Лабораторная работа 7

«Блочные алгоритмы шифрования»

Теоретическая часть

Понятие композиционного шифра

Комбинация нескольких подряд примененных простых шифров, (например, перестановки или подстановки) дает в результате более сложное преобразование, называемое **комбинированным (композиционным) шифром**. Этот шифр обладает более сильными криптографическими возможностями, чем отдельная перестановка или подстановка.

Вернемся к примеру из "Простейшие методы шифрования с закрытым ключом" , в котором производится шифрование методом перестановки с фиксированным периодом. Пусть период перестановки d=6, а ключ К равен 436215. Это означает, что в каждом блоке из шести символов четвертый символ становится на первое место, третий – на второе, шестой – на третье и т.д. Зашифруем с помощью выбранного ключа слово СИГНАЛ:

$$СИГНАЛ \xrightarrow{K=436215} НГЛИСА$$

Будем предполагать, что противнику известен метод шифрования, но неизвестен ключ. Если противник перехватит сообщение НГЛИСА, ему понадобится, как указывалось в "Простейшие методы шифрования с закрытым ключом" , не более 720 попыток (при использовании метода полного перебора). Для того чтобы изучить 720 вариантов на самом деле требуется не так уж много времени. Предположим, что на изучение каждого варианта у противника уходит 1 секунда. Тогда на все 720 попыток потребуется всего 12 минут. Таким образом, не более чем за 12 минут работы противник узнает наш ключ и сможет в дальнейшем расшифровывать все сообщения, закрытые тем же ключом. Если же анализ производится с использованием компьютера, для дешифрации НГЛИСА и поиска ключа потребуется гораздо меньше времени.

Обозначим ключ в методе Цезаря k_1 ($1<=k_1<=31$), а ключ при перестановке – k_2. Тогда общий ключ $K = (k_1, k_2)$. Таким образом, если К = (5, 436215), это значит, что вначале шифруемые символы заменяются по методу Цезаря с ключом 5, а затем в каждом блоке из шести символов производится

перестановка с ключом 436215. Выполним в два этапа шифрование слова СИГНАЛ:

1 *этап* **(***замена***):** СИГНАЛ $\xrightarrow{k1=5}$ ЦОИТЕР

2 *этап* **(***перестановка***):** ЦОИТЕР $\xrightarrow{k2=436215}$ ТИРОЦЕ

Можно записать также и так:

СИГНАЛ $\xrightarrow{K=(5,436215)}$ ТИРОЦЕ

Количество возможных ключей в шифре Цезаря равно в нашем случае 31, поэтому общее число вариантов возможных ключей (пространство ключей) в примененном комбинированном шифре равно 31x720=22320. Таким образом, действительно, полученный комбинированный шифр значительно сильнее отдельно выполненных замены и перестановки.

Для затруднения криптоанализа статистическими методами можно использовать наш комбинированный шифр дважды с одним и тем же ключом:

Цикл шифрования **1**

1 *этап* **(***замена***):** СИГНАЛ $\xrightarrow{k1=5}$ ЦОИТЕР

2 *этап* **(***перестановка***):** ЦОИТЕР $\xrightarrow{k2=436215}$ ТИРОЦЕ

Цикл шифрования **2**

1 *этап* **(***замена***):** ТИРОЦЕ $\xrightarrow{k1=5}$ ЧОХУЫЛ

2 *этап* **(***перестановка***):** ЧОХУЫЛ $\xrightarrow{k2=436215}$ УХЛОЧЫ

В результате двух подряд выполненных циклов шифрования слово СИГНАЛ превратилось в УХЛОЧЫ. При этом пространство ключей шифра не изменилось, однако за счет двухкратного шифрования статистические закономерности исходного текста замаскировались сильнее.

Алгоритмы симметричного шифрования могут обрабатывать исходный текст блоками или потоком. В зависимости от этого различают *блочные* алгоритмы симметричного шифрования и *поточные*. Блок текста рассматривается как неотрицательное целое число либо как несколько независимых неотрицательных целых чисел. Длина блока всегда выбирается равной степени двойки, например, 64, 128, 256 бит.

Операции, используемые в блочных алгоритмах симметричного шифрования

Рассмотрим операции, используемые в большинстве алгоритмов симметричного шифрования. Будем при этом помнить, что рассматриваемые операции применяются к двоичным данным. Любая информация, например, изображения или текст, могут быть представлены в двоичном виде. Благодаря этому при шифровании не приходится задумываться о смысле передаваемых сообщений.

Одна из часто используемых операций – операция побитового сложения по модулю 2, обозначаемая XOR или $\oplus$. Принципы выполнения этой операции подробно рассмотрены в "Простейшие методы шифрования с закрытым ключом" . При сложении по модулю 2 операнды обрабатываются поразрядно. В разряде результата ставится единица, если в соответствующих разрядах операндов присутствует нечетное число единиц. Например, сложим по модулю 2 два 16-разрядных числа:

Номер разряда:	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Операнд 1:	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
Операнд 2:	0	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1
Сумма по мод. 2:	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0	1

Эта операция имеет очень удобное свойство: вычитание по модулю два есть то же самое, что и сложение, поэтому один из операндов может быть получен путем прибавления к сумме другого операнда.

Также в блочных алгоритмах шифрования широко используется *операция сложения по модулю* 2^{32} *или по модулю* 2^{16}. Эта операция представляет собой обыкновенное сложение двоичных чисел без учета переноса в старший 32-й или 16-й разряд результата. Например, сложим по модулю 2^{16} два 16-разрядных числа:

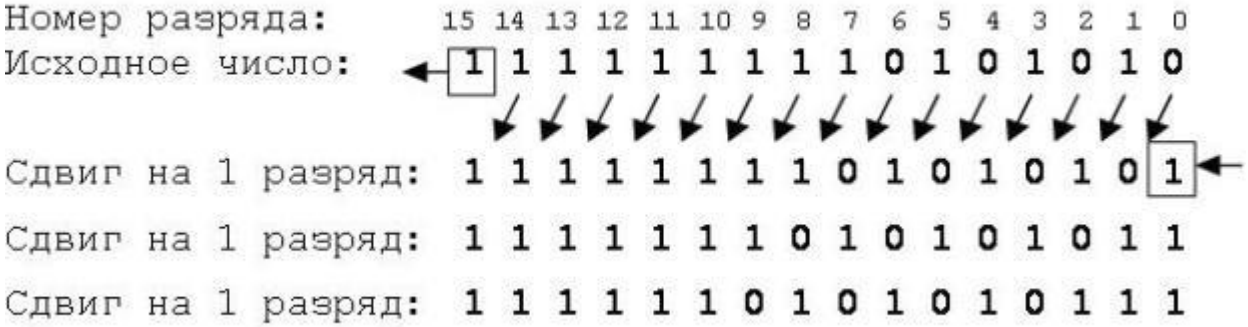
Номер разряда:	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Операнд 1:	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
Операнд 2:	0	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1
Сумма по мод.2^{16}:	(1)	0	0	0	1	1	1	0	1	1	1	0	1	1	1	0	1

Перенос из 15-го разряда, обозначенный в примере как единица в скобках, дальше не используется и поэтому отбрасывается.

Циклический сдвиг передвигает цепочку бит на некоторое число разрядов влево или вправо. Двоичное число при выполнении операции сдвига напоминает длинную гусеницу, выползающую с одной стороны туннеля и заползающую с другой. При циклическом сдвиге влево биты, выходящие слева за разрядную сетку дописываются справа на освободившиеся места.

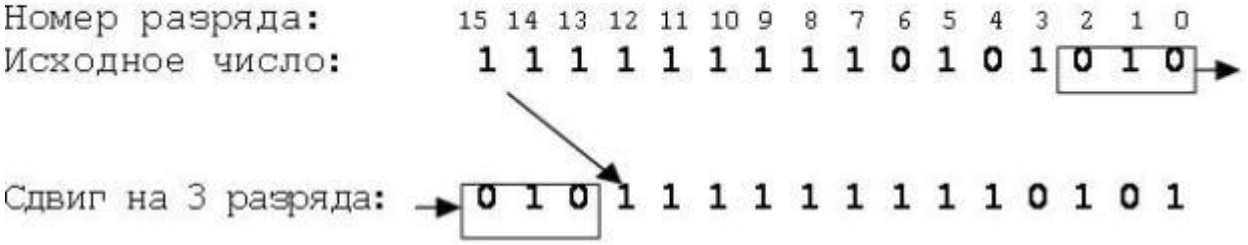
При циклическом сдвиге вправо все биты передвигаются цепочкой вправо, а те, которым не хватает места, переносятся в хвост цепочки. Например, выполним циклический сдвиг двоичного числа влево на 3 разряда. Для этого будем 3 раза переписывать двоичные цифры, каждый раз смещая их влево на 1 разряд и перенося знаки, выходящие из пятнадцатого разряда на место нулевого.

Циклический сдвиг влево на 3 разряда (←)



Аналогично выполняется и циклический сдвиг вправо. Например, при сдвиге вправо на 3 разряда нулевой, первый и второй биты исходного числа выходят из разрядной сетки и запоминаются, все остальные биты перемещаются вправо на 3 позиции, затем запомненные цифры записываются на тринадцатое, четырнадцатое и пятнадцатое места.

Циклический сдвиг вправо на 3 разряда (→)



При выполнении *табличной подстановки* группа битов отображается в другую группу битов. При этой операции один блок двоичных данных заменяется по определенному правилу или таблице другим блоком. Например, можно заменять каждую группу из трех двоичных цифр другой группой из трех цифр по следующей таблице:

Вход	**Выход**
000	011
001	101
010	000

011	111
100	010
101	110
110	001
111	100

Если каждое значение, записанное в столбцах "Вход" и "Выход" записать не в двоичном, а в десятичном виде, то ту же самую таблицу замен можно будет записать более кратко, например, так:

```
0->3, 1->5, 2->0, 3->7, 4->2, 5->6, 6->1, 7->4
```

Первая цифра в такой записи представляет значение на входе, а вторая – на выходе. Если значения входов упорядочены по возрастанию в обычном порядке, то можно вообще не писать первую цифру, а записать только соответствующие значения выходов:

```
3, 5, 0, 7, 2, 6, 1, 4.
```

То есть в качестве замены для значения 3-битового блока выбирается элемент из таблицы замен с порядковым номером, равным значению заменяемого блока.

Если необходимо заменять группы из четырех двоичных цифр, то таблица замен должна содержать уже 16 значений. В общем случае для n-битовых блоков таблица замен должна содержать 2^n элементов.

Табличную подстановку в литературе иногда называют заменой с использованием S-блоков или S-box. (Буква S взята от английского слова substitution – подстановка).

С помощью операции *перемещения* биты сообщения переупорядочиваются. Перемещение называют также permutation или P-блоком.

Структура блочного алгоритма симметричного шифрования

Таким образом, в алгоритмах симметричного шифрования часто используются операции сложения по модулю 2, сложения по модулю 2^{16} или 2^{32}, циклического сдвига, замены и перестановки.

Эти операции циклически повторяются в алгоритме N раз, образуя так называемые *раунды* или *шаги*. Исходными данными для каждого раунда являются выход предыдущего раунда и ключ, который получен по определенному алгоритму из общего ключа шифрования K. Ключ раунда называется *подключом* K_i. В результате блочный алгоритм шифрования может быть представлен следующим образом (рис. 3.1).

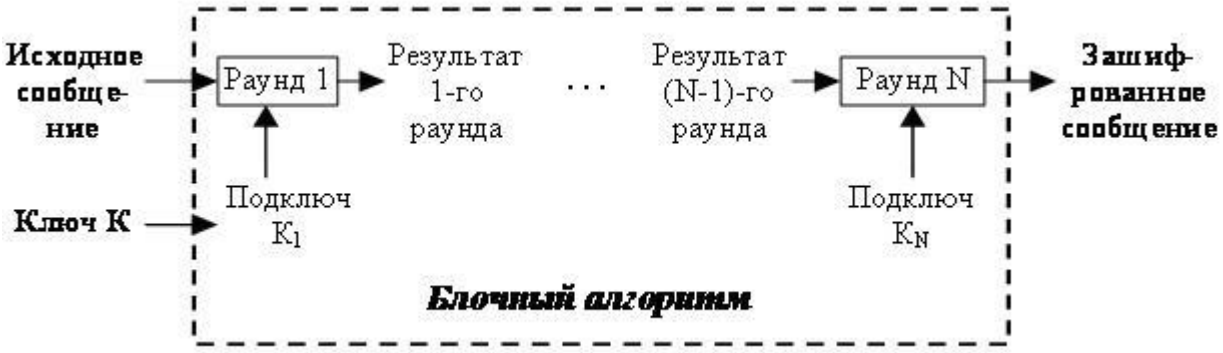


Рис. 3.1. Структура блочного алгоритма симметричного шифрования

Блочные алгоритмы шифрования применяются к двоичным данным. В общем случае процедура блочного шифрования преобразовывает n-битный блок открытого текста в k-битный блок зашифрованного текста. Число блоков длины n равно 2^n. Для того чтобы преобразование было обратимым, каждый из таких блоков должен преобразовываться в свой уникальный блок зашифрованного текста. Длина блока всегда выбирается равной степени двойки, например, 64, 128, 256 бит.

Практическая часть

Выполните следующие задания:

1. Сложите по модулю 2:
   - двоичные числа 10101100 и 11001010 ;
   - десятичные числа 15 и 10 ;
   - шестнадцатеричные числа 0B5 и 37.

Примечание: десятичные и шестнадцатеричные числа необходимо сначала перевести в двоичный вид.

2. Сложите по модулю 2^8:
   - двоичные числа 10101100 и 11001010 ;
   - десятичные числа 155 и 100 ;
   - шестнадцатеричные числа 0B5 и 37.

Примечание: десятичные числа необходимо сначала перевести в двоичный вид.

3. Выполните операцию циклического сдвига:
   - влево на 5 разрядов для двоичного числа 10101100 ;
   - вправо на 4 разряда для шестнадцатеричного числа 9E ;
   - вправо на 2 разряда для шестнадцатеричного числа 55.

Примечание: шестнадцатеричные числа необходимо сначала перевести в двоичный вид.

4. Пусть каждые три бита входного сообщения заменяются по следующей таблице замен:

Вход	Выход
000	011
001	101
010	000
011	111
100	010
101	110
110	001
111	100

5. Выполните разбиение исходного сообщения на блоки по три бита и произведите поблочную замену для следующих сообщений, представленных в цифровом виде:

- $1010\ 1100\ 1100_{(2)}$
- $2356_{(10)}$
- $0B57_{(16)}$

Примечание: десятичные и шестнадцатеричные числа необходимо сначала перевести в двоичный вид.

Вопросы для защиты работы

1. Какой шифр называют комбинированным или композиционным шифром?
2. Какие факторы влияют на стойкость блочного алгоритма шифрования?
3. Какие простейшие операции применяются в блочных алгоритмах шифрования?
4. В чем отличие блочных алгоритмов шифрования от поточных?
5. Что понимается под "раундом" алгоритма шифрования?
6. Каковы требования к блочному алгоритму шифрования?
7. Почему блочный алгоритм шифрования должен иметь простую и понятную структуру?
8. Что понимается под требованием "высокой криптостойкости" алгоритма шифрования?