ESCUELA SUPERIOR DE CÓMPUTO

INSTITUTO POLITÉCNICO NACIONAL

CABALLERO HUESCA CARLOS EDUARDO

MARTÍNEZ GARCÍA BRANDO JOSUÉ

Reporte

Laboratorio #2

Algoritmo de Euclides Extendido

CRYPTOGRAPHY

3CV1

Díaz Santiago Sandra

Teoría

Algoritmo extendido de Euclides.

Si $\boldsymbol{mcd(a,b)=d}$, con $a>b$ entonces existen enteros u y v tales que $\boldsymbol{d=u*a+v*b}$ es decir, el mcd de dos números se puede expresar como la combinación lineal de esos dos números con coeficientes enteros.

El Algoritmo de Euclides Extendido permite determinar los valores de u y v de la igualdad anterior y es una aplicación directa del Algoritmo de Euclides sólo hay que ir despejando de la última división obtenida hasta llegar a la primera.

El algoritmo también permite calcular el inverso de un número.

Ejemplo:

$\mathrm{mcd}(141,96)$

$141=96*1+45$

$96=45*2+6$

$45=6*7+3$

$6=3*2+0$

Ahora vamos a calcular u y v

$141=141*1+96*0$

$96=141*0+96*1$

$45=141-96=(141*1+96*0)-(141*0+96*1)=141(1)+96(-1)$

$6=96-45*2=(141*0+96*1)-\big(141*1+96(-1)\big)*2=141(-2)+96(3)$

$3=45-6*7=\big(141*1+96(-1)\big)-\big(141(-2)+96(3)\big)*7=141(\mathbf{15})+96(-\mathbf{22})$

$u=15 \qquad v=-22$

Ataque a texto plano conocido (cifrado Hill)

Supongamos que Oscar sabe que se trata de un Hill **m=2** posee **Friday**->**PQCFKU**

Entonces, de las tres parejas tipo (fr)->(PQ) sabrá que:
ek(5,17)=(15,16)
ek(8,3)=(2,5)
ek(0,24)=(10,20)

Se plantea y resuelve un sistema lineal y se obtiene la matriz K usada como clave.

Ejercicios de Programación.

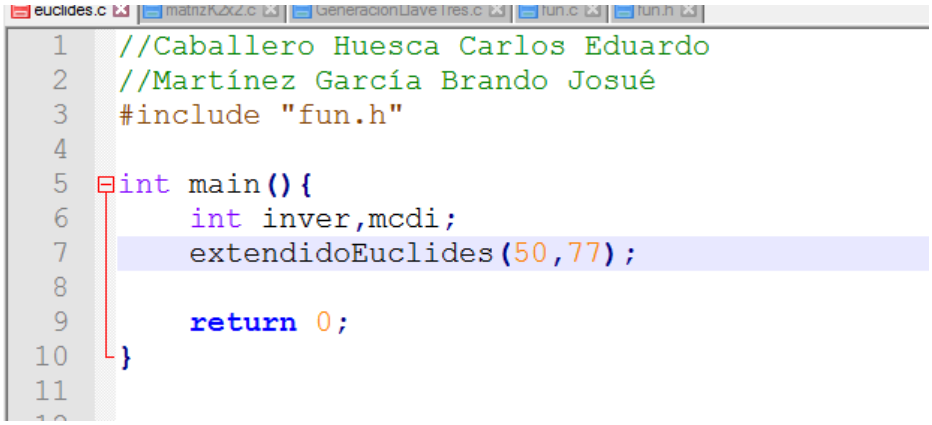
Diseña una función que implemente el algoritmo de Euclides extendido

Modifica el algoritmo anterior para que retorne solo el inverso multiplicativo.

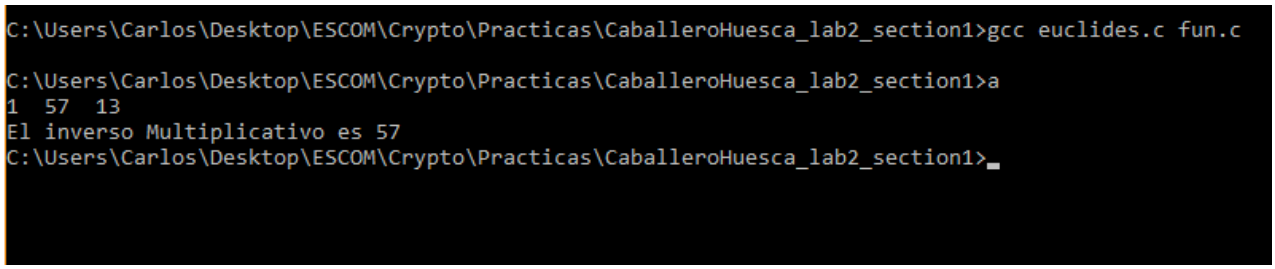
```
void extendidoEuclides(int a, int b){

    int
tieneinversa,inversoMultiplicativo,mod;
    int q=0,r=0,i;
    int x1=0,x2=1,y1=1,y2=0;
    int x=0, y=0, d=0;
    int resultado[3]={20,15,1};
                //d,x,y
    mod=b;
    tieneinversa = mcd(a,b);

    if(tieneinversa==1){


    if(b!=0){

        while(b>0){

            q=a/b;
            r=a-(q*b);
            x=x2-(q*x1);
            y=y2-(q*y1);

            a=b;
            b=r;
            x2=x1;
            x1=x;
            y2=y1;
            y1=y;

        }

        resultado[0]=a;
        resultado[1]=x2;
        resultado[2]=y2;
```

```
    else{
        resultado[0]=a; //1
        resultado[1]=1; //20
        resultado[2]=0; //13
    }


    while(resultado[1]<0){

resultado[1]=resultado[1]+mod;
        }

    for(i=0;i<3;i++){
        printf("%d
",resultado[i]);
    }

    printf("\nEl inverso
Multiplicativo es
%d",resultado[1]);


    }
    else{
    printf("no  tiene inversa");
    }
}
```

Pruebas



```c
//Caballero Huesca Carlos Eduardo
//Martínez García Brando Josué
#include "fun.h"

int main(){
    int inver,mcdi;
    extendidoEuclides(50,77);

    return 0;
}
```



```
C:\Users\Carlos\Desktop\ESCOM\Crypto\Practicas\CaballeroHuesca_lab2_section1>gcc euclides.c fun.c

C:\Users\Carlos\Desktop\ESCOM\Crypto\Practicas\CaballeroHuesca_lab2_section1>a
1  57  13
El inverso Multiplicativo es 57
C:\Users\Carlos\Desktop\ESCOM\Crypto\Practicas\CaballeroHuesca_lab2_section1>
```

Bibliografía

Rodríguez, Francisco. Aritmética Computacional. 1st ed. Ciudad de México: N.p., 2016. Web. 04 Sep. 2016.