**Лабораторная работа №4**
**«Хэш-функции и ЭЦП в криптографии»**

**Цель**:
получить навыки кодирования и декодирования электронно-цифровой подписи при помощи алгоритмов DSA, RSA, Эль-Гамаля, а также получить навыки в поиске и обработке хеш-образов.

## ПРАКТИЧЕСКАЯ ЧАСТЬ

**Пример 1:** Найти хеш-образ сообщения «ИНФОРМ».

**Решение:**

1. Возьмем 2 простых числа p = 13 и q = 19
2. Определим n = p * q = 13*19 = 247
3. Случайным образом выберем вектор инициализации $H_0 = 8$
4. При помощи таблицы прямого счета русского алфавита (алфавит с номерами букв) преобразуем сообщение в последовательность: (10, 15, 22, 16, 18, 14).
   Таким образом получим: $M_1 = 10$, $M_2 = 15$, $M_3 = 22$, $M_4 = 16$, $M_5 = 18$, $M_6 = 14$.
5. Используем формулу: $H_i = (H_{i-1} + M_i)^2 \bmod n$, для преобразования хеш-образа сообщения
6. Рассчитаем все хеш-образы до последнего. Последний хеш-образ – это и есть хеш-образа сообщения M

$$H_1 = (H_0 + M_1)^2 \, mod \, n = (8 + 10)^2 \, mod \, 247 = 324 \; mod 247 = 77$$
$$H_2 = (H_1 + M_2)^2 \, mod \, n = (77 + 15)^2 \, mod \, 247 = 8464 \; mod 247 = 66$$
$$H_3 = (H_2 + M_3)^2 \, mod \, n = (66 + 22)^2 \, mod \, 247 = 7744 \; mod 247 = 87$$
$$H_4 = (H_3 + M_4)^2 \, mod \, n = (87 + 16)^2 \, mod \, 247 = 10609 \; mod 247 = 235$$
$$H_5 = (H_4 + M_5)^2 \, mod \, n = (235 + 18)^2 \, mod \, 247 = \; 64009 \, mod 247 = 36$$
$$H_6 = (H_5 + M_6)^2 \, mod \, n = (36 + 14)^2 \, mod \, 247 = 2500 \; mod 247 = 30$$

7. В итоге получаем хеш-образ сообщения «ИНФОРМ» равный 30.

**Задача 1:** Найти хеш-образ сообщения, согласно своему варианту, если параметры p = 17 и q = 23.

| № Варианта | Исходное сообщение |
|---|---|
| **1.** | ЭЛЕКТРОННО ЦИФРОВАЯ ПОДПИСЬ |
| **2.** | ШИФРОВАНИЕ С ОТКРЫТЫМ КЛЮЧОМ |
| **3.** | КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ |

| | |
|---|---|
| **4.** | СЕРТИФИКАЦИЯ И ЛИЦЕНЗИРОВАНИЕ |
| **5.** | ЗАЩИТА ИНФОРМАЦИИ ПРИ ВЫВОДЕ |
| **6.** | НЕСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ |
| **7.** | ГЕНЕРАЦИЯ И РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ |
| **8.** | ТРЕБОВАНИЯ К КРИПТОСИСТЕМАМ |
| **9.** | ПРИЗНАКИ ЗАРАЖЕНИЯ КОМПЬЮТЕРА |
| **10.** | НЕДОСТАТКИ ПАРОЛЬНОЙ ЗАЩИТЫ |
| **11.** | СТЕНОГРАФИЧЕСКАЯ ИНФОРМАЦИЯ |
| **12.** | ОСОБЕННОСТИ МЕЖСЕТЕВОГО ЭКРАНА |
| **13.** | ЗАЩИТА ОТ ПОЛИМОРФНЫХ ВИРУСОВ |
| **14.** | СПОСОБЫ ЗАЩИТЫ ОТ СТЕЛС ВИРУСОВ |
| **15.** | ОПРЕДЕЛЕНИЕ ЗАГРУЗОЧНОГО ВИРУСА |
| **16.** | ЛОГИЧЕСКИЕ БОМБЫ И ЗАЩИТА ОТ НИХ |
| **17.** | СЛУЧАЙНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ |
| **18.** | ИНФОРМАЦИЯ КАК ОБЪЕКТ ЗАЩИТЫ |
| **19.** | РАБОТЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ |
| **20.** | ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ |
| **21.** | АКТУАЛЬНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ |
| **22.** | МЕТОДИКА РАЗГРАНИЧЕНИЯ ДОСТУПА |
| **23.** | СИСТЕМА ШИФРОВАНИЯ ЭЛЬ ГАМАЛЯ |
| **24.** | ХЕШ ОБРАЗ ЗАДАННОГО СООБЩЕНИЯ |
| **25.** | РАЗРАБОТКА ПЛАНА ЗАЩИТЫ СИСТЕМЫ |
| **26.** | СПОСОБЫ РАСПРОСТРАНЕНИЯ СПАМА |
| **27.** | РАЗРАБОТКА ПОЛИТИКИ БЕЗОПАСНОСТИ |
| **28.** | ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ |
| **29.** | ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ |
| **30.** | МОДУЛЬ ФИЛЬТРАЦИИ СЕТЕВОГО ТРАФИКА |

ТАБЛИЦА ПРЯМОГО СЧЁТА РУССКОГО ЯЗЫКА (АЛФАВИТА)

| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |

| Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |

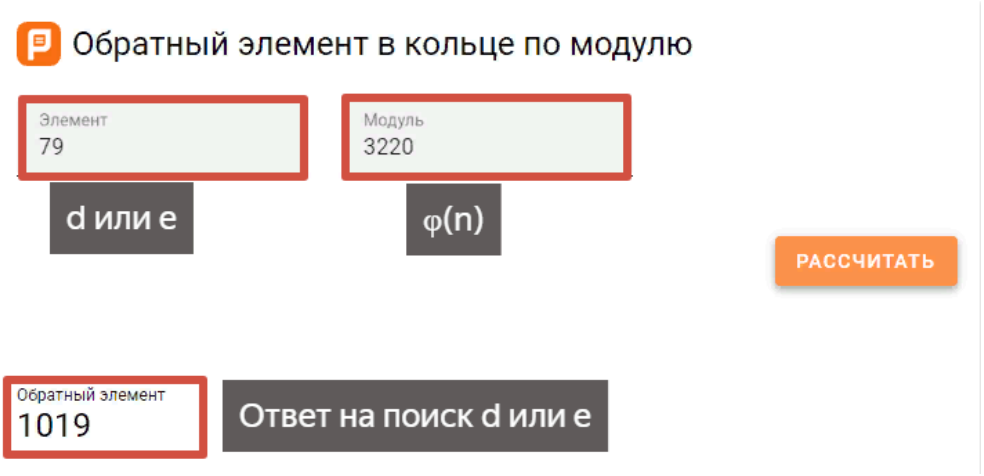
**Пример 2:** Используя хеш-образ сообщения, полученный в предыдущем задании, вычислить ЭЦП по схеме RSA.

**Решение:**

1. Хеш-образ сообщения, полученный в предыдущем задании,

равен 30

2. Пусть закрытый ключ d = 29 (Возьмем из таблицы простых чисел)
3. Тогда ЭЦП будет следующей: $s = H^d \bmod n = 30^{29} \bmod 247 = 140$
4. Рассчитаем функцию Эйлера: $\phi(n) = (p-1)(q-1) = 12 * 18 = 216$
5. Открытый ключ e можно рассчитать, используя ранее знакомый калькулятор: https://planetcalc.ru/3311/:




Если ввести ключ d и $\phi(n)$, то ключ e будет равен 149.

6. Теперь проверим ЭЦП: $H = s^e \bmod n = 140^{149} \bmod 247 = 30$
7. Видно, что хеш-образ совпал с тем, что пришел к нам из предыдущего задания, а это означает, что ЭЦП верна автору.

**Задача 2:** Используя хеш-образ сообщения, полученный в предыдущем задании, вычислить ЭЦП по схеме RSA, согласно своему варианту. Закрытый ключ возьмите из таблицы простых чисел:

**Простые числа**

| | | | | |
|---|---|---|---|---|
| 11 | 13 | 17 | 19 | 23 |
| 29 | 31 | 37 | 41 | 43 |
| 47 | 53 | 59 | 61 | 67 |
| 71 | 73 | 79 | 83 | 89 |
| 97 | 101 | 103 | 107 | 109 |
| 113 | 127 | 131 | 137 | 139 |
| 149 | 151 | 157 | 163 | 167 |
| 173 | 179 | 181 | 191 | 193 |
| 197 | 199 | 211 | 223 | 227 |
| 229 | 233 | 239 | 241 | 251 |
| 257 | 263 | 269 | 271 | 277 |
| 281 | 283 | 293 | 307 | 311 |
| 313 | 317 | 331 | 337 | 347 |
| 349 | 353 | 359 | 367 | 373 |
| 379 | 383 | 389 | 397 | 401 |
| 409 | 419 | 421 | 431 | 433 |
| 439 | 443 | 449 | 457 | 461 |
| 463 | 467 | 479 | 487 | 491 |
| 499 | 503 | 509 | 521 | 523 |
| 541 | 547 | 557 | 563 | 569 |
| 571 | 577 | 587 | 593 | 599 |

**Пример 3:** Для заданного сильно простого числа p = 607 и соответствующего простого числа q = 101, открытого текста M = 45 осуществить подписание сообщения при помощи схемы ЭЦП DSA. Остальные параметры определить самостоятельно. Проверить правильность цифровой подписи.

**Решение:**

1. Выберем закрытый ключ такой что: $1 < x < q-1$, т.е. $1 < x < 100$, например, x = 83
2. Для нахождения элемента g воспользуемся формулой: $g=h^{(p-1)/q} mod\ p$, где h любое число меньшее p-1. Если (p-1)/q получается дробной, то возьмите только целую часть!
   Пусть h = 11, тогда $g = 11^{(607-1)/101} \bmod 607 = 335$
3. Рассчитаем y: $y = g^x \bmod p = 335^{83} \bmod 607 = 348$
4. Выберем некоторое число k такое что: $1 < k < q-1$, например, k = 75
5. Для расчёта ЭЦП нужно найти $k^{-1}$: $k^{-1} \bmod q = 75^{-1} \bmod 101 = 66$ (калькулятор тот же, что в примере 2)
6. Генерация ЭЦП:
   $r = (g^k \bmod p) \bmod q = (335^{75} \bmod 607) \bmod 101 = 325 \bmod 101 = 22$
   $s = (M + x*r) * k^{-1} \bmod q = (45 + 83*22) * 66 \bmod 101 =$
   $= (45 + 1826) * 66 \bmod 101 = 123486 \bmod 101 = 64$

7. Проверка ЭЦП:
   $w = s^{-1} \bmod q = 64^{-1} \bmod 101 = 30 \bmod 101 = 30$
   $u_1 = (M * w) \bmod q = (45 * 30) \bmod 101 = 1350 \bmod 101 = 37$
   $u_2 = (r * w) \bmod q = (22 * 30) \bmod 101 = 54$
   $a = ((g^{u1} * y^{u2}) \bmod p) \bmod q = ((335^{37} * 348^{54}) \bmod 607) \bmod 101 =$
   $= ((247 * 193) \bmod 607) \bmod 101 = 325 \bmod 101 = 22$
8. Получаем, что a = r, т.е. 22 = 22, а, следовательно, ЭЦП верна.

**Задача 3:** Для заданного сильно простого числа p и соответствующего простого числа q, открытого текста M и порождающего элемента g, согласно своему варианту самостоятельно определить остальные параметры схемы ЭЦП DSA и осуществить подписание сообщения. Проверить правильность цифровой подписи.

| Варианты | p | q | M |
|---|---|---|---|
| **1** | 101 | 11 | 5 |
| **2** | 103 | 13 | 6 |
| **3** | 107 | 17 | 7 |
| **4** | 109 | 19 | 8 |
| **5** | 113 | 23 | 9 |
| **6** | 127 | 29 | 4 |
| **7** | 131 | 31 | 5 |
| **8** | 137 | 37 | 6 |
| **9** | 139 | 41 | 7 |
| **10** | 149 | 43 | 8 |
| **11** | 151 | 47 | 9 |

| Варианты | p | q | M |
|---|---|---|---|
| **12** | 157 | 53 | 10 |
| **13** | 163 | 59 | 11 |
| **14** | 167 | 61 | 12 |
| **15** | 173 | 67 | 13 |
| **16** | 179 | 71 | 14 |
| **17** | 181 | 73 | 15 |
| **18** | 191 | 79 | 16 |
| **19** | 193 | 83 | 17 |
| **20** | 197 | 89 | 18 |
| **21** | 199 | 97 | 19 |
| **22** | 211 | 101 | 20 |

**Пример 4:** Для заданной пары простых чисел p = 113 и q = 131 и открытого текста M = 765 определить самостоятельно остальные параметры схемы ЭЦП RSA и осуществить подписание сообщения. Проверить правильность цифровой подписи.

**Решение:**

1. Найдем n: $n = p * q = 113 * 131 = 14803$
2. Рассчитаем функцию Эйлера: $\phi(n) = (p-1)(q-1) = 112 * 130 = 14560$
3. Выберем открытый ключ e = 19
4. Рассчитаем закрытый ключ d как в примере 2, тогда получим d = 2299
5. Генерация ЭЦП:
   $s = M^d \bmod n = 765^{2299} \bmod 14803 = 11917$
6. Проверка ЭЦП:
   $M' = s^e \bmod n = 11917^{19} \bmod 14803 = 765$

7. Получаем, что $M^{'}$ = M, т.е. 765 = 765, а, следовательно, ЭЦП верна.

**Задача 4:** Для заданной пары простых чисел p и q и открытого текста M, согласно своему варианту определить самостоятельно остальные параметры схемы ЭЦП RSA и осуществить подписание сообщения. Проверить правильность цифровой подписи.

Число e взять из таблицы простых чисел.

| Варианты | p | q | M |
|---|---|---|---|
| **1** | 101 | 191 | 50 |
| **2** | 103 | 193 | 51 |
| **3** | 107 | 197 | 52 |
| **4** | 109 | 199 | 53 |
| **5** | 113 | 211 | 54 |
| **6** | 127 | 223 | 55 |
| **7** | 131 | 227 | 56 |
| **8** | 137 | 229 | 57 |
| **9** | 139 | 233 | 58 |
| **10** | 149 | 239 | 59 |
| **11** | 151 | 241 | 60 |

| Варианты | p | q | M |
|---|---|---|---|
| **12** | 157 | 251 | 61 |
| **13** | 163 | 257 | 62 |
| **14** | 167 | 263 | 63 |
| **15** | 173 | 269 | 64 |
| **16** | 179 | 271 | 65 |
| **17** | 181 | 277 | 66 |
| **18** | 191 | 281 | 67 |
| **19** | 193 | 283 | 68 |
| **20** | 197 | 293 | 69 |
| **21** | 199 | 307 | 70 |
| **22** | 211 | 181 | 71 |

**Пример 5:** Для заданного простого числа p = 131, числа g = 2 и открытого текста M = 92, определить самостоятельно остальные параметры схемы ЭЦП Эль-Гамаля и осуществить подписание сообщения. Проверить правильность цифровой подписи.

**Решение:**

1. Выберем закрытый ключ x такое что: $1 \leq x \leq p - 1$, например x = 66
2. Рассчитаем y: $y = g^x \bmod p = 2^{66} \bmod 131 = 129$
3. Выберем некоторое число k такое что: 1 < k < p-1 и НОД(k, p-1) = 1, например, k = 43
4. Для расчёта ЭЦП нужно найти $k^{-1}$: $k^{-1} \bmod (p-1) = 43^{-1} \bmod 130 = 127$
5. Генерация ЭЦП:
   $a = g^k \bmod p = 2^{43} \bmod 131 = 17$
   $s = (M - x*a) * k^{-1} \bmod p-1 = (92 - 66*17) * 127 \bmod 130 =$
   $= (92 - 82) * 127 \bmod 130 = 10 * 127 \bmod 130 = 100$
6. Проверка ЭЦП:
   $y^a * a^s \bmod p = g^M \bmod p$
   $129^{17} * 17^{100} \bmod 131 = 2^{92} \bmod 131$
   $59 * 107 \bmod 131 = 25$
   $25 = 25$

7. Получаем равенство, а, следовательно, ЭЦП верна.

**Задача 5:** Для заданного простого числа p, числа g и открытого текста M, согласно своему варианту (остальные параметры x и k возьмите из примера 5), осуществить подписание сообщения по схеме ЭЦП Эль-Гамаля. Проверить правильность цифровой подписи.

| **Варианты** | **p** | **g** | **M** |
|---|---|---|---|
| **1** | 283 | 3 | 33 |
| **2** | 293 | 2 | 34 |
| **3** | 307 | 5 | 35 |
| **4** | 311 | 17 | 36 |
| **5** | 313 | 10 | 37 |
| **6** | 317 | 2 | 38 |
| **7** | 331 | 3 | 39 |
| **8** | 337 | 10 | 40 |
| **9** | 347 | 2 | 41 |
| **10** | 349 | 2 | 42 |
| **11** | 353 | 3 | 43 |

| **Варианты** | **p** | **g** | **M** |
|---|---|---|---|
| **12** | 359 | 7 | 44 |
| **13** | 367 | 6 | 45 |
| **14** | 373 | 2 | 46 |
| **15** | 379 | 2 | 47 |
| **16** | 383 | 5 | 48 |
| **17** | 389 | 2 | 49 |
| **18** | 397 | 5 | 50 |
| **19** | 401 | 3 | 51 |
| **20** | 409 | 21 | 52 |
| **21** | 419 | 2 | 53 |
| **22** | 421 | 2 | 54 |