

Министерство науки и высшего образования  
Российской Федерации  
Ярославский государственный университет  
им. П. Г. Демидова  
Кафедра алгебры и математической логики

**С. И. Яблокова**

**Задачи по криптографическим методам защиты  
информации  
Симметричные и асимметричные криптосистемы**

*Практикум*

Ярославль  
ЯрГУ  
2022

УДК 004.056.5(076.5)  
ББК 3973.2-018.2я73-4  
Я14

*Рекомендовано*  
*Редакционно-издательским советом университета*  
*в качестве учебного издания. План 2022 года.*

Рецензент  
кафедра алгебры и математической логики ЯрГУ

**Яблокова, Светлана Ивановна.**

Задачи по криптографическим методам защиты  
Я14 информации. Симметричные и асимметричные  
криптосистемы : практикум / С. И. Яблокова ; Яросл.  
гос. ун-т им. П. Г. Демидова. – Ярославль : ЯрГУ. –  
2022. – Ч. 2. – 80 с.

Практикум содержит задачи по криптографическим методам защиты информации и описание некоторых симметричных криптосистем, криптосистем с открытым ключом и алгоритмов цифровой подписи, используемых при решении задач. Приведены указания и примеры с подробным разбором методов решения.

Предназначен для студентов, изучающих дисциплину "Криптографические методы защиты информации".

УДК 004.056.5(076.5)  
ББК 3973.2-018.2я73-4

© ЯрГУ, 2022

## Оглавление

Введение	4
<b>Симметрические криптосистемы</b>	
Шифры гаммирования	5
Шифр простой неравнозначной замены	6
Шифр вертикальной перестановки	7
<b>Системы шифрования с открытым ключом</b>	
Криптосистема RSA	10
Шифрсистема Эль Гамала	13
Шифрсистема на основе проблемы рюкзака	14
<b>Цифровые подписи</b>	16
Схема подписи RSA	17
Схема подписи Рабина	20
Схема подписи Фиата – Шамира	23
Цифровая подпись Эль Гамала	26
Схема подписи Шнорра	28
Цифровая подпись Диффи – Лампорта	31
<b>Задачи</b>	33
Ответы	43
<b>Задачи для самостоятельного решения</b>	46
Таблицы	78
Литература	78

## Введение

В практикуме содержатся задачи по криптографическим методам защиты информации. Эта дисциплина изучается студентами специальности "Компьютерная безопасность" на четвертом курсе, студентами специальности "Информационная безопасность" на третьем курсе. Кроме того, она является одним из спецкурсов по выбору для студентов четвертого курса специальности "Математика и компьютерные науки."

Для решения предлагаемых в практикуме задач требуется знание основных исторических и современных криптосистем симметричного и асимметричного шифрования, алгоритмов вычисления цифровых подписей, знание определения и свойств сравнений, умение проводить вычисления в кольцах вычетов, использовать расширенный алгоритм Евклида, знание основных понятий алгебры. Задания, связанные с вычислениями в кольцах вычетов, как правило, вызывают наибольшие трудности.

Практикум начинается с напоминания некоторых криптосистем симметричного шифрования и систем шифрования с открытым ключом, а также схем вычисления цифровой подписи. Каждая криптосистема иллюстрируется примерами использования алгоритмов шифрования и дешифрования. Большинство алгоритмов описано в терминах сравнений, что позволяет отказаться от громоздких таблиц, которыми первоначально пользовались в этих криптосистемах. Далее предлагаются задачи по курсу для решения на практических занятиях, которые снабжены ответами. В заключение предлагается набор заданий для самостоятельного решения, которые могут быть использованы для контрольных работ и экзаменационных заданий. В приложении приведены таблицы, которые можно использовать при шифровании и дешифровании в различных криптосистемах.

## Симметричные криптосистемы

### Шифры гаммирования

В силу простоты технической реализации и высоких криптографических качеств эти шифры получили широкое распространение. В основе таких шифров лежит метод "наложения" ключевой последовательности, называемой *гаммой*, на открытый текст. "Наложение" заключается в позначном (побуквенном) сложении или вычитании по некоторому модулю. Уравнения шифрования могут иметь вид

$$y_i \equiv x_i + \gamma_i \pmod{n}, \quad (1)$$

$$y_i \equiv x_i - \gamma_i \pmod{n}, \quad (2)$$

$$y_i \equiv \gamma_i - x_i \pmod{n}, \quad (3)$$

где  $\{\gamma_i\}$  — периодическая последовательность, образуемая повторением некоторого ключевого слова. Шифры, задаваемые формулами (1)–(3), называются шифрами *модульного гаммирования*.

**Пример 1.** Используя формулу (3), зашифровать сообщение *конечное множество*, взяв в качестве гаммы слово **"проекция"**. Записывая буквы гаммы над соответствующими буквами сообщения и заменяя те и другие их числовыми эквивалентами из кольца  $\mathbf{Z}_{33}$  по таблице 1, получаем

16 17 15 5 11 23 9 32    16 17 15 5 11 23 9 32 16

11 15 14 5 24 14 15 5    13 14 15 7 5 18 19 2 15.

По формуле (3) из чисел, стоящих в верхней строке, следует вычесть стоящие под ними числа, проводя вычисления в кольце  $\mathbf{Z}_{33}$ . В результате получаем

5, 2, 1, 0, 20, 9, 27, 27    3, 3, 0, 31, 6, 5, 23, 30, 1

или криптограмму

*евбауиѡѡ ггаюёеуэб.*

Если воспользоваться формулой (1), то получим шифр Виженера, тогда результатом будет последовательность

27, 32, 29, 10, 2, 4, 24, 4    29, 31, 30, 12, 16, 8, 28, 1, 31

или криптограмма

*ѡяъйвдчд ѡюэлпзыбю.*

## Шифр простой неравнозначной замены

Рассмотрим один простой шифр, ставящий в соответствие шифрвеличинам целые числа разной значности, т. е. шифр-текст будет представлен последовательностью цифр. Такой шифр можно построить, например, используя частоту появления букв алфавита в тексте. Известно, что наиболее часто встречаются в текстах, написанных на русском языке, буквы *о, е(ё), а, и, т, н* (в порядке убывания частот). В текстах, написанных на английском языке, наиболее часто встречаются *е, t, а, i, о, n, ,s, r*. Возьмем прямоугольную таблицу размера  $4 \times 7$ , в которую записан систематически перемешанный английский алфавит, расширенный символами "."(точка) и (пробел). Самые высокочастотные буквы занумерованы цифрами от 0 до 7. Остальные буквы и символы занумерованы по столбцам таблицы двузначными числами от 80 до 99. При шифровании каждая буква открытого текста заменяется соответствующим ей числом, согласно полученной таблице. Поскольку в таблицу включен символ пробела, то разделять слова при шифровании не требуется. Пусть ключ перемешивания – это слово **inspiration**. Наша таблица в этом случае будет выглядеть так:

i 0	n 1	s 6	p 88	r 7	a 5	t 3
o 4	b 82	c 85	d 89	e 2	f 94	g 97
h 80	j 83	k 86	l 90	m 92	q 95	u 98
v 81	w 84	x 87	y 91	z 93	· 96	 99

Тогда открытый текст *differential calculation* при шифровании перейдет в следующую последовательность цифр:

8909494272130590998559085989053041.

При расшифровании мы должны разделить числовую последовательность на отдельные числа. Если знаком является цифра от 0 до 7, то отделяем одну такую цифру, если это цифра 8 или 9, то отделяем две последовательно идущие цифры. Удобно работать с эквивалентной таблицей, в которой буквы, соответствующие числам, легко находятся

	0	1	2	3	4	5	6	7	8	9
	i	n	e	t	o	a	s	r	—	—
8	h	v	b	j	w	c	k	x	p	d
9	l	y	m	z	f	q	·	g	u	

## Шифр вертикальной перестановки

Этот шифр использует прямоугольную таблицу, в которую записывается открытое сообщение обычным образом (по строкам слева направо). Шифртекст выписывается по столбцам (сверху вниз), при этом порядок выбора столбцов определяется числовым ключом.

**Пример 2.** В таблицу  $5 \times 6$  впишем фразу  
*Cryptography is secret writing*  
и получим зашифрованный текст на ключе (5,3,6,1,2,4).

<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>
C	R	Y	P	T	O
G	R	A	P	H	Y
I	S	S	E	C	R
E	T	W	R	I	T
I	N	G			

Выписываем буквы, стоящие в столбцах, указанных ключом, получаем

*thciyaswgoyrtcgieirrstnpper.*

При расшифровании в первую очередь следует определить число длинных столбцов, т. е. число букв в последней строке прямоугольной таблицы. Для этого разделим число букв сообщения на длину числового ключа. Искомым числом будет остаток от деления. Далее с помощью ключа можно поставить строки криптограммы в нужные столбцы и по строкам прочитать сообщение. В примере 20 сообщение содержит 27 букв, а длина ключа равна 6, значит,

$$27 = 4 \cdot 6 + 3,$$

т. е. имеется 3 длинных столбца. Очевидно, это 3 первых столбца. Смотрим на ключ. В криптограмме первым записан 5-й столбец, он короткий, т. е. содержит 4 буквы. Отделяем первые 4 буквы *thci*, они будут стоять в 5-м столбце. Следующий столбец криптограммы 3-й, он длинный, т. е. содержит 5 букв. Отделяем следующие 5 букв *uaswg* и ставим в 3-й столбец таблицы. Далее, согласно ключу, стоит 6-й столбец, он короткий. Значит, следующие 4 буквы криптограммы *oyrt* надо поставить в 6-й столбец таблицы. Затем должны идти 1-й и 2-й столбцы, они оба длинные, т. е. отделяем по 5 букв и ставим в 1-й и 2-й столбцы таблицы (это 5-граммы *cgiei* и *rrstn*). Наконец, последние 4 буквы криптограммы должны стоять в 4-м столбце таблицы, который является коротким.



### Пример 3. Криптограмма

*egtiweacacikfosrenpyttmogsiGnrprnherretriyege*

получена шифром вертикальной перестановки на ключе (7, 3, 8, 6, 1, 4, 2, 5). Расшифровать криптограмму. Ключ состоит из 8 чисел, значит, в таблице 8 столбцов. Криптограмма состоит из 45 букв. Так как

$$45 = 5 \cdot 8 + 5,$$

то в таблице имеется 5 длинных столбцов и 3 коротких. Короткими, очевидно, являются три последние столбца: 6-й, 7-й, 8-й. Количество строк в таблице равно 6, т. е. имеем 3 столбца из 5 букв и 5 столбцов из 6 букв.

В соответствии с ключом криптограмма разбивается на отрезки длин

$$5, 6, 5, 5, 6, 6, 6, 6,$$

соответственно, т. е.

*egtiw eacaci kfosr enpyt tmogsi Gnrprn herret riyheg.*

Эти отрезки ставим в соответствующие столбцы таблицы. В результате получаем

1	2	3	4	5	6	7	8
t	h	e	G	r	e	e	k
m	e	a	n	i	n	g	f
o	r	c	r	y	p	t	o
g	r	a	p	h	y	i	s
s	e	c	r	e	t	w	r
i	t	i	n	g			

и открытый текст:

*the Greek meaning for cryptography is secret writing.*

## Системы шифрования с открытым ключом.

### Криптосистема RSA

Асимметричная система шифрования – это система с двумя ключами, один из которых является открытым (общедоступным) ключом, а другой – секретным (известным только владельцу). Стойкость алгоритма RSA основана на сложности задачи факторизации больших целых чисел. Пусть  $p$  и  $q$  ( $p \neq q$ ) – два больших целых простых числа и  $n = pq$ . Пусть целые числа  $e$  и  $d$  таковы, что

$$pq \equiv 1 \pmod{\varphi(n)},$$

где  $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$  – значение функции Эйлера от числа  $n$ . Открытый ключ:  $k_1 = (n, e)$ , секретный ключ:  $k_2 = (p, q, d)$ .

Если  $M$  – блок открытого текста, а  $C$  – соответствующий блок шифрованного текста, то правило зашифрования есть

$$C = E_{k_1}(M) = M^e \pmod{n}. \quad (4)$$

Обратное преобразование задается формулой

$$M = D_{k_2}(C) = C^d \pmod{n}. \quad (5)$$

**Пример 4.** Пусть  $p = 23$ ,  $q = 41$ , тогда  $n = pq = 943$ ,  $\varphi(n) = 22 \cdot 40 = 880$ . В качестве открытой экспоненты возьмем  $e = 3$ . Зашифруем сообщение *sequence* по системе RSA с выбранным открытым ключом  $e = 3$ ,  $n = 943$ .

Каждую букву сообщения заменим ее числовым эквивалентом по таблице 2, представив этот числовой эквивалент в двоичной системе счисления. Поскольку мощность языка равна 26, то для представления наибольшего вычета по модулю 26 требуется 5 двоичных разрядов, поэтому для каждой буквы сообщения отведем 5 двоичных разрядов:

$$s \rightarrow 18 = 10010_{(2)}, \quad e \rightarrow 4 = 00100_{(2)}, \quad q \rightarrow 16 = 10000_{(2)},$$

$$u \rightarrow 20 = 10100_{(2)}, \quad e \rightarrow 4 = 00100_{(2)}, \quad n \rightarrow 13 = 01101_{(2)},$$

$$c \rightarrow 2 = 00010_{(2)}, \quad e \rightarrow 4 = 00100_{(2)}.$$

Запишем полученную последовательность двоичных разрядов в строку

$$10010 \ 00100 \ 10000 \ 10100 \ 00100 \ 01101 \ 00010 \ 00100.$$

Так как  $2^9 < n = 943 < 2^{10}$ , то разобьем полученную последовательность на блоки длины 9, дописывая незначащие нули в начало, если число разрядов не кратно 9:

$$000001001 \ 000100100 \ 001010000 \ 100011010 \ 001000100$$

$$\begin{array}{ccccc} M_1 & M_2 & M_3 & M_4 & M_5 \\ M_1 = \underbrace{000001001}_9, & M_2 = \underbrace{000100100}_9, & M_3 = \underbrace{001010000}_9, \\ M_4 = \underbrace{100011010}_9, & M_5 = \underbrace{001000100}_9. \end{array}$$

Каждому выделенному блоку  $M_i$  ( $i = 1, \dots, 5$ ) поставим в соответствие десятичное число

$$\begin{aligned} M_1 &= 000001001_{(2)} = 9, & M_2 &= 000100100_{(2)} = 36, \\ M_3 &= 001010000_{(2)} = 80, & M_4 &= 100011010_{(2)} = 282, \\ M_5 &= 001000100_{(2)} = 68. \end{aligned}$$

Теперь зашифруем каждый блок по формуле (4):

$$\begin{aligned} C_1 &\equiv M_1^3 \pmod{943} \equiv 9^3 \equiv 729 \pmod{943}, \\ C_2 &\equiv M_2^3 \pmod{943} \equiv 36^3 \equiv 449 \pmod{943}, \\ C_3 &\equiv M_3^3 \pmod{943} \equiv 80^3 \equiv 894 \pmod{943}, \\ C_4 &\equiv M_4^3 \pmod{943} \equiv 282^3 \equiv 285 \pmod{943}, \\ C_5 &\equiv M_5^3 \pmod{943} \equiv 68^3 \equiv 424 \pmod{943}. \end{aligned}$$

Итак, криптограмма имеет вид

$$(C_1, C_2, C_3, C_4, C_5) = (729, 449, 894, 285, 424).$$

Если мы хотим представить ее последовательностью двоичных разрядов, то следует перевести каждое  $C_i$  ( $i = 1, \dots, 5$ ) в двоичную систему счисления, отводя под каждое число 10 двоичных разрядов.

**Пример 5.** Получена криптограмма (81, 162, 144), зашифрованная по системе RSA. Найти открытый текст, если он написан на английском языке, и секретный ключ есть  $p = 11$ ,  $q = 17$  и  $d = 7$ . По формуле (5), учитывая, что  $n = pq = 11 \cdot 17 = 187$ , вычислим соответствующие блоки открытого текста  $M_i$  ( $i = 1, \dots, 5$ ) :

$$\begin{aligned} M_1 &\equiv C_1^d \equiv 81^7 \pmod{187} \equiv 38, \\ M_2 &\equiv C_2^d \equiv 162^7 \pmod{187} \equiv 2, \\ M_3 &\equiv C_3^d \equiv 144^7 \pmod{187} \equiv 100. \end{aligned}$$

Так как  $2^7 < 187 < 2^8$ , то отводим под двоичное представление каждого блока 7 двоичных разрядов:

$$\begin{aligned} 38 &= 0100110_{(2)}, \\ 2 &= 0000010_{(2)}, \\ 100 &= 1100100_{(2)}. \end{aligned}$$

Тогда открытое сообщение записывается двоичной последовательностью: 0100110 0000010 1100100.

Отделяем блоки по 5 двоичных разрядов, начиная с конца последовательности (незначащий 0 в начале строки опускаем):

$$10011 \quad 00000 \quad 01011 \quad 00100$$

Находя по таблице 2 буквы английского алфавита, соответствующие полученным числовым эквивалентам, имеем

$$\begin{aligned} 10011_{(2)} &= 19 \rightarrow t \\ 00000_{(2)} &= 0 \rightarrow a \\ 01011_{(2)} &= 11 \rightarrow l \\ 00100_{(2)} &= 4 \rightarrow e \end{aligned}$$

или  $t a l e$ . Это и есть открытый текст.

## Шифрсистема Эль Гамала

Криптографическая стойкость этой криптосистемы основана на сложности проблемы логарифмирования в мультипликативной группе конечного поля.

Пусть  $p$  — большое простое число,  $\alpha$  — образующая мультипликативной группы  $\mathbf{Z}_p^*$ ,  $a$  — целое число,  $1 \leq a \leq p - 2$ . Вычисляем

$$\beta = \alpha^a \pmod{p}. \quad (6)$$

Открытый ключ  $k_1 = (p, \alpha, \beta)$ , секретным ключом является число  $a$ , т. е.  $k_2 = (a)$ . Правило шифрования на ключе  $k_1$  определяется формулой

$$E_{k_1}(M) = (C_1, C_2),$$

где

$$C_1 \equiv \alpha^r \pmod{p}, \quad C_2 \equiv M\beta^r \pmod{p}. \quad (7)$$

Здесь  $r$  — случайно выбираемое число из интервала  $[0, p - 2]$ . Правило расшифрования на ключе  $k_2$  определяется формулой

$$M = D_{k_2}(C_1, C_2) \equiv C_2(C_1^a)^{-1} \pmod{p}. \quad (8)$$

**Пример 6.** Возьмем  $p = 31$ ,  $\alpha = 11$ ,  $a = 7$  и зашифруем по системе Эль Гамала сообщение  $M = 21$ .

Выберем  $r = 3$ , по формуле (6)  $\beta \equiv 11^7 \pmod{31} \equiv 13$ , тогда

$$\begin{aligned} C_1 &\equiv 11^3 \pmod{31} \equiv 29, \\ C_2 &\equiv 21 \cdot 13^3 \pmod{31} \equiv 9 \end{aligned}$$

и получаем криптограмму  $(C_1, C_2) = (29, 9)$ .

**Пример 7.** Получена криптограмма  $(9, 3)$ , вычисленная по схеме Эль Гамала с  $p = 31$ . Зная секретный ключ  $a = 5$ , найти сообщение  $M$ . По формуле (7) вычислим

$$M \equiv 3(9^5)^{-1} \pmod{31} \equiv 3(-6)^{-1} \pmod{31} \equiv 3 \cdot 5 \equiv 15.$$

## Шифрсистема на основе проблемы рюкзака

Пусть задано множество натуральных чисел

$$A = \{a_1, a_2, \dots, a_n\}$$

и натуральное число  $S$ . Задачу об укладке рюкзака можно сформулировать следующим образом:

существует ли такой набор чисел  $x_i$  (где  $x_i = 0$  или  $x_i = 1$ ),  $i=1, \dots, n$ , для которого

$$\sum_{i=1}^n x_i a_i = S.$$

Это сложная задача, ее решение с полиномиальной сложностью до сих пор неизвестно. Однако решение подобной задачи в случае *супервозрастающей* последовательности чисел из множества  $A$  получить очень легко.

*Супервозрастающей* назовем последовательность натуральных чисел  $(b_1, b_2, \dots, b_n)$ , если

$$b_i > \sum_{j=1}^{i-1} b_j, \quad 2 \leq i \leq n.$$

Для супервозрастающей последовательности задача решается следующим образом:

цикл по  $i := n$  шагом  $-1$  до  $1$  выполнять

{если  $b_i \leq S$ , то  $(x_i = 1$  и  $S := S - b_i)$ , иначе  $x_i = 0$ }.

Для вычисления секретного и соответствующего открытого ключей следует:

1. Выбрать супервозрастающую последовательность  $(b_1, b_2, \dots, b_n)$  и модуль  $m$  такой, что

$$m > \sum_{i=1}^n b_i.$$

2. Выбрать случайное число  $w$ ,  $1 < w < m - 1$  такое, что  $\text{НОД}(w, m) = 1$ .

3. Выбрать случайную подстановку  $\pi$  чисел  $\{1, 2, \dots, n\}$ .
4. Вычислить элементы последовательности  $a_1, a_2, \dots, a_n$  по формуле

$$a_i = wb_{\pi(i)} \pmod{m} \quad (i = 1, 2, \dots, n). \quad (8)$$

Открытым ключом является последовательность  $(a_1, a_2, \dots, a_n)$  и число  $m$ , секретным – подстановка  $\pi$  и последовательность  $(b_1, b_2, \dots, b_n)$ . Число  $n$  равно количеству битов в двоичной записи шифруемого сообщения  $M$ , т. е.

$$M = m_1m_2 \dots m_{n_2}, \quad m_i \in \{0, 1\}.$$

*Алгоритм шифрования* состоит из двух шагов:

1. Представить сообщение  $M$  в виде бинарной последовательности  $m_1m_2 \dots m_n$ .

2. Вычислить  $C = \sum_{i=1}^n m_i a_i \pmod{m}$ . (9)

*Алгоритм расшифрования* содержит три шага:

1. Вычислить  $H = w^{-1}C \pmod{m}$ .
2. Решая проблему рюкзака для супервозрастающей последовательности, найти числа  $z_i \in \{0, 1\}$  такие, что

$$H = \sum_{i=1}^n z_i b_i.$$

3. Найти биты представления сообщения  $M$  по формуле  $m_i = z_{\pi(i)}$ ,  $(i = 1, 2, \dots, n)$ .

**Пример 8.** Возьмем супервозрастающую последовательность

$$b_1 = 1, \quad b_2 = 3, \quad b_3 = 5, \quad b_4 = 10, \quad b_5 = 20, \quad b_6 = 40$$

и  $m = 83$ . Пусть  $\pi = (134526)$  – цикл длины 6, а  $w = 5$ .

Сначала найдем открытый ключ:

$$a_1 = 5b_{\pi(1)} = 5b_3 = 25, \quad a_2 = 5b_{\pi(2)} = 5b_6 = 200 \equiv 34 \pmod{83},$$

$$a_3 = 5b_{\pi(3)} = 5b_4 = 50, \quad a_4 = 5b_{\pi(4)} = 5b_5 = 100 \equiv 17 \pmod{83},$$

$$a_5 = 5b_{\pi(5)} = 5b_2 = 15, \quad a_6 = 5b_{\pi(6)} = 5b_1 = 5,$$

откуда

$$(a_1, a_2, \dots, a_6) = (25, 34, 50, 17, 15, 5).$$

Зашифруем сообщение  $M = 55$ . Так как  $55 = 110111_{(2)}$ , то

$$C = a_1 + a_2 + a_4 + a_5 + a_6 = 25 + 34 + 17 + 15 + 5 = 96 \equiv 13 \pmod{83}.$$

**Пример 9.** Получена криптограмма  $C = 64$ . Прочитать сообщение, если в качестве открытого и секретного ключей взяты данные из примера 8.

Вычисляем  $H \equiv 5^{-1} \cdot 64 \pmod{83}$ .

Так как  $5^{-1} \equiv 50 \pmod{83}$ , то  $H \equiv 50 \cdot 64 \pmod{83} \equiv 46$ .

Решаем проблему рюкзака для супервозрастающей последовательности  $(b_1, b_2, \dots, b_6)$ . Очевидно,

$$46 = 46 = b_6 + b_3 + b_1 (= 40 + 5 + 1),$$

значит,  $z_1 = z_3 = z_6 = 1$ ,  $z_2 = z_4 = z_5 = 0$ .

Находим биты в представлении сообщения  $M$  :

$$m_1 = z_{\pi(1)} = z_3 = 1, \quad m_2 = z_{\pi(2)} = z_6 = 1, \quad m_3 = z_{\pi(3)} = z_4 = 0,$$

$$m_4 = z_{\pi(4)} = z_5 = 0, \quad m_5 = z_{\pi(5)} = z_2 = 0, \quad m_6 = z_{\pi(6)} = z_1 = 1,$$

откуда  $M = 110001_{(2)} = 49$ .

## Цифровые подписи

Цифровые подписи используются для аутентификации участников информационного обмена, в случае когда стороны не доверяют друг другу. Схема цифровой подписи включает два алгоритма: один — для вычисления подписи, а второй — для проверки подписи. Вычисление подписи может быть выполнено только автором подписи, поэтому зависит от секретного ключа, известного только подписывающей стороне. Алгоритм проверки подписи должен быть общедоступным, чтобы проверить правильность подписи мог каждый. Следовательно, в этом случае используется открытый ключ.



## Схема подписи RSA

Пусть  $p$  и  $q$  ( $p \neq q$ ) — большие простые числа и  $n = pq$ . Открытый  $e$  и секретный  $d$  ключи выбираются так, чтобы

$$ed \equiv 1 \pmod{\varphi(n)},$$

где  $\varphi(n) = (p-1)(q-1)$  — функция Эйлера. Пусть  $h(M)$  — некоторая хеш-функция от сообщения  $M$ , известная и получателю, и отправителю.

*Алгоритм вычисления подписи под сообщением  $M$ :*

1. Вычислить  $r = h(M)$ .
2. Вычислить подпись  $s \equiv r^d \pmod{n}$ .

*Алгоритм проверки подписи:*

1. Вычислить  $t \equiv s^e \pmod{n}$ .
2. Вычислить  $r = h(M)$ .
3. Проверить равенство  $t = r$ . Если оно выполняется, то подпись подлинная.

Если  $(M, s)$  — сообщение с правильной подписью, то пара  $(\tilde{M}, \tilde{s})$  также будет сообщением с правильной подписью, если

$$h(\tilde{M}) \equiv h^k(M) \pmod{n},$$

$$\tilde{s} \equiv s^k \pmod{n}$$

для некоторого целого  $k$ .

Пара  $(\tilde{M}, \tilde{s})$  может быть создана следующим образом:

1. Выбрать новое сообщение  $\tilde{M}$ , вычислить  $h(\tilde{M})$ , найти  $\log_{h(M)} h(\tilde{M}) = k$  и вычислить  $\tilde{s} \equiv s^k \pmod{n}$   
либо

2. Найти  $\tilde{r} \equiv h^k(M) \pmod{n}$  для некоторого известного  $k$ , затем подобрать  $\tilde{M}$ , так чтобы выполнялось  $h(\tilde{M}) = \tilde{r}$ .

Поэтому стойкость подписи RSA не превышает сложности вычисления дискретного логарифма в группе  $\mathbf{Z}_n^*$  или сложности обращения хеш-функции.

**Пример 10.** Пусть  $p = 7$ ,  $q = 11$  и  $n = 77$ , а секретный ключ  $d = 43$ . Значение хеш-функции от сообщения получается побитовым сложением по модулю два 4-битовых блоков, на которые разбивается сообщение, каждая буква которого представляется 5 битами своего числового эквивалента.

Подпишем сообщение *cipher*.

Поставим буквам сообщения их числовые эквиваленты по таблице 2 и запишем каждое число 5 двоичными разрядами:

$$\underbrace{00010}_c \underbrace{01000}_i \underbrace{01111}_p \underbrace{00111}_h \underbrace{00100}_e \underbrace{10001}_r$$

Начиная с конца, разделим сообщение на 4-битовые блоки, отбрасывая незначущие нули в начале сообщения:

$$\underbrace{0100} \underbrace{1000} \underbrace{0111} \underbrace{1001} \underbrace{1100} \underbrace{1001} \underbrace{0001} .$$

Теперь побитово сложим полученные блоки по модулю 2.

$$\begin{array}{r} 0100 \\ 1000 \\ 0111 \\ \oplus 1001 \\ 1100 \\ 1001 \\ \underline{0001} \\ 0110, \end{array}$$

следовательно,  $h(M) = 0110_{(2)} = 6$ .

Вычислим подпись  $s \equiv 6^{43} \pmod{77} \equiv 62$ .

**Пример 11.** Получено сообщение *key* с подписью  $s = 11$ . При тех же  $p, q, n, h(M)$  и  $e = 7$ , что и в примере 10, проверить правильность подписи.

Сначала вычислим  $t \equiv s^7 \pmod{n} \equiv 11^7 \pmod{77}$ . Нетрудно проверить, что  $s \equiv 11 \pmod{77}$ .

Вычислим значение хеш-функции от полученного сообщения. Слово *key* представляется двоичной последовательностью

01010 00100 11000;

разбиваем ее на 4-битовые блоки:    010   1000   1001   1000  
и побитово складываем по модулю 2:

$$\begin{array}{r} 010 \\ 1000 \\ \oplus 1001 \\ \hline 1000 \\ \hline 1011. \end{array}$$

В результате  $h(M) = 1011_{(2)} = 11$ .

Значение хеш-функции совпадает с подписью, значит, она подлинная.

**Пример 12.** Известна правильная подпись под сообщением *cipher*,  $s = 62$  и число  $n = 77$ . Не зная секретного ключа, найти правильную подпись под сообщением *Paris*, если хеш-функция задана так же, как в примере 10.

Найдем  $h(\tilde{M})$ , то есть значение хеш-функции от слова *cipher*. Последовательность

01111 0000 10001 01000 10010

разобьем на блоки по 4 бита и сложим побитово по модулю 2:

$$\begin{array}{r} 1111 \\ 0000 \\ 0100 \\ \oplus 0101 \\ \hline 0001 \\ \hline 0010 \\ \hline 1101. \end{array}$$

Итак  $h(\tilde{M}) = 13$ . Найдем  $k$  такое, что  $h(\tilde{M}) = h^k(M)$ , то есть

$$k = \log_{h(M)} h(\tilde{M}) = \log_6 13 \pmod{77},$$

так как  $h(M) = 6$  (см. пример 1). Поскольку числа небольшие, то эту задачу можно решить, перебирая степени числа 6 по модулю 77:

$$6^2 \equiv 36, \quad 6^3 \equiv -15 \equiv 62, \quad 6^4 \equiv -13 \equiv 64, \quad 6^5 \equiv -78 \equiv -1 \equiv 76,$$

$$6^6 \equiv -6 \equiv 71, \quad 6^7 \equiv -36 \equiv 41, \quad 6^8 \equiv 15, \quad 6^9 \equiv 13 \pmod{77}.$$

Значит,  $k = 9$  и правильная подпись вычисляется как

$$\tilde{s} \equiv s^9 \equiv 62^9 \pmod{77} \equiv 41.$$

### Схема подписи Рабина

Пусть  $n = pq$ , где  $p, q$  — различные большие простые числа. Подписываемое сообщение  $M$  представляется последовательностью двоичных битов

$$M = m_1 m_2 \dots m_t, \quad m_i \in \mathbf{Z}_2.$$

*Алгоритм вычисления подписи:*

1. Выработать случайный двоичный вектор  $r = (r_1 r_2 \dots r_s)$ ,  $r_i \in \mathbf{Z}_2$  и составить конкатенацию

$$M || r = (m_1 m_2 \dots m_t r_1 r_2 \dots r_s).$$

2. Последовательности  $M || r$  сопоставить целое число  $\alpha \in \mathbf{Z}_n$ . (Например, можно применить к  $M || r$  некоторую хеш-функцию и найти вычет хеш-образа по модулю  $n$ . )

3. Проверить, является ли  $\alpha$  квадратичным вычетом по модулю  $n$ . (Для проверки можно вычислить символы Лежандра  $\left(\frac{\alpha}{p}\right)$  и  $\left(\frac{\alpha}{q}\right)$ .) Если  $\alpha$  не является квадратом по модулю  $n$ , то возвратиться на шаг 1 и выработать другой вектор  $r$ .

Если  $\alpha$  является квадратом по модулю  $n$ , то вычислить

$$\sqrt{\alpha} \pmod{p} \equiv \beta_p \quad \text{и} \quad \sqrt{\alpha} \pmod{q} \equiv \beta_q$$

и найти  $\sqrt{\alpha} \pmod{n}$ , для чего следует решить систему сравнений:

$$\begin{cases} \beta \equiv \beta_p \pmod{p} \\ \beta \equiv \beta_q \pmod{q}. \end{cases}$$

Подписью для  $M$  является пара  $(r, \beta) = (r_1 r_2 \dots r_s, \beta)$ .

*Алгоритм проверки подписи:*

1. Вычислить  $\tilde{\alpha} \equiv \beta^2 \pmod{n}$ .
2. Последовательности  $M||r$  сопоставить целое число  $\alpha \in \mathbb{Z}_n$  (по тому же правилу, что и при вычислении подписи).
3. Если  $\tilde{\alpha} \equiv \alpha \pmod{n}$ , то подпись подлинная.

**Пример 13.** Пусть  $p = 15$ ,  $q = 31$ , значит,  $n = 13 \cdot 31 = 403$ . Подписать сообщение  $M = \text{round}$ .

Сначала запишем сообщение двоичными битами, пользуясь таблицей 2 и отводя под каждую букву сообщения по 5 двоичных битов:

$$M = \underbrace{10001}_r \underbrace{01110}_o \underbrace{10100}_u \underbrace{01101}_n \underbrace{00011}_d.$$

В качестве вектора  $r$  возьмем последовательность битов

$$0101000101,$$

тогда

$$M||r = 10001011101010001101000110101000101.$$

Целое число  $\alpha$  получим, применяя к полученной последовательности хеш-функцию побитового сложения по модулю два 5-битовых блоков, на которые разбивается последовательность

$M||r :$

10001  
01110  
10100  
 $\oplus$ 01101  
00011  
01010  
00101  
01010.

Поскольку  $01010_{(2)} = 10$  и

$$\begin{aligned} \left(\frac{10}{13}\right) &= \left(\frac{2}{13}\right) \left(\frac{5}{13}\right) = (-1)^{\frac{13^2-1}{8}} (-1)^{\frac{13-1}{2} \cdot \frac{5-1}{2}} \left(\frac{13}{5}\right) \\ &= (-1) \left(\frac{3}{5}\right) = (-1)(-1)^{\frac{5-1}{2} \cdot \frac{3-1}{2}} \left(\frac{5}{3}\right) = (-1) \left(\frac{2}{3}\right) = \\ &\quad (-1)(-1)^{\frac{3^2-1}{8}} = (-1)(-1) = 1, \\ \left(\frac{10}{31}\right) &= \left(\frac{2}{31}\right) \left(\frac{5}{31}\right) = (-1)^{\frac{31^2-1}{8}} (-1)^{\frac{31-1}{2} \cdot \frac{5-1}{2}} \left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = 1, \end{aligned}$$

то 10 является квадратом по модулю 403. Находим

$$\begin{cases} \sqrt{10} \pmod{13} \equiv 6 \\ \sqrt{10} \pmod{31} \equiv 14. \end{cases}$$

Далее решаем систему сравнений

$$\begin{cases} \beta \equiv 6 \pmod{13} \\ \beta \equiv 14 \pmod{31}. \end{cases}$$

Из первого сравнения имеем  $\beta = 6 + 13t$ , где  $t \in \mathbb{Z}$ . Подставляя полученное выражение во второе сравнение, получаем

$$6 + 13t \equiv 14 \pmod{31}$$

или  $13t \equiv 8 \pmod{31}$ , откуда  $t \equiv 3 \pmod{31}$  или  $t = 3 + 31k$ . Значит,  $\beta = 6 + 13(3 + 31k) = 45 + 403k$ , т. е.  $\beta \equiv 45 \pmod{403}$ . Итак, получена подпись под нашим сообщением  $(0101000101, 45)$ .

**Пример 14.** Проверить подпись  $(1010001010000001, 74)$  под сообщением  $M = \textit{standard}$ , если  $n = 391$ . Число  $\alpha$  получается с помощью хеш-функции предыдущего примера. Составим конкатенацию  $M||r$ :

1001010011000000110100011000001000100011101000101000001,

найдем число  $\alpha$ , складывая побитово по модулю два 5-битовые блоки, на которые разбивается полученная последовательность

$$\begin{array}{r} 10010 \\ 10011 \\ 00000 \\ 01101 \\ \oplus 00011 \\ 00000 \\ 10001 \\ 10100 \\ 01010 \\ \underline{00001} \\ 00010, \end{array}$$

т. е.  $\alpha = 2$ . Возведем  $\beta = 74$  в квадрат по модулю 391:

$\tilde{\alpha} = 74^2 = 5476 \equiv 2 \pmod{391}$ . Итак, подпись верна.

### Схема подписи Фиата – Шамира

Пусть  $h$  — хеш-функция, преобразующая любое исходное сообщение в битовую строку длины  $m$ . Пусть  $n = pq$ , где  $p$  и  $q$  — два различных простых числа. Секретным ключом служат  $m$  различных случайных чисел  $a_i \in \mathbf{Z}_n^*$ . Открытым ключом является набор из  $m$  чисел  $b_i \in \mathbf{Z}_n$ , где  $b_i \equiv (a_i^{(-1)})^2 \pmod{n}$ .

*Алгоритм вычисления подписи:*

1. Выбрать случайное число  $r$ ,  $1 \leq r \leq n - 1$ .
2. Вычислить  $u \equiv r^2 \pmod{n}$ .
3. Вычислить  $h(M||u) = (s_1 s_2 \dots s_m)$ .
4. Вычислить  $t \equiv r \prod_{i=1}^m a_i^{s_i} \pmod{n}$ .

Подписью для сообщения  $M$  служит пара  $(s_1 s_2 \dots s_m, t)$ .

*Алгоритм проверки подписи:*

1. Вычислить  $\omega \equiv t^2 \prod_{i=1}^m b_i^{s_i} \pmod{n}$ .
2. Вычислить  $h(M||\omega) = (s'_1 s'_2 \dots s'_m)$ .
3. Проверить равенство  $s_1 s_2 \dots s_m = s'_1 s'_2 \dots s'_m$ . Если оно выполнено, то подпись подлинная.

**Пример 15.** Пусть  $p = 7$ ,  $q = 11$ , тогда  $n = 77$ .

В качестве хеш-функции возьмем побитовое сложение по модулю два 4-битовых блоков, на которые разбивается наше сообщение, записанное в двоичной системе счисления, с присоединенным числом  $u$ , также записанным в двоичной системе счисления. Выход хеш-функции содержит 4 бита, значит, следует выбрать в качестве секретного ключа 4 случайных числа из  $\mathbb{Z}_{77}^*$ . Пусть это числа  $a_1 = 2$ ,  $a_2 = 3$ ,  $a_3 = 5$ ,  $a_4 = 13$ .

Выберем  $r = 4$ , тогда  $u \equiv 16 \pmod{77}$ . Подпишем сообщение  $M = \text{escape}$ . Запишем  $M$  последовательностью двоичных битов и присоединим двоичное представление  $u = 16 = 10000_{(2)}$  :

001001001000010000000011110010010000.

Разобьем полученную последовательность (начиная с конца) на 4-битовые блоки

$\underbrace{0001} \underbrace{0010} \underbrace{0100} \underbrace{0010} \underbrace{0000} \underbrace{0011} \underbrace{1100} \underbrace{1001} \underbrace{0000},$

дописывая в начало незначащий нуль. Теперь вычислим значе-



ние хеш-функции

$$\begin{array}{r}
 0001 \\
 0010 \\
 0100 \\
 0010 \\
 \oplus 0000 \\
 0011 \\
 1100 \\
 1001 \\
 \underline{0000} \\
 0011
 \end{array}$$

Тогда

$$t \equiv 4a_1^0 \cdot a_2^0 \cdot a_3^1 \cdot a_4^1 \equiv 4 \cdot 5 \cdot 13 \equiv 260 \equiv 29 \pmod{77}.$$

Получена подпись (0011, 29).

**Пример 16.** Проверить подпись (1110, 73) под сообщением *gate*, если хеш-функция вычисляется как в предыдущем примере, а открытый ключ есть  $b_1 = 58$ ,  $b_2 = 60$ ,  $b_3 = 37$ ,  $b_4 = 36$ . Вычислим

$$\omega = 73^2 \cdot b_1^1 \cdot b_2^1 \cdot b_3^1 \cdot b_4^0 \equiv 73^2 \cdot 58 \cdot 60 \cdot 37 \pmod{77} \equiv 25,$$

тогда  $M||\omega = 0011000000100110010011001$ .

Разбивая на 4-битовые блоки

$$\underbrace{0110} \quad \underbrace{0000} \quad \underbrace{0100} \quad \underbrace{1100} \quad \underbrace{1001} \quad \underbrace{1001}$$

и складывая побитово по модулю 2, получаем

$$\begin{array}{r}
 0110 \\
 0100 \\
 \oplus 1100 \\
 1001 \\
 \underline{1001} \\
 1110,
 \end{array}$$

откуда  $(s'_1 s'_2 s'_3 s'_4) = (1110)$ . Итак,  $(s'_1 s'_2 s'_3 s'_4) = (s_1, s_2, s_3, s_4)$ , значит, подпись верна.

## Цифровая подпись Эль Гамала

Стойкость этой подписи основана на сложности задачи дискретного логарифмирования. Пусть  $p$  — большое простое число,  $\alpha$  — примитивный элемент поля  $\mathbb{Z}_p$  (образующая мультипликативной группы поля  $\mathbb{Z}_p$ ). Секретный ключ  $a$  есть случайное число в интервале  $[1, p-2]$ .

Пусть  $\beta \equiv \alpha^a \pmod{p}$ . Открытый ключ — это набор  $(p, \alpha, \beta)$ .

### *Алгоритм вычисления подписи*

1. Выбрать случайное целое число  $r$ ,  $1 \leq r \leq p-2$ .
2. Вычислить  $\gamma \equiv \alpha^r \pmod{p}$ .
3. Для сообщения  $M$  вычислить  $\delta \equiv (M - a\gamma)r^{-1} \pmod{p-1}$ .  
Подписью под сообщением  $M$  служит пара  $(\gamma, \delta)$ .

**Замечание.** Поскольку для вычисления  $\delta$  требуется существование обратного элемента к  $r$  по модулю  $p-1$ , то при выборе  $r$  об этом следует позаботиться, т. е.  $r \in \mathbb{Z}_{p-1}^*$ .

### *Алгоритм проверки подписи*

1. Проверить неравенство  $\gamma < p$ . Если оно не выполнено, то подпись недействительна.

2. Проверить сравнение  $\beta^\gamma \gamma^\delta \equiv \alpha^M \pmod{p}$ .

Если оно выполняется, то подпись верна, в противном случае подпись недействительна.

**Замечание.** Число  $r$  тоже должно быть секретным, так как, зная это число и значение цифровой подписи под сообщением  $M$ , легко вычислить секретный ключ  $a$ . Действительно,

$$a \equiv (M - \delta r) \gamma^{-1} \pmod{p-1}.$$

Кроме того, число  $r$  не должно повторяться для различных подписей, полученных при одном значении секретного ключа.

В противном случае секретный ключ  $a$  также можно вычислить. Действительно, если для сообщений  $M_1$  и  $M_2$  использовать одно и то же число  $r$ , то  $\gamma_1 = \gamma_2 \equiv \alpha^r \pmod{p}$ , тогда

$$\alpha\gamma = M_1 - \delta_1 r \quad \text{и} \quad \alpha\gamma = M_2 - \delta_2 r,$$

откуда

$$M_1 - M_2 = (\delta_1 - \delta_2)r,$$

значит,

$$r \equiv (M_1 - M_2)(\delta_1 - \delta_2)^{-1} \pmod{p-1},$$

а знание  $r$ , как мы видели, позволяет найти секретный ключ  $a$ .

**Пример 17.** Пусть  $p = 47$ . В качестве образующей мультипликативной группы  $\mathbb{Z}_{47}^*$  можно взять  $\alpha = 5$ . Действительно, порядок этого элемента по модулю 47 равен 46, так как

$$\begin{aligned} 5^2 &\equiv 25 \pmod{47}, \\ 5^{23} &\equiv -1 \pmod{47}. \end{aligned}$$

Выберем секретный ключ  $a = 9$ , тогда  $\beta \equiv 5^9 \pmod{47} \equiv 40$ . Итак, открытый ключ есть  $(47, 9, 40)$ .

Вычислим подпись под сообщением  $M = 12$ . Возьмем в качестве  $r$  число 5 (5 обратимо по модулю 46). Тогда

$$\gamma \equiv 5^5 \pmod{47} \equiv 23,$$

$$\delta \equiv (12 - 9 \cdot 23)5^{-1} \pmod{46} \equiv 35 \cdot 37 \pmod{46} \equiv 7.$$

Значит, подписью является пара  $(23, 7)$ .

**Пример 18.** Получена подпись  $(15, 15)$  под сообщением  $M = 10$ . Зная открытый ключ  $(41, 7, 22)$ , проверить подпись.

По условию  $p = 41$ ,  $\alpha = 7$  и  $\beta = 22$ . Кроме того,  $\gamma = \delta = 15$ . Поскольку  $\gamma < 41$ , то остается проверить сравнение

$$\beta^\gamma \gamma^\delta \equiv \alpha^M \pmod{p}.$$

Сначала вычислим левую часть сравнения. Следует найти  $\beta^\gamma \equiv 22^{15} \pmod{41}$ . Имеем

$$\begin{aligned} 22^2 &= 484 \equiv 33 \pmod{41}, \\ 22^4 &\equiv 33^2 \equiv 1089 \equiv 23 \pmod{41}, \\ 22^8 &\equiv 23^2 \equiv 529 \equiv 37 \pmod{41}, \\ 22^{12} &\equiv 23 \cdot 37 \equiv 851 \equiv -10 \pmod{41}, \\ 22^{14} &\equiv (-10) \cdot 33 \equiv -330 \equiv -2 \pmod{41}, \\ 22^{15} &\equiv 22 \cdot (-2) \equiv -44 \equiv -3 \pmod{41}. \end{aligned}$$

Теперь вычислим  $\gamma^\delta \pmod{p} \equiv 15^{15} \pmod{41}$  :

$$\begin{aligned} 15^2 &= 225 \equiv 20 \pmod{41}, \\ 15^4 &\equiv 20^2 \equiv 400 \equiv -10 \pmod{41}, \\ 15^8 &\equiv (-10)^2 \equiv 100 \equiv 18 \pmod{41}, \\ 15^{12} &\equiv 18 \cdot (-10) \equiv -180 \equiv 25 \pmod{41}, \\ 15^{14} &\equiv 25 \cdot 20 \equiv 500 \equiv 8 \pmod{41}, \\ 15^{15} &\equiv 15 \cdot 8 \equiv 120 \equiv -3 \pmod{41}. \end{aligned}$$

Значит,  $\beta^\gamma \gamma^\delta \equiv (-3) \cdot (-3) \equiv 9 \pmod{41}$ .

Теперь вычислим число в правой части сравнения  $\alpha^M \equiv 7^{10} \pmod{41}$  :

$$\begin{aligned} 7^2 &\equiv 49 \equiv 8 \pmod{41}, \quad 7^4 \equiv 8^2 \equiv 64 \equiv 23 \pmod{41}, \\ 7^8 &\equiv 23^2 \equiv 529 \equiv 37 \pmod{41}, \quad 7^{10} \equiv 37 \cdot 8 \equiv 296 \equiv 9 \pmod{41}, \end{aligned}$$

т. е.  $\beta^\gamma \gamma^\delta \equiv 9 \equiv \alpha^M$ . Следовательно, подпись верна.

### Схема подписи Шнорра

Пусть  $p$  — простое число,  $q$  — простое число, делящее  $p-1$ . Рассмотрим подгруппу  $G$  порядка  $q$  в мультипликативной группе поля  $\mathbb{Z}_p$ . Пусть  $\alpha$  — образующая группы  $G$ , т. е. элемент порядка  $q$ . Секретным ключом является число  $a$ ,  $1 \leq a < q$ . Пусть  $\beta \equiv \alpha^a \pmod{p}$ . Открытым ключом является тройка  $(p, \alpha, \beta)$ .

*Алгоритм вычисления подписи:*

1. Выбрать случайное число  $r$ ,  $0 < r < q$ .
  2. Вычислить  $\gamma \equiv \alpha^r \pmod{p}$ .
  3. Вычислить  $\varepsilon = h(M||\gamma)$ , где  $h$  — выбранная хеш-функция,  $M$  — подписываемое сообщение.
  4. Вычислить  $\delta \equiv r - a\varepsilon \pmod{q}$ .
- Подписью под сообщением  $M$  является пара  $(\varepsilon, \delta)$ .

*Алгоритм проверки подписи:*

1. Вычислить  $\gamma' \equiv \alpha^\delta \beta^\varepsilon \pmod{p}$ .
2. Вычислить  $\varepsilon' = h(M||\gamma')$ .
3. Проверить равенство  $\varepsilon = \varepsilon'$ . Если оно выполняется, то подпись подлинная, иначе подпись недействительна.

**Пример 19.** Пусть  $p = 131$ . Мультипликативная группа  $\mathbb{Z}_{131}^*$  имеет порядок 130. Порядок подгруппы  $G$  должен делить число 130 и быть простым числом, очевидно,  $q = 13$ . Теперь найдем образующую в группе  $G$ . Для этого сначала найдем образующую группы  $\mathbb{Z}_{131}^*$ . Проверим элемент 2:

$$2^{10} = 1024 \equiv 107 \pmod{131},$$

$$2^{26} \equiv 53 \pmod{131},$$

$$2^{65} \equiv -1 \pmod{131},$$

значит, 2 является образующей группы  $\mathbb{Z}_{131}^*$ , тогда  $2^{10} \equiv 107$  есть элемент порядка 13 и может быть взят в качестве образующей группы  $G$ .

Выберем секретный ключ  $a = 4$ , тогда

$$\beta \equiv 107^4 \pmod{131} \equiv 84.$$

Пусть выбрана хеш-функция, являющаяся побитовым сложением по модулю два 4-битовых блоков конкатенации  $M||\gamma$ , где  $M$  и  $\gamma$  записаны в битовом представлении.

Вычислим подпись под сообщением  $M = \textit{fruit}$ , взяв  $r = 5$ .  
Имеем

$$\gamma \equiv 107^5 \pmod{131} \equiv 10784 \equiv 8988 \equiv 80 \pmod{131}.$$

Тогда, записывая каждую букву сообщения 5-битовым блоком, согласно таблице 2, а число  $\gamma$  представляя в двоичной системе последовательностью битов 1010000, получаем

$$M||\gamma = \underbrace{0010} \underbrace{1100} \underbrace{0110} \underbrace{1000} \underbrace{1000} \underbrace{1001} \underbrace{1101} \underbrace{0000}.$$

Вычислим хеш-функцию от  $M||\gamma$  :

$$\begin{array}{r} 0010 \\ 1100 \\ 0110 \\ \oplus 1000 \\ 1000 \\ 1001 \\ \underline{1101} \\ 1100_{(2)}. \end{array}$$

Так как  $1100_{(2)} = 12$ , то  $\delta = 5 - 4 \cdot 12 \pmod{13} \equiv 9$ .

Итак, подпись под нашим сообщением есть  $(12, 9)$ .

**Пример 20.** Проверить правильность подписи  $(12, 9)$ , полученной под сообщением *sparse*, если открытый ключ есть  $(131, 107, 62)$ , а хеш-функция определена так же, как в примере 19.

Вычислим  $\gamma' = \alpha^\delta \beta^\varepsilon$ . Сначала найдем  $\alpha^\delta$  и  $\beta^\varepsilon$  по модулю 131:

$$\alpha^\delta \equiv 107^9 \equiv (107^3)^3 \equiv 62^3 \equiv 39 \pmod{131},$$

$$\beta^\varepsilon \equiv 62^{12} \equiv 62^2 \cdot 62^4 \cdot 62^8 \equiv 45 \cdot 60 \cdot 63 \equiv 112 \pmod{131},$$

откуда  $\gamma' \equiv 39 \cdot 112 \pmod{131} \equiv 45$ , т. е.  $\gamma' = 101101_{(2)}$ .

Составим конкатенацию  $M||\gamma'$  :

$$100 \underbrace{1001} \underbrace{1110} \underbrace{0000} \underbrace{0001} \underbrace{0001} \underbrace{0010} \underbrace{1101}.$$

Значение хеш-функции найдем, складывая побитово по модулю два 4-битовые блоки полученной последовательности битов:

$$\begin{array}{r}
 0100 \\
 1001 \\
 1110 \\
 \oplus 0001 \\
 0001 \\
 0010 \\
 \underline{1101} \\
 1100_{(2)}
 \end{array}$$

т. е.  $\varepsilon' = 1100_{(2)} = 12$ . Значение  $\varepsilon'$  совпало с полученным значением  $\varepsilon$ , значит, подпись подлинная.

### Цифровая подпись Диффи – Лампорта

Эта цифровая подпись создана на основе симметричных систем шифрования. Сообщение представлено  $n$  двоичными битами

$$M = m_1 m_2 \dots m_n, \quad m_i \in \{0, 1\}, \quad i = 1, \dots, n.$$

Выбираем  $2n$  случайных секретных ключей, разбивая их на  $n$  пар:

$$K = [(k_{10}, k_{11}), (k_{20}, k_{21}), \dots, (k_{n0}, k_{n1})].$$

Эти ключи используются для шифрования выбранной симметричной криптосистемой. Алгоритм шифрования на ключе  $k_{ij}$  обозначим  $E_{k_{ij}}$ . Выберем  $n$  пар случайных чисел:

$$S = [(s_{10}, s_{11}), (s_{20}, s_{21}), \dots, (s_{n0}, s_{n1})],$$

где  $s_{ij} \in \{0, 1\}$ ,  $i = 1, \dots, n$ ;  $j = 1, 2$ , и вычислим значения

$$R_{ij} = E_{k_{ij}}(s_{ij}), \quad i = 1, \dots, n; \quad j = 0, 1.$$

Составим набор

$$R = [(R_{10}, R_{11}), (R_{20}, R_{21}), \dots, (R_{n0}, R_{n1})].$$

Наборы  $S$  и  $R$  являются открытыми. Подпись для сообщения  $M$  имеет вид

$$(k_{1m_1}, k_{2m_2}, \dots, k_{nm_n}).$$

Для проверки подписи следует убедиться, что выполнены равенства

$$R_{ij} = E_{k_{ij}}(s_{ij}), \quad j = m_i, \quad i = 1, \dots, n.$$

**Пример 21.** Пусть  $M = 10101_{(2)}$ . Выберем секретные ключи. Пусть

$$K = [(2, 1), (3, 1), (0, 1), (5, 1), (4, 3)]$$

и

$$S = [(1, 1), (0, 1), (0, 1), (1, 0), (0, 0)].$$

Выберем простейший алгоритм шифрования:

$$E_{k_{ij}}(s_{ij}) = s_{ij} \oplus k_{ij} \quad (i = 1, \dots, 5; j = 0, 1).$$

Теперь найдем набор  $R$  :

$$\begin{aligned} R_{10} &\equiv 1 + 2 \pmod{2} \equiv 1, & R_{11} &\equiv 1 + 1 \pmod{2} \equiv 0, \\ R_{20} &\equiv 3 + 0 \pmod{2} \equiv 1, & R_{21} &\equiv 1 + 1 \pmod{2} \equiv 0, \\ R_{30} &\equiv 0 + 0 \pmod{2} \equiv 0, & R_{31} &\equiv 1 + 1 \pmod{2} \equiv 0, \\ R_{40} &\equiv 1 + 5 \pmod{2} \equiv 0, & R_{41} &\equiv 0 + 1 \pmod{2} \equiv 1, \\ R_{50} &\equiv 0 + 4 \pmod{2} \equiv 0, & R_{51} &\equiv 0 + 3 \pmod{2} \equiv 1, \end{aligned}$$

значит,

$$R = [(1, 0), (1, 0), (0, 0), (0, 1), (0, 1)].$$

Подпись под сообщением  $M$  имеет вид

$$(k_{11}, k_{20}, k_{31}, k_{40}, k_{51}) = (1, 3, 1, 5, 3).$$



**Пример 22.** При тех же наборах открытых ключе  $S$  и  $R$  получена подпись  $(3, 5, 2, 7, 4)$  под сообщением  $= 11010_{(2)}$ . Проверим ее правильность. Так как  $m_1 = m_2 = m_4 = 1$ ,  $m_3 = m_5 = 0$ , то следует вычислить  $R_{11}$ ,  $R_{21}$ ,  $R_{30}$ ,  $R_{41}$  и  $R_{50}$ . (Считаем, что шифрование выполняется по правилу предыдущего примера.)

$$R_{11} \equiv k_{11} + s_{11} \pmod{2} \equiv 3 + 1 \equiv 0 \pmod{2},$$

$$R_{21} \equiv k_{21} + s_{21} \pmod{2} \equiv 5 + 1 \equiv 0 \pmod{2},$$

$$R_{30} \equiv k_{30} + s_{30} \pmod{2} \equiv 2 + 0 \equiv 0 \pmod{2},$$

$$R_{41} \equiv k_{41} + s_{41} \pmod{2} \equiv 7 + 0 \equiv 1 \pmod{2},$$

$$R_{50} \equiv k_{50} + s_{50} \pmod{2} \equiv 4 + 0 \equiv 0 \pmod{2}.$$

Поскольку полученные значения  $R_{ij}$  совпали с соответствующими элементами последовательности  $R$ , то подпись правильная.

## Задачи

### Задание 1

При помощи следующей таблицы зашифровать сообщение (в последней клетке таблицы номер 99 присвоен пробелу):

i	n	f	o	r	m	a
0	1	85	4	7	94	5
t	b	c	d	e	g	h
3	82	86	89	2	95	97
j	k	l	p	q	s	u
80	83	87	90	92	6	98
v	w	x	y	z	.	
81	84	88	91	93	96	99

1. *analytical geometry*;
2. *a smooth function*.

С помощью этой же таблицы расшифровать сообщение:

3. 39729989486989421369957299952198012995189993972996353  
294213699572993798397859887;
4. 3972996379886398729948599397299862878799864949087288.

При помощи следующей таблицы зашифровать сообщение  
(в последней клетке таблицы номер 99 присвоен пробелу):

c	o	n	f	i	d	e
80	4	1	88	0	94	2
t	a	l	b	g	h	j
3	5	85	89	92	95	97
k	m	p	q	r	s	u
81	83	86	90	7	6	98
v	w	x	y	z	.	
82	84	87	91	93	96	99

5. *the information is correct;*
6. *critical points are nondegenerate.*

С помощью этой же таблицы расшифровать сообщение:

7. 832940805859901884783530419906998041880942130585.

При помощи следующей таблицы зашифровать сообщение  
(в последней клетке таблицы номер 94 присвоен пробелу):

и	н	ф	о	р	м	а	ц
3	4	76	0	82	85	2	91
я	б	в	г	д	е	ж	з
70	73	77	80	83	1	88	92
к	л	п	с	т	у	х	ч
71	74	78	5	6	86	89	93
ш	щ	ы	ь	э	ю	.	
72	75	79	81	84	87	90	94

8. *достаточные условия существования;*
9. *компактный полиэдр.*

С помощью этой же таблицы расшифровать сообщение:

10. 7237682947882056039441822774092429340394922851479;

11. 718237860242743929478060934080094723768229492  
851479.

## Задание 2

Зашифровать сообщение шифром вертикальной перестановки на данном ключе:

1. *шифр табличного гаммирования*; **ключ**: (5,4,2,6,1,3);
2. *аффинный блочный шифр*; **ключ**: (4,5,2,1,6,3).

Расшифровать сообщение, зашифрованное шифром вертикальной перестановки на данном ключе:

3. *озвркаиатиаернижсиафеплрн*; **ключ**: (2,4,5,6,3,1);
4. *флгомнмаиуоряоомнрвашидгии*; **ключ**: (6,3,1,5,2,4).

Расшифровать сообщение, зашифрованное шифром вертикальной перестановки:

5. *мввусннжеоорсфянтрпеаиииие* (речь идет о шифровании);
6. *иноерощфнбзоеешаоиавсн* (речь идет о шифровании).

7. Расшифровать криптограмму

*озиерлпоесакдяттанрорек,*

если текст зашифрован вертикальной перестановкой, и известно, что ключ имеет длину 6, причем третья цифра ключа равна 6, а последняя равна 4.

## Задание 3

Зашифровать сообщение шифром гаммирования, используя данную формулу и данный ключ:

1. *код аутентификации или имитовставка*;  $y_i \equiv x_i + \gamma_i \pmod{n}$ ; **ключ**: гаммирование;
2. *протокол идентификации*;  $y_i \equiv x_i - \gamma_i \pmod{n}$ ; **ключ**: целостность;
3. *цифровая подпись*;  $y_i \equiv \gamma_i - x_i \pmod{n}$ ; **ключ**: вектор.

Расшифровать сообщение, зашифрованное шифром гаммирования на заданном ключе с использованием данной формулы:

4. *бцшхгг ёявшффэцн*;  $y_i \equiv x_i + \gamma_i \pmod{n}$ ; **ключ**: шифр;

5. *вфндяытх агдовт сыпктсьщаф*;  $y_i \equiv x_i - \gamma_i \pmod{n}$ ;

**ключ**: аутентификация;

6. *жфэьгзяг иочитгвизний*;  $y_i \equiv \gamma_i - x_i \pmod{n}$ ; **ключ**: целостность.

## Задание 4

Расшифровать две криптограммы, полученные с помощью шифра гаммирования, определенного формулой  $y_i \equiv x_i + \gamma_i \pmod{n}$ , на одном и том же ключе. Найти ключ шифрования:

1. *длягцюэйфэу; ёдеышсхахблзв* (в сообщениях есть слово "шифр");

2. *юебщцрэншыкяцхог; энсофщяетопщдккбыи* (в сообщениях имеется буквосочетание "квадр");

3. *тщжщнкягвуеячкягкнжб*;

*кнжбмлздюбаяглжрясыбоядуюд*

(в сообщениях есть слово "шифр");

4. *двыуумпуухтнёщвучектзяуьнийюээх; зуыщвфлсьлзсчюф-ефзяцяжщр* (в сообщениях есть слово "функция");

5. *ттезхлвщулифофкфепмнбьфи; ьбдхёоцуфсгыпгпёенд* (в сообщениях есть слово "предел").

## Задание 5

Пользуясь шифрсистемой RSA с  $n = pq$ , зашифровать данное сообщение на открытом ключе  $e$ . Найти секретный ключ:

1.  $p = 13$ ,  $q = 29$ ,  $e = 5$ ,  $h \in \mathbb{Z}_p$ ;

2.  $p = 11$ ,  $q = 17$ ,  $e = 7$ ,  $s \in \mathbb{Z}_t$ ;

3.  $p = 7$ ,  $q = 13$ ,  $e = 5$ ,  $a \in \mathbb{Z}_r$ ;

4.  $p = 5, \quad q = 23, \quad e = 3, \quad w \ i \ n \ k;$
5.  $p = 5, \quad q = 13, \quad e = 5, \quad c \ o \ n \ e.$

### Задание 6

Прочитать сообщение  $(C_1, C_2, \dots, C_k)$ , зашифрованное шифрсистемой RSA, если дано число  $n$  и секретный ключ  $d$ . Сообщение написано на английском языке:

1.  $(37, 56, 56), \quad n = 77, \quad d = 11;$
2.  $(25, 66, 78), \quad n = 95, \quad d = 5;$
3.  $(12, 0, 39), \quad n = 55, \quad d = 9;$
4.  $(74, 17), \quad n = 133, \quad d = 7;$
5.  $(1, 53, 32, 10), \quad n = 65, \quad d = 7.$

### Задание 7

Пользуясь шифрсистемой Эль-Гамала на открытом ключе  $\{p, \alpha, \beta\}$ , зашифровать сообщение  $M$ , взяв в качестве случайного показателя число  $r$  :

1.  $\{29, 2, 3\}, \quad M = 10, \quad r = 3;$
2.  $\{31, 3, 19\}, \quad M = 21, \quad r = 4;$
3.  $\{37, 2, 17\}, \quad M = 13, \quad r = 5;$
4.  $\{41, 7, 15\}, \quad M = 12, \quad r = 6;$
5.  $\{43, 3, 28\}, \quad M = 11, \quad r = 4.$

### Задание 8

Прочитать сообщение  $(C_1, C_2)$ , зашифрованное шифрсистемой Эль Гамала, если дано число  $p$  и секретный ключ  $a$  :

1.  $(9, 5), \quad p = 23, \quad a = 5;$
2.  $(8, 11), \quad p = 29, \quad a = 5;$
3.  $(32, 3), \quad p = 53, \quad a = 6;$
4.  $(31, 43), \quad p = 47, \quad a = 3;$
5.  $(5, 26) \quad p = 59, \quad a = 7.$

## Задание 9

Пользуясь шифрсистемой на основе *проблемы рюкзака*, зашифровать сообщение  $M$ , если секретный ключ состоит из су-  
первозрастающей последовательности  $(b_1, b_2, \dots, b_6)$ , чисел  $m$ ,  
 $w$  и подстановки  $\pi$ . Найти открытый ключ:

1.  $M = 31, (1, 2, 4, 8, 17), \quad m = 37, w = 3,$   
 $\pi = (13524);$
2.  $M = 27, (1, 3, 5, 11, 21), \quad m = 43, w = 4,$   
 $\pi = (14253);$
3.  $M = 57, (1, 2, 4, 8, 16, 32), \quad m = 71, w = 3,$   
 $\pi = (132)(456);$
4.  $M = 45, (1, 4, 6, 12, 34, 68), \quad m = 137, w = 7,$   
 $\pi = (152436);$
5.  $M = 43, (1, 3, 5, 10, 20, 40), \quad m = 83, w = 5,$   
 $\pi = (134526).$

## Задание 10

Прочитать сообщение, зашифрованное шифрсистемой на ос-  
нове *проблемы рюкзака*, если дан секретный ключ  
 $(b_1, b_2, \dots, b_6)$ ,  $m$ ,  $w$  и  $\pi$ :

1.  $C = 23, (1, 2, 4, 8, 17), \quad m = 37, w = 3,$   
 $\pi = (13524);$
2.  $C = 41, (1, 3, 5, 11, 21), \quad m = 43, w = 4,$   
 $\pi = (14253);$
3.  $C = 32, (1, 2, 4, 8, 16, 32), \quad m = 71, w = 3,$   
 $\pi = (132)(456);$
4.  $C = 118, (1, 4, 6, 12, 34, 68), \quad m = 137, w = 7,$   
 $\pi = (152436);$

$$5. \quad C = 6, (1, 3, 5, 10, 20, 40), \quad m = 83, w = 5, \\ \pi = (134526).$$

### Задание 11

Вычислить подпись под данным сообщением по схеме RSA, если даны числа  $p$ ,  $q$  и секретный ключ  $d$ . Хэш-код получается побитовым сложением по модулю два  $k$ -битовых блоков, на которые разбивается сжимаемое сообщение. (Каждая буква сообщения представляется 5-битовым блоком своего числового эквивалента.) Найти открытый ключ  $e$ .

1. *code*,  $p = 11, q = 17, d = 23, k = 5$ ;
2. *rule*,  $p = 7, q = 13, d = 17, k = 5$ ;
3. *last*,  $p = 5, q = 19, d = 17, k = 5$ ;
4. *most*,  $p = 7, q = 11, d = 11, k = 5$ ;
5. *state*,  $p = 11, q = 19, d = 19, k = 5$ .

### Задание 12

Получено сообщение с подписью  $s$ . Проверить подпись, если она вычислена по схеме RSA с модулем  $n$  и открытым ключом  $e$ . Хэш-код получается побитовым сложением по модулю два  $k$ -битовых блоков, на которые разбивается сжимаемое сообщение. Каждая буква сообщения представляется 5-битовым блоком своего числового эквивалента:

1. *mark*,  $s = 4, n = 91, e = 17, k = 5$ ;
2. *cork*,  $s = 8, n = 115, e = 21, k = 3$ ;
3. *cane*,  $s = 25, n = 133, e = 13, k = 3$ ;
4. *sun*,  $s = 106, n = 143, e = 11, k = 3$ ;
5. *one*,  $s = 154, n = 161, e = 23, k = 5$ .

### Задание 13

Используя систему RSA с данным модулем  $n$ , подделать подпись для данного сообщения  $M_1$ , если известна правильная подпись  $s$  под сообщением  $M$  и хэш-код  $h$  сообщения  $M$  ( $h = h(M)$ ). Значение хэш-функции для сообщения  $M_1$  получается побитовым сложением по модулю два  $k$ -битовых блоков, на которые разбивается сообщение  $M_1$ , каждая буква которого записана своим битовым числовым эквивалентом:

1. *may*,  $n = 187$ ,  $s = 181$ ,  $h = 3$ ,  $k = 5$ ;
2. *matter*,  $n = 65$ ,  $s = 41$ ,  $h = 11$ ,  $k = 5$ ;
3. *fare*,  $n = 91$ ,  $s = 75$ ,  $h = 17$ ,  $k = 5$ ;
4. *matter*,  $n = 77$ ,  $s = 49$ ,  $h = 7$ ,  $k = 5$ ;
5. *much*,  $n = 115$ ,  $s = 73$ ,  $h = 13$ ,  $k = 5$ .

### Задание 14

Вычислить подпись под данным сообщением по схеме Рабина, если даны  $p$ ,  $q$  и случайный вектор  $r$ . Хэш-код получается побитовым сложением по модулю два 5-битовых блоков, на которые разбивается сообщение с присоединенным вектором  $r$  :

1. *round*,  $p = 13$ ,  $q = 31$ ,  $r = (0101000101)$ ;
2. *lot*,  $p = 11$ ,  $q = 19$ ,  $r = (1010000001)$ ;
3. *room*,  $p = 11$ ,  $q = 13$ ,  $r = (1011001000)$ ;
4. *while*,  $p = 7$ ,  $q = 17$ ,  $r = (1110101001)$ ;
5. *copper*,  $p = 17$ ,  $q = 23$ ,  $r = (1001101000)$ .

### Задание 15

Получено данное сообщение с подписью  $(r, \beta)$ . Проверить подпись, если она вычислена по схеме Рабина с открытым ключом  $n$ . Хэш-код вычисляется как побитовое сложение по модулю два 5-битовых блоков, на которые разбивается данное сообщение с присоединенным вектором  $r$  :



1. *month*,  $r = (0010111000)$ ,  $\beta = 385$ ,  $n = 551$ ;
2. *many*,  $r = (0111010010)$ ,  $\beta = 446$ ,  $n = 551$ ;
3. *company*,  $r = (1010101101)$ ,  $\beta = 380$ ,  $n = 527$ ;
4. *sugar*,  $r = (0010110011)$ ,  $\beta = 103$ ,  $n = 589$ ;
5. *model*,  $r = (1001110001)$ ,  $\beta = 44$ ,  $n = 481$ .

### Задание 16

Пользуясь цифровой подписью Фиата – Шамира, подписать данное сообщение, если дано число  $n$ , набор секретных ключей  $(a_1, a_2, \dots, a_s)$  и число  $r$ . Каждую букву передаваемого сообщения представить в виде 5-битовой последовательности, присоединяемую цифру  $u$  записать в двоичной системе счисления. Хеш-функция есть побитовое сложение по модулю два  $k$ -битовых блоков полученной последовательности  $M||u$ . Вычислить набор открытых ключей:

1. *fruit*,  $n = 77$ ,  $(2, 3, 5, 13, 15)$ ,  $r = 5$ ,  $k = 5$ ;
2. *system*,  $n = 65$ ,  $(3, 7, 11, 19, 23)$ ,  $r = 5$ ,  $k = 5$ ;
3. *clock*,  $n = 143$ ,  $(2, 4, 5, 7)$ ,  $r = 7$ ,  $k = 4$ ;
4. *press*,  $n = 91$ ,  $(3, 5, 6, 15)$ ,  $r = 15$ ,  $k = 4$ ;
5. *change*,  $n = 95$ ,  $(3, 4, 7, 13)$ ,  $r = 13$ ,  $k = 4$ .

### Задание 17

Проверить подпись  $(s_1, s_2, \dots, s_l, t)$  под данным сообщением, если она вычислена по схеме Фиата – Шамира, причем дано число  $n$  и открытый ключ  $(b_1, b_2, \dots, b_m)$ . Каждая буква передаваемого сообщения представлена в виде 5-битовой последовательности, а присоединяемая цифра  $u$  записывается в двоичной системе счисления. Хеш-функция есть побитовое сложение

по модулю два  $k$ -битовых блоков полученной последовательности:

1. *escape*, (01111, 73),  $n = 77$ , (58, 60, 37, 36, 64),  $k = 5$ ;
2. *circle*, (00110, 56),  $n = 65$ , (29, 4, 36, 56, 29),  $k = 5$ ;
3. *music*, (1000, 16),  $n = 143$ , (36, 9, 103, 108),  $k = 4$ ;
4. *rmember*, (1011, 55),  $n = 91$ , (81, 51, 43, 36),  $k = 4$ ;
5. *porch*, (1011, 22),  $n = 95$ , (74, 6, 64, 9),  $k = 4$ .

### Задание 18

Подписать сообщение  $M$  по схеме Эль Гамала, если даны  $p$ ,  $\alpha$ , секретный ключ  $a$  и случайное число  $r$  :

1.  $M = 21$ ,  $p = 67$ ,  $\alpha = 2$ ,  $a = 13$ ,  $r = 7$ ;
2.  $M = 11$ ,  $p = 43$ ,  $\alpha = 3$ ,  $a = 6$ ,  $r = 5$ ;
3.  $M = 12$ ,  $p = 67$ ,  $\alpha = 2$ ,  $a = 8$ ,  $r = 7$ ;
4.  $M = 19$ ,  $p = 47$ ,  $\alpha = 5$ ,  $a = 5$ ,  $r = 5$ ;
5.  $M = 18$ ,  $p = 53$ ,  $\alpha = 2$ ,  $a = 9$ ,  $r = 11$ .

### Задание 19

Получено сообщение с подписью  $(\gamma, \delta)$ . Проверить подпись, если она вычислена по схеме Эль Гамала и известен открытый ключ  $p$ ,  $\alpha$ ,  $\beta$  :

1.  $M = 12$ , (15, 19),  $p = 41$ ,  $\alpha = 7$ ,  $\beta = 38$ ;
2.  $M = 10$ , (23, 25),  $p = 47$ ,  $\alpha = 5$ ,  $\beta = 40$ ;
3.  $M = 15$ , (22, 27),  $p = 53$ ,  $\alpha = 2$ ,  $\beta = 34$ ;
4.  $M = 13$ , (28, 25),  $p = 43$ ,  $\alpha = 3$ ,  $\beta = 25$ ;
5.  $M = 22$ , (15, 14),  $p = 41$ ,  $\alpha = 7$ ,  $\beta = 23$ .

### Задание 20

Пользуясь цифровой подписью Шнорра, подписать данное сообщение, если даны  $p$ ,  $q$ ,  $\alpha$ , секретный ключ  $a$  и случайное

число  $r$ . Каждая буква передаваемого сообщения представляется в виде 5-битовой последовательности, а присоединяемая цифра  $\gamma$  записывается в двоичной системе счисления. Хеш-функция есть побитовое сложение по модулю два  $k$ -битовых блоков полученной последовательности:

1. *tongue*,  $p = 59, q = 29, \alpha = 4, a = 5, r = 6, k = 5$ ;
2. *frost*,  $p = 151, q = 15, \alpha = 2, a = 3, r = 5, k = 5$ ;
3. *name*,  $p = 151, q = 10, \alpha = 92, a = 2, r = 7, k = 4$ ;
4. *habit*,  $p = 107, q = 53, \alpha = 4, a = 6, r = 7, k = 4$ ;
5. *flame*,  $p = 83, q = 41, \alpha = 4, a = 7, r = 11, k = 5$ .

### Задание 21

Проверить подпись  $(\varepsilon, \delta)$  под данным сообщением, если она вычислена по схеме цифровой подписи Шнорра с данными  $p, q, \alpha$  и  $\beta$ . Каждая буква передаваемого сообщения представляется в виде 5-битовой последовательности, а присоединяемая цифра  $\gamma$  записывается в двоичной системе счисления. Хеш-функция есть побитовое сложение по модулю два  $k$ -битовых блоков полученной последовательности:

1. *region*,  $(2, 7), p = 131, q = 13, \alpha = 107, \beta = 84, k = 4$ ;
2. *segment*,  $(2, 2), p = 89, q = 11, \alpha = 4, \beta = 2, k = 4$ ;
3. *cloud*,  $(7, 6), p = 67, q = 11, \alpha = 14, \beta = 64, k = 5$ ;
4. *cover*,  $(23, 7), p = 47, q = 23, \alpha = 25, \beta = 8, k = 5$ ;
5. *barn*,  $(10, 5), p = 53, q = 13, \alpha = 16, \beta = 24, k = 4$ .

### Ответы

1.

1).515879130865879995249423791;

2).599694443979985981863041;

3). *the documents are genuine and the statements are truthful*;

4). *the structure of the cell complex*;

- 5). 3952990188478353041990699804772803;
- 6). 807030805859986401369957299141942922127532;
- 7). *medical information is confidential*;
- 8). 83056260934791948657407737094586751567707724370;
- 9). 71085782716479394780743848382;
- 10). *шифр простой неравнозначной замены*;
- 11). *криптоанализ поточного шифра замены*.

## 2.

- 1). *тнмарчавилорьяомнишбгиифиго*; 2). *илиноифйыаынрн-чфббй*; 3). *криптоанализ шифра Виженера*; 4). *шифр модульного гаммирования*; 5). *система шифрования по Виженеру*; **ключ:** (2,7,4,5,3,1,6); 6). *зашифрованное сообщение*; **ключ:** (4,6,5,1,3,2); 7). *протокол разделения секрета*; **ключ:** (3,2,6,5,1,4).

## 3.

- 1). *нор мъгунтцэннагхс цгк изсчсвюяитцв*; 2). *цлгдэшбэ чсичнэёчштзчц*; 3). *лъцаовё ыдкбщуро*; 4). *индекс совпадения*; 5). *взаимный индекс совпадения*; 6). *протокол идентификации*.

## 4.

- 1). *блочный шифр*; *групповой шифр*; **гамма:** *гусли*; 2). *латинский квадрат*; *квадратная решетка*; **гамма:** *теория*;
- 3). *аффинный поточный шифр*; *шифр модульного гаммирования*; **гамма:** *тетраэдр*; 4). *функция действительной переменной*; *непрерывная функция в точке*; **гамма:** *полиэдр*;
- 5). *предел последовательности*; *ряд сходится к пределу*; **гамма:** *квадрат*.

## 5.

- 1). (243,58,297); 2). (1,85,145); 3). (23,75); 4). (8,110,101,28); 5). (54,38,56).

## 6.

- 1). *try*; 2). *van*; 3). *may*; 4). *key*; 5). *lock*.

## 7.

- 1). (8,9); 2). (19,30); 3). (32,25); 4). (20,19); 5). (38,25).

**8.**

1).  $M=15$ ; 2).  $M=9$ ; 3).  $M=23$ ; 4).  $M=14$ ; 5).  $M=16$ .

**9.**

1). 22; 2). 31; 3). 45; 4). 78; 5). 76.

**10.**

1). 7; 2). 8; 3). 15; 4). 54; 5). 25.

**11.**

1). 88; 2). 10; 3). 40; 4). 47; 5). 22.

**12.**

1). – 5). подпись верна.

**13.**

1). 113; 2). 31; 3). 74; 4). 56; 5). 94.

**14.**

1). (0101000101,110); 2). (1000000011,180); 3). (1011001000,82);  
4). (1110101001,108); 5). (1001101000,74).

**15.**

1). – 5). подпись верна.

**16.**

1). (00010,65); 2). (11010,45); 3). (1000,14); 4). (0111,16);  
5). (1000,39).

**17.**

1). – 5). подпись верна.

**18.**

1). (61,50); 2). (28,19); 3). (61,64); 4). (23,36); 5). (34,40).

**19.**

1). – 5). подпись верна.

**20.**

1). (31,25); 2). (22,14); 3). (4,9); 4). (13,35); 5). (27,27).

**21.**

1). – 5). подпись верна.

# Задачи для самостоятельного решения

## Задание 1

Зашифровать сообщение шифром вертикальной перестановки на данном ключе:

1. (4, 3, 1, 5, 2, 7, 6); *he that buys land buys many stones;*
2. (2, 5, 1, 3, 4); *a thought tha tbrings me hope;*
3. (6, 5, 1, 3, 2, 4); *so much has been given away;*
4. (3, 7, 1, 6, 4, 2, 5); *kind hearts are more than coronets;*
5. (4, 1, 5, 3, 6, 2); *here are a little proverb;*
6. (4, 3, 5, 1, 2); *get it off your chest;*
7. (6, 4, 1, 3, 2, 5); *too wise to take counsel;*
8. (4, 3, 5, 2, 1); *he fled for his life;*
9. (7, 5, 2, 6, 3, 4, 1); *he grinned from ear to ear;*
10. (6, 3, 8, 5, 1, 4, 2, 7); *the critical mood becomes the creative attitude;*
11. (5, 4, 2, 3, 6, 1); *la grandmere a donne une double reponse;*
12. (4, 6, 1, 5, 3, 2); *courir en tirant la langue;*
13. (3, 7, 5, 1, 4, 2, 6); *prendre quelque une sous son aile;*
14. (3, 1, 5, 2, 4); *prendre les mains nues;*
15. (3, 6, 1, 5, 2, 4); *etre suspendu a un cheveu;*
16. (4, 2, 5, 1, 3); *never torment your soul;*
17. (3, 6, 5, 7, 2, 1, 4); *a little proverb that you ough to know;*
18. (2, 6, 5, 1, 4, 3); *day comes again tomorrow;*
19. (4, 1, 5, 3, 2); *so little remains behind;*
20. (2, 6, 5, 3, 1, 4); *voila on chien est enterre;*
21. (5, 3, 4, 1, 2); *mesurer à sa toise;*
22. (3, 5, 2, 1, 4); *le monde est étroit;*
23. (6, 3, 1, 5, 2, 4); *ne pas se trouver de place;*
24. (3, 5, 2, 1, 6, 4); *muet comme un poisson;*
25. (4, 1, 5, 3, 2); *ni deux ni un et demi;*
26. (4, 3, 1, 5, 2); *ne pas sentir ses pieds;*

27. (5, 3, 6, 1, 2, 4); *ni vers levillage ni vers la ville;*
28. (3, 6, 1, 5, 4, 2); *cela ne ressemble à rien;*
29. (2, 5, 6, 1, 3, 4); *verser du vide dans du creux;*
30. (3, 5, 1, 6, 2, 4); *la première hirondelle.*

## Задание 2

Расшифровать сообщение, зашифрованное шифром вертикальной перестановки на данном ключе (знак ' считать буквой):

1. (4, 2, 1, 5, 3), *lddherecvpaseiueuge;*
2. (5, 1, 2, 3, 4), *erlqleseusvecseco;*
3. (4, 5, 2, 6, 1, 3), *râartssesetnomdosueenletbds;*
4. (3, 2, 4, 5, 6, 1), *givbeclcïtaleatcidoeurenseasn;*
5. (3, 5, 4, 6, 2, 7, 1), *odmhseeanuaoeypssefnusaltsrsc;*
6. (2, 5, 4, 1, 3), *rbllftrseeaeimelaode;*
7. (3, 4, 1, 5, 2), *trardêjheteoleest;*
8. (3, 4, 5, 1, 6, 2), *riguesq' ofouuiarenitlderus;*
9. (4, 2, 1, 5, 3), *iruaodgeiafsrnrtr;*
10. (2, 1, 5, 6, 4, 3), *eaucivsveafnpulundataé;*
11. (6, 5, 2, 3, 1, 4), *vaheeranndcéone' elislsm;*
12. (3, 4, 7, 6, 1, 5, 2), *euspqcrupuhslloeereuatqe érlsss;*
13. (3, 7, 6, 1, 4, 5, 2), *nyunrxqgadudeeiulaxqurue';*
14. (2, 4, 1, 5, 3), *zelhdiueecqus é necargo;*
15. (7, 2, 6, 4, 5, 3, 1), *uhoulsgqcdeudreucqetseoi;*
16. (4, 5, 1, 6, 3, 2), *tcnedmonmcsrereueeoe;*
17. (2, 4, 6, 3, 1, 5), *dmclnrfeeeiscéaaarld;*
18. (3, 5, 6, 1, 4, 2), *yueeueo ôlxnutertcects é sodls;*
19. (4, 2, 5, 6, 1, 3), *eolesemunalxtmsen é ysfs;*
20. (3, 5, 2, 1, 4), *luaromprlnesiasa;*
21. (5, 1, 2, 3, 6, 4), *nrrefutroneetcpueeovneoe;*
22. (4, 6, 2, 1, 3, 5), *ttlñîrsiroesmstmeusauea;*
23. (3, 4, 6, 5, 2, 1), *eelatmuserulvccneoambeloedn;*
24. (4, 1, 5, 2, 6, 3), *erarvnucuosepurersidn;*

25. (2, 5, 4, 6, 3, 1), *eeonicrunéegccuvanorehuctprneuer*;
26. (3, 1, 6, 2, 4, 5), *emrnsfsnllruaoocteuoddsies*;
27. (3, 7, 2, 5, 4, 1, 6), *eeenaàciaaofdneesuhrmmlplu*;
28. (5, 1, 3, 6, 2, 7, 4), *puenyooprssrstasloutbeuu*;
29. (6, 7, 1, 2, 4, 5, 3), *mcaomhrmleueolrsenesrospn*;
30. (3, 6, 1, 2, 4, 5), *trnlratsvogoudupeeeie*.

### Задание 3

Расшифровать сообщение, зашифрованное шифром гаммирования на данном ключе  $\Gamma$  по формуле  $y_i \equiv \gamma_i - x_i \pmod{n}$ , где  $\gamma_i$  — буква ключа,  $x_i$  — буква открытого текста,  $y_i$  — буква криптограммы:

1.  $\Gamma = \textit{question}$ ; *fu loae vzwdro*;
2.  $\Gamma = \textit{malade}$ ; *mvgara kmzoz kz pxgo*;
3.  $\Gamma = \textit{asperites}$ ; *ampcn riaamklm*;
4.  $\Gamma = \textit{poisson}$ ; *ykvpbk cp cuffofl le as zflme*;
5.  $\Gamma = \textit{tenebres}$ ; *iav bxxh rfluaaj zqfa kaa mrwbp*;
6.  $\Gamma = \textit{corneille}$ ; *xojwa xh saqzz*;
7.  $\Gamma = \textit{blanche}$ ; *wlswy rxxakty fxntw cyp sbuygyp lnzzjyp*;
8.  $\Gamma = \textit{frapper}$ ; *arsyl oxbgkvl ckrzw elm tbxd klnfbz*;
9.  $\Gamma = \textit{locutions}$ ; *folrpr lnft up sfrzv fxgl*;
10.  $\Gamma = \textit{phenomenes}$ ; *wdrfx srj pklqnj lmrvc mec pafb*;
11.  $\Gamma = \textit{dependance}$ ; *rehruznfl tz rlf vzpzp tz jlru*;
12.  $\Gamma = \textit{responsabilites}$ ; *za zlbfb xbut qpm grwfx*;
13.  $\Gamma = \textit{oblige}$ ; *vxyap mo qlvakk yhrpwkkh qcm lxyo*;
14.  $\Gamma = \textit{histoire}$ ; *zx s io xrrboo iavlkd*;
15.  $\Gamma = \textit{personnage}$ ; *kejbk lgamzkaa s ncnne*;
16.  $\Gamma = \textit{habituer}$ ; *nnx xfhyxd yuigcqe*;
17.  $\Gamma = \textit{surpasser}$ ; *duaawfkn ryx dywkhtna*;
18.  $\Gamma = \textit{supplanter}$ ; *xgrpfwv rfgg vc asjynn*;
19.  $\Gamma = \textit{realisation}$ ; *wwfue qmhwk lkeh hp qtleb*;
20.  $\Gamma = \textit{courant}$ ; *hgzaw lfqcq zgw zp tggynq*;



21.  $\Gamma = \text{etoile}$ ; *wi o xl tegioh dwpb thrbzk*;
22.  $\Gamma = \text{renfermer}$ ; *dr ybky ua prmvbn gm treytb*;
23.  $\Gamma = \text{buissons}$ ; *zgoay osoz ro nkd mhbhg*;
24.  $\Gamma = \text{projet}$ ; *be zvkcyr df cfvwxbn ql phjpppxr*;
25.  $\Gamma = \text{coutures}$ ; *qkdyqjthyw rthz kf joilc*;
26.  $\Gamma = \text{silencieux}$ ; *yvh ctuxtqgo i jei y pqaeoq aav vekdta*;
27.  $\Gamma = \text{terrain}$ ; *ie odgjnlnr og fftdgn*;
28.  $\Gamma = \text{corneille}$ ; *qojhne jxsqk xaa iaakqkyua*;
29.  $\Gamma = \text{montagne}$ ; *la fawp kau ljzd rfajw*;
30.  $\Gamma = \text{grincement}$ ; *se tjil aabp brawy nykcpp gi mctba*.

#### Задание 4

Пользуясь шифрсистемой RSA с  $n = pq$ , зашифровать данные сообщения на открытом ключе  $e$ . Найти секретный ключ:

1.  $p = 5, \quad q = 29, \quad e = 3, \quad m \text{ е о р у я};$
2.  $p = 7, \quad q = 23, \quad e = 5, \quad o \text{ т е л ь};$
3.  $p = 11, \quad q = 13, \quad e = 7, \quad c \text{ о д е};$
4.  $p = 17, \quad q = 19, \quad e = 5, \quad h \text{ е а d};$
5.  $p = 5, \quad q = 29, \quad e = 5, \quad к \text{ у р с ы};$
6.  $p = 7, \quad q = 23, \quad e = 7, \quad л \text{ е м м а};$
7.  $p = 11, \quad q = 13, \quad e = 11, \quad d \text{ u s t};$
8.  $p = 17, \quad q = 19, \quad e = 11, \quad r \text{ а с е};$
9.  $p = 5, \quad q = 29, \quad e = 9, \quad к \text{ а н а л};$
10.  $p = 7, \quad q = 23, \quad e = 13, \quad м \text{ у н у с};$
11.  $p = 11, \quad q = 13, \quad e = 13, \quad b \text{ u r n};$
12.  $p = 17, \quad q = 19, \quad e = 13, \quad h \text{ а n d};$
13.  $p = 5, \quad q = 29, \quad e = 11, \quad я \text{ д р о};$
14.  $p = 7, \quad q = 23, \quad e = 17, \quad n \text{ л ю с};$
15.  $p = 11, \quad q = 13, \quad e = 17, \quad f \text{ i r e};$
16.  $p = 17, \quad q = 19, \quad e = 7, \quad v \text{ о t e};$
17.  $p = 5, \quad q = 29, \quad e = 13, \quad с \text{ в я з ь};$
18.  $p = 7, \quad q = 23, \quad e = 19, \quad з \text{ н а к};$

19.  $p = 11, \quad q = 13, \quad e = 19, \quad g \ r \ i \ e \ f;$
20.  $p = 17, \quad q = 19, \quad e = 17, \quad r \ a \ i \ n;$
21.  $p = 5, \quad q = 17, \quad e = 5, \quad м \ a \ ч \ т \ a;$
22.  $p = 7, \quad q = 19, \quad e = 11, \quad т \ o \ ч \ к \ a;$
23.  $p = 5, \quad q = 17, \quad e = 11, \quad f \ l \ a \ s \ h;$
24.  $p = 7, \quad q = 19, \quad e = 7, \quad т \ a \ r \ k;$
25.  $p = 5, \quad q = 17, \quad e = 7, \quad к \ p \ a \ н;$
26.  $p = 7, \quad q = 19, \quad e = 5, \quad в \ e \ т \ e \ p;$
27.  $p = 7, \quad q = 19, \quad e = 13, \quad b \ o \ a \ r;$
28.  $p = 5, \quad q = 17, \quad e = 13, \quad s \ o \ n \ g;$
29.  $p = 5, \quad q = 17, \quad e = 9, \quad з \ a \ n \ a \ x;$
30.  $p = 7, \quad q = 19, \quad e = 17, \quad g \ l \ o \ v \ e.$

### Задание 5

Прочитать сообщение  $(C_1, C_2, \dots, C_k)$ , зашифрованное шифрсистемой RSA, если дано число  $n$  и секретный ключ  $d$ . Сообщение написано на английском языке:

1.  $(173, 128), \quad n = 253, \quad d = 17;$
2.  $(159, 4, 64), \quad n = 187, \quad d = 7;$
3.  $(1, 44, 60, 25), \quad n = 115, \quad d = 21;$
4.  $(13, 1, 0, 47), \quad n = 95, \quad d = 17;$
5.  $(32, 41, 54, 20), \quad n = 85, \quad d = 5;$
6.  $(41, 32, 56), \quad n = 65, \quad d = 7;$
7.  $(46, 18, 73, 42), \quad n = 77, \quad d = 11;$
8.  $(130, 122), \quad n = 253, \quad d = 21;$
9.  $(85, 44, 110), \quad n = 187, \quad d = 13;$
10.  $(1, 35, 83, 36), \quad n = 115, \quad d = 23;$
11.  $(11, 24, 90), \quad n = 95, \quad d = 5;$
12.  $(9, 14, 40), \quad n = 85, \quad d = 13;$
13.  $(50, 43, 42), \quad n = 65, \quad d = 17;$
14.  $(50, 71, 114), \quad n = 143, \quad d = 11;$
15.  $(22, 0, 160), \quad n = 253, \quad d = 9;$

16.  $(34, 38, 69), \quad n = 187, \quad d = 31;$
17.  $(3, 50, 61, 57), \quad n = 95, \quad d = 7;$
18.  $(8, 66, 56), \quad n = 85, \quad d = 19;$
19.  $(53, 58, 62), \quad n = 65, \quad d = 23;$
20.  $(31, 60, 51), \quad n = 65, \quad d = 31;$
21.  $(143, 89, 76), \quad n = 145, \quad d = 15;$
22.  $(22, 64, 73), \quad n = 145, \quad d = 33;$
23.  $(68, 37, 63), \quad n = 145, \quad d = 39;$
24.  $(66, 1, 80), \quad n = 91, \quad d = 29;$
25.  $(1, 27, 46, 3), \quad n = 91, \quad d = 31;$
26.  $(8, 3, 1, 24), \quad n = 87, \quad d = 19;$
27.  $(49, 47, 33), \quad n = 87, \quad d = 13;$
28.  $(1, 86, 87, 34), \quad n = 93, \quad d = 11;$
29.  $(1, 76, 108, 46), \quad n = 111, \quad d = 29;$
30.  $(69, 111, 38), \quad n = 143, \quad d = 11.$

### Задание 6

Пользуясь шифрсистемой Эль-Гамала на открытом ключе  $\{p, \alpha, \beta\}$ , зашифровать сообщение  $M$ , взяв в качестве случайного показателя число  $r$  :

1.  $\{43, 3, 30\}, \quad M = 27, \quad r = 5;$
2.  $\{47, 5, 21\}, \quad M = 15, \quad r = 7;$
3.  $\{37, 2, 13\}, \quad M = 23, \quad r = 9;$
4.  $\{31, 11, 6\}, \quad M = 16, \quad r = 4;$
5.  $\{41, 6, 24\}, \quad M = 29, \quad r = 6;$
6.  $\{37, 5, 16\}, \quad M = 31, \quad r = 10;$
7.  $\{53, 8, 48\}, \quad M = 18, \quad r = 4;$
8.  $\{59, 6, 47\}, \quad M = 12, \quad r = 11;$
9.  $\{61, 7, 57\}, \quad M = 23, \quad r = 10;$
10.  $\{67, 2, 18\}, \quad M = 13, \quad r = 7;$

11.  $\{43, 5, 24\}$ ,  $M = 15$ ,  $r = 3$ ;
12.  $\{47, 13, 32\}$ ,  $M = 21$ ,  $r = 9$ ;
13.  $\{37, 5, 18\}$ ,  $M = 19$ ,  $r = 13$ ;
14.  $\{31, 3, 17\}$ ,  $M = 29$ ,  $r = 5$ ;
15.  $\{41, 7, 13\}$ ,  $M = 11$ ,  $r = 3$ ;
16.  $\{37, 2, 18\}$ ,  $M = 25$ ,  $r = 11$ ;
17.  $\{53, 3, 14\}$ ,  $M = 6$ ,  $r = 9$ ;
18.  $\{59, 2, 40\}$ ,  $M = 47$ ,  $r = 13$ ;
19.  $\{61, 2, 6\}$ ,  $M = 33$ ,  $r = 13$ ;
20.  $\{67, 7, 57\}$ ,  $M = 22$ ,  $r = 7$ ;
21.  $\{71, 7, 59\}$ ,  $M = 13$ ,  $r = 8$ ;
22.  $\{73, 5, 59\}$ ,  $M = 41$ ,  $r = 6$ ;
23.  $\{79, 3, 6\}$ ,  $M = 33$ ,  $r = 8$ ;
24.  $\{83, 2, 56\}$ ,  $M = 11$ ,  $r = 3$ ;
25.  $\{89, 3, 17\}$ ,  $M = 23$ ,  $r = 4$ ;
26.  $\{97, 5, 21\}$ ,  $M = 39$ ,  $r = 7$ ;
27.  $\{71, 7, 8\}$ ,  $M = 15$ ,  $r = 10$ ;
28.  $\{73, 5, 15\}$ ,  $M = 43$ ,  $r = 11$ ;
29.  $\{79, 3, 12\}$ ,  $M = 45$ ,  $r = 2$ ;
30.  $\{83, 2, 45\}$ ,  $M = 20$ ,  $r = 5$ .

### Задание 7

Прочитать сообщение  $(C_1, C_2)$ , зашифрованное шифрсистемой Эль Гамаля, если дано число  $p$  и секретный ключ  $a$  :

1.  $(32, 14)$ ,  $p = 67$ ,  $a = 23$ ;
2.  $(22, 11)$ ,  $p = 53$ ,  $a = 11$ ;
3.  $(40, 6)$ ,  $p = 47$ ,  $a = 7$ ;
4.  $(18, 16)$ ,  $p = 37$ ,  $a = 13$ ;
5.  $(6, 35)$ ,  $p = 61$ ,  $a = 13$ ;

6.  $(25, 13), p = 43, a = 10;$
7.  $(12, 7), p = 31, a = 5;$
8.  $(8, 66), p = 71, a = 7;$
9.  $(23, 18), p = 59, a = 9;$
10.  $(22, 29), p = 41, a = 6;$
11.  $(13, 52), p = 67, a = 13;$
12.  $(34, 48), p = 53, a = 7;$
13.  $(13, 39), p = 47, a = 5;$
14.  $(15, 17), p = 37, a = 8;$
15.  $(44, 13), p = 61, a = 11;$
16.  $(12, 15), p = 43, a = 5;$
17.  $(25, 12), p = 31, a = 7;$
18.  $(4, 20), p = 71, a = 6;$
19.  $(10, 36), p = 59, a = 17;$
20.  $(12, 20), p = 41, a = 7;$
21.  $(27, 23), p = 89, a = 8;$
22.  $(43, 39), p = 97, a = 8;$
23.  $(64, 91), p = 101, a = 13;$
24.  $(3, 55), p = 73, a = 11;$
25.  $(12, 62), p = 79, a = 16;$
26.  $(32, 25), p = 83, a = 8;$
27.  $(22, 67), p = 89, a = 10;$
28.  $(8, 54), p = 97, a = 10;$
29.  $(28, 69), p = 101, a = 9;$
30.  $(27, 7), p = 71, a = 31.$

### Задание 8

Пользуясь шифрсистемой на основе *проблемы рюкзака*, зашифровать сообщение  $M$ , если секретный ключ состоит из су-

первозрастающей последовательности  $(b_1, b_2, \dots, b_6)$ , чисел  $m$ ,  $w$  и подстановки  $\pi$ . Найти открытый ключ:

1.  $M = 59, (1, 4, 6, 12, 25, 50), \quad m = 101, w = 5,$   
 $\pi = (143562);$
2.  $M = 37, (1, 3, 7, 13, 26, 51), \quad m = 107, w = 3,$   
 $\pi = (153624);$
3.  $M = 41, (1, 2, 5, 9, 19, 37), \quad m = 79, w = 4,$   
 $\pi = (163452);$
4.  $M = 53, (1, 3, 5, 11, 21, 43), \quad m = 89, w = 6,$   
 $\pi = (136245);$
5.  $M = 43, (1, 3, 6, 12, 23, 47), \quad m = 97, w = 7,$   
 $\pi = (146352);$
6.  $M = 61, (1, 4, 7, 13, 26, 53), \quad m = 107, w = 5,$   
 $\pi = (135)(246);$
7.  $M = 49, (1, 2, 4, 9, 17, 35), \quad m = 71, w = 3,$   
 $\pi = (135426);$
8.  $M = 38, (1, 5, 7, 14, 29, 57), \quad m = 131, w = 5,$   
 $\pi = (146)(253);$
9.  $M = 29, (1, 4, 8, 15, 30, 60), \quad m = 131, w = 7,$   
 $\pi = (154)(263);$
10.  $M = 37, (1, 2, 5, 11, 20, 41), \quad m = 83, w = 5,$   
 $\pi = (136)(245);$
11.  $M = 49, (1, 4, 6, 12, 25, 50), \quad m = 107, w = 7,$   
 $\pi = (153624);$
12.  $M = 25, (1, 3, 7, 15, 26, 51), \quad m = 113, w = 6,$   
 $\pi = (135642);$
13.  $M = 62, (1, 2, 5, 9, 19, 37), \quad m = 83, w = 8,$   
 $\pi = (125463);$

14.  $M = 57, (1, 3, 5, 11, 21, 43), \quad m = 97, w = 9,$   
 $\pi = (135264);$
15.  $M = 63, (1, 3, 6, 12, 23, 47), \quad m = 101, w = 11,$   
 $\pi = (132546);$
16.  $M = 55, (1, 4, 7, 13, 26, 53), \quad m = 113, w = 10,$   
 $\pi = (143)(265);$
17.  $M = 45, (1, 2, 4, 9, 17, 35), \quad m = 79, w = 7,$   
 $\pi = (136)(254);$
18.  $M = 28, (1, 5, 7, 14, 29, 57), \quad m = 137, w = 9,$   
 $\pi = (163524);$
19.  $M = 27, (1, 4, 8, 15, 30, 60), \quad m = 137, w = 4,$   
 $\pi = (134652);$
20.  $M = 51, (1, 2, 5, 11, 20, 41), \quad m = 89, w = 11,$   
 $\pi = (153)(426);$
21.  $M = 62, (1, 7, 9, 19, 38, 75), \quad m = 151, w = 2,$   
 $\pi = (136245);$
22.  $M = 59, (1, 3, 5, 10, 20, 41), \quad m = 83, w = 4,$   
 $\pi = (154623);$
23.  $M = 39, (1, 2, 6, 11, 21, 42), \quad m = 89, w = 3,$   
 $\pi = (163542);$
24.  $M = 43, (1, 4, 8, 15, 29, 60), \quad m = 127, w = 5,$   
 $\pi = (146)(523);$
25.  $M = 47, (1, 5, 8, 15, 30, 60), \quad m = 127, w = 6,$   
 $\pi = (135)(264);$
26.  $M = 49, (1, 7, 9, 19, 38, 75), \quad m = 157, w = 7,$   
 $\pi = (135264);$
27.  $M = 37, (1, 3, 5, 10, 20, 41), \quad m = 89, w = 9,$   
 $\pi = (145263);$

28.  $M = 63, (1, 2, 6, 11, 21, 42), \quad m = 97, w = 8,$   
 $\pi = (164325);$
29.  $M = 45, (1, 4, 8, 15, 29, 60), \quad m = 131, w = 3,$   
 $\pi = (153)(264);$
30.  $M = 47, (1, 5, 8, 15, 30, 60), \quad m = 131, w = 10,$   
 $\pi = (154263).$

### Задание 9

Прочитать сообщение  $C$ , зашифрованное шифрсистемой на основе *проблемы рюкзака*, если дан секретный ключ  $(b_1, b_2, \dots, b_6), m, w$  и  $\pi$  :

1.  $C = 60, \quad (1, 3, 5, 11, 21, 43), m = 89, \quad w = 3,$   
 $\pi = (146523);$
2.  $C = 53, \quad (1, 4, 6, 13, 25, 51), m = 103, \quad w = 4,$   
 $\pi = (153642);$
3.  $C = 77, \quad (1, 2, 5, 9, 20, 39), m = 79, \quad w = 5,$   
 $\pi = (1345)(26);$
4.  $C = 66, \quad (1, 5, 7, 15, 30, 60), m = 131, \quad w = 7,$   
 $\pi = (156)(243);$
5.  $C = 80, \quad (1, 3, 6, 12, 24, 47), m = 97, \quad w = 6,$   
 $\pi = (163524);$
6.  $C = 4, \quad (1, 4, 7, 13, 26, 52), m = 107, \quad w = 3,$   
 $\pi = (124365);$
7.  $C = 26, \quad (1, 2, 4, 8, 17, 35), m = 71, \quad w = 10,$   
 $\pi = (145362);$
8.  $C = 108, \quad (1, 5, 7, 14, 29, 57), m = 127, \quad w = 11,$   
 $\pi = (156432);$



9.  $C = 61$ ,  $(1, 6, 8, 17, 33, 66)$ ,  $m = 131$ ,  $w = 9$ ,  
 $\pi = (1463)(25)$ ;
10.  $C = 88$ ,  $(1, 3, 7, 12, 24, 48)$ ,  $m = 97$ ,  $w = 2$ ,  
 $\pi = (136452)$ ;
11.  $C = 46$ ,  $(1, 3, 5, 11, 21, 43)$ ,  $m = 97$ ,  $w = 5$ ,  
 $\pi = (13)(26)(45)$ ;
12.  $C = 51$ ,  $(1, 4, 6, 13, 25, 51)$ ,  $m = 107$ ,  $w = 6$ ,  
 $\pi = (146)(235)$ ;
13.  $C = 13$ ,  $(1, 2, 5, 9, 20, 39)$ ,  $m = 83$ ,  $w = 3$ ,  
 $\pi = (14)(2536)$ ;
14.  $C = 67$ ,  $(1, 5, 7, 15, 30, 60)$ ,  $m = 137$ ,  $w = 2$ ,  
 $\pi = (15)(24)(36)$ ;
15.  $C = 67$ ,  $(1, 3, 6, 12, 24, 47)$ ,  $m = 101$ ,  $w = 9$ ,  
 $\pi = (156432)$ ;
16.  $C = 87$ ,  $(1, 4, 7, 13, 26, 52)$ ,  $m = 109$ ,  $w = 6$ ,  
 $\pi = (123546)$ ;
17.  $C = 30$ ,  $(1, 2, 4, 8, 17, 35)$ ,  $m = 83$ ,  $w = 9$ ,  
 $\pi = (154)(263)$ ;
18.  $C = 47$ ,  $(1, 5, 7, 14, 29, 57)$ ,  $m = 131$ ,  $w = 8$ ,  
 $\pi = (143526)$ ;
19.  $C = 45$ ,  $(1, 6, 8, 17, 33, 66)$ ,  $m = 137$ ,  $w = 4$ ,  
 $\pi = (152)(463)$ ;
20.  $C = 31$ ,  $(1, 3, 7, 12, 24, 48)$ ,  $m = 101$ ,  $w = 7$ ,  
 $\pi = (154263)$ ;
21.  $C = 70$ ,  $(1, 2, 4, 9, 17, 35)$ ,  $m = 71$ ,  $w = 5$ ,  
 $\pi = (143265)$ ;
22.  $C = 3$ ,  $(1, 3, 5, 10, 21, 41)$ ,  $m = 83$ ,  $w = 4$ ,  
 $\pi = (163542)$ ;

23.  $C = 70$ ,  $(1, 4, 6, 13, 25, 50)$ ,  $m = 101$ ,  $w = 2$ ,  
 $\pi = (136254)$ ;
24.  $C = 31$ ,  $(1, 5, 7, 14, 28, 56)$ ,  $m = 113$ ,  $w = 3$ ,  
 $\pi = (125634)$ ;
25.  $C = 85$ ,  $(1, 3, 6, 11, 22, 44)$ ,  $m = 89$ ,  $w = 6$ ,  
 $\pi = (154)(263)$ ;
26.  $C = 29$ ,  $(1, 2, 4, 9, 17, 35)$ ,  $m = 83$ ,  $w = 4$ ,  
 $\pi = (145326)$ ;
27.  $C = 28$ ,  $(1, 3, 5, 10, 21, 41)$ ,  $m = 89$ ,  $w = 3$ ,  
 $\pi = (164235)$ ;
28.  $C = 74$ ,  $(1, 4, 6, 13, 25, 50)$ ,  $m = 103$ ,  $w = 5$ ,  
 $\pi = (135246)$ ;
29.  $C = 70$ ,  $(1, 5, 7, 14, 28, 56)$ ,  $m = 127$ ,  $w = 6$ ,  
 $\pi = (123546)$ ;
30.  $C = 61$ ,  $(1, 3, 6, 11, 22, 44)$ ,  $m = 101$ ,  $w = 2$ ,  
 $\pi = (146)(253)$ .

### Задание 10

Вычислить подпись под данным сообщением по схеме RSA, если даны числа  $p$ ,  $q$  и секретный ключ  $d$ . Хэш-код получается побитовым сложением по модулю два  $k$ -битовых блоков, на которые разбивается сжимаемое сообщение. (Каждая буква сообщения представляется 5-битовым блоком своего числового эквивалента.) Найти открытый ключ  $e$ .

1. *cover*,  $p = 11$ ,  $q = 13$ ,  $d = 13$ ,  $k = 5$ ;
2. *coat*,  $p = 5$ ,  $q = 29$ ,  $d = 33$ ,  $k = 5$ ;
3. *shrub*,  $p = 17$ ,  $q = 19$ ,  $d = 19$ ,  $k = 5$ ;
4. *scrap*,  $p = 7$ ,  $q = 23$ ,  $d = 29$ ,  $k = 5$ ;

5. *piece*,  $p = 11$ ,  $q = 17$ ,  $d = 21$ ,  $k = 5$ ;
6. *heap*,  $p = 11$ ,  $q = 23$ ,  $d = 23$ ,  $k = 5$ ;
7. *pile*,  $p = 5$ ,  $q = 23$ ,  $d = 15$ ,  $k = 5$ ;
8. *camp*,  $p = 5$ ,  $q = 11$ ,  $d = 13$ ,  $k = 4$ ;
9. *laurel*,  $p = 5$ ,  $q = 13$ ,  $d = 11$ ,  $k = 4$ ;
10. *tune*,  $p = 5$ ,  $q = 17$ ,  $d = 11$ ,  $k = 4$ ;
11. *palm*,  $p = 5$ ,  $q = 19$ ,  $d = 13$ ,  $k = 4$ ;
12. *valve*,  $p = 7$ ,  $q = 13$ ,  $d = 5$ ,  $k = 4$ ;
13. *eraser*,  $p = 7$ ,  $q = 17$ ,  $d = 7$ ,  $k = 4$ ;
14. *swan*,  $p = 7$ ,  $q = 19$ ,  $d = 5$ ,  $k = 4$ ;
15. *lion*,  $p = 7$ ,  $q = 29$ ,  $d = 11$ ,  $k = 3$ ;
16. *track*,  $p = 5$ ,  $q = 29$ ,  $d = 23$ ,  $k = 3$ ;
17. *light*,  $p = 11$ ,  $q = 13$ ,  $d = 19$ ,  $k = 3$ ;
18. *blade*,  $p = 17$ ,  $q = 19$ ,  $d = 35$ ,  $k = 3$ ;
19. *ribbon*,  $p = 11$ ,  $q = 23$ ,  $d = 31$ ,  $k = 3$ ;
20. *pose*,  $p = 11$ ,  $q = 17$ ,  $d = 31$ ,  $k = 3$ ;
21. *nurse*,  $p = 13$ ,  $q = 17$ ,  $d = 11$ ,  $k = 5$ ;
22. *charge*,  $p = 5$ ,  $q = 31$ ,  $d = 11$ ,  $k = 4$ ;
23. *case*,  $p = 7$ ,  $q = 11$ ,  $d = 11$ ,  $k = 3$ ;
24. *wind*,  $p = 11$ ,  $q = 19$ ,  $d = 7$ ,  $k = 3$ ;
25. *life*,  $p = 13$ ,  $q = 19$ ,  $d = 31$ ,  $k = 5$ ;
26. *ocean*,  $p = 5$ ,  $q = 37$ ,  $d = 17$ ,  $k = 4$ ;
27. *paint*,  $p = 7$ ,  $q = 31$ ,  $d = 17$ ,  $k = 3$ ;
28. *circle*,  $p = 11$ ,  $q = 29$ ,  $d = 11$ ,  $k = 5$ ;
29. *plumb*,  $p = 5$ ,  $q = 41$ ,  $d = 3$ ,  $k = 4$ ;
30. *reply*,  $p = 7$ ,  $q = 37$ ,  $d = 7$ ,  $k = 3$ .

## Задание 11

Получено сообщение с подписью  $s$ . Проверить подпись, если она вычислена по схеме RSA с модулем  $n$  и открытым ключом  $e$ . Хэш-код получается побитовым сложением по модулю два  $k$ -битовых блоков, на которые разбивается сжимаемое сообщение. Каждая буква сообщения представляется 5-битовым блоком своего числового эквивалента:

1. *barter*,  $s = 72$ ,  $n = 203$ ,  $e = 13$ ,  $k = 3$ ;
2. *match*,  $s = 257$ ,  $n = 323$ ,  $e = 17$ ,  $k = 3$ ;
3. *june*,  $s = 118$ ,  $n = 145$ ,  $e = 33$ ,  $k = 3$ ;
4. *offer*,  $s = 142$ ,  $n = 161$ ,  $e = 19$ ,  $k = 4$ ;
5. *winter*,  $s = 46$ ,  $n = 143$ ,  $e = 11$ ,  $k = 3$ ;
6. *spring*,  $s = 41$ ,  $n = 119$ ,  $e = 17$ ,  $k = 4$ ;
7. *range*,  $s = 18$ ,  $n = 115$ ,  $e = 49$ ,  $k = 3$ ;
8. *ransom*,  $s = 61$ ,  $n = 91$ ,  $e = 59$ ,  $k = 4$ ;
9. *brush*,  $s = 61$ ,  $n = 133$ ,  $e = 59$ ,  $k = 5$ ;
10. *bunch*,  $s = 14$ ,  $n = 253$ ,  $e = 49$ ,  $k = 4$ ;
11. *store*,  $s = 83$ ,  $n = 95$ ,  $e = 31$ ,  $k = 3$ ;
12. *show*,  $s = 149$ ,  $n = 187$ ,  $e = 89$ ,  $k = 5$ ;
13. *rest*,  $s = 65$ ,  $n = 85$ ,  $e = 13$ ,  $k = 4$ ;
14. *brush*,  $s = 15$ ,  $n = 55$ ,  $e = 37$ ,  $k = 3$ ;
15. *store*,  $s = 37$ ,  $n = 65$ ,  $e = 17$ ,  $k = 3$ ;
16. *way*,  $s = 109$ ,  $n = 145$ ,  $e = 69$ ,  $k = 4$ ;
17. *branch*,  $s = 128$ ,  $n = 253$ ,  $e = 17$ ,  $k = 4$ ;
18. *way*,  $s = 54$ ,  $n = 85$ ,  $e = 57$ ,  $k = 5$ ;
19. *amuse*,  $s = 113$ ,  $n = 187$ ,  $e = 31$ ,  $k = 5$ ;
20. *letter*,  $s = 9$ ,  $n = 95$ ,  $e = 61$ ,  $k = 3$ ;
21. *level*,  $s = 77$ ,  $n = 259$ ,  $e = 23$ ,  $k = 5$ ;

22. *half*,  $s = 9$ ,  $n = 205$ ,  $e = 13$ ,  $k = 5$ ;
23. *show*,  $s = 280$ ,  $n = 319$ ,  $e = 17$ ,  $k = 4$ ;
24. *cake*,  $s = 24$ ,  $n = 217$ ,  $e = 7$ ,  $k = 3$ ;
25. *note*,  $s = 180$ ,  $n = 185$ ,  $e = 5$ ,  $k = 5$ ;
26. *stick*,  $s = 105$ ,  $n = 247$ ,  $e = 11$ ,  $k = 4$ ;
27. *point*,  $s = 100$ ,  $n = 209$ ,  $e = 17$ ,  $k = 5$ ;
28. *ration*,  $s = 37$ ,  $n = 77$ ,  $e = 13$ ,  $k = 5$ ;
29. *ferry*,  $s = 19$ ,  $n = 155$ ,  $e = 13$ ,  $k = 4$ ;
30. *disk*,  $s = 125$ ,  $n = 221$ ,  $e = 7$ ,  $k = 5$ .

## Задание 12

Используя систему RSA с данным  $n$ , подделать подпись для данного сообщения  $M_1$ , если известна правильная подпись  $s$  под сообщением  $M$  и хэш-код  $h$  сообщения  $M$  ( $h = h(M)$ ). Значение хэш-функции для сообщения  $M_1$  получается побитовым сложением по модулю два  $k$ -битовых блоков, на которые разбивается сообщение  $M_1$ , каждая буква которого записана своим 5-битовым числовым эквивалентом:

1. *swan*,  $n = 203$ ,  $s = 72$ ,  $h = 2$ ,  $k = 4$ ;
2. *tiger*,  $n = 323$ ,  $s = 257$ ,  $h = 2$ ,  $k = 5$ ;
3. *palm*,  $n = 145$ ,  $s = 118$ ,  $h = 3$ ,  $k = 4$ ;
4. *pile*,  $n = 161$ ,  $s = 142$ ,  $h = 9$ ,  $k = 5$ ;
5. *swan*,  $n = 143$ ,  $s = 50$ ,  $h = 6$ ,  $k = 4$ ;
6. *rest*,  $n = 119$ ,  $s = 54$ ,  $h = 3$ ,  $k = 4$ ;
7. *store*,  $n = 115$ ,  $s = 18$ ,  $h = 3$ ,  $k = 4$ ;
8. *swan*,  $n = 91$ ,  $s = 61$ ,  $h = 17$ ,  $k = 4$ ;
9. *swan*,  $n = 133$ ,  $s = 61$ ,  $h = 17$ ,  $k = 4$ ;
10. *scrap*,  $n = 253$ ,  $s = 14$ ,  $h = 15$ ,  $k = 5$ ;
11. *prize*,  $n = 95$ ,  $s = 83$ ,  $h = 7$ ,  $k = 5$ ;

12. *merry*,  $n = 187$ ,  $s = 149$ ,  $h = 13$ ,  $k = 5$ ;
13. *owner*,  $n = 85$ ,  $s = 65$ ,  $h = 5$ ,  $k = 4$ ;
14. *stand*,  $n = 55$ ,  $s = 15$ ,  $h = 5$ ,  $k = 5$ ;
15. *palm*,  $n = 65$ ,  $s = 27$ ,  $h = 7$ ,  $k = 4$ ;
16. *swan*,  $n = 145$ ,  $s = 109$ ,  $h = 4$ ,  $k = 4$ ;
17. *fight*,  $n = 253$ ,  $s = 128$ ,  $h = 6$ ,  $k = 5$ ;
18. *bunch*,  $n = 85$ ,  $s = 54$ ,  $h = 14$ ,  $k = 5$ ;
19. *cover*,  $n = 187$ ,  $s = 113$ ,  $h = 14$ ,  $k = 5$ ;
20. *prize*,  $n = 95$ ,  $s = 9$ ,  $h = 4$ ,  $k = 5$ ;
21. *train*,  $n = 253$ ,  $s = 33$ ,  $h = 15$ ,  $k = 4$ ;
22. *drum*,  $n = 55$ ,  $s = 47$ ,  $h = 5$ ,  $k = 4$ ;
23. *cross*,  $n = 187$ ,  $s = 101$ ,  $h = 14$ ,  $k = 4$ ;
24. *step*,  $n = 115$ ,  $s = 43$ ,  $h = 16$ ,  $k = 4$ ;
25. *bird*,  $n = 203$ ,  $s = 23$ ,  $h = 2$ ,  $k = 4$ ;
26. *song*,  $n = 133$ ,  $s = 85$ ,  $h = 17$ ,  $k = 5$ ;
27. *flame*,  $n = 119$ ,  $s = 27$ ,  $h = 3$ ,  $k = 4$ ;
28. *film*,  $n = 85$ ,  $s = 63$ ,  $h = 5$ ,  $k = 5$ ;
29. *raft*,  $n = 145$ ,  $s = 19$ ,  $h = 3$ ,  $k = 3$ ;
30. *dress*,  $n = 133$ ,  $s = 5$ ,  $h = 15$ ,  $k = 5$ .

### Задание 13

Вычислить подпись под данным сообщением по схеме Рабина, если даны  $p$ ,  $q$  и случайный вектор  $r$ . Хэш-код получается побитовым сложением по модулю два 5-битовых блоков, на которые разбивается сообщение с присоединенным вектором  $r$  :

1. *change*,  $p = 29$ ,  $q = 43$ ,  $r = (1101001000)$ ;
2. *music*,  $p = 13$ ,  $q = 23$ ,  $r = (1001010001)$ ;
3. *riddle*,  $p = 17$ ,  $q = 43$ ,  $r = (1000001001)$ ;

4. *break*,  $p = 11$ ,  $q = 19$ ,  $r = (1001101000)$ ;
5. *floor*,  $p = 13$ ,  $q = 23$ ,  $r = (1000100010)$ ;
6. *shift*,  $p = 17$ ,  $q = 23$ ,  $r = (0010100110)$ ;
7. *shout*,  $p = 11$ ,  $q = 13$ ,  $r = (1011001001)$ ;
8. *urgent*,  $p = 19$ ,  $q = 23$ ,  $r = (1010101010)$ ;
9. *bridge*,  $p = 17$ ,  $q = 23$ ,  $r = (1010100001)$ ;
10. *octave*,  $p = 19$ ,  $q = 29$ ,  $r = (1100110000)$ ;
11. *window*,  $p = 11$ ,  $q = 31$ ,  $r = (0101100110)$ ;
12. *address*,  $p = 23$ ,  $q = 31$ ,  $r = (0110101010)$ ;
13. *name*,  $p = 17$ ,  $q = 31$ ,  $r = (0101001101)$ ;
14. *plain*,  $p = 19$ ,  $q = 31$ ,  $r = (0010000010)$ ;
15. *nurse*,  $p = 29$ ,  $q = 31$ ,  $r = (0011100101)$ ;
16. *mark*,  $p = 29$ ,  $q = 31$ ,  $r = (0101001001)$ ;
17. *chair*,  $p = 13$ ,  $q = 31$ ,  $r = (1010100011)$ ;
18. *spot*,  $p = 17$ ,  $q = 31$ ,  $r = (0111100111)$ ;
19. *border*,  $p = 29$ ,  $q = 31$ ,  $r = (0101100100)$ ;
20. *whale*,  $p = 13$ ,  $q = 37$ ,  $r = (1000100011)$ ;
21. *guard*,  $p = 23$ ,  $q = 37$ ,  $r = (1010011000)$ ;
22. *game*,  $p = 19$ ,  $q = 43$ ,  $r = (1000111001)$ ;
23. *order*,  $p = 11$ ,  $q = 43$ ,  $r = (0111000010)$ ;
24. *master*,  $p = 17$ ,  $q = 41$ ,  $r = (1001101001)$ ;
25. *fruit*,  $p = 17$ ,  $q = 43$ ,  $r = (1010100001)$ ;
26. *wind*,  $p = 31$ ,  $q = 41$ ,  $r = (1011001100)$ ;
27. *burden*,  $p = 31$ ,  $q = 41$ ,  $r = (0010100011)$ ;
28. *danger*,  $p = 11$ ,  $q = 37$ ,  $r = (1010001010)$ ;
29. *lemon*,  $p = 31$ ,  $q = 43$ ,  $r = (1101010100)$ ;
30. *flier*,  $p = 29$ ,  $q = 37$ ,  $r = (1010100001)$ .

## Задание 14

Получено данное сообщение с подписью  $(r, \beta)$ . Проверить подпись, если она вычислена по схеме Рабина с открытым ключом  $n$ . Хэш-код вычисляется как побитовое сложение по модулю два 5-битовых блоков, на которые разбивается данное сообщение с присоединенным вектором  $r$  :

1. *smile*,  $r = (1001000011)$ ,  $\beta = 294$ ,  $n = 697$ ;
2. *cirve*,  $r = (1001110001)$ ,  $\beta = 294$ ,  $n = 1271$ ;
3. *example*,  $r = (0101001101)$ ,  $\beta = 100$ ,  $n = 1247$ ;
4. *piece*,  $r = (0101101100)$ ,  $\beta = 304$ ,  $n = 943$ ;
5. *tram*,  $r = (1001101001)$ ,  $\beta = 384$ ,  $n = 1271$ ;
6. *table*,  $r = (0111000110)$ ,  $\beta = 94$ ,  $n = 1763$ ;
7. *author*,  $r = (0111100101)$ ,  $\beta = 309$ ,  $n = 1591$ ;
8. *consul*,  $r = (1011001000)$ ,  $\beta = 215$ ,  $n = 943$ ;
9. *shelter*,  $r = (1010100011)$ ,  $\beta = 344$ ,  $n = 533$ ;
10. *family*,  $r = (1010101001)$ ,  $\beta = 354$ ,  $n = 1333$ ;
11. *arrow*,  $r = (1001000101)$ ,  $\beta = 313$ ,  $n = 731$ ;
12. *order*,  $r = (0111000101)$ ,  $\beta = 1124$ ,  $n = 1271$ ;
13. *wing*,  $r = (0101011001)$ ,  $\beta = 480$ ,  $n = 817$ ;
14. *lace*,  $r = (1001101011)$ ,  $\beta = 1160$ ,  $n = 1517$ ;
15. *porch*,  $r = (1001000001)$ ,  $\beta = 609$ ,  $n = 989$ ;
16. *flour*,  $r = (0110000011)$ ,  $\beta = 344$ ,  $n = 1517$ ;
17. *rumour*,  $r = (0110101001)$ ,  $\beta = 1168$ ,  $n = 1247$ ;
18. *fashion*,  $r = (1000101000)$ ,  $\beta = 304$ ,  $n = 943$ ;
19. *power*,  $r = (0110100101)$ ,  $\beta = 262$ ,  $n = 1271$ ;
20. *water*,  $r = (1010101111)$ ,  $\beta = 58$ ,  $n = 559$ ;
21. *orange*,  $r = (1001001001)$ ,  $\beta = 273$ ,  $n = 1007$ ;



22. *side*,  $r = (0101001011)$ ,  $\beta = 910$ ,  $n = 1643$ ;
23. *floor*,  $r = (1001000010)$ ,  $\beta = 806$ ,  $n = 901$ ;
24. *shelf*,  $r = (1010000001)$ ,  $\beta = 331$ ,  $n = 689$ ;
25. *water*,  $r = (1001001000)$ ,  $\beta = 1232$ ,  $n = 1961$ ;
26. *peace*,  $r = (1001010010)$ ,  $\beta = 280$ ,  $n = 901$ ;
27. *cork*,  $r = (1010001110)$ ,  $\beta = 121$ ,  $n = 1219$ ;
28. *hole*,  $r = (1100110010)$ ,  $\beta = 68$ ,  $n = 1537$ ;
29. *taste*,  $r = (1000101011)$ ,  $\beta = 70$ ,  $n = 611$ ;
30. *flaw*,  $r = (1001101001)$ ,  $\beta = 618$ ,  $n = 799$ .

### Задание 15

Пользуясь цифровой подписью Фиата – Шамира, подписать данное сообщение, если дано число  $n$ , набор секретных ключей  $(a_1, a_2, \dots, a_s)$  и число  $r$ . Каждую букву передаваемого сообщения представить в виде 5-битовой последовательности, присоединяемую цифру  $u$  записать в двоичной системе счисления. Хеш-функция есть побитовое сложение по модулю два  $k$ -битовых блоков полученной последовательности  $M||u$ . Вычислить набор открытых ключей:

1. *gate*,  $n = 65$ ,  $(2, 3, 4, 6)$ ,  $r = 10$ ,  $k = 4$ ;
2. *exotic*,  $n = 187$ ,  $(2, 3, 5, 8, 10)$ ,  $r = 13$ ,  $k = 5$ ;
3. *crew*,  $n = 77$ ,  $(2, 3, 4, 6)$ ,  $r = 9$ ,  $k = 4$ ;
4. *screen*,  $n = 221$ ,  $(2, 4, 5, 10, 11)$ ,  $r = 15$ ,  $k = 5$ ;
5. *expert*,  $n = 133$ ,  $(3, 5, 9, 11)$ ,  $r = 5$ ,  $k = 4$ ;
6. *torch*,  $n = 91$ ,  $(2, 5, 8, 10, 11)$ ,  $r = 11$ ,  $k = 5$ ;
7. *sketch*,  $n = 323$ ,  $(2, 3, 5, 7, 9)$ ,  $r = 6$ ,  $k = 5$ ;
8. *stage*,  $n = 55$ ,  $(2, 6, 7, 9)$ ,  $r = 11$ ,  $k = 4$ ;
9. *label*,  $n = 391$ ,  $(2, 5, 6, 8, 10)$ ,  $r = 21$ ,  $k = 5$ ;
10. *south*,  $n = 143$ ,  $(3, 5, 7, 15)$ ,  $r = 14$ ,  $k = 4$ ;

11. <i>lawyer</i> , $n = 437$ ,	$(2, 4, 7, 9, 10)$ , $r = 7$ , $k = 5$ ;
12. <i>apple</i> , $n = 51$ ,	$(2, 5, 8, 10)$ , $r = 19$ , $k = 4$ ;
13. <i>scene</i> , $n = 209$ ,	$(3, 6, 8, 10, 13)$ , $r = 15$ , $k = 5$ ;
14. <i>berry</i> , $n = 95$ ,	$(3, 4, 7, 11, 13)$ , $r = 10$ , $k = 5$ ;
15. <i>poison</i> , $n = 247$ ,	$(3, 5, 7, 9, 11)$ , $r = 16$ , $k = 5$ ;
16. <i>anchor</i> , $n = 85$ ,	$(2, 3, 7, 11)$ , $r = 12$ , $k = 4$ ;
17. <i>amber</i> , $n = 119$ ,	$(3, 6, 9, 11)$ , $r = 13$ , $k = 4$ ;
18. <i>sorrel</i> , $n = 161$ ,	$(2, 6, 8, 11, 17)$ , $r = 9$ , $k = 5$ ;
19. <i>shield</i> , $n = 69$ ,	$(2, 5, 7, 10, 14)$ , $r = 8$ , $k = 5$ ;
20. <i>wedge</i> , $n = 115$ ,	$(3, 7, 11, 13)$ , $r = 11$ , $k = 4$ ;
21. <i>feast</i> , $n = 145$ ,	$(2, 7, 8, 11, 13)$ , $r = 5$ , $k = 5$ ;
22. <i>knife</i> , $n = 155$ ,	$(4, 6, 9, 11, 17)$ , $r = 10$ , $k = 5$ ;
23. <i>sand</i> , $n = 203$ ,	$(2, 3, 5, 13)$ , $r = 3$ , $k = 4$ ;
24. <i>cart</i> , $n = 217$ ,	$(4, 5, 9, 20, 23)$ , $r = 11$ , $k = 5$ ;
25. <i>forgery</i> , $n = 253$ ,	$(2, 4, 7, 10, 13)$ , $r = 7$ , $k = 5$ ;
26. <i>silk</i> , $n = 319$ ,	$(9, 13, 15, 19, 23)$ , $r = 12$ , $k = 5$ ;
27. <i>action</i> , $n = 341$ ,	$(3, 7, 10, 13, 15)$ , $r = 23$ , $k = 5$ ;
28. <i>circle</i> , $n = 87$ ,	$(2, 5, 8, 10)$ , $r = 6$ , $k = 4$ ;
29. <i>linen</i> , $n = 93$ ,	$(2, 5, 7, 10, 17)$ , $r = 7$ , $k = 5$ ;
30. <i>profit</i> , $n = 111$ ,	$(2, 5, 8, 11, 13)$ , $r = 12$ , $k = 5$ .

## Задание 16

Проверить подпись  $(s_1, s_2, \dots, s_l, t)$  под данным сообщением, если она вычислена по схеме Фиата – Шамира, причем дано число  $n$  и открытый ключ  $(b_1, b_2, \dots, b_m)$ . Каждая буква передаваемого сообщения представляется в виде 5-битовой последовательности, а присоединяемая цифра  $u$  записывается в двоичной системе счисления.

Хеш-функция есть побитовое сложение по модулю два

$k$ -битовых блоков полученной последовательности:

1. *storm*, (1100, 24),  $n = 437$ , (328, 82, 330, 232),  $k = 4$ ;
2. *noise*, (10011, 26),  $n = 51$ , (13, 49, 4, 25, 43),  $k = 5$ ;
3. *joke*, (10000, 10),  $n = 391$ , (98, 219, 315, 55, 348),  $k = 5$ ;
4. *rustle*, (10110, 36),  $n = 65$ , (49, 29, 61, 56, 36),  $k = 5$ ;
5. *driver*, (00100, 112),  $n = 247$ , (55, 168, 121, 61, 49),  $k = 5$ ;
6. *sword*, (0001, 60),  $n = 143$ , (16, 103, 108, 75),  $k = 4$ ;
7. *print*, (0110, 31),  $n = 77$ , (58, 60, 53, 15),  $k = 4$ ;
8. *stack*, (11001, 166),  $n = 209$ , (93, 180, 49, 23, 47),  $k = 5$ ;
9. *support*, (0110, 36),  $n = 91$ , (23, 51, 64, 81),  $k = 4$ ;
10. *seam*, (00010, 84),  $n = 323$ , (81, 36, 168, 178, 4),  $k = 5$ ;
11. *boat*, (0100, 17),  $n = 55$ , (14, 26, 9, 36),  $k = 4$ ;
12. *casket*, (11000, 128),  $n = 221$ , (166, 152, 168, 42, 179),  $k = 5$ ;
13. *shawl*, (1010, 72),  $n = 95$ , (74, 6, 64, 11),  $k = 4$ ;
14. *pattern*, (01101, 154),  $n = 161$ , (121, 85, 78, 4, 39),  $k = 5$ ;
15. *scent*, (10100, 30),  $n = 69$ , (52, 58, 31, 49, 25),  $k = 5$ ;
16. *miracle*, (00101, 139),  $n = 187$ , (47, 104, 15, 38, 144),  $k = 5$ ;
17. *sense*, (11001, 15),  $n = 85$ , (64, 19, 59, 26, 84),  $k = 5$ ;
18. *honour*, (10010, 8),  $n = 115$ , (64, 54, 96, 49, 39),  $k = 5$ ;
19. *respect*, (11110, 20),  $n = 133$ , (74, 16, 23, 11, 85),  $k = 5$ ;
20. *article*, (11101, 8),  $n = 119$ , (53, 43, 72, 60, 50),  $k = 5$ ;
21. *veil*, (1011, 194),  $n = 253$ , (190, 174, 31, 210),  $k = 4$ ;
22. *plate*, (1111, 83),  $n = 87$ , (22, 7, 34, 67),  $k = 4$ ;
23. *stream*, (0010, 32),  $n = 145$ , (109, 74, 34, 6),  $k = 4$ ;
24. *torrent*, (11001, 7),  $n = 93$ , (70, 67, 19, 40, 28),  $k = 5$ ;
25. *praise*, (10100, 229),  $n = 341$ , (38, 174, 133, 113, 97),  $k = 5$ ;
26. *walk*, (1000, 52),  $n = 155$ , (126, 55, 111, 41),  $k = 4$ ;

27. *soil*, (11100, 90),  $n = 111$ , (28, 40, 85, 100, 67),  $k = 5$ ;  
 28. *mercy*, (10010, 10),  $n = 203$ , (51, 158, 65, 197, 120),  $k = 5$ ;  
 29. *poem*, (0111, 21),  $n = 217$ , (95, 191, 142, 134),  $k = 4$ ;  
 30. *right*, (11101, 59),  $n = 319$ , (256, 168, 207, 38, 199),  $k = 5$ .

### Задание 17

Подписать сообщение  $M$  по схеме Эль Гамала, если даны  $p$ ,  $\alpha$ , секретный ключ  $a$  и случайное число  $r$  :

1.  $M = 67$ ,  $p = 131$ ,  $\alpha = 2$ ,  $a = 12$ ,  $r = 7$ ;
2.  $M = 121$ ,  $p = 79$ ,  $\alpha = 3$ ,  $a = 4$ ,  $r = 5$ ;
3.  $M = 117$ ,  $p = 47$ ,  $\alpha = 5$ ,  $a = 7$ ,  $r = 3$ ;
4.  $M = 93$ ,  $p = 113$ ,  $\alpha = 3$ ,  $a = 5$ ,  $r = 9$ ;
5.  $M = 45$ ,  $p = 83$ ,  $\alpha = 2$ ,  $a = 8$ ,  $r = 7$ ;
6.  $M = 103$ ,  $p = 43$ ,  $\alpha = 3$ ,  $a = 19$ ,  $r = 5$ ;
7.  $M = 204$ ,  $p = 127$ ,  $\alpha = 3$ ,  $a = 15$ ,  $r = 11$ ;
8.  $M = 38$ ,  $p = 89$ ,  $\alpha = 3$ ,  $a = 6$ ,  $r = 9$ ;
9.  $M = 108$ ,  $p = 37$ ,  $\alpha = 5$ ,  $a = 11$ ,  $r = 13$ ;
10.  $M = 73$ ,  $p = 73$ ,  $\alpha = 5$ ,  $a = 4$ ,  $r = 7$ ;
11.  $M = 133$ ,  $p = 109$ ,  $\alpha = 11$ ,  $a = 8$ ,  $r = 5$ ;
12.  $M = 123$ ,  $p = 59$ ,  $\alpha = 2$ ,  $a = 9$ ,  $r = 7$ ;
13.  $M = 148$ ,  $p = 71$ ,  $\alpha = 7$ ,  $a = 7$ ,  $r = 11$ ;
14.  $M = 85$ ,  $p = 67$ ,  $\alpha = 2$ ,  $a = 17$ ,  $r = 7$ ;
15.  $M = 59$ ,  $p = 103$ ,  $\alpha = 2$ ,  $a = 7$ ,  $r = 5$ ;
16.  $M = 95$ ,  $p = 61$ ,  $\alpha = 2$ ,  $a = 23$ ,  $r = 13$ ;
17.  $M = 53$ ,  $p = 137$ ,  $\alpha = 3$ ,  $a = 10$ ,  $r = 5$ ;
18.  $M = 215$ ,  $p = 101$ ,  $\alpha = 2$ ,  $a = 9$ ,  $r = 7$ ;
19.  $M = 43$ ,  $p = 53$ ,  $\alpha = 2$ ,  $a = 9$ ,  $r = 9$ ;
20.  $M = 197$ ,  $p = 67$ ,  $\alpha = 5$ ,  $a = 5$ ,  $r = 7$ ;

21.  $M = 135, \quad p = 139, \alpha = 2, a = 15, \quad r = 7;$
22.  $M = 97, \quad p = 149, \alpha = 2, a = 11, \quad r = 9;$
23.  $M = 100, \quad p = 151, \alpha = 7, a = 9, \quad r = 11;$
24.  $M = 121, \quad p = 163, \alpha = 2, a = 6, \quad r = 5;$
25.  $M = 143, \quad p = 167, \alpha = 5, a = 8, \quad r = 7;$
26.  $M = 203, \quad p = 173, \alpha = 2, a = 3, \quad r = 11;$
27.  $M = 199, \quad p = 179, \alpha = 2, a = 7, \quad r = 5;$
28.  $M = 315, \quad p = 181, \alpha = 2, a = 10, \quad r = 7;$
29.  $M = 241, \quad p = 157, \alpha = 5, a = 11, \quad r = 5;$
30.  $M = 187, \quad p = 191, \alpha = 19, a = 6, \quad r = 13.$

### Задание 18

Получено сообщение с подписью  $(\gamma, \delta)$ . Проверить подпись, если она вычислена по схеме Эль Гамала и известен открытый ключ  $p, \alpha, \beta$  :

1.  $M = 111, \quad (22, 23), \quad p = 53, \quad \alpha = 2, \beta = 12;$
2.  $M = 147, \quad (8, 61), \quad p = 101, \quad \alpha = 2, \beta = 54;$
3.  $M = 113, \quad (35, 18), \quad p = 61, \quad \alpha = 2, \beta = 18;$
4.  $M = 26, \quad (42, 62), \quad p = 109, \quad \alpha = 11, \beta = 22;$
5.  $M = 115, \quad (21, 32), \quad p = 97, \quad \alpha = 5, \beta = 40;$
6.  $M = 209, \quad (6, 99), \quad p = 137, \quad \alpha = 3, \beta = 18;$
7.  $M = 204, \quad (6, 6), \quad p = 61, \quad \alpha = 2, \beta = 44;$
8.  $M = 136, \quad (55, 8), \quad p = 103, \quad \alpha = 2, \beta = 50;$
9.  $M = 134, \quad (21, 86), \quad p = 107, \quad \alpha = 2, \beta = 42;$
10.  $M = 87, \quad (30, 3), \quad p = 43, \quad \alpha = 3, \beta = 12;$
11.  $M = 110, \quad (83, 13), \quad p = 131, \quad \alpha = 2, \beta = 119;$
12.  $M = 54, \quad (11, 33), \quad p = 47, \quad \alpha = 5, \beta = 40;$
13.  $M = 113, \quad (14, 79), \quad p = 83, \quad \alpha = 2, \beta = 28;$

14.  $M = 165$ ,  $(109, 124)$ ,  $p = 127$ ,  $\alpha = 3$ ,  $\beta = 4$ ;
15.  $M = 97$ ,  $(54, 31)$ ,  $p = 79$ ,  $\alpha = 3$ ,  $\beta = 6$ ;
16.  $M = 143$ ,  $(54, 59)$ ,  $p = 113$ ,  $\alpha = 3$ ,  $\beta = 40$ ;
17.  $M = 143$ ,  $(66, 55)$ ,  $p = 89$ ,  $\alpha = 3$ ,  $\beta = 42$ ;
18.  $M = 87$ ,  $(29, 33)$ ,  $p = 79$ ,  $\alpha = 3$ ,  $\beta = 8$ ;
19.  $M = 135$ ,  $(47, 25)$ ,  $p = 71$ ,  $\alpha = 7$ ,  $\beta = 45$ ;
20.  $M = 79$ ,  $(31, 66)$ ,  $p = 73$ ,  $\alpha = 5$ ,  $\beta = 15$ ;
21.  $M = 108$ ,  $(35, 6)$ ,  $p = 53$ ,  $\alpha = 2$ ,  $\beta = 11$ ;
22.  $M = 146$ ,  $(128, 78)$ ,  $p = 179$ ,  $\alpha = 2$ ,  $\beta = 77$ ;
23.  $M = 53$ ,  $(40, 7)$ ,  $p = 59$ ,  $\alpha = 2$ ,  $\beta = 10$ ;
24.  $M = 102$ ,  $(14, 8)$ ,  $p = 83$ ,  $\alpha = 2$ ,  $\beta = 7$ ;
25.  $M = 84$ ,  $(18, 6)$ ,  $p = 67$ ,  $\alpha = 2$ ,  $\beta = 16$ ;
26.  $M = 74$ ,  $(14, 8)$ ,  $p = 53$ ,  $\alpha = 3$ ,  $\beta = 31$ ;
27.  $M = 27$ ,  $(10, 5)$ ,  $p = 47$ ,  $\alpha = 5$ ,  $\beta = 11$ ;
28.  $M = 71$ ,  $(35, 6)$ ,  $p = 61$ ,  $\alpha = 2$ ,  $\beta = 6$ ;
29.  $M = 73$ ,  $(28, 9)$ ,  $p = 43$ ,  $\alpha = 3$ ,  $\beta = 10$ ;
30.  $M = 138$ ,  $(32, 2)$ ,  $p = 103$ ,  $\alpha = 2$ ,  $\beta = 16$ .

### Задание 19

Пользуясь цифровой подписью Шнорра, подписать данное сообщение, если даны  $p$ ,  $q$ ,  $\alpha$ , секретный ключ  $a$  и случайное число  $r$ . Каждая буква передаваемого сообщения представляется в виде 5-битовой последовательности, а присоединяемая цифра  $\gamma$  записывается в двоичной системе счисления. Хеш-функция есть побитовое сложение по модулю два  $k$ -битовых блоков полученной последовательности:

1. *block*,  $p = 229$ ,  $q = 19$ ,  $\alpha = 43$ ,  $a = 17$ ,  $r = 2$ ,  $k = 4$ ;
2. *form*,  $p = 227$ ,  $q = 113$ ,  $\alpha = 4$ ,  $a = 6$ ,  $r = 11$ ,  $k = 4$ ;
3. *saucer*,  $p = 47$ ,  $q = 23$ ,  $\alpha = 25$ ,  $a = 8$ ,  $r = 14$ ,  $k = 3$ ;

4. *bean*,  $p = 53, q = 13, \alpha = 16, a = 6, r = 9, k = 4$ ;
5. *battle*,  $p = 223, q = 37, \alpha = 60, a = 16, r = 23, k = 5$ ;
6. *side*,  $p = 199, q = 11, \alpha = 125, a = 6, r = 8, k = 4$ ;
7. *glass*,  $p = 59, q = 29, \alpha = 4, a = 14, r = 12, k = 4$ ;
8. *marsh*,  $p = 67, q = 11, \alpha = 64, a = 3, r = 5, k = 4$ ;
9. *pain*,  $p = 191, q = 19, \alpha = 52, a = 5, r = 10, k = 4$ ;
10. *forest*,  $p = 179, q = 89, \alpha = 4, a = 8, r = 18, k = 4$ ;
11. *board*,  $p = 79, q = 13, \alpha = 18, a = 2, r = 6, k = 5$ ;
12. *struggle*,  $p = 83, q = 41, \alpha = 4, a = 5, r = 8, k = 5$ ;
13. *bangle*,  $p = 173, q = 43, \alpha = 16, a = 5, r = 10, k = 4$ ;
14. *burden*,  $p = 167, q = 83, \alpha = 25, a = 4, r = 11, k = 4$ ;
15. *team*,  $p = 89, q = 11, \alpha = 64, a = 5, r = 8, k = 4$ ;
16. *razor*,  $p = 107, q = 53, \alpha = 4, a = 7, r = 11, k = 5$ ;
17. *armour*,  $p = 131, q = 13, \alpha = 107, a = 3, r = 6, k = 3$ ;
18. *cabin*,  $p = 157, q = 13, \alpha = 130, a = 9, r = 10, k = 5$ ;
19. *future*,  $p = 139, q = 23, \alpha = 64, a = 5, r = 10, k = 4$ ;
20. *bunch*,  $p = 149, q = 37, \alpha = 16, a = 7, r = 10, k = 5$ ;
21. *grass*,  $p = 53, q = 13, \alpha = 15, a = 4, r = 7, k = 4$ ;
22. *smoke*,  $p = 191, q = 19, \alpha = 32, a = 6, r = 4, k = 5$ ;
23. *melon*,  $p = 83, q = 41, \alpha = 28, a = 3, r = 5, k = 5$ ;
24. *fever*,  $p = 173, q = 43, \alpha = 23, a = 7, r = 5, k = 4$ ;
25. *iron*,  $p = 107, q = 53, \alpha = 13, a = 5, r = 9, k = 4$ ;
26. *pupil*,  $p = 131, q = 13, \alpha = 62, a = 5, r = 7, k = 5$ ;
27. *sight*,  $p = 59, q = 29, \alpha = 5, a = 10, r = 8, k = 4$ ;
28. *expert*,  $p = 67, q = 11, \alpha = 14, a = 6, r = 8, k = 4$ ;
29. *notion*,  $p = 139, q = 23, \alpha = 34, a = 4, r = 7, k = 4$ ;
30. *statue*,  $p = 47, q = 23, \alpha = 10, a = 5, r = 8, k = 4$ .

## Задание 20

Проверить подпись  $(\varepsilon, \delta)$  под данным сообщением, если она вычислена по схеме цифровой подписи Шнорра с данными  $p, q, \alpha$  и  $\beta$ . Каждая буква передаваемого сообщения представляется в виде 5-битовой последовательности, а присоединяемая цифра  $\gamma$  записывается в двоичной системе счисления. Хеш-функция есть побитовое сложение по модулю два  $k$ -битовых блоков полученной последовательности:

1. *cotton*,  $(30, 6), p = 83, q = 41, \alpha = 4, \beta = 33, k = 5;$
2. *storm*,  $(3, 39), p = 173, q = 43, \alpha = 16, \beta = 22, k = 4;$
3. *bottle*,  $(15, 1), p = 199, q = 11, \alpha = 125, \beta = 62, k = 4;$
4. *speed*,  $(5, 38), p = 107, q = 53, \alpha = 4, \beta = 61, k = 4;$
5. *budget*,  $(31, 1), p = 47, q = 23, \alpha = 25, \beta = 8, k = 5;$
6. *office*,  $(8, 2), p = 53, q = 13, \alpha = 16, \beta = 28, k = 4;$
7. *truck*,  $(2, 18), p = 229, q = 19, \alpha = 43, \beta = 60, k = 4;$
8. *vacancy*,  $(6, 6), p = 139, q = 23, \alpha = 64, \beta = 55, k = 5;$
9. *polish*,  $(7, 12), p = 59, q = 29, \alpha = 4, \beta = 17, k = 5;$
10. *knave*,  $(14, 15), p = 149, q = 37, \alpha = 16, \beta = 63, k = 4;$
11. *currency*,  $(3, 6), p = 131, q = 13, \alpha = 107, \beta = 84, k = 4;$
12. *version*,  $(3, 104), p = 227, q = 113, \alpha = 4, \beta = 40, k = 4;$
13. *import*,  $(14, 3), p = 67, q = 11, \alpha = 64, \beta = 25, k = 4;$
14. *chief*,  $(11, 10), p = 89, q = 11, \alpha = 64, \beta = 8, k = 4;$
15. *giant*,  $(12, 51), p = 167, q = 83, \alpha = 2, \beta = 22, k = 4;$
16. *cycle*,  $(15, 15), p = 223, q = 37, \alpha = 60, \beta = 15, k = 5;$
17. *belief*,  $(13, 5), p = 79, q = 13, \alpha = 18, \beta = 65, k = 4;$
18. *heather*,  $(2, 5), p = 191, q = 19, \alpha = 52, \beta = 136, k = 4;$
19. *creed*,  $(6, 2), p = 157, q = 13, \alpha = 130, \beta = 16, k = 5;$
20. *version*,  $(22, 44), p = 179, q = 89, \alpha = 4, \beta = 95, k = 5;$



21. *stage*,  $(4, 11)$ ,  $p = 131$ ,  $q = 13$ ,  $\alpha = 62$ ,  $\beta = 80$ ,  $k = 5$ ;
22. *plot*,  $(13, 12)$ ,  $p = 47$ ,  $q = 23$ ,  $\alpha = 21$ ,  $\beta = 2$ ,  $k = 4$ ;
23. *fate*,  $(29, 6)$ ,  $p = 173$ ,  $q = 43$ ,  $\alpha = 106$ ,  $\beta = 84$ ,  $k = 5$ ;
24. *report*,  $(3, 7)$ ,  $p = 53$ ,  $q = 13$ ,  $\alpha = 28$ ,  $\beta = 15$ ,  $k = 5$ ;
25. *board*,  $(13, 18)$ ,  $p = 191$ ,  $q = 19$ ,  $\alpha = 6$ ,  $\beta = 136$ ,  $k = 5$ ;
26. *staff*,  $(2, 10)$ ,  $p = 67$ ,  $q = 11$ ,  $\alpha = 62$ ,  $\beta = 9$ ,  $k = 4$ ;
27. *slang*,  $(13, 1)$ ,  $p = 139$ ,  $q = 23$ ,  $\alpha = 36$ ,  $\beta = 79$ ,  $k = 5$ ;
28. *lodger*,  $(8, 26)$ ,  $p = 59$ ,  $q = 29$ ,  $\alpha = 22$ ,  $\beta = 41$ ,  $k = 4$ ;
29. *trial*,  $(13, 37)$ ,  $p = 107$ ,  $q = 53$ ,  $\alpha = 34$ ,  $\beta = 48$ ,  $k = 5$ ;
30. *plant*,  $(1, 39)$ ,  $p = 83$ ,  $q = 41$ ,  $\alpha = 3$ ,  $\beta = 25$ ,  $k = 5$ .

## Задание 21

Подписать сообщение по схеме Диффи – Лампорта, если дан набор секретных ключей  $K = [(k_{10}, k_{11}), \dots, (k_{t0}, k_{t1})]$  и набор случайных битов  $S = [(s_{10}, s_{11}), \dots, (s_{t0}, s_{t1})]$ . Найти набор битов  $R$ , если  $r_{ij} = k_{ij} + s_{ij} \pmod{2}$ ,  $i = 1, \dots, t$ ,  $j = 0, 1$  :

1.  $M = 19$ ,  $K = [(7, 3), (5, 6), (2, 1), (4, 2), (11, 9)]$ ,  
 $S = [(1, 1), (0, 1), (1, 1), (1, 0), (0, 0)]$ ;
2.  $M = 23$ ,  $K = [(3, 6), (9, 1), (4, 3), (8, 1), (5, 4)]$ ,  
 $S = [(0, 1), (1, 0), (1, 0), (1, 1), (0, 0)]$ ;
3.  $M = 17$ ,  $K = [(5, 2), (4, 1), (3, 8), (6, 7), (10, 1)]$ ,  
 $S = [(1, 0), (0, 1), (1, 1), (1, 0), (1, 1)]$ ;
4.  $M = 18$ ,  $K = [(3, 2), (4, 5), (7, 1), (9, 5), (6, 4)]$ ,  
 $S = [(0, 1), (1, 1), (1, 0), (0, 0), (1, 0)]$ ;
5.  $M = 15$ ,  $K = [(4, 3), (2, 1), (8, 9), (4, 5)]$ ,  
 $S = [(0, 1), (0, 1), (1, 1), (1, 0)]$ ;
6.  $M = 9$ ,  $K = [(9, 7), (3, 1), (8, 5), (2, 4)]$ ,  
 $S = [(1, 1), (1, 0), (0, 0), (1, 0)]$ ;
7.  $M = 11$ ,  $K = [(13, 5), (11, 7), (2, 6), (3, 4)]$ ,  
 $S = [(1, 0), (0, 1), (0, 1), (1, 1)]$ ;
8.  $M = 13$ ,  $K = [(7, 6), (11, 3), (9, 4), (6, 2)]$ ,

- $S = [(1, 1), (0, 1), (1, 1), (1, 0)];$   
 9.  $M = 26, \quad K = [(5, 0), (3, 1), (4, 7), (8, 6), (4, 2)],$   
 $S = [(1, 1), (0, 1), (1, 0), (1, 0), (1, 1)];$   
 10.  $M = 23, \quad K = [(3, 1), (2, 5), (6, 1), (4, 8), (7, 6)],$   
 $S = [(1, 0), (0, 1), (1, 1), (0, 1), (1, 1)];$   
 11.  $M = 27, \quad K = [(7, 1), (6, 3), (8, 9), (5, 1), (4, 6)],$   
 $S = [(0, 1), (1, 0), (1, 1), (1, 0), (0, 1)];$   
 12.  $M = 20, \quad K = [(4, 9), (1, 3), (5, 8), (7, 6), (10, 3)],$   
 $S = [(1, 0), (1, 0), (1, 1), (0, 1), (1, 1)];$   
 13.  $M = 21, \quad K = [(5, 4), (3, 2), (4, 9), (6, 1), (5, 8)],$   
 $S = [(1, 1), (1, 0), (0, 1), (1, 1), (1, 0)];$   
 14.  $M = 25, \quad K = [(7, 6), (1, 2), (3, 1), (4, 2), (6, 7)],$   
 $S = [(1, 0), (0, 1), (0, 1), (1, 1), (1, 0)];$   
 15.  $M = 14, \quad K = [(1, 2), (3, 5), (4, 7), (8, 9)],$   
 $S = [(0, 1), (1, 0), (1, 0), (1, 1)];$   
 16.  $M = 17, \quad K = [(3, 1), (1, 2), (4, 5), (6, 1), (8, 3)],$   
 $S = [(1, 1), (1, 1), (0, 1), (1, 1), (1, 0)];$   
 17.  $M = 12, \quad K = [(5, 1), (6, 3), (1, 8), (9, 4)],$   
 $S = [(0, 1), (1, 0), (0, 1), (1, 1)];$   
 18.  $M = 22, \quad K = [(3, 1), (4, 5), (2, 7), (1, 3), (5, 8)],$   
 $S = [(0, 1), (1, 0), (1, 1), (1, 1), (0, 1)];$   
 19.  $M = 30, \quad K = [(2, 5), (4, 3), (1, 8), (3, 5), (4, 6)],$   
 $S = [(0, 1), (1, 0), (0, 1), (1, 1), (1, 0)];$   
 20.  $M = 29, \quad K = [(1, 2), (3, 4), (6, 5), (7, 3), (8, 1)],$   
 $S = [(0, 1), (0, 1), (1, 1), (1, 0), (1, 1)];$   
 21.  $M = 26, \quad K = [(9, 1), (4, 5), (3, 2), (7, 4), (8, 6)],$   
 $S = [(1, 0), (0, 1), (1, 1), (1, 0), (0, 1)];$   
 22.  $M = 24, \quad K = [(11, 2), (3, 6), (4, 5), (8, 0), (9, 6)],$   
 $S = [(0, 1), (1, 1), (1, 0), (0, 1), (1, 1)];$   
 23.  $M = 10, \quad K = [(1, 3), (5, 7), (9, 6), (8, 4)],$   
 $S = [(1, 0), (0, 1), (1, 1), (1, 0)];$   
 24.  $M = 17, \quad K = [(2, 5), (8, 3), (4, 9), (6, 1), (10, 3)],$

- $S = [(1, 1), (1, 0), (0, 0), (0, 1), (1, 0)];$   
 25.  $M = 28, \quad K = [(12, 1), (3, 7), (9, 5), (4, 6), (8, 11)],$   
 $S = [(1, 0), (0, 1), (1, 1), (0, 1), (0, 0)];$   
 26.  $M = 31, \quad K = [(2, 1), (4, 5), (3, 6), (9, 7), (10, 8)],$   
 $S = [(1, 1), (1, 0), (0, 1), (1, 1), (0, 0)];$   
 27.  $M = 29, \quad K = [(3, 5), (6, 9), (8, 1), (2, 7), (4, 11)],$   
 $S = [(0, 1), (1, 0), (0, 1), (1, 1), (1, 0)];$   
 28.  $M = 18, \quad K = [(1, 2), (4, 5), (6, 9), (7, 8), (4, 3)],$   
 $S = [(0, 0), (1, 0), (0, 1), (1, 0), (1, 1)];$   
 29.  $M = 25, \quad K = [(4, 7), (2, 9), (5, 1), (3, 8), (6, 10)],$   
 $S = [(1, 0), (1, 1), (0, 0), (0, 1), (1, 0)];$   
 30.  $M = 23, \quad K = [(3, 5), (4, 7), (8, 2), (6, 1), (9, 3)],$   
 $S = [(0, 1), (1, 0), (1, 1), (0, 1), (1, 0)].$

## Задание 22

Проверить подпись  $(k_{1i_1}, k_{2i_2}, \dots, k_{ti_t})$  под сообщением  $M$ , если она получена по схеме Диффи – Лампорта с наборами открытых ключей

$$S = [(s_{10}, s_{11}), \dots, (s_{t0}, s_{t1})], \quad R = [(r_{10}, r_{11}), \dots, (r_{t0}, r_{t1})]$$

и  $r_{ij} = k_{ij} + s_{ij} \pmod{2}, \quad i = 1, \dots, t, \quad j = 0, 1 :$

1.  $(1, 5, 3, 4, 8), \quad M = 26, \quad S = [(1, 0), (0, 1), (1, 1), (1, 0), (0, 1)],$   
 $R = [(0, 1), (0, 0), (0, 1), (0, 0), (0, 1)];$
2.  $(2, 6, 4, 8, 9), \quad M = 24, \quad S = [(0, 1), (1, 1), (1, 0), (0, 1), (1, 1)],$   
 $R = [(1, 1), (0, 1), (1, 1), (0, 1), (0, 1)];$
3.  $(3, 5, 6, 8), \quad M = 10, \quad S = [(1, 0), (0, 1), (1, 1), (1, 0)],$   
 $R = [(0, 1), (1, 0), (0, 1), (1, 0)];$
4.  $(5, 8, 4, 6, 3), \quad M = 17, \quad S = [(1, 1), (1, 0), (0, 0), (0, 1), (1, 0)],$   
 $R = [(1, 0), (1, 1), (0, 1), (0, 0), (1, 1)];$
5.  $(1, 7, 5, 4, 8), \quad M = 28, \quad S = [(1, 0), (0, 1), (1, 1), (0, 1), (0, 0)],$   
 $R = [(1, 1), (1, 0), (0, 0), (0, 1), (0, 1)];$
6.  $(1, 5, 6, 7, 8), \quad M = 31, \quad S = [(1, 1), (1, 0), (0, 1), (1, 1), (0, 0)],$

- $R = [(1, 0), (1, 1), (1, 1), (0, 0), (0, 0)];$   
 7.  $(5, 9, 1, 2, 11), M = 29, S = [(0, 1), (1, 0), (0, 1), (1, 1), (1, 0)],$   
 $R = [(1, 0), (1, 1), (0, 0), (1, 0), (1, 1)];$   
 8.  $(2, 4, 6, 8, 4), M = 18, S = [(0, 0), (1, 0), (0, 1), (1, 0), (1, 1)],$   
 $R = [(1, 0), (1, 1), (0, 0), (0, 0), (1, 0)];$   
 9.  $(7, 9, 5, 3, 10), M = 25, S = [(1, 0), (1, 1), (0, 0), (0, 1), (1, 0)],$   
 $R = [(1, 1), (1, 0), (1, 1), (1, 1), (1, 0)];$   
 10.  $(5, 4, 2, 1, 3), M = 23, S = [(0, 1), (1, 0), (1, 1), (0, 1), (1, 0)],$   
 $R = [(1, 0), (1, 1), (1, 1), (0, 0), (0, 1)];$   
 11.  $(2, 3, 5, 6, 5, 7), M = 35, S = [(1, 0), (0, 1), (1, 1), (0, 1), (1, 1), (1, 0)],$   
 $R = [(0, 0), (1, 1), (0, 1), (0, 0), (1, 0), (1, 1)];$   
 12.  $(4, 5, 6, 3, 8, 4), M = 37, S = [(0, 1), (1, 1), (1, 0), (1, 0), (1, 1), (1, 0)],$   
 $R = [(1, 1), (0, 1), (1, 1), (0, 1), (1, 1), (1, 0)];$   
 13.  $(3, 5, 7, 4, 3), M = 29, S = [(0, 1), (0, 1), (1, 1), (1, 0), (1, 1)],$   
 $R = [(1, 0), (0, 0), (1, 0), (1, 1), (1, 0)];$   
 14.  $(3, 9, 5, 6, 3, 1), M = 39, S = [(0, 1), (1, 0), (1, 0), (1, 0), (1, 1), (0, 1)],$   
 $R = [(0, 0), (0, 0), (0, 1), (1, 0), (1, 0), (1, 0)];$   
 15.  $(2, 9, 5, 10, 8, 7), M = 33, S = [(1, 0), (0, 1), (1, 1), (1, 0), (0, 1), (1, 1)],$   
 $R = [(0, 0), (1, 0), (0, 1), (1, 1), (0, 1), (0, 0)];$   
 16.  $(3, 6, 5, 10, 1, 4), M = 53, S = [(0, 1), (1, 0), (1, 1), (0, 1), (0, 1), (1, 1)],$   
 $R = [(1, 0), (1, 0), (0, 1), (1, 1), (1, 1), (1, 1)];$   
 17.  $(8, 5, 4, 3, 6, 5), M = 51, S = [(0, 1), (1, 0), (1, 1), (1, 1), (1, 0), (1, 0)],$   
 $R = [(1, 1), (0, 1), (1, 0), (0, 0), (1, 0), (1, 1)];$   
 18.  $(8, 1, 4, 6, 2, 3), M = 47, S = [(0, 1), (1, 1), (0, 1), (0, 1), (1, 1), (1, 0)],$   
 $R = [(1, 1), (0, 1), (1, 1), (1, 1), (0, 1), (0, 1)];$   
 19.  $(7, 8, 11, 1, 12, 4), M = 45, S = [(0, 1), (1, 0), (1, 0), (1, 1), (1, 0), (1, 1)],$   
 $R = [(1, 0), (1, 1), (0, 1), (1, 0), (1, 1), (0, 1)];$   
 20.  $(4, 11, 5, 10, 1, 0), M = 43, S = [(0, 1), (1, 0), (1, 1), (1, 0), (1, 1), (0, 1)],$   
 $R = [(1, 1), (0, 1), (1, 0), (1, 0), (1, 0), (1, 1)];$   
 21.  $(3, 2, 8, 4, 1, 7), M = 46, S = [(0, 1), (1, 0), (1, 1), (1, 0), (0, 1), (0, 1)],$   
 $R = [(1, 0), (1, 1), (1, 1), (0, 0), (0, 0), (1, 0)];$   
 22.  $(9, 2, 7, 3, 1, 17), M = 38, S = [(0, 1), (1, 1), (1, 1), (0, 1), (1, 1), (1, 0)],$

- $R = [(1, 0), (1, 0), (0, 1), (1, 0), (1, 0), (0, 1)];$   
 23.  $(7, 4, 5, 2, 8, 9), M = 34, S = [(0, 1), (0, 1), (1, 0), (1, 1), (1, 1), (1, 0)],$   
 $R = [(1, 0), (0, 1), (0, 1), (1, 0), (0, 1), (0, 0)];$   
 24.  $(2, 9, 6, 7, 8, 7), M = 52, S = [(1, 1), (1, 0), (1, 1), (0, 1), (1, 0), (0, 1)],$   
 $R = [(0, 1), (1, 1), (1, 0), (1, 0), (1, 0), (1, 0)];$   
 25.  $(7, 3, 5, 1, 2, 1), M = 49, S = [(0, 1), (1, 0), (1, 1), (1, 0), (0, 1), (1, 1)],$   
 $R = [(1, 0), (1, 1), (0, 1), (0, 0), (0, 0), (1, 0)];$   
 26.  $(1, 6, 4, 3, 1, 11), M = 54, S = [(1, 0), (1, 1), (0, 0), (1, 1), (0, 1), (0, 1)],$   
 $R = [(1, 1), (0, 1), (0, 1), (1, 0), (0, 0), (1, 0)];$   
 27.  $(4, 10, 8, 6, 9, 4), M = 41, S = [(0, 1), (1, 1), (0, 1), (1, 0), (1, 0), (1, 1)],$   
 $R = [(1, 1), (1, 0), (1, 1), (1, 0), (0, 1), (1, 1)];$   
 28.  $(5, 4, 7, 1, 6), M = 22, S = [(1, 0), (0, 0), (1, 0), (1, 1), (0, 1)],$   
 $R = [(1, 1), (0, 1), (0, 1), (1, 0), (0, 1)];$   
 29.  $(3, 8, 7, 6, 9, 1), M = 55, S = [(1, 0), (1, 1), (0, 1), (0, 1), (1, 1), (0, 1)],$   
 $R = [(1, 1), (0, 1), (1, 0), (1, 1), (1, 0), (0, 0)];$   
 30.  $(3, 4, 7, 9, 10, 1), M = 58, S = [(1, 0), (1, 1), (0, 1), (0, 1), (1, 1), (1, 0)],$   
 $R = [(1, 1), (0, 1), (1, 0), (1, 0), (1, 1), (0, 1)].$

**Таблица 1**

а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
19	20	21	22	23	24	25	26	27	28	29	30	31	32

**Таблица 2**

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

t	u	v	w	x	y	z
19	20	21	22	23	24	25

## Литература

1. Основы криптографии / А. П. Алферов [и др.]. – М. : Гелиос, 2001. – 480 с.
2. Нечаев, В. И. Элементы криптографии. Основы теории защиты информации. / В. И. Нечаев. – М. : Высшая школа, 1999. – 109 с.
3. Введение в криптографию / под ред. В. В. Яценко. – СПб. : Питер, 2001. – 288 с.

Учебное издание

**Яблокова** Светлана Ивановна

**Задачи по криптографическим методам  
защиты информации**

**Симметричные криптосистемы**

*Практикум*

Редактор, корректор Л. Н. Селиванова

Верстка С. И. Яблокова

Подписано в печать 26.05.22. Формат 60 × 84 1/8

Усл. печ. л. 9,3. Уч.-изд. л. 2,3.

Тираж 2 экз. Заказ

Оригинал-макет подготовлен  
в редакционно-издательском отделе ЯрГУ.

Ярославский государственный университет  
им. П. Г. Демидова  
150003, Ярославль, ул. Советская, 14.