**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»

Вариант 15

Выполнил: студент гр. ИП-31

Коваленко А.И

Принял: профессор

Кудин В. П.

Гомель 2023

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

**Задания:**

1. Найти хеш-образ своей фамилии, используя хеш-функцию Hi = (Hi–1 + Mi)^2 mod n, где n = p·q.
2. Показать как меняется хеш-образ при изменении одной из букв в фамилии (вычислить h(M’), где M’ – фамилия с одной измененной буквой).
3. Показать (вычислить h(M’’)) как меняется хеш-образ при перестановке любых двух букв в фамилии.
4. Используя полученный ранее хеш-образ вычислить электронную цифровую подпись для своей фамилии по схеме RSA. При вычислении подписи использовать алгоритм быстрого возведения в степень по модулю.

**Вариант 15**

p=7, q=31

**ХОД РАБОТЫ**

|  |
| --- |
| 15. p=7, q=31 |

**Задание 1.** Найти хеш-образ своей фамилии, используя хеш-функцию

где *n = pq = 217.*

Фамилия – К О В А Л Е Н К О

12 16 3 1 13 6 15 12 16

Пронумеруем буквы:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **К** | **О** | **В** | **А** | **Л** | **Е** | **Н** | **К** | **О** |
| 12 | 16 | 3 | 1 | 13 | 6 | 15 | 12 | 16 |

**211**.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **К** | **О** | **В** | **А** | **Л** | **Е** | **Н** | **К** | **О** |
| 12 | 16 | 3 | 1 | 13 | 6 | 15 | 12 | 16 |
| 144 | 211 | 9 | 100 | 183 | 133 | 204 | 1 | 72 |

**Задание 2.** Показать как меняется хеш-образ при изменении одной из букв в фамилии (вычислить h(M’), где M’ – фамилия с одной измененной буквой).

Фамилия – К О В А Л Е **К** К О

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **К** | **О** | **В** | **А** | **Л** | **Е** | **К** | **К** | **О** |
| 12 | 16 | 3 | 1 | 13 | 6 | 12 | 12 | 16 |
| 144 | 211 | 9 | 100 | 183 | 133 | **193** | **144** | **211** |

**Задание 3.** Показать (вычислить h(M’’)) как меняется хеш-образ при перестановке любых двух букв в фамилии.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **К** | **О** | **В** | **А** | **О** | **Е** | **Н** | **К** | **Л** |
| 12 | 16 | 3 | 1 | 16 | 6 | 15 | 12 | 13 |
| 144 | 211 | 9 | 100 | 183 | 133 | 193 | 144 | 211 |

H1...

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **К** | **О** | **В** | **А** | **О** | **Е** | **Н** | **К** | **Л** |
| 12 | 16 | 3 | 1 | 16 | 6 | 15 | 12 | 13 |
| 144 | 211 | 9 | 100 | 2 | 64 | 165 | 81 | 1 |

**Задание 4.** Используя полученный ранее хеш-образ вычислить электронную цифровую подпись для своей фамилии по схеме RSA. При вычислении подписи использовать алгоритм быстрого возведения в степень по модулю.

180.

Пусть K0 = 7

Вычисление цифровой подписи сообщения для сообщения

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

M = коваленко

S = 9

*Доказано*

**Вывод:** успешно изучили принципы формирования электронной цифровой подписи.