**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)
```

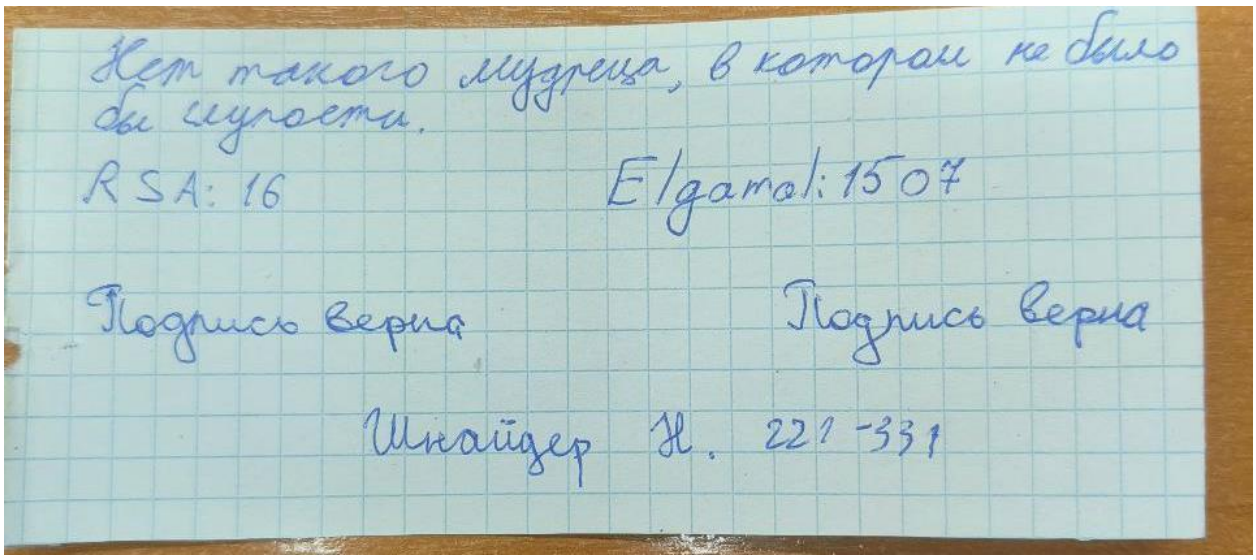
```
        print('Цифровая подпись не подтверждена')
        result = 'Цифровая подпись не подтверждена'
    return result
a = int(input("выберите режим(1 - карточка, 2 - текст > 1000 символов): "))
mod = 0
if a == 1:
    mod = 32
else:
    mod == 99
# # для подпись RSA
print("RSA подпись")
P = int(input("P = "))

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")
```




```
выберите режим(1 - карточка, 2 - текст > 1000 символов): 1
RSA подпись
P = 3
Q = 11
Введите текст: неттакогомудрецазптвкоторомнебылобыглупоститчк
Введите E: 3
N =  33
F =  20
E =  3
D =  7
S =  16
h =  4
h0 =  4
4 равен 4
Цифровая подпись подтверждена
Elgamal подпись
Введите текст : неттакогомудрецазптвкоторомнебылобыглупоститчк
P = 47
G =  11
X =  5
Y =  29
K =  3
A =  15
h0 =  4
B =  7.0
h =  4
A1 =  24 равен A2 =  24
Цифровая подпись подтверждена
PS C:\Users\Sergey\Desktop\УЧЁБА\Крипта\2sem>
```

```
Elgamal подпись
Введите текст : А судьи кто? – За древностию лет К свободной жизни их вражда непримирима, Сужденья черпают из забытых газет Времён Очаковских и покоренья Крыма; Всегда готовые к журьбе, Поют все песнь одну и ту же
, Не замечая об себе: Что старее, то хуже. Где? укажите нам, отечества отцы, Которых мы должны принять за образцы? Не эти ли, грабительством богаты? Защиту от суда в друзьях нашли, в родстве, Великолепные соорудя
палаты, Где разливаются в пирах и мотовстве, И где не воскресят клиенты-иностранцы Прошедшего житья подлейшие черты. Да и кому в Москве не зажимали рты Обеды, ужины и танцы? Не тот ли, вы к кому меня ещё с пелен,
Для замыслов каких-то непонятных, Дитей возили на поклон? Тот Нестор негодяев знатных, Толпою окружённый слуг; Усердствуя, они в часы вина и драки И честь, и жизнь его не раз спасали: вдруг На них он выменял борзы
е три собаки!!! Или вон тот ещё, который для затей На крепостной балет согнал на многих фурах От матерей, отцов отторженных детей?! Сам погружён умом в Зефирах и в Амурах, Заставил всю Москву дивиться их красе! Но
должников не согласил к отсрочке: Амуры и Зефиры все Распроданы поодиночке!!! Вот те, которые дожили до седин! Вот уважать кого должны мы на безлюдьи! Вот наши строгие ценители и судьи! Теперь пускай из нас один,
Из молодых людей, найдётся – враг исканий, Не требуя ни мест, ни повышенья в чин, В науки он вперит ум, алчущий познаний; Или в душе его сам бог возбудит жар К искусствам творческим, высоким и прекрасным, – Они т
отчас: разбой! пожар! И прослывёт у них мечтателем! опасным!! – Мундир! один мундир! он в прежнем их быту Когда-то укрывал, расшитый и красивый, Их слабодушие, рассудка нищету; И нам за ними в путь счастливый! И в
жёнах, дочерях – к мундиру та же страсть! Я сам к нему давно ль от нежности отрёкся?! Теперь уж в это мне ребячество не впасть; Но кто б тогда за всеми не повлекся? Когда из гвардии, иные от двора Сюда на время п
риезжали, – Кричали женщины: ура! И в воздух чепчики бросали!
P = 43
G =  2
X =  14
Y =  1
K =  5
A =  32
h0 =  9
B =  13.0
h =  9
A1 =  39 равен A2 =  39
Цифровая подпись подтверждена
PS C:\Users\Sergey\Desktop\УЧЁБА\Крипта\2sem>
```

```
выберите режим(1 - карточка, 2 - текст > 1000 символов): 2
RSA подпись
P = 13
Q = 17
Введите текст: А судьи кто? – За древностию лет К свободной жизни их вражда непримирима, Сужденья черпают из забытых газет Времён Очаковских и покоренья Крыма; Всегда готовые к журьбе, Поют все песнь одну и ту же,
 Не замечая об себе: Что старее, то хуже. Где? укажите нам, отечества отцы, Которых мы должны принять за образцы? Не эти ли, грабительством богаты? Защиту от суда в друзьях нашли, в родстве, Великолепные соорудя п
алаты, Где разливаются в пирах и мотовстве, И где не воскресят клиенты-иностранцы Прошедшего житья подлейшие черты. Да и кому в Москве не зажимали рты Обеды, ужины и танцы? Не тот ли, вы к кому меня ещё с пелен, Д
ля замыслов каких-то непонятных, Дитёй возили на поклон? Тот Нестор негодяев знатных, Толпою окружённый слуг; Усердствуя, они в часы вина и драки И честь, и жизнь его не раз спасали: вдруг На них он выменял борзые
 три собаки!!! Или вон тот ещё, который для затей На крепостной балет согнал на многих фурах От матерей, отцов отторженных детей?! Сам погружён умом в Зефирах и в Амурах, Заставил всю Москву дивиться их красе! Но
должников не согласил к отсрочке: Амуры и Зефиры все Распроданы поодиночке!!! Вот те, которые дожили до седин! Вот уважать кого должны мы на безлюдьи! Вот наши строгие ценители и судьи! Теперь пускай из нас один,
Из молодых людей, найдётся – враг исканий, Не требуя ни мест, ни повышенья в чин, В науки он вперит ум, алчущий познаний; Или в душе его сам бог возбудит жар К искусствам творческим, высоким и прекрасным, – Они то
тчас: разбой! пожар! И прослывёт у них мечтателем! опасным!! – Мундир! один мундир! он в прежнем их быту Когда-то укрывал, расшитый и красивый, Их слабодушие, рассудка нищету; И нам за ними в путь счастливый! И в
жёнах, дочерях – к мундиру та же страсть! Я сам к нему давно ль от нежности отрёкся?! Теперь уж в это мне ребячество не впасть; Но кто б тогда за всеми не повлекся? Когда из гвардии, иные от двора Сюда на время пр
иезжали, – Кричали женщины: ура! И в воздух чепчики бросали!
N =  221
F =  192
E =  17
D =  113
S =  94
h =  9
h0 =  9
9 равен 9
Цифровая подпись подтверждена
Elgamal подпись
```