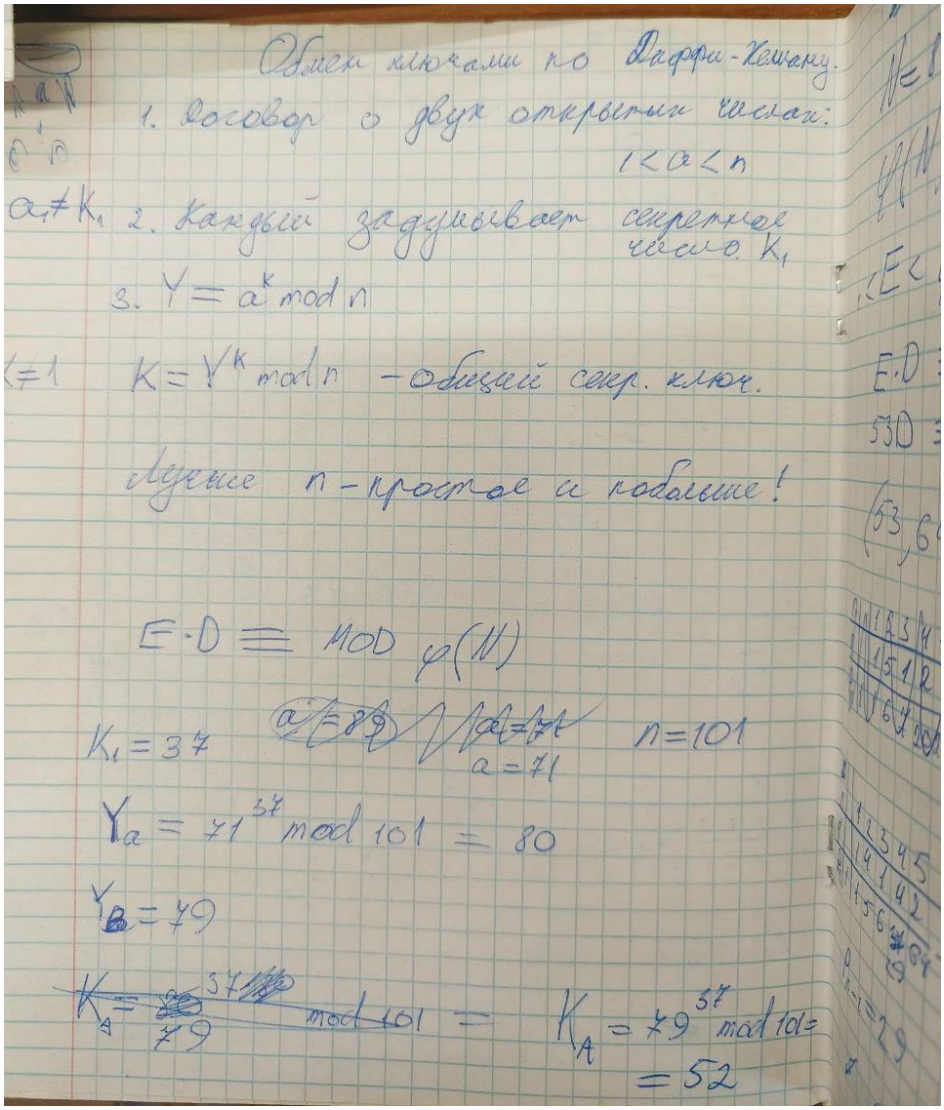
Обмен ключами по Диффи-Хелману

```
import random

### ОБМЕН КЛЮЧАМИ ПО ДИФФИ-ХЕЛЛМАНУ ###
def dfplayer1(p1, N, A):
    K = p1 # Секретный ключ 1 пользователя
    Y1 = (A ** K) % N # Открытый ключ
    return N, A, Y1, K

def dfplayer2(N, A, Y1, p2):
    K = p2 # Секретный ключ 2 пользователя
    Y2 = (A ** K) % N # Открытый ключ
    K = (Y1 ** p2) % N # Общий ключ
    return Y2, K

def dfplayer1key(Y2, KU2, N, K1):
    KU1 = (Y2 ** K1) % N # Общий ключ
    print("Секретный ключ первого пользователя:", KU1)
    if KU1 == KU2 and KU1 not in [0,1] and KU2 not in [0,1]:
        print("Ключи совпали")
        return True
    elif  KU1 in [0,1] and KU2 in [0,1]:
        print("Ключи не выработен")
        return True
    else:
        print("Ключи не совпали")
        return False

def is_prime(n):
    if n <= 1:
        return False
    if n <= 3:
        return True
    if n % 2 == 0 or n % 3 == 0:
        return False
    i = 5
    while i * i <= n:
        if n % i == 0 or n % (i + 2) == 0:
            return False
        i += 6
    return True

### Обмен ключами ###
print("ОБМЕН КЛЮЧАМИ ПО ДИФФИ-ХЕЛЛМАНУ")

while True:
    start_over = False

    while True:
        N = int(input("Введите N (простое число и не равное 1) = "))
```

```
        if is_prime(N) and N != 1:
            break
        print("N должно быть простым числом и не может быть равным 1.")

    while True:
        A = int(input("Введите A (не равное 1 и меньшее N) = "))
        if A != 1 and A < N:
            break
        print("A должно быть меньше N и не может быть равно 1.")

    while True:
        p1 = int(input("Первый пользователь вводит секретный ключ (не равный 1 и
p1 < N - 1) = "))
        if p1 != 1 and p1 < N and (A ** p1) % N != 1:
            break
        print("Секретный ключ не удовлетворяет условие. Пожалуйста, введите
другое значение.")

    while True:
        p2 = int(input("Второй пользователь вводит секретный ключ (не равный 1 и
p1 < N - 1) = "))
        if p2 != 1 and p2 < N and (A ** p2) % N != 1:
            break
        print("Секретный ключ не удовлетворяет условие. Пожалуйста, введите
другое значение.")

    itog = dfplayer1(p1, N, A)
    print("N =", itog[0])
    print("A =", itog[1])
    print("Открытый ключ первого пользователя:", itog[2])

    itog2 = dfplayer2(itog[0], itog[1], itog[2], p2)
    print("Открытый ключ второго пользователя:", itog2[0])
    print("Секретный ключ второго пользователя:", itog2[1])

    start_over = dfplayer1key(itog2[0], itog2[1], itog[0], itog[3])
    prodolg = int(input("Обменятсяь ещё раз (1 - да, 0 - нет) "))
    if prodolg:
        print("Новый обмен:")
    else:
        break
```



Пример работы:

```
PS C:\Users\Sergey\Desktop\УЧЕБА\Крипта\2sem> & c:/Users/Sergey/Desktop/УЧЕБА/Крипта/2sem/ve/Scripts/python.exe c:/Users/Sergey/Desktop/УЧЕБА/Крипта/2sem/Block_K/Diffie-He
ОБМЕН КЛЮЧАМИ ПО ДИФФИ-ХЕЛЛМАНУ
Введите N (простое число и не равное 1) = 101
Введите A (не равное 1 и меньшее N) = 71
Первый пользователь вводит секретный ключ (не равный 1 и p1 < N - 1) = 31
Второй пользователь вводит секретный ключ (не равный 1 и p1 < N - 1) = 37
N = 101
A = 71
Открытый ключ первого пользователя: 79
Открытый ключ второго пользователя: 80
Секретный ключ второго пользователя: 52
Секретный ключ первого пользователя: 52
Ключи совпали
```