Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Дисциплина: Теория информации (ТИ)

ОТЧЕТ

По лабораторной работе №4

Тема работы: Электронная цифровая подпись

Выполнил

студент: гр. 051007 Захаренко Н.А.

Проверил: Болтак С.В.

Минск 2022

**ЭЦП\_DSA**

**Тест 1:**

<Файл пуст>

Хеш-функция: H(m) = H0 = 100

q= 433

p=19919 (p-1=19918=2\*23\*433)

h= 2, тогда g=8489, h принадлежит [2,p-2], при этом g>1.

x=11, x принадлежит [1,q-1], тогда y=gx mod p

Открытый ключ - p, q, y, закрытый - x.

k= 17, k принадлежит [1,q-1].

**ЭЦП:**

r = 5

s = 111

**Проверка:**

w = 394

u1 = 430

u2 = 238

v = 5

v = r = 5

**Тест 2:**

BSUIR

Хеш-функция: H(m) = 74

q= 593

p= 3559 (p-1=3558=2\*3\*593)

h= 3, тогда g= 729 , h принадлежит [2,p-2], при этом g>1.

x=17, x принадлежит [1,q-1], тогда y= 2201

k= 23, k принадлежит [1,q-1].

**ЭЦП:**

r = 250

s = 188

**Проверка:**

w = 552

u1 = 524

u2 = 424

v = 250

v = r = 250

**Тест 3:**

<Фотография>

Хеш-функция: H(m) = 177

q= 277

p= 9973 (p-1=9972=2\*2\*3\*3\*277)

h= 2, тогда g= 1640 , h принадлежит [2,p-2], при этом g>1.

x=100, x принадлежит [1,q-1], тогда y= 9002

k= 50, k принадлежит [1,q-1].

**ЭЦП:**

r = 200

s = 121

**Проверка:**

w = 87

u1 = 164

u2 = 226

v = 200

v = r = 200