**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ**

**ГОМЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ П. О. СУХОГО**

Факультет автоматизированных и информационных систем

Кафедра «Информатика»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 4

по дисциплине **«Основы защиты информации»**

на тему: **«**Электронная цифровая подпись**»**

Выполнила: студентка гр. ИП-32

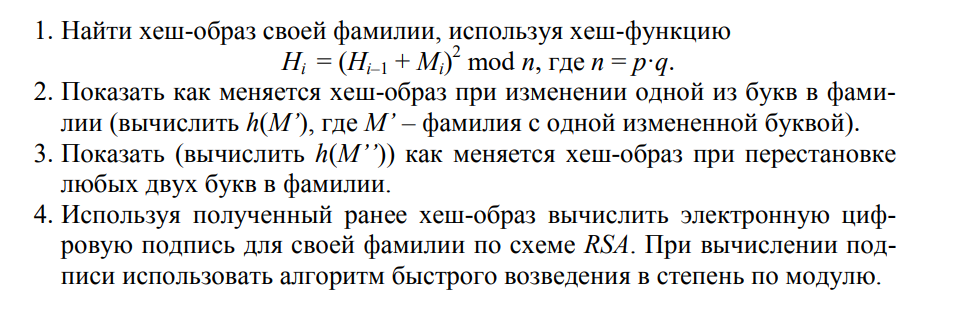
Суховенко Э.С.

Принял: профессор Кудин В.П.

Гомель 2022

**Цель работы:** изучить принципы формирования электронной цифровой подписи.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ





1)

Вычислим хеш-образ для слова “суховенко”  
М принимает вид М = {19, 21, 23, 16, 3, 6, 15, 12, 16}

q = 7

p = 23

n = p \* q = 7 \* 23 = 161

Положим, что

Таким образом h(M) = = 32

2)

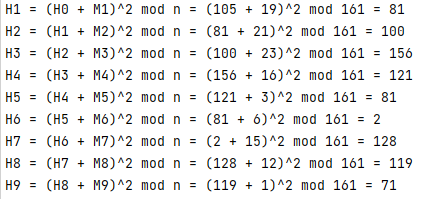
Вычислим хеш-образ для слова “суховенка”  
М принимает вид М = {19, 21, 23, 16, 3, 6, 15, 12, 1}

q = 7

p = 23

n = p \* q = 7 \* 23 = 161

Положим, что



Таким образом h(M) = = 71

3)

Вычислим хеш-образ для слова “суховенок”  
М принимает вид М = {19, 21, 23, 16, 3, 6, 15, 16, 12}

q = 7

p = 23

n = p \* q = 7 \* 23 = 161

Положим, что

Таким образом h (M``) = = 119

4)

q = 7

p = 23

n = p \* q = 7 \* 23 = 161

Выберем секретный ключ КC, который является взаимно простым с

НОД(5, 132) = 1

Вычисление цифровой подписи сообщения для сообщения

Проверка действительности полученного сообщения с подписью {M’, S}

M = суховенко

S = 2

*Доказано*

**Вывод:** В ходе выполнения данной лабораторной работы были изучены принципы работы криптосистемы с открытым ключом на основе алгоритма RSA.