

## **Содержание**

ВВЕДЕНИЕ.....	5
ОСНОВНЫЕ ПОНЯТИЯ .....	10
1. УЧЕБНЫЙ АЛГОРИТМ ШИФРОВАНИЯ.....	12
1.1 Предпосылки создания учебного алгоритма шифрования .....	12
1.2 Схема Фейстеля .....	12
1.3 Общий вид учебного алгоритма шифрования.....	14
1.4 Функция F .....	15
1.5 Использование раундовых подключений .....	19
1.6 Использование одного и того же алгоритма для шифрования и дешифрования данных .....	20
1.7 Пример шифрования данных с использованием учебного алгоритма шифрования.....	25
1.8 Контрольные вопросы.....	34
1.9 Задачи для самостоятельного решения .....	35
2. МЕТОД ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА .....	39
2.1 Понятие дифференциального криptoанализа. Общие сведения.....	39
2.2 Дифференциальный криptoанализ одного раунда шифрования.....	44
2.3 Дифференциальный криptoанализ трех раундов шифрования.....	48
2.4 Контрольные вопросы.....	57
3. МЕТОД ЛИНЕЙНОГО КРИПТОАНАЛИЗА .....	58
3.1 Понятие линейного криptoанализа. Общие сведения.....	58
3.2 Нахождение эффективных линейных статистических аналогов для одного раунда шифрования .....	61
3.3 Нахождение эффективных линейных статистических аналогов для трех раундов шифрования.....	77
3.4 Определение битов ключа с помощью эффективных линейных статистических аналогов .....	85
3.5 Контрольные вопросы.....	87

Лабораторная работа №1 .....	89
Изучение метода дифференциального криptoанализа блочных шифров.....	89
Подготовка к работе .....	89
Методические указания по выполнению лабораторной работы .....	90
Пример выполнения лабораторной работы .....	95
Контрольные вопросы.....	118
Лабораторная работа №2.....	119
Изучение метода линейного криptoанализа блочных шифров .....	119
Подготовка к работе .....	119
Методические указания по выполнению лабораторной работы .....	120
Пример выполнения лабораторной работы .....	130

## ВВЕДЕНИЕ

Не секрет, что стремление защитить свои интересы было присуще человеку с давних пор. Еще в древности человек использовал различные варианты кодирования информации, изобретал устройства, которые бы способствовали созданию более стойких шифров и при этом обеспечивали легкость шифрования.

Современная криптография основана на понятии односторонней функции  $f(x)$ . Не вдаваясь в формальные математические определения, отметим одно ее свойство: инвертировать функцию, т. е. вычислить  $x$ , зная только  $f(x)$ , крайне сложно. Стойкость шифров, помимо собственно алгоритма шифрования, во многом определяется и длиной ключа. Современная криптография исходит из того, что сам алгоритм рано или поздно все равно станет известен противнику. Все сообщения, передаваемые по открытым каналам связи, могут быть перехвачены, так что ключ шифра остается его единственным секретом.

Можно сказать, что теория информации в современном понимании получила начало своего развития с работы Огюста Кергоффса «Военная криптография», опубликованной в 1883 году. Позднее Клод Шеннон в своей работе «Теория связи в секретных системах» [1], опубликованной в 1949 году, сформулировал необходимые и достаточные условия недешифруемости системы шифрования. Долгое время криптография оставалась секретной наукой, в тайны которой был посвящен лишь узкий круг лиц. Это было естественно. Так как в первую очередь она была направлена на сохранение государственных секретов. Ситуация стала меняться во второй половине XX века с появлением персональных компьютеров. Когда практически каждый человек получил возможность оперировать электронной информацией, возникла естественная потребность как-то защищать эту информацию от посторонних глаз. Широкое распространение получило использование симметричной криптографии, а

несколько позднее и ассиметричной. В 1976 году в США был утвержден стандарт шифрования данных DES (Data Encryption Standard) [2], который использовался довольно длительное время (более 20 лет). Естественно, что у людей возникло желание проверить: а действительно ли предлагаемые алгоритмы для шифрования конфиденциальных данных обеспечивают сохранность информации? Для того, чтобы ответить на этот вопрос необходимо было провести ряд достаточно сложных исследований. Так, исследования в области анализа стойкости шифров постепенно стали причиной того, что в криптологии выделилось два родственных направления, теснейшим образом связанных между собой: криптография и криptoанализ. Прослеживая историю развития этих направлений, можно сказать, что одним из блочных алгоритмов наиболее часто подвергавшийся различного рода атакам является алгоритм шифрования DES. Именно для анализа этого алгоритма шифрования были разработаны такие мощные атаки как линейный и дифференциальный криptoанализ, которые в дальнейшем стали применяться к целому классу блочных шифров.

Современные алгоритмы блочного шифрования разрабатываются таким образом, чтобы аналитик имел как можно меньше шансов отыскать секретный ключ, с помощью которого были зашифрованы данные, даже если ему известен сам алгоритм шифрования и есть в наличие несколько текстов и соответствующих им шифртекстов. Приступая к задаче анализа первым делом аналитик определяет тот набор данных, который ему изначально известен для анализа.

Так, если известен алгоритм шифрования и есть хотя бы одна пара открытый – шифрованный текст, то самым естественным способом анализа, который сразу приходит в голову, является последовательное опробование всех возможных вариантов ключа, которые могли быть использованы. Опробование производят до тех пор, пока зашифрование открытого текста на очередном ключе не приведет к получению имеющегося шифрованного сообщения. Такой способ анализа в разных источниках литературы имеет

разные названия, например «Метод полного перебора»[3] или «Метод грубой силы» [4] или «Метод атаки в лоб» [2] или «Brut-force атака» [4]. У этого метода анализа есть одно неоспоримое преимущество: рано или поздно искомый ключ будет найден и для этого будет необходим минимальный набор данных. Быстрота нахождения секретного ключа будет зависеть от его длины и от вычислительной мощи, которая есть в наличии у аналитика. А также от доли везения. Ведь может случиться так, что искомый ключ встретится одним из первых. В работе [3] достаточно подробно описано, как оценивать сложность подобного рода анализа.

Вместе с тем нам известно, что одним из важных свойств информации является ее своевременность. Поэтому применение метода полного перебора на практике не используется. Еще бы, ведь когда разрабатывался алгоритм шифрования DES длина его фактического секретного ключа была определена в 56 бит. То есть для того, чтобы перебрать все возможные варианты секретных ключей, необходимо было сделать  $2^{56}$  опробований. С помощью имевшихся в то время вычислительных средств это можно было бы сделать за несколько десятков лет! Конечно, с той поры как был разработан алгоритм шифрования DES, в развитии вычислительной технике произошел огромный скачок и вычислительные мощи возросли в тысячи раз. Но даже сегодня провести полный перебор секретных ключей для алгоритма DES за один день весьма проблематично. В связи с тем, что вычислительная мощь с каждым днем неумолимо растет, стандарт DES был заменен на новый стандарт AES (Advanced Encryption Standard), где длина секретного ключа возросла до 128 бит. Так или иначе, в криптографии принято время анализа с помощью метода полного перебора считать эталонным. Что это означает? Это значит, что если аналитику удастся провести анализ алгоритма шифрования быстрее, чем это можно сделать с помощью полного перебора, то данный алгоритм шифрования будет считаться уязвимым, в связи с чем его использовать для шифрования данных будет нецелесообразно.

Как уже отмечалось ранее, в начале 90-х годов прошлого века были предложены два способа анализа алгоритма шифрования DES, которые позволяли осуществлять атаку быстрее, чем это можно было бы сделать с помощью метода полного перебора. Метод линейного криптоанализа (linear cryptanalysis) был предложен японским ученым М. Матсui [5] и позволял проводить анализ путем опробования  $2^{47}$  пар текстов, зашифрованных на одном секретном ключе. Здесь сразу следует отметить, что хоть степенной показатель в количестве опробований сократился со значения 56 до значения 47, возникло условие, практически невыполнимое – наличие огромного объема информации, зашифрованной на одном и том же ключе!!! Метод дифференциального криптоанализа (differential cryptanalysis) был предложен Э.Бихамом и А.Шамиром [6, 7]. С помощью этого метода сложность анализа сократилась до  $2^{37}$ . Однако опять же, для проведения анализа необходимо было иметь  $2^{37}$  особым образом подобранных текстов, зашифрованных на одном и том же секретном ключе. Не смотря на накладываемые ограничения в использовании новых предложенных методов анализа – это был прорыв! Дальнейшее развитие этих методов показало возможность их применения к целому классу блочных шифров, позволило выявить слабые места других используемых алгоритмов шифрования. Сегодня оба эти метода, а также некоторые их усовершенствования, например, линейно-дифференциальный метод, метод невозможных дифференциалов, широко используются для оценки стойкости вновь создаваемых шифров. Именно поэтому специалисту по защите информации необходимо иметь представление о механизмах анализа блочных шифров с использованием современных методов криптоанализа.

Для того, чтобы научиться применять методы анализа на практике, необходимо что называется «в живую потрогать» их, то есть иметь возможность применить эти методы к блочному шифру от начала и до конца, начиная с анализа самого алгоритма шифрования до получения секретного ключа. Встает вопрос: а как это лучше всего сделать? Если использовать

какой-либо известный алгоритм шифрования, то это будет трудоемкая, практически невыполнимая задача. В 2003 году нами был разработан целый комплекс лабораторных работ по изучению современных методов криптоанализа блочных шифров. В основу его было положено использование простых учебных алгоритмов шифрования. В состав комплекса вошли работы по изучению методов линейного и дифференциального криптоанализа блочных шифров, имеющих различные схемы построения (схему Фейстеля, и сеть SPN), а также работа по изучению метода слайдовой атаки (slide attack). В течение пяти лет данные лабораторные работы были опробованы на кафедре Безопасности Информационных Технологий тогда еще Таганрогского радиотехнического университета (ТРТУ), а ныне Таганрогского технологического института Южного федерального университета (ТТИ ЮФУ). Сами лабораторные работы были довольно подробно представлены в учебном пособии «Современные алгоритмы шифрования и методы их анализа», вышедшем в 2006 году в издательстве Гелиос АРВ [8]. За время использования данных лабораторных работ были выявлены существенные недостатки, как в самом используемом учебном алгоритме шифрования, так и в изложении материала, что побудило нас существенным образом переработать и усовершенствовать материал для лучшего понимания механизмов работы методов анализа.

## ОСНОВНЫЕ ПОНЯТИЯ

**Алгоритм шифрования (шифр)** – некоторое обратимое математическое преобразование сообщения с целью сокрытия его содержания.

**Раунд (цикл) шифрования** – последовательность действий, многократно повторяемая для зашифрования или дешифрования сообщений.

**Открытый текст** – сообщение, подлежащее зашифрованию.

**Закрытый текст (шифртекст)** – сообщение, полученное в результате зашифрования открытого сообщения.

**Дифференциал (разность)** – результат операции сложения по модулю два двух сообщений на одном и том же этапе шифрования.

**Характеристика** – пара дифференциалов один из которых образован входными значениями некоторого преобразования, а второй – выходными значениями этого же преобразования. Дифференциал на входе преобразования также часто называют *входной разностью*, а дифференциал на выходе преобразования – *выходной разностью*.

**Раундовая характеристика** – пара дифференциалов один из которых образован входными значениями раунда шифрования, а второй – выходными значениями того же раунда.

**Вероятность характеристики** – вероятность, с которой выходная разность характеристики будет получена для заданной входной разности характеристики.

**Правильная пара текстов** – две пары текстов вида открытый – закрытый текст, для которых открытые тексты образуют входную разность заданной характеристики, а закрытые тексты – выходную разность этой же характеристики.

**Линейный статистический аналог нелинейной функции шифрования** – величина  $Q$ , равная сумме по модулю два скалярных произведений входного вектора  $X$ , выходного вектора  $Y$  и вектора секретного ключа  $K$  соответственно с двоичными векторами  $\alpha$ ,  $\beta$  и  $\gamma$ , имеющими хотя бы одну координату равную единице:  $Q = (X, \alpha) \oplus (Y, \beta) \oplus (K, \gamma)$  в том случае, если вероятность того, что  $Q=0$  отлична от 0,5 ( $P(Q=0) \neq 0,5$ ).

**Отклонение линейного статистического аналога** – величина  $\eta = |1 - 2p|$ , где  $p$  – вероятность, с которой выполняется линейный аналог.

# **1. УЧЕБНЫЙ АЛГОРИТМ ШИФРОВАНИЯ**

## **1.1 Предпосылки создания учебного алгоритма шифрования**

Как уже отмечалось во введении, затруднительно использовать в учебных целях один из известных на сегодняшний день алгоритмов блочного шифрования. Это связано в первую очередь с тем, что известные и широко используемые шифры оперируют блоками данных достаточно большой длины и, как правило, устойчивы к известным видам анализа. Нам же необходимо рассмотреть такой шифр, который бы поддавался анализу. Более того, необходимо, чтобы анализ такого шифра можно было бы провести за время, отведенное в учебном процессе для лабораторных работ. Конечно, в таком случае рассматриваемый шифр оказывается нестойким и по сути дела непригодным для использования его в целях сокрытия данных. Но только так можно рассмотреть основные механизмы, используемые в современных видах анализа с тем, чтобы в дальнейшем на практике уметь оценить стойкость используемых шифров. Более того, эти механизмы необходимо знать и учитывать в случае разработки новых алгоритмов шифрования.

## **1.2 Схема Фейстеля**

Известно, что на сегодняшний день алгоритмы блочного шифрования могут быть организованы двумя основными способами: либо по схеме Фейстеля (Feistel block cipher) [9] как в случае с алгоритмами DES и ГОСТ 28147-89, либо по принципу сети на основе подстановок и перемешивания (сети SPN) как в случае с новым стандартом США – AES. Лабораторные работы, которые будут представлены ниже, направлены на анализ алгоритмов блочного шифрования, построенных по схеме Фейстеля. В классическом варианте при организации шифрования данных по схеме Фейстеля блок открытого текста разбивается на две равные части – правую и

левую. Очевидно, что длина блока при этом должна быть четной. В каждом раунде одна из частей подвергается преобразованию при помощи некоторой функции  $F$  и так называемого раундового подключа  $K_i$ , полученного из исходного секретного ключа  $K$ . Результат операции суммируется по модулю 2 (операция XOR) с другой частью. Затем левая и правая части меняются местами. Три этих преобразования (преобразование с помощью функции  $F$ , сложение данных по модулю два, обмен местами двух частей) представляют собой один раунд (или как его называют в отечественной литературе - цикл) криптографического преобразования.

Классическая схема Фейстеля представлена на рис. 1. Преобразования в каждом раунде одинаковы за тем исключением, что в цикле последнего раунда не выполняется перестановка левой и правой частей. Это сделано для того, чтобы стало возможным использовать один и тот же алгоритм шифрования как для зашифрования данных, так и для дешифрования. При дешифровании на алгоритм накладывается всего одно условие – раундовые подключи  $K_i$  должны быть использованы в обратном порядке. Ниже мы более подробно рассмотрим механизмы, за счет использования которых становится возможным использование одного и того же алгоритма как для шифрования, так и для дешифрования данных.

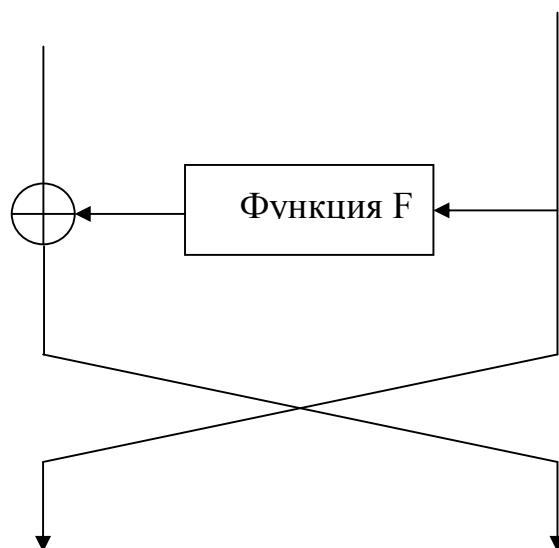


Рисунок 1 – Схема Фейстеля

Схема Фейстеля допускает некоторые модификации. Так, например, исходный блок данных может быть разбит не на две равные части, а на четыре. Подробнее об этом можно прочесть в работе [8].

### 1.3 Общий вид учебного алгоритма шифрования

Для рассмотрения методов линейного и дифференциального криптоанализа мы будем использовать некоторый Учебный Алгоритм Шифрования. Алгоритм этот построен по схеме Фейстеля и содержит в себе три раунда шифрования. Общий вид алгоритма представлен на рис. 2.

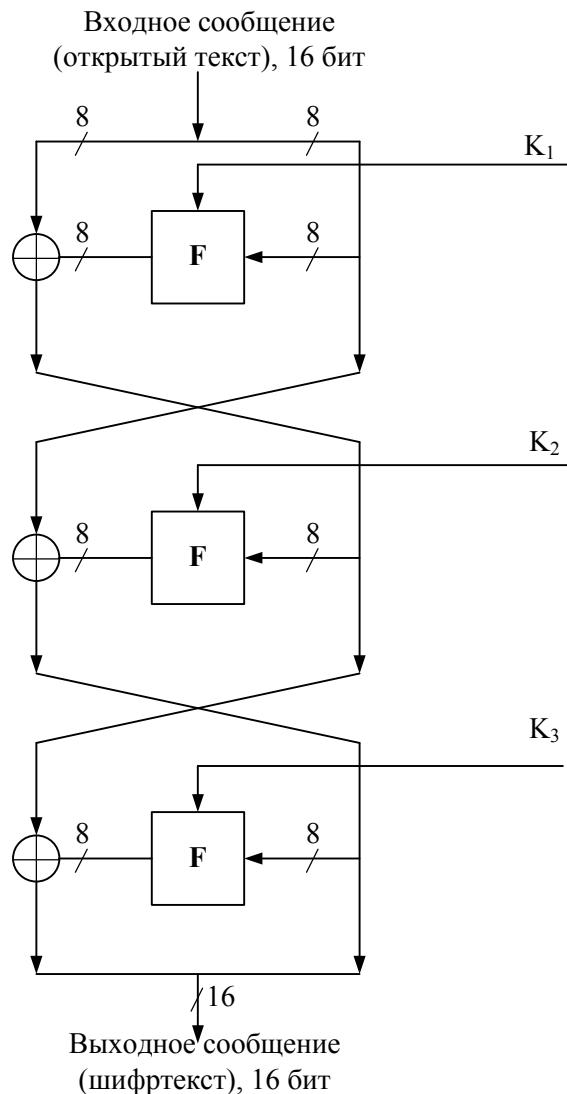


Рисунок 2 – Общий вид Учебного алгоритма шифрования

Как видно из рисунка 2, такая организация алгоритма шифрования повторяет структуру алгоритма шифрования DES за тем исключением, что сокращено количество раундов шифрования и отсутствуют начальная и конечная перестановки. Отсутствие перестановок объясняется тем, что они по своей сути фактически не влияют на криптографическую стойкость преобразуемых данных. Их наличие в Учебном Алгоритме Шифрования всего лишь усложнило бы понимание механизмов анализа. Более того, дальше будет показано, что функция F, осуществляющая главное криптографическое преобразование в своем составе содержит преобразования, по своей структуре аналогичные преобразованиям, входящим в состав функции F алгоритма шифрования DES. Именно поэтому такой алгоритм можно назвать DES-подобным алгоритмом шифрования.

Итак, рассмотрим более подробно алгоритм шифроварния, представленный на рис. 2. Исходное сообщение, которое подлежит преобразованию с помощью данного Учебного алгоритма шифрования, представляет собой последовательность из 16 бит, которые разделяются на две части. Правая часть сообщения преобразуется с помощью функции F под воздействием раундового ключа, после чего складывается по модулю два с левой частью и части сообщения меняются местами. Алгоритм состоит из трех таких раундов, при этом в последнем раунде правая и левая части не меняются местами, а остаются на своих местах, образуя выходное шифрованное сообщение.

#### **1.4 Функция F**

Теперь перейдем к рассмотрению преобразования, выполняемого с помощью функции F (см. рис. 3). На вход функции F поступает 8 битов (половина от преобразуемого блока данных). Они проходят через блок перестановки с расширением так, что на выходе мы получаем 12 бит. Расширение происходит путем дублирования некоторых позиций исходного

8-битового сообщения. Данные таблицы перестановки с расширением приведены в таблице 1. Сразу следует оговориться и отметить, что наполнение таблицы перестановки с расширением, представленное в таблице 1 не является фиксированным. Для каждого варианта лабораторных работ будет задана своя таблица перестановки с расширением.

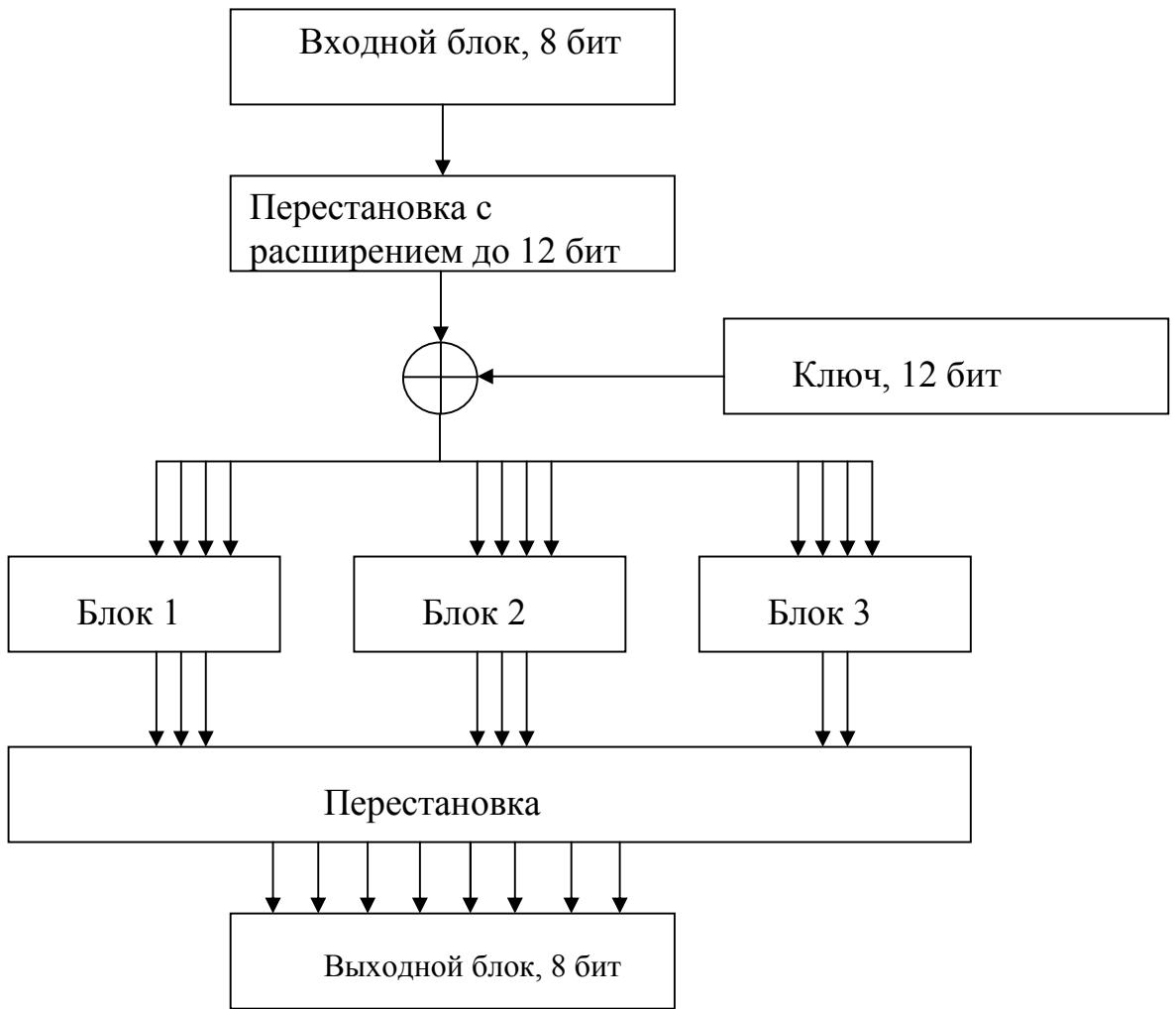


Рисунок 3 – Функция F

После прохождения через перестановку с расширением вновь образованное 12-битовое сообщение складывается по модулю два с секретным раундовым 12-битовым подключом, выработанным из исходного секретного ключа.

Результат сложения разбивается на три группы по четыре бита, каждая из которых проходит соответственно через блоки замены: Блок1, Блок 2 и Блок 3. При этом на выходе первых двух блоков замены образуется три бита, а на выходе третьего блока – два.

Замена в первых двух блоках производится по приведенным таблицам замены (соответственно таблицы 2 и 3) по следующему принципу. Пусть на вход блока замены поступают четыре бита  $a_1, a_2, a_3, a_4$ . При этом первый бит определяет номер строки (если  $a_1 = 0$ , то это соответствует первому столбцу, а если  $a_1 = 1$  – второму), а остальные три – номер столбца ( $000 =$  первому столбцу,  $111 =$  восьмому столбцу) в таблице замены. Результат на пересечении строки и столбца образует выходное значение блока замены.

Несколько иначе дело обстоит с третьим блоком. Из него в отличие от первых двух выходит не три бита, а два. Замена осуществляется согласно таблице 4. При этом, если  $a_1, a_2, a_3, a_4$  – входные биты Блока 3, то биты  $a_1$  и  $a_4$  определяют номер строки таблицы замены, а биты  $a_2$  и  $a_3$  – номер столбца (подобно тому, как происходит замена данных с помощью S-блоков алгоритма DES).

Здесь также стоит заметить, что наполнение трех блоков замены не будет являться фиксированным и будет различаться для каждого индивидуального варианта выполняемой работы.

На выходе из блоков замены образуется 8-битовое сообщение, которое претерпевает перестановку согласно таблице 5. Результат работы перестановки образует 8-битовое сообщение, которое появляется на выходе преобразования функции F.

Таблица 1

Таблица перестановки с расширением

3	4	1	2	6	8	5	7	3	8	2	4
---	---	---	---	---	---	---	---	---	---	---	---

Таблица 2

Таблица замены в блоке 1

<b>a2a3a4</b>	<b>000</b>	<b>001</b>	<b>010</b>	<b>011</b>	<b>100</b>	<b>101</b>	<b>110</b>	<b>111</b>
<b>a1</b>								
<b>0</b>	4	6	1	3	5	7	2	5
<b>1</b>	5	7	2	4	6	1	3	6

Таблица 3

Таблица замены в блоке 2

<b>a2a3a4</b>	<b>000</b>	<b>001</b>	<b>010</b>	<b>011</b>	<b>100</b>	<b>101</b>	<b>110</b>	<b>111</b>
<b>a1</b>								
<b>0</b>	3	5	7	2	4	6	1	7
<b>1</b>	4	6	1	3	5	7	2	1

Таблица 4

Таблица замены в блоке 3

<b>a2a3</b>	<b>00</b>	<b>01</b>	<b>10</b>	<b>11</b>
<b>a1 a4</b>				
<b>00</b>	1	3	2	1
<b>01</b>	2	1	3	2
<b>10</b>	3	2	1	3
<b>11</b>	1	3	2	1

Таблица 5

Таблица перестановки

8	7	3	2	5	4	1	6
---	---	---	---	---	---	---	---

Выход функции F складывается по модулю два с левой частью сообщения, образуя новую левую часть текста. Правая часть сообщения остается неизменной (то есть такой, какая поступала на вход функции F

данного раунда). После этого правая и левая части меняются местами и поступают на вход второго раунда шифрования. Важно отметить, что в последнем раунде правая и левая части не меняются местами. Это сделано для того, чтобы зашифрованные тексты можно было расшифровать с использованием этого же алгоритма шифрования.

## 1.5 Использование раундовых подключей

В каждом раунде при преобразовании данных с помощью функции F происходит сложение данных с секретным раундовым подключом. Каждый раундовый подключ (их всего три – по количеству раундов в алгоритме шифрования) имеет длину 12 битов и вырабатывается из исходного 24-битового ключа по схеме, отображенной на рисунке 4.

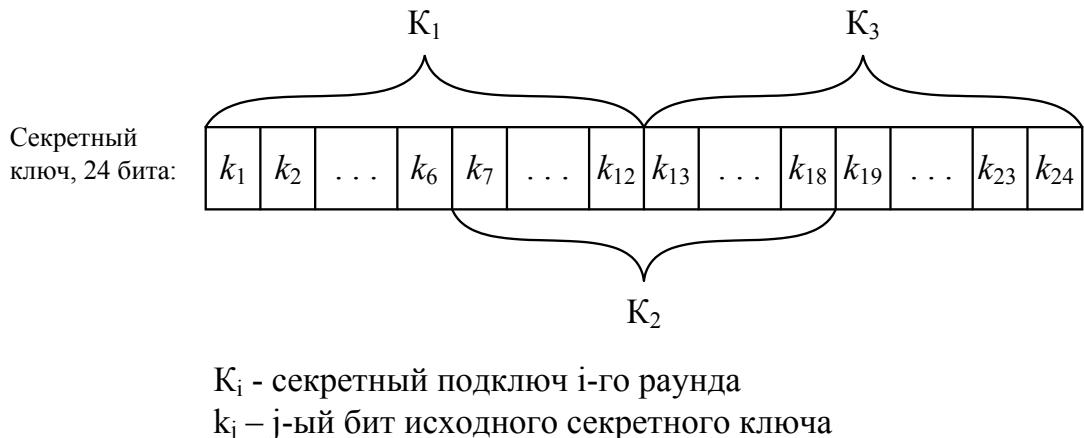


Рисунок 4 – Выработка раундового подключа

Как видно из рисунка 4, исходный ключ имеет длину 24 бита, которые пронумерованы слева направо от одного до 24 (т.е. бит  $k_1$  – самый старший, а бит  $k_{24}$  – самый младший). Таким образом, первые 12 битов с  $k_1$  до  $k_{12}$  образуют первый подключ  $K_1$ , который используется в первом раунде шифрования. Двенадцать битов с  $k_7$  до  $k_{18}$  образуют второй подключ  $K_2$ , который используется во втором раунде шифрования. И, наконец, последние

12 битов с  $k_{13}$  до  $k_{24}$  образуют третий подключ  $K_3$ , который используется в последнем раунде шифрования.

## **1.6 Использование одного и того же алгоритма для шифрования и дешифрования данных**

Как уже отмечалось ранее, один и тот же симметричный алгоритм блочного шифрования, построенный по схеме Фейстеля, может использоваться как для шифрования данных, так и для их дешифрования. Рассмотрим более подробно за счет каких механизмов это становится возможным.

На рис. 5 представлены раунды учебного алгоритма шифрования и представлено описание преобразования входного сообщения  $X$  при его прохождении через раунды шифрования. На вход алгоритма шифрования поступает сообщение  $X$ , которое необходимо зашифровать. Так как алгоритм построен по схеме Фейстеля, то происходит разделение исходного сообщения  $X$  на две части: левую часть сообщения  $XL$  и правую часть сообщения  $XR$ . Правая часть сообщения, т.е. значение  $XR$  поступает на вход функции  $F$  первого раунда шифрования, где шифруется с использованием подключа  $K_1$ . Значение, полученное в результате прохождения  $XR$  через функцию  $F$ , обозначим как  $F(XR, K_1)$ . Выход функции  $F$  первого раунда шифрования складывается по модулю 2 с левой частью исходного сообщения  $XL$ :  $F(XR, K_1) \oplus XL$ . Полученное выражение для удобства дальнейшей работы удобно обозначить какой-либо переменной, например, переменной  $\alpha$ :

$$F(XR, K_1) \oplus XL = \alpha. \quad (1)$$

Преобразование первого раунда шифрования заканчивается тем, что правая и левая части сообщения меняются местами. Таким образом, на вход функции  $F$  второго раунда шифрования поступает значение  $\alpha$ , где оно

шифруется с использованием ключа  $K_2$ . В результате такого преобразования, на выходе функции  $F$  второго раунда шифрования образуется значение  $F(\alpha, K_2)$ .

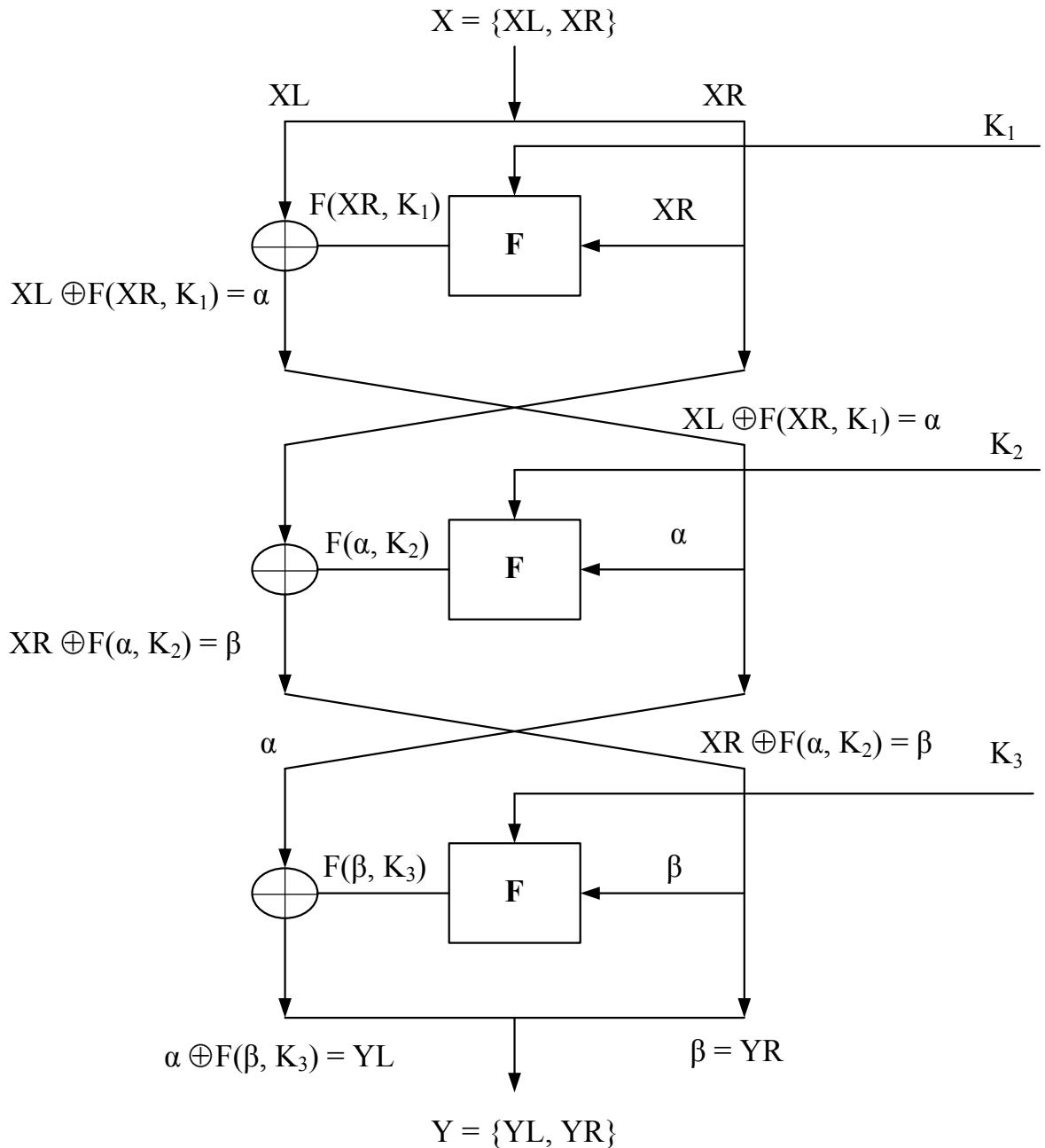


Рисунок 5 – Преобразование сообщения при шифровании

Выход функции  $F$  второго раунда шифрования складывается по модулю 2 с левой частью сообщения, поступившего на вход второго раунда

шифрования, то есть со значением  $XR: F(\alpha, K_2) \oplus XR$ . Полученное выражение для удобства дальнейшей работы удобно обозначить какой-либо переменной, например, переменной  $\beta$ :

$$F(\alpha, K_2) \oplus XR = \beta. \quad (2)$$

Преобразование второго раунда шифрования заканчивается тем, что правая и левая части сообщения меняются местами. Таким образом, на вход функции  $F$  третьего раунда шифрования поступает значение  $\beta$ , где оно шифруется с использованием ключа  $K_3$ . В результате такого преобразования, на выходе функции  $F$  третьего раунда шифрования образуется значение  $F(\beta, K_3)$ .

Выход функции  $F$  третьего раунда шифрования складывается по модулю 2 с левой частью сообщения, поступившего на вход третьего раунда шифрования, то есть со значением  $\alpha: F(\beta, K_3) \oplus \alpha$ .

В результате шифрования левая часть шифрованного сообщения будет равна значению  $F(\beta, K_3) \oplus \alpha$ , а правая – значению  $\beta$ . Эти части сообщения, обозначенные как  $YL, YR$  и будут составлять шифртекст:

$$F(\beta, K_3) \oplus \alpha = YL; \quad (3)$$

$$\beta = F(\alpha, K_2) \oplus XR = YR; \quad (4)$$

$$Y = \{YL, YR\}. \quad (5)$$

Теперь рассмотрим обратный процесс, то есть процесс, при котором из шифрованного сообщения  $Y$  будет восстановлено исходное сообщение  $X$  (рис. 6). Известно, что при дешифровании необходимо использовать тот же алгоритм, что был использован при шифровании данных. Отличие заключается только в том, что раундовые подключи необходимо использовать в обратном порядке. То есть при дешифровании в первом раунде будет использован подключ  $K_3$ , а в последнем – подключ  $K_1$ .

При дешифровании на вход алгоритма поступает зашифрованный текст  $Y$ , который состоит из двух половинок:  $Y = \{YL, YR\}$ . Правая часть этого сообщения, то есть значение  $YR = \beta$ , поступает на вход функции  $F$  первого раунда, где шифруется с помощью подключа  $K_3$ . В результате на выходе функции  $F$  первого раунда образуется значение  $F(\beta, K_3)$ .

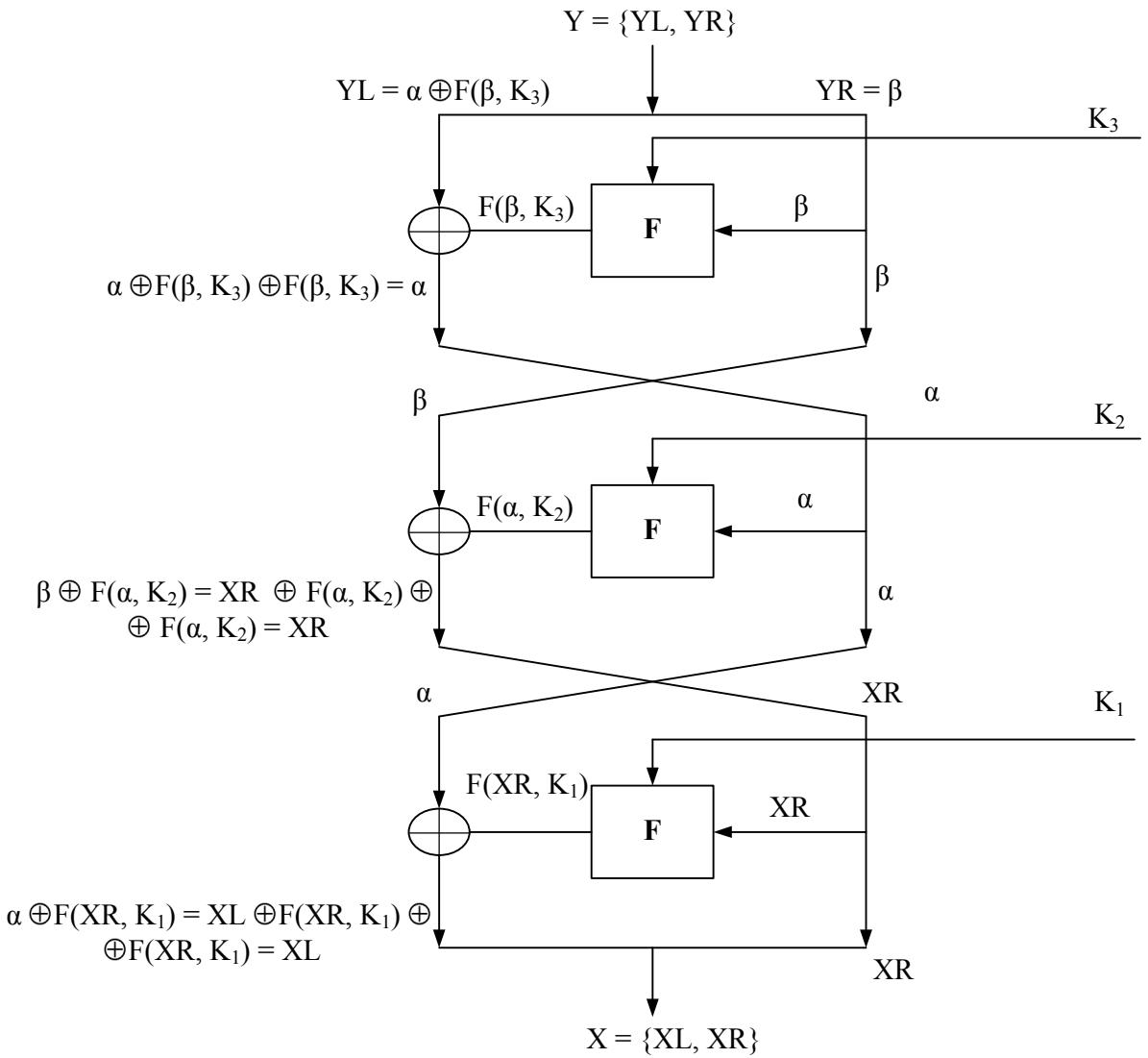


Рисунок 6 – Преобразование сообщения при дешифровании

Выход функции  $F$  первого раунда шифрования складывается по модулю 2 с левой частью сообщения, поступившего на вход первого раунда

шифрования, то есть со значением  $YL$ . В результате образуется сумма:  $YL \oplus F(\beta, K_3)$ . Заменим значение  $YL$  в соответствии с формулой (3):

$$YL \oplus F(\beta, K_3) = F(\beta, K_3) \oplus \alpha \oplus F(\beta, K_3) = \alpha$$

Получается, что в результате сложения по модулю два левой части входного сообщения первого раунда и выхода функции  $F$  первого раунда образуется значение  $\alpha$  (так как два одинаковых значения  $F(\beta, K_3)$  в результате сложения по модулю два образуют ноль). После этого правая и левая части сообщения меняются местами. Таким образом, на вход второго раунда поступает сообщение, левая часть которого равна  $\beta$ , а правая – равна  $\alpha$ .

После прохождения через функцию  $F$  второго раунда значение  $\alpha$  преобразуется в значение  $F(\alpha, K_2)$ , так как во втором раунде происходит шифрование с использованием раундового подключа  $K_2$ .

Выход функции  $F$  второго раунда шифрования складывается по модулю 2 с левой частью сообщения, поступившего на вход второго раунда, то есть со значением  $\beta$ . В результате образуется сумма:  $\beta \oplus F(\alpha, K_2)$ . Заменим значение  $\beta$  в соответствии с формулой (2):

$$\beta \oplus F(\alpha, K_2) = F(\alpha, K_2) \oplus XR \oplus F(\alpha, K_2) = XR$$

Таким образом, в результате сложения по модулю два левой части входного сообщения первого раунда и выхода функции  $F$  первого раунда образуется значение  $XR$ . После этого правая и левая части сообщения меняются местами. Так, на вход третьего раунда поступает сообщение, левая часть которого равна  $\alpha$ , а правая – равна  $XR$ .

В заключении, на вход функции  $F$  третьего раунда поступает значение  $XR$ , которое под действием раундового подключа  $K_1$ , преобразуется в значение  $F(XR, K_1)$ .

Выход функции F последнего раунда складывается по модулю 2 с левой частью сообщения, поступившего на вход третьего раунда, то есть со значением  $\alpha$ . В результате образуется сумма:  $\alpha \oplus F(XR, K_1)$ . Заменим значение  $\alpha$  в соответствии с формулой (1):

$$\alpha \oplus F(XR, K_1) = F(XR, K_1) \oplus XL \oplus F(XR, K_1) = XL$$

В результате сложения по модулю два левой части входного сообщения первого раунда и выхода функции F первого раунда образуется значение XL.

В итоге левая часть выходного сообщения будет равна значению XL, а правая – значению XR:  $X = \{XL, XR\}$ . Эти части сообщения и будут составлять искомое значение, которое ранее нами было зашифровано.

## **1.7 Пример шифрования данных с использованием учебного алгоритма шифрования**

Для того, чтобы лучше освоить принцип шифрования данных с использованием блочных симметричных шифров, рассмотрим пример шифрования данных с помощью учебного алгоритма шифрования. Для этого возьмем сообщение  $X = 55203_{10}$  и ключ  $K = 1760619_{10}$ . Первым делом необходимо перевести эти сообщения в двоичную систему счисления. При переводе необходимо помнить, что сообщение X должно занимать 16 бит, а ключ K – 24 бита. Если в случае перевода в двоичную систему счисления полученная последовательность битов оказывается короче, чем того требует алгоритм шифрования, необходимо дописать недостающее число нулей к старшим значащим разрядам. Таким образом, в результате перевода чисел, получим:

$$X = 1101\ 0011\ 1010\ 0011$$
$$K = 0001\ 1010\ 1101\ 1101\ 0110\ 1011$$

Обратите внимание, что в значении ключа K появились три старших нуля. Следующим шагом является определение раундовых подключей в соответствии с рис. 4:

$$K_1 = 0001\ 1010\ 1101;$$

$$K_2 = 1011\ 0111\ 0101;$$

$$K_3 = 1101\ 0110\ 1011.$$

Итак, на вход алгоритма шифрования поступает блок данных из 16 бит  $X = 1101\ 0111\ 1010\ 0011$ , который разделяется на две части по 8 бит: левую часть – 1101 0111 и правую часть – 1010 0011. Для наглядности процесс зашифрования данных представлен на рисунке 7.

Правая часть сообщения (значение 1010 0011) поступает на вход функции F первого раунда шифрования, где преобразуется с использованием раундового подключа  $K_1$  в соответствии с рис. 3.

Первым преобразованием функции F является перестановка с расширением, которая направлена на перемешивание и размножение битов исходного сообщения. Для того, чтобы применить перестановку с расширением, необходимо пронумеровать биты исходной последовательности от 1 до 8 слева направо. После этого биты исходной последовательности необходимо преобразовать с помощью таблицы 1. Так, в соответствии с таблицей 1, третий бит исходной последовательности станет первым, четвертый бит – вторым, первый бит третьим и т.д. В результате преобразования исходная последовательность 1010 0011 преобразуется к виду 1010 0101 1100. Для наглядности процесс применения перестановки с расширением изображен на рис. 8.

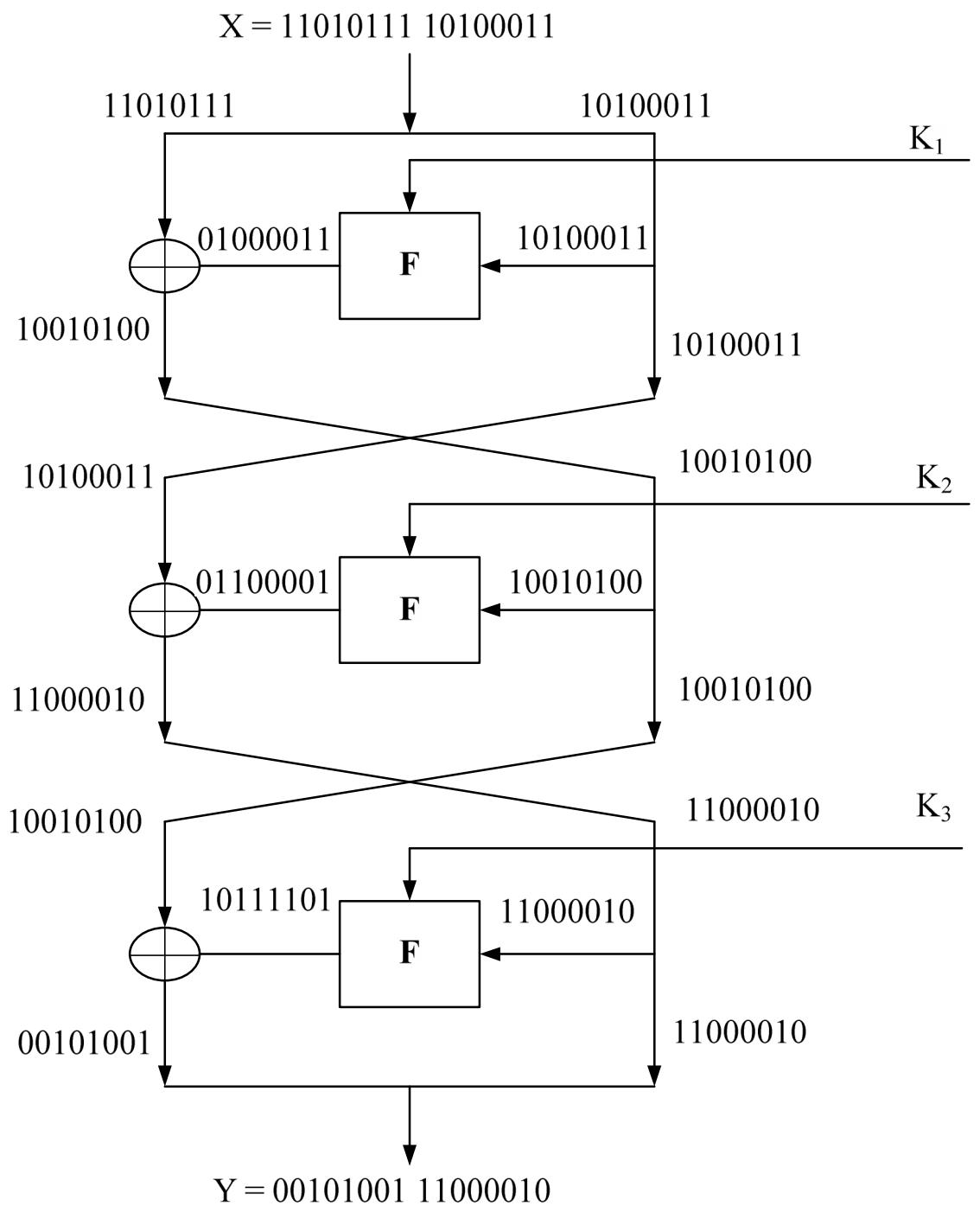


Рисунок 7 – Процесс шифрования сообщения  $X = 11010111\ 10100011$  с помощью секретного ключа  $K = 0001\ 1010\ 1101\ 1101\ 0110\ 1011$

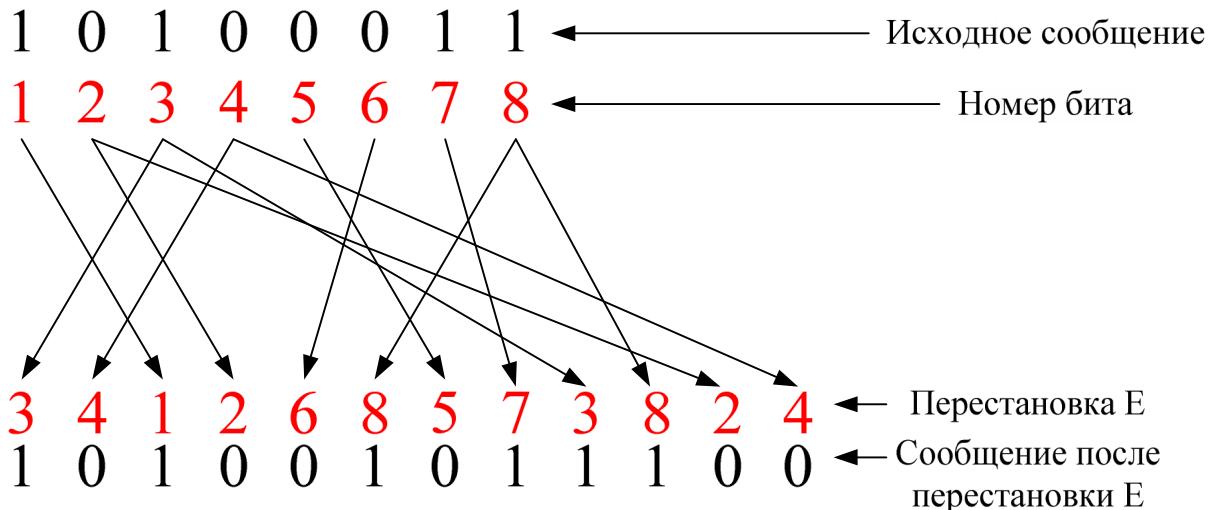


Рисунок 8 – Применение операции перестановки с расширением

После перестановки  $E$  происходит сложение данных с раундовым подключением  $K_1$  по модулю 2. Напомним, что операция сложения по модулю 2 работает следующим образом: если складываются два одинаковых бита (то есть или два ноля, или две единицы), то в результате сложения образуется 0; если же складываются два разных бита (0 и 1 или 1 и 0), то в результате сложения образуется 1. Итак, в результате сложения по модулю 2 данных после перестановки с расширением и раундового подключа  $K_1$  получается значение 1011 1111 0001 (см. рис. 9).

$$\begin{array}{r}
 \oplus \quad 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0 \\
 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \\
 \hline
 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1
 \end{array}$$

Сообщение после перестановки  $E$

Raундовый подключ  $K_1$

$E \oplus K_1$

Рисунок 9 – Сложение данных после перестановки с расширением с раундовым подключом  $K_1$ .

После сложения с раундовым подключом последовательность из 12 битов разбивается на три группы по четыре бита. Каждая из групп поступает

на вход одного из трех блоков замены, где преобразуется в соответствии с таблицами 2 – 4. Напомним, что первые два блока замены имеют одинаковый принцип работы. Работа третьего блока несколько отличается от первых. Рассмотрим данные преобразования более подробно. Так, в соответствии с последовательностью, полученной после сложения с раундовым подключом, на вход первого блока замены поступает значение 1011. Первый бит последовательности указывает на номер строки в таблице 2, последние три бита – на номер столбца. В результате такого преобразования на выходе блока замены образуется значение 100. Для наглядности процесс преобразования данных с помощью первого блока замены представлен на рис. 10. Аналогичным образом на вход второго блока замены поступает значение 1111, которое в соответствии с табл. 3 преобразуется к значению 001.

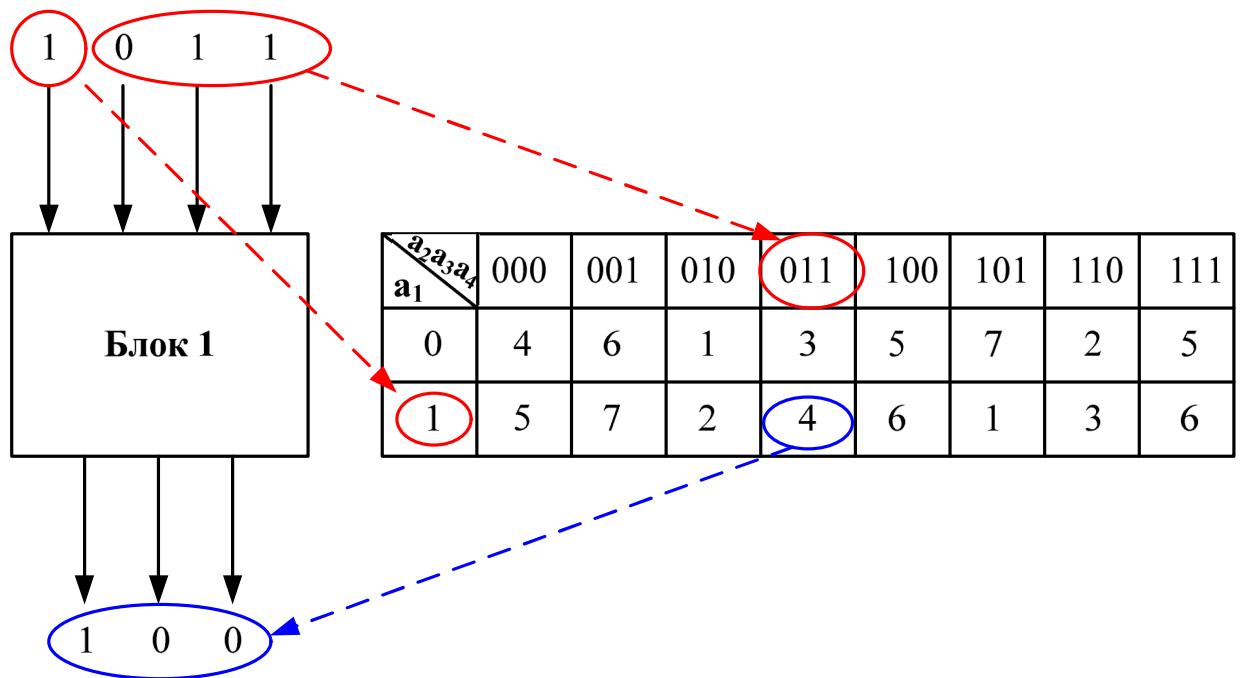


Рисунок 10 – Преобразование данных с помощью первого блока замены

Последние четыре бита последовательности 0001 заменяются с помощью третьего блока замены в соответствии с таблицей 4. Здесь первый и

последний биты входа в Блок 3, то есть значение 01, образуют номер строки в таблице замены, а средние два бита, то есть значение 00, образуют номер столбца. В результате преобразования на выходе блока замены образуется значение 10 ( обратим внимание, что на выходе последнего блока замены образуется два бита в отличие от первых двух блоков, где на выходе были трехбитовые значения). Для наглядности процесс преобразования данных с использованием последнего блока замены представлен на рис. 11.

Таким образом, после применения преобразования с помощью блоков замены на выходе образуется последовательность из 8 бит: 100 001 10

Последним преобразованием функции F является обычная перестановка, работа которой осуществляется в соответствии с таблицей 5 и аналогична работе перестановки с расширением, которая была описана раньше. В результате перестановки последовательность 10000110 преобразуется в последовательность 01000011, которая и является выходом функции F первого раунда шифрования (см. рис. 7).

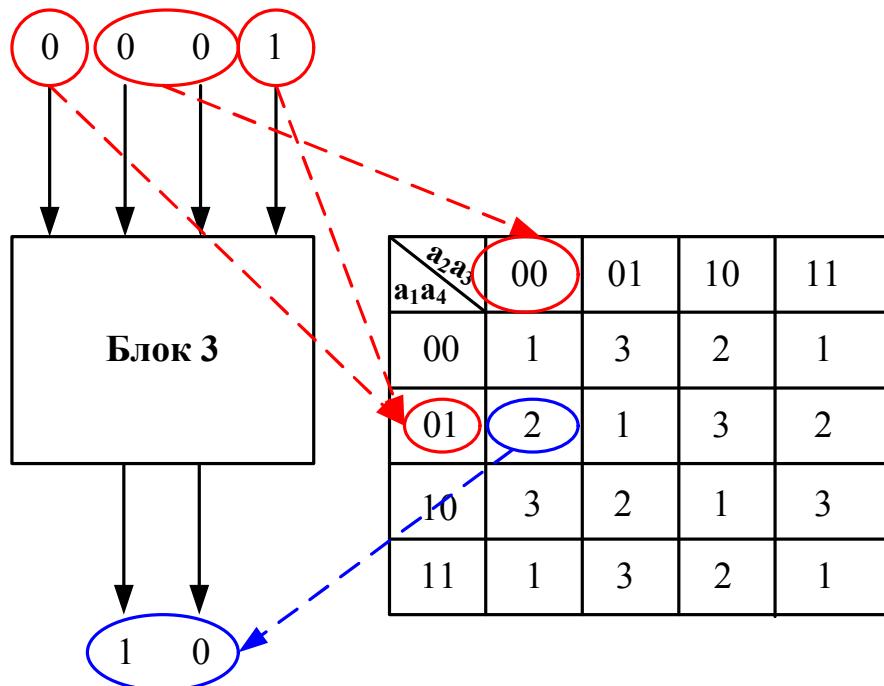


Рисунок 11 - Преобразование данных с помощью третьего блока замены

После того, как выполнено преобразование с помощью функции F, необходимо сложить левую часть сообщения на входе первого раунда шифрования (значение 11010111) с выходом функции F первого раунда шифрования (то есть со значением 01000011). В результате образуется значение 10010100. Далее правая и левая части сообщения меняются местами, то есть на вход второго раунда шифрования поступает последовательность 10100011 10010100.

Преобразования дальнейших двух раундов схожи с теми, которые были проведены в первом раунде шифрования. Мы не будем здесь повторять подробное описание одних и тех же действий. Однако, для того, чтобы проследить дальнейшие преобразования, отобразим их с помощью функции F для второго и третьего раундов, представленных соответственно на рис. 12 и 13.

На вход функции F второго раунда шифрования поступает значение 1001 0100, которое преобразуется к значению 0110 0001 в соответствии с рисунком 12. После этого выход функции F второго раунда шифрования (то есть значение 0110 0001) складывается по модулю два с левой частью сообщения на входе второго раунда шифрования (значение 1010 0011). В результате образуется значение 1100 0010. Далее правая и левая части сообщения меняются местами, то есть на вход третьего раунда шифрования поступает последовательность 10010100 11000010.

Так, на вход функции F третьего раунда шифрования поступает значение 1100 0010, которое преобразуется к значению 1011 1101 в соответствии с рисунком 13. После этого выход функции F третьего раунда шифрования (то есть значение 1011 1101) складывается по модулю два с левой частью сообщения на входе третьего раунда шифрования (значение 10010100). В результате образуется значение 0010 1001. Так как третий раунд шифрования является последним, то в нем не происходит обмена данными между правой и левой частями сообщения. Таким образом, на выход третьего

раунда шифрования поступает последовательность 00101001 11000010, которая и является искомым шифрованным сообщением.

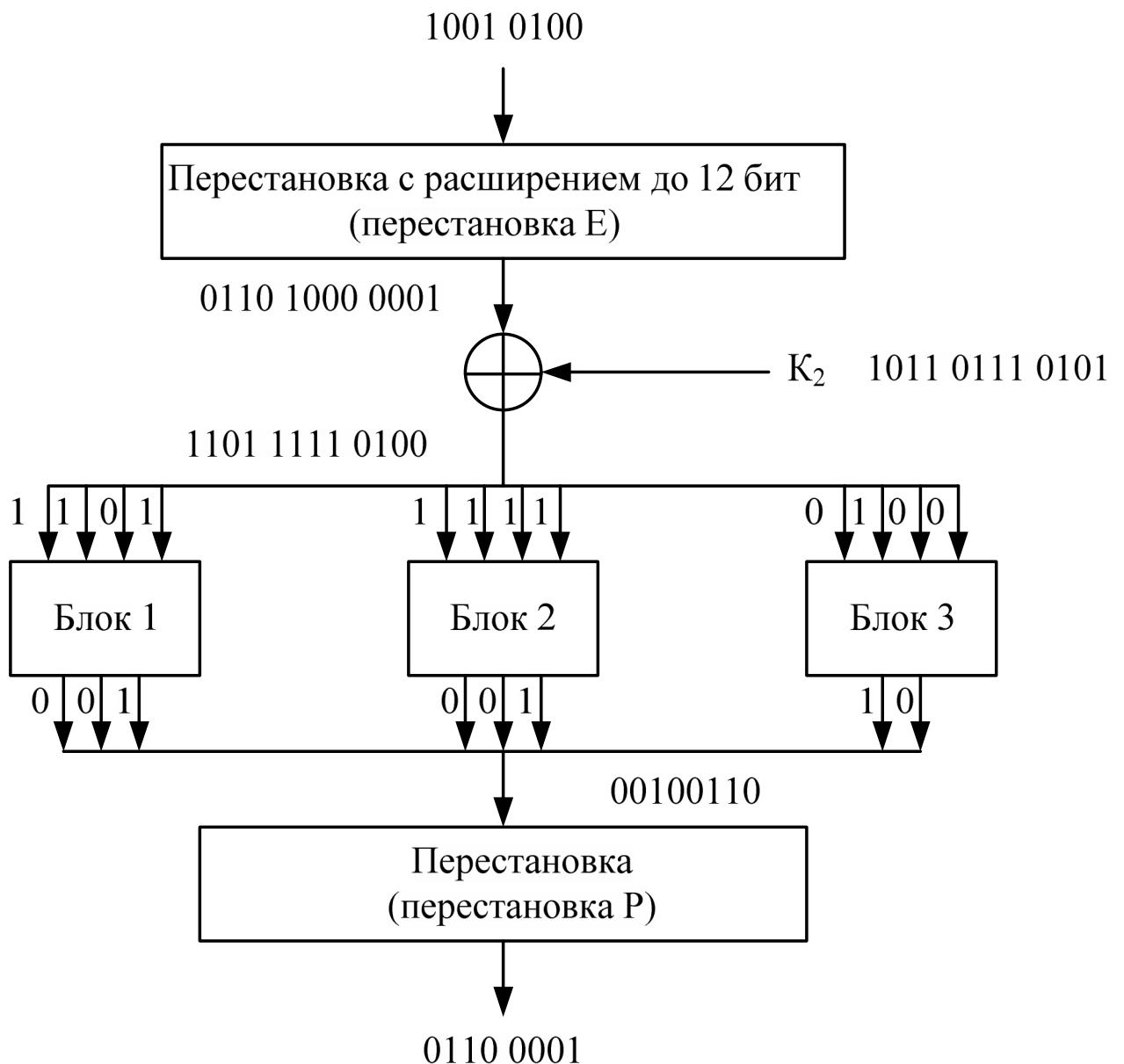


Рисунок 12 – Преобразование функции  $F$  второго раунда

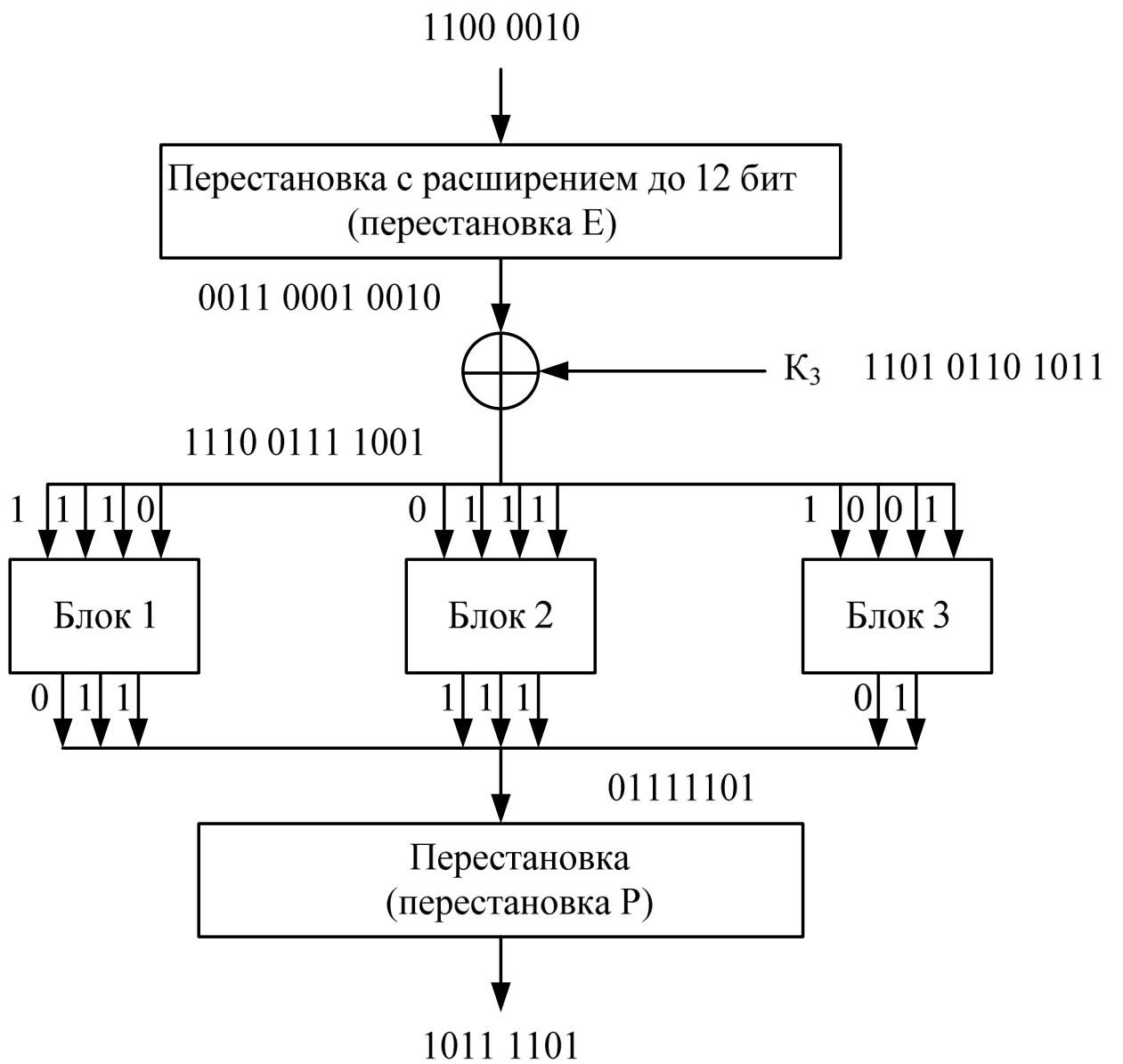


Рисунок 13 – Преобразование функции F третьего раунда

Дешифрование данных проводится по той же схеме, что и шифрование, с той разницей, что раундовые подключи используются в обратном порядке. Процесс дешифрования сообщения 00101001 11000010 представлен на рис. 14. Вы можете выполнить его самостоятельно, после чего сверить все промежуточные значения.

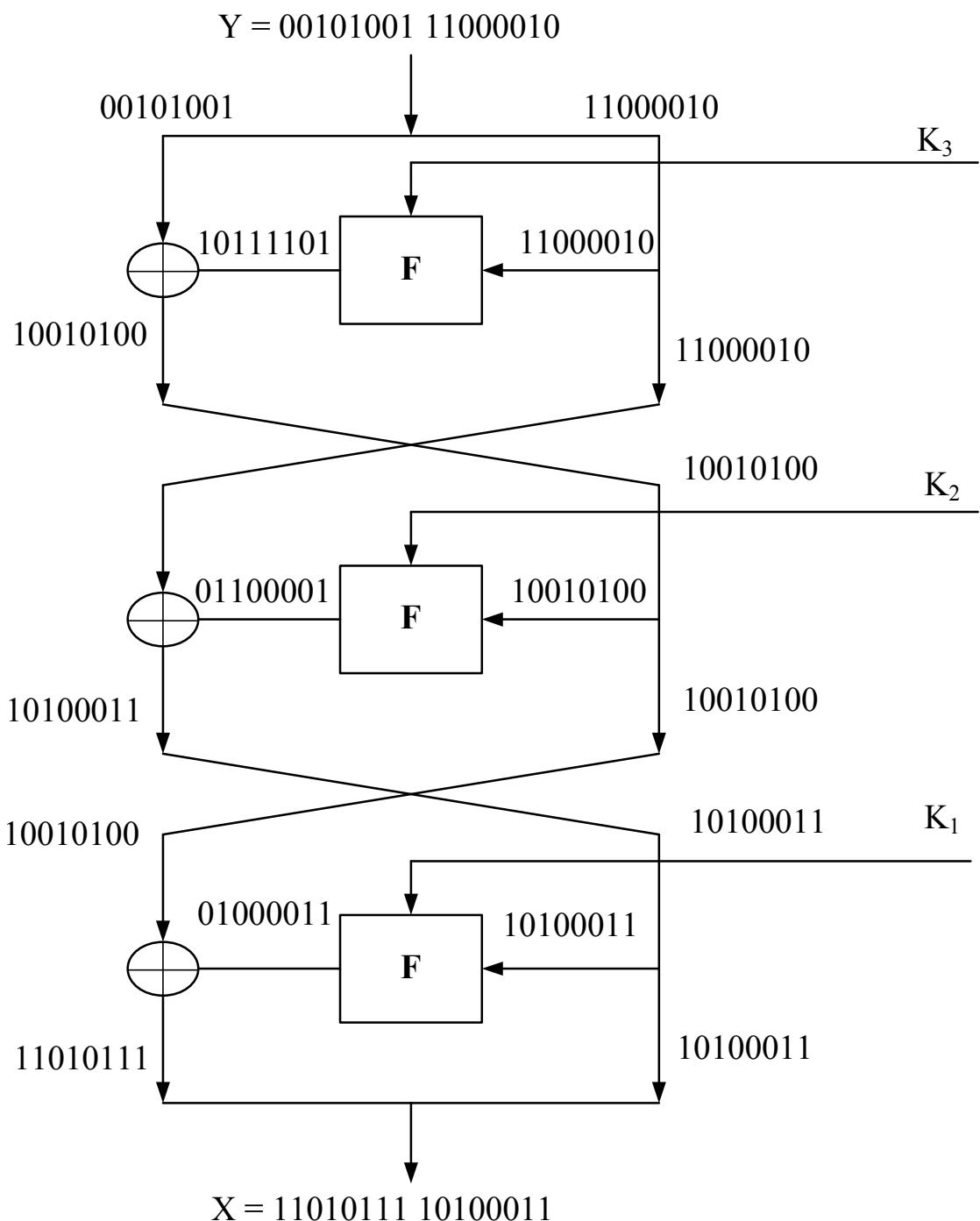


Рисунок 14 – Процесс дешифрования сообщения  $Y = 00101001 \ 11000010$  с помощью секретного ключа  $K = 0001 \ 1010 \ 1101 \ 1101 \ 0110 \ 1011$

## 1.8 Контрольные вопросы

1. Дайте определение Алгоритму шифрования.
2. Опишите принцип организации шифрования данных с использованием классической схемы Фейстеля.

3. Опишите работу учебного алгоритма шифрования.
4. Как работают блоки замены в учебном алгоритме шифрования?
5. В чем заключается особенность работы перестановки с расширением?
6. Как работает операция сложения по модулю два?
7. Почему один и тот же алгоритм шифрования, построенный по схеме Фейстеля, можно использовать как для зашифрования данных, так и для их дешифрования?
8. Чем отличается процесс дешифрования данных от процесса зашифрования?
9. Сколько различных ключей можно использовать для шифрования данных с помощью учебного алгоритма шифрования?

## **1.9 Задачи для самостоятельного решения**

### ***Задание №1***

Выполните сложение данных по модулю два. Сложение выполняйте в двоичной системе счисления. Результат вычислений переведите в систему счисления, в которой представлены слагаемые (нижние индексы слагаемых указывают на систему счисления, в которой они представлены).

- |                               |                              |
|-------------------------------|------------------------------|
| a) $173_{10} \oplus 21_{10}$  | d) $47_{16} \oplus 29_{16}$  |
| б) $113_{10} \oplus 75_{10}$  | е) $127_8 \oplus 215_8$      |
| в) $DE_{16} \oplus FC_{16}$   | ж) $C8_{16} \oplus 7B_{16}$  |
| г) $A23_{16} \oplus 18B_{16}$ | з) $58_{10} \oplus 137_{10}$ |

### ***Задание №2***

Выполните замену данных с использованием блоков замены учебного алгоритма шифрования

- a) Блок 1, входное сообщение 0100;

- б) Блок 1, входное сообщение 1100;
- в) Блок 2 входное сообщение 0010;
- г) Блок 2 входное сообщение 0110;
- д) Блок 3 входное сообщение 1001;
- е) Блок 3 входное сообщение 0000;
- ж) Блок 2 входное сообщение 1001;
- з) Блок 3 входное сообщение 1010.

### ***Задание №3***

Выполните преобразование данных с помощью перестановки с расширением в соответствии с таблицей 1.

- а) Входное сообщение 11011101;
- б) Входное сообщение 00110110;
- в) Входное сообщение 01001001;
- г) Входное сообщение 11101101;
- д) Входное сообщение 01000101;
- е) Входное сообщение 11101001.

### ***Задание №4***

Выполните преобразование данных с помощью обычной перестановки в соответствии с таблицей 5.

- а) Входное сообщение 01101101;
- б) Входное сообщение 10110111;
- в) Входное сообщение 10001010;
- г) Входное сообщение 00011010;
- д) Входное сообщение 11011101;
- е) Входное сообщение 01011111.

### ***Задание №5***

Выполните обратное преобразование данных, полученных в результате преобразования с помощью перестановки с расширением в соответствии с таблицей 1.

- а) Входное сообщение 011101010111;
- б) Входное сообщение 100101111110;
- в) Входное сообщение 110110011011;
- г) Входное сообщение 011101110111;
- д) Входное сообщение 111001001101;
- е) Входное сообщение 100110001010;
- ж) Входное сообщение 101101111110;
- з) Входное сообщение 100111001110.

### ***Задание №6***

Выполните обратное преобразование данных, полученных в результате преобразования с помощью обычной перестановки в соответствии с таблицей 5.

- 1) Входное сообщение 10001011;
- 2) Входное сообщение 11011000;
- 3) Входное сообщение 01010110;
- 4) Входное сообщение 01101100;
- 5) Входное сообщение 11000111;
- 6) Входное сообщение 01011101;
- 7) Входное сообщение 01100001;
- 8) Входное сообщение 11000100.

### **Задание №7**

Зашифруйте сообщение X на ключе K с помощью учебного алгоритма шифрования. Сообщение X и ключ K представлены в десятичном виде. Ответ также представьте в десятичном виде.

№	X	K
1	43827	9375679
2	56241	8354877
3	18354	3150189
4	215	13745678
5	3784	3956874
6	53112	5138975
7	55555	10185130
8	10378	11252511
9	31825	5178345
10	812	7845832
11	41576	8123445
12	31567	569784
13	65112	3150192
14	382	7345679
15	25386	8345678
16	7536	12053864
17	8254	1073895
18	13112	6783759
19	44444	7814580
20	27356	3150012

## 2. МЕТОД ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА

### 2.1 Понятие дифференциального криптоанализа. Общие сведения.

Само название дифференциальный криптоанализ происходит от английского слова *difference*, то есть разность. Именно поэтому в отечественной литературе этот вид анализа еще иногда называют разностным методом. Исходя из названия, можно понять, что при рассмотрении возможности анализа некоторого блочного алгоритма шифрования ученым пришло в голову рассматривать не отдельные тексты, а пары текстов. Понятно, что два взятых текста будут иметь различия в некоторых позициях (далее по тексту мы будем вести речь о текстах или сообщениях, подвергающихся зашифрованию, однако подразумевать будем их двоичное представление, так как рассматриваемые нами алгоритмы блочного шифрования оперируют двоичной информацией). Для того, чтобы определить это различие, достаточно пару текстов сложить между собой по модулю два. Результат такого сложения даст на выходе значение 0 в тех позициях, в которых исходные тексты были равны между собой (то есть оба бита были равны нулю или единице), и соответственно значение 1 в тех позициях, в которых исходные тексты отличались. Например, рассмотрим два 4-битовых сообщения:  $X = 0011$  и  $X' = 1010$ . Определим различие этих сообщений:

$$\begin{array}{r} \oplus \\ X = 0 \ 0 \ 1 \ 1 \\ X' = 1 \ 0 \ 1 \ 0 \\ \hline \Delta X = 1 \ 0 \ 0 \ 1 \end{array}$$

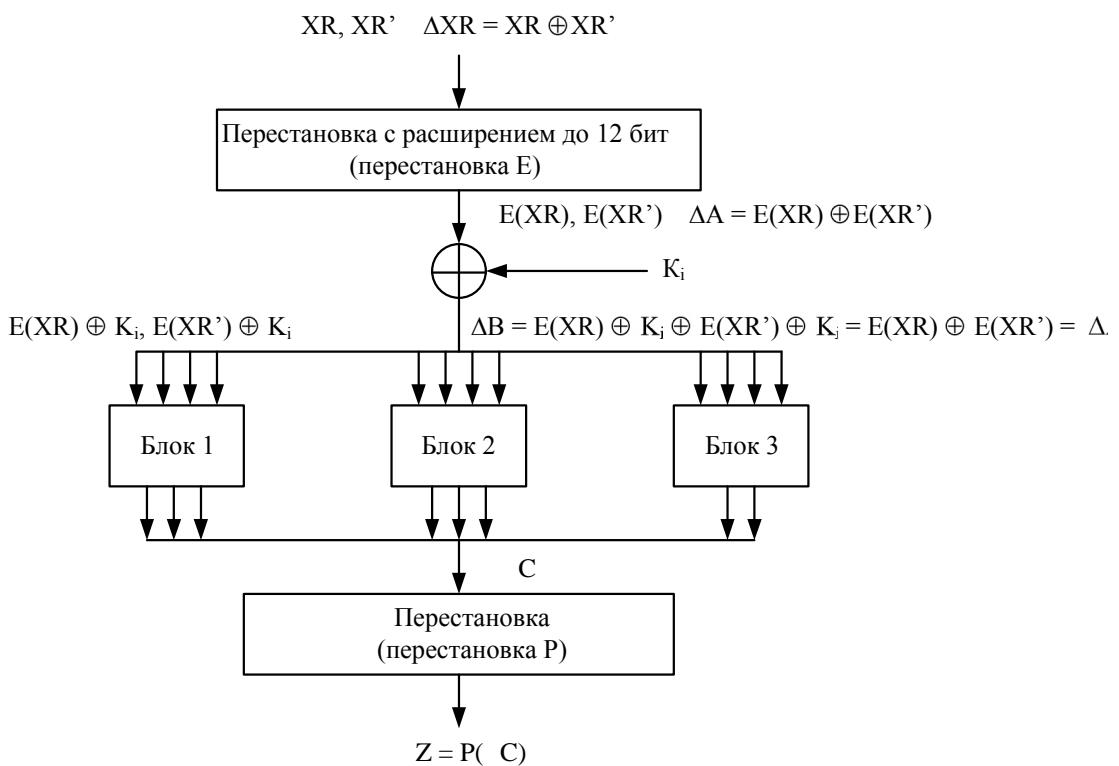
В результате сложения текстов  $X$  и  $X'$  была получена разность  $\Delta X = 1001$ , полученное значение  $\Delta X$  принято называть дифференциалом или разностью.

В дифференциальном криптоанализе значение разности (дифференциала) принято обозначать символом  $\Delta$ . Разность, полученная в результате сложения текстов  $X$  и  $X'$  показывает, что во второй и третьей позициях исходные сообщения  $X$  и  $X'$  были равны, а в первой и четвертой отличались друг от друга. Здесь сразу же стоит оговориться, что и для рассматриваемых нами алгоритмов шифрования, и для рассматриваемых сообщений нумерация позиций битов ведется слева направо от единицы, в отличие, например, от машинного представления двоичной информации, когда самый младший бит находится справа и отсчет ведется от нуля.

Итак, мы рассмотрели понятие разности. Возникает вопрос: за счет каких механизмов становится возможным провести анализ, рассматривая не сами сообщения, а их различия. Для того, чтобы ответить на этот вопрос, рассмотрим процесс преобразования таких разностей при их прохождении через функцию  $F$ , например, Учебного алгоритма шифрования, который будет использован в лабораторных работах (см. рис. 15)

Будем считать, что на вход рассматриваемой функции  $F$  поступает два независимых сообщения  $XR$  и  $XR'$  (индекс  $R$  обозначает правую часть сообщения  $X$ , поступающего на вход раунда шифрования, от англ. right - правый), разность которых равна  $\Delta XR$ . Мы знаем, что первое преобразование, которому будут подвергнуты сообщения  $XR$  и  $XR'$  – это перестановка с расширением. Обычно ее еще называют E-перестановка (от англ. Expansion – расширение). Так как таблица, в соответствии с которой работает перестановка с расширением, нам известна, то мы легко можем определить значения  $E(XR)$  и  $E(XR')$ , которые появятся на выходе этой перестановки для соответствующих значений  $XR$  и  $XR'$ . А значит, мы можем определить, чему будет равно значение разности на выходе E-перестановки. Обозначим это значение разности как  $\Delta A$ , тогда получим:

$$\Delta A = E(XR) \oplus E(XR').$$



15 –

F

,

$K_i$ .

( R ) ( R )

( R )  $\oplus K_i$ , ( R' )

( R' )  $\oplus K_i$ , ,

(

):

$$= ( R ) \oplus K_i \oplus ( R' ) \oplus K_i = ( R ) \oplus ( R' ) = .$$

,

,

R R'

,  
K<sub>i</sub> R,  
R'. , ,  
. , ,  
изменяет сами  
**сообщения, не оказывает влияния на разность**

,  
,

( ),  
,

( ). , ,  
.

,  
,

- ( . Permutation -  
).

, ,  
-

Z

, F.  
.

F,

,  
 .  
 ,  
 ,  
 :  
 ,  
 ?  
 ,  
 . 16.

$$\begin{array}{ccccccc}
 X & = & X & \oplus & X & = & 0 \\
 & & \downarrow & & \downarrow & & \\
 & & F & \leftarrow K & F & \leftarrow K & \\
 & & \downarrow & & \downarrow & & \\
 Y & = & Y & \oplus & Y & = & 0
 \end{array}$$

16 -

, , ,  
 , , ,  
 , , ,  
 )

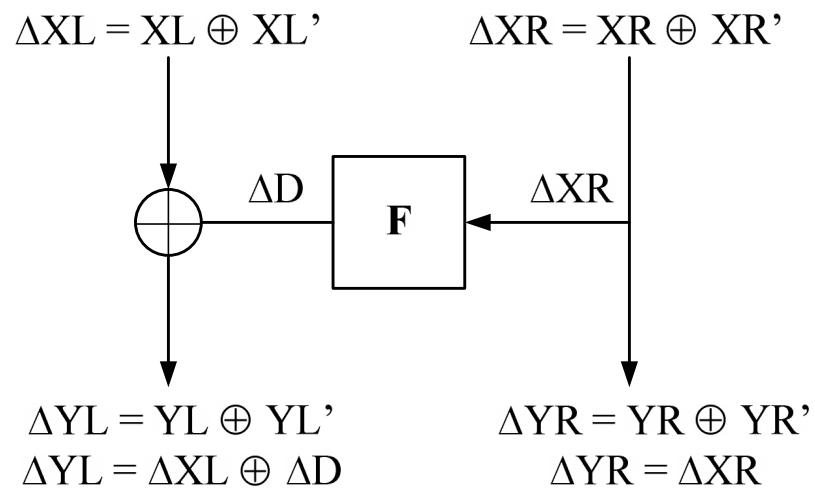
, , ,  
 Y. ,

, **всегда**, = 1,

## 2.2 Дифференциальный криптоанализ одного раунда шифрования

F

17.



17 –

$XL( \quad ) \quad XR( \quad )$

).  $Y$

$YL( \quad ) \quad YR( \quad )$

,  
17.

$$X = (XL, XR)$$

$$X' = (XL', XR').$$

XL,

-

XR.

XR

F.

,

F

.

17

D.

XL

$$F - D,$$

YL:

$$YL = XL \oplus D,$$

YR

XR,

:

$$YR = XR.$$

,

18. , 17,

$$X - X',$$

XR,

F-

, ,

F-

,

18,

D.

,

,

XL

D:

XL = D.

,

,

,

,

( XL = D)

F ( D),

:

YL = XL  $\oplus$  D = 0

,

,

19.

,

,

,

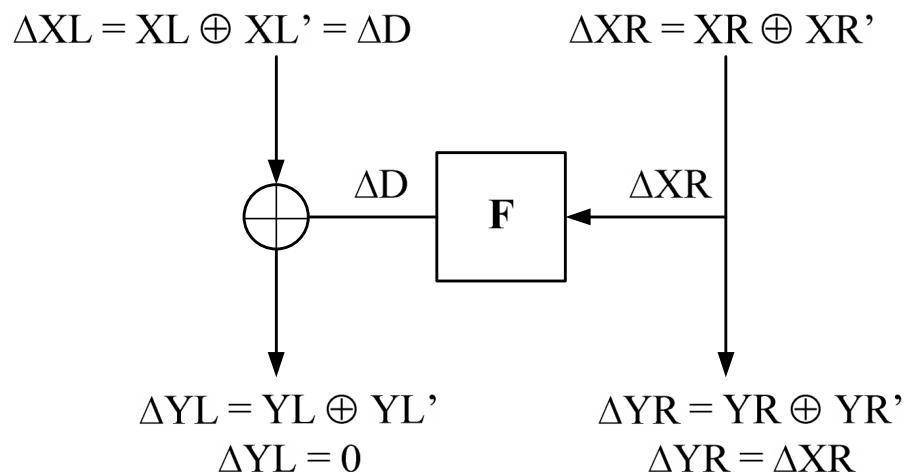
( XR = 0).

,

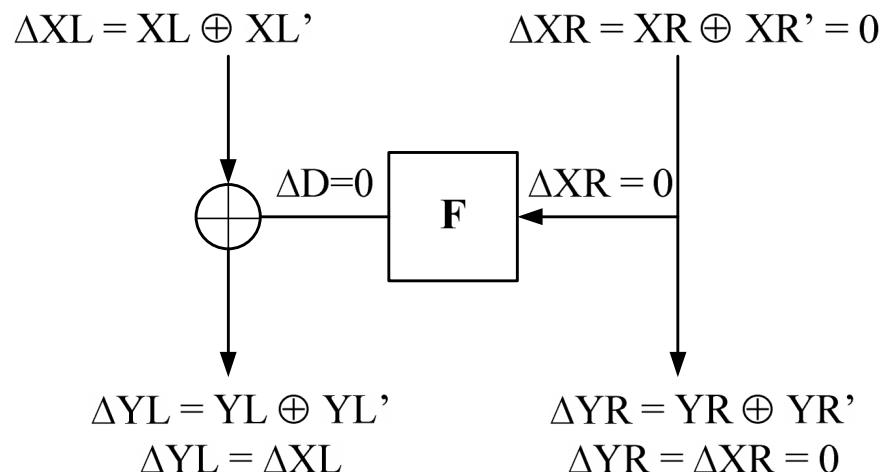
16,

,

0. 100 %-,  
 F , 19,  
 , ( D = 0). ,



18 -



19 - ,

20.

*Характеристика* –

*входной разностью,*

*– выходной разностью.*

*Раундовая характеристика* –

*Вероятность характеристики* –

## 2.3 Дифференциальный криптоанализ трех раундов шифрования

21.

18.

$X \quad X'$ ,

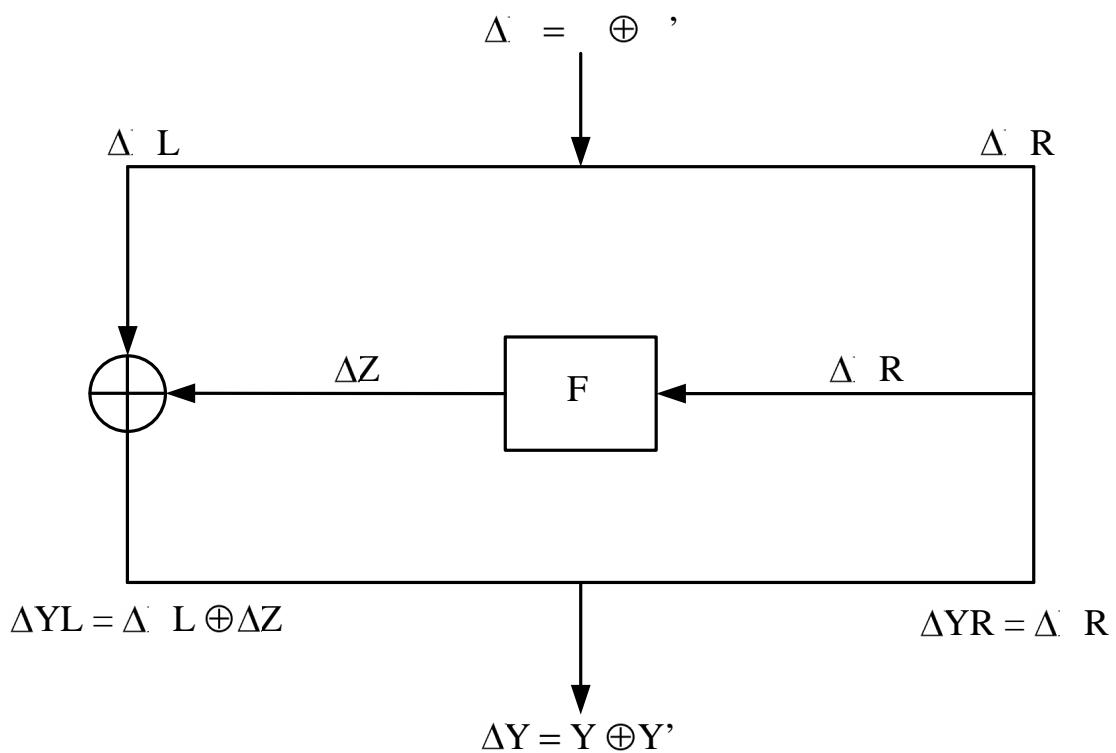
$XR$ .

$XR$

$(\quad XR, \quad D)$

$X \quad X'$

D.



$(\Delta X, \Delta Y) -$

$(\Delta X_R, \Delta Z) -$

$\Delta X$   
—  
 $\Delta X_R$   
—

$\Delta Y$   
—  
 $\Delta Z$   
—

20 -

,  $F$

, .

$F$

$F$

2                    XR (    21),

F

,                    XR.    ,                    21

F    ,                    D,

:                    ?

.    ,

XR    D

F    p<sub>1</sub>.

,

p<sub>2</sub> = 1.

,    F.    ,

( G = 0).    ,

YL    ,    F

,                    :

YL = G ⊕     = 0 ⊕     =

F-

,

,

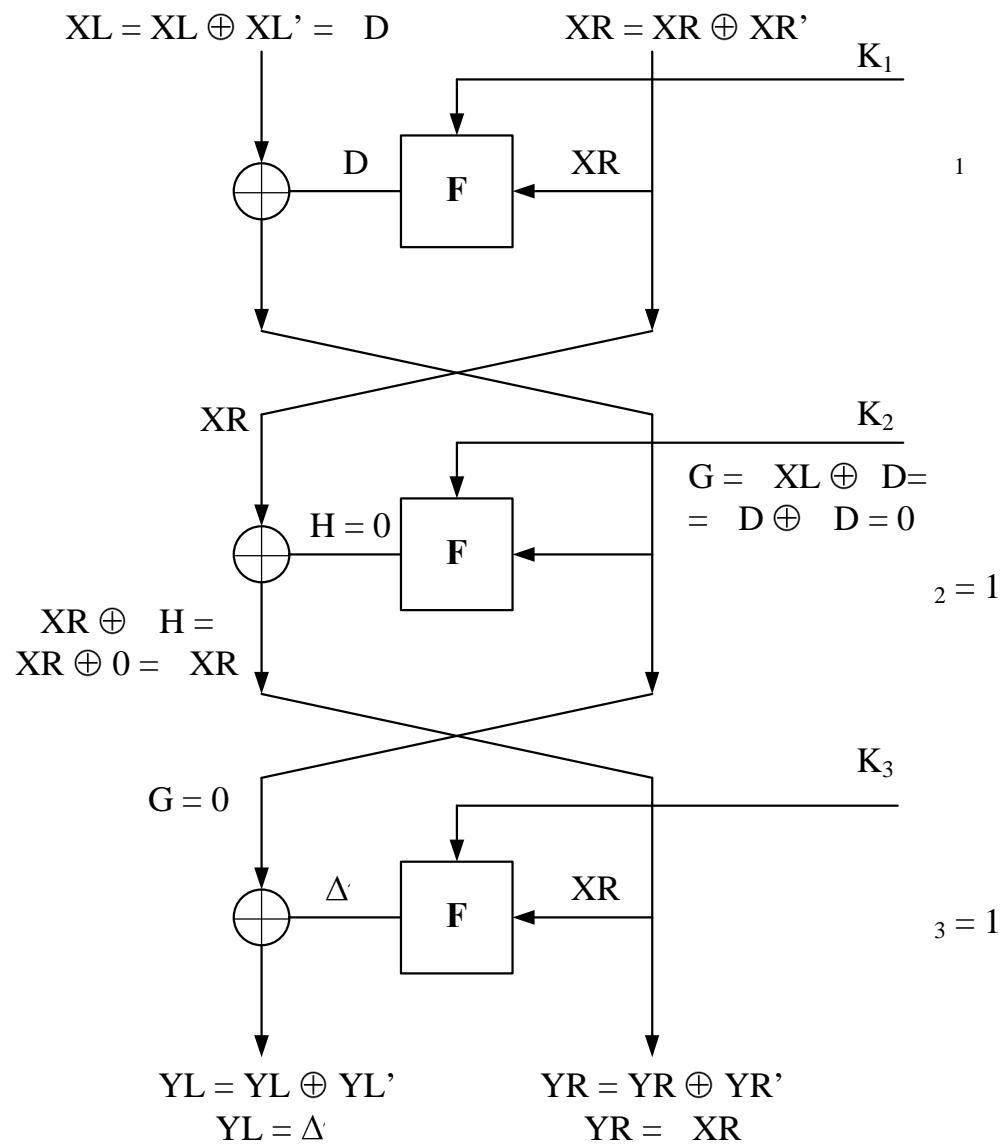
p<sub>3</sub> = 1,

F    .

,    21,    ,

:    ,    ( XL= D,    XR);

,    ( ,    XR).



21 -

, ,  
 3-, ,  
 .  
 :

$$p = p_1 * p_2 * p_3 = p_1 * 1 * 1 = p_1.$$

, ,  
,  
?

*наиболее вероятное*

, , ,  
, , ,  
21.

,  
:  
, , , ,

,  
:  
 $X = (XL, XR) \quad X' = (XL', XR')$ .  
 $X$   
 $= (XL, XR)$ .

,  
 $F(X, XR)$   
 $F(X, XR')$   
 $D(X, X')$   
,

:  $Y = (YL, YR) \quad Y' = (YL', YR')$ .

,  
,

,  
,  
,  
 $YR$ .  
 $YR$

XR,

:

YR = XL.

,

X X',

Y Y'

*правильной парой текстов.*

,

,

:

1 3.

,

F-

,

,

.

.

,

F

.

F

:

XR XR',

XR.

F,

,

D,

,

,

,

F-

.

15

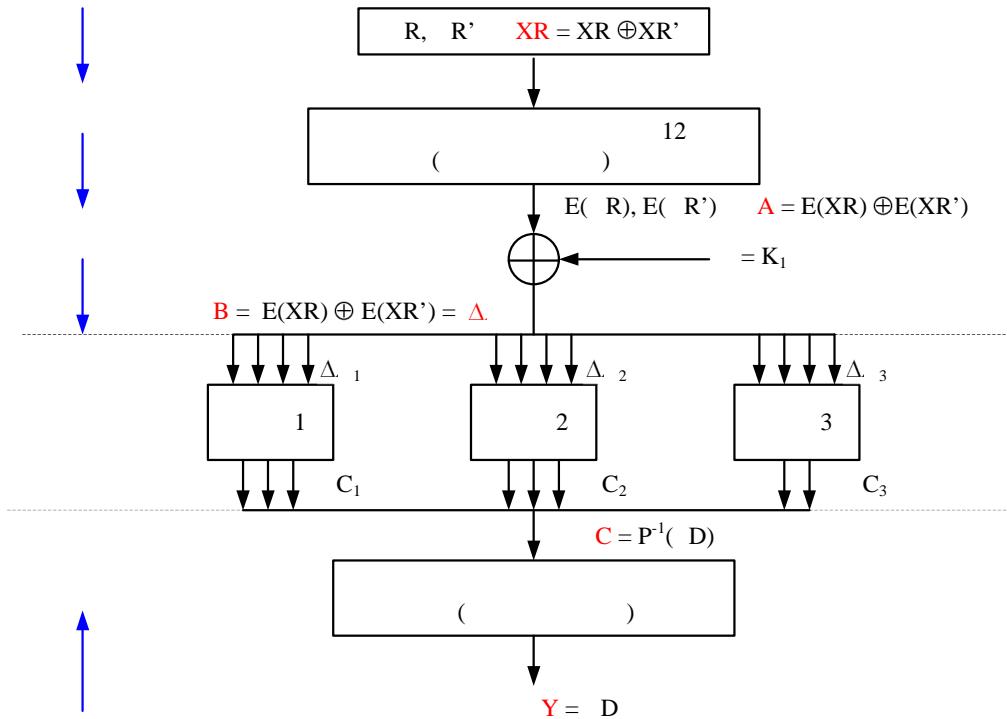
,

22.

,

15,

3-



22 -

22 , , ,  
 $F$  , , ,  $B =$   
 $A$  , , ,  $E(XR)$   
 $E(XR')$ .  $K_1.$   
 $F$  , ,  
 $C$ ,  
 $D$

22

$-1$ .

,  
 $F$ .

,

$A$

$2^n$

,

$n -$

,

,

,

,

,

,

,

$1,$

$2$

$3$

$1,$

$2$

$3.$

$j,$

$j -$

,

,

.

23

$$X_{Text1} \oplus X_{Text2} = \Delta A$$

↓      ↓

Блок замены

Блок замены

↓      ↓

$$Y_{Text1} \oplus Y_{Text2} = \Delta C$$

23 –

,

,

:

$E(XR) \oplus K_1 = E(XR') \oplus K_1.$

$E(XR) \oplus K_1 = X_{Text1};$

$$E(XR') \oplus K_1 = X\_Text2.$$

, , : ;

$$K_1 = E(XR) \oplus X\_Text1;$$
$$K_1 = E(XR') \oplus X\_Text2.$$

1.

1.

,

—

.

.

,

F

,

: YR

YR'.

F

,

YR. **Важно!**

,

,

F

,

,

F

,

F

21,

F

,

,

,

,

,

YL.

## 2.4 Контрольные вопросы

1.

?

2.

F

,       $\Delta^- = \Delta^+$  ?

3.

?      ?

4.

,      ,      ?

?

5.

?

6.

?

7.

?

8.

n-

?

9.

?

10.

$\Delta$  ,

n      ?

### **3. МЕТОД ЛИНЕЙНОГО КРИПТОАНАЛИЗА**

#### **3.1 Понятие линейного криптоанализа. Общие сведения.**

90-

XX

(Matsui).

[5]

DES,

$2^{47}$ .

,

,

, [5],

,

,

,

E ( . Encryption – ),

Y:

$$Y = E(X, K). \quad (6)$$

Y.

(6)

• •

,

(6)

,

p.

p

0,5 (

0

).

,

,

,

.

### Определение.

(6)

Q,

,

Y

$\alpha, \gamma,$

:

$$Q = (X, \alpha) \oplus (Y, \beta) \oplus (K, \gamma) \quad (7)$$

,

, Q=0

0,5 ( (Q=0) 0,5).

,

,

,

,

Определение.

$$\eta = |1 - 2|, \quad - \quad ,$$

,

$$= 0,5.$$

,

$$p_1 = \frac{1}{8}, \quad p_2 = \frac{7}{8} \quad p_3 = \frac{1}{4}.$$

:

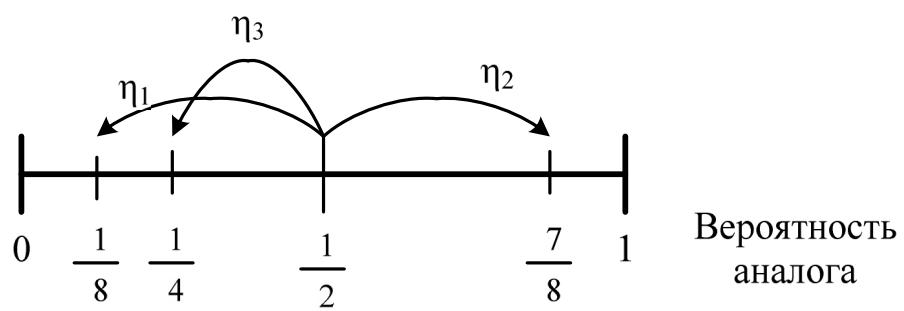
$$\eta_1 = |1 - 2p_1| = \left|1 - 2\frac{1}{8}\right| = \left|1 - \frac{1}{4}\right| = \frac{3}{4};$$

$$\eta_2 = |1 - 2p_2| = \left|1 - 2\frac{7}{8}\right| = \left|1 - \frac{7}{4}\right| = \left|-\frac{3}{4}\right| = \frac{3}{4};$$

$$\eta_3 = |1 - 2p_3| = \left|1 - 2\frac{1}{4}\right| = \left|1 - \frac{1}{2}\right| = \frac{1}{2}.$$

, ,

24.



24 –

24 , =0,5

=1

=1. ,

,

$\frac{3}{4}$ .

,

:

1. ( )

,

.

2.

:

( - ),

.

3.

( )

,

,

(

).

.

### **3.2 Нахождение эффективных линейных статистических аналогов для одного раунда шифрования**

1,

,

,

.

,

,

— 7 — 9.

6,

6

7	1	3	8	2	4	6	5	3	1	6	7
---	---	---	---	---	---	---	---	---	---	---	---

7

1

a2a3a4	000	001	010	011	100	101	110	111
a1								
0	1	5	5	1	7	2	3	7
1	2	6	6	3	4	0	0	4

8

2

a2a3a4	000	001	010	011	100	101	110	111
a1								
0	7	2	0	5	2	7	0	5
1	4	4	3	3	1	1	6	6

3

<b>a2a3</b>	<b>00</b>	<b>01</b>	<b>10</b>	<b>11</b>
<b>a1 a4</b>				
<b>00</b>	3	3	2	2
<b>01</b>	3	3	2	2
<b>10</b>	1	1	0	0
<b>11</b>	1	1	0	0

,

.

, ,

,

.

.

(7)

,

Y

 $\alpha, \gamma.$ 

,

,

,

,

(7)

:

 $Q = (X \oplus K, \alpha) \oplus (Y, \beta).$ 

(8)

,

(8)

:

$$(X \oplus K, \alpha) = (X \oplus K)_1 \alpha_1 \oplus \dots \oplus (X \oplus K)_n \alpha_n, \quad (9)$$

$$(Y, \beta) = Y_1 \beta_1 \oplus \dots \oplus Y_m \beta_m, \quad (10)$$

n -

,

m -

.

$$(9) \quad (10)$$

,

$\alpha$  ,

1.

$\alpha$

,

, Q=0.

$\alpha$

,

,

,

,

,

.

— .

,

$\alpha$

,

1.

,

,

$\alpha$

0001      1111 (      15

).

001      111 (      7      )

—

01      11

(      3      ).

$(\alpha, \beta)$

-

$(\alpha, \beta) = (1011, 101)$ .

16

(      0000      1111).

7

,

10.

$(X \oplus K)$	Y
0000	001
0001	101
0010	101
0011	001
0100	111
0101	010
0110	011
0111	111
1000	010
1001	110
1010	110
1011	011
1100	100
1101	000
1110	000
1111	100

$$\begin{array}{ll}
((X \oplus K), Y) & 10: ((X \oplus K), Y) \\
= (0000, 001). & Q: \\
& (8)
\end{array}$$

$$\begin{aligned}
Q = & (X \oplus K, \alpha) \oplus (Y, \beta) = (X \oplus K)_1 \alpha_1 \oplus (X \oplus K)_2 \alpha_2 \oplus (X \oplus K)_3 \alpha_3 \oplus (X \oplus K)_4 \alpha_4 \oplus \\
& \oplus Y_1 \beta_1 \oplus Y_2 \beta_2 \oplus Y_3 \beta_3 \oplus Y_4 \beta_4 = 0 \bullet 1 \oplus 0 \bullet 0 \oplus 0 \bullet 1 \oplus 0 \bullet 1 \oplus 0 \bullet 1 \oplus 0 \bullet 0 \oplus 1 \bullet 1 = 1
\end{aligned}$$

$$\begin{array}{ll}
Q & 15 \\
((X \oplus K), Y) & 10. \\
11. &
\end{array}$$

$$Q = (\alpha, \beta) = (1011, 101)$$

$(X \oplus K)$	$Y$	$Q = (X \oplus K, \alpha) \oplus (Y, \beta) =$ $Q = (X \oplus K)_1 \alpha_1 \oplus (X \oplus K)_2 \alpha_2 \oplus (X \oplus K)_3 \alpha_3 \oplus$ $\oplus (X \oplus K)_4 \alpha_4 \oplus Y_1 \beta_1 \oplus Y_2 \beta_2 \oplus Y_3 \beta_3 \oplus Y_4 \beta_4$
0000	001	$Q = 0 \bullet 1 \oplus 0 \bullet 0 \oplus 0 \bullet 1 \oplus 0 \bullet 1 \oplus 0 \bullet 1 \oplus 0 \bullet 0 \oplus 1 \bullet 1 = 1$
0001	101	$Q = 0 \bullet 1 \oplus 0 \bullet 0 \oplus 0 \bullet 1 \oplus 1 \bullet 1 \oplus 1 \bullet 1 \oplus 0 \bullet 0 \oplus 1 \bullet 1 = 1$
0010	101	$Q = 0 \bullet 1 \oplus 0 \bullet 0 \oplus 1 \bullet 1 \oplus 0 \bullet 1 \oplus 1 \bullet 1 \oplus 0 \bullet 0 \oplus 1 \bullet 1 = 1$
0011	001	$Q = 0 \bullet 1 \oplus 0 \bullet 0 \oplus 1 \bullet 1 \oplus 1 \bullet 1 \oplus 0 \bullet 1 \oplus 0 \bullet 0 \oplus 1 \bullet 1 = 1$
0100	111	$Q = 0 \bullet 1 \oplus 1 \bullet 0 \oplus 0 \bullet 1 \oplus 0 \bullet 1 \oplus 1 \bullet 1 \oplus 1 \bullet 0 \oplus 1 \bullet 1 = 0$
0101	010	$Q = 0 \bullet 1 \oplus 1 \bullet 0 \oplus 0 \bullet 1 \oplus 1 \bullet 1 \oplus 0 \bullet 1 \oplus 1 \bullet 0 \oplus 0 \bullet 1 = 1$
0110	011	$Q = 0 \bullet 1 \oplus 1 \bullet 0 \oplus 1 \bullet 1 \oplus 0 \bullet 1 \oplus 0 \bullet 1 \oplus 1 \bullet 0 \oplus 1 \bullet 1 = 0$
0111	111	$Q = 0 \bullet 1 \oplus 1 \bullet 0 \oplus 1 \bullet 1 \oplus 1 \bullet 1 \oplus 1 \bullet 1 \oplus 1 \bullet 0 \oplus 1 \bullet 1 = 0$
1000	010	$Q = 1 \bullet 1 \oplus 0 \bullet 0 \oplus 0 \bullet 1 \oplus 0 \bullet 1 \oplus 0 \bullet 1 \oplus 1 \bullet 0 \oplus 0 \bullet 1 = 1$
1001	110	$Q = 1 \bullet 1 \oplus 0 \bullet 0 \oplus 0 \bullet 1 \oplus 1 \bullet 1 \oplus 1 \bullet 1 \oplus 1 \bullet 0 \oplus 0 \bullet 1 = 1$
1010	110	$Q = 1 \bullet 1 \oplus 0 \bullet 0 \oplus 1 \bullet 1 \oplus 0 \bullet 1 \oplus 1 \bullet 1 \oplus 1 \bullet 0 \oplus 0 \bullet 1 = 1$
1011	011	$Q = 1 \bullet 1 \oplus 0 \bullet 0 \oplus 1 \bullet 1 \oplus 1 \bullet 1 \oplus 0 \bullet 1 \oplus 1 \bullet 0 \oplus 1 \bullet 1 = 0$
1100	100	$Q = 1 \bullet 1 \oplus 1 \bullet 0 \oplus 0 \bullet 1 \oplus 0 \bullet 1 \oplus 1 \bullet 1 \oplus 0 \bullet 0 \oplus 0 \bullet 1 = 0$
1101	000	$Q = 1 \bullet 1 \oplus 1 \bullet 0 \oplus 0 \bullet 1 \oplus 1 \bullet 1 \oplus 0 \bullet 1 \oplus 0 \bullet 0 \oplus 0 \bullet 1 = 0$
1110	000	$Q = 1 \bullet 1 \oplus 1 \bullet 0 \oplus 1 \bullet 1 \oplus 0 \bullet 1 \oplus 0 \bullet 1 \oplus 0 \bullet 0 \oplus 0 \bullet 1 = 0$
1111	100	$Q = 1 \bullet 1 \oplus 1 \bullet 0 \oplus 1 \bullet 1 \oplus 1 \bullet 1 \oplus 1 \bullet 1 \oplus 0 \bullet 0 \oplus 0 \bullet 1 = 0$

$$11, 8, 16, Q, 0.$$

$$, , P(Q=0) = \frac{8}{16} = \frac{1}{2}.$$

$$(\alpha, \beta).$$

12.

$$\alpha, - .$$

$$, \quad Q=0. \quad , \quad 12 \\ (\alpha=1011) \quad (=101) \quad \frac{1}{2}.$$

12

	001	010	011	100	101	110	111
$\alpha$							
0001	$\frac{1}{2}$						
0010	$\frac{5}{8}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{1}{2}$	$\frac{3}{8}$
0011	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{1}{8}$
0100	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{1}{8}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$
0101	$\frac{5}{8}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{1}{2}$	$\frac{3}{8}$
0110	$\frac{1}{2}$						
0111	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
1000	$\frac{1}{8}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{1}{2}$	$\frac{3}{8}$
1001	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$
1010	$\frac{1}{2}$						
1011	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	$\frac{1}{2}$
1100	$\frac{1}{2}$	1	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
1101	$\frac{1}{2}$						
1110	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$
1111	$\frac{5}{8}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{1}{8}$	$\frac{1}{2}$	$\frac{3}{8}$

, 8 9.

13 14.

13

	001	010	011	100	101	110	111
$\alpha$							
0001	$\frac{5}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{5}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{1}{2}$
0010	$\frac{1}{2}$						
0011	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{1}{2}$
0100	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{2}$
0101	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{1}{2}$
0110	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
0111	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{1}{2}$
1000	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	$\frac{1}{2}$	$\frac{1}{2}$
1001	$\frac{5}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{5}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{1}{2}$
1010	$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
1011	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{1}{2}$
1100	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{1}{2}$
1101	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{1}{2}$
1110	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
1111	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{1}{2}$

	01	10	11
$\alpha$			
0001	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
0010	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
0011	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
0100	0	$\frac{1}{2}$	$\frac{1}{2}$
0101	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
0110	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
0111	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
1000	$\frac{1}{2}$	0	$\frac{1}{2}$
1001	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
1010	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
1011	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
1100	$\frac{1}{2}$	$\frac{1}{2}$	1
1101	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
1110	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
1111	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$

12 – 14

,

12

,

1 ( $= 1$ )

,

$$1 \quad \frac{3}{4} \left( = \frac{1}{8} \right).$$

$$13 \quad ( = 0 \quad = 1) \\ 1 \quad ( = \frac{1}{4} \quad = \frac{3}{4}),$$

$$1 \quad \frac{1}{2}, \quad ,$$

14

$$( = 0 \quad = 1) \quad 1.$$

$$14 \quad \frac{1}{2},$$

$(\alpha, )$

$$(\alpha, ), \quad , \quad Q=0,$$

,

$$, \quad 1.$$

$$25. \quad 16- \quad ,$$

$$: \quad XL \quad - \quad XR.$$

$$F \quad XR.$$

F

$$^i, \quad i- \quad . \quad F$$

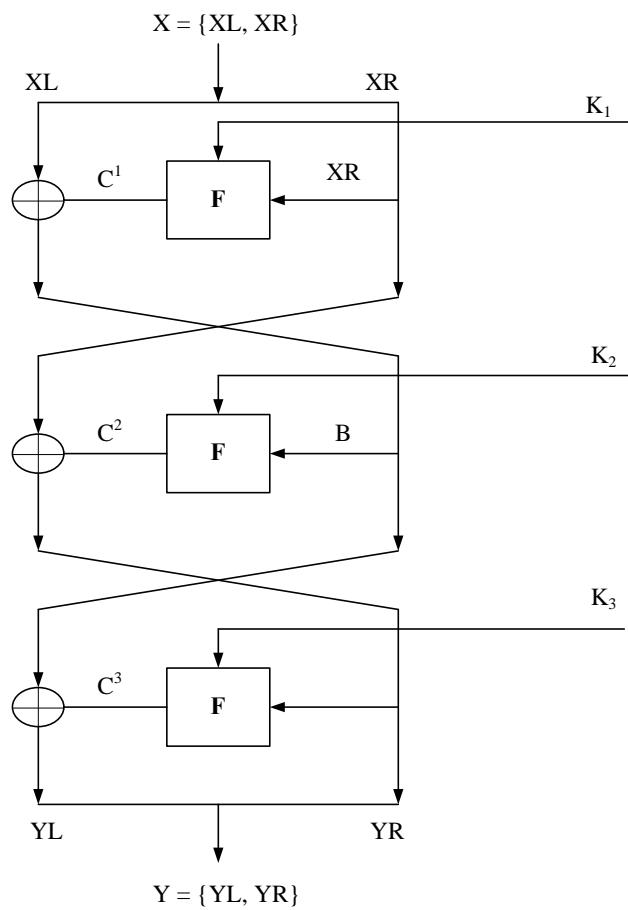
$$, \quad . \quad Y,$$

$$: \quad YL \quad - \quad YR.$$

,

F

YR.



25 -

F

X.

F

9 —

16 —

( . 26).

12 ,

26.

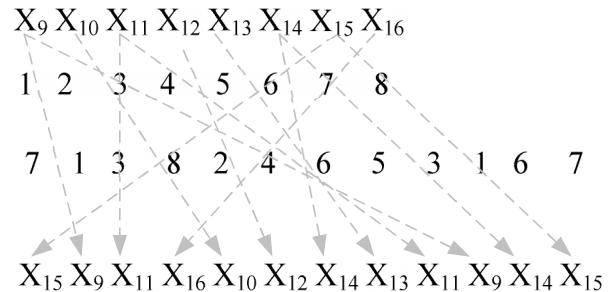
Исходный порядок битов:

Порядковая нумерация битов:

Таблица перестановки с расширением:

Порядок битов после применения  
перестановки с расширением:

26 –



12

( . . . . . . . . 4).

,

4

27

F

25.

,

F

8-

1.

F

—

,

27

1

.. 8 1 ..

,

,

1 1 .. 8 1

,

,

.. , ,

,

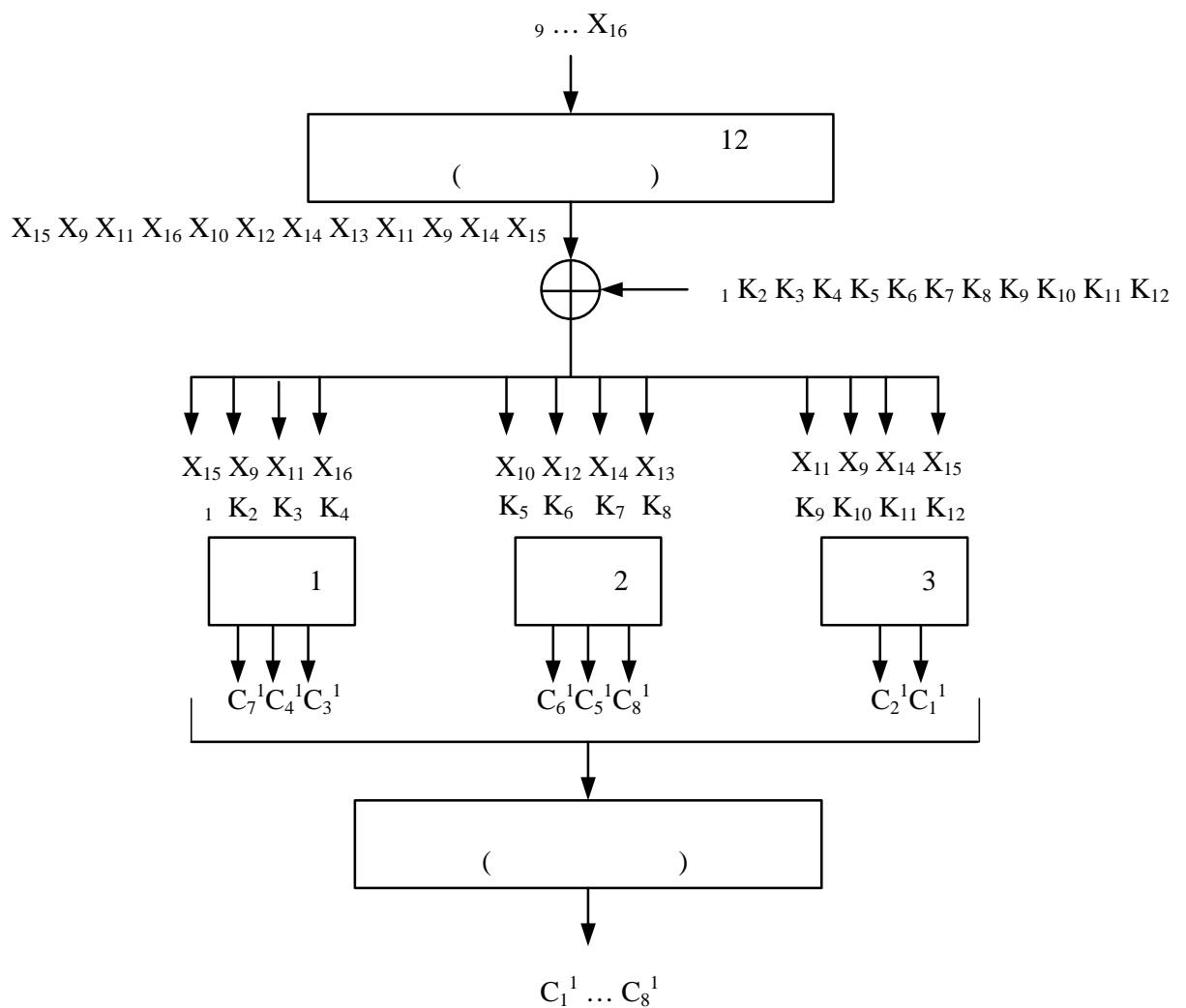
( . . . . . . . .

5).

,

-1

28.



27 -

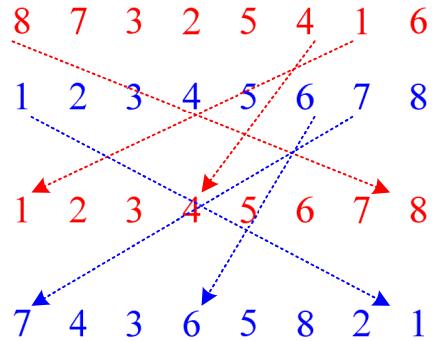
$$\begin{array}{ccccccc}
 & , & & , & & & \\
 & 7^1 & 4^1 & 3^1, & & & \\
 & - & & & & & \\
 8^1, & & & & 2^1 & 1^1. & 
 \end{array}$$

Прямая перестановка Р

Порядок битов

Восстановленный  
порядок битов

Обратная перестановка  $P^{-1}$



28 –

$-1$

,

,

,

$(\alpha, \beta)$ ,

,

$Q=0$ ,

(

).

.

12,

,

$(\alpha, \beta) = (0100, 011)$ ,

$(Q=0) = \frac{1}{8} \cdot$

,

,

$Q$

,

,

$(X \oplus K, \alpha) = (Y, \beta)$ .

,

$(X, \alpha) \oplus (K, \alpha) = (Y, \beta)$ .

$(Y, \beta)$

,

$(Y, \beta) -$

$$(X, \alpha) \oplus (Y, \beta) = (K, \alpha) \quad (11)$$

$$(11) \quad Y = \begin{matrix} & & & \\ & 15 & 9 & 11 & 16 \\ & 1 & 2 & 3 & 4 \\ & 7^1 & 4^1 & 3^1 \end{matrix}, \quad (11):$$

$$X_{15}\alpha_1 \oplus X_9\alpha_2 \oplus X_{11}\alpha_3 \oplus X_{16}\alpha_4 \oplus C_7^1\beta_1 \oplus C_4^1\beta_2 \oplus C_3^1\beta_3 = K_1\alpha_1 \oplus K_2\alpha_2 \oplus K_3\alpha_3 \oplus K_4\alpha_4, \quad (12)$$

$$(12) \quad (\alpha, \beta) = (0100, 011),$$

$$X_{15} \bullet 0 \oplus X_9 \bullet 1 \oplus X_{11} \bullet 0 \oplus X_{16} \bullet 0 \oplus C_7^1 \bullet 0 \oplus C_4^1 \bullet 1 \oplus C_3^1 \bullet 1 = K_1 \bullet 0 \oplus K_2 \bullet 1 \oplus K_3 \bullet 0 \oplus K_4 \bullet 0,$$

$$X_9 \oplus C_4^1 \oplus C_3^1 = K_2, \quad (13)$$

$$(Q=0) = \frac{1}{8}.$$

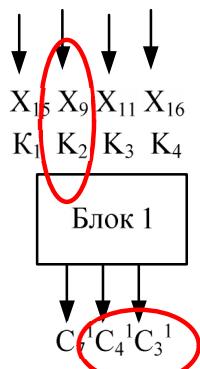
$$1 \quad \alpha \quad . \quad 29( )$$

,

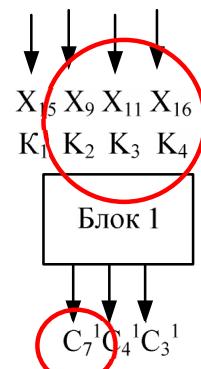
$$( \quad 27),$$

$$(\alpha, \beta) = (0111, 100) ( \quad 29( )).$$

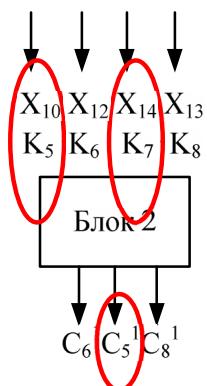
$$X_9 \oplus X_{11} \oplus X_{16} \oplus C_7^1 = K_2 \oplus K_3 \oplus K_4 \quad (14)$$



a)



б)



в)



г)

29 –

(14)

$$12 \quad (Q=0)=1.$$

29

( 29 ( ))

$$X_{10} \oplus X_{14} \oplus C_5^1 = K_5 \oplus K_7, \quad (15)$$

( 29 ( ))

$$X_9 \oplus C_1^1 = K_{10}, \quad (16)$$

(15)

$$13 \quad (Q=0)=0 \quad (16)$$

$$14 - (Q=0)=0.$$

### 3.3 Нахождение эффективных линейных статистических аналогов для трех раундов шифрования

$$(13) - (16)$$

C.

,

,

,

,

.

(13),

$$C_3^1 \quad C_4^1. \quad 25.$$

1

,

,

F

$$, \quad C_3^1 \quad C_4^1$$

$$C_3^1 = _3 \oplus _3, \quad (17)$$

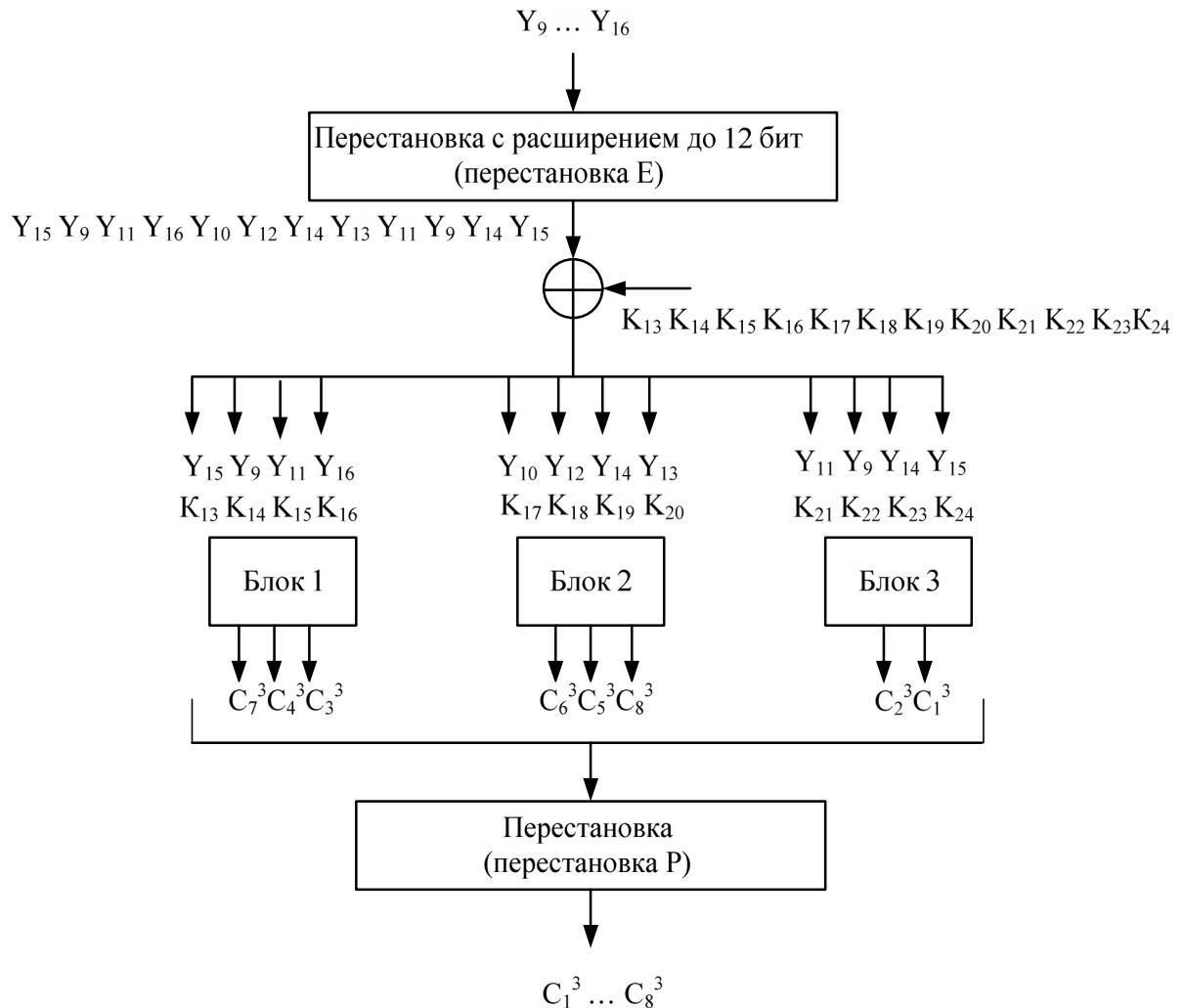
$$C_4^1 = _4 \oplus _4. \quad (18)$$

$$(\alpha, ) = (0100,$$

011), (13).

F

(30).



30 –

F

Y,

Y<sub>9</sub> ... Y<sub>16</sub>.

12

$$( \dots \quad 4), \quad {}_{13} \dots {}_{24}.$$

$$, \quad \quad \quad 4$$

$$\quad \quad \quad . \quad \quad \quad 30$$

F

.

, , ,

$$25. \quad , \quad F$$

$$8- \quad \quad \quad {}^3. \quad \quad \quad {}^3. \quad \quad \quad {}^3. \quad \quad \quad {}^3.$$

, , ,

.

$$, \quad (\alpha, \beta) = (0100, 011);$$

$$Y_9 \oplus C_4^3 \oplus C_3^3 = K_{14}, \quad (19)$$

$$(Q=0) = \frac{1}{8}.$$

$$(19) \quad C_3^3 \quad C_4^3.$$

$$25. \quad , \quad {}^3. \quad \quad \quad ,$$

$$Y, \quad ,$$

F

$$, \quad C_3^3 \quad C_4^3$$

$$C_3^3 = Y_3 \oplus \quad _3, \quad (20)$$

$$C_4^3 = Y_4 \oplus \quad _4. \quad (21)$$

$$(13) \quad (19):$$

$$X_9 \oplus C_4^1 \oplus C_3^1 \oplus Y_9 \oplus C_4^3 \oplus C_3^3 = K_2 \oplus K_{14}. \quad (22)$$

$$(22) \quad (17), (18), (20), (21). \quad :$$

$$X_9 \oplus X_4 \oplus B_4 \oplus X_3 \oplus B_3 \oplus Y_9 \oplus Y_4 \oplus B_4 \oplus Y_3 \oplus B_3 = K_2 \oplus K_{14};$$

$$X_9 \oplus X_4 \oplus X_3 \oplus Y_9 \oplus Y_4 \oplus Y_3 = K_2 \oplus K_{14} \quad (23)$$

,

F

$$, \quad (23),$$

$$2 \quad 14.$$

$$, \quad (23) \quad Q$$

Q<sub>1</sub>

$$Q_2. \quad , \quad Q_1$$

$$, \quad _1 = (Q_1=0). \quad ,$$

$$Q_2 \quad , \quad _2 = (Q_2=0). \quad ,$$

$$, \quad Q_1 \quad , \quad : \quad$$

$$_3 = (Q_1=1) = 1 - (Q_1=0) = 1 - _1.$$

$$, \quad Q_2 \quad ,$$

:

$$_4 = (Q_2=1) = 1 - (Q_2=0) = 1 - _2.$$

$$Q_3 = Q_1 \oplus Q_2.$$

$$, \quad Q_3 = 0. \quad Q_3$$

$$\begin{array}{ccccc} & \vdots & Q_1 & Q_2 & \\ Q_1 & Q_2 & \cdot & , & \vdots \end{array},$$

$$\begin{aligned} p(Q_3 = 0) &= (Q_1=0)^* (Q_2=0) + (Q_1=1)^* (Q_2=1) = {}_1 \cdot {}_2 + {}_3 \cdot {}_4 = \\ &= {}_1 \cdot {}_2 + (1 - {}_1)(1 - {}_2) = {}_1 \cdot {}_2 + 1 - {}_1 \cdot {}_2 + {}_1 \cdot {}_2 = 1 - {}_1 \cdot {}_2 + 2 \cdot {}_1 \cdot {}_2 \end{aligned} \quad (24)$$

$$\begin{array}{ccccc} & Q_1 & Q_2 & & \\ & \vdots & & & \\ {}_1 & = & {}_2 & = & , \end{array} \quad (24) \quad \vdots$$

$$p(Q_3 = 0) = 1 - 2 \cdot + 2 \cdot^2. \quad (25)$$

(23)

$$= \frac{1}{8}. \quad ,$$

$$(25), \quad Q$$

(23):

$$p = 1 - 2p + 2p^2 = 1 - 2 \frac{1}{8} + 2 \left( \frac{1}{8} \right)^2 = 1 - \frac{1}{4} + 2 \frac{1}{64} = \frac{25}{32}.$$

,

$$(\alpha, \beta) = (0100, 011).$$

F

(31).

F

8

$$\vdots \quad 1 \quad \dots \quad 8.$$

,

12

( . . . 4),

7

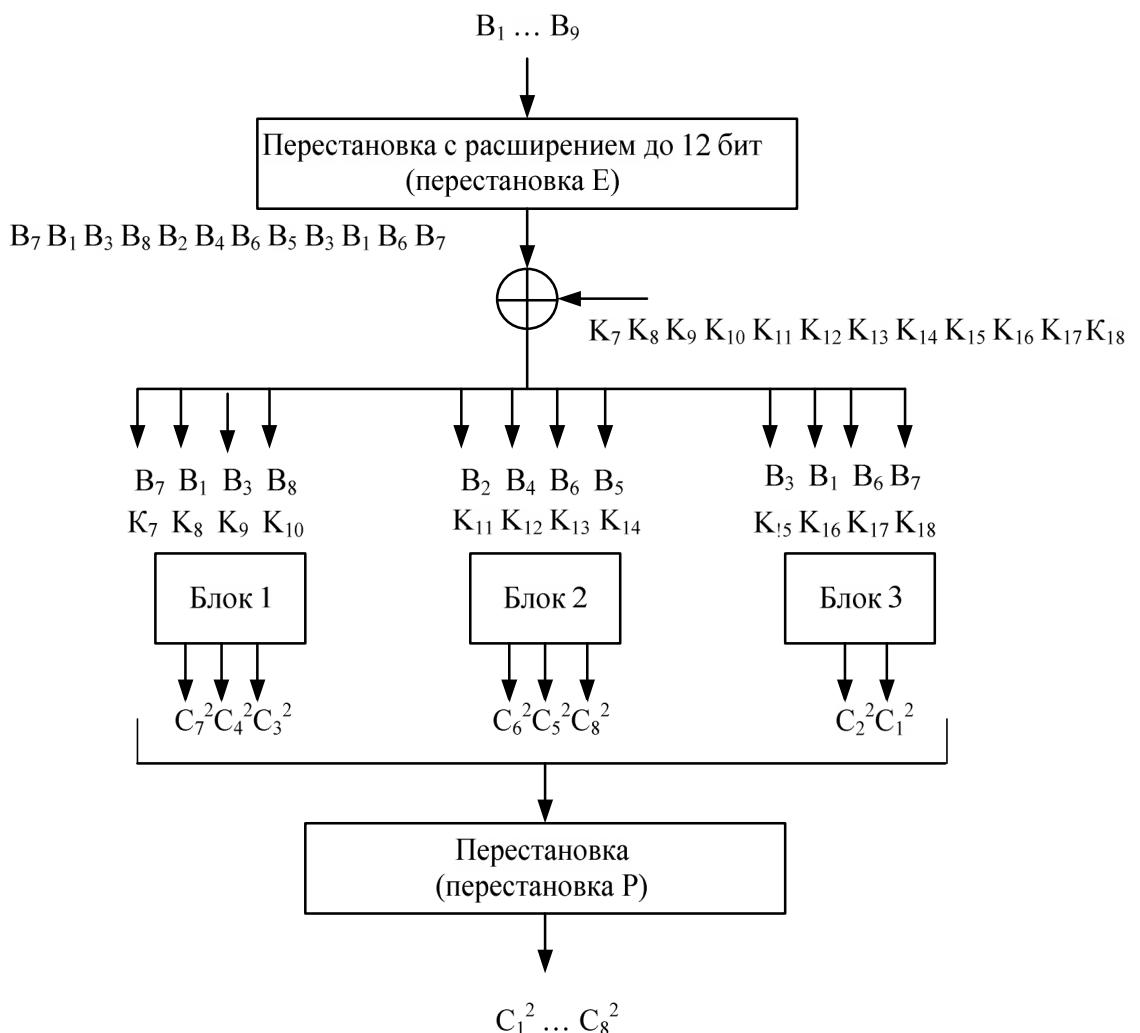
18.

,

4

31

F



31 -

,

,

25.

,

F

$$8 \cdot \overset{2}{\dots} \quad \overset{2}{\dots} \quad \overset{2}{\dots} \quad \overset{2}{\dots} \quad \overset{2}{\dots}$$

$$\cdot \quad , \quad \cdot \quad , \quad \cdot$$

$$, \quad (\alpha, \beta) = (0100, 011):$$

$$B_1 \oplus C_4^2 \oplus C_3^2 = K_8, \quad (26)$$

$$(Q=0) = \frac{1}{8}.$$

$$(26)$$

$$25$$

$$2$$

$$,$$

$$Y.$$

$$\cdot \quad \cdot \quad \cdot \quad ,$$

$$,$$

$$_{11} \cdot \quad , \quad C_3^2 \quad C_4^2$$

$$C_3^2 = Y_{11} \oplus Y_{11}, \quad (27)$$

$$C_4^2 = Y_{12} \oplus Y_{12}. \quad (28)$$

$$1 \cdot$$

$$F \quad \quad \quad 1, \quad \quad \quad$$

$$1 = Y_1 \oplus Y_1^1. \quad (28)$$

$$(26),$$

$$(28), \quad : \quad$$

$$X_1 \oplus C_1^1 \oplus C_4^2 \oplus C_3^2 = K_8, \quad (29)$$

$$_{(29)}$$

$$_1^1$$

$$_{1^1}.$$

$$,$$

$$_1^1$$

$$= 01.$$

$$(14), \quad , \quad \alpha = 0100,$$

$$= 01 \quad \quad \quad Q$$

$$, \quad \frac{1}{2}.$$

$$(16)$$

$$(Q=0)=0. \quad \quad \quad (16) \quad (29),$$

$$:$$

$$X_1 \oplus X_9 \oplus C_4^2 \oplus C_3^2 = K_8 \oplus K_{10}. \quad (30)$$

$$(30) \quad (27) \quad (28),$$

$$X_1 \oplus X_9 \oplus X_{12} \oplus Y_{12} \oplus X_{11} \oplus Y_{11} = K_8 \oplus K_{10}. \quad (31)$$

$$(31)$$

$$, \quad Q = 0, \quad . \quad \quad \quad (16) \quad ,$$

$$= 0, \quad (29) \quad \quad \quad _2 = \frac{1}{8}.$$

$$(31) \quad (24):$$

$$p(Q_3 = 0) = 1 - _1 - _2 + 2 _1 _2 = 1 - 0 - \frac{1}{8} + 2 * 0 * \frac{1}{8} = \frac{7}{8}.$$

Y

$$F \subset C^3.$$

,

,

.

,

,

,

.

### 3.4 Определение битов ключа с помощью эффективных линейных статистических аналогов

$$, Q = 0.$$

$$Y_i -$$

,

:

$$X_i \oplus Y_j = K_m. \quad (32)$$

$$(32) , Q = 0 \quad ( >$$

$$\frac{1}{2}), , \quad (32)$$

.

$$Q = X_i \oplus Y_j \oplus K_m, , \quad Q$$

$$, X_i \oplus Y_j$$

$$K_m.$$

$$(32) \quad , \quad Q = 0 \quad ($$

$$< \frac{1}{2}), \quad , \quad (32)$$

$$X_i \oplus Y_j - K_m. \quad (33)$$

$$, \quad Q = X_i \oplus Y_j \oplus K_m, \quad , \\ Q \\ X_i \oplus Y_j \quad K_m.$$

$$N \quad : \quad -$$

$$Y, \\ N, \quad ,$$

$$- Y \\ (32). \quad ,$$

$$, \quad T < N/2, \quad X_i \oplus Y_j \\ : X_i \oplus Y_j = 1. \quad , \\ , \quad T > N/2, \quad X_i \oplus Y_j \\ : X_i \oplus Y_j = 0.$$

$$T < \frac{N}{2}, \quad X_i \oplus Y_j = 1. \quad : \\$$

$$> \frac{1}{2}, \quad X_i \oplus Y_j = K_m, \quad K_m = 1;$$

$$< \frac{1}{2}, \quad X_i \oplus Y_j = K_m, \quad K_m = 0.$$

$$T > \frac{N}{2}, \quad X_i \oplus Y_j = 0. \quad : \\$$

$$> \frac{1}{2}, \quad X_i \oplus Y_j = K_m, \quad K_m = 0;$$

$$< \frac{1}{2}, \quad X_i \oplus Y_j = K_m, \quad K_m = 1.$$

.

### 3.5 Контрольные вопросы

1. ?
2. ?
3. ?
4. , ?
5. ?
6. , ?
7. ?
8. 3- ?

9.

,

?

10.

?

11.

?

12. ,

?

## **Лабораторная работа №1.**

### **Изучение метода дифференциального криптоанализа блочных шифров**

#### **Цель работы**

#### **Подготовка к работе**

1.

Crypto1\_1.exe

( $\Delta_x$ ,  $\Delta_y$ ,  $\Delta_z$ ,  $\Delta_w$ ,  $\Delta_{\text{key}}$ ).

:

1.

2.

$(\Delta_x, \Delta_y)$ .

3.

4.

$(\Delta_x, \Delta Y)$

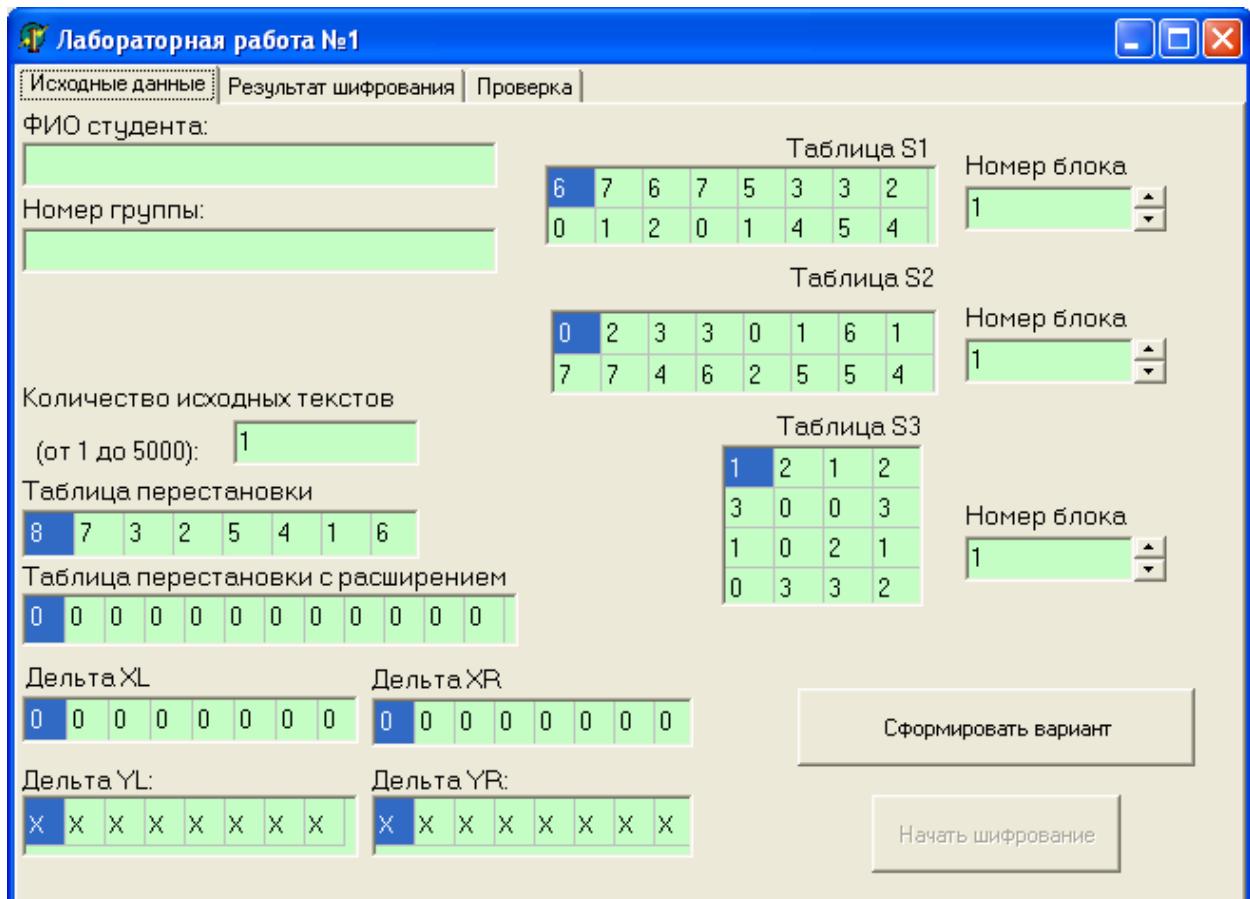
## Методические указания по выполнению лабораторной работы

Cryptol\_1.exe.

Cryptol\_1.exe

,

32.



32 –

«

»

,

«

» «

». !!!ВНИМАНИЕ!!!

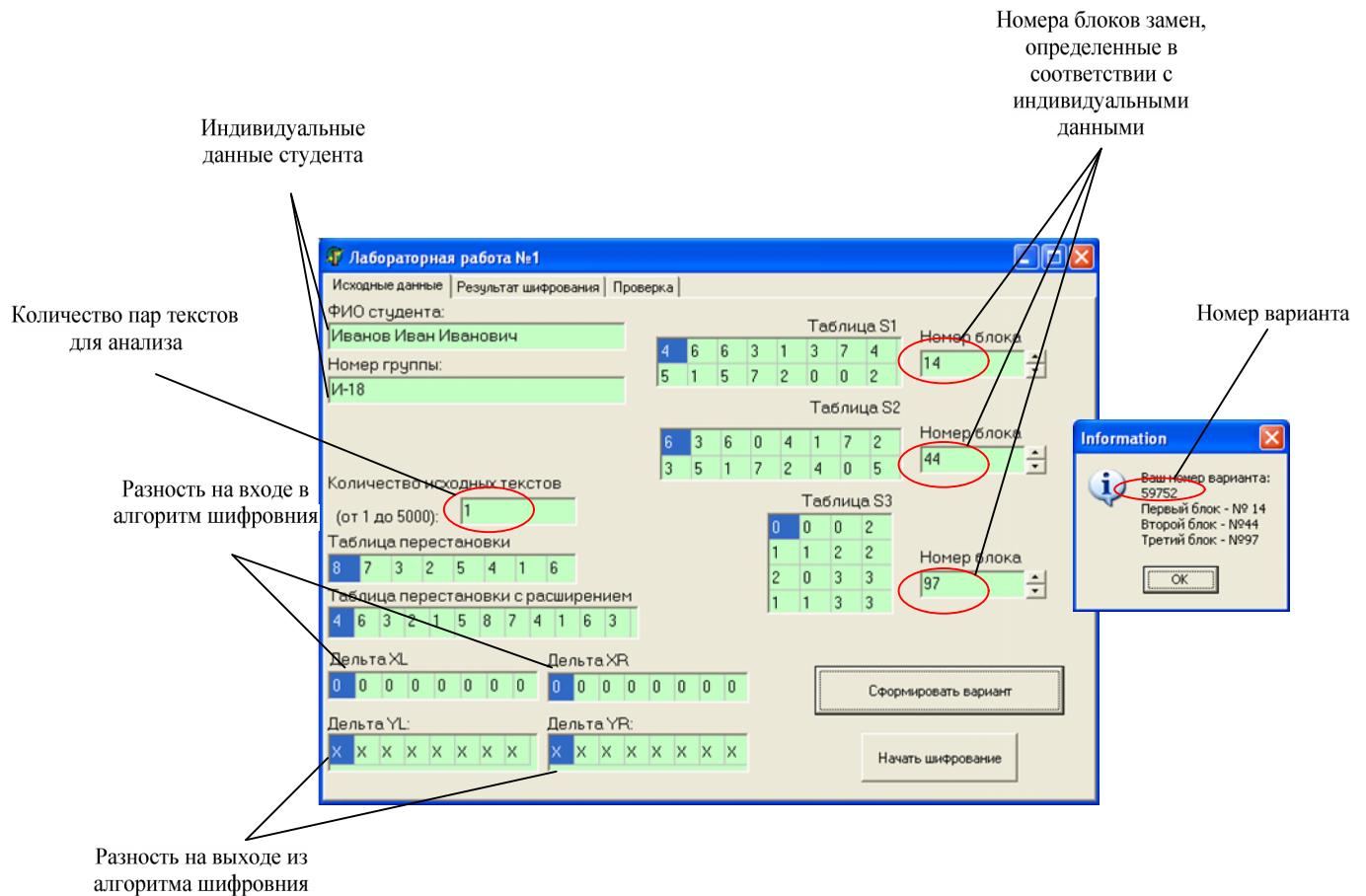
,

(

)

,

33.



33 –

33

-18

59752,

,

14, 44 97

.

( 32

).

,

,

, ,  
.  
,  
«  
» ,  
,  
,  
( « XL» « XR »),  
( « YL» « YR »).

,

“x”. **!!!ВНИМАНИЕ!!!**

, Crypto1\_1.exe

,  
.  
(  
XL, XR),  
( YL, YR),  
,

34.

« »

,  
,  
« »  
( . 35),

**Лабораторная работа №1**

Исходные данные | Результат шифрования | Проверка |

XL	XR	YL	YR
10101110	01000110	01001100	11000001
00110001	00111000	10010011	10111111
10011111	01111110	11011111	01111110
00011111	11000001	10100000	01101000
10000000	10111111	00001101	00010110
10011111	01111110	10101101	01111110
01111011	10100101	00011010	11111100
11100100	11011011	11000101	10000010
10011111	01111110	11011111	01111110

Сохранить в файл

34 –

,

**Лабораторная работа №1**

Исходные данные | Результат шифрования | Проверка |

Искомый ключ

K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12	K13	K14	K15	K16	K17	K18	K19	K20	K21	K22	K23	K24
0	1	0	0	1	0	1	1	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0

**Information**



Лабораторная работа №1  
Иванов Иван Иванович  
Группа И-18  
Биты ключа найдены верно!

**OK**

35 –

**Рекомендуется следующий порядок работы:**

1.   Crypto1\_1.exe.
2.   ,
3.   ,
- «  ».
4.   .
5.   ,
- (                           XL,                   XR,                   YL,                   YR).
6.   «  
    »,  
  ,
7.   «                                »,  
   .
8.   ,
9.   ,  
    (   )  
   5 – 8.
10.   (  
   ,  
  ).

**Отчет по лабораторной работе должен содержать:**

- 1.
2.   .
- 3.
- ,
- ( $\Delta$  ,  $\Delta$  ).

4.

,

5.

6.

7.

### Пример выполнения лабораторной работы

18. , 59752.

,  
15 – 17,

– 18.

15

1

a2a3a4	000	001	010	011	100	101	110	111
a1								
0	4	6	6	3	1	3	7	4
1	5	1	5	7	2	0	0	2

16

2

<b>a2a3a4</b>	<b>000</b>	<b>001</b>	<b>010</b>	<b>011</b>	<b>100</b>	<b>101</b>	<b>110</b>	<b>111</b>
<b>a1</b>								
<b>0</b>	6	3	6	0	4	1	7	2
<b>1</b>	3	5	1	7	2	4	0	5

17

3

<b>a2a3</b>	<b>00</b>	<b>01</b>	<b>10</b>	<b>11</b>
<b>a1 a4</b>				
<b>00</b>	0	0	0	2
<b>01</b>	1	1	2	2
<b>10</b>	2	0	3	3
<b>11</b>	1	1	3	3

18

4	6	3	2	1	5	8	7	4	1	6	3
---	---	---	---	---	---	---	---	---	---	---	---

,

15.

15

,

,

.

19.

0000	100
0001	110
0010	110
0011	011
0100	001
0101	011
0110	111
0111	100
1000	101
1001	001
1010	101
1011	111
1100	010
1101	000
1110	000
1111	010

, 15 19 ,

19,

15, ,  
 $\Delta \cap \{12\},$ ,  
 $-\Delta \cap \{8\}.$

$\Delta$

$$\begin{aligned}
 & \Delta_m, \quad \Delta_m, \quad m - \\
 & (\quad \quad \quad \quad \quad \quad 22). \\
 & , \quad \quad \quad \quad \quad \quad \Delta_1, \\
 & 4 \quad , \quad \quad \quad \quad \quad \quad 2^4 = 16 \quad \quad \quad \Delta_1 \\
 & (0000 \quad 1111). \quad \quad \quad \quad \quad \quad 16 \\
 & . \quad , \quad \quad \quad \quad \quad \quad 20 \quad \quad \quad \quad \quad \quad 16 \\
 & \Delta_1 = 0010.
 \end{aligned}$$

20

1	2	$\Delta_1$
0000	0010	$0000 \oplus 0010 = 0010$
0001	0011	$0001 \oplus 0011 = 0010$
0010	0000	$0010 \oplus 0000 = 0010$
0011	0001	$0011 \oplus 0001 = 0010$
0100	0110	$0100 \oplus 0110 = 0010$
0101	0111	$0101 \oplus 0111 = 0010$
0110	0100	$0110 \oplus 0100 = 0010$
0111	0101	$0111 \oplus 0101 = 0010$
1000	1010	$1000 \oplus 1010 = 0010$
1001	1011	$1001 \oplus 1011 = 0010$
1010	1000	$1010 \oplus 1000 = 0010$
1011	1001	$1011 \oplus 1001 = 0010$
1100	1110	$1100 \oplus 1110 = 0010$
1101	1111	$1101 \oplus 1111 = 0010$
1110	1100	$1110 \oplus 1100 = 0010$
1111	1101	$1111 \oplus 1101 = 0010$

19,

,

20

$\Delta_1 : 0000 \quad 0010.$

19, , 0000

100, 0010 – 110.

$$\Delta_{-1} = 100 \oplus 110 = 010.$$

$$\Delta_{-1} = 0010 \quad ,$$

$$21.$$

21

$$\Delta_{-1}$$

$$\Delta_{-1}$$

1	2	1	2	$\Delta_{-1}$
0000	0010	010	110	$100 \oplus 110 = 010$
0001	0011	110	011	$110 \oplus 011 = 101$
0010	0000	110	100	$110 \oplus 100 = 010$
0011	0001	011	110	$011 \oplus 110 = 101$
0100	0110	001	111	$001 \oplus 111 = 110$
0101	0111	011	100	$011 \oplus 100 = 111$
0110	0100	111	001	$111 \oplus 001 = 110$
0111	0101	100	011	$100 \oplus 011 = 111$
1000	1010	101	101	$101 \oplus 101 = 000$
1001	1011	001	111	$001 \oplus 111 = 110$
1010	1000	101	101	$101 \oplus 101 = 000$
1011	1001	111	001	$111 \oplus 001 = 110$
1100	1110	010	000	$010 \oplus 000 = 010$
1101	1111	000	010	$000 \oplus 010 = 010$
1110	1100	000	010	$000 \oplus 010 = 010$
1111	1101	010	000	$010 \oplus 000 = 010$

$$21 \quad ,$$

$$\Delta_{-1} = 0010,$$

$$\Delta_{-1} = 010,$$

$$- \quad \Delta_{-1} = 110,$$

$$- \quad \Delta_{-1} = 101, \Delta_{-1} =$$

$$000 \quad \Delta_{-1} = 111.$$

$$\Delta_{-1} (001, 011, 100)$$

**никогда**

!

$$\Delta_{-1}.$$

$$22,$$

$$\Delta_{-1},$$

$$\Delta_{-1}.$$

$\Delta_1$	000	001	010	011	100	101	110	111
$\Delta_1$								
0000	16	0	0	0	0	0	0	0
0001	0	0	10	2	2	2	0	0
0010	2	0	6	0	0	2	4	2
0011	6	0	2	0	4	2	0	2
0100	0	4	0	0	0	8	0	4
0101	0	0	2	2	2	2	0	8
0110	2	0	2	4	0	2	0	6
0111	2	4	2	0	0	6	0	2
1000	0	2	0	6	2	0	2	4
1001	0	6	0	2	2	4	2	0
1010	0	8	2	2	2	2	0	0
1011	0	0	0	8	0	0	4	4
1100	0	2	4	2	2	0	6	0
1101	4	2	0	2	6	0	2	0
1110	0	0	2	2	10	2	0	0
1111	0	4	0	0	0	0	12	0

21

22.

,

,

,

.

1.

2<sup>n</sup>,

n -

,

;

2<sup>d</sup>, d -

.

2.

$$\Delta_m = 0000$$

$$\Delta_m = 0000 \text{ (}$$

. . 2.1).

3.

$$2^n, \quad n -$$

,

4.

,

( .

21).

$$(\Delta_1, \Delta_1)$$

,

$$, \quad 16.$$

22

,

23.

23

$$(\Delta_1 = 1111, \Delta_1 = 110). \quad \Delta_1 = 0000,$$

$$= 1$$

$$\Delta_1 = 000$$

,

.

.

23

$\Delta_1$	000	001	010	011	100	101	110	111
$\Delta_1$								
0000	1	0	0	0	0	0	0	0
0001	0	0	5/8	1/8	1/8	1/8	0	0
0010	1/8	0	3/8	0	0	1/8	1/4	1/8
0011	3/8	0	1/8	0	1/4	1/8	0	1/8
0100	0	1/4	0	0	0	1/2	0	1/4
0101	0	0	1/8	1/8	1/8	1/8	0	1/2

0110	1/8	0	1/8	1/4	0	1/8	0	3/8
0111	1/8	1/4	1/8	0	0	3/8	0	1/8
1000	0	1/8	0	3/8	1/8	0	1/8	1/4
1001	0	3/8	0	1/8	1/8	1/4	1/8	0
1010	0	1/2	1/8	1/8	1/8	1/8	0	0
1011	0	0	0	1/2	0	0	1/4	1/4
1100	0	1/8	1/4	1/8	1/8	0	3/8	0
1101	1/4	1/8	0	1/8	3/8	0	1/8	0
1110	0	0	1/8	1/8	5/8	1/8	0	0
1111	0	1/4	0	0	0	0	3/4	0

24,

25

23 24,

24

$\Delta_2$	000	001	010	011	100	101	110	110
$\Delta_2$								
0000	1	0	0	0	0	0	0	0
0001	0	0	0	0	0	1/2	1/2	0
0010	1/8	1/8	3/8	3/8	0	0	0	0
0011	0	0	0	0	3/8	1/8	3/8	1/8
0100	0	1/2	1/2	0	0	0	0	0
0101	0	0	0	0	1/4	0	0	3/4
0110	1/8	3/8	1/8	3/8	0	0	0	0
0111	0	0	0	0	3/8	3/8	1/8	1/8

1000	0	0	0	0	0	1/4	1/4	1/2
1001	1/4	1/4	1/4	1/4	0	0	0	0
1010	0	0	0	0	3/8	3/8	1/8	1/8
1011	1/8	3/8	1/8	3/8	0	0	0	0
1100	0	0	0	0	1/4	1/4	1/4	1/4
1101	1/4	1/4	1/4	1/4	0	0	0	0
1110	0	0	0	0	3/8	1/8	3/8	1/8
1111	1/8	1/8	3/8	3/8	0	0	0	0

25

$\Delta_3$	00	01	10	11
$\Delta_3$				
0000	1	0	0	0
0001	3/8	3/8	1/8	1/8
0010	3/4	0	1/4	0
0011	3/8	3/8	1/8	1/8
0100	1/8	1/8	3/8	3/8
0101	0	1/4	1/2	1/4
0110	1/8	1/8	3/8	3/8
0111	0	1/4	1/2	1/4
1000	3/8	3/8	1/8	1/8
1001	0	3/4	0	1/4
1010	3/8	3/8	1/8	1/8
1011	0	3/4	0	1/4
1100	0	0	1/2	1/2
1101	1/8	1/8	3/8	3/8
1110	1/4	0	1/4	1/2
1111	1/8	1/8	3/8	3/8

,

,

$\Delta = (\Delta_1, \Delta_2, \Delta_3)$ ,  $\Delta =$

– 25 26.

23

26

$\Delta_1$	$\Delta_2$	$\Delta_3$
1111	0101	0010
		1001
		1011

26,

$\Delta = (\Delta_1, \Delta_2, \Delta_3)$ :

111101010010  
111101011001  
111101011011

,

.

,

12

18.

:

,

,

$\Delta =$

111101011011,

36.

,

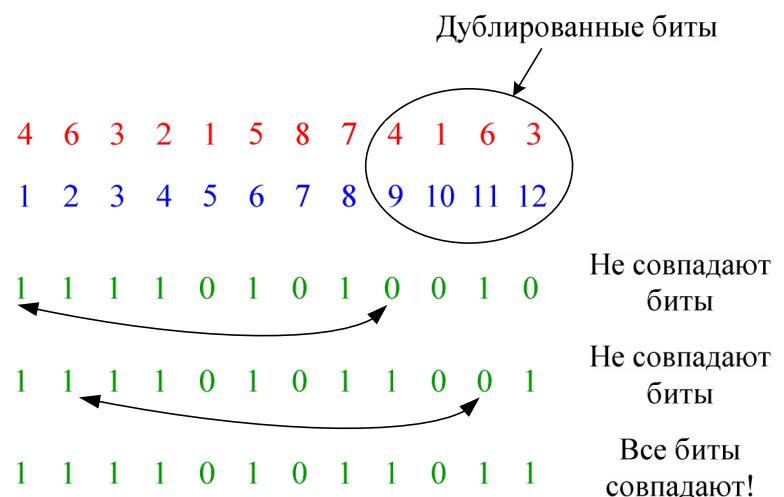
$\Delta$

, , ,

,

:

- Прямая перестановка Е
- Порядок битов
- Первое возможное значение  $\Delta A$
- Второе возможное значение  $\Delta A$
- Третье возможное значение  $\Delta A$



36 –

$\Delta$

$$\Delta = (\Delta_1, \Delta_2, \Delta_3),$$

23 – 25

$$\Delta_1 = 1111$$

$$\Delta_1 = \frac{3}{4}$$

$$\Delta_2 = 110,$$

$$\Delta_2 = \frac{3}{4}$$

$$\Delta_3 = 111$$

$$\Delta_3 = 1011$$

$$\Delta_3 = \frac{3}{4}$$

$$\Delta_3 = 01.$$

$$\Delta_3 =$$

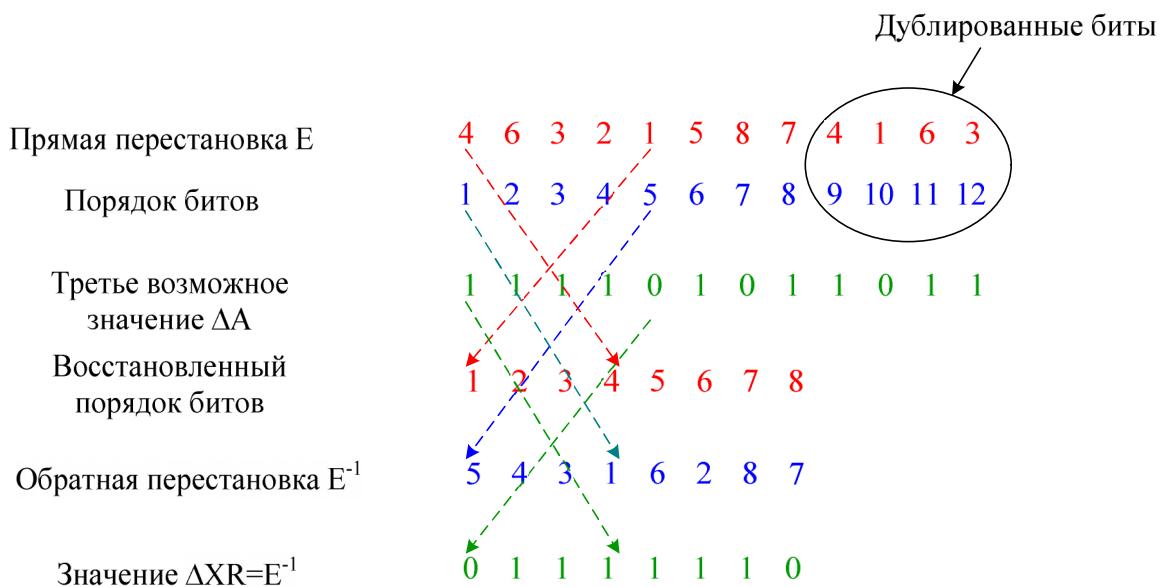
$$(\Delta_1, \Delta_2, \Delta_3) = 11011101.$$

18, ,

, — . .

18,

37.



37 –

$\Delta X R$

37

,

,

,

,

8-

,

12-

-1

.

,

8

12,

37:

$$\Delta = 111101011011$$

$$\Delta X R = 01111110.$$

,

5

$$\Delta = 11011101.$$

F,

$$\Delta D = P(\Delta) =$$

$$10011111.$$

$\Delta$

$\Delta D$

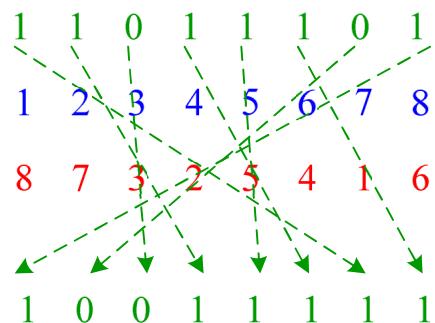
38.

Значение  $\Delta C$

Порядок битов

Прямая перестановка Р

Значение  $P(\Delta C)$



38 –

$\Delta$

$\Delta D$

,

,

,

F

,

,

2

21.

21

39.

39

,

.

,

01111110.

:  $\Delta XL = 10011111$ ,  $\Delta XR =$

,

.

$\Delta YR = 01111110.$

.

.

,

$\Delta XL$ ,  $\Delta XR$ ,  $\Delta YR$

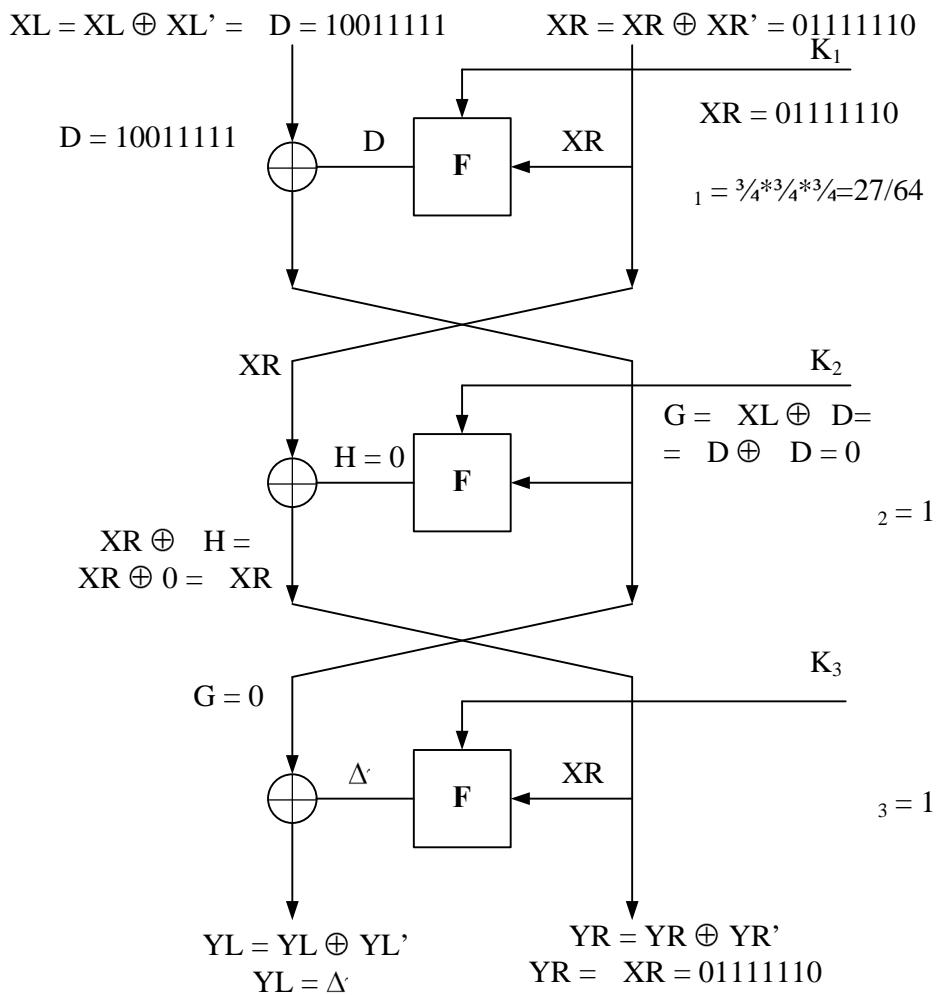
( .

32).

,

«

».



39 –

« »,

X'

( $\Delta XL, \Delta XR$ ), ,

, . ,

$\Delta YR$ ,  $(X, Y) - (X', Y')$

« » ( . 34).

**!!!ВАЖНО!!!**

,

$\Delta XL$ ,  $\Delta XR$

$\Delta YR$ .

**!!!ВАЖНО!!!**

«                           »                           «  
 »                           »  
 .                           ,  
 ,                           save.txt,                   «  
 ».                        save.txt                   ,  
 .                           ,

27.

27

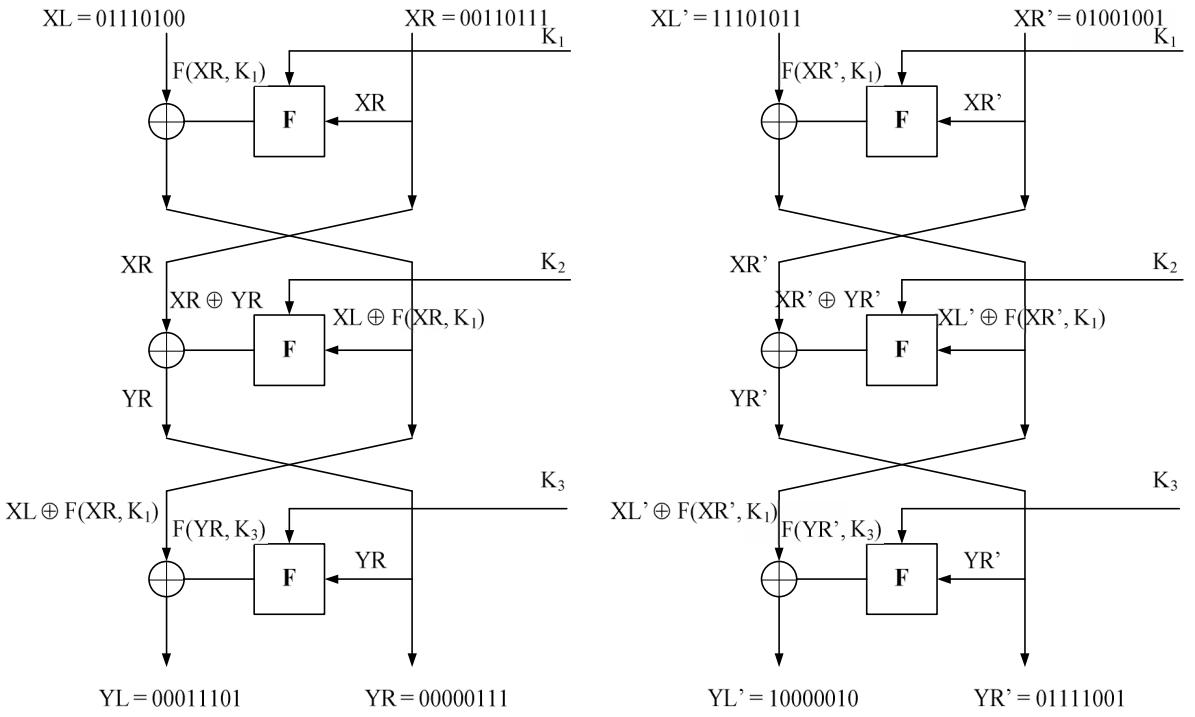
	XL	XR	YL	YR
(X, Y)	01110100	00110111	00011101	00000111
(X', Y')	11101011	01001001	10000010	01111001
	10011111	01111110	10011111	01111110

,

X X'

Y Y'

40.



40 -

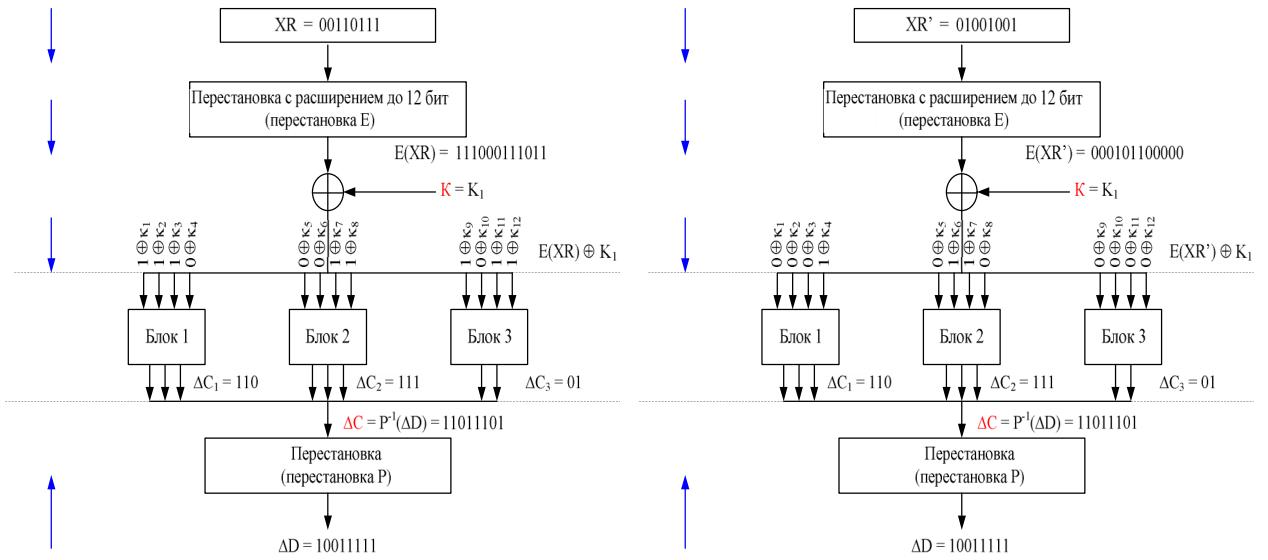
$40$   
 $,$   
 $,$   
 $,$   
 $F$   
 $XR = 00110111,$   
 $XR \quad XR'$   
 $-$   
 $F$   
 $F$   
 $F(XR, K_1) \quad F(XR', K_1)$   
 $.$   
 $,$   
 $,$   
 $($   
 $39),$   
 $,$   
 $F$

$\Delta D = 10011111.$

$F$

$XR \quad XR'.$

41.



41 –

$XR \quad XR'$

$XR \quad XR': \quad (XR) = 111000111011 \quad (XR') = 000101100000.$

$(XR) \quad (XR')$

$\Delta D = 10011111.$

$\Delta D^{-1},$

41,

$1110 \oplus K_1^1 \quad 0001 \oplus K_1^1.$

$\Delta_{-1} = 110.$ ,  
 $\Delta_{-1} = 1111 ($ .  
 $\Delta_{-1} = 1111$   
 $\Delta_{-1} ($ .  
 $28).$ ,  
 $\Delta_{-1} = 110.$ ,  
 $\Delta_{-1} = 1111$   
 $\Delta_{-1} ($ .  
 $36).$

28

$\Delta_{-1} = 1111$

1	2	1	2	$\Delta_{-1}$
0000	1111	100	010	110
0001	1110	110	000	110
0010	1101	110	000	110
0011	1100	011	010	001
0100	1011	001	111	110
0101	1010	011	101	110
0110	1001	111	001	110
0111	1000	100	101	001
1000	0111	101	100	001
1001	0110	001	111	110
1010	0101	101	011	110
1011	0100	111	001	110
1100	0011	010	011	001
1101	0010	000	110	110
1110	0001	000	110	110
1111	0000	010	100	110

,

$K_1^1:$

$$1110 \oplus K_1^1 = 1$$

$$0001 \oplus K_1^1 = 2$$

, 12  $K_1^1$ :  
 1110, 1111, 1100, 1010, 1011, 1000, 0111, 0100, 0101, 0011, 0000, 0001.

$K_1^1$ . ,  
 $K_1^2$ :  
 $K_1^3$ . ,  
 29,

29

	$K_1^1$	$K_1^2$	$K_1^3$
0000	6	4	3
0001	5	4	3
0010	4	5	7
0011	1	5	4
0100	7	5	4
0101	6	5	7
0110	5	4	3
0111	3	3	3
1000	2	2	4
1001	5	2	7
1010	5	5	3
1011	7	7	3
1100	2	3	3
1101	3	3	3
1110	5	5	7
1111	5	4	4

29

$K_1^1$

: 0100 1011,

$K_1^2$

1011, ,

,

$K_1^3$

: 0010, 0101, 1001 1110.

,

:

010010110010

010010110101

010010111001

010010111110

10110110010

10110110101

10110111001

10110111110

,

12

.

( . 4),

12

$K_3$ .

,

40

,

F

YR YR'.

F

,

39,

$\Delta$

YL.

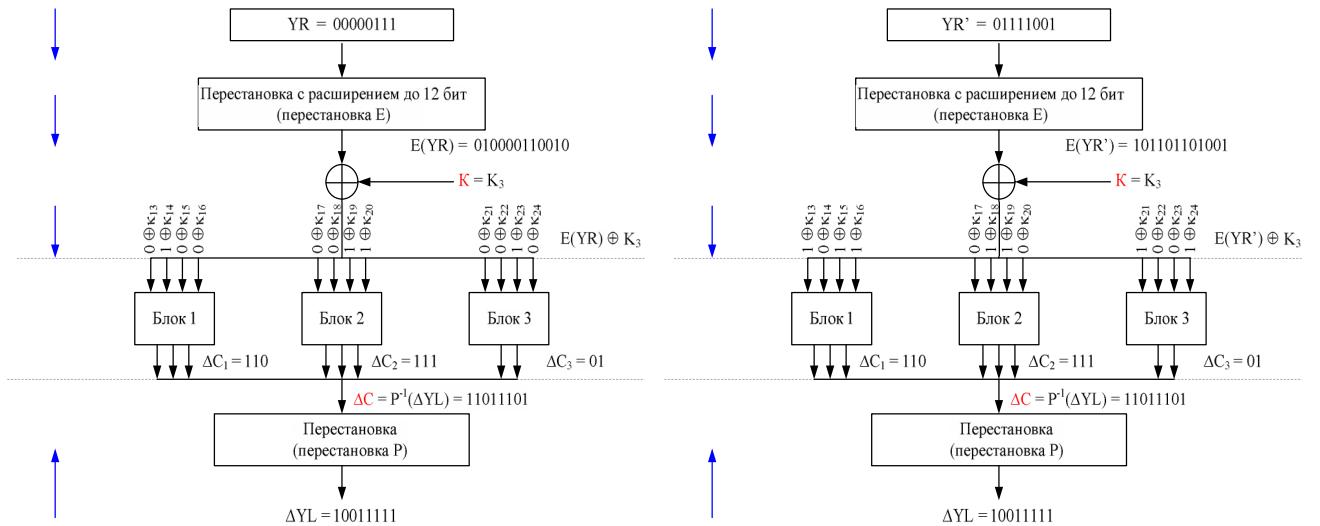
,

42

,

41.

,



42 –

$YR - YR'$

,  
30,

30

	$K_3^1$	$K_3^2$	$K_3^3$
0000	5	7	7
0001	3	5	4
0010	2	1	4
0011	1	2	4

0100	7	3	2
0101	3	4	5
0110	4	3	4
0111	1	1	7
1000	1	7	3
1001	3	5	4
1010	4	3	3
1011	5	5	7
1100	1	3	7
1101	2	5	4
1110	3	4	4
1111	5	3	3

30  $K_3^1$

0100,  $K_3^2$

: 0000 1000, , ,

,  $K_3^3$

: 0000, 0111, 1011 1100. ,

:

010000000000

010000000111

010000001011

010000001100

010010000000

010010000111

010010001011

010010001100

, 64

. , , , , .

, , , .

64

,

$2^{24}$

35.

### **Контрольные вопросы**

1.

2.

?

3.

$(\Delta_+, \Delta_-)$ .

4.

?

5.

?

## **Лабораторная работа №2.**

### **Изучение метода линейного криптоанализа блочных шифров**

#### **Цель работы**

.

—

,

#### **Подготовка к работе**

1.

,

.

Crypto2\_1.exe

( , , , , ).

:

1.

( $\alpha$ , ),

2.

( $\alpha$ , ), ( )

, Q .

3.

15

4.

Q .

,

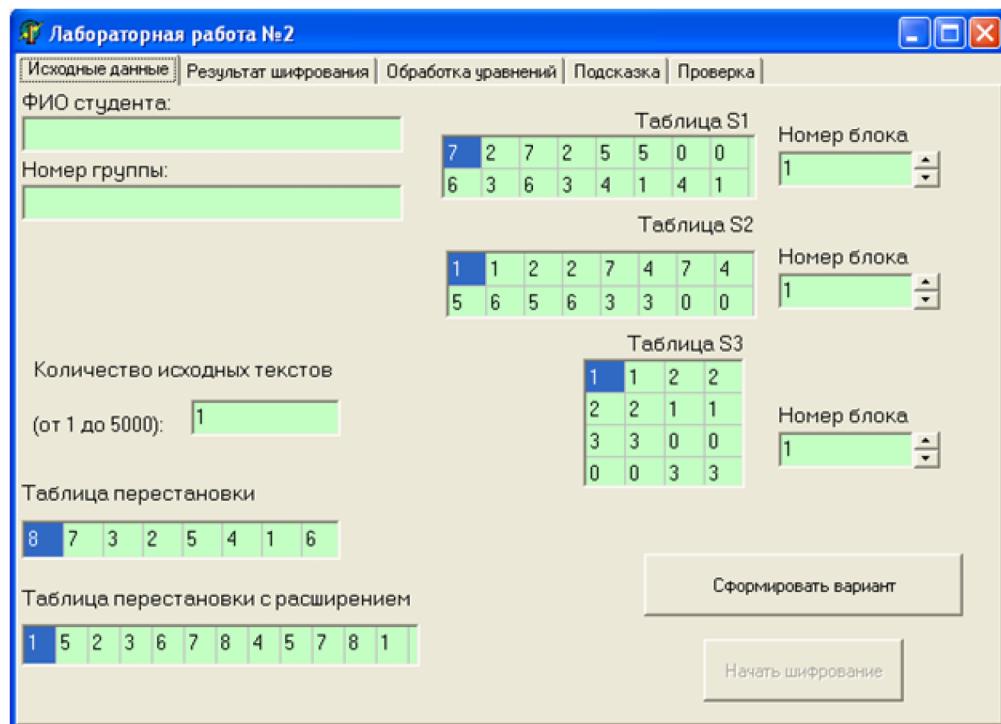
## Методические указания по выполнению лабораторной работы

Crypto2\_1.exe.

Crypto2\_1.exe

,

43.



43 –

«

»

,

«

» «

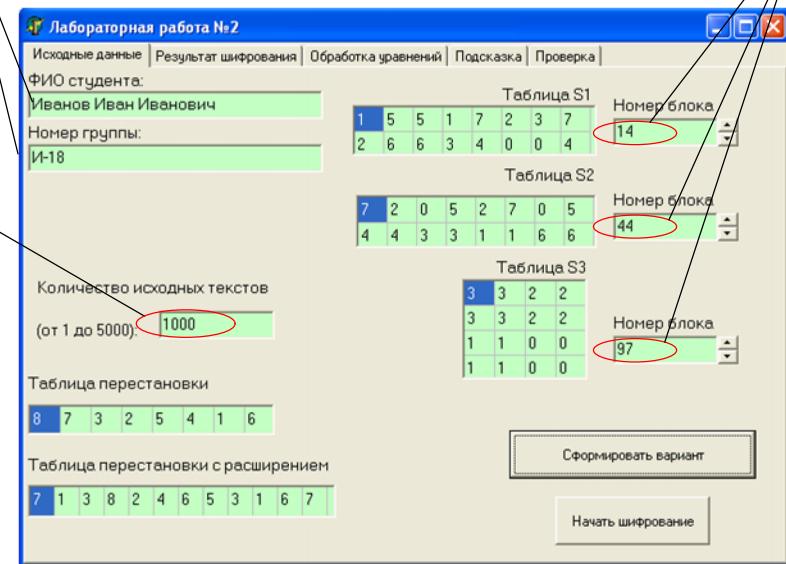
». !!!ВНИМАНИЕ!!!

,

(

)

44.



44 –

44

-18 , 59752,  
, 14, 44 97 .

Crypto2\_1.exe

45.

Save.txt,

XL	XR	YL	YR
10001010	11110000	11101100	01110010
00101001	11001111	10010010	11100001
00010100	01011000	01000000	11000001
11100100	10011000	10000100	01010111
11101101	10110011	10010000	01110010
10100111	01001001	00001100	01100101
10111101	00111111	00101011	00011101
00100101	10101000	10101010	11001000
01111110	00101011	00010101	10100101
10111000	00111011	00000001	00011100
01001100	00101111	01101001	11011001
01101111	01101110	00110001	11111010

45 –

»,  
« »,  
Y,

«

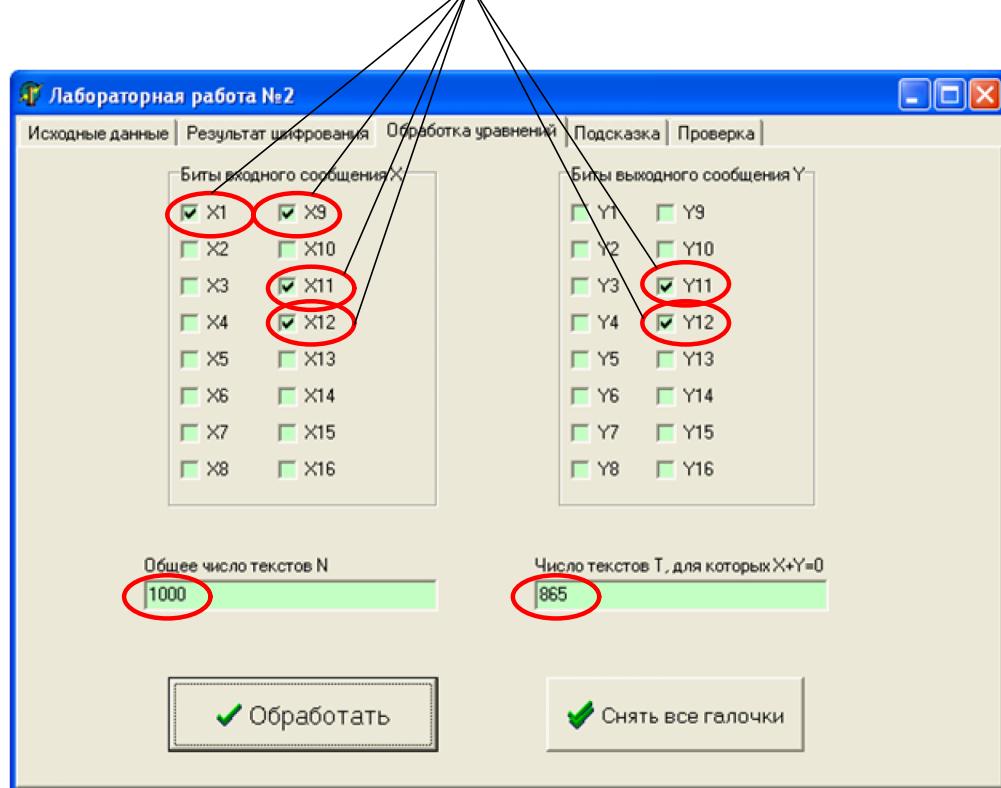
Y» ( . . 46).

, « ».

, ,

, ,

. . 3.4.



46 –

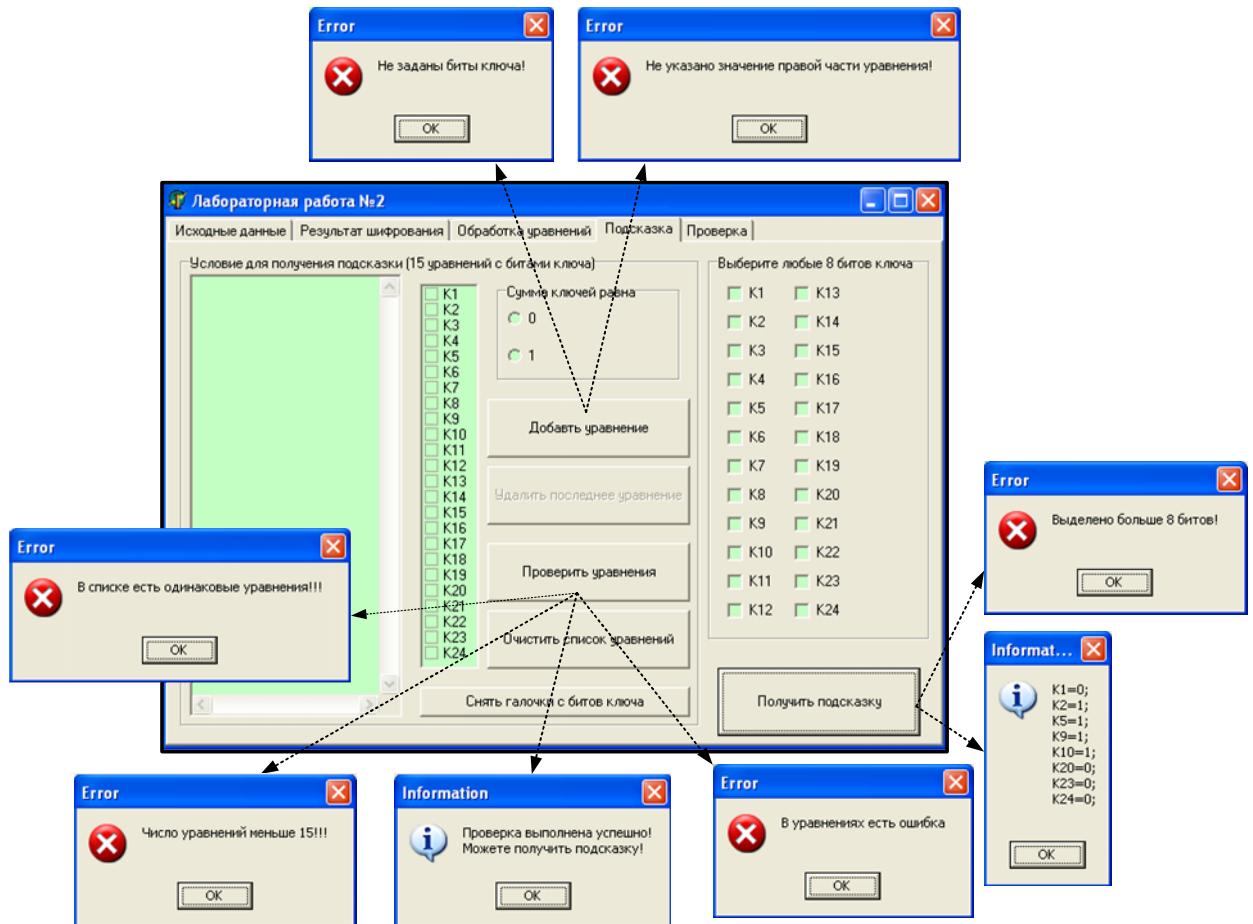
15

(

15

).

123



«».

— ; — ,

— ,

, «».

, «».

, «».

— ,

, «».

:

— 15;

— ; — ,

— 15 ,

, ,

48,

, ,

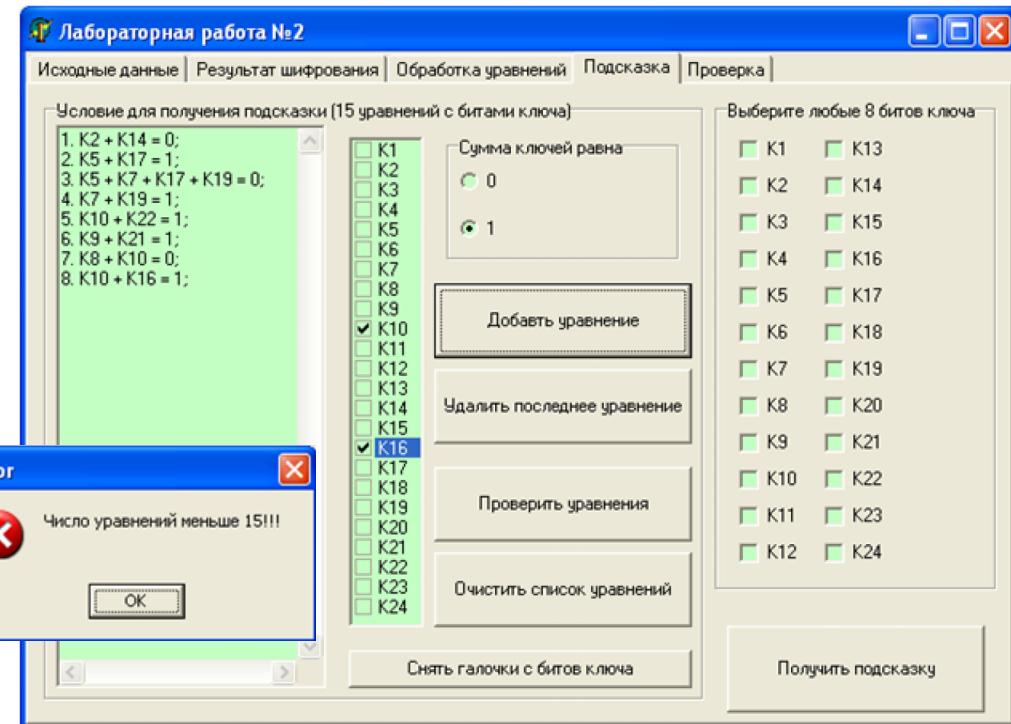
, ,

49 ,

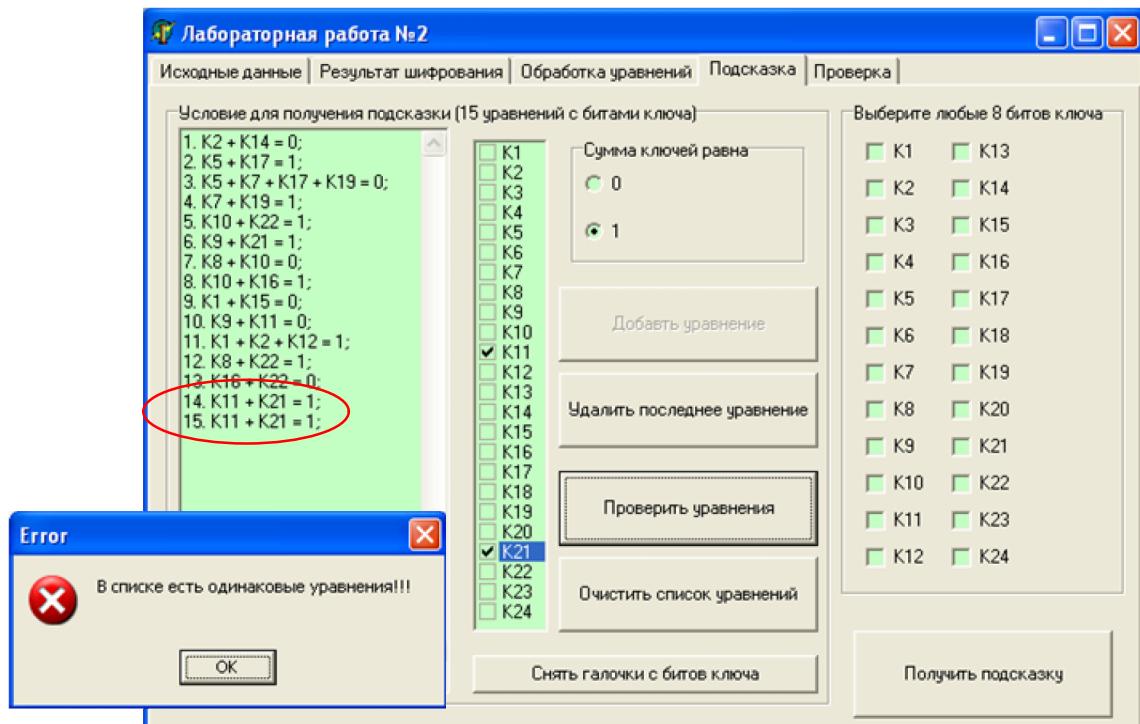
,

,

,



48 –



49 –

«

»

,

,

,

:

;

;

—

«

».

,

,

«

»

,

,

«

».

«

»

,

«

8

».

15

,

,

,

«

»

«

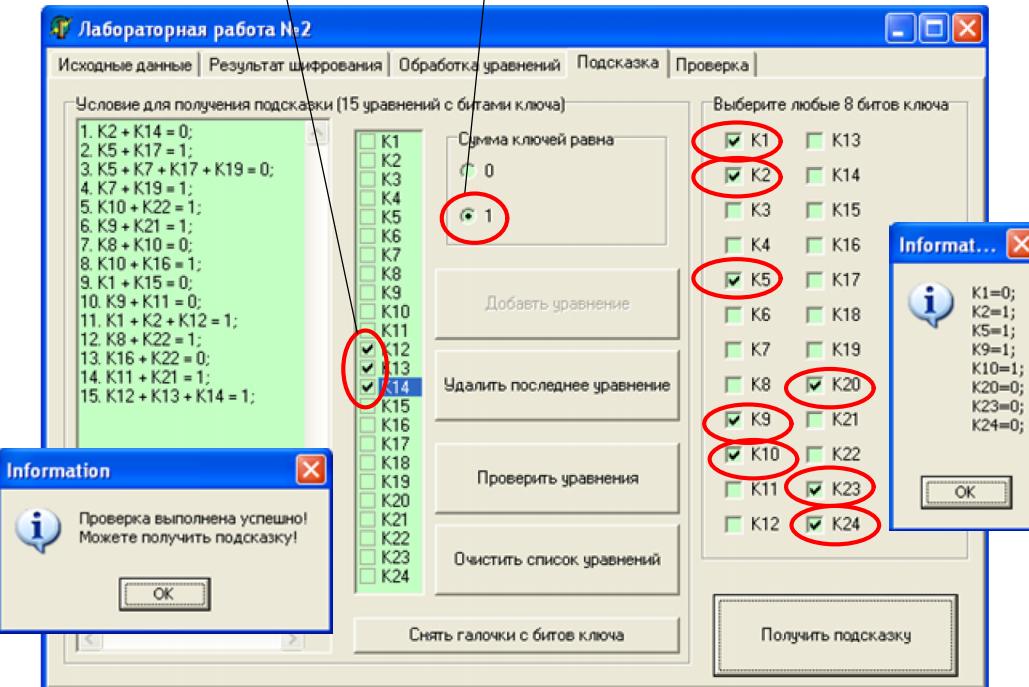
».

( .

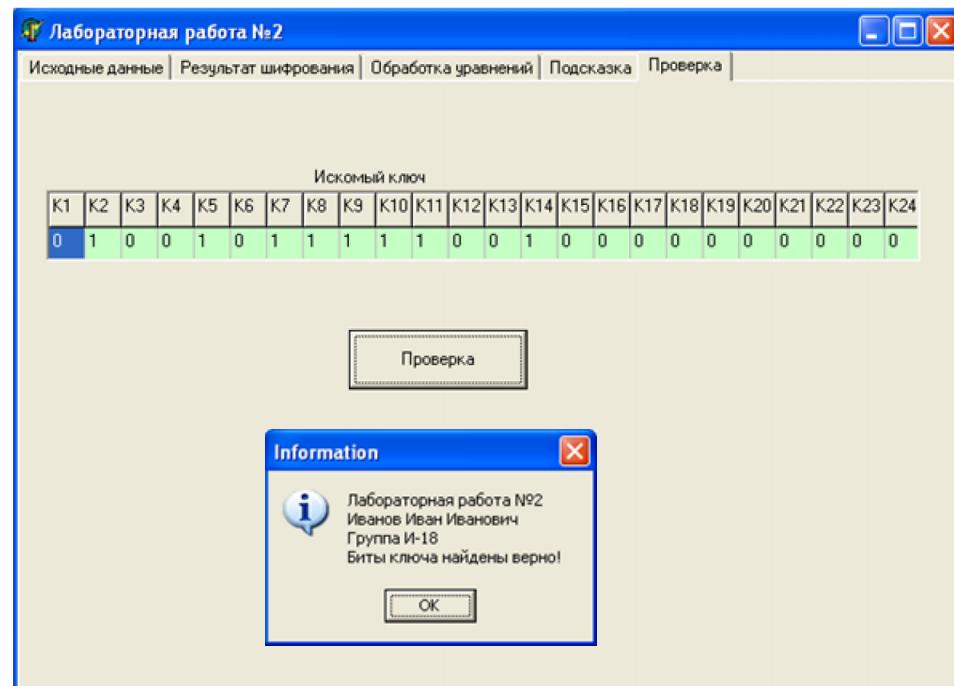
51),

Биты ключа для  
последнего  
введенного уравнения

Значение правой  
части уравнения



50 –



51 –

**Рекомендуется следующий порядок работы:**

## **Отчет по лабораторной работе должен содержать:**

4. 15

5.

6.

7. ,

8.

9.

**Пример выполнения лабораторной работы**

18. , 59752.

, 7 – 9,

6.

3.

( $\alpha$ , ).

, 7 – 9,

23 – 25.

3

, (

(23) (31)).

31.

31

, .

Y

,

$Q=0$ .

31

,

$Q=0$ ,

,

. . 3.3.

31

	,	$(\alpha, \beta)$				
1,1	(0100, 011)	$\frac{1}{8}$	$X_9 \oplus K_2 = C_4^1 \oplus C_3^1$		$X_9 \oplus Y_9 \oplus X_4 \oplus Y_4 \oplus$ $\oplus X_3 \oplus Y_3 = K_2 \oplus K_{14}$	$\frac{25}{32}$
3,1	(0100, 011)	$\frac{1}{8}$	$Y_9 \oplus K_{14} = C_4^3 \oplus C_3^3$			
1,1	(0111, 100)	1	$X_9 \oplus X_{11} \oplus X_{16} \oplus$ $\oplus K_2 \oplus K_3 \oplus K_4 = C_7^1$		$X_9 \oplus X_{11} \oplus X_{16} \oplus X_7 \oplus$ $\oplus Y_9 \oplus Y_{11} \oplus Y_{16} \oplus Y_7 =$ $= K_2 \oplus K_3 \oplus K_4 \oplus$ $\oplus K_{14} \oplus K_{15} \oplus K_{16}$	1
3,1	(0111, 100)	1	$Y_9 \oplus Y_{11} \oplus Y_{16} \oplus$ $\oplus K_{14} \oplus K_{15} \oplus K_{16} = C_7^3$			
1,1	(1011, 110)	1	$X_{15} \oplus X_{11} \oplus X_{16} \oplus$ $\oplus K_1 \oplus K_3 \oplus K_4 = C_7^1 \oplus C_4^1$		$X_{15} \oplus X_{11} \oplus X_{16} \oplus X_7 \oplus$ $\oplus X_4 \oplus Y_{15} \oplus Y_{11} \oplus Y_{16} \oplus$ $\oplus Y_7 \oplus Y_4 = K_1 \oplus K_3 \oplus$ $\oplus K_4 \oplus K_{13} \oplus K_{15} \oplus K_{16}$	1
3,1	(1011, 110)	1	$Y_{15} \oplus Y_{11} \oplus Y_{16} \oplus K_{13} \oplus$ $\oplus K_{15} \oplus K_{16} = C_7^3 \oplus C_4^3$			
1,1	(1100, 010)	1	$X_{15} \oplus X_9 \oplus K_1 \oplus K_2 = C_4^1$		$X_{15} \oplus X_9 \oplus X_4 \oplus Y_{15} \oplus Y_9 \oplus$ $\oplus Y_4 = K_1 \oplus K_2 \oplus K_{13} \oplus K_{14}$	1
3,1	(1100, 010)	1	$Y_{15} \oplus Y_9 \oplus K_{13} \oplus K_{14} = C_4^3$			
1,1	(1111, 101)	$\frac{1}{8}$	$X_{15} \oplus X_9 \oplus X_{11} \oplus X_{16} \oplus$ $\oplus K_1 \oplus K_2 \oplus K_3 \oplus K_4 =$ $= C_7^1 \oplus C_3^1$		$X_{15} \oplus X_9 \oplus X_{11} \oplus X_{16} \oplus$ $\oplus X_7 \oplus X_3 \oplus Y_{15} \oplus Y_9 \oplus$ $\oplus Y_{11} \oplus Y_{16} \oplus Y_7 \oplus Y_3 =$	

	3,1	(1111, 101)	$\frac{1}{8}$	$\begin{aligned} Y_{15} \oplus Y_9 \oplus Y_{11} \oplus Y_{16} \oplus K_{13} \oplus \\ \oplus K_{14} \oplus K_{15} \oplus K_{16} = \\ = C_7^3 \oplus C_3^3 \end{aligned}$		$\frac{25}{32}$
	1,2	(1000, 101)	1	$X_{10} \oplus K_5 = C_6^1 \oplus C_8^1$	$\begin{aligned} X_{10} \oplus X_6 \oplus X_8 \oplus Y_{10} \oplus Y_6 \oplus \\ \oplus Y_8 = K_5 \oplus K_{17} \end{aligned}$	1
	3,2	(1000, 101)	1	$Y_{10} \oplus K_{17} = C_6^3 \oplus C_8^3$		
	1,2	(1010, 010)	0	$\begin{aligned} X_{10} \oplus X_{14} \oplus K_5 \oplus K_7 = \\ = C_5^1 \end{aligned}$	$\begin{aligned} X_{10} \oplus X_{14} \oplus X_5 \oplus Y_{10} \oplus \\ \oplus Y_{14} \oplus Y_5 = K_5 \oplus K_7 \oplus \\ \oplus K_{17} \oplus K_{19} \end{aligned}$	1
	3,2	(1010, 010)	0	$\begin{aligned} Y_{10} \oplus Y_{14} \oplus K_{17} \oplus K_{19} = \\ = C_5^3 \end{aligned}$		
	1,2	(0100, 011)	$\frac{3}{4}$	$X_{12} \oplus K_6 = C_5^1 \oplus C_8^1$	$\begin{aligned} X_{12} \oplus X_5 \oplus X_8 \oplus Y_{12} \oplus \\ \oplus Y_5 \oplus Y_8 = K_6 \oplus K_{18} \end{aligned}$	$\frac{5}{8}$
	3,2	(0100, 011)	$\frac{3}{4}$	$Y_{12} \oplus K_{18} = C_5^3 \oplus C_8^3$		
	1,2	(1110, 001)	$\frac{1}{4}$	$\begin{aligned} X_{10} \oplus X_{12} \oplus X_{14} \oplus K_5 \oplus \\ \oplus K_6 \oplus K_7 = C_8^1 \end{aligned}$	$\begin{aligned} X_{10} \oplus X_{12} \oplus X_{14} \oplus X_8 \oplus \\ \oplus Y_{10} \oplus Y_{12} \oplus Y_{14} \oplus Y_8 = \\ = K_5 \oplus K_6 \oplus K_7 \oplus K_{17} \oplus \\ \oplus K_{18} \oplus K_{19} \end{aligned}$	$\frac{9}{16}$
	3,2	(1110, 001)	$\frac{1}{4}$	$\begin{aligned} Y_{10} \oplus Y_{12} \oplus Y_{14} \oplus K_{17} \oplus \\ \oplus K_{18} \oplus K_{19} = C_8^3 \end{aligned}$		
	1,3	(0100, 01)	0	$X_9 \oplus K_{10} = C_1^1$	$\begin{aligned} X_9 \oplus X_1 \oplus Y_9 \oplus Y_1 = \\ = K_{10} \oplus K_{22} \end{aligned}$	1
	3,3	(0100, 01)	0	$Y_9 \oplus K_{22} = C_1^3$		
	1,3	(1000, 01)	0	$X_{11} \oplus K_9 = C_2^1$	$\begin{aligned} X_{11} \oplus X_2 \oplus Y_{11} \oplus Y_2 = \\ = K_9 \oplus K_{21} \end{aligned}$	1
	3,3	(1000, 01)	0	$Y_{11} \oplus K_{21} = C_2^3$		
	1,3	(0100, 01)	0	$X_9 \oplus K_{10} = C_1^1$	$\begin{aligned} X_9 \oplus X_1 \oplus X_{12} \oplus X_{11} \oplus \\ \oplus Y_{12} \oplus Y_{11} = K_8 \oplus K_{10} \end{aligned}$	$\frac{7}{8}$
	2,1	(0100, 011)	$\frac{1}{8}$	$B_1 \oplus K_8 = C_4^2 \oplus C_3^2$		
	1,3	(0100, 01)	0	$X_9 \oplus K_{10} = C_1^1$	$X_1 \oplus Y_9 = K_{10} \oplus K_{16}$	1
	2,3	(0100, 01)	0	$B_1 \oplus K_{16} = C_1^2$		
	1,1	(1000, 001)	$\frac{1}{8}$	$X_{15} \oplus K_1 = C_3^1$	$\begin{aligned} X_3 \oplus X_{10} \oplus X_{15} \oplus Y_{10} = \\ = K_1 \oplus K_{15} \end{aligned}$	$\frac{7}{8}$
	2,3	(1000, 10)	0	$B_3 \oplus K_{15} = C_2^2$		
	1,1	(0111, 100)	1	$\begin{aligned} X_9 \oplus X_{11} \oplus X_{16} \oplus \\ \oplus K_2 \oplus K_3 \oplus K_4 = C_7^1 \end{aligned}$	$\begin{aligned} X_9 \oplus X_{16} \oplus X_7 \oplus Y_{11} = \\ = K_2 \oplus K_3 \oplus K_4 \oplus K_7 \end{aligned}$	$\frac{1}{8}$
	2,1	(1000, 001)	$\frac{1}{8}$	$B_7 \oplus K_7 = C_3^2$		
	1,3	(1000, 01)	0	$X_{11} \oplus K_9 = C_2^1$	$\begin{aligned} X_2 \oplus X_{11} \oplus X_{14} \oplus X_{16} \oplus \\ \oplus V \oplus V - K \oplus K \end{aligned}$	0

	2,2	(1000, 101)	1	$B_2 \oplus K_{11} = C_6^2 \oplus C_8^2$		
	1,1	(1100, 010)	1	$X_{15} \oplus X_9 \oplus K_1 \oplus K_2 = C_4^1$	$X_4 \oplus X_{13} \oplus X_{16} \oplus X_{15} \oplus$ $\oplus X_9 \oplus Y_{13} \oplus Y_{16} = K_1 \oplus$ $\oplus K_2 \oplus K_{12}$	$\frac{3}{4}$
	2,2	(0100, 011)	$\frac{3}{4}$	$B_4 \oplus K_{12} = C_5^2 \oplus C_8^2$		
	3,3	(0100, 01)	0	$Y_9 \oplus K_{22} = C_1^3$	$Y_9 \oplus Y_1 \oplus X_{12} \oplus X_{11} \oplus$ $\oplus Y_{12} \oplus Y_{11} = K_8 \oplus K_{22}$	$\frac{7}{8}$
	2,1	(0100, 011)	$\frac{1}{8}$	$B_1 \oplus K_8 = C_4^2 \oplus C_3^2$		
	3,3	(0100, 01)	0	$Y_9 \oplus K_{22} = C_1^3$	$Y_1 \oplus X_9 = K_{16} \oplus K_{22}$	1
	2,3	(0100, 01)	0	$B_1 \oplus K_{16} = C_1^2$		
	3,1	(0111, 100)	1	$Y_9 \oplus Y_{11} \oplus Y_{16} \oplus$ $\oplus K_{14} \oplus K_{15} \oplus K_{16} = C_7^3$	$X_{11} \oplus Y_7 \oplus Y_9 \oplus Y_{16} =$ $= K_7 \oplus K_{14} \oplus K_{15} \oplus K_{16}$	$\frac{1}{8}$
	2,1	(1000, 001)	$\frac{1}{8}$	$B_7 \oplus K_7 = C_3^2$		
	3,3	(1000, 01)	0	$Y_{11} \oplus K_{21} = C_2^3$	$X_{14} \oplus X_{16} \oplus Y_2 \oplus X_{14} \oplus$ $\oplus Y_{16} \oplus Y_{11} = K_{11} \oplus K_{21}$	0
	2,2	(1000, 101)	1	$B_2 \oplus K_{11} = C_6^2 \oplus C_8^2$		
	3,1	(1100, 010)	1	$Y_{15} \oplus Y_9 \oplus K_{13} \oplus K_{14} = C_4^3$	$X_{13} \oplus X_{16} \oplus Y_4 \oplus Y_{13} \oplus$ $\oplus Y_{16} \oplus Y_{15} \oplus Y_9 = K_{12} \oplus$ $\oplus K_{13} \oplus K_{14}$	$\frac{3}{4}$
	2,2	(0100, 011)	$\frac{3}{4}$	$B_4 \oplus K_{12} = C_5^2 \oplus C_8^2$		

,

.

1000

( « »).

32.

: , , Q=0, ,

, . . 3.4.

N=1000

1	$X_9 \oplus Y_9 \oplus X_4 \oplus Y_4 \oplus X_3 \oplus Y_3 = K_2 \oplus K_{14}$	$\frac{25}{32}$	765	$K_2 \oplus K_{14} = 0$
2	$X_9 \oplus X_{11} \oplus X_{16} \oplus X_7 \oplus Y_9 \oplus Y_{11} \oplus Y_{16} \oplus Y_7 = K_2 \oplus K_3 \oplus K_4 \oplus K_{14} \oplus K_{15} \oplus K_{16}$	1	1000	$K_2 \oplus K_3 \oplus K_4 \oplus K_{14} \oplus K_{15} \oplus K_{16} = 0$
3	$X_{15} \oplus X_{11} \oplus X_{16} \oplus X_7 \oplus X_4 \oplus Y_{15} \oplus Y_{11} \oplus Y_{16} \oplus Y_7 \oplus Y_4 = K_1 \oplus K_3 \oplus K_4 \oplus K_{13} \oplus K_{15} \oplus K_{16}$	1	1000	$K_1 \oplus K_3 \oplus K_4 \oplus K_{13} \oplus K_{15} \oplus K_{16} = 0$
4	$X_{15} \oplus X_9 \oplus X_4 \oplus Y_{15} \oplus Y_9 \oplus Y_4 = K_1 \oplus K_2 \oplus K_{13} \oplus K_{14}$	1	497	, $\frac{N}{2}$
5	$X_{15} \oplus X_9 \oplus X_{11} \oplus X_{16} \oplus X_7 \oplus X_3 \oplus Y_{15} \oplus Y_9 \oplus Y_{11} \oplus Y_{16} \oplus Y_7 \oplus Y_3 = K_1 \oplus K_2 \oplus K_3 \oplus K_4 \oplus K_{13} \oplus K_{14} \oplus K_{15} \oplus K_{16}$	$\frac{25}{32}$	775	$K_1 \oplus K_2 \oplus K_3 \oplus K_4 \oplus K_{13} \oplus K_{14} \oplus K_{15} \oplus K_{16} = 0$
6	$X_{10} \oplus X_6 \oplus X_8 \oplus Y_{10} \oplus Y_6 \oplus Y_8 = K_5 \oplus K_{17}$	1	0	$K_5 \oplus K_{17} = 1$
7	$X_{10} \oplus X_{14} \oplus X_5 \oplus Y_{10} \oplus Y_{14} \oplus Y_5 = K_5 \oplus K_7 \oplus K_{17} \oplus K_{19}$	1	1000	$K_5 \oplus K_7 \oplus K_{17} \oplus K_{19} = 0$
8	$X_{12} \oplus X_5 \oplus X_8 \oplus Y_{12} \oplus Y_5 \oplus Y_8 = K_6 \oplus K_{18}$	$\frac{5}{8}$	648	$K_6 \oplus K_{18} = 0$
9	$X_{10} \oplus X_{12} \oplus X_{14} \oplus X_8 \oplus Y_{10} \oplus Y_{12} \oplus Y_{14} \oplus Y_8 = K_5 \oplus K_6 \oplus K_7 \oplus K_{17} \oplus K_{18} \oplus K_{19}$	$\frac{9}{16}$	632	$K_5 \oplus K_6 \oplus K_7 \oplus K_{17} \oplus K_{18} \oplus K_{19} = 0$
10	$X_9 \oplus X_1 \oplus Y_9 \oplus Y_1 = K_{10} \oplus K_{22}$	1	0	$K_{10} \oplus K_{22} = 1$
11	$X_{11} \oplus X_2 \oplus Y_{11} \oplus Y_2 = K_9 \oplus K_{21}$	1	0	$K_9 \oplus K_{21} = 1$
12	$X_9 \oplus X_1 \oplus X_{12} \oplus X_{11} \oplus Y_{12} \oplus Y_{11} = K_8 \oplus K_{10}$	$\frac{7}{8}$	875	$K_8 \oplus K_{10} = 0$
13	$X_1 \oplus Y_9 = K_{10} \oplus K_{16}$	1	0	$K_{10} \oplus K_{16} = 1$
14	$X_3 \oplus X_{10} \oplus X_{15} \oplus Y_{10} = K_1 \oplus K_{15}$	$\frac{7}{8}$	873	$K_1 \oplus K_{15} = 0$
15	$X_9 \oplus X_{16} \oplus X_7 \oplus Y_{11} = K_2 \oplus K_3 \oplus K_4 \oplus K_7$	$\frac{1}{8}$	123	$K_2 \oplus K_3 \oplus K_4 \oplus K_7 = 0$
16	$X_2 \oplus X_{11} \oplus X_{14} \oplus X_{16} \oplus Y_{14} \oplus Y_{16} = K_9 \oplus K_{11}$	0	0	$K_9 \oplus K_{11} = 0$
17	$X_4 \oplus X_{13} \oplus X_{16} \oplus X_{15} \oplus X_9 \oplus Y_{13} \oplus Y_{16} = K_1 \oplus K_2 \oplus K_{12}$	$\frac{3}{4}$	234	$K_1 \oplus K_2 \oplus K_{12} = 1$

18	$Y_9 \oplus Y_1 \oplus X_{12} \oplus X_{11} \oplus Y_{12} \oplus Y_{11} = K_8 \oplus K_{22}$	$\frac{7}{8}$	123	$K_8 \oplus K_{22} = 1$
19	$Y_1 \oplus X_9 = K_{16} \oplus K_{22}$	1	1000	$K_{16} \oplus K_{22} = 0$
20	$X_{11} \oplus Y_7 \oplus Y_9 \oplus Y_{16} = K_7 \oplus K_{14} \oplus K_{15} \oplus K_{16}$	$\frac{1}{8}$	142	$K_7 \oplus K_{14} \oplus K_{15} \oplus K_{16} = 0$
21	$X_{14} \oplus X_{16} \oplus Y_2 \oplus X_{14} \oplus Y_{16} \oplus Y_{11} = K_{11} \oplus K_{21}$	0	1000	$K_{11} \oplus K_{21} = 0$
22	$X_{13} \oplus X_{16} \oplus Y_4 \oplus Y_{13} \oplus Y_{16} \oplus Y_{15} \oplus Y_9 = K_{12} \oplus K_{13} \oplus K_{14}$	$\frac{3}{4}$	238	$K_{12} \oplus K_{13} \oplus K_{14} = 1$

21 ( 32  
4 ).

$$K_2 \oplus K_{14} = 0, \quad (34)$$

$$K_2 \oplus K_3 \oplus K_4 \oplus K_{14} \oplus K_{15} \oplus K_{16} = 0, \quad (35)$$

$$K_1 \oplus K_3 \oplus K_4 \oplus K_{13} \oplus K_{15} \oplus K_{16} = 0, \quad (36)$$

$$K_1 \oplus K_2 \oplus K_3 \oplus K_4 \oplus K_{13} \oplus K_{14} \oplus K_{15} \oplus K_{16} = 0, \quad (37)$$

$$K_5 \oplus K_{17} = 1, \quad (38)$$

$$K_5 \oplus K_7 \oplus K_{17} \oplus K_{19} = 0, \quad (39)$$

$$K_6 \oplus K_{18} = 0, \quad (40)$$

$$K_5 \oplus K_6 \oplus K_7 \oplus K_{17} \oplus K_{18} \oplus K_{19} = 0, \quad (41)$$

$$K_{10} \oplus K_{22} = 1, \quad (42)$$

$$K_9 \oplus K_{21} = 1, \quad (43)$$

$$K_8 \oplus K_{10} = 0, \quad (44)$$

$$K_{10} \oplus K_{16} = 1, \quad (45)$$

$$K_1 \oplus K_{15} = 0, \quad (46)$$

$$K_2 \oplus K_3 \oplus K_4 \oplus K_7 = 0, \quad (47)$$

$$K_9 \oplus K_{11} = 0, \quad (48)$$

$$K_1 \oplus K_2 \oplus K_{12} = 1, \quad (49)$$

$$K_8 \oplus K_{22} = 1, \quad (50)$$

$$K_{16} \oplus K_{22} = 0, \quad (51)$$

$$K_7 \oplus K_{14} \oplus K_{15} \oplus K_{16} = 0, \quad (52)$$

$$K_{11} \oplus K_{21} = 0, \quad (53)$$

$$K_{12} \oplus K_{13} \oplus K_{14} = 1. \quad (54)$$

$$(34) - (54) \quad : \quad 20, \quad 23, \quad 24.$$

, , .

$$1, \quad 2, \quad 5, \quad 9, \quad 10 \quad ( \quad . \quad \quad \quad \quad 50).$$

:

$$_1 = 0,$$

$$_2 = 1,$$

$$_5 = 1,$$

$$_9 = 1,$$

$$_{10} = 1,$$

$$_{20} = 0,$$

$$_{23} = 0,$$

$$_{24} = 0.$$

$$(34) - (54) \quad : \quad$$

$$K_{14} = 1, \quad (55)$$

$$K_3 \oplus K_4 \oplus K_{14} \oplus K_{15} \oplus K_{16} = 1, \quad (56)$$

$$K_3 \oplus K_4 \oplus K_{13} \oplus K_{15} \oplus K_{16} = 0, \quad (57)$$

$$K_3 \oplus K_4 \oplus K_{13} \oplus K_{14} \oplus K_{15} \oplus K_{16} = 1, \quad (58)$$

$$K_{17} = 0, \quad (59)$$

$$K_7 \oplus K_{17} \oplus K_{19} = 1, \quad (60)$$

$$K_6 \oplus K_7 \oplus K_{17} \oplus K_{18} \oplus K_{19} = 1, \quad (61)$$

$$K_{22} = 0, \quad (62)$$

$$K_{21} = 0, \quad (63)$$

$$K_8 = 1, \quad (64)$$

$$K_{16} = 0, \quad (65)$$

$$K_{15} = 0, \quad (66)$$

$$K_3 \oplus K_4 \oplus K_7 = 1, \quad (67)$$

$$K_{11} = 1, \quad (68)$$

$$K_{12} = 0. \quad (69)$$

$$(55), (65), (66) \quad (52), \quad : \quad$$

$$K_7 = 1. \quad (70)$$

$$(55), (69) \quad (54), \quad : \quad$$

$$K_{13} = 0. \quad (71)$$

$$(59) \quad (70) \quad (60), \quad : \quad$$

$$K_{19} = 0. \quad (72)$$

$$(70) \quad (67), \quad : \quad$$

$$K_3 \oplus K_4 = 0. \quad (73)$$

$$(73), \quad , \quad _3 \quad _4$$

$$(40), \quad , \quad _6 \quad _{18}$$

$$\cdot, \quad , \quad (16) \quad ).$$

4.

$$33. \quad ,$$

.

	-	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	0	1	0	0	1	0	1	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
2	0	1	0	0	1	1	1	1	1	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0
3	0	1	1	1	1	0	1	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
4	0	1	1	1	1	1	1	1	1	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0

,

( 51).

## Ответы к задачам для самостоятельного решения

### **Глава 1**

#### ***Задание №1***

,

( ).

- 1)  $173_{10} \oplus 21_{10} = 10101101_2 \oplus 00010101_2 = 10111000_2 = 184_{10}$
- 2)  $113_{10} \oplus 75_{10} = 01110001_2 \oplus 01001011_2 = 00111010_2 = 58_{10}$
- 3)  $DE_{16} \oplus FC_{16} = 11011110_2 \oplus 11111100_2 = 00100010_2 = 22_{16}$
- 4)  $A23_{16} \oplus 18B_{16} = 101000100011_2 \oplus 000110001011_2 = 101110101000_2 = 8_{16}$
- 5)  $47_{16} \oplus 29_{16} = 00101111_2 \oplus 00011101_2 = 00110010_2 = 32_{16}$
- 6)  $127_8 \oplus 215_8 = 001010111_2 \oplus 010001101_2 = 011011010_2 = 332_8$
- 7)  $C8_{16} \oplus 7B_{16} = 11001000_2 \oplus 01111011_2 = 10110011_2 = 3_{16}$
- 8)  $58_{10} \oplus 137_{10} = 00111010_2 \oplus 10001001_2 = 10110011_2 = 179_{10}$

#### ***Задание №2***

- 1) 1, 0100 101 ( 2, ( 0), ( 100)).
- 2) 1, 1100 110 ( 2, ( 1), ( 100)).
- 3) 2 0010 111 ( 3, ( 0), ( 010)).
- 4) 2 0110 001 ( 3, ( 0), ( 110)).
- 5) 3 1001 01 ( 3, ( 11), ( 00)).

- 6) 3 0000 01 ( 4,  
     ( 00), ( 00)).
- 7) 2 1001 110 ( 4,  
     3, ( 1), ( 001)).
- 8) 3 1010 10 ( 4,  
     ( 10), ( 01)).

### ***Задание №3***

1.

- |    |          |               |
|----|----------|---------------|
| 1) | 11011101 | 01111100111;  |
| 2) | 00110110 | 110010011001; |
| 3) | 01001001 | 000101100110; |
| 4) | 11101101 | 101111101110; |
| 5) | 01000101 | 000111000110; |
| 6) | 11101001 | 101101101110. |

### ***Задание №4***

5.

- |    |          |           |
|----|----------|-----------|
| 1) | 01101101 | 10111001; |
| 2) | 10110111 | 11100111; |
| 3) | 10001010 | 01001010; |
| 4) | 00011010 | 01001100; |
| 5) | 11011101 | 10011111; |
| 6) | 01011111 | 11011101. |

### **Задание №5**

,

1.

- |    |              |           |
|----|--------------|-----------|
| 1) | 011101010111 | 11010011; |
| 2) | 100101111110 | 01101011; |
| 3) | 110110011011 | 01110110; |
| 4) | 011101110111 | 11011011; |
| 5) | 111001001101 | 10110001; |
| 6) | 100110001010 | 01100100; |
| 7) | 101101111110 | 11101011; |
| 8) | 100111001110 | 01100101. |

Пояснения к решению:

1,

,

—

..

.,

1,

,

,

., ,

,

,

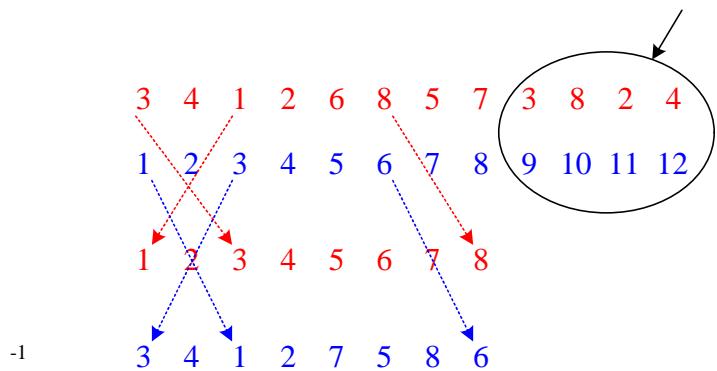
,

,

,

-1

52.



52-

-1

52

,

,

,

,

,  
8-

,  
,

12-

-1

8                  12,

52.

12-

### **Задание №6**

,

5.

- |    |          |           |
|----|----------|-----------|
| 1) | 10001011 | 10001101; |
| 2) | 11011000 | 01001011; |
| 3) | 01010110 | 11010010; |

4)	01101100	00111010;
5)	11000111	10010111;
6)	01011101	01011110;
7)	01100001	00100110;
8)	11000100	00010011.

Пояснения к решению:

-1

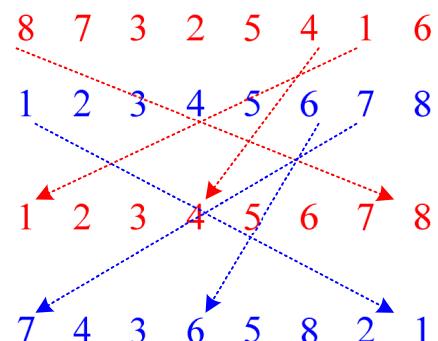
53.

Прямая перестановка Р

Порядок битов

Восстановленный  
порядок битов

Обратная перестановка  $P^{-1}$



53 –

-1

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. .. //  
[http://www.enlight.ru/crypto/articles/shannon/shann\\_i.htm](http://www.enlight.ru/crypto/articles/shannon/shann_i.htm)
2. .. : , ,  
— .: , 2002. — . 648.
3. .. .. .. ..  
: . — - , 2000. — 78 .
4. .. ..  
. : - , 2009. — 576 .
5. Matsui M., Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology – EUROCRYPT’93, Springer-Verlag, 1998, p.386.
6. Biham E., Shamir A., Differential Cryptanalysis of the Full 16-round DES, Crypto’92, Springer-Velgar, 1998, p.487
7. Biham E., Shamir A., Differential Cryptanalysis of DES-like Cryptosystems, Extended Abstract, Crypto’90, Springer-Velgar, 1998, p.2
8. .. .. ..  
— .: , 2006. — 376 .
9. Feistel H, Cryptography and Computer Privacy, May 1973 //  
<http://www.apprendre-en-ligne.net/crypto/bibliotheque/feistel/index.html>