Лабораторная работа №3
«Международный алгоритм шифрования данных IDEA»

1. Цель работы:

Изучение работы международного алгоритма шифрования данных IDEA.

2. Основные теоретические сведения:

Международный алгоритм шифрования данных (IDEA - International Data Encryption Algorithm) представляет собой симметричный блочный шифр. Его разработали сотрудники Швейцарского федерального института технологий (Swiss Federal Institute of Technology) Сюдзя Лай (Xuejia Lai) и Джеймс Массей (James Massey). Оригинальная версия алгоритма была опубликована в 1990г. Усовершенствованная версия, изменения в которой были призваны повысить стойкость алгоритма в отношении методов дифференциального криптоанализа, была представлена в 1991г. и подробно описана в 1992г.

2.1. Внутренняя структура алгоритма

IDEA представляет собой блочный шифр, использующий 128-битовый ключ для шифрования данных блоками по 64 бита. Для сравнения напомним, что DES тоже работает с 64-битовыми блоками, но шифрует их с помощью 56-битового ключа.

Принципы, которые легли в основу конструкции IDEA, можно разделить на две группы: задачей одних было повышение криптоаналитической стойкости, а задачей других - обеспечение простоты реализации.

Конфузия в IDEA достигается путем смешанного использования трех различных операций. Каждая из операций предполагает два 16-битовых входных значения, в результате обработки которых получается одно 16-битовое выходное значение:

- Побитовое исключающее "ИЛИ", обозначаемое символом $\oplus$.
- Сложение целых чисел по модулю 2^{16} (по модулю 65536) с входными и выходными значениями, рассматриваемыми как 16-битовые целые числа без знака. Эта операция обозначается символом $\boxplus$.
- Умножение целых чисел по модулю $2^{16}+1$ (по модулю 65537) с входными и выходными значениями, рассматриваемыми как 16-битовые целые числа без знака, за исключением блока, состоящего из одних нулей, который интерпретируется как 2^{16}. Эта операция обозначается символом $\odot$.

Например,

$$0\ 000\ 000\ 000\ 000\ 000 \odot 1\ 000\ 000\ 000\ 000\ 000 = 1\ 000\ 000\ 000\ 000\ 001,$$

так как

$$2^{16} \times 2^{15} \bmod (2^{16} + 1) = 2^{15} + 1.$$

Эти операции являются несогласованными в следующем смысле.

1. Никакие две из этих трех операций не подчиняются дистрибутивному закону. Например:
$$a \boxplus (b \odot c) \neq (a \boxplus b) \odot (a \boxplus c).$$
2. Никакие две из этих трех операций не подчиняются ассоциативному закону. Например:
$$a \boxplus (b \oplus c) \neq (a \boxplus b) \oplus c.$$

Использование таких несогласованных операций в комбинации обеспечивает высокую сложность преобразования входного значения, что значительно затрудняет криптоанализ данного алгоритма по сравнению с алгоритмом DES, в котором используется только операция XOR (исключающее "ИЛИ").

Диффузия в IDEA обеспечивается в основном строительном блоке алгоритма, называемом мультипликативно-аддитивной (МА) структурой (рис. 1). На вход такой структуры поступает два 16-битовых значения, получаемых из открытого текста, и два 16-битовых подключа, получаемых из ключа шифрования, а на выходе генерируется два 16-битовых выходных значения. Вычислительный эксперимент с проверкой всех возможностей показывает, что любой выходной бит первого раунда шифрования зависит как от каждого бита входного значения, полученного из открытого текста, так и от каждого бита подключей. В алгоритме данная структура используется последовательно восемь раз, что обеспечивает очень высокие показатели диффузии. Более того, можно доказать, что данная структура предусматривает наименьшее число операций (а именно четыре), при котором достигается полная диффузия.

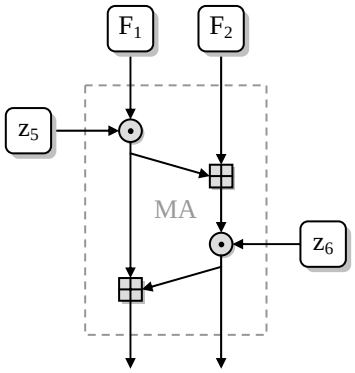

Рис. 1. Мультипликативно-аддитивная структура (МА).

2.2. Шифрование IDEA

Общая схема процесса шифрования IDEA показана на рис. 2. Как и в любой схеме шифрования, на вход поступает два типа данных - открытый текст и ключ. В данном случае длина блока открытого текста равна 64 битам, а длина ключа - 128 битам.

В левой части рисунка видно, что алгоритм IDEA предполагает восемь раундов шифрования, после которых выполняется функция выходного преобразования. Поступившее на вход значение разделяется на четыре 16-битовых подблока.

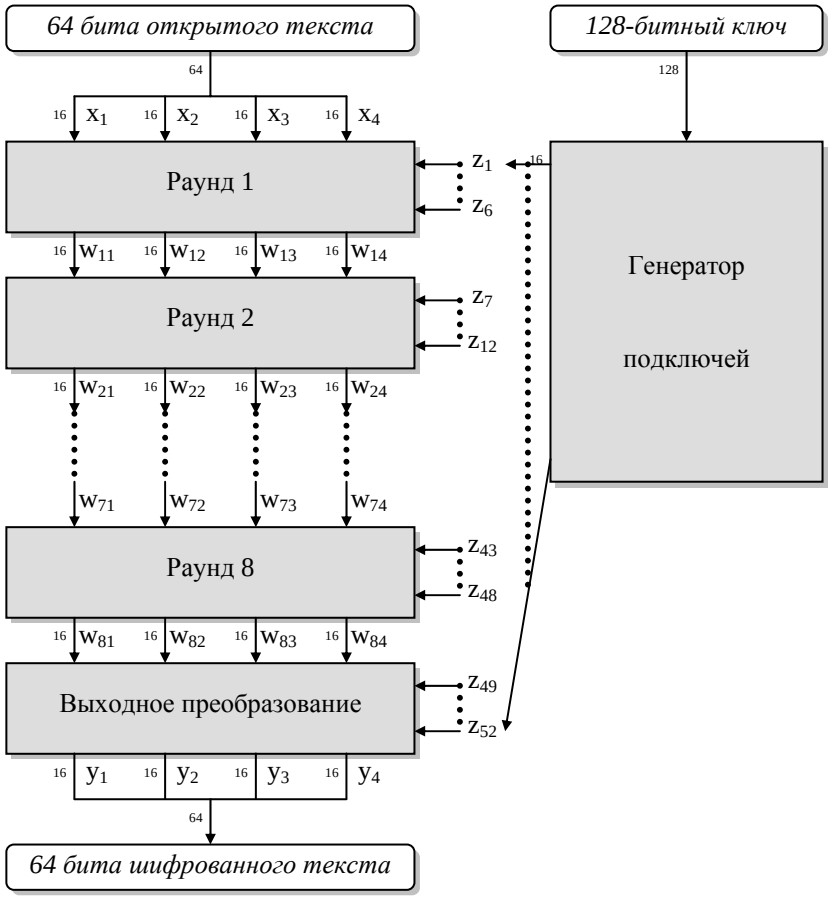

Рис. 2. Структура алгоритма IDEA.

На вход каждого раунда шифрования подается четыре 16-битовых блока, из которых генерируется четыре выходных 16-битовых блока. Выходное преобразование тоже генерирует четыре 16-битовых блока, в результате конкатенации которых получается 64-битовый шифрованный текст. В каждом раунде задействовано шесть 16-битовых подключей, а в выходном преобразовании — четыре, что в сумме составляет 52 подключа. Как показано в правой части рис. 2, все эти 52 подключа генерируются из исходного 128-битового ключа.

2.3. Детали алгоритма шифрования

Давайте проведем анализ отдельного раунда, схема которого показана на рис.3. На самом деле на рис. 3 показана схема первого раунда. Последующие раунды имеют точно такую же структуру, но используют другие подключи и другие входные данные. Как видим, структура шифра IDEA отличается от классической структуры шифров Файстеля. Раунд начинается с преобразования, которое с помощью операции сложения и умножения связывает четыре входных подблока с четырьмя подключами. Это преобразование представлено серым прямоугольником вверху рис. 3. Четыре выходных блока этого преобразования связываются с помощью операции XOR с целью получения двух 16-битовых блоков, которые затем подаются на вход структуры MA (см. рис. 1), представленной на рисунке нижним серым прямоугольником. Кроме того, структура MA получает на входе два подключа, а в результате обработки всех полученных данных на выходе этой структуры генерируется два 16-битовых значения.

Наконец, четыре блока, полученных на выходе первого преобразования, связываются с помощью операции XOR с двумя блоками, получаемыми на

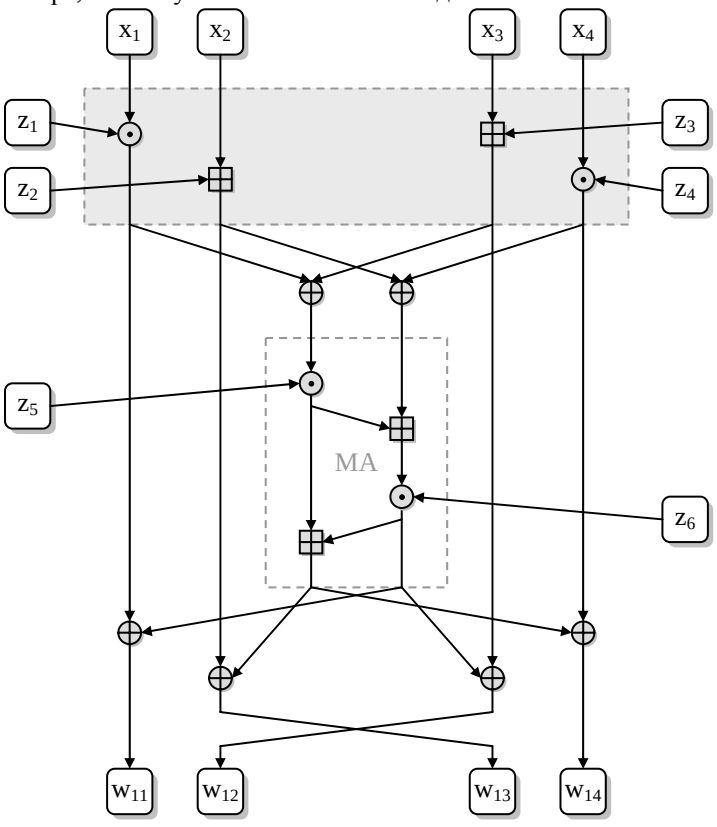

Рис. 3. Один раунд шифрования IDEA (первый раунд)

выходе структуры МА, и в результате имеется четыре выходных блока данного раунда. Обратите внимание на то, что два выходных значения, отчасти зависящих от второго и третьего входных значений (X_2 и X_3), меняются местами, образуя второе и третье выходные значения (W_{12} и W_{13}). Это увеличивает степень перемешивания обрабатываемых битов и делает алгоритм менее уязвимым в отношении методов дифференциального криптоанализа.

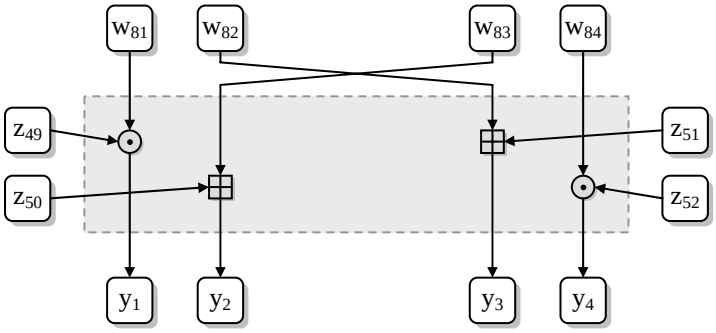

Рис. 4. Выходное преобразование IDEA

Схема девятой стадии алгоритма, обозначенной на рис. 2 как выходное преобразование, показана на рис. 4. Обратите внимание на то, что она имеет структуру, подобную структуре той части предыдущего раунда шифрования, которая представлена верхним серым прямоугольником на рис. 3. Единственное отличие в том, что второй и третий входные подблоки перед обработкой меняются местами. Фактически это означает отмену операции обмена, выполненной в конце восьмого раунда. Наличие этих лишних перестановок объясняется стремлением использовать одну и ту же структуру как для шифрования, так и для дешифрования. Обратите внимание и на то, что в отличие от восьми предыдущих раундов, на девятой стадии используется не шесть подключей, а только четыре.

2.4. Вычисление подключей

Возвращаясь к рис. 2, видно, что все 52 16-битовых подключа генерируются из 128-битового ключа шифрования. При этом применяется следующая схема. Первые восемь подключей, обозначенные $Z_1, Z_2, ..., Z_8$, образуются непосредственно из ключа: Z_1 равен первым (наиболее значимым) 16 битам ключа шифрования, Z_2 - следующим 16 битам и т.д. Затем к ключу шифрования применяется циклический сдвиг влево на 25 битов и создается восемь следующих подключей. Эта процедура повторяется до тех пор, пока не будут получены все 52 подключа. На рис. 5 показано соответствие битов всех подключей битам исходного ключа.

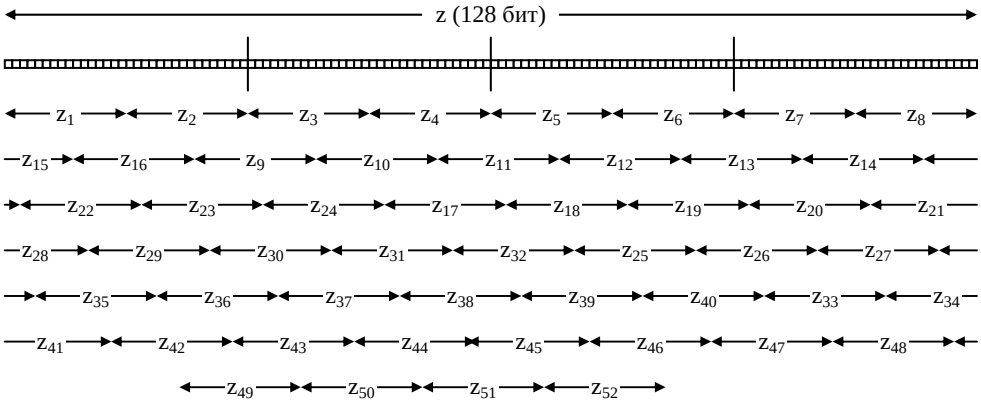

Рис. 5. Подключи IDEA

Эта схема обеспечивает эффективный механизм изменения битов ключа, используемых в подключах всех восьми раундов. Обратите внимание на то, что первый подключ каждого раунда использует свой диапазон битов исходного ключа. Если обозначить весь ключ шифрования как Z[1..128], то на первые ключи восьми раундов шифрования придутся следующие диапазоны битов исходного ключа.

Z_1 = Z[1..16], Z_{25} = Z[76..91],
Z_7 = Z[94..112], Z_{31} = Z[44..59],
Z_{13} = Z[90..105], Z_{37} = Z[34..52],
Z_{19} = Z[83..98], Z_{43} = Z[30..45].

Для всех раундов, за исключением первого и восьмого, 96 битов подключей, используемых для раунда, не представляют собой непрерывного битового фрагмента исходного ключа, поэтому даже между ключами раундов нет простой взаимосвязи, которая получалась бы, например, с помощью сдвига. Это объясняется тем, что в каждом раунде фигурирует только шесть из восьми подключей, получаемых в результате сдвига битов исходного ключа.

2.5. Дешифрование IDEA

Процесс дешифрования практически идентичен процессу шифрования. При дешифровании шифрованный текст подается на вход той же самой структуры IDEA (см. рис. 2) — разница заключается только в ином выборе подключей. Подключи дешифрования $U_1, ..., U_{62}$ получаются из подключей шифрования по следующей схеме.

1. Первых четыре подключа для i-го раунда дешифрования получается из первых четырех подключей (10 - i)-го раунда шифрования, если 9-м раундом считать выходное преобразование. Первый и четвертый подключи дешифрования равны мультипликативным обращениям по модулю $2^{16} + 1$ первого и четвертого подключей

шифрования соответственно. Для раундов со 2-го по 8-й второй и третий подключи дешифрования равны аддитивным обращениям по модулю 2^{16} третьего и второго подключей шифрования соответственно. Для раундов 1 и 9 второй и третий подключи дешифрования равны аддитивным обращениям по модулю 2^{16} второго и третьего подключей шифрования соответственно.

2. Для первых восьми раундов два последних подключа i-го раунда дешифрования равны двум последним подключам (9 - i)-го раунда шифрования.

Таблица 1. Подключи шифрования и дешифрования

	Шифрование	
Стадия	Обозначение	Эквивалент
Раунд 1	$Z_1\ Z_2\ Z_3\ Z_4\ Z_5\ Z_6$	Z[1.. 96]
Раунд 2	$Z_7\ Z_8\ Z_9\ Z_{10}\ Z_{11}\ Z_{12}$	Z[97..128; 26.. 89]
Раунд 3	$Z_{13}\ Z_{14}\ Z_{15}\ Z_{16}\ Z_{17}\ Z_{18}$	Z[90..128; 1.. 25; 51..82]
Раунд 4	$Z_{19}\ Z_{20}\ Z_{21}\ Z_{22}\ Z_{23}\ Z_{24}$	Z[83..128; 1.. 50]
Раунд 5	$Z_{25}\ Z_{26}\ Z_{27}\ Z_{28}\ Z_{29}\ Z_{30}$	Z[76..128; 1.. 43]
Раунд 6	$Z_{31}\ Z_{32}\ Z_{33}\ Z_{34}\ Z_{35}\ Z_{36}$	Z[44.. 75; 101..128; 1..36]
Раунд 7	$Z_{37}\ Z_{38}\ Z_{39}\ Z_{40}\ Z_{41}\ Z_{42}$	Z[37..100; 126..128; 1..29]
Раунд 8	$Z_{43}\ Z_{44}\ Z_{45}\ Z_{46}\ Z_{47}\ Z_{48}$	Z[30..125]
Преобразование	$Z_{49}\ Z_{50}\ Z_{51}\ Z_{52}$	Z[23.. 86]
	Дешифрование	
Стадия	Обозначение	Эквивалент
Раунд 1	$U_1\ U_2\ U_3\ U_4\ U_5\ U_6$	$Z_{49}^{-1}\ -Z_{50}\ -Z_{51}\ Z_{52}^{-1}\ Z_{47}\ Z_{48}$
Раунд 2	$U_7\ U_8\ U_9\ U_{10}\ U_{11}\ U_{12}$	$Z_{43}^{-1}\ -Z_{45}\ -Z_{44}\ Z_{46}^{-1}\ Z_{41}\ Z_{42}$
Раунд 3	$U_{13}\ U_{14}\ U_{15}\ U_{16}\ U_{17}\ U_{18}$	$Z_{37}^{-1}\ -Z_{39}\ -Z_{38}\ Z_{40}^{-1}\ Z_{35}\ Z_{36}$
Раунд 4	$U_{19}\ U_{20}\ U_{21}\ U_{22}\ U_{23}\ U_{24}$	$Z_{31}^{-1}\ -Z_{33}\ -Z_{32}\ Z_{34}^{-1}\ Z_{29}\ Z_{30}$
Раунд 5	$U_{25}\ U_{26}\ U_{27}\ U_{28}\ U_{29}\ U_{30}$	$Z_{25}^{-1}\ -Z_{27}\ -Z_{26}\ Z_{28}^{-1}\ Z_{23}\ Z_{24}$
Раунд 6	$U_{31}\ U_{32}\ U_{33}\ U_{34}\ U_{35}\ U_{36}$	$Z_{19}^{-1}\ -Z_{21}\ -Z_{20}\ Z_{22}^{-1}\ Z_{17}\ Z_{18}$
Раунд 7	$U_{37}\ U_{38}\ U_{39}\ U_{40}\ U_{41}\ U_{42}$	$Z_{13}^{-1}\ -Z_{15}\ -Z_{14}\ Z_{16}^{-1}\ Z_{11}\ Z_{12}$
Раунд 8	$U_{43}\ U_{44}\ U_{45}\ U_{46}\ U_{47}\ U_{48}$	$Z_7^{-1}\ -Z_9\ -Z_8\ Z_{10}^{-1}\ Z_5\ Z_6$
Преобразование	$U_{49}\ U_{50}\ U_{51}\ U_{52}$	$Z_1^{-1}\ -Z_2\ -Z_3\ Z_4^{-1}$

Указанные соотношения представлены в табл. 1. Для обозначения мультипликативного обратного служит обозначение Z_j^{-1}, так что

$$Z_j \odot Z_j^{-1}=1.$$

Поскольку число $2^{16}+1$ является простым, для любого отличного от нуля целого значения $Z_j < 2^{16}$ найдется значение, являющееся для Z_j мультипликативным обратным по модулю $2^{16}+1$. Для обозначения аддитивного обратного по модулю 2^{16} используется обозначение $-Z_j$ поэтому

$$Z_j \boxplus Z_j^{-1}=1.$$

Чтобы убедиться в том, что тот же алгоритм шифрования с подключами дешифрования дает нужный результат, рассмотрим рис. 5, в левой части которого представлена схема шифрования в направлении сверху вниз, а в правой - схема дешифрования в направлении снизу вверх. Каждый раунд разбит на две подстадии - преобразование и субшифрование. Стадия преобразования соответствует верхнему серому прямоугольнику на рис. 3, а стадия субшифрования - остальным операциям, выполняющимся в ходе очередного раунда.

Рассмотрим самые нижние прямоугольники на обеих схемах. При шифровании на выходе функции выходного преобразования имеем

$$Y_1 = W_{81} \odot Z_{49},\ Y_3 = W_{82} \boxplus Z_{51},$$
$$Y_2 = W_{83} \boxplus Z_{50},\ Y_4 = W_{84} \odot Z_{52}.$$

При дешифровании на выходе первой подстадии первого раунда получаем следующее:

$$J_{11} = Y_1 \odot U_1,\quad J_{13} = Y_3 \boxplus U_3,$$
$$J_{12} = Y_2 \boxplus U_2,\quad J_{14} = Y_4 \odot U_4.$$

Заменив соответствующие значения эквивалентными, получим

$$J_{11} = Y_1 \odot Z_{49}^{-1} = W_{81} \odot Z_{49} \odot Z_{49}^{-1} = W_{81}$$
$$J_{12} = Y_2 \boxplus -Z_{50}^{-1} = W_{83} \boxplus Z_{50} \boxplus -Z_{50}^{-1} = W_{83}$$
$$J_{13} = Y_3 \boxplus -Z_{51}^{-1} = W_{82} \boxplus Z_{51} \boxplus -Z_{51}^{-1} = W_{82}$$
$$J_{14} = Y_4 \odot Z_{52}^{-1} = W_{84} \odot Z_{52} \odot Z_{52}^{-1} = W_{84}$$

Таким образом, выходные значения первой подстадии первого раунда дешифрования совпадают с входными значениями последней стадии шифрования, за исключением того, что второй и третий блок оказываются переставленными. Теперь рассмотрим следующие соотношения, которые можно вывести из рис. 3.

$$W_{81} = I_{81} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})$$
$$W_{82} = I_{82} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})$$
$$W_{83} = I_{83} \oplus MA_L(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})$$
$$W_{84} = I_{84} \oplus MA_L(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})$$

где $MA_R(X, Y)$ обозначает правое выходное значение структуры MA для входных значений X и Y, а $MA_L(X, Y)$ — левое выходное значение структуры MA для входных значений X и Y (см. рис. 4.3). Тогда

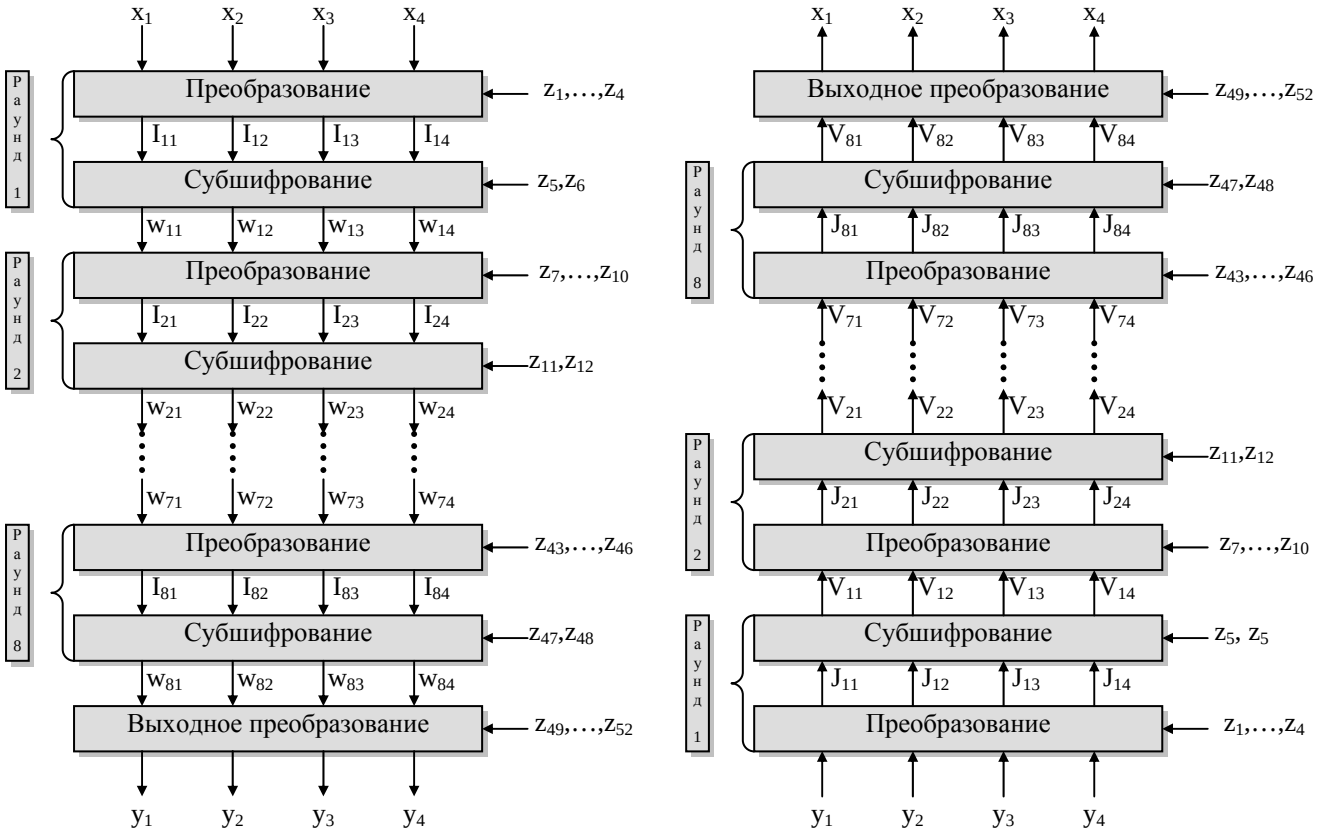

Рис. 5. Шифрование и дешифрование IDEA

$$V_{11} = J_{11} \oplus MA_R(J_{11} \oplus J_{13}, J_{12} \oplus J_{14}) = W_{81} \oplus MA_R(W_{81} \oplus W_{82}, W_{83} \oplus W_{84}) =$$
$$= I_{81} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus MAR[I_{81} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus I_{83} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}),$$
$$I_{82} \oplus MA_L(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus I_{84} \oplus MA_L(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})] =$$
$$= I_{81} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) = I_{81}$$

Точно также получаем

$$V_{12}=I_{83},$$
$$V_{13}=I_{82},$$
$$V_{14}=I_{84}.$$

Таким образом, выходные значения второй подстадии процесса дешифрования совпадают с входными значениями предпоследней подстадии шифрования, за исключением того, что второй и третий блок оказываются переставленными. Продолжая аналогичные рассуждения, можно показать, что такое соответствие сохранится для всех соответствующих подстадий на рис. 5 до тех пор, пока мы не будем иметь

$$V_{81}=I_{11},$$
$$V_{82}=I_{13},$$
$$V_{83}=I_{12},$$
$$V_{84}=I_{14}.$$

Наконец, поскольку выходное преобразование процесса дешифрования эквивалентно преобразованию первой подстадии процесса шифрования, если не считать обмена местами второго и третьего блоков, мы видим, что на выходе всего процесса дешифрования получаются значения, совпадающие с входными значениями процесса шифрования.

3. Задание на лабораторную работу

1. С помощью Excel получить 128-битный ключ из четырех 32-битных чисел, приведенных в таблице.
2. Получить 52 16-битных подключа.
3. Используя IDEA зашифровать 64-битый открытый текст, полученный из четырех 16-битных чисел приведенных в таблице.

4. Варианты заданий на лабораторную работу:

№	4 32-битных числа образующих ключ				4 16-битных числа образующих открытый текст			
1	4050550955	1605609391	4072650953	2152509687	61904	17310	49332	16838
2	3217524078	2403608413	220733990	2132960021	23281	48426	61322	62166
3	2137223569	459343409	2680294027	3370150015	8248	4274	21485	59702
4	1075145906	4163724195	376717186	2219674323	14972	49039	64549	9420
5	2885975751	302960335	2682933859	568218567	57489	57178	58988	30068
6	1586307963	841351430	2179807788	2359332974	30425	13917	56939	17718
7	2191764735	950737461	1947099742	3033432935	46300	10349	23793	19091
8	4147992390	2081233322	4285451989	289725500	39775	48619	45844	18491
9	576108729	1713995562	402245469	3725944755	54171	5668	14583	540
10	2399549051	381429369	2286282825	486592193	14874	31769	11971	14579
11	393327998	128957248	3288823206	3493307983	11807	64096	39837	31323
12	2606312739	70330012	2517484261	2158024061	40342	41798	36831	59151
13	3794939534	4139631718	3078930822	4151652064	48396	5174	59525	1652
14	3577581374	7326287	962773068	2179082687	48955	41478	12122	42939
15	3501841911	889864385	2094791617	2429906296	37853	29010	63013	62542
16	2693915442	2426276426	1759041402	2963030821	54876	50950	50052	35178
17	852664571	2836643571	621087970	22512852	56104	21150	58913	45125
18	4035136389	1411881013	3116347662	1209113068	56257	52244	21832	23699
19	318881032	1594100400	3205816004	3621080407	53194	43438	62533	36669
20	1607101676	2998369029	364525601	3941447786	45131	41642	27624	28623
21	248398732	1836539904	2732787650	1192019110	28245	16411	19540	19907
22	890165977	2557132947	2216548152	143908829	63409	15955	24504	10610
23	2969264366	1398732807	542853407	746873068	38580	59076	3798	25437
24	3520017987	3482905064	2378572684	4250781116	48505	59241	1647	27147
25	812530895	505809740	2349458837	610845889	7207	61616	17148	33653
26	724334849	2815019107	2771474347	2731938081	23516	49432	55626	62234
27	2134355966	570028486	2690612222	2672240553	19151	57471	17500	30614
28	2977185637	855373018	1985636339	1229062488	16664	52628	45543	20768
29	4005400952	870708442	2462685962	587359993	35645	15999	65399	5252
30	344931996	3285617794	1114899366	837881789	57666	1521	10762	30688
31	2772528401	1700561126	1779933219	2104400047	56491	59008	12778	39399
32	4111386705	678808895	806078506	3644787109	50661	46435	45336	9531
33	1848927409	3357319529	2375975537	1177994508	11319	19121	33535	53737
34	102000513	1616164732	629459960	3339002714	35408	64809	15403	45901
35	1927301123	1433622983	3662567245	1770538537	29656	10802	3656	51812
36	1011099420	388835343	1961682440	4218523310	25784	18564	6198	21704
37	950662036	1378832407	46026433	3357679952	16831	5118	53683	7160
38	100601274	859828621	2844273055	1687011393	33108	50046	26656	413
39	1070285717	454812969	1647162556	4289798755	51205	54682	63862	50346
40	2398699168	3212104873	970936454	4180732566	47275	31621	26770	61736
41	636558462	1707113513	1157167982	3238723746	49897	14949	16503	25208
42	3370888672	2327086900	2611729377	1337139405	39742	25044	22561	10944
43	797380120	1830349005	2266390857	3113796624	58559	4618	13266	41245
44	2252425784	2554071043	3752822840	2554201727	45137	14713	15568	25680
45	2899698915	3677194934	876251366	194339887	19236	1341	38403	51543