**Danh sách bài tập thực hành   
Thuật toán trong An toàn thông tin 2021**

Bài 1. Biểu diễn số A thành một ma trận (sẽ giới hạn kích thước số A không quá lớn)

Ví dụ:

* *P=21****47483647****; W=8; Số nguyên a=38762497*

KQ: A= [2 79 120 1]

* *P=2147483647; W=8; Số nguyên a=568424364*

KQ: A= [33 225 119 172]

Bài 2. Cài đặt chương trình tính tổng của hai số lớn trong hai trường hợp:

* Mỗi số đã được cho dưới dạng một mảng biểu diễn.
* Mỗi số chưa được biểu diễn thành mảng

Ví dụ:

*P=2147483647; W=8; a=38762497; b= 568424364*

A= [2 79 120 1]

B= [33 225 119 172]

*P=2147483647; W=8*

*KQ A+B* =(0, [36 48 239 173])

**Bài 3. Cài đặt chương trình tính hiệu của hai số lớn trong hai trường hợp:**

**- Mỗi số đã được cho dưới dạng một mảng biểu diễn**

**- Mỗi số chưa được biểu diễn thành mảng**

**Ví dụ:**

*P=2147483647; W=8; a=38762497; b= 568424364*

A= [2 79 120 1]

B= [33 225 119 172]

KQ: c=a-b=(1, [224 110 0 85])

**Bài 4. Cài đặt chương trình phép cộng trên Fp**

**Ví dụ:** *P=2147483647; W=8; a=2147483646; b= 2147483643*

A=[127 255 255 254]

B=[127 255 255 251]

KQ: [127 255 255 250]

**Bài 5. Cài đặt chương trình tính phép trừ trên Fp**

*Ví dụ: p=2147483647; W=8; a=38762497; b= 568424364*

KQ:[ 96 110 0 84]

**Bài 6. Cài đặt chương trình tính phép nhân**

*Ví dụ: p=2147483647; W=8; a=524647; b= 32549*

A=[0 8 1 103]

B=[0 0 127 37]

c=a.b=[0 0 0 3 249 218 76 227]

**Bài 7. Cài đặt chương trình tính ước chung lớn nhất của 2 so a và b**

*Ví dụ: a= 28150488 b= 10507620* =>gcd(a,b)=12

*a= b= 345632* => gcd(a,b)=1

**Bài 8.** Cài đặt chương trình **tính nghịch đảo trên Fp dùng Euclide mở rộng**

*Ví dụ: p= 489573857; a= 45682375* => a^-1 mod p = 242160691

**Bài 9. Viết chương trình tìm tất cả các số nguyên tố <=n với n nhập vào từ bàn phím**

**Ví dụ: n=30 à [2,3,5,7,11,13,17,19,23,29]**

**Bài 10. Viết chương trình tìm một thừa số không tầm thường của một số n nhập từ bàn phím:**

**Ví dụ: *n=*43567127 à *KQ: d=7181***

**Bài 11. Viết chương trình tìm phân tích nguyên tố của một số nhập vào từ bàn phím:**

**Ví dụ:** *n=20* **à** coso=[2,5], somu=[2,1]

*n=12*  à coso=[2,3], somu=[2,1]

**Bài 12. Viết chương trình kiểm tra tính nguyên tố của một số n nhập vào từ bàn phím**

**Ví dụ: 17 à Nguyên tố**

**19 à Nguyên tố**

**21 à Hợp số**

**Bài 13.** *Viết chương trình kểm tra một số n nhập từbàn phím có phải là một số* camichael hay không?

Ví dụ: n=561 à số camichael

N=22 à Không phải camichael

**Bài 14.** Viết chương trình liệt kê tất cả các số camichael nhỏ hơn hoặc bằng n nhập từ bàn phím

**Bài 15.** Viết chương trình kiểm tra số nguyên tố với xác suất nằm trong khoảng cho trước.

**Bài 16.** Cài đặt thuật toán tìm kiếm mẫu P trong đoạn văn bản T kết quả trả về vị trí xuất hiện của mẫu P và số lần lặp tính toán, số phép tính theo Boyer Moore với P và T nhập vào từ bàn phím

**Bài 17.** Cài đặt thuật toán tìm kiếm mẫu P trong đoạn văn bản T kết quả trả về vị trí xuất hiện của mẫu P và số lần lặp tính toán, số phép tính theo Knuth-Moris-Pratt với P và T nhập vào từ bàn phím

**Bài 18.** Cài đặt thuật toán tìm kiếm mẫu P trong đoạn văn bản T kết quả trả về vị trí xuất hiện của mẫu P và số lần lặp tính toán, số phép tính theo thuật toán vét cạn Với P và T nhập vào từ bàn phím