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

1. Найти хеш-образ своей фамилии, используя хеш-функцию
$$H_i = (H_{i-1} + M_i)^2 \bmod n, \text{ где } n = p \cdot q.$$
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.

3. p=19, q=11

1)

Вычислим хеш-образ для слова “Кирпиченко”

M принимает вид M = {12, 10,18, 17, 10, 25, 6,15,12,16}

q = 19

p = 11

n = p * q = 19 * 11 = 209

Положим, что $H_0 = 120$

$$H1 = (H0 + M1)^2 mod\ n = (120 + 12)^2 mod\ 209 = 77$$
$$H2 = (H1 + M2)^2 mod\ n = (77 + 10)^2 mod\ 209 = 45$$
$$H3 = (H2 + M3)^2 mod\ n = (45 + 18)^2 mod\ 209 = 207$$
$$H4 = (H3 + M4)^2 mod\ n = (207 + 17)^2 mod\ 209 = 16$$
$$H5 = (H4 + M5)^2 mod\ n = (16 + 10)^2 mod\ 209 = 49$$
$$H6 = (H5 + M6)^2 mod\ n = (49 + 25)^2 mod\ 209 = 42$$
$$H7 = (H6 + M7)^2 mod\ n = (42 + 6)^2 mod\ 209 = 5$$
$$H8 = (H7 + M8)^2 mod\ n = (5 + 15)^2 mod\ 209 = 191$$
$$H9 = (H8 + M9)^2 mod\ n = (191 + 12)^2 mod\ 209 = 36$$
$$H10 = (H9 + M10)^2 mod\ n = (36 + 16)^2 mod\ 209 = 196$$

Таким образом h(M) = H_{10} = 196

2)

Вычислим хеш-образ для слова “Кирпиченка”

M принимает вид M = {12, 10,18, 17, 10, 25, 6,15,12,1}

q = 19

p = 11

n = p * q = 19* 11 = 209

Положим, что $H_0 = 120$

$$H\,1 = (H\,0 + M\,1)^2 mod\, n = (120 + 12)^2 mod\ 209 = 77$$
$$H\,2 = (H\,1 + M\,2)^2 mod\, n = (77 + 10)^2 mod\ 209 = 45$$
$$H\,3 = (H\,2 + M\,3)^2 mod\, n = (45 + 18)^2 mod\ 209 = 207$$
$$H\,4 = (H\,3 + M\,4)^2 mod\, n = (207 + 17)^2 mod\ 209 = 16$$
$$H\,5 = (H\,4 + M\,5)^2 mod\, n = (16 + 10)^2 mod\ 209 = 49$$
$$H\,6 = (H\,5 + M\,6)^2 mod\, n = (49 + 25)^2 mod\ 209 = 42$$
$$H\,7 = (H\,6 + M\,7)^2 mod\, n = (42 + 6)^2 mod\ 209 = 5$$
$$H\,8 = (H\,7 + M\,8)^2 mod\, n = (5 + 15)^2 mod\ 209 = 191$$
$$H\,9 = (H\,8 + M\,9)^2 mod\, n = (191 + 12)^2 mod\ 209 = 36$$
$$H\,10 = (H\,9 + M\,10)^2 mod\, n = (36 + 1)^2 mod\ 209 = 115$$

Таким образом h (M`) = H_{10} = 115

3)

Вычислим хеш-образ для слова “Кирпиченок”

M принимает вид M = {12, 10,18, 17, 10, 25, 6,15,16,12}

q = 19

p = 11

n = p * q = 19 * 11 = 209

Положим, что $H_0 = 120$

$$H\,1 = (H\,0 + M\,1)^2 mod\, n = (120 + 12)^2 mod\ 209 = 77$$
$$H\,2 = (H\,1 + M\,2)^2 mod\, n = (77 + 10)^2 mod\ 209 = 45$$
$$H\,3 = (H\,2 + M\,3)^2 mod\, n = (45 + 18)^2 mod\ 209 = 207$$
$$H\,4 = (H\,3 + M\,4)^2 mod\, n = (207 + 17)^2 mod\ 209 = 16$$
$$H\,5 = (H\,4 + M\,5)^2 mod\, n = (16 + 10)^2 mod\ 209 = 49$$
$$H\,6 = (H\,5 + M\,6)^2 mod\, n = (49 + 25)^2 mod\ 209 = 42$$
$$H\,7 = (H\,6 + M\,7)^2 mod\, n = (42 + 6)^2 mod\ 209 = 5$$
$$H\,8 = (H\,7 + M\,8)^2 mod\, n = (5 + 15)^2 mod\ 209 = 191$$
$$H\,9 = (H\,8 + M\,9)^2 mod\, n = (191 + 16)^2 mod\ 209 = 4$$
$$H\,10 = (H\,9 + M\,10)^2 mod\, n = (4 + 12)^2 mod\ 209 = 47$$

Таким образом h (M``) = H_{10} = 47

4)

q = 19

p = 11

n = p * q = 19 * 11 = 209

$$\varphi(n) = 180$$

Выберем секретный ключ КС, который является взаимно простым с $\phi(n)$ $К_о$ = 7

$$К_с = К_о^{\varphi(r)-1}\ mod\ \varphi(r)$$

$$К_с = 7^{179}\ mod\ 180 = 103$$

Проверка: $103 * 7\ mod\ 180 = 721\ mod\ 180 = 1$

Вычисление цифровой подписи сообщения для сообщения

$$S\ =\ h(M)^{\text{Кс}}\ mod\ r\ =\ 196\text{^}103 mod\ 209 = 80$$

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

M' = Кирпиченко

$m' = h(M') = 196$

$$m = S^{Ko}\ mod\ r = 80^7\ mod\ 209 = 196$$

Доказано

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