

Московский технический университет связи и информатики  
Кафедра Информационной безопасности

Методические указания  
для выполнения контрольной работы  
по дисциплине «Основы информационной безопасности»  
(направление 090302)

Москва 2019 г.

Методические указания  
для выполнения контрольной работы  
по дисциплине «Основы информационной безопасности»  
(направление 090302)

Составители: О. И. Шелухин д.т.н., профессор  
А.В.Ванюшина, ст.преподаватель

Издание утверждено на заседании кафедры. Протокол №1 от 30.08.2018г.

Рецензент: А.Г. Симонян, , к.т.н., доцент

## Содержание

Задание	2
Примеры выполнения заданий	3
Приложение А. Алгоритм шифрования ГОСТ 28147-89	11
Приложение Б. Символы кириллицы (альтернативная кодовая таблица ASCII)	14
Приложение В. Блок подстановки в алгоритме шифрования ГОСТ 28147-89	15
Приложение Г. Алгоритм шифрования RSA	17
Приложение Д. Таблица простых чисел	20
Приложение Е. Функция хеширования	21
Литература	22

**Задание №1. Алгоритм шифрования ГОСТ 28147-89.**

Выполните первый цикл алгоритма шифрования ГОСТ 28147 89 в режиме простой замены. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые 4 буквы.

**Задание №2. Алгоритм шифрования RSA.**

Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа  $p$  и  $q$  из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

**Задание №3. Функция хеширования.**

Найти хеш-образ своей Фамилии, используя хеш-функцию  $H_i = (H_{i-1} + M_i)^2 \bmod n$ , где  $n = pq$ ,  $p, q$  взять из Задания №3.

## Примеры выполнения заданий

**Задание №1. Алгоритм шифрования ГОСТ 28147-89.** Выполните первый цикл алгоритма шифрования ГОСТ 28147-89 в режиме простой замены. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые 4 буквы.

Исходные данные для зашифрования: КОЗИНА Г

Для ключа возьмем последовательность состоящую из 32 букв:

**АЛИНа пошла в лес собирать грибы**

Для первого подключа Х используем первые 4 буквы ключа: АЛИН.

Переводим исходный текст и первый подключ в двоичную последовательность (см. Приложение Б):

исходный текст

К	11001010
О	11001110
З	11000111
И	11001000
Н	11001101
А	11000000
пробел	00100000
Г	11000011

первый подключ Х0

А	11000000
---	----------

Л	11001011
И	11001000
Н	11001101

Таким образом, первые 64 бита определяют входную последовательность

L0: 11001010 11001110 11000111 11001000

R0: 11001101 11000000 00100000 11000011

следующие 32 бита определяют первый подключ

X0: 11000000 11001011 11001000 11001101

I. Найдем значение функции преобразования  $f(R0, X0)$  (см. Приложение А)

1). Вычисление суммы R0 и X0 по  $\text{mod } 2^{32}$

R0: 1100 1101 1100 0000 0010 0000 1100 0011

X0: 1100 0000 1100 1011 1100 1000 1100 1101

---

1000 1110 1000 1011 1110 1001 1001 0000

2). Преобразование в блоке подстановки

Результат суммирования  $R0+X0$  по  $\text{mod } 2^{32}$

1000 1110 1000 1011 1110 1001 1001 0000

преобразуем в блоке подстановки (см. Приложение В). Для каждого 4-битного блока вычислим его адрес в таблице подстановки. Номер блока соответствует номеру столбца, десятичное значение блока соответствует номеру строки в таблице. Таким образом, 5-тый блок (1011) заменяется заполнением 11-ой строки и пятого столбца в таблице подстановки (1110).

номера блоков

8	7	6	5	4	3	2	1
1000	1110	1000	1011	1110	1001	1001	0000

соответствующие номера строк в таблице подстановки

8	14	8	11	14	9	9	0
---	----	---	----	----	---	---	---

заполнение

9	2	3	14	5	15	3	4
---	---	---	----	---	----	---	---

результат

1001 0010 0011 1110 0101 1111 0011 0100

3). Циклический сдвиг результата п.2 на 11 бит влево

1111 0010 1111 1001 1010 0100 1001 0001

II. Вычисляем  $R1 = f(R0, X0) \oplus L0$ .

Результат преобразования функции  $f(R0, X0)$  складываем с  $L0$  по mod2:

L0:	1100 1010	1100 1110	1100 0111	1100 1000
$f(R0, X0)$ :	1111 0010	1111 1001	1010 0100	1001 0001
R1:	0011 1000	0011 0111	0110 0011	0101 1001

**Задание №2. Алгоритм шифрования RSA.** Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа  $p$  и  $q$

из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

I. Генерация ключей (см. Приложение Г).

Выберем два простых числа  $p = 13$  и  $q = 19$  (см. Приложение Д).

Тогда модуль

$$n = pq = 13 \cdot 19 = 247$$

и функция Эйлера

$$\varphi(n) = (p-1)(q-1) = 12 \cdot 18 = 216.$$

Закрытый ключ  $d$  выбираем из условий  $d < \varphi(n)$  и  $d$  взаимно просто с  $\varphi(n)$ , т.е.  $d$  и  $\varphi(n)$  не имеют общих делителей.

Пусть  $d = 25$ .

Открытый ключ  $e$  выбираем из условий  $e < \varphi(n)$  и  $de \equiv 1 \pmod{\varphi(n)}$ :  $e < 216$ ,  $25e \equiv 1 \pmod{216}$ .

Последнее условие означает, что число  $25e-1$  должно делиться на 216 без остатка.

Таким образом, для определения  $e$  нужно подобрать такое число  $k$ , что  $25e-1 = 216k$ .

При  $k=14$  получаем  $25e=3024+1$  или  $e=121$ .

В нашем примере

$(121, 247)$  – открытый ключ,

$(25, 247)$  – секретный ключ.

II. Шифрование.



Представим шифруемое сообщение «КГЛ» как последовательность целых чисел. Согласно алфавиту (**Приложение Б.2**) буква «К» соответствует числу 12, буква «Г» - числу 4 и буква «Л» - числу 13.

Зашифруем сообщение, используя открытый ключ (121, 247):

$$C_1 = (12^{121}) \bmod 247 = 12$$

$$C_2 = (4^{121}) \bmod 247 = 199$$

$$C_3 = (13^{121}) \bmod 247 = 91$$

Таким образом, исходному сообщению (12, 4, 13) соответствует криптограмма (12, 199, 91).

### III. Расшифрование

Расшифруем сообщение (12, 199, 91), пользуясь секретным ключом (25, 247):

$$M_1 = (12^{25}) \bmod 247 = 12$$

$$M_2 = (199^{25}) \bmod 247 = 4$$

$$M_3 = (91^{25}) \bmod 247 = 13$$

В результате расшифрования было получено исходное сообщение (12, 4, 13), то есть "КГЛ".

*Замечания.*

$$a \equiv b \pmod{n} \Leftrightarrow a - b \text{ делится на } n$$

1. Числа  $a$  и  $b$  сравнимы по  $\bmod n$ , если их разность делится на  $n$ :

Например,

$$6 \equiv 2 \pmod{4}, \quad 15 \equiv 3 \pmod{6}, \quad 45 \equiv 1 \pmod{22}.$$

2. Вычисления можно производить, используя правила модульной

$$a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$$

алгебры:

$$a = b(\bmod n) \Rightarrow ac = bc(\bmod n)$$

Для рассматриваемого примера получим

$$12^3 = 1728 \equiv 246 \bmod 247 = -1 \bmod 247$$

$$12^{120} = (12^3)^{40} = (-1)^{40} \bmod 247 = 1 \bmod 247$$

$$12^{121} = 12 \bmod 247 = 12$$

$$4^4 = 256 \bmod 247 = 9 \bmod 247$$

$$4^{12} = (4^4)^3 \bmod 247 = 9^3 \bmod 247 = 729 \bmod 247 = 235 \bmod 247$$

$$4^{60} = (4^{12})^5 = 235^5 = 716703146875 = 144 \bmod 247$$

$$4^{120} = (4^{60})^2 = 144^2 = 20736 \equiv 235 \bmod 247$$

$$4^{121} = 4 \cdot 4^{120} = 235 \cdot 4 = 940 \equiv 199 \bmod 247 \text{ и т.д.}$$

**Задание №3. Функция хеширования.** Найти хеш-образ своей Фамилии, используя хеш-функцию  $H_i = (H_{i-1} + M_i)^2 \bmod n$ , где  $n = pq$ ,  $p, q$  взять из Задания №2.

Хешируемое сообщение «КОЗИНА». Возьмем два простых числа  $p=13$ ,  $q=19$  (см. Приложение Е). Определим  $n=pq=13*19=247$ . Вектор инициализации  $H_0$  выберем равным 8 (выбираем случайным образом). Слово «КОЗИНА» согласно **Приложению Б.2** представлено последовательностью чисел (12, 16, 9, 10, 15, 1) по номерам букв в алфавите. Таким образом,

$$n=247, H_0=8, M_1=12, M_2=16, M_3=9, M_4=10, M_5=15, M_6=1.$$

Используя формулу

$$H_i = (H_{i-1} + M_i)^2 \bmod n,$$

получим хеш-образ сообщения «КОЗИНА»:

$$H_1 = (H_0 + M_1)^2 \bmod n = (8 + 12)^2 \bmod 247 = 400 \bmod 247 = 153$$

$$H_2=(H_1+M_2)^2 \bmod n = (153 + 16)^2 \bmod 247 = 28561 \bmod 247 = 156$$

$$H_3=(H_2+M_3)^2 \bmod n = (156 + 9)^2 \bmod 247 = 27225 \bmod 247 = 55$$

$$H_4=(H_3+M_4)^2 \bmod n = (55 + 10)^2 \bmod 247 = 4225 \bmod 247 = 26$$

$$H_5=(H_4+M_5)^2 \bmod n = (26 + 15)^2 \bmod 247 = 1681 \bmod 247 = 199$$

$$H_6=(H_5+M_6)^2 \bmod n = (199 + 1)^2 \bmod 247 = 40000 \bmod 247 = 233$$

В итоге получаем хеш-образ сообщения «КОЗИНА», равный 233.

Межгосударственный стандарт шифрования ГОСТ 28147-89 предусматривает 4 режима работы:

- режим простой замены;
- режим гаммирования;
- режим гаммирования с обратной связью;
- режим выработки имитовставки.

### **Простая замена.**

Режим простой замены является основой для всех остальных режимов. Длина блока - 64 бита, длина ключа – 256 бит, количество подключей – 32, длина подключа - 32 бита, число циклов – 32.

Открытые данные, подлежащие зашифрованию, разбиваются на 64-битные блоки, которые обрабатываются независимо друг от друга (Так как блоки данных шифруются независимо друг от друга, при зашифровании двух одинаковых блоков открытого текста получаются одинаковые блоки шифротекста и наоборот.). Схема обработки 64-битного блока показана на Рис.1-2.

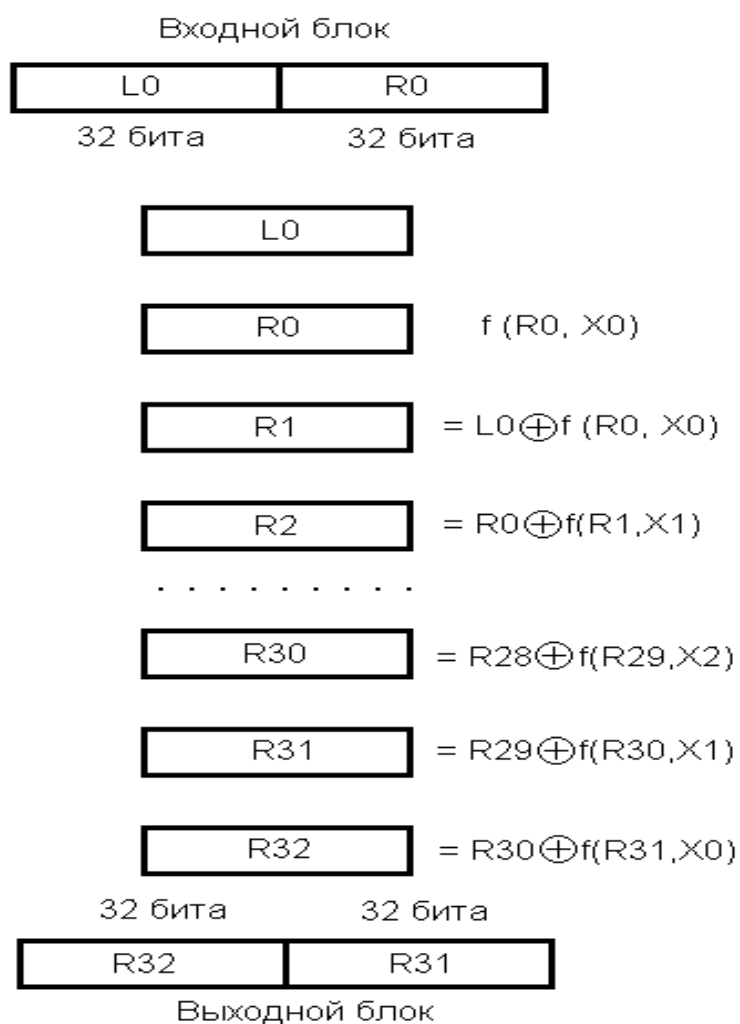
Процедура зашифрования 64-битного блока включает 32 цикла. В каждом цикле используется свой подключ, который вырабатывается из основного ключа. Размер массива открытых или зашифрованных данных, подвергающийся соответственно зашифрованию или расшифрованию, должен быть кратен 64 битам, после выполнения операции размер полученного массива данных не изменяется.

Режим простой замены применяется для шифрования короткой, ключевой информации.

В режимах гаммирования вырабатывается гамма шифра блоками по 64 бита с применением ГОСТ в режиме простой замены. В первом режиме

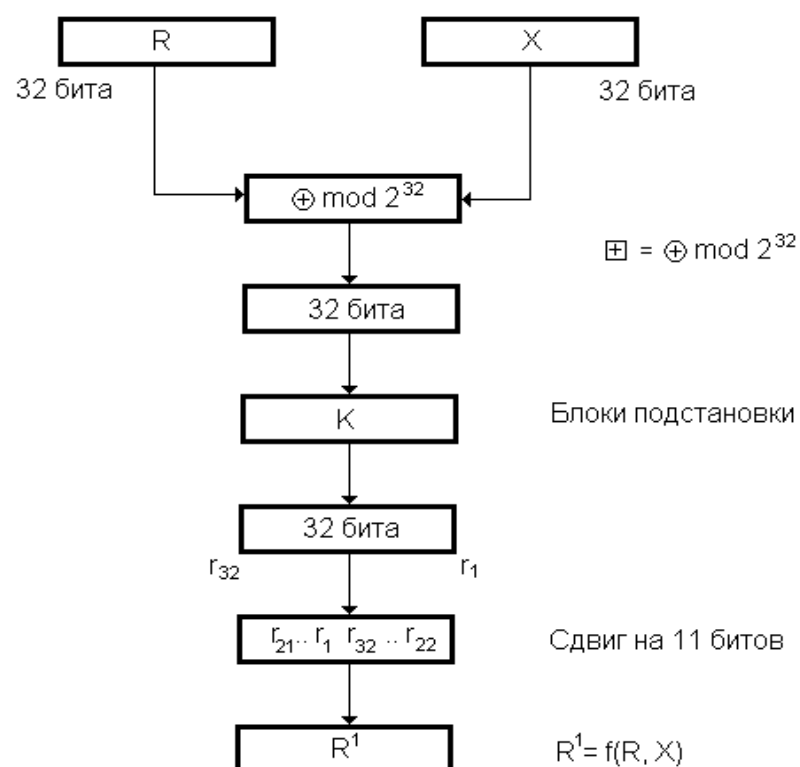
гамма не зависит от шифруемых данных, во втором – зависит от шифрблоков.

Режим выработки имитовставки предназначен для обнаружения случайных или умышленных искажений данных. Имитовставка вырабатывается (с помощью первых 16 циклов ГОСТ в режиме простой замены) из открытых данных и ключа и добавляется при передаче по каналу связи к блокам зашифрованных данных.



где  $\oplus$  - сложение по модулю 2

**Рис. 1. Алгоритм шифрования ГОСТ 28147-89 (режим простой замены).**



**Рис. 2. Функция преобразования  $f(R, X)$  в алгоритме ГОСТ 28147-89.**

**Приложение Б. Символы кириллицы (альтернативная кодовая  
таблица ASCII)**

Сим-л	Дес.	Двоич.	Сим-л	Дес.	Двоич.
А	192	11000000	б	225	11100001
Б	193	11000001	в	226	11100010
В	194	11000010	г	227	11100011
Г	195	11000011	д	228	11100100
Д	196	11000100	е	229	11100101
Е	197	11000101	ж	230	11100110
Ж	198	11000110	з	231	11100111
З	199	11000111	и	232	11101000
И	200	11001000	й	277	11101001
Й	201	11001001	к	234	11101010
К	202	11001010	л	235	11101011
Л	203	11001011	м	236	11101100
М	204	11001100	н	237	11101101
Н	205	11001101	о	238	11101110
О	206	11001110	п	239	11101111
П	207	11001111	р	240	11110000
Р	208	11010000	с	241	11110001
С	209	11010001	т	242	11110010
Т	210	11010010	у	243	11110011
У	211	11010011	ф	244	11110100
Ф	212	11010100	х	245	11110101
Х	213	11010101	ц	246	11110110
Ц	214	11010110	ч	247	11110111
Ч	215	11010111	ш	248	11111000
Ш	216	11011000	щ	249	11111001
Щ	217	11011001	ъ	250	11111010

Ъ	218	11011010	Ы	251	11111011
Ы	219	11011011	Ь	252	11111100
Ь	220	11011100	Э	253	11111101
Э	221	11011101	Ю	254	11111110
Ю	222	11011110	Я	255	11111111
Я	223	11011111	пробел	32	00100000
а	224	11100000			

## Приложение Б.2

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	

## Приложение В. Блок подстановки в алгоритме шифрования ГОСТ

28147-89

	8	7	6	5	4	3	2	1
0	1	13	4	6	7	5	14	4
1	15	11	11	12	13	8	11	10
2	13	4	10	7	10	1	4	9
3	0	1	0	1	1	13	12	2
4	5	3	7	5	0	10	6	13
5	7	15	2	15	8	3	13	8
6	10	5	1	13	9	4	15	0
7	4	9	13	8	15	2	10	14
8	9	0	3	4	14	14	2	6
9	2	10	6	10	4	15	3	11
10	3	14	8	9	6	12	8	1



11	14	7	5	14	12	7	1	12
12	6	6	9	0	11	6	0	7
13	11	8	12	3	2	0	7	15
14	8	2	15	11	5	9	5	5
15	12	12	14	2	3	11	9	3

Пример. Пусть 32-битная последовательность имеет вид

100	101	110	010	111	010	000	100
1	1	0	1	0	0	0	1

Разобьем входную последовательность на 8 блоков по 4 бита. Шестой блок 1100 пропускаем через 6-ой узел подстановки по следующему правилу: преобразуем двоичное число 1100 к десятичному виду – 12. Заполнение 12-ой строки для 6-ого узла подстановки равно 9, что в двоичном виде есть 1001. Таким образом, 4-битный блок 1100 заменяется на 1001. Остальные блоки заменяются аналогично.

8	7	6	5	4	3	2	1	номер узла
100	101	110	010	111	010	000	100	вход
1	1	0	1	0	0	0	1	
9	11	12	5	14	4	0	9	адрес
2	7	9	15	5	10	14	11	заполнение
001	011	100	111	010	101	111	101	результат
0	1	1	1	1	0	0	1	

Выходная последовательность имеет вид

001	011	100	111	010	101	111	101
-----	-----	-----	-----	-----	-----	-----	-----

0	1	1	1	1	0	0	1
---	---	---	---	---	---	---	---

### **Приложение Г. Алгоритм шифрования RSA**

Алгоритм шифрования RSA относится к криптографическим системам с открытым ключом. Криптосистемы с открытым ключом (асимметричные криптосистемы) были разработаны во второй половине семидесятых годов. В асимметричных криптосистемах процедуры прямого и обратного криптопреобразования выполняются на различных ключах и не имеют между собой очевидных и легко прослеживаемых связей, позволяющих по одному ключу определить другой. В такой схеме знание только ключа зашифрования не позволяет расшифровать сообщение, поэтому он не является секретным элементом шифра и обычно публикуется участником обмена для того, чтобы любой желающий мог послать ему зашифрованное сообщение.

Принцип функционирования асимметричной криптосистемы заключается в следующем:

- пользователь А генерирует два ключа - открытый (незасекреченный) и секретный - и передает открытый ключ по незащищенному каналу пользователю Б;
- пользователь Б шифрует сообщение, используя открытый ключ шифрования пользователя А;
- пользователь Б посылает зашифрованное сообщение пользователю А по незащищенному каналу;
- пользователь А получает зашифрованное сообщение и дешифрует его, используя свой секретный ключ.

Пары {открытый ключ; секретный ключ} вычисляются с помощью специальных алгоритмов, причем ни один ключ не может быть выведен из другого.

## Криптографическая система RSA (Rivest-Shamir-Adleman)

Авторами алгоритма RSA, предложенного в 1977 г., являются Р.Риверст (Rivest), А.Шамир (Shamir) и А.Адлеман (Adleman). Надежность алгоритма основывается на трудности факторизации (разложения на множители) больших чисел и трудности вычисления дискретных алгоритмов (нахождения  $x$  при известных  $a$ ,  $b$  и  $n$  из уравнения  $a^x = b \pmod{n}$ ).

Алгоритм RSA состоит из трех частей: генерации ключей, шифрования и расшифрования.

### 1. Генерация ключей.

Выберем два больших различных простых числа  $p$  и  $q$  (Натуральное число называется простым, если оно делится только на себя и на 1.) и найдем их произведение

$$n = pq .$$

Вычислим функцию Эйлера  $\varphi(n)$  по формуле

$$\varphi(n) = (p-1)(q-1).$$

Закрытый ключ  $d$  выбираем из условий

$$d < \varphi(n) \text{ и}$$

$$d \text{ взаимно просто с } \varphi(n),$$

т.е.  $d$  и  $\varphi(n)$  не имеют общих делителей.

Открытый ключ  $e$  выбираем из условий

$$e < \varphi(n) \text{ и}$$

$$de = 1 \pmod{\varphi(n)} .$$

Последнее условие означает, что разность  $de - 1$  должна делиться на  $\varphi(n)$  без остатка. Для определения числа  $e$  нужно подобрать такое число  $k$ , что

$$de - 1 = \varphi(n) * k .$$

В алгоритме RSA

$(e, n)$  – открытый ключ,

$(d, n)$  – секретный ключ.

## 2. Шифрование.

Исходное сообщение разбивается на блоки  $M_i$  одинаковой длины. Каждый блок представляется в виде большого десятичного числа, меньшего  $n$ , и шифруется отдельно. Шифрование блока  $M$  ( $M$  - десятичное число) осуществляется по следующей формуле

$$M^e = C \pmod{n},$$

где  $C$  – шифрблок, соответствующий блоку открытого сообщения  $M$ . Шифрблоки соединяются в шифрограмму.

## 3. Расшифрование.

При расшифровании шифрограмма разбивается на блоки известной длины и каждый шифрблок расшифровывается отдельно по следующей формуле

$$C^d = M \pmod{n}.$$

**Приложение Д. Таблица простых чисел.**

1	2	3	5	7
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

## Приложение Е. Функция хеширования

Функцией хеширования (хеш-функцией) называется преобразование данных, переводящее строку битов  $M$  произвольной длины в строку битов  $h(M)$  некоторой фиксированной длины (несколько десятков или сотен бит).

Хеш-функция  $h(M)$  должна удовлетворять следующим условиям:

1. хеш-функция  $h(M)$  должна быть чувствительна к любым изменениям входной последовательности  $M$ ;
2. для данного значения  $h(M)$  должно быть невозможно найти значение  $M$ ;
3. для данного значения  $h(M)$  должно быть невозможно найти значение  $M' \neq M$  такое, что  $h(M') = h(M)$ .

Ситуация, при которой для различных входных последовательностей  $M$ ,  $M'$  совпадают значения их хеш-образов:  $h(M) = h(M')$ , называется коллизией.

При построении хеш-образа входная последовательность  $M$  разбивается на блоки  $M_i$  фиксированной длины и обрабатывается поблочно по формуле

$$H_i = f(H_{i-1}, M_i).$$

Хеш-значение, вычисляемое при вводе последнего блока сообщения, становится хеш-значением (хеш-образом) всего сообщения.

В качестве примера рассмотрим упрощенный вариант хеш-функции из рекомендаций МККТТ X.509:

$$H_i = (H_{i-1} + M_i)^2 \bmod n,$$

где  $n = pq$ ,  $p$  и  $q$  – большие простые числа,  $H_0$  – произвольное начальное заполнение,  $M_i$  –  $i$ -тый блок сообщения  $M = M_1 M_2 \dots M_k$ .

## Литература

1. А.А. Малюк, В.С. Горбатов, В.И.Королев, В.М.Фомичев, А.П.Дураковский, Т.А.Кондратьева Введение в информационную безопасность / Под ред. В.С. Горбатова. – М.: Горячая линия – Телеком, 2016. - 288 с.
2. Баричев С.Г., Гончаров В.В. Основы современной криптографии. М.: Горячая линия - Телеком, 2001.
3. Фомичев В.М. Симметричные криптосистемы. Краткий обзор основ криптологии для шифросистем с секретным ключом: Учебное пособие. – М.: МИФИ, 1995. – 44 с.
4. Винокуров А.Ю. Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров Intel x86.