

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  $H_0 = 100$  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  $H_i = (H_{i-1} + M_i)^2 \bmod q$ , где  $q = 107$ , и начальное значение  $H_0 = 100$ :

$$\begin{aligned}H_1 &= (100 + 10)^2 \bmod 107 = 110^2 \bmod 107 = 9 \\H_2 &= (9 + 19)^2 \bmod 107 = 28^2 \bmod 107 = 35 \\H_3 &= (35 + 17)^2 \bmod 107 = 52^2 \bmod 107 = 29 \\H_4 &= (29 + 21)^2 \bmod 107 = 50^2 \bmod 107 = 39 \\H_5 &= (39 + 4)^2 \bmod 107 = 43^2 \bmod 107 = 30 \\H_6 &= (30 + 1)^2 \bmod 107 = 31^2 \bmod 107 = 105 \\H_7 &= (105 + 15)^2 \bmod 107 = 120^2 \bmod 107 = 62 \\H_8 &= (62 + 15)^2 \bmod 107 = 77^2 \bmod 107 = 44 \\H_9 &= (44 + 29)^2 \bmod 107 = 73^2 \bmod 107 = 86 \\H_{10} &= (86 + 11)^2 \bmod 107 = 97^2 \bmod 107 = 100 \\H_{11} &= (100 + 0)^2 \bmod 107 = 100^2 \bmod 107 = 49 \\H_{12} &= (49 + 7)^2 \bmod 107 = 56^2 \bmod 107 = 33 \\H_{13} &= (33 + 8)^2 \bmod 107 = 41^2 \bmod 107 = 76\end{aligned}$$

Таким образом, хеш-образ для фразы "Испуганный Ёж" при  $H_0 = 100$  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  $g = h^{((p-1)/q)} \bmod p = 2^{(642/107)} \bmod 643 = 2^6 \bmod 643 = 64$
2. Вычисляем открытый ключ  $y = g^x \bmod p = 64^{45} \bmod 643 = 181$
3. Хеш-образ сообщения  $h(M) = 76$  (вычислен выше)
4. Вычисляем первый компонент подписи  $r$ :  
 $r = (g^k \bmod p) \bmod q = (64^{31} \bmod 643) \bmod 107 = 36$
5. Вычисляем мультипликативно обратное к  $k$  по модулю  $q$ :  
 $k^{-1} \bmod q = 31^{-1} \bmod 107 = 31^{(q-2)} \bmod 107 = 31^{105} \bmod 107 = 38$
6. Вычисляем второй компонент подписи  $s$ :  
 $s = k^{-1} * (h(M) + xr) \bmod q = 38 * (76 + 4536) \bmod 107 = 38 * (76 + 1620 \bmod 107) \bmod 107 = 38 * (76 + 86) \bmod 107 = 38 * 162 \bmod 107 = 34$

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  $w = s^{-1} \bmod q = 34^{-1} \bmod 107 = 66$
2. Вычислить параметры:  
 $u1 = h(M) * w \bmod q = 76 * 66 \bmod 107 = 37$   
 $u2 = r * w \bmod q = 36 * 66 \bmod 107 = 63$
3. Вычислить проверочное значение:  
 $v = (g^{u1} * y^{u2} \bmod p) \bmod q = (64^{37} * 181^{63} \bmod 643) \bmod 107 = 36$
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, **Но=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/сч. 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.

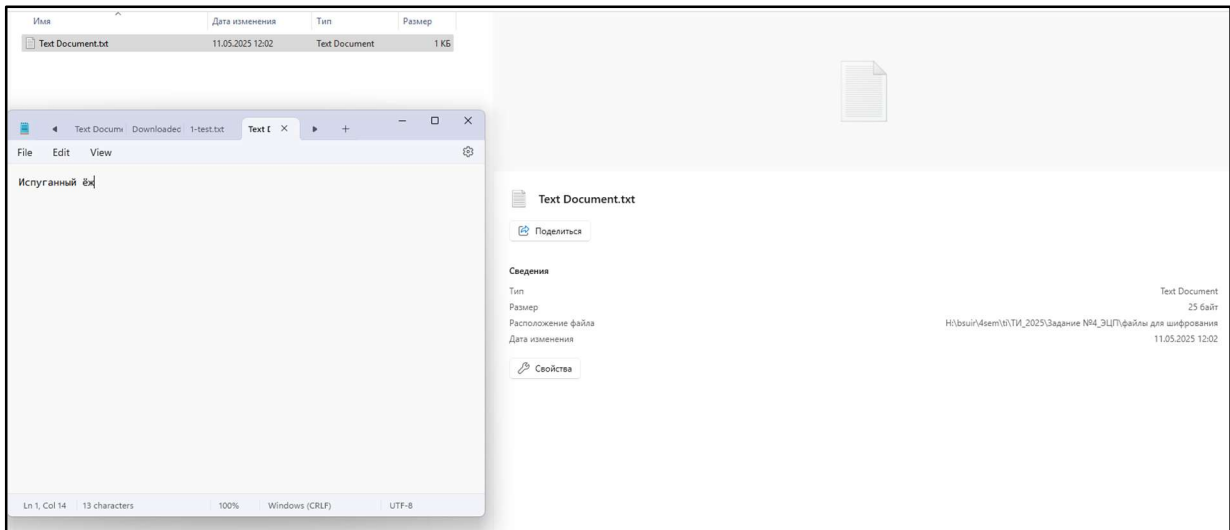
Для возведения в степень использовать быстрый алгоритм возведения в степень по модулю.

При нахождении обратного элемента  $s^{-1} \bmod q$  или  $k^{-1} \bmod q$  использовать *малую теорему Ферма* в виде:  $s^{-1} \bmod q = s^{q-2} \bmod q$

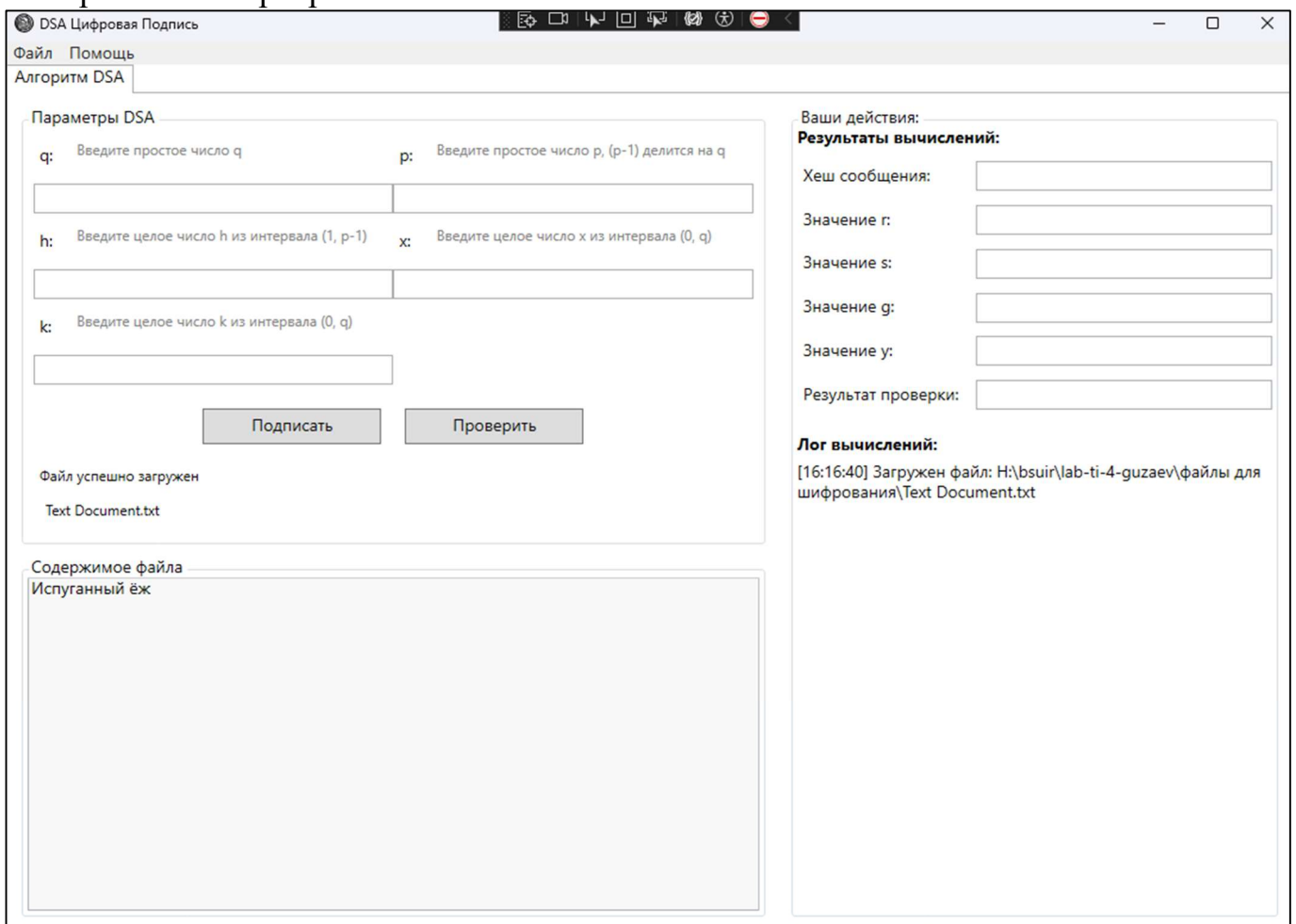
## Тесты:

### 1) Текстовый файл:

Исходное содержимое:



Отображение в программе:



## Результат подписи:

DSA Цифровая Подпись

Файл

Помощь

Алгоритм DSA

Параметры DSA

q: q является простым числом

107

p: p является простым числом и (p-1) делится на q

643

h: h находится в допустимом диапазоне (1, p-1)

2

x: x находится в допустимом диапазоне (0, q)

45

k: k находится в допустимом диапазоне (0, q)

31

Подписать

Проверить

Файл успешно загружен

Text Document.txt

Содержимое файла

Испуганный ёж

Ваши действия:

Результаты вычислений:

Хеш сообщения:

Значение g:

Значение s:

Значение g:

64

Значение u:

181

Результат проверки:

Лог вычислений:

[12:06:52] Загружен файл: H:\bsuir\4sem\ti\TI\_2025\Задание №4\_ЭЦП\файлы для шифрования\Text Document.txt

DSA Цифровая Подпись

Файл

Помощь

Алгоритм DSA

Параметры DSA

q: q является простым числом

107

p: p является простым числом и (p-1) делится на q

643

h: h находится в допустимом диапазоне (1, p-1)

2

x: x находится в допустимом диапазоне (0, q)

45

k: k находится в допустимом диапазоне (0, q)

31

Подписать

Проверить

Подпись успешно сгенерирована и добавлена в файл

H:\bsuir\lab-ti-4-guzaev\файлы для шифрования\Text Document.txt

Содержимое файла

-----BEGIN DSA SIGNATURE-----

r=36

s=42

p=643

q=107

g=64

u=181

-----END DSA SIGNATURE-----

Испуганный ёж

Ваши действия:

Результаты вычислений:

Хеш сообщения:

3

Значение g:

36

Значение s:

42

Значение g:

64

Значение u:

181

Результат проверки:

Лог вычислений:

[16:18:48] Шаг хеширования:  $(47 + 189)^2 \bmod 107 = 56$

[16:18:48] Шаг хеширования:  $(56 + 209)^2 \bmod 107 = 33$

[16:18:48] Шаг хеширования:  $(33 + 139)^2 \bmod 107 = 52$

[16:18:48] Шаг хеширования:  $(52 + 208)^2 \bmod 107 = 83$

[16:18:48] Шаг хеширования:  $(83 + 185)^2 \bmod 107 = 27$

[16:18:48] Шаг хеширования:  $(27 + 32)^2 \bmod 107 = 57$

[16:18:48] Шаг хеширования:  $(57 + 209)^2 \bmod 107 = 29$

[16:18:48] Шаг хеширования:  $(29 + 145)^2 \bmod 107 = 102$

[16:18:48] Шаг хеширования:  $(102 + 208)^2 \bmod 107 = 14$

[16:18:48] Шаг хеширования:  $(14 + 182)^2 \bmod 107 = 3$

[16:18:48] Вычислено  $r = (g^u \bmod p) \bmod q = (64^{181} \bmod 643) \bmod 107 = 36$

[16:18:48] Вычислено  $k^{-1} \bmod q = 31^{105} \bmod 107 = 38$

[16:18:48] Вычислено  $s = k^{-1} * (\text{hash} + x * r) \bmod q = 38 * (3 + 45 * 36) \bmod 107 = 42$

[16:18:48] Сгенерирована подпись:  $r = 36, s = 42$

[16:18:48] Подпись добавлена в начало исходного файла: H:\bsuir\lab-ti-4-guzaev\файлы для шифрования\Text Document.txt

5

Text Document (3).txt13.05.2025 16:11Text Document1 KB


Text Document.txt13.05.2025 16:18Text Document1 KB

1-test.txtText DocumText DocumText f X

FileEditView

|-----BEGIN DSA SIGNATURE-----  
r=36  
s=42  
p=643  
q=187  
g=64  
y=181  
-----END DSA SIGNATURE-----  
  
Испуганный ёж

Ln 1, Col 1105 characters100%Unix (LF)UTF-8



Text Document.txt

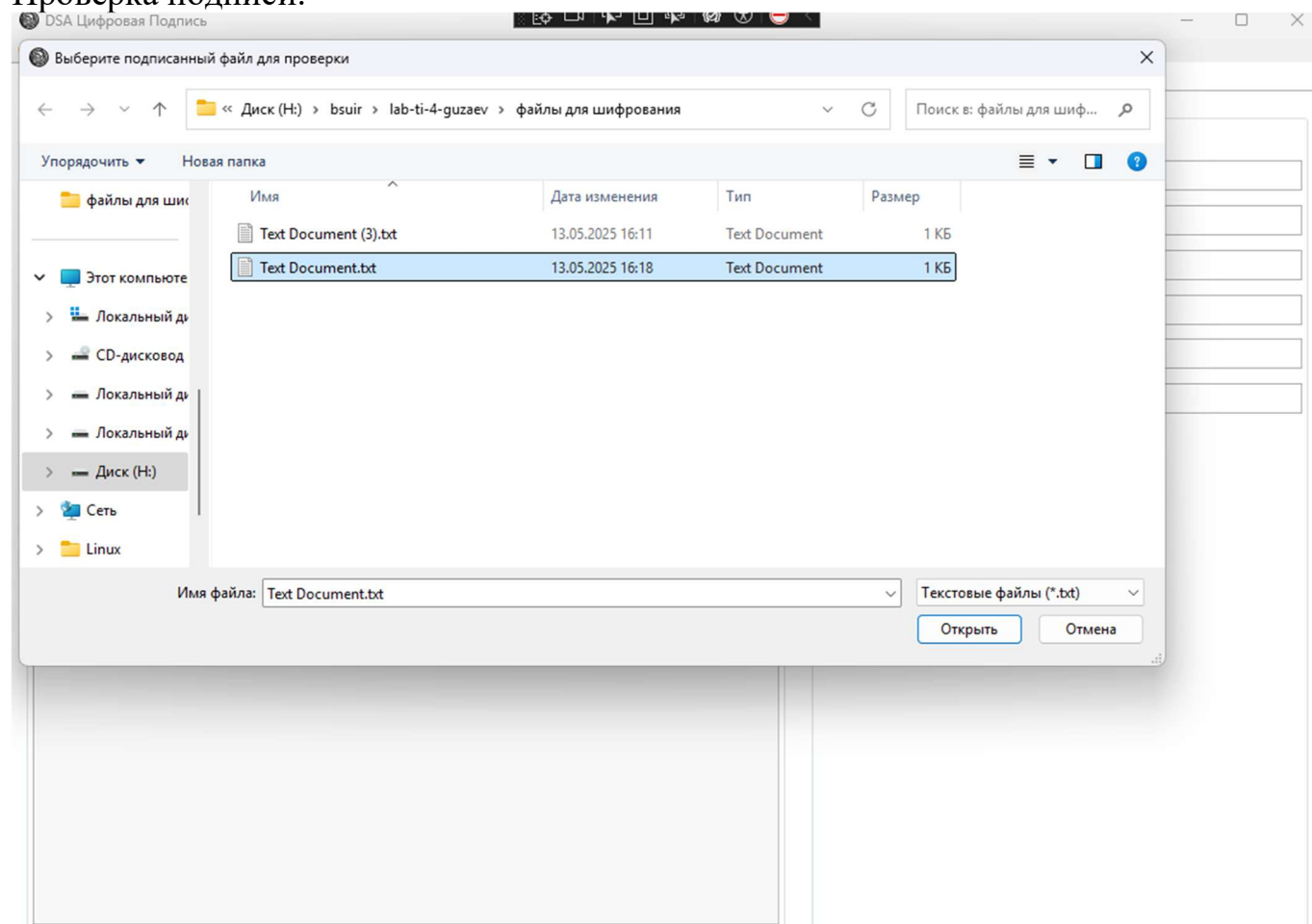
Поделиться

Сведения

ТипText Document  
Размер117 байт  
Расположение файлаH:\bsui\lab-8-4-gizzen\файлы для шифрования  
Дата изменения13.05.2025 16:18

Свойства

## Проверка подписи:



DSA Цифровая Подпись

Файл

Помощь

Алгоритм DSA

Параметры DSA

q: q является простым числом

107

p: Введите целое число p

643

h: Введите целое число h из интервала (1, p-1)

h:

x: Введите целое число x из интервала (0, q)

x:

k: Введите целое число k из интервала (0, q)

k:

Подписать

Проверить

Проверка подписи: ПОДПИСЬ ВЕРНА

H:\bsuir\lab-ti-4-guzae\файлы для шифрования\Text Document.txt

Содержимое файла

Испуганный ёж

Ваши действия:

Результаты вычислений:

Хеш сообщения:

3

Значение g:

36

Значение s:

42

Значение g:

64

Значение y:

181

Результат проверки:

ПОДПИСЬ ВЕРНА

Лог вычислений:

[16:19:15] Шаг хеширования:  $(47 + 189)^2 \bmod 107 = 56$

[16:19:15] Шаг хеширования:  $(56 + 209)^2 \bmod 107 = 33$

[16:19:15] Шаг хеширования:  $(33 + 139)^2 \bmod 107 = 52$

[16:19:15] Шаг хеширования:  $(52 + 208)^2 \bmod 107 = 83$

[16:19:15] Шаг хеширования:  $(83 + 185)^2 \bmod 107 = 27$

[16:19:15] Шаг хеширования:  $(27 + 32)^2 \bmod 107 = 57$

[16:19:15] Шаг хеширования:  $(57 + 209)^2 \bmod 107 = 29$

[16:19:15] Шаг хеширования:  $(29 + 145)^2 \bmod 107 = 102$

[16:19:15] Шаг хеширования:  $(102 + 208)^2 \bmod 107 = 14$

[16:19:15] Шаг хеширования:  $(14 + 182)^2 \bmod 107 = 3$

[16:19:15] Вычислено  $w = s^{-1} \bmod q = 42^{-1} \bmod 107 = 79$

[16:19:15] Вычислено  $u1 = \text{hash} * w \bmod q = 3 * 79 \bmod 107 = 23$

[16:19:15] Вычислено  $u2 = r * w \bmod q = 36 * 79 \bmod 107 = 62$

[16:19:15] Вычислено  $v = (g^{u1} * y^{u2} \bmod p) \bmod q = (64^{23} * 181^{62} \bmod 643) \bmod 107 = 36$

[16:19:15] Результат проверки: ПОДПИСЬ ВЕРНА

8



Проверки на ошибки:

DSA Цифровая Подпись

ФайлПомощь

Алгоритм DSA

Параметры DSA

q: q должно быть простым числом

1

p: p должно быть простым числом

1

h: h должно быть в диапазоне (1, p-1)

1

x: x должно быть в диапазоне (0, q)

1

k: k должно быть в диапазоне (0, q)

1

Подписать

Проверить

Файл успешно загружен

Text Document.txt

Содержимое файла

Испуганный ёж

Ваши действия:

Результаты вычислений:

Хеш сообщения:

Значение g:

Значение s:

Значение g:

Значение y:

Результат проверки:

Лог вычислений:

[12:06:52] Загружен файл: H:\bsuir\4sem\ti\ТИ\_2025\Задание №4\_ЭЦП\файлы для шифрования\Text Document.txt

DSA Цифровая Подпись

ФайлПомощь

Алгоритм DSA

Параметры DSA

q: q должно быть простым числом

1

p: p является простым числом и (p-1) делится на k

101

h: h должно быть в диапазоне (1, p-1)

1

x: x должно быть в диапазоне (0, q)

1

k: k должно быть в диапазоне (0, q)

1

Подписать

Проверить

Файл успешно загружен

Text Document.txt

Содержимое файла

Испуганный ёж

Ваши действия:

Результаты вычислений:

Хеш сообщения:

Значение g:

Значение s:

Значение g:

Значение y:

Результат проверки:

Лог вычислений:

[12:06:52] Загружен файл: H:\bsuir\4sem\ti\ТИ\_2025\Задание №4\_ЭЦП\файлы для шифрования\Text Document.txt

DSA Цифровая Подпись

ФайлПомощь

Алгоритм DSA

Параметры DSA

q: q является простым числом

643

p: p является простым числом, но (p-1) не делится

43

h: h должно быть в диапазоне (1, p-1)

1

x: x должно быть в диапазоне (0, q)

1

k: k должно быть в диапазоне (0, q)

1

Подписать

Проверить

Файл успешно загружен

Text Document.txt

Содержимое файла

Испуганный ёж

Ваши действия:

Результаты вычислений:

Хеш сообщения:

Значение г:

Значение s:

Значение g:

Значение у:

Результат проверки:

Лог вычислений:

[12:06:52] Загружен файл: H:\bsuir\4sem\ti\ТИ\_2025\Задание №4\_ЭЦП\файлы для шифрования\Text Document.txt