

УО «Белорусский государственный университет информатики и
радиоэлектроники»
Кафедра ПОИТ

Отчет по лабораторной работе №4
по предмету «Теория информации»
Вариант 2

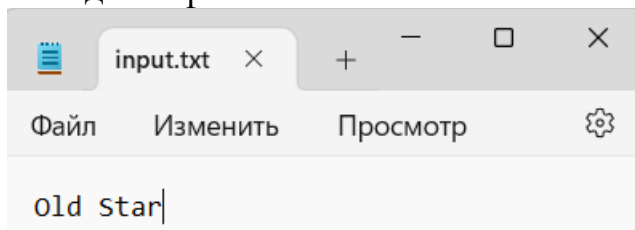
Выполнил:
Брезгунов Ю.А.

гр. 351003
Проверила:
Болтак С.В.

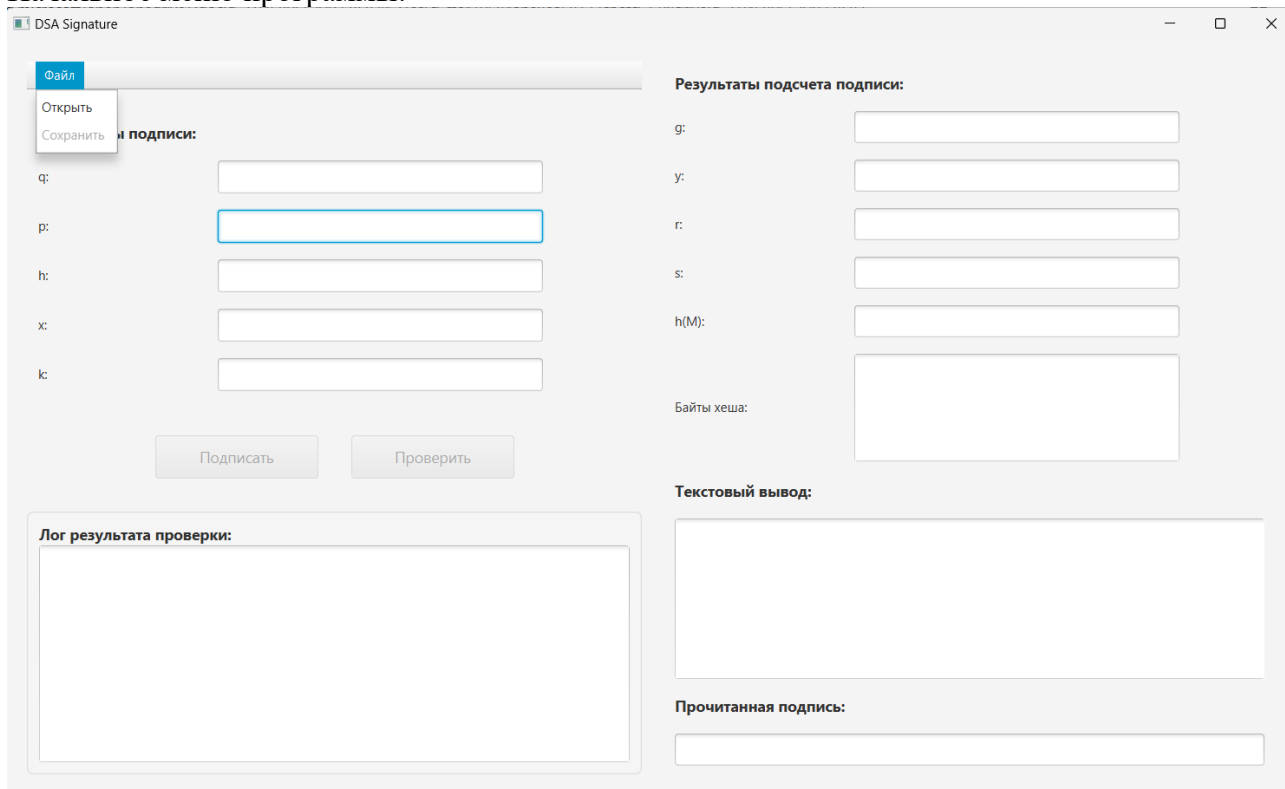
Минск 2025

Примеры работы программы

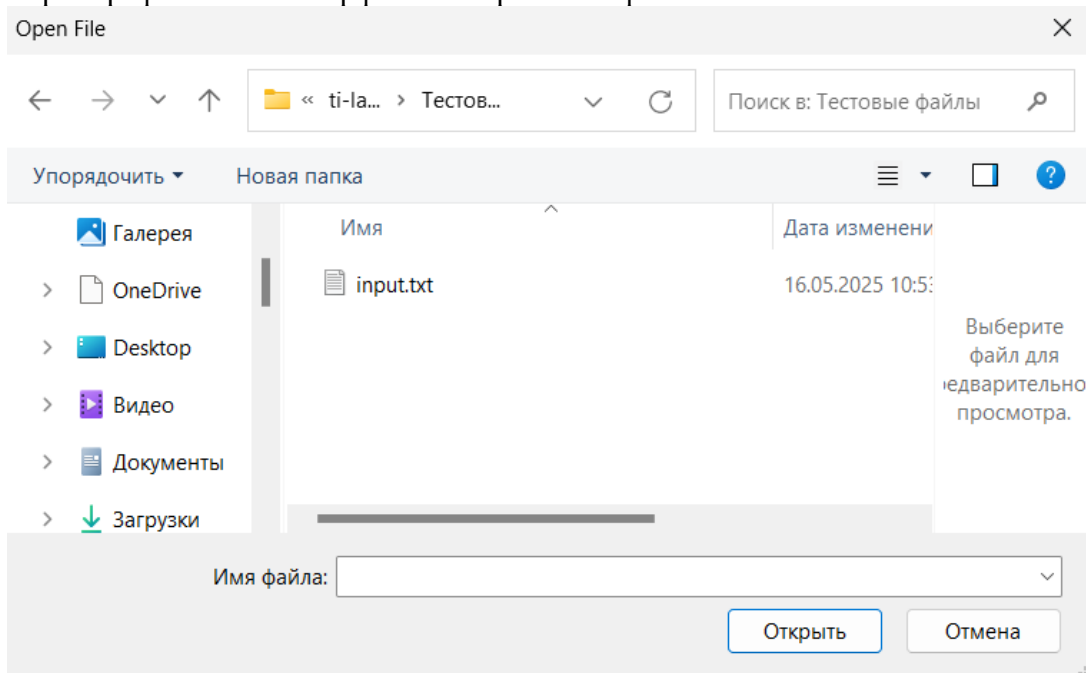
Исходный файл:



Начальное меню программы:



Через графический интерфейс выберем наш файл:



Файл открыт:

Файл

Параметры подписи:

q:

127

r:

509

h:

52

x:

19

k:

84

Подписать

Проверить

Лог результата проверки:

Результаты подсчета подписи:

g:

y:

r:

s:

h(M):

Байты хеша:

Текстовый вывод:

Old Star

[79, 108, 100, 32, 83, 116, 97, 114]

Прочитанная подпись:

В файле нет подписи или она была изменена и записана в неправильном формате

Программа всегда пытается найти в файле подпись, но так как ее сейчас нет, появляется надпись “В файле нет подписи или она была изменена и записана в неправильном формате” и кнопка проверить становится неактивной.

Подпишем файл:

Файл

Параметры подписи:

q:

127

r:

509

h:

52

x:

19

k:

84

Подписать

Проверить

Лог результата проверки:

Результаты подсчета подписи:

g:

340

y:

389

r:

123

s:

9

h(M):

70

Байты хеша:

[100, 37, 70, 71, 68, 68, 74, 31, 70]

Текстовый вывод:

Old Star

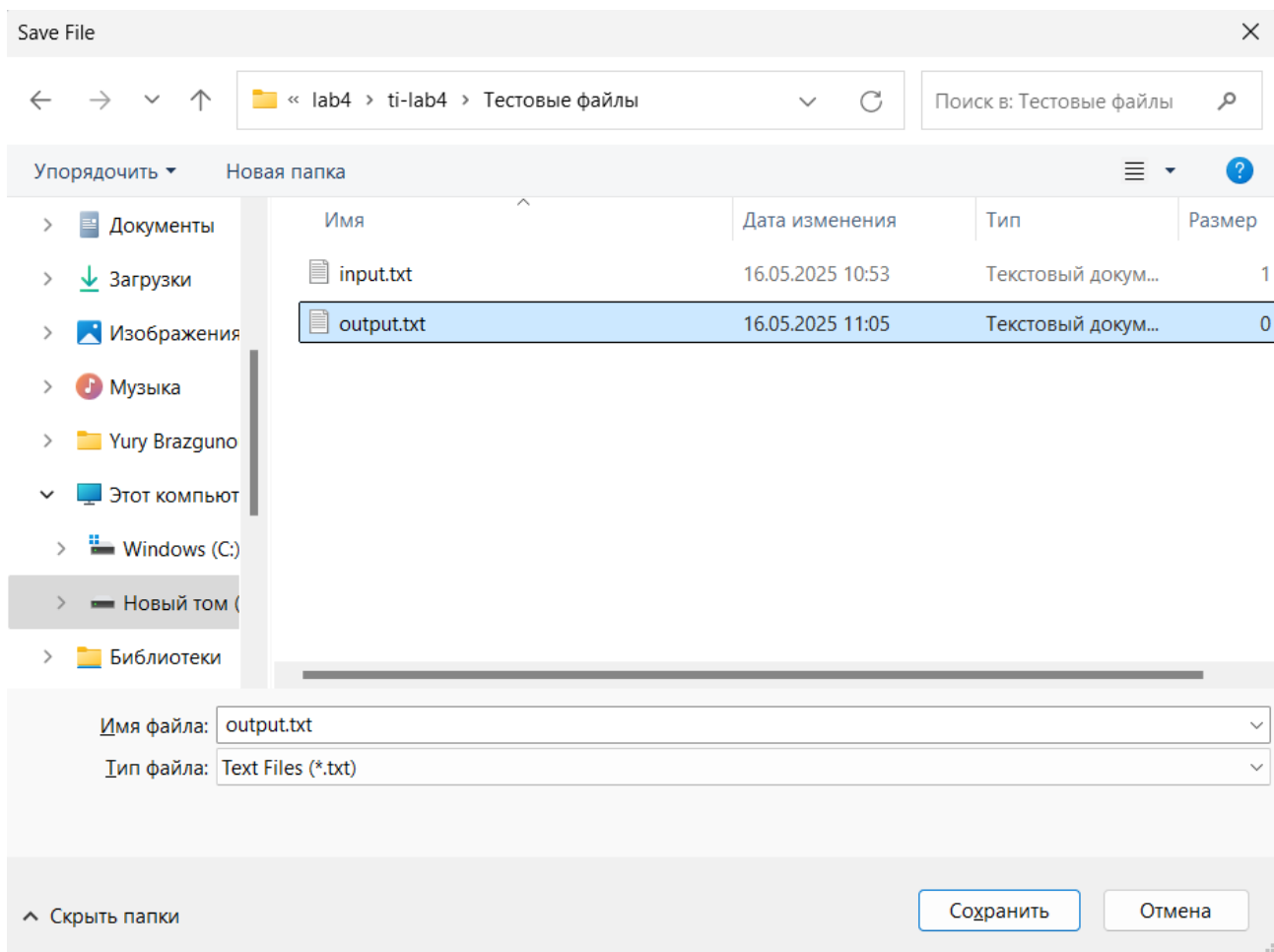
[79, 108, 100, 32, 83, 116, 97, 114]

Прочитанная подпись:

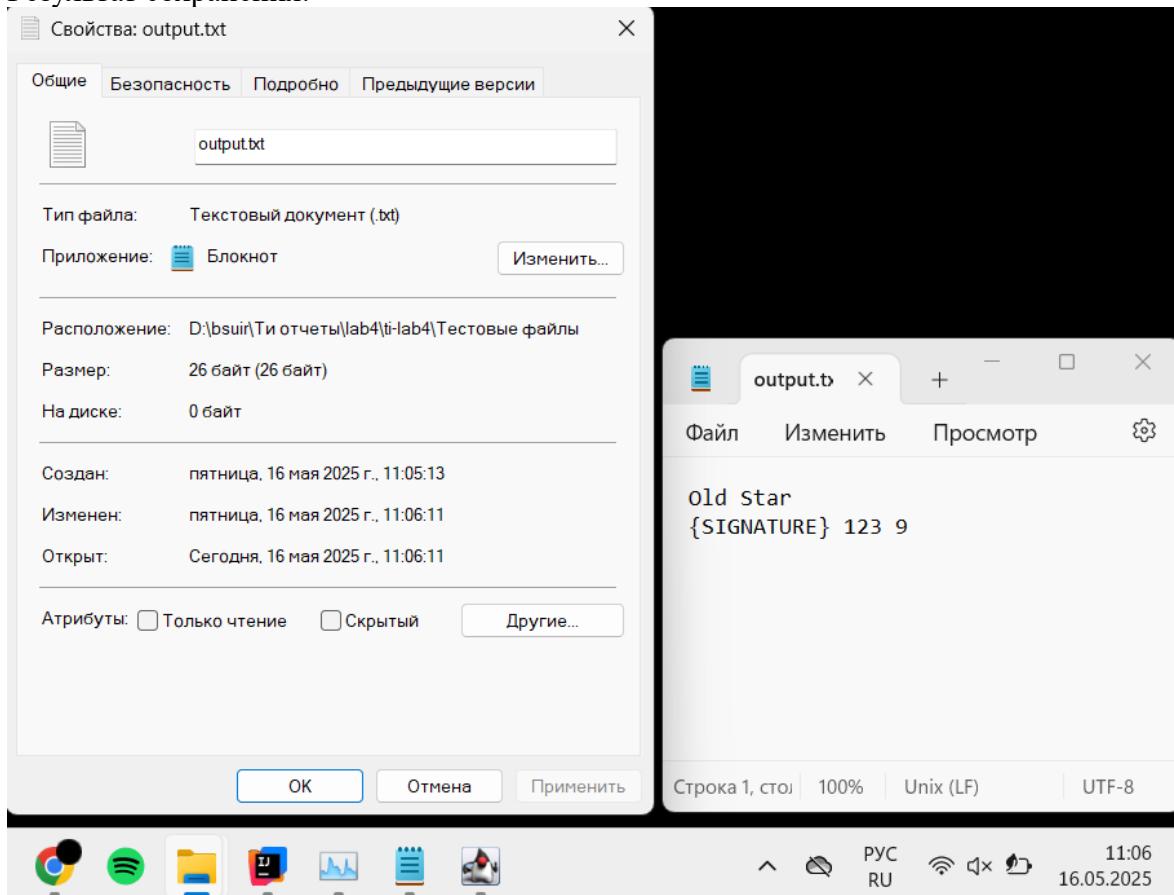
В файле нет подписи или она была изменена и записана в неправильном формате

Результат подписи: $r = 123$, $s = 9$

Теперь сохраним, выбрав файл через графический интерфейс:



Результат сохранения:



Откроем этот файл для проверки:

DSA Signature

Файл

Параметры подписи:

q:

127

p:

509

h:

52

x:

19

k:

84

Подписать

Проверить

Лог результата проверки:

Результаты подсчета подписи:

g:

y:

r:

s:

h(M):

Байты хеша:

Текстовый вывод:

Old Star

[79, 108, 100, 32, 83, 116, 97, 114]

Прочитанная подпись:

r = 123, s = 9

Как видно в правом нижнем углу, подпись была прочитана.
Теперь проверим ее:

DSA Signature

Файл

Параметры подписи:

q:

127

p:

509

h:

52

x:

19

k:

84

Подписать

Проверить

Лог результата проверки:

g = 340 // $g = h^{\frac{(p-1)}{q}} \bmod p$
y = 389 // $y = g^x \bmod p$
hash = 70 // h(M)
w = 113 // $w = s^{-1} \bmod q$
u1 = 36 // $u1 = \text{hash} * w \bmod q$
u2 = 56 // $u2 = r * w \bmod q$
v = 123 // $v = (g^{u1} * y^{u2} \bmod p) \bmod q$
r из файла = 123
Результат: Подпись ВЕРНА

Результаты подсчета подписи:

g:

y:

r:

s:

h(M):

Байты хеша:

Текстовый вывод:

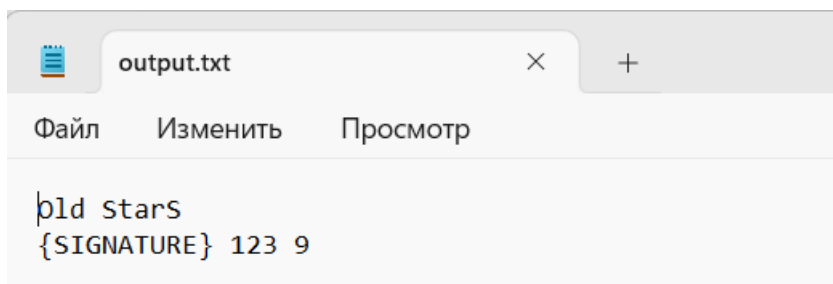
Old Star

[79, 108, 100, 32, 83, 116, 97, 114]

Прочитанная подпись:

r = 123, s = 9

Так как r из файла и v совпали, то подпись верна.
А теперь изменим файл с результатом (добавим S в конец строки):



И откроем:

DSA Signature

Файл

Параметры подписи:

q: 127

p: 509

h: 52

x: 19

k: 84

Подписать Проверить

Результаты подсчета подписи:

g:

y:

r:

s:

h(M):

Байты хеша:

Текстовый вывод:

Old StarS
[79, 108, 100, 32, 83, 116, 97, 114, 83]

Прочитанная подпись:

r = 123, s = 9

Лог результата проверки:

```
g = 340 // g = h^((p-1)/q) mod p  
y = 389 // y = g^x mod p  
hash = 41 // h(M)  
w = 113 // w = s^(-1) mod q  
u1 = 61 // u1 = hash * w mod q  
u2 = 56 // u2 = r * w mod q  
v = 82 // v = (g^u1 * y^u2 mod p) mod q  
r из файла = 123  
Результат: Подпись НЕВЕРНА
```

Как можно заметить, даже при тех же числах подпись неверна, так как поменялся хэш входной строки.

Также в программе есть проверки на ввод, например:

Параметры подписи:

q: 127

p: 510

h: 52

x: 19

k: 84

Error

Число p не простое

OK