Московский Физико-Технический Институт
(Государственный Университет)

DEAL. Data Encryption Algorithm with Lager blocks.

Эссе по курсу “Теория защиты информации”
студента 013 группы
Грехова Алексея.

Москва 2004

DEAL. Data Encryption Algorithm with Lager blocks.

1. Введение.

DES (или DEA) – блочный шифр с размером блока 64 бита и 64-х битным ключом, в котором эффективны 56 бит. Это – итеративный 16-и цикловой шифр, в нем шифр-текст вычисляется путем итеративного приложения цикловой функции к открытому тексту. DES имеет так называемую Фейстелеву структуру.

Для современных приложений размер ключа DES стал слишком мал. Показано, что сконструировать специализированное устройство, способное произвести исчерпывающий поиск ключа DES в среднем всего за 3.5 часа, будет стоить примерно 1 миллион US$. К тому же, недавно было показано, что и от программных атак ключ размером 56 бит не предоставляет значительной защиты – ключ DES был найден путем исчерпывающего поиска средствами распространенными по Internet'у.

Был предложен r-цикловой Фейстелев шифр, использующий DES в качестве цикловой функции. В результате получается шифр с размером блока 128 бит и $r \cdot 64$ битами цикловых ключей, получаемых по алгоритму расписания ключей. Расписание ключей разработано так, что размер ключа может принимать одно из трех различных значений: 128, 192 или 256 бит. Мы рекомендуем при первых двух размерах ключа положить $r = 6$, а при размере ключа 256 бит $r = 8$. Ниже мы объясним, почему мы рекомендуем $r \geq 6$. Если биты проверки четности каждого байта ключа не используются при шифровании, как это происходит в DES, действующие размеры ключей уменьшаются до 112-и, 168-и и 224-х бит соответственно. Исчерпывающий поиск ключа еще совершенно невозможен (см., например, обсуждение размеров ключей в). К тому же, для успешной атаки по подобранному шифр-тексту необходимо ввести порядка 2^{64} блоков шифр-текста. Скорость предложенного нами шифра такая же, как у тройного DES'а, если использовать 6 зашифрований для закрытия двух блоков открытого текста по 64 бита, более того, его можно применять с использованием существующих средств DES.

Национальный Институт Стандартов и Технологии (NIST) недавно объявил о намерении стандартизировать новый алгоритм шифрования, Advanced Encryption Standart, как замену DES. Заявление NIST о том, что до того, как AES будет готов, пройдет несколько лет, и что они намерены признать «Тройной DES-алгоритм, раз он принят стандартом ANSI», делает инициативу ANSI даже более важной.

2. DEAL.

DEAL (Data Encryption Algorithm with Larger blocks – Алгоритм Шифрования Данных с Укрупненными блоками) является 128-и битным блочным шифром с размерами ключа 128, 192 и 256 бит, что далее здесь будет обозначаться DEAL-128, DEAL-192 и DEAL-256 соответственно. Все версии могут использоваться в любом из четырех стандартных режимах DES'a. Мы начнем с описания работы DEAL в режиме ECB. Пусть $C = E_B(A)$ означает зашифрованное DES значение 64-х битного A на ключе B, и пусть $Y = EA_Z(X)$ означает зашифрование DEAL 128-и

битного X на ключе Z. Открытый текст P разделяется на блоки P_i по 128 бит каждый, $P = P_1, P_2, \ldots, P_n$. Расписание ключей принимает ключ K и возвращает r ключей DES RK_i, где $i = 1, \ldots, r$, как описано ниже. Обозначим X^L и X^R левую и правую части X соответственно. Шифр-текст вычисляется следующим образом. Положим $X_0^L = P_i^L$, $X_0^R = P_i^R$ и вычислим для $j = 1, \ldots, r$

$$X_j^L = E_{RK_j}(X_{j-1}^L) \oplus X_{j-1}^R \quad (1)$$

$$X_j^R = X_{j-1}^L . \quad (2)$$

Положим $C_i = X_r^L \| X_r^R$. На рис. 1 показан один цикл DEAL. Для DEAL-128 и DEAL-192 мы предлагаем использовать 6 циклов, т. е. r = 6. Однако, как мы увидим ниже, этого может быть недостаточно для DEAL-

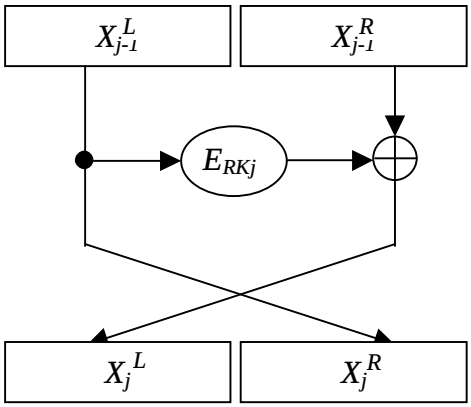

Рисунок 1: Один цикл DEAL.

256, здесь предлагается использовать 8 циклов, r = 8. Представляется, что версия с размером ключа 256 бит используется только когда требуется особенно сильное зашифрование.

Заметим, что последнем цикле DEAL половины блока местами меняются. Причина в следующем: правая часть шифр-текста C_i не шифруется в последнем цикле i-ого зашифрования, и только левая часть входа i + 1-ого зашифрования (который равен $C_i \oplus P_{i+1}$) шифруется на последнем цикле. Т. о. правая часть C_i осталась бы не перезашифрованной два цикла. Это может дать поле деятельности злоумышленникам, тем более, что шифр состоит всего из 6-и или 8-и циклов. Заметим, что аналогичное свойство есть и у DES в режиме CBC. Правда, похоже это труднее было бы использовать, ведь у DES 16 циклов. Позволим себе отметить, что обмен местами правой и левой частей на последнем цикле не влияет на стойкость блочного шифра в режиме ECB.

Работа режима CBC более подробно описана в [16]. Итак, обозначим блоки открытого текста по 128 бит $P_1, P_2, \ldots, P_n$ и $C_1, C_2, \ldots, C_n$ – соответствующие им блоки шифр-текста. Тогда:

$$C_i = EA_K(C_{i-1} \oplus P_i),$$

где C_0 – начальное значение.

В DES начальная перестановка IP первой применяется к открытому тексту, и аналогично перед выходом шифр-текст пропускается через обратную к ней IP^{-1}. Возможно увеличить скорость DEAL, если убрать из используемого DES эти начальную и конечную перестановки. Легко

показать, что для получения корректной реализации DEAL'а IP должна быть приложена к обоим частям открытого текста перед зашифрованием, а IP^{-1} – к обоим частям шифр-текста.

На вход расписания ключей подается s ключей DES, K_1, … , K_s, для s = 2, 3, 4, каждый по 64 бит (включая 8 проверочных бит, старших бит каждого байта), на выходе получается r ключей DES, RK_i. Мы используем общий метод, приложимый ко всем трем размерам ключа. Во-первых расширяем s ключей до r ключей, путем повторения и XOR'ения с новой константой для каждого нового повторения. Зашифровываем расширенный список ключей DES'ом в режиме CBC с фиксированным ключом и нулевым начальным значением. Из полученных блоков шифр-текста и формируются подключи RK_i. Далее мы приводим точные определения каждого из расписаний ключей, здесь K = 0x1234 5678 90ab $cdef_x$ (шестнадцатеричное число) – фиксированный ключ DES.

В DEAL-128 подключи генерируются следующим образом:

$$
\begin{aligned}
RK_1 &= E_K(K_1),\\
RK_2 &= E_K(K_2 \oplus RK_1),\\
RK_3 &= E_K(K_1 \oplus \langle 1\rangle \oplus RK_2),\\
RK_4 &= E_K(K_2 \oplus \langle 2\rangle \oplus RK_3),\\
RK_5 &= E_K(K_1 \oplus \langle 4\rangle \oplus RK_4),\\
RK_6 &= E_K(K_2 \oplus \langle 8\rangle \oplus RK_5),
\end{aligned}
$$

где $\langle i\rangle$ – 64-х битное целое число, в котором i – 1-ый бит (индексация идет с 0) установлен, а остальные очищены. Например, $\langle 1\rangle$ может быть представлено как шестнадцатеричное "$0x8000\ 0000\ 0000\ 0000_x$".

В DEAL-192 подключи генерируются следующим образом:

$$
\begin{aligned}
RK_1 &= E_K(K_1),\\
RK_2 &= E_K(K_2 \oplus RK_1),\\
RK_3 &= E_K(K_3 \oplus RK_2),\\
RK_4 &= E_K(K_1 \oplus \langle 1\rangle \oplus RK_3),\\
RK_5 &= E_K(K_2 \oplus \langle 2\rangle \oplus RK_4),\\
RK_6 &= E_K(K_3 \oplus \langle 4\rangle \oplus RK_5).
\end{aligned}
$$

Эти версии расписания ключей требуют 6 расписаний ключей DES и 6 зашифрований DES на фиксированном ключе. Подключи нужно сгенерировать только один раз, если их впоследствии сохранить.

В DEAL-256 подключи генерируются следующим образом:

$$
\begin{aligned}
RK_1 &= E_K(K_1),\\
RK_2 &= E_K(K_2 \oplus RK_1),\\
RK_3 &= E_K(K_3 \oplus RK_2),\\
RK_4 &= E_K(K_4 \oplus RK_3),
\end{aligned}
$$

$$RK_5 = E_K\left(K_1 \oplus \langle 1\rangle \oplus RK_4\right),$$
$$RK_6 = E_K\left(K_2 \oplus \langle 2\rangle \oplus RK_5\right),$$
$$RK_7 = E_K\left(K_3 \oplus \langle 4\rangle \oplus RK_6\right),$$
$$RK_8 = E_K\left(K_4 \oplus \langle 8\rangle \oplus RK_7\right).$$

Эта версия расписания ключей требует 8 расписаний ключей DES и 8 зашифрований DES на фиксированном ключе. Подключи нужно сгенерировать только один раз, если их впоследствии сохранить.

Заметим, что для всех версий расписания ключей 64-х битные величины RK_i используются как ключи DES, поэтому биты проверки четности RK_i не используются в i-ом цикле. Однако, все 64 бита RK_i, как выхода шифрования на ключе K, используются при генерации следующего подключа.

Принципы разработки расписания ключей, во-первых, состоят в том, чтобы подключи зависели от наибольшего числа битов основного ключа, но не требовали при этом много работы, во-вторых, при вводе s основных ключей размером по 64 бит, любые s последовательных подключей должны иметь энтропию $s \cdot 56$ бит, и, наконец, не должно быть очевидно зависимых и слабых ключей и не должно остаться свойство дополнительности. Заметим, что последние две проблемы присутствуют и в DES, и –все три – в тройном DES. Мы заметили, что если основные ключи размером по 64 бита каждый, может найтись пара ключей, генерирующих одинаковые множества подключей. Однако, число таких ключей, похоже, настолько невелико, что не представляет угрозы DEAL'у, применяемому для шифрования.

Смещения $\langle i\rangle$ введены для предотвращения появления слабых ключей. Если бы их не было, существовали бы ключи, для которых все подключи были равны. Например, для DEAL-128 ключи $K_1 = K_2 = D_K(0)$ сгенерировали бы 6 подключей со значением 0. Смещения и шифрование на фиксированном ключе предотвращают появление слабых и зависимых ключей и свойства дополнительности.

Заметим, что если бит проверки четности используется в каждом байте основного ключа, действующие размеры предложенных ключей составляют 112, 168 и 224 бит соответственно.

3. Стойкость DEAL'а. (Предоставлено автором)

Что можно сказать о стойкости DEAL'а в целом? Прежде всего, заметим, что для DEAL простая атака meet-in-the-middle (встретить по середине), аналогичная такой атаке на двойной DES, отыщет ключи за время порядка 2^{168} зашифрований для шести, и 2^{224} зашифрований для восьми циклов DEAL соответственно, независимо от расписания ключей. Именно поэтому, предлагается в DEAL-256 производить по крайней мере 8 циклов зашифрования. Для DEAL-128 исчерпывающий поиск ключа займет время порядка 2^{112} зашифрований.

Самая быстрая из известных атак по нахождению ключа на DEAL (с шестью циклами), которую мы сознаем, – общая атака на 6-и цикловые

Фейстелевы шифры, в приложении к DEAL, она требует порядка 2^{121} зашифрований DES, используя порядка 2^{70} выбранных открытых текстов, для любого расписания ключей. В дальнейшем определим разность между двумя последовательностями бит, как побитное XOR.

В конце этого раздела подведем итог особенностям DEAL.

- DEAL имеет размер блока 128 бит и размер ключа 128, 192 или 256 бит (действующий размер, соответственно,– 112, 168 или 224 бита).
- Атака по подобранному шифр-тексту требует порядка 2^{64} блоков шифр-текста.
- Нет известных, вероятных атак.
- DEAL с шестью циклами имеет скорость, аналогичную скорости тройного DES.
- DEAL может использоваться в стандартных режимах работы.
- DEAL может быть реализован на имеющемся аппаратном и программном обеспечение DES.
- Нет очевидно слабых ключей и устранено свойство дополнительности.

Наконец, позволим себе заметить, что ввиду довольно сложного расписания ключей, DEAL не практично использовать в случайных функциях.

4. Заключение.

Мы описали блочный шифр, DEAL, с размером блока 128 бит и размером ключа 128, 192 или 256 бит, как альтернативу существующим тройным режимам шифрования. DEAL может использоваться во всех четырех, разработанных для DES, стандартных режимах шифрования. Для первых двух размеров ключа схема шифрует два блока по 64 бита, используя шесть зашифрований DES, таким образом ее производительность равна производительности тройного DES. Производительность DEAL с восемью циклами (и размером ключа 256 бит) равна DES в режиме CBCM. Благодаря большим размерам блока и ключа, исчерпывающий поиск ключа и атака по подобранному шифр-тексту невыполнимы. К тому же, избегаются слабые места DES и тройного DES. Нет очевидно слабых ключей, не осталось свойства дополнительности, и успех атак по зависимому ключу весьма маловероятен. Мы рекомендовали ANSI принять DEAL, как часть. Кроме того, мы предлагаем DEAL, как возможный кандидат на Advanced Encryption Standard.

5. Стойкость DEAL. Анализ DEAL, как кандидата на AES.

Собственно результаты:

- Существуют эквивалентные ключи для DEAL-192 и DEAL-256. Алгоритм нахождения требует около шести шифрований DES, чтобы найти набор из 256 эквивалентных ключей для DEAL-192, и

восемь шифрований DES, чтобы найти 256 эквивалентных ключей для DEAL-256.

- Существуют эквивалентные ключи для DEAL-128 и алгоритм их нахождения, требующий около 2^{64} вычислений для нахождения пары эквивалентных ключей.
- Атака математически-связанных ключей (related-key attack) на DEAL-192 и DEAL-256, требующая три блока открытого текста, под 2^{33} ключами с точным соответствием, $3*2^{45}$ байт памяти и около 2^{137} шифрований DEAL, чтобы найти последние два цикловых подключа для DEAL-192 и DEAL-256. (С большим количеством памяти это можно сделать быстрее).
- Несколько возможных расширений этих атак. DEAL-192 может быть дешифрован до четырех циклов, а затем может быть применена атака Бихама (Biham's) на четырехцикловый цепной DES; DEAL-256 может быть дешифрован до шести циклов, а затем может быть применена атака на шестицикловый DEAL-192.

Эти результаты интересны как для практики, так и для теории. Похоже, что DEAL будет иметь некоторое применение в будущем. DEAL кандидат на AES, но даже если он не станет финалистом, он почти наверняка будет использоваться. Как было указано на первой конференции по AES, широкое распространение «железа под DES» делает DEAL относительно легким для реализации во многих устройствах за очень низкую цену.

В реальном применении эквивалентные ключи DEAL'а имеют важное практическое следствие – они делают многие стандартные методы хэширования ненадежными.

Атака основанная на математически зависимых ключах вероятно менее применима, но все ещё может быть важна для некоторых приложений эти атаки «снимают» два последних цикла DEAL ценой примерно 2^{137} шифрований DEAL, используя $3*2^{45}$ байт памяти и требует все те же три блока открытого текста, зашифрованного 2^{33} зависимыми ключами. Возможны компромиссы времени-памяти.

В настоящее время, имея $3*2^{69}$ байт памяти, атака будет занимать 2^{113} вычислительных ресурсов, восстанавливая два последних подключа. После, можно реализовать атака Бихама (Biham's) на четырехцикловый цепной DES, которая требует ещё 2^{33} блока открытого текста, зашифрованного только одним ключом, и 2^{88} времени. Таким образом, вся атака займет приблизительно 2^{113} вычислительной работы, $3*2^{69}$ байт памяти, все те же три блока открытого текста, зашифрованного 2^{33} зависимыми ключами, ещё 2^{32} блока открытого текста, зашифрованного только одним ключом, которые должны быть выбраны ПОСЛЕ завершения первой атаки. По сравнению с лучшей из ранее известных атак, требующей 2^{119} вычислительной работы, 2^{64} памяти и 2^{70} выбранных открытых текстов.

На теоретическом уровне эти результаты показывают важный факт: Широко считается, что «назначение ключей» (key shedule), которое использует сильные элементы криптографии будет практически неуязвимо к криптографическому анализу. Это утверждение, к сожалению, не верно. В DEAL используется сильный шифр в очевидно-разумном направлении чтобы обрабатывать ключ. Однако, использованный метод оставляет уязвимость шифра к анализу зависимого ключа, также оставляет возможность эквивалентных ключей.

Заключение.
В этой статье продемонстрирована слабость образования ключей в DEAL, относительно эквивалентных ключей и зависимых ключей. Атака «зависимых ключей» наиболее интересна (требует 2^{128} шифрований DES).

Литература.

1. L. Knudsen: *DEAL- A 128-bit Block Cipher*, AES-Proposal, Juni 1998
http://th.informatik.uni-mannheim.de/m/lucks/papers/deal.ps.gz
2. J. Kelsey, B. Schneier: *Key-Schedule Cryptoanalysis of DEAL*,
http://www.counterpane.com/deal.pdf