thoat.grid(column=1, row=11)

def mahoa_DES(self):
    txt = pad(self.plaintxt.get()).encode()
    key = pad(self.keytxt.get()).encode()
    cipher = DES.new(key, DES.MODE_ECB)
    entxt = cipher.encrypt(txt)

```

```

entxt = base64.b64encode(entxt)
self.ciphertxt.delete(0,END)
self.ciphertxt.insert(INSERT,entxt)

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

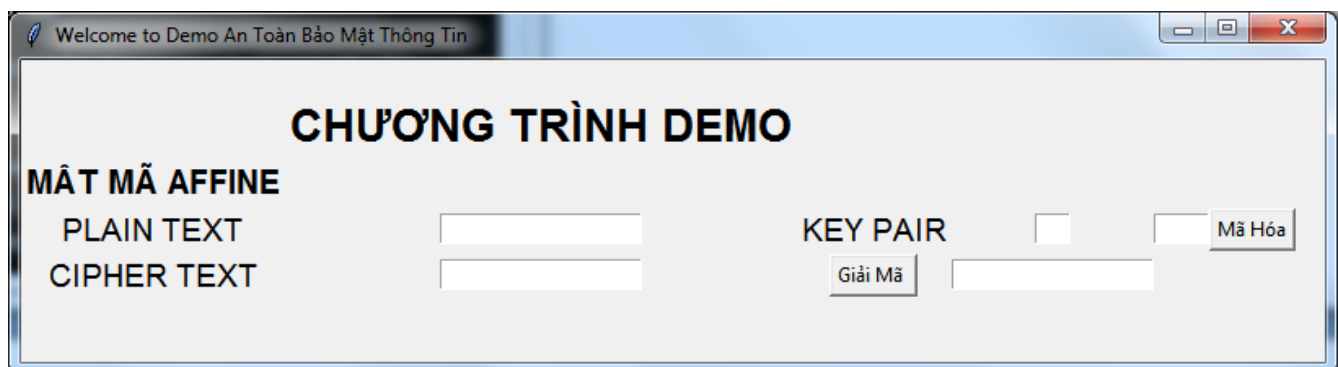
```

Bước 3. Cải tiến giao diện chính như hình 3.



Hình 3 - Giao diện chính sau khi cải tiến

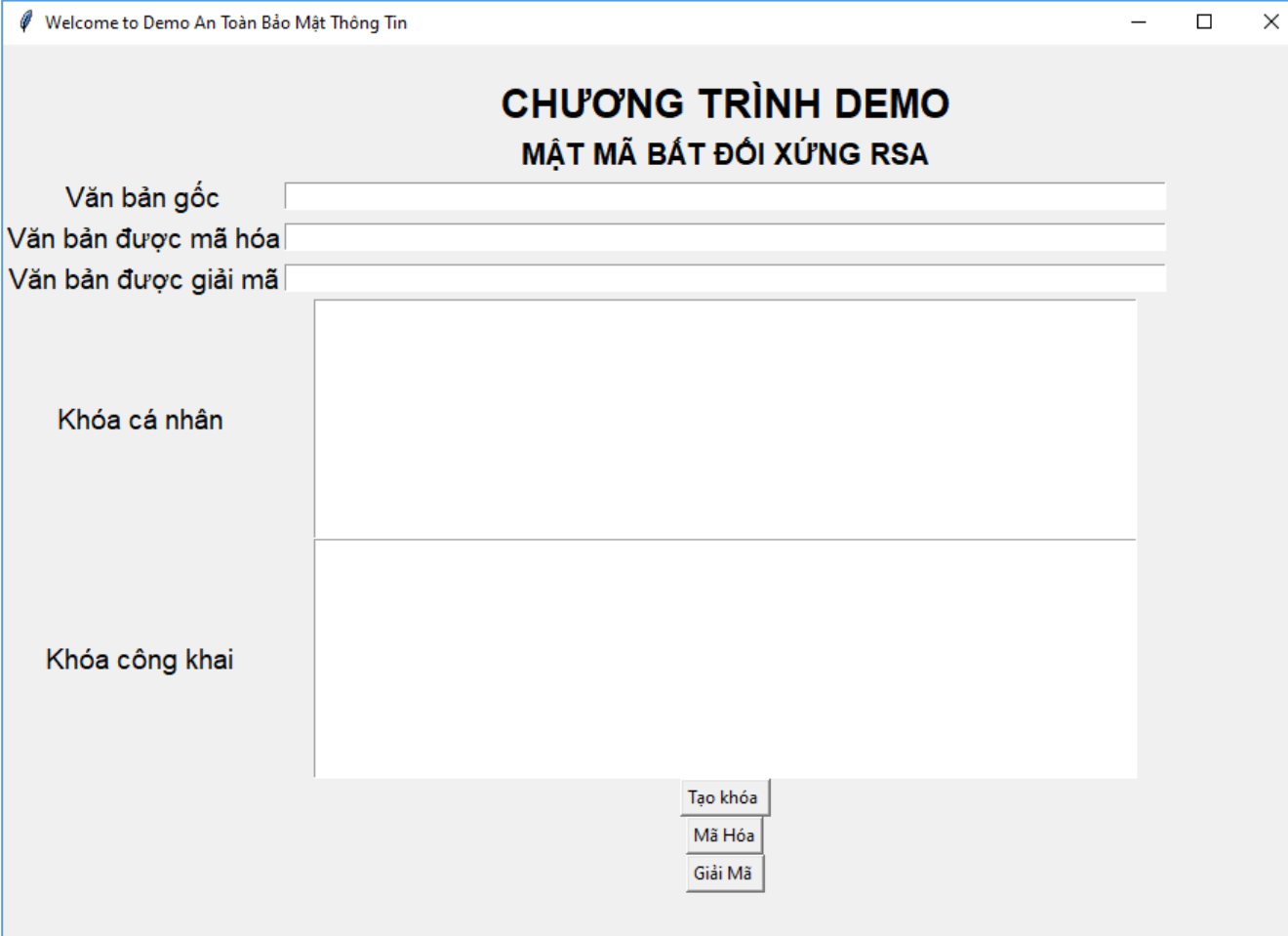
Bước 4. Cài đặt sự kiện cho nút "Mã hóa Affine". Khi nhấn chuột vào nút này, phần mềm sẽ hiển thị chương trình mã hóa Affine như hình 4.



Hình 4 - chương trình mã hóa Affine

Gợi ý code: xem lại bài thực hành 1.

Bước 5. Cài đặt sự kiện cho nút "Mã hóa DES". Khi nhấn chuột vào nút này, phần mềm sẽ hiển thị chương trình mã hóa RSA như hình 5.



Welcome to Demo An Toàn Bảo Mật Thông Tin

CHƯƠNG TRÌNH DEMO MẬT MÃ BẤT ĐỐI XỨNG RSA

Văn bản gốc

Văn bản được mã hóa

Văn bản được giải mã

Khóa cá nhân

Khóa công khai

Tạo khóa

Mã Hóa

Giải Mã

Hình 5 - chương trình mã hóa RSA

Gợi ý code: xem lại bài thực hành 3.

Bước 6. Học viên hoàn thiện bài tập và nộp bài (tập tin Python) trên hệ thống. Cần lưu ý đặt tên tập tin python theo đúng quy định. Ở đầu file python cần ghi rõ các thông tin sau:

```
# Ho va ten sinh vien:  
# Ma so sinh vien:  
# STT:
```