**RSA и Elgamal**

Подписи реализованы в одном коде

import random

import math

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

def pred(s):

    llst = ['а','б','в','г','д','е','ж','з','и','й','к','л','м','н','о','п','р','с','т','у','ф','х','ц','ч','ш','щ','ъ','ы','ь','э','ю','я']

    s = s.lower().replace(' ', '')

    for sim in s:

        if sim not in llst:

            if sim == '.':

                s = s.replace('.', 'тчк')

            elif sim == ',':

                s = s.replace(',', 'зпт')

            elif sim == '-':

                s = s.replace('-', 'тире')

            elif sim == 'ё':

                s = s.replace('ё', 'е')

            elif sim == '0':

                s = s.replace('0', 'ноль')

            elif sim == '1':

                s = s.replace('1', 'один')

            elif sim == '2':

                s = s.replace('2', 'два')

            elif sim == '3':

                s = s.replace('3', 'три')

            elif sim == '4':

                s = s.replace('4', 'четыре')

            elif sim == '5':

                s = s.replace('5', 'пять')

            elif sim == '1':

                s = s.replace('6', 'шесть')

            elif sim == '2':

                s = s.replace('7', 'семь')

            elif sim == '3':

                s = s.replace('8', 'восемь')

            elif sim == '4':

                s = s.replace('9', 'девять')

            else:

                s = s.replace(sim, '')

    return s

def hesh(str,p,i):

    alp = " АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"

    if i==0:

        q=(alp.index(str[i])\*\*2)%p

        return q

    else:

        q=((hesh(str,p,i-1)+alp.index(str[i]))\*\*2)%p

        return q

### RSA подпись ###

def decrsakey(s, P, Q, mod):

    llst = ['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф',

            'х', 'ц', 'ч', 'ш', 'щ', 'ъ', 'ы', 'ь', 'э', 'ю', 'я']

    s = pred(s)

    D = 7

    N = P \* Q

    F = (P - 1) \* (Q - 1)

    arr = [i for i in range(2, F) if math.gcd(i, F) == 1]

    # E = random.choice(arr)

    E = int(input("Введите E: "))

    if (E < 1) or (E > mod) or math.gcd(E, F) != 1:

        print("неверное E")

        return 0

    print("N = ", N)

    print("F = ", F)

    print("E = ", E)

    for i in range(10000):

        if i \* E % F == 1 and i != E:

            D = i

            break

    print("D = ", D)

    h = 4

    for x in s:

        x = llst.index(x)

        h = ((h + x) \*\* 2) % mod

    S = h \*\* D % N

    print("S = ", S)

    return s, S, E, N, D

def checkrsakey(s, key, mod):

    s = pred(s)

    S = int(key[0])

    E = int(key[1])

    N = int(key[2])

    llst = ['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф',

            'х', 'ц', 'ч', 'ш', 'щ', 'ъ', 'ы', 'ь', 'э', 'ю', 'я']

    ho = 4

    for x in s:

        x = llst.index(x)

        ho = ((ho + x) \*\* 2) % mod

    h = S \*\* E % N

    print("h = ", h)

    print("h0 = ", h)

    if h == ho:

        print(h, "равен", ho)

        print('Цифровая подпись подтверждена')

        result = 'Цифровая подпись подтверждена'

    else:

        print(h, "не равен", ho)

        print('Цифровая подпись не подтверждена')

        result = 'Цифровая подпись не подтверждена'

    return result

## Elgamal подпись ###

def phi(n: int) -> int:

    result = n

    i = 2

    while i \*\* 2 < n:

        while n % i == 0:

            n /= i

            result -= result / i

        i += 1

    if n > 1:

        result -= result / n

    return result

def decelgakey(s, P, mod):

    llst = ['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф',

            'х', 'ц', 'ч', 'ш', 'щ', 'ъ', 'ы', 'ь', 'э', 'ю', 'я']

    s = pred(s)

    h = 4

    for x in s:

        x = llst.index(x)

        h = ((h + x) \*\* 2) % mod

    X = random.randint(2, P - 1)

    X = 5

    G = random.randint(2, P - 1)

    G = 11

    print("G = ", G)

    print("X = ", X)

    Y = G \*\* X % P

    print("Y = ", Y)

    arr = [i for i in range(2, 10) if math.gcd(i, P - 1) == 1]

    K = random.choice(arr)

    K = 3

    print("K = ", K)

    A = (G \*\* K) % P

    print("A = ", A)

    print("h0 = ", h)

    B = ((h - A \* X) \* K \*\* (phi(P - 1) - 1)) % (P - 1)

    print("B = ", B)

    return s, Y, A, B, P, G, X

def checkelgakey(s, key, mod):

    s = pred(s)

    y = int(key[0])

    a = int(key[1])

    b = int(key[2])

    p = int(key[3])

    g = int(key[4])

    llst = ['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф',

            'х', 'ц', 'ч', 'ш', 'щ', 'ъ', 'ы', 'ь', 'э', 'ю', 'я']

    h = 4

    for x in s:

        x = llst.index(x)

        h = ((h + x) \*\* 2) % mod

    print("h = ", h)

    A1 = (y \*\* a \* a \*\* b) % p

    A2 = g \*\* h % p

    if A1 == A2:

        print("A1 = ",A1, "равен","A2 = ", A2)

        print('Цифровая подпись подтверждена')

        result = 'Цифровая подпись подтверждена'

    else:

        print("A1 = ", A1, " не равен","A2 = ", A2)

        print('Цифровая подпись не подтверждена')

        result = 'Цифровая подпись не подтверждена'

    return result

a = int(input("выберите режим(1 - карточка, 2 - текст > 1000 символов): "))

mod = 0

if a == 1:

    mod = 32

else:

    mod == 99

# # для подпись RSA

print("RSA подпись")

P = int(input("P = "))

if is\_prime(P):

    Q = int(input("Q = "))

    if is\_prime(Q):

        if P \* Q >= 32:

            text = str(input("Введите текст: "))

            res = decrsakey(text, P, Q, mod)

            checkrsakey(text, [res[1],res[2],res[3]], mod)

        else:

            print("Произведение p и q меньше длинны алфавиты (32)")

    else:

        print("Q не простое число")

else:

    print("P не простое число")

#для подписи Elgamal

print("Elgamal подпись")

text = str(input("Введите текст : "))

P = int(input("P = "))

if P > 40 and is\_prime(P):

    res = decelgakey(text, P, mod)

    # print("Зашифрованный текст = ", res[0])

    checkelgakey(res[0], res[1:], mod)

else:

    print("P должен быть больше 40 и простым числом")







