Отчёт по лабораторной работе №7

Дискретное логарифмирование в конечном поле

Федюшина Ярослава Андреевна

Содержание

Список иллюстраций

Задание

Реализовать код программно

Выполнение лабораторной работы

Python

def ext_euclid(a, b): if b==0: return a, 1, 0 else: d, xx, yy = ext_euclid(b, a%b) x = yy y = xx - (a//b)*yy return d, x, y

def inverse(a, n): return ext_euclid(a, n)[1]

def xab(x, a, b, xxx): (G, H, P, Q) = xxx sub = x%3

```
if sub == 0:
    x = x*xxx[0] % xxx[2]
    a = (a+1)%Q

if sub == 1:
    x = x*xxx[1] % xxx[2]
    b = (b+1) % xxx[2]

if sub == 2:
    x = x*x % xxx[2]
    a = a*2 % xxx[3]
    b = b*2 % xxx[3]

return x, a, b
```

def pollard(G, H, P): Q = int((P-1)//2) x = G*H a = 1 b = 1 X = x A = a B = b

```
for i in range(1, P):
    x, a, b = xab(x, a, b, (G, H, P, Q))
    X, A, B = xab(X, A, B, (G, H, P, Q))
    X, A, B = xab(X, A, B, (G, H, P, Q))

    if x == X:
        break

nom = a-A
denom = B-b
res = (inverse(denom, Q)*nom)%Q
if verify(G, H, P, res):
    return res
return res + Q
```

def verify(g, h, p, x): return pow(g, x, p) == h

args = (10, 64, 107)

res = pollard(*args) print(args, ” : “, res) print(”Validates: “, verify(args[0], args[1], args[2], res))

Вывод

В ходе выполнения данной лабораторной работы мы смогли реализовать код программно и получить результат (10, 64, 107) : 20 Validates: True