УДК 681.3.06: 519.248.681

В. И. ДОЛГОВ, д-р техн. наук, В. И. РУЖЕНЦЕВ, М. А. ФЕДОТОВ,
А. П. МЕЛЕЦКИЙ, М. В. ПИНЧУК

MDES-128 С ТАБЛИЦАМИ ПОДСТАНОВОК СЛУЧАЙНОГО ТИПА

Американский стандарт шифрования DES является одним из наиболее популярных и известных симметричных шифров. Вот уже более 20 лет этот алгоритм находится в центре внимания специалистов. Его можно считать наиболее глубоко и досконально исследованным. Несмотря на многочисленные критические замечания, он выдержал проверку временем и сохранил авторитет одного из надежных для прошедшего этапа инструментов защиты информации во многих государственных и коммерческих структурах (автоматизированных системах управления). Сегодня, однако, прогресс в области вычислительной техники ставит на повестку дня вопрос замены этого стандарта новым. Размер ключа DES стал слишком мал для современных приложений. Не так давно в работах [1,2] показано, что, затратив около 1 млн. $ (против 20 млн. $, названных в работе 1977 года [3]), возможно создание специализированного аппаратного устройства, которое за время менее 1 часа выполнит атаку на ключ DES методом полного перебора. Можно напомнить и свежий пример, когда ключ DES был найден методом простого перебора с использованием инструментария, распространенного в Internet. Таким образом, и при использовании возможностей программных средств 56-битный ключ также может уже не обеспечить надежной защиты.

Здесь следует заметить, что на проблему слишком маленького размера ключа было обращено внимание почти сразу же после публикации DES [3]. Поэтому, для случаев, когда есть основания опасаться очень серьезного криптоанализа, уже давно обсуждаются возможности увеличения длины используемого ключа путем композиции DES шифрований. Простейшей из таких возможностей является последовательное использование дважды одного и того же шифра, однако для алгоритма DES с фиксированными таблицами *S*-блоков двойное шифрование с независимым выбором ключей не приводит в теоретическом плане к повышению стойкости процедуры шифрования. В этом случае существует способ оптимизации переборной процедуры, называемый встречной атакой [4], который требует для криптоанализа число шагов, пропорциональное 2^n, где n – длина ключа, т.е. совпадающее с числом возможных ключей для однократного DES (правда, взамен требуется машинная память такого же порядка).

Чаще DES используют в режиме тройного шифрования, при котором открытый текст шифруется 3 раза с тремя независимыми ключами. Данный метод получил название тройной DES. Ряд недостатков различных вариантов этого подхода детально обсуждаются в [5] и других работах. Тем не менее, Комитет X9.F.1 Американского Национального института Стандартов (ANSI) работал над принятием наборов режимов для трехкратного (тройного) шифрования с использованием DES [6.7].

Отметим также еще раз работу [5], в которой предлагается 6-ти цикловый шифр, который использует DES в качестве цикловой функции. Результатом является 128-битный блочный шифр, который назван DEAL–A, с 64-битными циклическими подключами, которые получаются из выбранного пользователем ключа, согласно алгоритму генерации ключей. Система так же быстра, как тройной DES, в котором используется 6 шифрований для того, чтобы зашифровать два 64-битных блока открытого текста. Заметим, наконец, что 128-битный блочный шифр DEAL–A, строящийся на основе DES, предлагался кандидатом на NIST AES стандарт.

Заключая приведенный небольшой анализ подходов к композиции шифров DES, следует констатировать, что во всех представленных выше случаях приходится мириться с понижением быстродействия криптографических преобразований – характеристикой, которая представляется одной из наиболее ценных для симметричных шифров.

Мы хотим открыть новую страницу в изучении и исследовании возможностей использования ставшей уже классической схемы преобразований, примененной в стандарте шифрования данных DES. Основное внимание настоящей работы сосредотачивается на развитии подхода, позволяющего преодолеть одновременно все ограничения стандарта DES – малую длину шифруемого блока и ключа, а также уязвимость стандарта к атакам дифференциального и линейного криптоанализов.

Для построения усовершенствованного симметричного шифра предлагается взять за основу идею, использованную при построении самого стандарта DES, но реализовать теперь ее для длины блока, равной 128 битам. Кроме того, в цикловую функцию шифра DES предлагается ввести дополнительную операцию – параметрический циклический сдвиг. Эта операция позволяет по-новому решить задачу обеспечения безопасности шифра.

Будем в дальнейшем называть рассматриваемый вариант построения новой процедуры шифрования DEA-128. В шифре DEA-128 в качестве левого и правого полублоков схемы Фестеля будут выступать уже 64-битные полублоки. Конечно, потребуется теперь использовать таблицу из 16 различных S-блоков и осуществить модификацию всех остальных преобразований для увеличенной в два раза длины блока: начальной и конечной перестановок IP и IP^{-1}, расширяющего преобразования E. таблицы перестановки P и алгоритма получения подключей K_i, $i = 1,2,\ldots,16$ [8]. Сосредоточим сначала внимание на детальном описании параметров алгоритма DEA-128.

Итак, в алгоритме DEA-128 входной блок A, состоящий из 128 двоичных символов, разбивается на две равные части по 64 бита: левый полублок L_0 и правый полублок R_0. Затем, как и в стандарте, осуществляется 16 циклов преобразования сообщения $A = (L_0R_0)$, так что в i-м цикле слово $(L_{i-1}R_{i-1})$ преобразуется в (L_iR_i) по правилам:

$$L_i = R_{i-1},\ R_i = L_{i-1} \oplus f(R_{i-1},K_i,K'_i),$$

где символ $\oplus$ обозначает операцию побитного суммирования по модулю 2; $f(R_{i-1},K_i,K'_i)$ – цикловая функция; (L_iR_i) – операция конкатенации (объединения) блоков L_i и R_i, $i = 0,1,\ldots,16$.

В цикловой функции $f(R_{i-1},K_i,K'_i)$ вычисление начинается с так называемого расширения, преобразующего 64 битный полублок R_i в 96-битный в соответствии с расширяющей таблицей E (фиксированного вида), которая, фактически, дополнительно вставляет копии 32 позиций. Полученные 96 бит гаммируются (побитно суммируются) с 96 битами подключа (K_i,K'_i), представляющего собой объединение двух 48-битных подключей, которые формируются в соответствии с алгоритмом развертывания подключей, используемым в самом стандарте DES. Результат гаммирования разбивается на 16 блоков по 6 бит, поступающих на S-блоки $S_1,S_2,\ldots,S_{16}$. В каждом из S-блоков, также как и в стандарте DES, входные 6 бит заменяются 4-мя выходными.

Шестнадцать 4-битных двоичных блоков, поступающих с выходов S-блоков, образуют 64-битный полублок. Двоичные элементы этого полублока подвергаются P-перестановке, задаваемой фиксированной таблицей.

Завершая описание основных операций DEA-128, остается заметить, что по аналогии со стандартом процедура шифрования начинается с начальной фиксированной перестановки IP и завершается применением к полученному результату обратной перестановки IP^{-1}.

Напоминаем также, что в самом конце выполнения всех 16 циклов алгоритма DES левый и правый полублоки меняются местами, так что результатом работы алгоритма DEA-128 является $E_{K,K}(A) = (R_{16}L_{16})$.

Приведем теперь конкретные параметры и характеристики модифицированных таблиц перестановок и подстановок, использованных в DEA-128.

Начальная перестановка IP, построенная по аналогии с идеей построения подстановки стандарта DES, представлена в виде табл. 1, где i_A обозначает номер позиции входного блока, а $IP(i_A)$ – номер позиции, в которой i_A-й бит входного блока окажется в результате перестановки.

Таблица 1

$IP(i_B)$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
I_B	114	98	82	66	50	34	18	2	116	100	84	68	52	36	20	4
$IP(i_B)$	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
I_B	118	102	86	70	54	38	22	6	120	104	88	72	56	40	24	8
$IP(i_B)$	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
i_B	122	106	90	74	58	42	26	10	124	108	92	76	60	44	28	12
$IP(i_B)$	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
i_B	126	110	94	78	62	46	30	14	128	112	96	80	64	48	32	16
$IP(i_B)$	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
I_B	113	97	81	65	49	33	17	1	115	99	83	67	51	35	19	3
$IP(i_B)$	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
I_B	117	101	85	69	53	37	21	5	119	103	87	71	55	39	23	7
$IP(i_B)$	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112
I_B	121	105	89	73	57	41	25	9	123	107	91	75	59	43	27	11
$IP(i_B)$	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
I_B	125	109	93	77	61	45	29	13	127	111	95	79	63	47	31	15

Математически эти преобразования можно представить в виде следующих двух соотношений:

$IP(i_A) = [2\cdot(64+1)-16\cdot i_A](\mathrm{mod}\ 130)$ для $IP(i_A) \le 64$ и

$IP(i_A) = [2\cdot(64+1)-16\cdot(i_A-64)-1](\mathrm{mod}\ 130)$ для $IP(i_A) > 64$

против $IP(i_A) = [2\cdot(32+1)-8\cdot i_A](\mathrm{mod}\ 66)$ $IP(i_A) \le 32$ и

$IP(i_A) = [2\cdot(32+1)-8\cdot(i_A-32)-1](\mathrm{mod}\ 66)$ $IP(i_A) > 32$ для стандартного DES.

Завершающая обратная перестановка представлена в табл. 2, где i_B обозначает номер позиции в блоке шифртекста, полученного в результате выполнения 16 циклов, а $IP^{-1}(i_B)$ – номер позиции, на которую поступает i_B-й бит указанного блока в результате перестановки.

Расширяющая перестановка E построена по принципу, используемому в алгоритме DES, и преобразует 64-битный полублок в 96-битный в соответствии с табл. 3, в которой j обозначает номер позиции бита в R_{i-1}, а j_E – номер позиции, куда поступает j-й бит в результате выполнения E-перестановки. В случае, когда j-й бит поступает в две позиции, номера позиций перечислены через запятую.

Таблица 2

$IP^{-1}(i_B)$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
i_B	72	8	80	16	88	24	96	32	104	40	112	48	120	56	128	64
$IP^{-1}(i_B)$	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
i_B	71	7	79	15	87	23	95	31	103	39	111	47	119	55	127	63
$IP^{-1}(i_B)$	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
i_B	70	6	78	14	86	22	94	30	102	38	110	46	118	54	126	62
$IP^{-1}(i_B)$	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
i_B	69	5	77	13	85	21	93	29	101	37	109	45	117	53	125	61
$IP^{-1}(i_B)$	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
i_B	68	4	76	12	84	20	92	28	100	36	108	44	116	52	124	60
$IP^{-1}(i_B)$	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
i_B	67	3	75	11	83	19	91	27	99	35	107	43	115	51	123	59
$IP^{-1}(i_B)$	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112
I_B	66	2	74	10	82	18	90	26	98	34	106	42	114	50	122	58
$IP^{-1}(i_B)$	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
i_B	65	1	73	9	81	17	89	25	97	33	105	41	113	49	121	57

Таблица 3

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
j_E	2,96	3	4	5,7	6,8	9	10	11,13	12,14	15	16	17,19	18,20	21	22	23,25
J	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
j_E	24,26	27	28	29,31	30,32	33	34	35,37	36,38	39	40	41,43	42,44	45	46	47,49
j	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
j_E	48,50	51	52	53,55	54,56	57	58	59,61	60,62	63	64	65,67	66,68	69	70	71,73
j	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
j_E	72,74	75	76	77,79	78,80	81	82	83,85	84,86	87	88	89,91	90,92	93	94	1,95

Для задания нелинейных S подстановок использовались 16 таблиц размером 4×16 каждая, отобранные в соответствии с методикой, предложенной в [9], т.е. при их формировании учитывалось выполнение критериев случайности.

Завершающим преобразованием в шифрующей функции алгоритма DES является P-перестановка. Она относится к перестановкам случайного типа (отвечает требованиям случайности [10]), а также удовлетворяет дополнительным ограничениям [11], представленным специалистами фирмы IBM – разработчиками стандарта: каждый из четырех выходов любого S-блока распределяется по позициям входов различных S-блоков на следующем цикле.

Для более полного соответствия DEA-128 с DES-64 нами применена P-перестановка, представляющая собой сдвоенную стандартную перестановку: биты с 1 по 33 преобразуются в соответствии

со стандартной перестановкой, а перестановка для битов с 33 по 64 рассчитывается по простой формуле:

$$P_{128}(i) = P_{64}(i) + 32.$$

Приведенный вариант перестановки был изучен, протестирован и при проверке лавинного эффекта показал лучшие результаты по сравнению с другими вариантами. Ниже приведена табл. 4 с *P*-перестановкой, используемой в обсуждаемом шифре.

Таблица 4

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

Предлагаемые изменения в классической схеме криптопреобразований DES

Увеличение только длины шифруемого блока при стандартной схеме криптопреобразований может повлечь за собой только ухудшение показателей безопасности нового алгоритма, а также создаст возможность применения к нему старых, проверенных на DES-64, атак.

Стараясь радикально не менять стандартную схему шифрования, для защиты от вышеперечисленных криптоаналитических атак мы ввели в каждый цикл алгоритма всего одну дополнительную нелинейную операцию. Эта операция названа нами "параметрический циклический сдвиг".

Порядок осуществления дополнительной операции следующий: в каждом цикле шифрования (дешифрования) после прохождения правого полублока через шифрующую функцию, производится его циклический сдвиг влево на число, определяемое младшими 6-ю битами этого же полублока. В остальном порядок выполнения операций не изменяется.

На рис.1 представлен модифицированный цикл DEA-128.

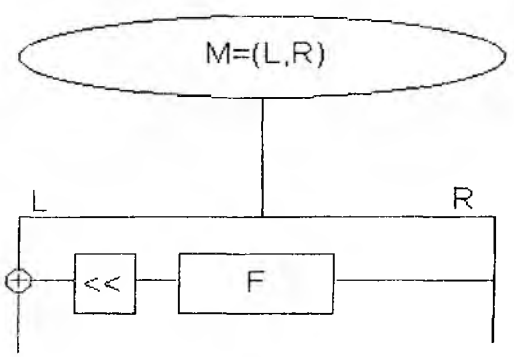

Рис. 1

Как показывает анализ и расчеты, параметрический сдвиг существенно уменьшает вероятности построения дифференциальных и линейных характеристик, что делает атаки дифференциального и линейного криптоанализов неэффективными.

Проверка статистической безопасности алгоритма шифрования данных DEA-128

Проверка статистической безопасности предлагаемой версии алгоритма шифрования выполнялась по методике, изложенной в работе [10].

Использовались четыре основных показателя статистической безопасности, традиционные для симметричных блочных шифров:

1. Число циклов алгоритма, начиная с которого криптограммы, полученные шифрованием двух, отличающихся на один бит блоков данных (открытых текстов), становятся устойчиво независимыми (в том смысле, что при дальнейшем увеличении числа циклов они остаются независимыми). Другими словами, необходимо было определить число циклов в алгоритме шифрования, начиная с которого изменение одного бита открытого текста приводит к изменению криптограммы приблизительно в половине битов. Этот показатель отражает качество, так называемого, лавинного эффекта.

2. Число циклов шифрования, при котором один и тот же открытый текст, зашифрованный на ключах, отличающихся одним битом, порождает устойчиво независимые (некоррелированные) криптограммы.

3. Коэффициент сжатия шифрованного текста при использовании процедуры архивирования Лемпела-Зива.

4. Корреляция входа-выхода, т.е. степень статистической связи открытого текста с соответствующим ему закрытым текстом.

Результаты, полученные в ходе статистических экспериментов, иллюстрируют табл. 5, 6. В табл. 5 приведены типичные значения математического ожидания числа единичных (ненулевых) бит в побитной сумме по модулю 2 пар, полученных на k-том цикле криптограмм, открытые тексты или ключи которых отличаются одним битом.

Таблица 5

№ цикла	Изменение 1 бита текста	Изменение 1 бита ключа
0	4,563	2,155
1	17,108	17,220
2	37,207	43,393
3	54,330	59,917
4	62,138	63,521
5	**63,911**	63,962
6	64,065	64,075
7	64,135	63,829
8	64,283	63,758
9	64,084	63,898
10	63,843	63,843
11	63,912	63,826
12	63,943	63,765
13	64,041	64,081
14	63,951	64,227
15	63,870	63,914
16	63,870	63,914

При исследовании показателей сжатия текстов с помощью процедуры архивирования Лемпела-Зива исследовались тексты трех категорий: обычный EXE-файл, текст редактора Microsoft Word и обычный текстовый файл. Результаты этих исследований, иллюстрирует табл. 6.

Таблица 6

Тип файла	Сжатие, %
Exe-файл	1,3-12,9
Документ Microsoft Word	43
Обычный текст	1,60

Статистическая независимость выходных битов от входных битов, в соответствии с полученными результатами, наблюдается при использовании 6 и более циклов шифрования, как и в случае стандартного шифра DES.

Во всех случаях обеспечивается сжатие шифрованного текста по Лемпелу-Зиву, аналогичное сжатию, достигаемому при использовании стандартной процедуры шифрования DES.

Коэффициент корреляции открытого и соответствующего ему шифрованного текста не превышает значения 0,001.

Рассматриваемая версия DES подобной процедуры шифрования обеспечивает удельную скорость криптопреобразований, превышающую более чем в два раза тройной DES и 128-битный блочный шифр DEAL–A, строящийся на основе DES, предлагаемый кандидатом на NIST AES стандарт. Этот момент может оказаться принципиальным для многих приложений.

Остается отметить, что использование процедуры параметрического сдвига в принципе позволяет по-новому подойти к обеспечению характеристик стойкости алгоритмов шифрования к атакам дифференциального и линейного криптоанализов. В частности, для рассмотренного варианта построения шифра отпадает необходимость выполнения одного из наиболее жестких требований к S-блокам стандарта DES – запрета однобитных переходов [12]. Вместе с тем, в рассмотренном варианте применения процедуры параметрического сдвига сохраняется необходимость запрета при отборе S-блоков переходов обнуляющего типа [11]. Более детальный анализ защищенности рассмотренной модифицированной процедуры шифрования от атак дифференциального и линейного криптоанализа выходит за рамки настоящей работы. Этому вопросу мы посвятим отдельное исследование.

Мы продолжаем изучать устойчивость нашей версии построения шифра и от других возможных атак. Однако основная идея – введение в процедуру криптографических преобразований DES подобных шифров дополнительной операции параметрического циклического сдвига – открывает возможность использования в качестве S-блоков в этих шифрах таблиц подстановок случайного типа (прошедших тесты на случайность) и вселяет в нас уверенность, что развиваемый подход может оказаться

достаточно эффективным и в других случаях. В частности, одним из перспективных решений в свете развиваемого подхода может стать использование таблиц *S*-блоков как еще одного секретного параметра шифра (подобно алгоритму ГОСТ 28147-89), что позволит добиться дальнейшего наращивания показателей безопасности.

Список литературы: 1. *Wiener M.J.* Efficient DES key search. Technical Report TR-244. School of Computer Science. Carleton University. Ottawa. Canada. May 1994. Presented at the Rump Session of CRUPTO'93. 2. *Wiener M.J.* Efficient DES key search - an update. CryptoBytes, 3(2): 6-6, 1998. 3. *Diffie W., Hellman M.* Exhaustive cryptanalysis of the NBS data encryption standard. Computer. P. 74-84. 1977. 4. *Вербицький О.В.* Вступ до криптології. Видавництво наук.-техн. літератури. Львів. 1998. 5. *Knudsen L.R.* DEAL – A 128-bit Block Cipher. 1998. P. 1-9. 6. *ANSI X9.F.1.* TDEA modes of operation. Draft 5.5. X9.52. March 29, 1996. 7. *NIST. AES announcement.* Draft. June 15, 1997. 8. *Барсуков В.С., Дворянкин С.В., Шеремет И.А.* Безопасность связи в каналах телекоммуникаций. М. Россия. 1993. Т.20. 123 с. 9. *Горбенко И.Д., Лисицкая И.В.* Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 2847-89 // Радиотехника. 1997. Вып 103. С. 121–130. 10. *Горбенко И.Д., Лисицкая И.В., Коряк А.С.* Анализ стойкости алгоритма ГОСТ 28147-89 при использовании подстановок случайного типа. // Радиоэлектроника и информатика. 1998. №1 (02). С. 39–43. 11. *Schneier B.* Applied Cryptography. Second Edition: protocols, algorithms and source code in C. Published by John Wiley & Sons. Inc, New York: Chichester Brisbane Toronto Singapore, 1996 – 158 p. 12. *Лисицкая И.В., Коряк А.С., Олейников Р.В.* К вопросу построения случайных *S*-блоков для алгоритма DES. Критерии отбора *S*-блоков. // Радиоэлектроника и информатика. 1999. №3. С. 94–100.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 6.03.2001