

Министерство образования Республики Беларусь  
Учреждение образования  
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей  
Кафедра программного обеспечения информационных технологий  
Дисциплина: ТИ (Теория информации)

**ОТЧЕТ**

по лабораторной работе № 4

Тема работы: Электронная цифровая подпись

Выполнил: гр. 951007

Воривода М.А.

Проверила:

Болтак С.В.

Минск 2021

# 1 SMOKE TEST

Проверка генерации ключей:

The application window titled 'Hello World' displays a list of generated keys on the left and input fields for a smoke test on the right. The keys are listed under 'Generated keys:' and include 'Public key:', 'P:', 'Q:', 'G:', 'Y:', 'PrivateKey:', and 'X:'. The input fields on the right are labeled Q, P, H, X, and K, and contain the following values: Q: 114560275297247836437898080638808651223, P: 3436808258917435093136942419164259536691, H: 262097917507958104295857333033617637090, X: 30980432227442833091117688752871914136, K: 68742727337159965319440006850336405388. Below the input fields is a 'Path to file...' field with a 'Browse' button. At the bottom, there are radio buttons for 'Custom hasher' (selected) and 'SHA1', and buttons for 'Sign', 'Check sign', and 'Generate keys'.

Generated keys:

Public key:

P:

3436808258917435093136  
942419164259536691

Q:

1145602752972478364378  
98080638808651223

G:

7038160319246564642037  
94776237969911471

Y:

1547376832280941481284  
216331981530076700

PrivateKey:

X:

3098043222744283309111  
7688752871914136

Q: 114560275297247836437898080638808651223

P: 3436808258917435093136942419164259536691

H: 262097917507958104295857333033617637090

X: 30980432227442833091117688752871914136

K: 68742727337159965319440006850336405388

Path to file...

Browse

☒ Custom hasher ☐ SHA1 Sign Check sign Generate keys

Проверка введённых значений:

The application window titled 'Hello World' displays the same generated keys as the previous screenshot. The input fields on the right now contain the following values: Q: 2, P: 8, H: 2, X: 4, K: 5. Below the input fields, a red error message is displayed: 'P is not prime; Q must be divider of P - 1; 0 < X < Q; 0 < K...'. The 'Path to file...' field and the bottom buttons remain the same.

Generated keys:

Public key:

P:

3436808258917435093136  
942419164259536691

Q:

1145602752972478364378  
98080638808651223

G:

7038160319246564642037  
94776237969911471

Y:

1547376832280941481284  
216331981530076700

PrivateKey:

X:

3098043222744283309111  
7688752871914136

Q: 2

P: 8

H: 2

X: 4

K: 5

P is not prime; Q must be divider of P - 1; 0 < X < Q; 0 < K...

Path to file...

Browse

☒ Custom hasher ☐ SHA1 Sign Check sign Generate keys

Подпись:

The text editor window titled 't.txt - Блокнот' shows the text 'BSUIR' in the main editing area. The menu bar includes 'Файл', 'Правка', and 'Формат'.

t.txt - Блокнот

Файл Правка Формат

BSUIR

Generated keys:  
Public key:  
P: 3436808258917435093136942419164259536691  
Q: 114560275297247836437898080638808651223  
G: 703816031924656464203794776237969911471  
Y: 1547376832280941481284216331981530076700  
PrivateKey:  
X: 30980432227442833091117688752871914136  
Generated keys:  
Public key:  
P: 52517099013000866350669657961385193212653  
Q: 320226213493907721650424743666982885443  
G: 10386245474874180417511911952252106826096  
Y: 10962370161180942953198612432344774676872  
PrivateKey:  
X: 193509915540233883608806970792700480456  
Hash generated: 188944726004275060637132076065686874327 for text:  
"BSUIR"  
Digital sign:  
r: 210328875776324633813983462320224049179  
s: 77069555820415535294233707680576231303

Q: 320226213493907721650424743666982885443

P: 52517099013000866350669657961385193212653

H: 115184872714442658914256166427296078087

X: 193509915540233883608806970792700480456

K: 76476764333478216355958048785576027758

D:\University\TI\Lab4FX\t.txt

Browse

☒ Custom hasher ☐ SHA1

Sign

Check sign

Generate keys

t\_signed.txt – Блокнот

Файл Правка Формат Вид Справка

210328875776324633813983462320224049179 77069555820415535294233707680576231303;BSUIR

Проверка подписи (верно):

Generated keys:  
Public key:  
P: 3436808258917435093136942419164259536691  
Q: 114560275297247836437898080638808651223  
G: 703816031924656464203794776237969911471  
Y: 1547376832280941481284216331981530076700  
PrivateKey:  
X: 30980432227442833091117688752871914136  
Generated keys:  
Public key:  
P: 52517099013000866350669657961385193212653  
Q: 320226213493907721650424743666982885443  
G: 10386245474874180417511911952252106826096  
Y: 10962370161180942953198612432344774676872  
PrivateKey:  
X: 193509915540233883608806970792700480456  
Hash generated: 188944726004275060637132076065686874327 for text:  
"BSUIR"  
Digital sign:  
r: 210328875776324633813983462320224049179  
s: 77069555820415535294233707680576231303  
Hash generated: 188944726004275060637132076065686874327 for text:  
"BSUIR"  
Checking sign:  
w: 34287289165949124070390282618521171478  
u1: 17207539046838638914612227690841680098  
u2: 235514470416547545115016205402842029893  
v: 210328875776324633813983462320224049179

Q: 320226213493907721650424743666982885443

P: 52517099013000866350669657961385193212653

H: 115184872714442658914256166427296078087

X: 193509915540233883608806970792700480456

K: 76476764333478216355958048785576027758

D:\University\TI\Lab4FX\t\_signed.txt

Browse


☒ Custom hasher ☐ SHA1

Sign

Check sign

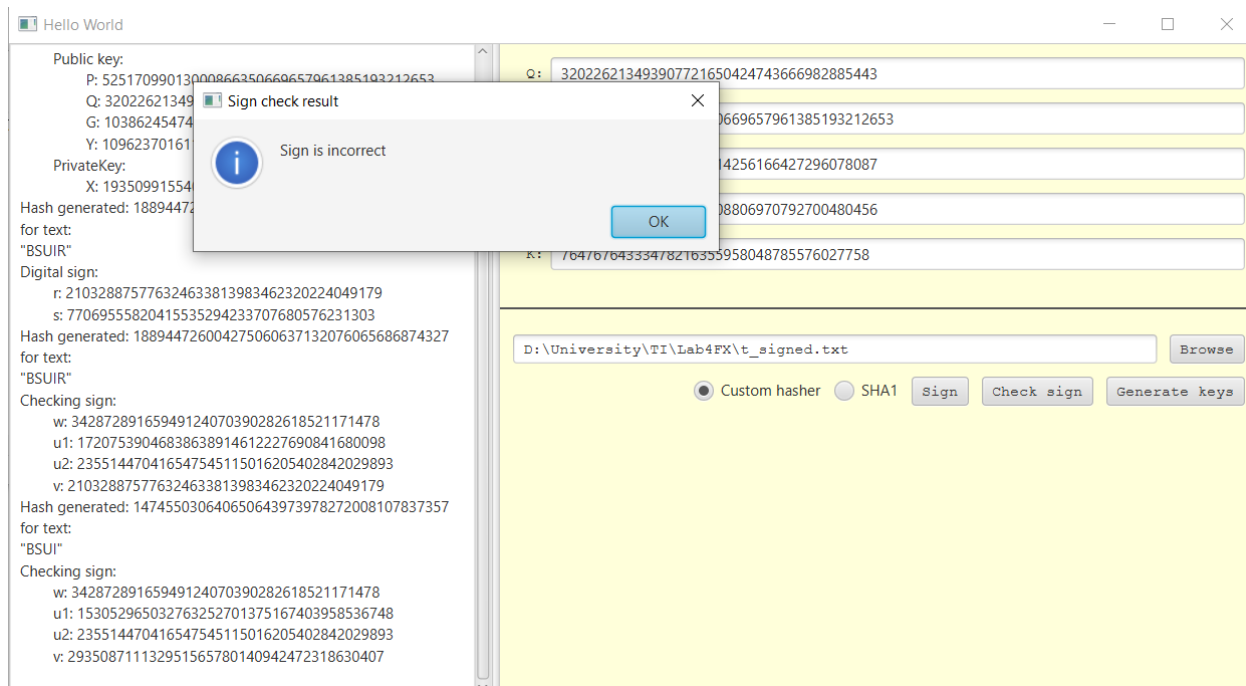
Generate keys

Sign check result

 Sign is correct

OK

Проверка подписи (неверно: исходное сообщение было изменено на «BSUI»):



## 2 РАСЧЁТЫ

### Быстрое возведение в степень

$$3^5 \bmod p = 3^5 \bmod 7$$
$$p - 1 = 6_{10} = 110_2$$

Степень 0:  $(1 \cdot 3) \bmod 7 = 3$

Степень 1:  $(3 \cdot 3) \bmod 7 = 2$

Степень 2:  $(2 \cdot 3) \bmod 7 = 6$

Степень 3:  $(6 \cdot 3) \bmod 7 = 4$

Степень 4:  $(4 \cdot 3) \bmod 7 = 5$

Степень 5:  $(5 \cdot 3) \bmod 7 = 1$

### Первообразный корень по модулю

Первообразный корень  $g$  по модулю  $m$  – это такое целое число, что

$$g^{\varphi(m)} = 1 \bmod m$$
$$g^l \neq 1 \bmod m, 1 \leq l < \varphi(m)$$

Нахождение первообразного корня по модулю 13.

$$\varphi(13) = 13 - 1 = 12 = 2 \cdot 2 \cdot 3$$
$$l = \{6, 4\}$$

$$g \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

$$1^6 \bmod 13 = 1, 1^4 \bmod 13 = 1$$

$$\mathbf{2^6 \bmod 13 = 12, 2^4 \bmod 13 = 3}$$

$$3^6 \bmod 13 = 1, 3^4 \bmod 13 = 3$$

$$4^6 \bmod 13 = 1, 4^4 \bmod 13 = 9$$

$$5^6 \bmod 13 = 12, 5^4 \bmod 13 = 1$$

$$\mathbf{6^6 \bmod 13 = 12, 6^4 \bmod 13 = 9}$$

$$\mathbf{7^6 \bmod 13 = 12, 7^4 \bmod 13 = 9}$$

$$8^6 \bmod 13 = 12, 8^4 \bmod 13 = 1$$

$$9^6 \bmod 13 = 1, 9^4 \bmod 13 = 9$$

$$10^6 \bmod 13 = 1, 10^4 \bmod 13 = 3$$

$$\mathbf{11^6 \bmod 13 = 12, 11^4 \bmod 13 = 12}$$

$$12^6 \bmod 13 = 1, 12^4 \bmod 13 = 1$$

## Расширенный алгоритм Евклида

Расширенный алгоритм Евклида позволяет найти наибольший общий делитель и коэффициенты из леммы Безу. Лемма Безу гласит о том, что для любых целых чисел  $a$  и  $b$  есть такие целые числа  $x$  и  $y$ , для которых верно равенство  $a * x + b * y = (a, b)$ .

Пусть  $a = 36$ ,  $b = 25$ . НОД( $a$ ,  $b$ ) = 1

$$x_n = x_{n-2} - q * x_{n-1}$$

$$y_n = y_{n-2} - q * y_{n-1}$$

<b>q</b>	<b>a</b>	<b>b</b>	<b>r</b>	<b>x<sub>n</sub></b>	<b>y<sub>n</sub></b>
-	36	25	-	1	0
-	36	25	-	0	1
1	36	25	11	1	-1
2	25	11	3	-2	3
3	11	3	2	7	-10
1	3	2	<b>1</b>	<b>-9</b>	<b>13</b>
2	2	1	<b>0</b>	-	-

$$-9 * 36 + 13 * 25 = -324 + 325 = 1$$