Симметричный блочный алгоритм шифрования, использующий преобразования Фейстеля

До недавнего времени наиболее популярным стандартным симметричным алгоритмом шифрования данных был ***DES*** (Data Encryption Standard). Алгоритм разработан фирмой IBM и в 1976 году был рекомендован Национальным институтом стандартов и технологий США (NIST) к использованию в открытых секторах экономики. И хотя сейчас на смену DES пришел другой симметричный алгоритм AES, будет весьма поучительно рассмотреть некоторые приемы, использованные в алгоритме DES, поскольку они носят достаточно универсальный характер и используются в других симметричных алгоритмах.

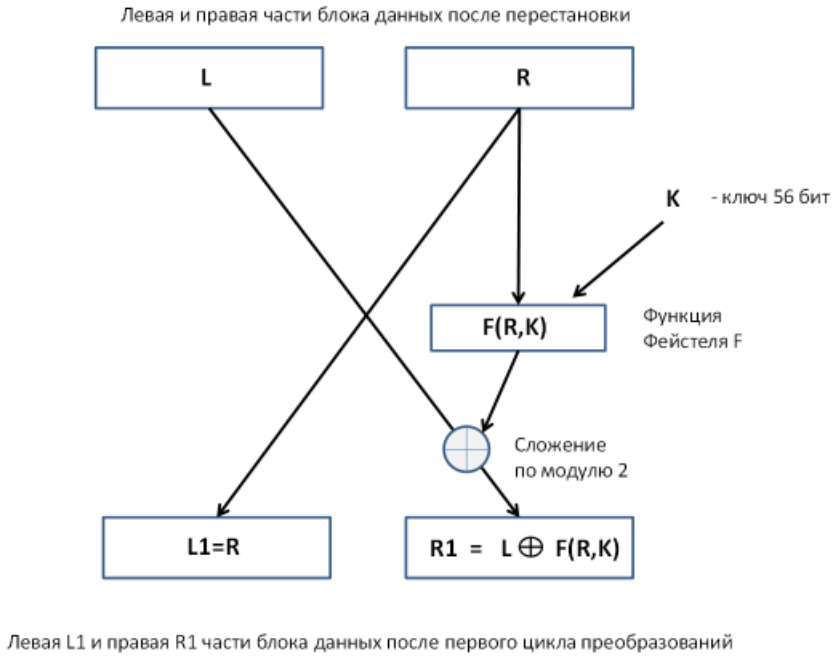

Рис. 1. Первый цикл преобразования Фейстеля.

Суть этого алгоритма заключается в следующем (рис. 1). Данные шифруются *поблочно*. Перед шифрованием любая форма представления данных преобразуется в числовую. Числа получают путем применения любой открытой процедуры преобразования блока текста в число. Пусть требуется зашифровать текст – RUSSIA2013. Исходный текст представим в числовой форме, например, путем замены каждой буквы ее шестнадцатеричным кодом ASCII:

R	U	S	S	I	A	2	0	1	3
1010010	1010101	1010011	1010011	1001001	1000001	0110010	0110000	0110001	0110011

После слияния получаем следующую последовательность длиной 70 бит:

1010010101010110100111010011100100110000010110010011000001100010110011

На вход шифрующей функции данные поступают блоками размером 64 бита, в этом примере мы ограничимся одним первым блоком, отбросив последние 6 бит:

10100101010101101001110100111001001100000101100100110000001100010

В алгоритме шифрования DES можно выделить несколько смысловых этапов.

1. Начальная перестановка

Перестановка битов в блоке данных выполняется в соответствии с правилом, заданным таблицей 1. То есть на место 1-го бита исходного текста ставится его 58-ой бит, на место 2 бита – 50-ый и так далее. (Подобные таблицы используются и на других этапах алгоритма DES, каждая из них содержит фиксированные для алгоритма DES значения. Эти таблицы являются неотъемлемыми компонентами алгоритма шифрования DES.)

Табл. 1. Начальная перестановочная таблица алгоритма DES

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

В результате перестановки получаем первый блок в следующем виде:

10100010011111110000001110010110100000101110110010010110010000010

2. Циклические преобразования Фейстеля.

После выполнения перестановки блок делится на две равные части по 32 бита каждая. Обозначим левую часть **L** и правую часть - **R.**

L= 10100010011111110000001110010110 1	**R**= 00000101110110010010110010000010

Алгоритм DES предполагает выполнение 16 циклов преобразований, называемых циклами Фейстеля, которые собственно и представляют собой процедуру шифрования. В каждом цикле выполняется преобразование данных, полученных в предыдущем цикле.

Рассмотрим первый цикл Фейстеля (рис.1), для которого исходными данными являются левая L и правая R части блока данных после перестановки. Результатом первого цикла являются новые значения левой части L1 и правой части R1.

L1 получается простой заменой на R.

Получение правой части R1 оказывается сложнее. Для этого сначала вычисляется функция Фейстеля F, параметрами которой являются исходное значение правой части R и секретный ключ K.

3. Преобразование ключа

Исходное значение секретного ключа должно иметь 64 бита. Затем по определенной схеме из битовой последовательности убирается 8 бит, так чтобы каждый байт ключа содержал нечетное число единиц. Эти биты используются для контроля целостности 56-битного ключа при хранении и передаче. Затем для оставшихся 56 бит ключа делаются перестановки, которые задаются таблицей, подобной табл. 1., но имеющей другие значения в ячейках. Далее выполняется циклический сдвиг всей последовательности влево на 1 позицию. (Сдвиг на 1 позицию выполняется также в циклах Фейстеля с номерами 2, 9 и 16; для остальных циклов последовательность сдвигается на 2 позиции.) Из полученной в результате сдвига 56-битовой последовательности убираются 8 бит, позиции которых указаны в еще одной таблице. В результате получается 48-битовый ключ K.

4. Вычисление функции F

Функция F вычисляется путем выполнения следующих действий:

- Расширение правой части R, состоящей из 32 битов, до 48. Это делается путем дублирования некоторых битов, позиции которых определены в специальной таблице алгоритма DES.
- Сложение по модулю 2 (операция XOR) ключа K и правой части R
- Преобразования 48-битовой суммы в 6-битовые блоки и замена их на 4-битовые по определенной в алгоритме схеме. В результате получается 32-битовая последовательность
- Перестановка битов в полученной последовательности

Затем вычисляется новое значение правой части R1 как сумма по модулю 2 значений функции F и левой части L.

На этом заканчивается первый цикл и происходит переход к следующему, второму циклу (рис. 2.).

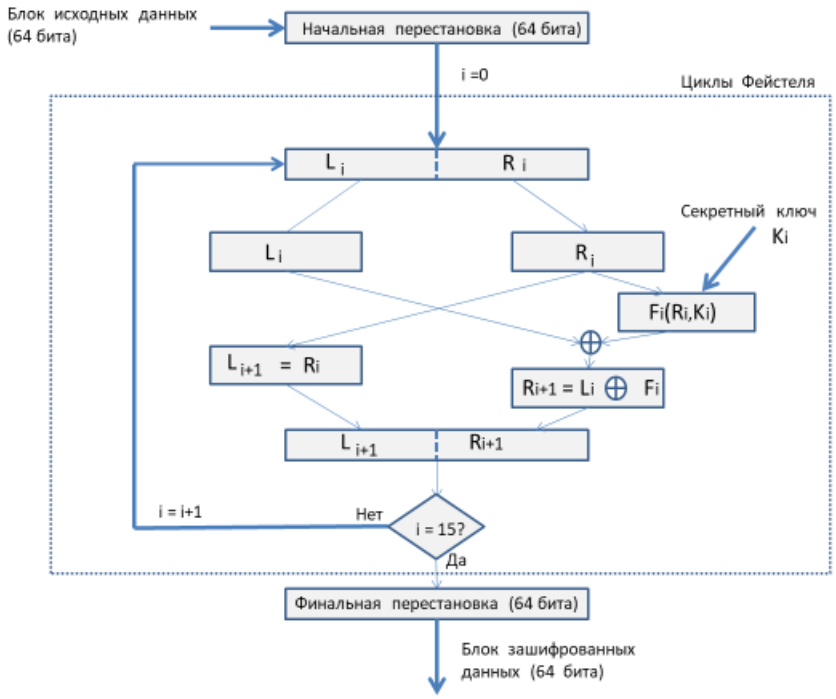

Рис. 2. Схема шифрования по алгоритму DES

5. Финальная перестановка

После того как будут выполнены все 16 циклов, делается финальная перестановка 64-битовой последовательности {L15,R15}. Эта перестановка является обратной по отношению к начальной, задаваемой таблицей 1. Так, например, на место 1 бита последовательности {L15,R15} ставится ее 40-ой бит, на место 2 бита – 8-ой бит и т.д.

Результат перестановки является зашифрованным значением исходного блока данных. Полный шифрованный текст получается путем слияния результатов шифрования для всех блоков исходного текста.

Процедура дешифрования выполняется как обратный процесс: выполняется перестановка, обратная финальной, откручиваются назад 16 циклов Фейстеля, в каждом из которых активно используется секретный ключ, и в завершение выполняется перестановка, обратная начальной.