Дискретное логарифмирование в конечном поле

Тагиев Байрам Алтай оглы

Содержание

# 1 Код

# -\*- coding: utf-8 -\*-  
  
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))

# 2 Результат

(10, 64, 107) : 20  
Validates: True