Ortega Silva Jorge Eduardo

Como ejecutarlo

Cuando se ejecuta el programa primero se mostrará la operación del inverso multiplicativo, las instrucciones las especifique en el programa, esta parte, pedirá un número para encontrar Z_n^*, después de este ejercicio finalizará pidiéndote un número para encontrar una llave válida para el algoritmo Affine cipher K(a,b), así como el inverso multiplicativo de a.

Descripción de las funciones

```
void affine(int n, int *serie){
    int cpm[50]={0}; //serie con numeros coprimos
    int ale1, ale2, ncpm;
    srand(time(0));
    ncpm=coprimos(n,cpm);
    ale1=rand()%(ncpm);//aleatorio de los coprimos
    ale2=rand()%n;// aleatorio entre 0 y n
    serie[0]=cpm[ale1];
    serie[1]=ale2;
    serie[2]=xgcd(serie[0],n);

}
```

Hace uso de las funciones generadas en el punto 1 y 2, para encontrar los números coprimos, para después con un número pseudoaleatorio seleccionar alguno de ellos y que este sea a, y después generar otro numero pseudoaleatorio entre el rango de n y que este sea b, por último, se busca el inverso multiplicativo del numero a y todo se manda en el arreglo de enteros que se proporcionó.

Ortega Silva Jorge Eduardo

```
int coprimos(int n, int *serie){
    int x=0, u=0, v=0;//Variables de respaldo
    int r=0, i=0, j=0;
    //para econtrar el gcd
    for(i=1, j=0; i<n; i++){
        u=i;
        v=n;
        while (v!=0) {
            x=v;
            r=u%v;
            v=r;
            u=x;
            //u es el gcd
        }
        if(u==1){
            serie[j]=i;
            j++;
        }
    }
    return j;// total de coprimos
}
```

Se crean variables auxiliares, para después con un for pasar por todos los números a partir de 0 menores a n, a estos números se les encuentra su máximo común divisor con n, con el método del algoritmo euclidiano, expresado dentro del ciclo while, este se detendrá cuando el residuo sea 0, así encontrando el mcd, si su resultado es uno se guarda en el arreglo que se proporcionó; se retorna el número de coprimos encontrados.

Ortega Silva Jorge Eduardo

```
int xgcd(int a, int n){
    int u=a, v=n;
    int q=0, x=0, x1=1, x2=0, r=0;
    int resultado;
    while(u!=1){
        q=v/u;
        r=v-(q*u);
        x=x2-(q*x1);
        v=u;
        u=r;
        x2=x1;
        x1=x;
    }
    if(x1>=0)
        return resultado=x1%n;
    else
        return resultado=n+x1;

}
```

Se hace uso del algoritmo euclidiano extendido, esto esta expresado dentro del ciclo while, este ciclo se repite hasta que el residuo sea uno, este bloque de código encuentra el número que al calcular su modulo nos da el inverso multiplicativo buscado

Ortega Silva Jorge Eduardo

Ejecuciones

```
----Inverso multiplicativo----
Se encontrara a^-1 mod n
Recuerde que 'a' tiene que ser menor a 'n' y coprimo de 'n'

Y que 'n' tiene que ser mayor a 0

Ingrese el valor de a: 5

Ingrese el valor de n: 13

5^-1 mod 13 = 8



----Numeros coprimos----
Recuerde que 'n' deber ser mayor a 1
Ingresa la n a la que se le encontrara su conjunto de numeros coprimos: 20


Z*n={ 1  3  7  9  11  13  17  19  }



----Affine cipher y a^-1 mod n----
Se encontrara una llave valida para Affine cipher (k=(a,b))
Ademas se entrara a^-1 mod n
Recuerde que 'n' deber ser mayor a 1
Ingrese el valor de n: 33

K=(2, 12)

2^-1 mod 33 = 17
```

Ortega Silva Jorge Eduardo

```
----Inverso multiplicativo----
Se encontrara a^-1 mod n
Recuerde que 'a' tiene que ser menor a 'n' y coprimo de 'n'

Y que 'n' tiene que ser mayor a 0

Ingrese el valor de a: 5

Ingrese el valor de n: 7

5^-1 mod 7 = 3



----Numeros coprimos----
Recuerde que 'n' deber ser mayor a 1
Ingresa la n a la que se le encontrara su conjunto de numeros coprimos: 7


Z*n={ 1  2  3  4  5  6  }



----Affine cipher y a^-1 mod n----
Se encontrara una llave valida para Affine cipher (k=(a,b))
Ademas se entrara a^-1 mod n
Recuerde que 'n' deber ser mayor a 1
Ingrese el valor de n: 16

K=(13, 4)

13^-1 mod 16 = 5
```

Ortega Silva Jorge Eduardo

```
----Inverso multiplicativo----
Se encontrara a^-1 mod n
Recuerde que 'a' tiene que ser menor a 'n' y coprimo de 'n'

Y que 'n' tiene que ser mayor a 0

Ingrese el valor de a: 7

Ingrese el valor de n: 26

7^-1 mod 26 = 15



----Numeros coprimos----
Recuerde que 'n' deber ser mayor a 1
Ingresa la n a la que se le encontrara su conjunto de numeros coprimos: 22


Z*n={ 1  3  5  7  9  13  15  17  19  21  }



----Affine cipher y a^-1 mod n----
Se encontrara una llave valida para Affine cipher (k=(a,b))
Ademas se entrara a^-1 mod n
Recuerde que 'n' deber ser mayor a 1
Ingrese el valor de n: 47

K=(43, 14)

43^-1 mod 47 = 35
```