**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

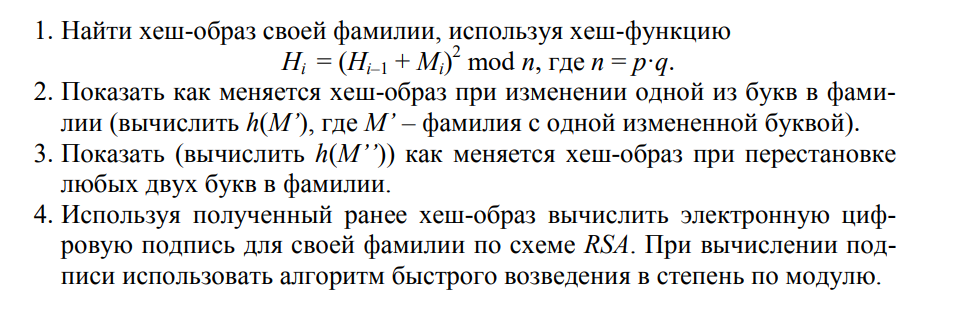
Кирпиченко Д.Д.

Принял: профессор Кудин В.П.

Гомель 2022

Цель работы: Изучить принципы формирования электронной цифровой подписи.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ



3. p=19, q=11

1)

Вычислим хеш-образ для слова “Кирпиченко”  
М принимает вид М = {12, 10,18, 17, 10, 25, 6,15,12,16}

q = 19

p = 11

n = p \* q = 19 \* 11 = 209

Положим, что

Таким образом h(M) = = 196

2)

Вычислим хеш-образ для слова “Кирпиченка”  
М принимает вид М = {12, 10,18, 17, 10, 25, 6,15,12,1}

q = 19

p = 11

n = p \* q = 19\* 11 = 209

Положим, что

Таким образом h (M`) = = 115

3)

Вычислим хеш-образ для слова “Кирпиченок”  
М принимает вид М = {12, 10,18, 17, 10, 25, 6,15,16,12}

q = 19

p = 11

n = p \* q = 19 \* 11 = 209

Положим, что

Таким образом h (M``) = = 47

4)

q = 19

p = 11

n = p \* q = 19 \* 11 = 209

Выберем секретный ключ КC, который является взаимно простым с

*Проверка:*

Вычисление цифровой подписи сообщения для сообщения

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

M’ = Кирпиченко

= 196

*Доказано*

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