**Лабораторная работа № 6**

**Тема:** «Исследование криптографических хэш-функций».

**Цель:** отработать навыки вычисления хэш-функций.

Задание 1.

1. Вычислите НОД (m, n) по алгоритму Евклида.

m=1092, n=689;

m = n\*q + r

m = 1092, n = 689, q = 1, r = 403

1092 = 689\*1 + 403

НОД (m, n) = НОД (b, r)

НОД (1092, 689) = НОД (689, 403)

689 = 403\*1 + 286

НОД (689, 403) = НОД (403, 286)

403 = 286\*1 + 117

НОД (403, 286) = НОД (286, 117)

286 = 117\*2 + 52

НОД (286, 117) = НОД (117, 52)

117 = 52\*2 + 13

НОД (117, 52) = НОД (52, 13)

52 = 13\*4 + 0

Ответ: НОД (1092, 689) = 13

2. Вычислите НОД(m, n) используя бинарный алгоритм.

m=1265, n=2024;

(1265, 2024) = (1265, 1012) = (1265, 506) = (1265, 253) = (253, 1012) =  
= (253, 506) = (253, 253) = 253

Ответ: НОД (1265, 2024) = 253

3. Вычислите функцию Эйлера для n = 734 (произвольное число)

734 = 2 \* 367

φ(734) = 734 \* (1 – 1/2) \* (1 – 1/367) = 366

Ответ: 366.

4. Покажите, что ab = 1 mod n.

a=14, b=448, n=493.

14448 = 1 mod 493

НОД (14, 493) = 1

φ(493) = (17-1) \* (29-1) = 448 = b

поэтому 14448 = 1 mod 493

5. Вычислите взаимообратное число для 5 по модулю 29.

5\*m = 1 mod 29

m = 5φ(29)-1 mod 29 = 527 mod 29 = 6

Проверка: 5 \* 6 mod 29 = 30 mod 29 = 1

Ответ: 6

6. Покажите, что mn mod r = k.

m=5, n=8, r=19, k=4.

Поскольку 8 = 2\*2\*2, то 58 = ((52)2)2

52 = 25 ( 52 )

252 = 625 ( (52)2 )

6252 = 390625 ( ((52)2)2 )

52 mod 19 = 6

62 mod 19 = 17

172 mod 19 = 4 (= k)

Задание 2.

1. Найти хеш-образ своей фамилии, используя хеш-функцию  
Hi= (Hi–1 + Mi)2 mod n, где n = p·q.

p=5, q=31, n=p\*q=155

M = МИКУЦЕВИЧ, M = {13, 9, 11, 20, 23, 5, 2, 9, 24}

H0 = 100

H1 = (100 + 13)² mod 155 = 59

H2 = (59 + 9)² mod 155 = 129

H3 = (129 + 11)² mod 155 = 70

H4 = (70 + 20)² mod 155 = 40

H5 = (40 + 23)² mod 155 = 94

H6 = (94 + 5)² mod 155 = 36

H7 = (36 + 2)² mod 155 = 49

H8 = (49 + 9)² mod 155 = 109

H9 = (109 + 24)² mod 155 = 19

Таким образом h(M) = H9 = 19

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

p=5, q=31, n=p\*q=155

M = МИКУЛЕВИЧ, M = {13, 9, 11, 20, 12, 5, 2, 9, 24}

H0 = 100

H1 = (100 + 13)² mod 155 = 59

H2 = (59 + 9)² mod 155 = 129

H3 = (129 + 11)² mod 155 = 70

H4 = (70 + 20)² mod 155 = 40

H5 = (40 + 12)² mod 155 = 69

H6 = (69 + 5)² mod 155 = 51

H7 = (51 + 2)² mod 155 = 19

H8 = (19 + 9)² mod 155 = 9

H9 = (9 + 24)² mod 155 = 4

Значит хеш-образ изменился на 15 при изменении одной буквы.

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

p=5, q=31, n=p\*q=155

M = МИУКЛЕВИЧ, M = {13, 9, 20, 11, 12, 5, 2, 9, 24}

H0 = 100

H1 = (100 + 13)² mod 155 = 59

H2 = (59 + 9)² mod 155 = 129

H3 = (129 + 20)² mod 155 = 36

H4 = (36 + 11)² mod 155 = 39

H5 = (39 + 12)² mod 155 = 121

H6 = (121 + 5)² mod 155 = 66

H7 = (66 + 2)² mod 155 = 129

H8 = (129 + 9)² mod 155 = 134

H9 = (134 + 24)² mod 155 = 9

Таким образом h(M) = H9 = 9

Хеш-образ изменился на 5 при перестановке двух букв.

4. Используя полученный ранее хеш-образ вычислить электронную цифровую подпись для своей фамилии по схеме RSA.

p=5, q=31, тогда модуль равен n=p\*q=155

Ключ d выбираем из условий, что n и d не имеют общих делителей.

Пусть d = 21.

Хеш-образ равен 9, а ключ равен (21, 9). Тогда электронная цифровая подпись вычисляется:

S=921 mod 155 = 39.

0000 – 0

0001 – 1

0010 – 2

0011 – 3

0100 – 4

0101 – 5

0110 – 6

0111 – 7

1000 – 8

1001 – 9

1010 – A

1011 – B

1100 – C

1101 – D

1110 – E

1111 – F

Таблица 1

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A3 69 2C | | | | | | | | |
| 1 | 0 | 1 | 0 |  | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| **1** | **1** | **1** | **0** | **0** | **1** | **1** | **0** |
| E6 | | | | | | | | |

Таблица 2

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10 BE 57 | | | | | | | | |
| 0 | 0 | 0 | 1 |  | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| **1** | **1** | **1** | **1** | **1** | **0** | **0** | **1** |
| F9 | | | | | | | | |

Таблица 3

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DA 14 90 | | | | | | | | |
| 1 | 1 | 0 | 1 |  | 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| **0** | **1** | **0** | **1** | **1** | **1** | **1** | **0** |
| 5E | | | | | | | | |

Таблица 4

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9E A6 23 | | | | | | | | |
| 1 | 0 | 0 | 1 |  | 1 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| **0** | **0** | **0** | **1** | **1** | **0** | **1** | **1** |
| 1B | | | | | | | | |

Таблица 5

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 82 0F B5 | | | | | | | | |
| 1 | 0 | 0 | 0 |  | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| **0** | **0** | **1** | **1** | **1** | **0** | **0** | **0** |
| 38 | | | | | | | | |

Таблица 6

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32 01 BF | | | | | | | | |
| 0 | 0 | 1 | 1 |  | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| **1** | **0** | **0** | **0** | **1** | **1** | **0** | **0** |
| 8C | | | | | | | | |

Контрольные вопросы.

1. Что в криптографии называется хеш-функцией?

Хеш-функция в криптографии - это математическая функция, которая преобразует входные данные произвольной длины в фиксированную длину (хеш-код) с определенными свойствами.

2. Для каких целей используются хеш-функции?

Хеш-функции используются для различных целей, включая:

- Гарантированное сохранение целостности данных: проверка, были ли данные изменены.

- Генерация уникальных идентификаторов для данных.

- Хранение паролей в безопасной форме.

- Быстрый поиск данных в хеш-таблицах.

- Цифровые подписи и аутентификация в криптографии.

3. Перечислите основные требования, предъявляемые к хеш-функциям.

Основные требования к хеш-функциям включают в себя:

- Однозначность: различным входам соответствуют различные хеши.

- Быстродействие: вычисление хеш-кода должно быть эффективным.

- Невозможность восстановления входных данных из хеш-кода (даже с знанием самого хеш-кода).

- Устойчивость к коллизиям: трудно найти два разных входа, дающих одинаковый хеш-код.

- Диффузия: малейшие изменения во входных данных должны приводить к значительным изменениям в хеш-коде.

- Равномерное распределение хеш-кодов.

4. Назовите примеры криптографических хеш-функций.

Примеры криптографических хеш-функций включают в себя SHA-256, SHA-3, MD5 (хотя MD5 считается устаревшей и небезопасной), и другие.

5. Каков российский стандарт на алгоритм формирования криптографической хеш-функции?

Российский стандарт на алгоритм формирования криптографической хеш-функции - это ГОСТ Р 34.11-2012, который описывает стандарты для российских криптографических хеш-функций, включая ГОСТ Р 34.11-94 и его более новую версию.

6. Каким образом можно использовать блочный алгоритм шифрования для формирования хеш-функции?

Блочный алгоритм шифрования можно использовать для формирования хеш-функции, например, путем применения шифрования ко входным данным и использования последнего блока (или нескольких блоков) в качестве хеш-кода. Это может быть достаточно безопасным, но стоит отметить, что обычно хеш-функции спроектированы специально для этой цели и могут обеспечивать более высокую производительность и безопасность.