Министерство образования и науки Российской Федерации
НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Ю.А. КОТОВ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

СТАНДАРТНЫЕ ШИФРЫ
ШИФРЫ С ОТКРЫТЫМ КЛЮЧОМ

Утверждено
Редакционно-издательским советом университета
в качестве учебного пособия

НОВОСИБИРСК
2017

УДК 004.056.55(075.8)
К 736

Рецензенты:
д-р техн. наук, профессор *В.И. Гужов,*
канд. техн. наук, доцент *Г.В. Трошина*

Работа подготовлена на кафедре защиты информации

Котов Ю.А.

К 736 Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом: учебное пособие / Ю.А. Котов. – Новосибирск: Изд-во НГТУ, 2017. – 67 с.

ISBN 978-5-7782-3411-6

Представлены основные стандартные симметричные шифры, шифры с открытым ключом, теоретические и прикладные свойства данной группы криптографических методов защиты информации, а также способы применения этих методов.

Предназначено для студентов, обучающихся по направлению 10.03.01 «Информационная безопасность» и специальности 10.05.03 «Информационная безопасность автоматизированных систем».

УДК 004.056.55(075.8)

ISBN 978-5-7782-3411-6

1. СТАНДАРТНЫЕ ШИФРЫ

1.1. Цели и схемы создания стандартных шифров

Стандартные массовые шифры направлены на практическое решение проблем, возникающих из теоретического решения задачи шифрования [1]. Как известно, для получения такого решения используемые ключи должны быть не меньше длины шифруемого текста, независимы от него и случайны [2–7]. Следовательно, возникает первая проблема – проблема объема. Если необходимо зашифровать объем данных V, то потребуется объем ключей, вообще говоря, больший V (в том числе имея в виду некоторый необходимый практический объем ключей для шифрования ключей), т. е. объем информации при использовании шифрования более чем удваивается по отношению к исходному объему – неравенство

$$V_{\text{шифр}} > 2V_{\text{исход}}. \qquad (1)$$

Следом возникает проблема увеличения времени доступа к используемой информации. Если время доступа к фрагменту данных J без использования шифрования составляло T_j, то при доступе к зашифрованным данным необходимо добавить время доступа к ключу J-го фрагмента T_{KJ}, которое в соответствии с (1) не меньше исходного T_j, а также время расшифрования данных $T_{\text{Ш}}$, которое также можно оценить как не меньшее T_j. Таким образом, время доступа к данным при использовании шифрования как минимум утраивается – неравенство

$$T_{\text{шифр}} > 3T_{\text{исход}}. \qquad (2)$$

И это, очевидно, еще не самая пессимистическая оценка.

Третья проблема очевидным образом связана с профессиональной неподготовленностью массового пользователя стандартных шифров. Методы шифрования имеют свои фундаментальные ограничения и недостатки. Они, как и способы их устранения (обхода) с помощью подготовки текста (см. приложение) и ключей, хорошо известны специалистам, но практически неизвестны – да и не должны быть известны – массовому пользователю.

Массовые стандартные алгоритмы шифрования должны быть направлены в первую очередь на решение трех указанных проблем.

Такое решение для массовых шифров лежит через решение задачи: как из «короткого» ключа небольшого размера (и возможно, «плохого») получить «хороший» «длинный» ключ, соответствующий требованиям шифрования [1]. Собственно, стандартные симметричные шифры представляют собой генераторы ключей (неважно, признают это авторы шифров или нет).

Основными блочными схемами формирования стандартных массовых шифров являются сеть Фейстеля и перестановочно-подстановочная SP-сеть [6].

Сеть Фейстеля

Образуется *n* раундами (циклами, шагами) циклического шифрования перестановкой и заменой (конкретно – гаммированием [2]).

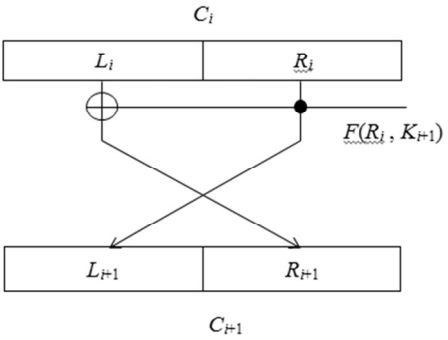

Рис. 1. Сеть Фейстеля

На рис. 1 $L_{i+1} = R_i$; $R_{i+1} = L_i(+)F(R_i, K_{i+1})$; F – функция шифрования; K_{i+1} – раундовый ключ; (+) – операция сложения по модулю 2.

Типичные представители: DES, ГОСТ 28147–89.

SP-сеть

Преобразование каждого цикла является следующей комбинацией замен (S-блоков) и перестановок (P-блоков) (рис. 2).

S-блок (узел замены) осуществляет отображение из множества двоичных векторов длины n во множество двоичных векторов длины m; n, m относительно малы, например 4, 6, 8, 16, 32. Бывает, что $n = m$. Математически S-блок является векторной булевой функцией.

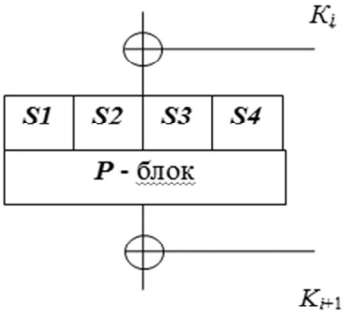

Рис. 2. SP-сеть

P-блок – перестановка на множестве координат двоичного вектора длины n, которое, как правило, достаточно большое (64, 128, …) и часто совпадает с длиной блока. Одной из отличительных особенностей SP-сетей является их внутренний параллелизм, делающий эффективным их применение в вычислительных системах с параллельной структурой [6].

Типичные представители: IDEA, AES.

В реальных шифрах сети Фейстеля и SP-сеть, как правило, используются совместно. Так, DES и ГОСТ 28147–89 – это не только сеть Фейстейля, но и SP-сеть, реализующая функцию шифрования.

1.2. Алгоритм шифрования DES

Алгоритм DES (Data Encryption Standard) был принят в качестве американского стандарта шифрования в 1980 г. Первые варианты появились в 1977 г. Предназначен для шифрования важной, но не секретной информации.

DES является блочным алгоритмом симметричного шифрования с длиной блока 64 бита. Симметрия алгоритма означает, что расшифрование выполняется по тому же ключу, что и шифрование.

Ключ длиной 56 бит размещен в блоке длиной 64 бита. Биты 8, 16, 24 и т. д. этого блока могут применяться для контроля четности и в ключе не используются. Процессы шифрования и расшифрования являются инверсными по отношению друг к другу, т. е. требуют обратного порядка применения ключевой информации и операций.

Параметры сети Фейстеля, реализованной в DES, включая начальную и конечную перестановки, функцию шифрования и получения раундовых ключей, установлены матрицами с фиксированными размерностями и значениями.

При описании алгоритма шифрования используются следующие обозначения:

- L и R – соответственно левая (старшая) и правая (младшая) части 64-битовой последовательности;
- LR – конкатенация последовательностей L и R. В этой последовательности биты последовательности R следуют за битами последовательности L;
- (+) – операция побитового сложения по модулю 2.

Процессы шифрования и расшифрования в DES

DES представляет собой комбинацию замен и перестановок. Выполнение над блоком одной такой комбинации называется раундом. Всего для получения блока зашифрованного сообщения проводится 16 раундов.

Последовательность действий, совершаемых в процессе шифрования данных, заключается в следующем.

1. Начальная перестановка по табл. 1 входной последовательности битов блока T_j. В результате бит 58 входной последовательности становится битом 1, бит 50 – битом 2 и т. д.

Таблица 1

Начальная и конечная перестановки DES

Начальная перестановка DES															
58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7
Конечная перестановка DES															
40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

2. Разделение переставленной последовательности битов на две последовательности: L_0 (биты 58, 50, 42,..., 8) и R_0 (биты 57, 49, 41, ..., 7), каждая из которых содержит 32 бита.

3. Итеративный процесс шифрования по формулам

$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \ (+) F(R_{i-1}, K_i), \ \ i = 1, 2, ..., 16. \end{cases} \tag{3}$$

4. Конечная перестановка по табл. 1. На последнем шаге итерации будут получены последовательности L_{16} и R_{16}, которые объединяются в 64-битовую последовательность $L_{16}R_{16}$. В полученной последовательности биты переставляются в соответствии с табл. 1. Как легко увидеть, данная перестановка является обратной по отношению к начальной, т. е. все биты снова занимают свои места, как в исходном сообщении.

5. Полученная последовательность из 64 бит и будет являться зашифрованной исходной последовательностью T_j.

Функция F называется функцией шифрования. Ее аргументами являются последовательность R, полученная на предыдущем шаге, и 48-битовый ключ K_i, являющийся результатом функции преобразования 64-битового ключа шифра. Подробно функция шифрования и алгоритм получения ключей K_i описаны ниже.

Процесс дешифрования данных является инверсным по отношению к процессу шифрования. Все действия должны быть выполнены в обратном порядке. Это означает, что расшифровываемые данные сначала переставляются в соответствии с конечной перестановкой (табл. 1), а затем над последовательностью бит $R_{16}L_{16}$ выполняются те же действия, что и в процессе шифрования, но в обратном порядке. Итеративный процесс дешифрования может быть описан формулами

$$\begin{cases} R_{i-1} = L_i, \\ L_{i-1} = R_i \ (+) F(L_i, K_i), \quad i = 16, 15, ..., 1. \end{cases} \tag{4}$$

На последнем шаге итерации будут получены последовательности L_0 и R_0, которые объединяются в 64-битовую последовательность L_0R_0. В полученной последовательности 64 бита переставляются в

соответствии с начальной перестановкой (табл. 1). Результат преобразования – исходная последовательность битов (расшифрованное 64-битовое значение).

Функция шифрования DES

Функция шифрования $F(R,K)$ схематически показана на рис. 3. Для вычисления значения функции F используется функция E (расширение 32 бит до 48), функции $S1$, $S2$, ..., $S8$ преобразования 6-битового числа в 4-битовое и функция P (перестановка битов в 32-битовой последовательности). Приведем определения этих функций. Аргументами функции шифрования являются R (32 бита) и K (48 бит).

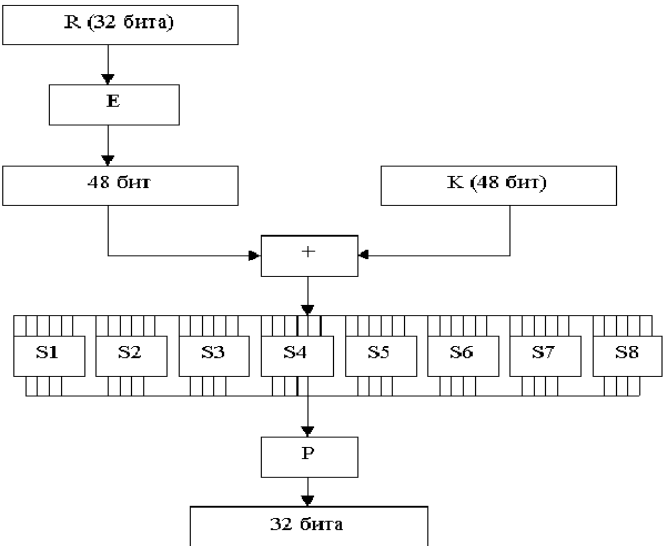

Рис. 3. Структурная схема вычисления функции $F(R_{i-1}, K_i)$

Результат функции $E(R)$ есть 48-битовое число, складывающиеся по модулю 2 с числом K. Таким образом, получается 48-битовая последовательность, рассматриваемая как конкатенация восьми строк длиной по 6 бит (т. е. $B_1B_2B_3B_4B_5B_6B_7B_8$). Результат функции $S_i(B_i)$ – 4-битовая последовательность, которую будем обозначать V_i. В результате конкатенации всех восьми полученных последовательностей V_i имеем 32-битовую последовательность $V = V_1V_2V_3V_4V_5V_6V_7V_8$. Наконец,

ОГЛАВЛЕНИЕ

Котов Юрий Алексеевич

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

СТАНДАРТНЫЕ ШИФРЫ. ШИФРЫ С ОТКРЫТЫМ КЛЮЧОМ

Учебное пособие

Редактор *М.О. Мокшанова*
Выпускающий редактор *И.П. Бровановa*
Корректор *Л.Н. Кинщт*
Дизайн обложки *А.В. Ладыжская*
Компьютерная верстка *Н.В. Гаврилова*

Подписано в печать 27.11.2017. Формат 60×84 1/16. Бумага офсетная. Тираж 50 экз.
Уч.-изд. л. 3,95. Печ. л. 4,25. Изд. № 172. Заказ № 1515. Цена договорная

Отпечатано в типографии
Новосибирского государственного технического университета
630073, г. Новосибирск, пр. К. Маркса, 20