

THỰC HÀNH BUỔI 1

Lập trình Python và mã hóa bằng giải thuật Affine

MỤC TIÊU

Nắm vững kiến thức về AT&BMTT

NỘI DUNG

Phần 0: Cài đặt Python 3

Phần 1: Viết chương trình thực hiện mã hóa

Phần 2: Viết chương trình thực hiện giải mã

Phần 3: Viết chương trình đơn giản với giao diện đồ họa

Phần 4: Tổng hợp

TÀI LIỆU THAM KHẢO:

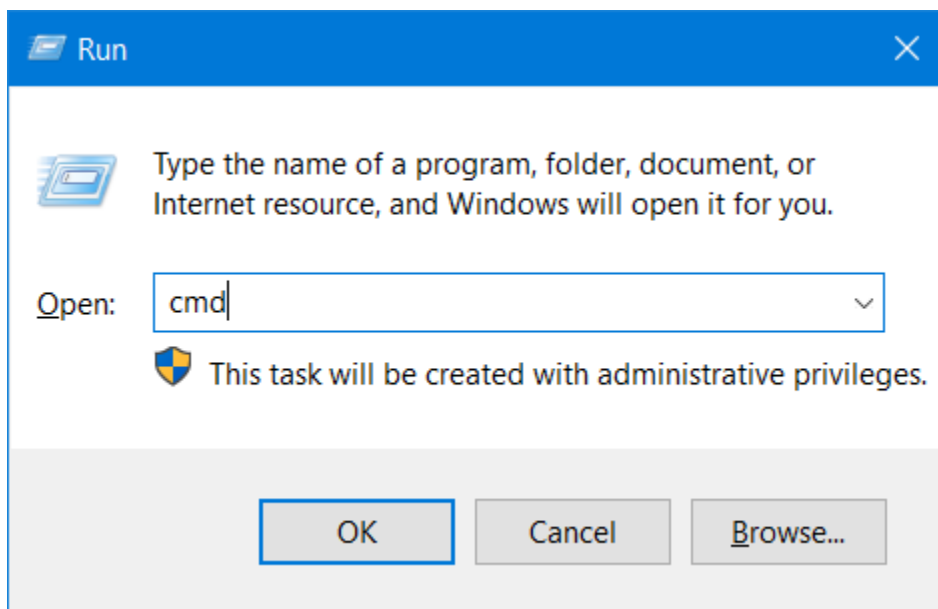
Hướng dẫn lập trình ngôn ngữ python www.cit.ctu.edu.vn/~dtngchi/oss/python.pdf

Phần 1: Viết chương trình thực hiện mã hóa

Bước 1: Tạo thư mục D:\CT204\TH1

Bước 2: Mở cửa sổ **cmd** tại thư mục vừa tạo

- Win-R > gõ **cmd** > ấn enter

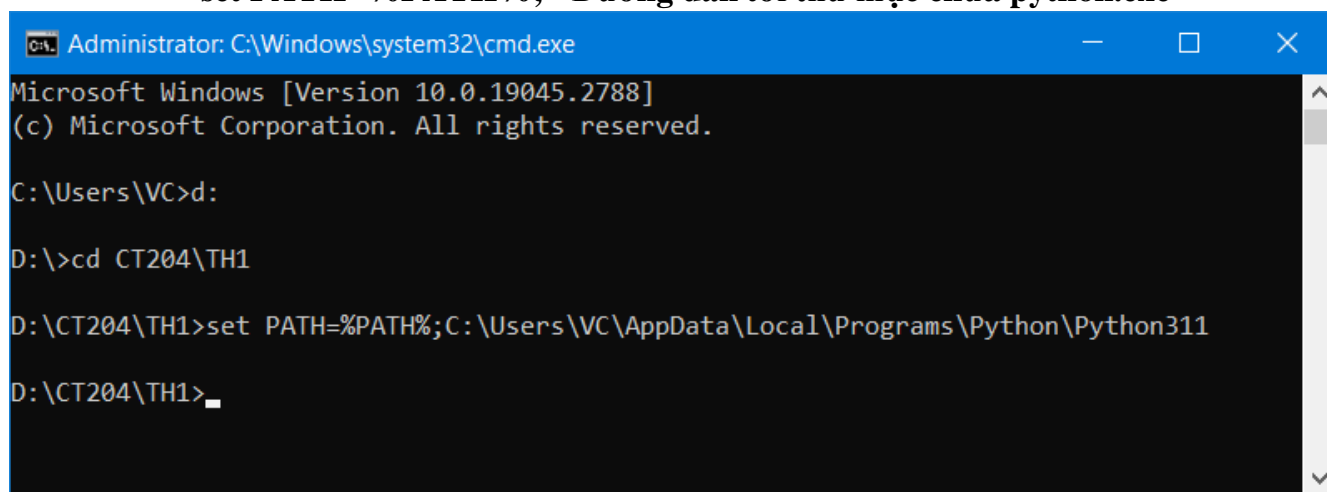


- Lần lượt gõ và chạy các lệnh trong cửa sổ cmd:

D:

cd D:\CT204\TH1

set PATH=%PATH%; "Đường dẫn tới thư mục chứa python.exe"



*Lưu ý: lệnh sau cùng không cần thiết nếu đã có thể chạy lệnh **python** trong cửa sổ **cmd**.*

Bước 3: Tạo và mở file text rỗng TH1-1.py

- Chạy lệnh **notepad TH1-1.py** trong cửa sổ cmd, bấm **yes**

Bước 4: Thêm vào file vừa tạo đoạn code sau và lưu file lại:

```
def Char2Num(c):  
    return ord(c)-65  
  
def Num2Char(n):  
    return chr(n+65)  
  
def encryptAF(txt,a,b,m):  
    r = ""  
    for c in txt:  
        e = (a*Char2Num(c)+b) % m  
        r = r+Num2Char(e)  
    return r  
  
print(encryptAF("HELLO", 3, 5, 26))
```

Bài tập:

1. Sửa lỗi chương trình trên và chạy thử

Phần 2: Viết chương trình thực hiện giải mã

Bước 1: Tạo file TH1-2.py có nội dung của file TH1-1.py và thêm đoạn mã sau để thực hiện giải mã:

```
# Chương trình Euclid Extended để tìm ước số chung lớn nhất của 2 số

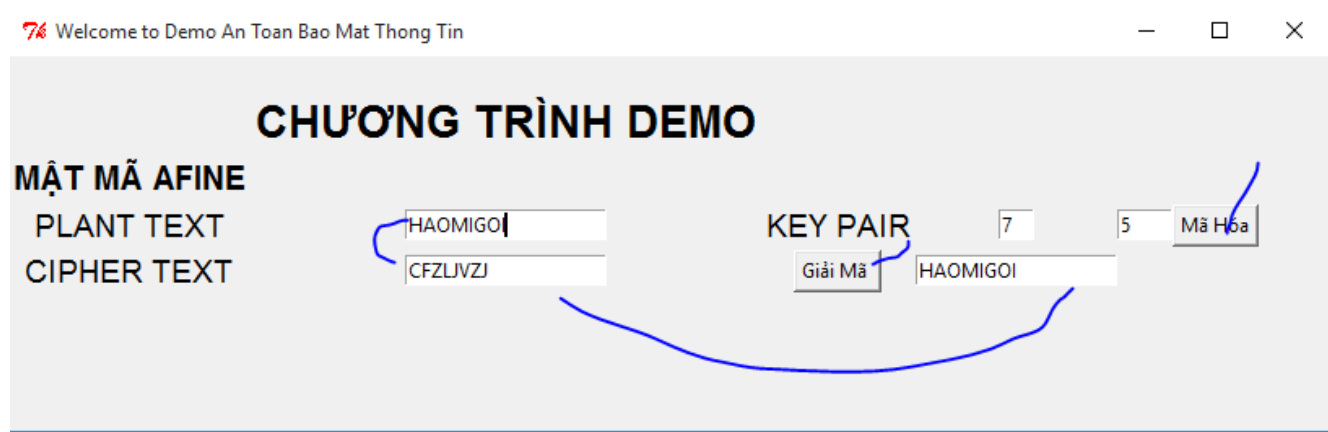
def xgcd(a, m):
    temp = m
    x0, x1, y0, y1 = 1, 0, 0, 1
    while m!=0:
        q, a, m = a // m, m, a % m
        x0, x1 = x1, x0 - q * x1
        y0, y1 = y1, y0 - q * y1
    if x0 < 0: x0 = temp+x0
    return x0

def decryptAF(txt,a,b,m):
    r = ""
    a1 = xgcd(a,m)
    for c in txt:
        e = (a1*(Char2Num(c)-b )) % m
        r = r+Num2Char(e)
    return r
```

Bài tập:

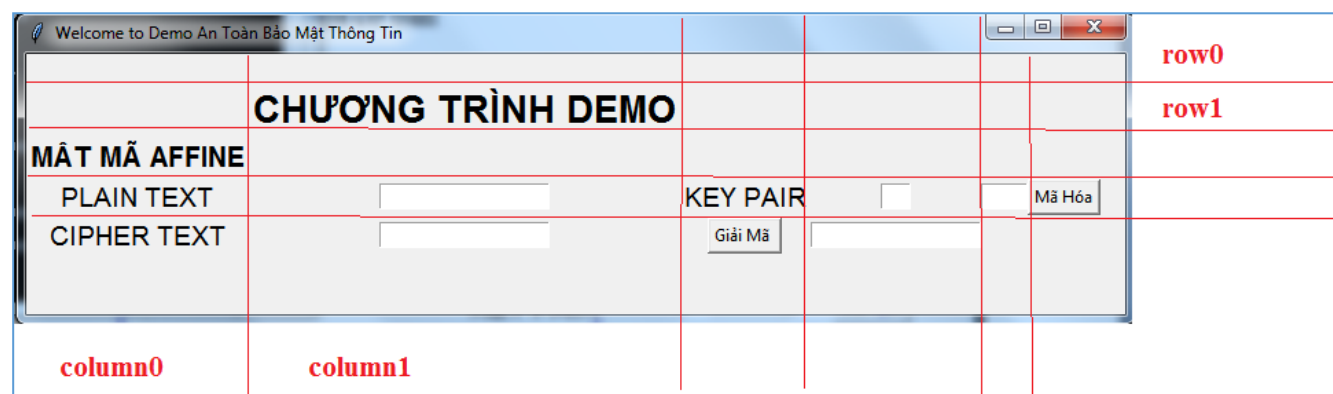
- Viết thêm code để thực hiện giải mã đoạn text bị mã hóa ở phần 1

Phần 3: Viết chương trình đơn giản với giao diện đồ họa



Yêu cầu tạo giao diện đồ họa như trên.

Gợi ý: với thư viện tkinter, chúng ta có thể tạo cửa sổ có thiết kế dạng lưới như sau:



Bước 1: Tạo file TH1-3.py:

```
# -*- coding: utf8 -*-
from tkinter import *

# Khởi tạo màn hình chính
window = Tk()
window.title("Welcome to Demo AT&BMTT")

# Thêm các control
lb0 = Label(window, text=" ", font=("Arial Bold", 10))
lb0.grid(column=0, row=0)
lb1 = Label(window, text="CHƯƠNG TRÌNH DEMO", font=("Arial Bold", 20))
lb1.grid(column=1, row=1)
lb2 = Label(window, text="MẬT MÃ AFFINE", font=("Arial Bold", 15))
lb2.grid(column=0, row=2)
plainlb3 = Label(window, text="PLAIN TEXT", font=("Arial", 14))
plainlb3.grid(column=0, row=3)
plaintxt = Entry(window, width=20)
plaintxt.grid(column=1, row=3)
KEYlb4 = Label(window, text="KEY PAIR", font=("Arial", 14))
```

```

KEYlb4.grid(column=2, row=3)
KEYA1 = Entry(window,width=3)
KEYA1.grid(column=3, row=3)
KEYB1 = Entry(window,width=5)
KEYB1.grid(column=4, row=3)

# Hoc vien bo sung code tai day
# de co duoc giao dien nhu yeu cau
# ...

# Tao nut co ten AFbtn
AFbtn = Button(window, text="Mã Hóa")
AFbtn.grid(column=5, row=3)

# Hoc vien bo sung code de tao nut co ten la DEAFbtn
# ...

# Hien thi cua so
window.geometry('800x600')
window.mainloop()

```

Bước 2 - Cài đặt sự kiện Click cho nút Mã Hóa

i. Thêm sự kiện mã hóa cho nút

```

AFbtn = Button(window, text="Mã hóa", command=mahoa)
AFbtn.grid(column=5, row=3)

```

ii. và cài đặt các hàm cần thiết

```

def Char2Num(c):
    return ord(c)-65

def Num2Char(n):
    return chr(n+65)

def encryptAF(txt,a,b,m):
    r = ""
    for c in txt:
        e = (a*Char2Num(c)+b) % m
        r = r+Num2Char(e)
    return r

def mahoa():
    a = int(KEYA1.get())
    b = int(KEYB1.get())
    m = 26
    entxt = encryptAF(plaintext.get(),a,b,m)
    ciphertxt3.delete(0,END)
    ciphertxt3.insert(INSERT,entxt)

```

```

def xgcd(a, m):
    temp = m
    x0, x1, y0, y1 = 1, 0, 0, 1
    while m!=0:
        q, a, m = a // m, m, a % m
        x0, x1 = x1, x0 - q * x1
        y0, y1 = y1, y0 - q * y1
    if x0 < 0: x0 = temp+x0
    return x0

def decryptAF(txt,a,b,m):
    r = ""
    a1 = xgcd(a,m)
    for c in txt:
        e = (a1*(Char2Num(c)-b )) % m
        r = r+Num2Char(e)
    return r

```

Cách kiểm tra: chuỗi đầu vào là "HAOMIGOI" và a=7, b=5. Kết quả nhận được sau khi mã hóa là "CFZLJVZJ". Sinh viên tự kiểm tra việc giải mã

Bài tập:

3. Nâng cấp phần mềm bên trên để có thể mã hóa thông điệp có dấu cách và phân biệt chữ hoa với chữ thường. Ví dụ: “Chúc bạn lam bai TOT”
4. Giả sử chúng ta nhận được một thông điệp đã bị mã hóa như sau

"LOLYLTQOLTHDZTDC"

và biết rằng thông điệp đó được mã hóa bằng thuật toán Affine và có chứa từ “LAMUOI”. Bạn hãy viết 1 chương trình Python (không cần giao diện đồ họa) để tìm ra thông điệp gốc.

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 các file Python cần ghi rõ các thông tin sau:

```

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

```