Шифрование гаммированием

Лабораторная работа №4

Шутенко Виктория

17 сентября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Шутенко Виктория михайловна
- студентка Магистратуры
- группы НФИмд-02-23
- Российский университет дружбы народов

Задание лабораторной работы

Задание лабораторной работы

1. Реализовать алгоритм Евклида.
2. Реализовать бинарный алгоритм Евклида.
3. Реализовать расширенный алгоритма Евклида.
4. Реализовать расширенный бинарный алгоритма Евклида.

Реализация алгоритма Евклида

[21]:
```
def euclid(a,b):
    while a!=0 and b!=0:
        if a>b:
            a%=b
        else:
            b%=a
    return a or b
```

[22]:
```
euclid(12345,54321)
```

[22]:
```
3
```

Реализация бинарного алгоритма Евклида

Реализация бинарного алгоритма Евклида

[26]:
```
def bin_euclid(a,b):
    if a==b:
        return a
    g=0
    while (a|b)&1==0:
        g+=1
        a>>=1
        b>>=1
    while a&1==0:
        a>>=1
    while b!=0:
        while b&1==0:
            b>>=1
        if a>b:
            a,b=b,a
        b-=a
    return a<<g
```

[27]:
```
bin_euclid(12345,54321)
```

[27]: 3

Реализация расширенного алгоритма Евклида

[31]:
```
def ext_euclid(a,b):
    if a==0:
        y=0
        x=1
        return b,y,x
    else:
        d,x,y=ext_euclid(b%a,a)
    return d,y-(b//a)*x,x
```

[32]:
```
ext_euclid(12345,54321)
```

[32]:
```
(3, 3617, -822)
```

Реализация расширенного бинарного алгоритма Евклида

Реализация расширенного бинарного алгоритма Евклида

[33]:
```
def ext_bin_euclid(a,b):
    g=1
    while(a%2==0) and (b%2==0):
        a/=2
        b/=2
        g*=2
    u=a
    v=b
    A=1
    B=0
    C=0
    D=1
    while u!=0:
        while u%2==0:
            u/=2
            if (A%2==0) and (B%2==0):
                A/=2
                B/=2
            else:
                A=(A+b)/2
                B=(B-a)/2
        while v%2==0:
            v/=2
            if (C%2==0) and (D%2==0):
                C/=2
                D/=2
            else:
                C=(C+b)/2
                D=(D-a)/2
        if u>=v:
            u-=v
            A-=C
            B-=D
        else:
            v-=u
            C-=A
            D-=B
    d=g*v
    x=C
    y=D
    return d,x,y
```

[34]:
```
ext_bin_euclid(12345,54321)
```

[34]:
```
(3.0, -14490.0, 3293.0)
```

Выводы

Выводы

1. Реализован алгоритм Евклида.
2. Реализован бинарный алгоритм Евклида.
3. Реализован расширенный алгоритма Евклида.
4. Реализован расширенный бинарный алгоритма Евклида.