УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе № 4

по предмету «Теория информации»

Вариант 2

Выполнил:

Гузаев Е.Д

Гр. 351003

Проверил:

Болтак С. В.

Минск 2025

Пример функции хэширования:

Вычисление хеш-образа с параметрами H₀ = 100 и q = 107

Сначала преобразуем фразу "Испуганный Ёж" в числовые значения согласно правилу 'А' = 1, 'Б' = 2, ..., 'Я' = 33:

* 'И' = 10
* 'с' (в верхнем регистре 'С') = 19
* 'п' (в верхнем регистре 'П') = 17
* 'у' (в верхнем регистре 'У') = 21
* 'г' (в верхнем регистре 'Г') = 4
* 'а' (в верхнем регистре 'А') = 1
* 'н' (в верхнем регистре 'Н') = 15
* 'н' (в верхнем регистре 'Н') = 15
* 'ы' (в верхнем регистре 'Ы') = 29
* 'й' (в верхнем регистре 'Й') = 11
* Пробел = 0
* 'Ё' = 7
* 'ж' (в верхнем регистре 'Ж') = 8

Получаем сообщение M = {10, 19, 17, 21, 4, 1, 15, 15, 29, 11, 0, 7, 8}

Используем формулу хеш-функции Hi = (Hi-1 + Mi)² mod q, где q = 107, и начальное значение H₀ = 100:

H₁ = (100 + 10)² mod 107 = 110² mod 107 = 9  
H₂ = (9 + 19)² mod 107 = 28² mod 107 = 35  
H₃ = (35 + 17)² mod 107 = 52² mod 107 = 29  
H₄ = (29 + 21)² mod 107 = 50² mod 107 = 39  
H₅ = (39 + 4)² mod 107 = 43² mod 107 = 30  
H₆ = (30 + 1)² mod 107 = 31² mod 107 = 105  
H₇ = (105 + 15)² mod 107 = 120² mod 107 = 62  
H₈ = (62 + 15)² mod 107 = 77² mod 107 = 44  
H₉ = (44 + 29)² mod 107 = 73² mod 107 = 86  
H₁₀ = (86 + 11)² mod 107 = 97² mod 107 = 100  
H₁₁ = (100 + 0)² mod 107 = 100² mod 107 = 49  
H₁₂ = (49 + 7)² mod 107 = 56² mod 107 = 33  
H₁₃ = (33 + 8)² mod 107 = 41² mod 107 = 76

Таким образом, хеш-образ для фразы "Испуганный Ёж" при H₀ = 100 и модуле q = 107 равен 76.

Применение алгоритма цифровой подписи DSA для фразы "Испуганный Ёж"

Параметры DSA:

* q = 107 (простое число)
* p = 643 (простое число, p-1 делится на q: 642/107 = 6)
* h = 2 (для вычисления g)
* x = 45 (закрытый ключ)
* k = 31 (случайное число для генерации подписи)

## Вычисление значений для создания подписи

1. Вычисляем g = h^((p-1)/q) mod p = 2^(642/107) mod 643 = 2^6 mod 643 = 64
2. Вычисляем открытый ключ y = g^x mod p = 64^45 mod 643 = 181
3. Хеш-образ сообщения h(M) = 76 (вычислен выше)
4. Вычисляем первый компонент подписи r:  
   r = (g^k mod p) mod q = (64^31 mod 643) mod 107 = 36
5. Вычисляем мультипликативно обратное к k по модулю q:  
   k^-1 mod q = 31^-1 mod 107 = 31^(q-2) mod 107 = 31^105 mod 107 = 38
6. Вычисляем второй компонент подписи s:  
   s = k^-1 \* (h(M) + xr) mod q = 38 \* (76 + 4536) mod 107 = 38 \* (76 + 1620 mod 107) mod 107 = 38 \* (76 + 86) mod 107 = 38 \* 162 mod 107 = 34

Таким образом, цифровая подпись DSA для фразы "Испуганный Ёж" с хеш-образом 76 представляет собой пару значений (r, s) = (36, 34).

## Проверка подписи

Получатель для проверки подписи должен выполнить:

1. Вычислить w = s^-1 mod q = 34^-1 mod 107 = 66
2. Вычислить параметры:  
   u1 = h(M) \* w mod q = 76 \* 66 mod 107 = 37  
   u2 = r \* w mod q = 36 \* 66 mod 107 = 63
3. Вычислить проверочное значение:  
   v = (g^u1 \* y^u2 mod p) mod q = (64^37 \* 181^63 mod 643) mod 107 = 36
4. Сравнить v и r: поскольку v = r = 36, подпись является подлинной.

**Задание:**

Реализовать программное средство, выполняющее вычисление и проверку электронной цифровой подписи (**ЭЦП**) текстового файла **на базе алгоритма DSA**. Для вычисления хеш-образа сообщения использовать функцию 3.2 из методических материалов (стр.22, **Н0=100),** вычисления функции необходимо выполнять по модулю числа ***q*.** Числа ***q, p, h, x* и *k*** ввести с клавиатуры. Произвести все необходимые проверки для параметров, вводимых с клавиатуры. В отдельное поле вывести полученный хеш сообщения в 10 с/cч. ЭЦП вывести как два целых числа (если одно из полученных значений *r* или *s* будет равно 0, то необходимо повторить вычисления для другого значения *k* для чего предложить повторно ввести ***k*** с клавиатуры). Сформировать новое сообщение, состоящее из исходного сообщения и добавленной к нему цифровой подписи. При проверке ЭЦП предусмотреть возможность выбора файла для проверки. На экран вывести результат проверки:

1 – сообщение о том верна подпись или нет;

2 – вычисленные при проверке значения.

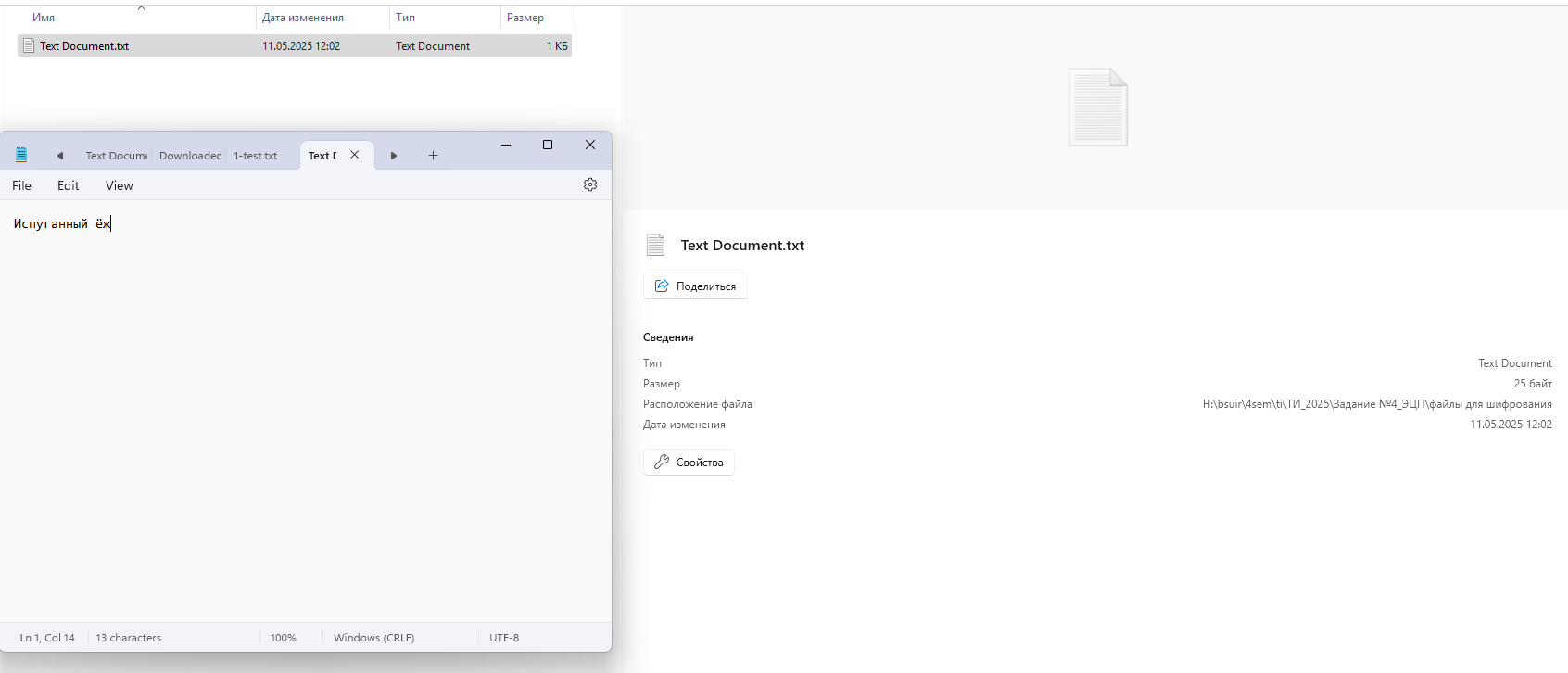
Для возведения в степень использовать быстрый алгоритм возведения в степень по модулю.

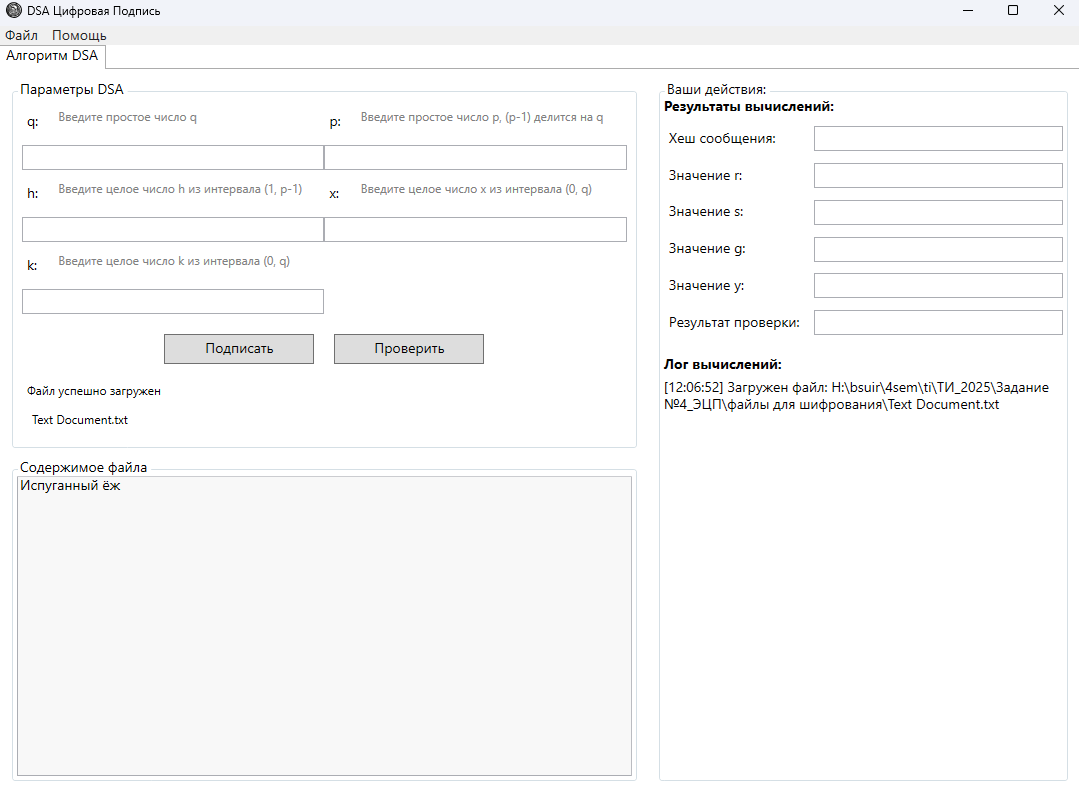
При нахождении обратного элемента ***s−1mod q*** или ***k−1 mod q*** использовать ***малую теорему Ферма*** в виде: ***s−1mod q = sq-2 mod q***

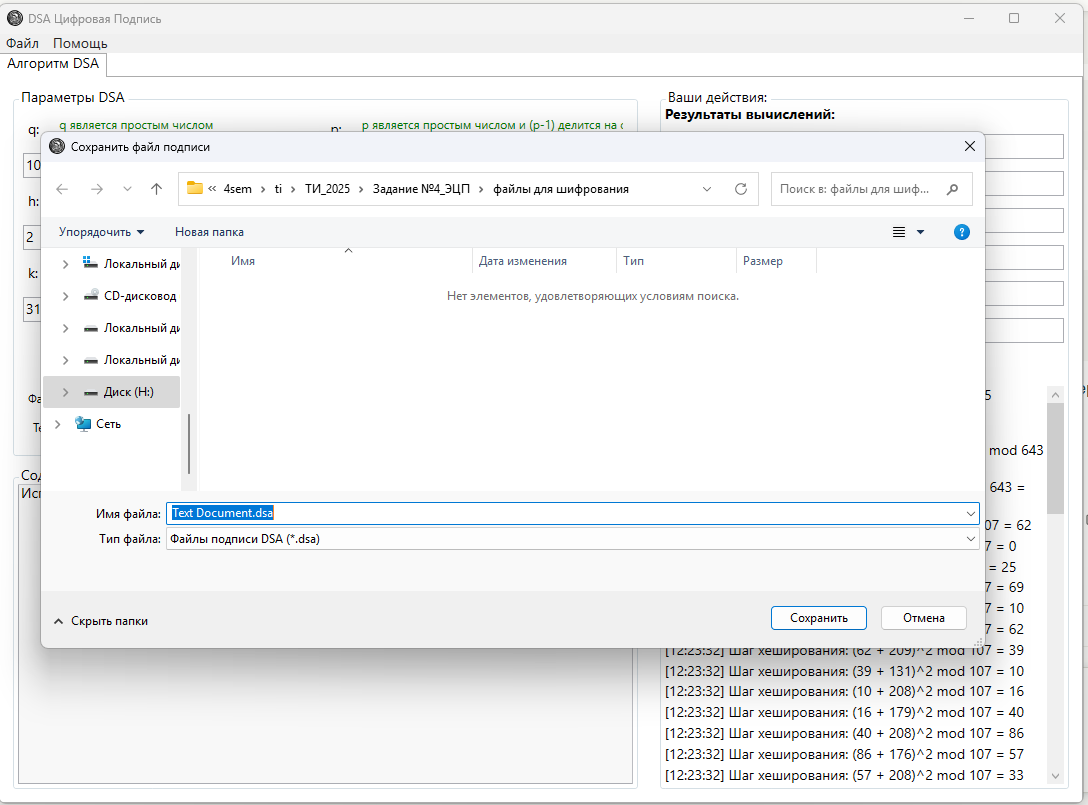
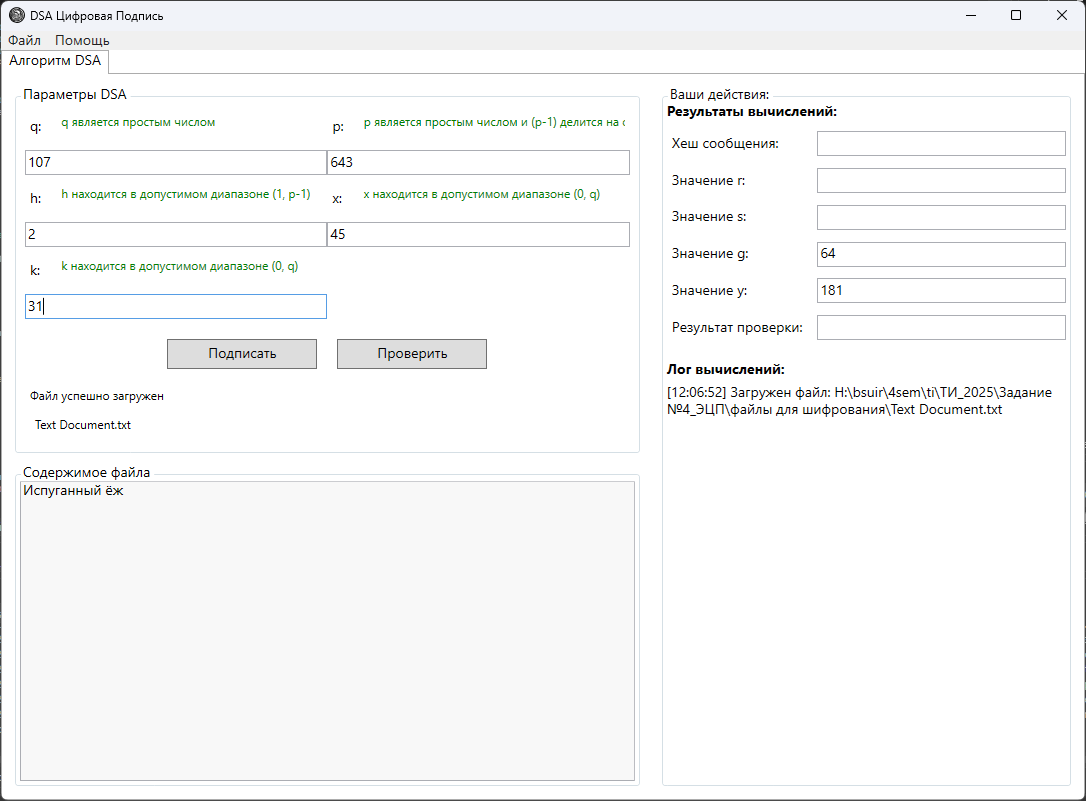
**Тесты:**

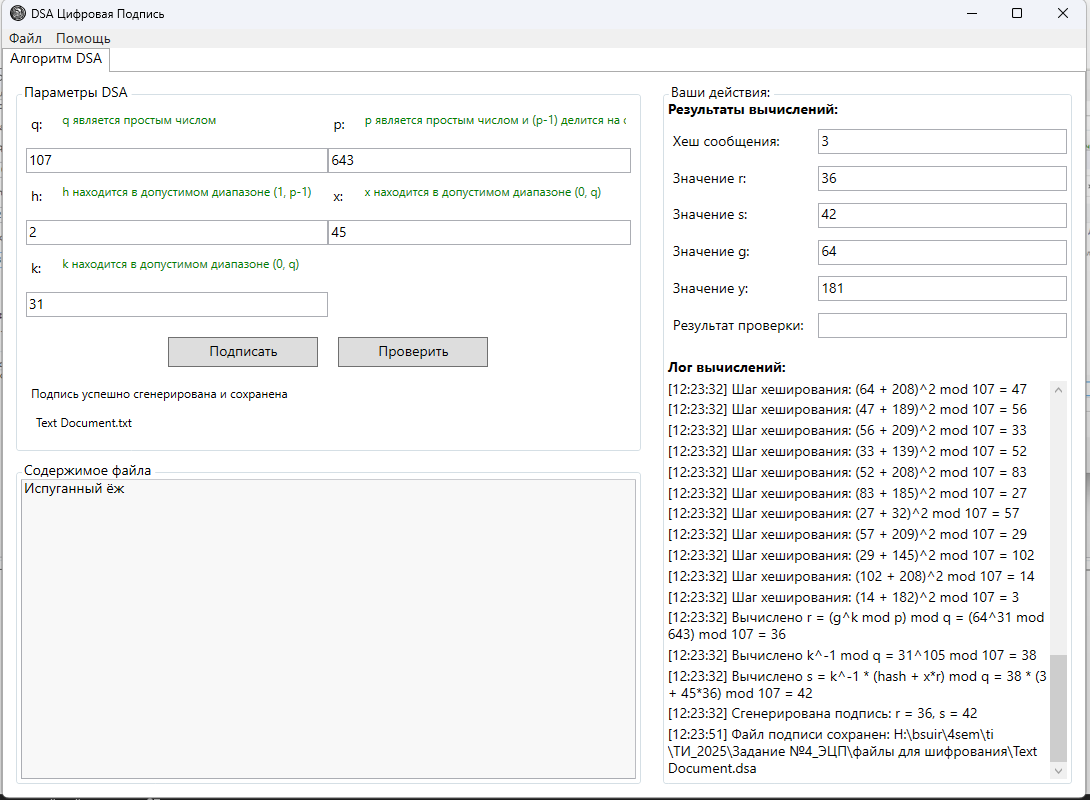
1. Текстовый файл:

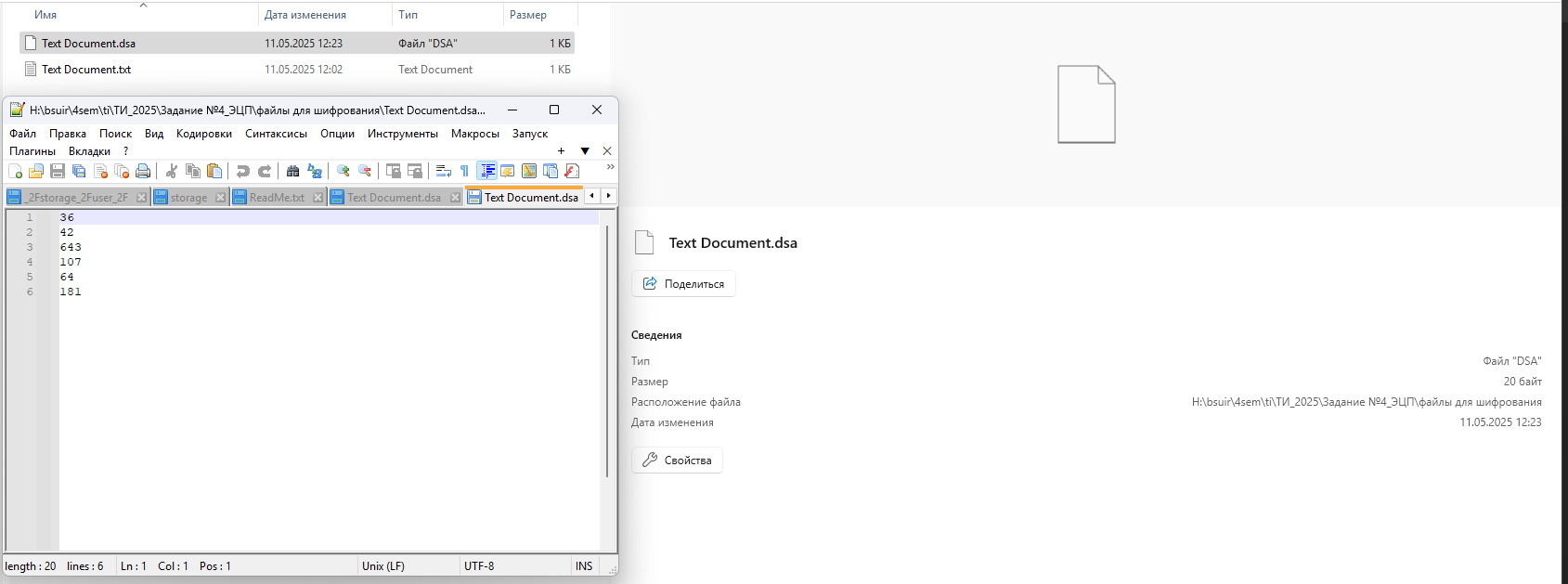
Исходное содержимое:

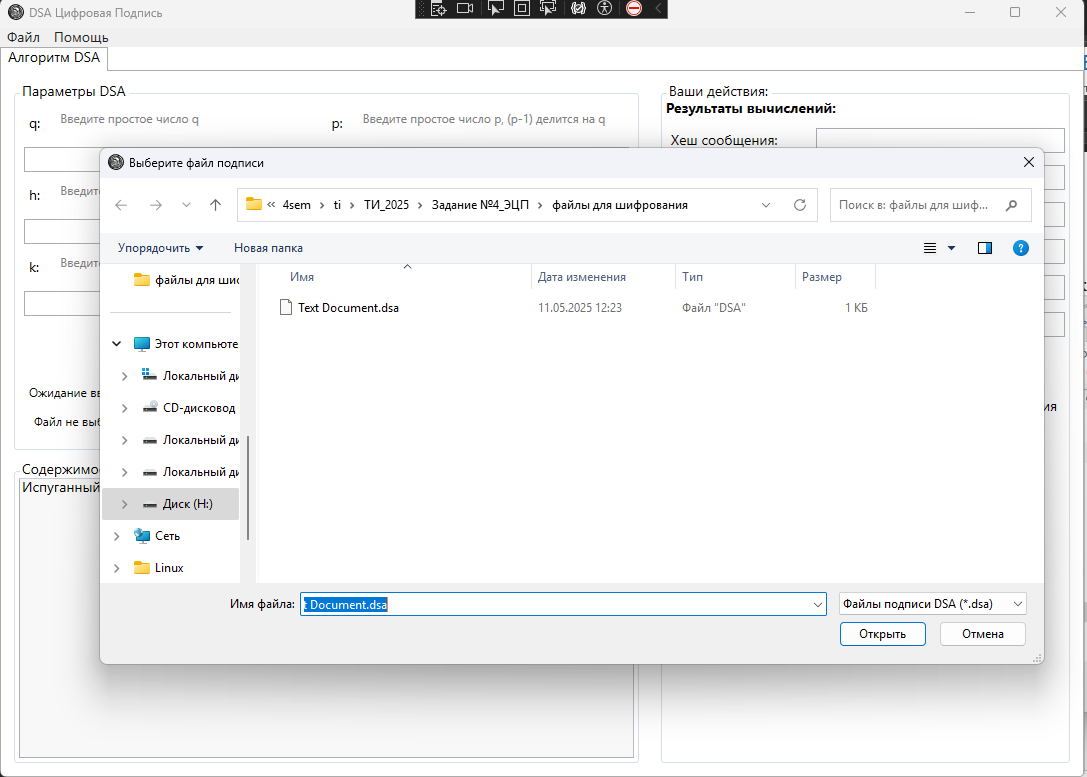
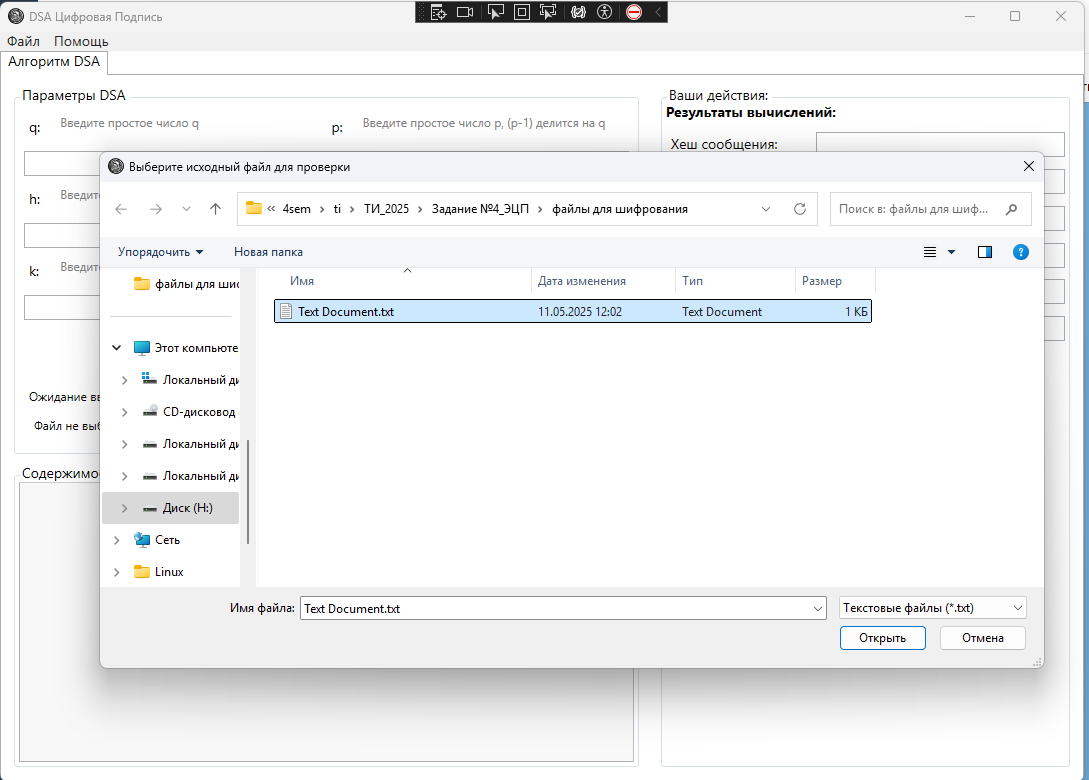


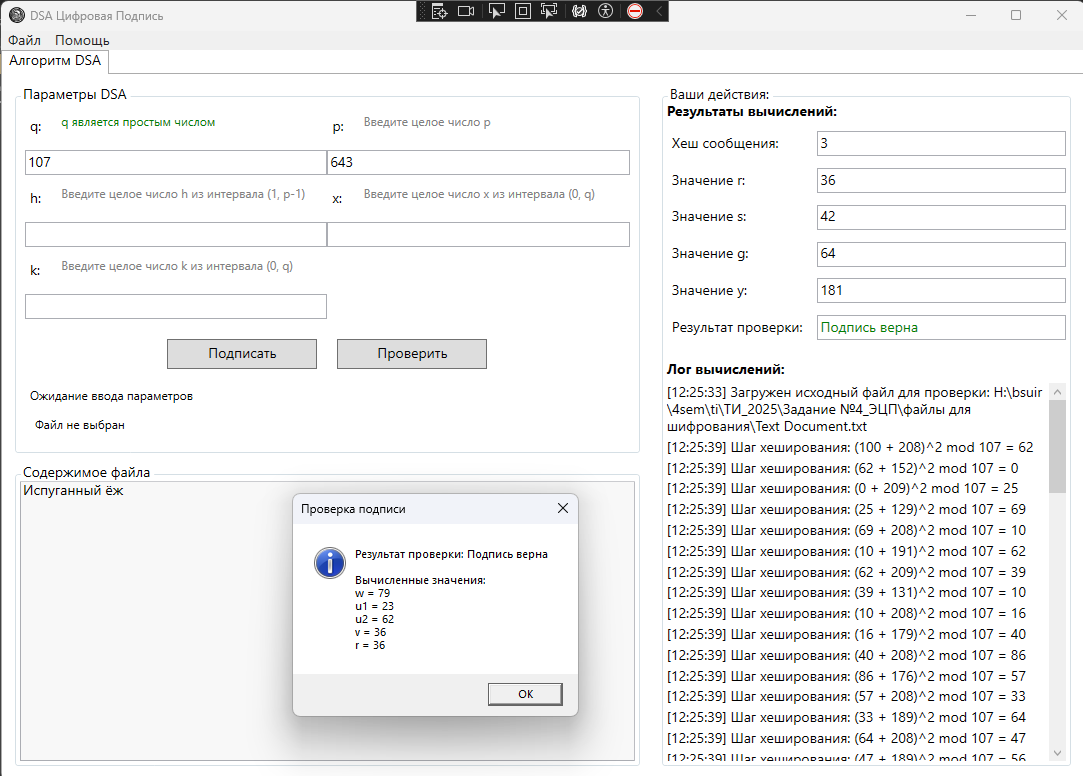
Отображение в программе:  


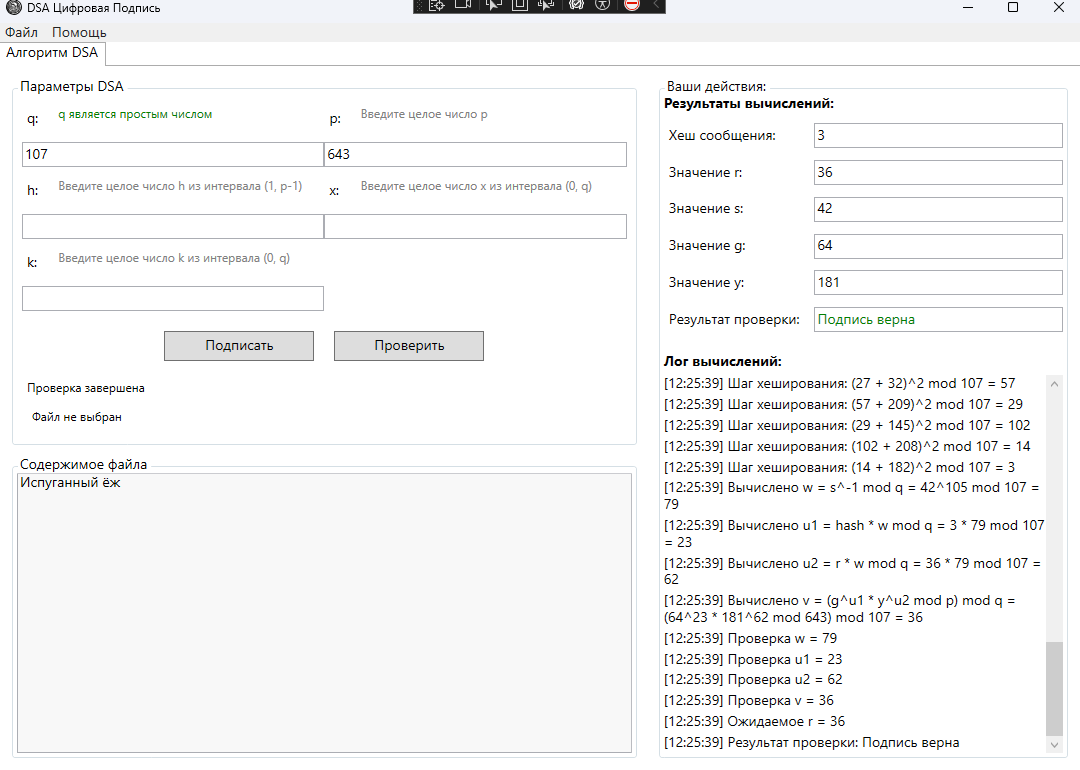
Результат подписи:  


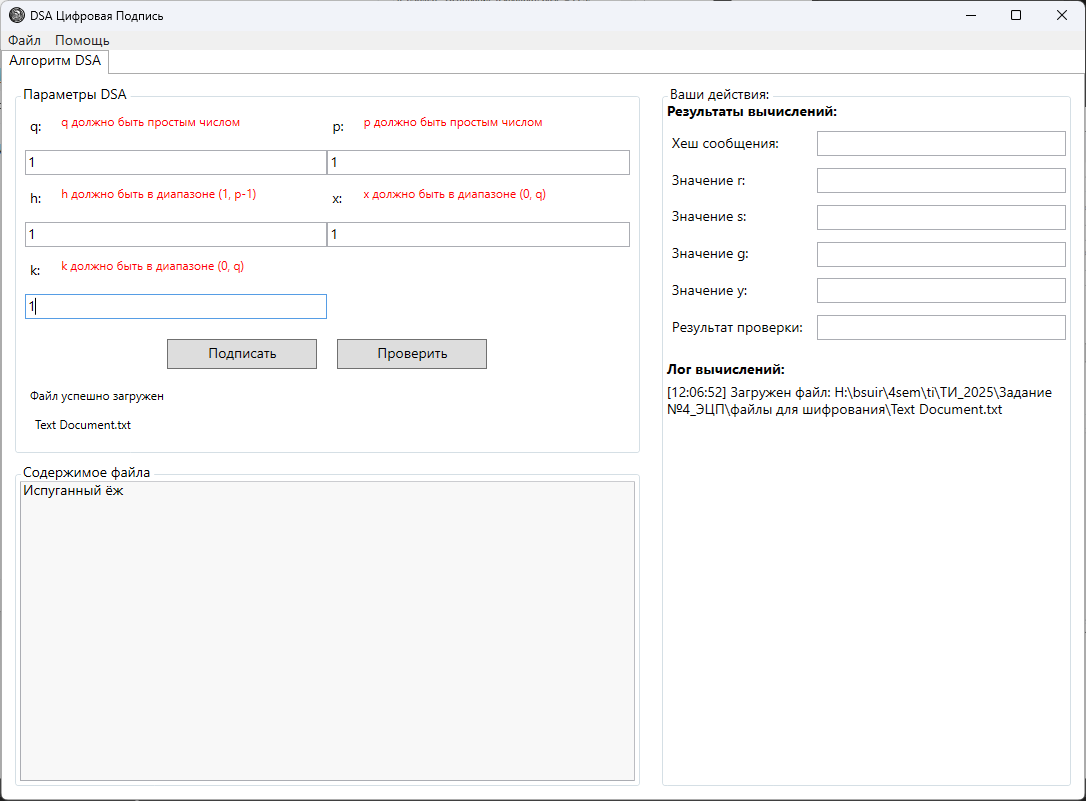




Проверка подписи: 





Проверки на ошибки::

