# **Разностный и линейный криптоанализ DES**

1 Слайд:

Сегодня я бы хотел поговорить о такой криптосистеме, как DES. Сегодня мы более подробно поговорим не столько про какие-то основы алгоритма шифрования DES, сколько про его слабости, а именно уязвимость к разностному и линейному криптоанализу.

2 Слайд:  
Для начала, вспомним основные моменты, которые рассказывались в предыдущем докладе. В 1977 году Национальное бюро Стандартов США (NBS) опубликовало стандарт шифрования данных ***Data Encryption Standard (DES)***, основанный на сети Фейстеля и предназначенный для использования в государственных и правительственных учреждениях США для защиты от несанкционированного доступа важной, но несекретной информации. Алгоритм, положенный в основу стандарта, распространялся достаточно быстро, и уже в 1980 году был одобрен ANSI. С этого момента DES превращается в стандарт не только по названию (Data Encryption Standard), но и фактически. Появляются программное обеспечение и специализированные микроЭВМ, предназначенные для шифрования/расшифрования информации в сетях передачи данных и на магнитных носителях. К настоящему времени DES является наиболее распространенным алгоритмом, используемым в системах защиты коммерческой информации. Более того реализация алгоритма DES в таких системах является просто признаком хорошего тона! За примерами далеко ходить не надо. Например, программа DISKREET из пакета Norton Utilities, предназначенная для создания зашифрованных разделов на диске, использует именно алгоритм DES. "Собственный алгоритм шифрования" отличается от DES только числом итераций при шифровании. Почему же DES добился такой популярности? Из его плюсов можно выделить плюсы на слайде, а именно … Что касается процесса шифрования, он заключается в начальной перестановке битов 64-битового блока, шестнадцати циклах шифрования и, наконец, обратной перестановки битов (см. рисунок на слайде). Также, этот алгоритм может использовать различные режимы…

3 Слайд:

А теперь укажем причину того, почему DES не совершенен. Укажем на слабости алгоритма DES. В течение прошлых нескольких лет критики разных стран нашли некоторые слабости в *DES*.

Мы кратко укажем на некоторые слабости, которые были обнаружены в структуре этого шифра.

**S-блоки**. В литературе указываются по крайней мере три проблемы S -блоков.

* В S -блоке 4 три бита выхода могут быть получены тем же самым способом, что и первый бит выхода: дополнением некоторых из входных битов.
* Два специально выбранных входа к массиву S -блока могут создать тот же самый выход.
* Можно получить тот же самый выход в одном единственном раунде, изменяя биты только в трех соседних S -блоках.

**P-блоки**. В структуре P -блока были найдены одна загадка и одна слабость.

* Не ясно, почему проектировщики *DES* использовали начальную и конечную перестановки. Эти перестановки не вносят никаких новых свойств с точки зрения безопасности.
* В перестановке расширения (в функции) первые и четвертые биты последовательностей на 4 бита повторяются.

4 Слайд:

**Размер ключа**. Критики утверждают, что самая серьезная слабость *DES* — это размер ключа (только  56 битов). Чтобы предпринять атаку грубой силы данного блока зашифрованного текста, злоумышленники должны проверить 256 ключей.

a. Используя доступную сегодня технологию, можно проверить один миллион ключей в секунду. Это означает, что потребуется более чем две тысячи лет, чтобы выполнить атаку грубой силы на *DES*, используя компьютер только с одним процессором.

b. Если мы можем сделать компьютер с одним миллионом чипов процессоров (параллельная обработка), то сможем проверить все множество ключей приблизительно за 20 часов. Когда был введен *DES*, стоимость такого компьютера была более чем несколько миллионов долларов, но она быстро снизилась. Специальный компьютер был создан в 1998 году — и нашел ключ за 112 часов.

c. Компьютерные сети также позволяют моделировать *параллельную обработку*. В 1977 году команда исследователей использовала 3500 компьютеров, подключенных к Internet, чтобы найти ключ *RSA* за 120 дней. Множество ключей было разделено среди всех этих компьютеров, и каждый компьютер был ответственен за проверку части домена *DES*. Если 3500 связанных в сеть компьютеров могут найти ключ через 120 дней, то секретное общество из 42 000 членов может найти ключ через 10 дней.

Приведенное выше показывает, что *DES* с размером ключа шифра 56 битов не обеспечивает достаточной безопасности. Для решения этой проблемы есть использование *тройного DES*(*3DES*) с двумя ключами ( 112 битов) или *тройного DES* с тремя ключами, однако сегодня мы отметим слабости классического DES с 56 битами.

**Слабые ключи**. Четыре ключа из 256 *возможных ключей* называются **слабыми ключами**. Слабые ключи — это одни из тех, которые после операции удаления проверочных бит состоят из всех нулей или всех единиц или половины нулей и половины единиц. Такие ключи показаны в табличке на слайде ниже.

Ключи раунда, созданные от любого из этих слабых ключей, — те же самые и имеют тот же самый тип, что и ключ шифра. Например, эти шестнадцать ключей раунда создают первый ключ, который состоит из всех нулей или всех единиц или наполовину из нулей и единиц.

Это происходит по той причине, что алгоритм генерирования ключей сначала делит ключ шифра на две половины. Смещение или перестановка блока не изменяют блок, если он состоит из всех нулей, или всех единиц, или наполовину из нулей и единиц.

В чем опасность использования слабых ключей? Если мы зашифровали блок слабым ключом и впоследствии расшифровали результат тем же самым слабым ключом, мы получаем первоначальный блок. Процесс создает один и тот же первоначальный блок, если мы расшифровываем блок дважды. Другими словами, каждый слабый ключ есть инверсия самого себя: Ek. (Ek (P)) = P, как это показано на схеме слева на слайде.

Также следует отметить, что существуют и возможно слабые ключи (их 48 штук). Возможно слабый ключ создает только четыре различных ключа раунда; другими словами, шестнадцать ключей раундов разделены на четыре группы, и каждая группа состоит из четырех одинаковых ключей раунда.

Теперь поговорим о том, как разностный и линейный криптоанализ оперируют с DES. А начнем мы с разностного.

Слайд 5:

*Дифференциальный криптоанализ* для *DES* был изобретен Бихамом (Biham) и Шамиром (Shamir). В этом криптоанализе *злоумышленник* концентрируется на *атаках с выборкой исходного текста*. *Анализ* использует *разность*в прохождении различных входных сигналов через устройство или программу шифрации. Термин *разность* здесь применяется, чтобы рассмотреть с помощью *операции* ИСКЛЮЧАЮЩЕЕ ИЛИ несовпадение двух различных входных сообщений (исходные тексты).

Дифференциальный профайл (он же профайл ИСКЛЮЧАЮЩЕЕ ИЛИ) показывает вероятностное отношение между входными разностями и разностями выхода S-блока. Подобные профайлы могут быть созданы для каждого из восьми S-блоков в DES.

Слайд 6:

Характеристика раунда подобна дифференциальному профайлу, но вычисляется для целого раунда. Она показывает вероятность, с которой одна входная разность создала бы разность определенного выхода. Стоит обратить внимание, что характеристика одна и та же для каждого раунда, потому что любое отношение, которое включает разности, не зависит от ключей раунда. На схеме я показал четыре различные характеристики раунда.

Хотя существует много характеристик для раунда, рисунок N.2 показывает только четыре из них. В каждой характеристике мы разделили входные разности и разности выхода в левые и правые секции. Каждая левая или правая разность состоят из 32 битов или восьми шестнадцатеричных цифр. Все эти характеристики могут быть найдены использующими программами, которые могут найти отношение входа-выхода в раунде DES. [Рисунок а](https://www.intuit.ru/studies/professional_retraining/940/courses/409/lecture/17871?page=1#image.N.2) показывает, что входная разность (x, 0000000016) дает на выходе разность (x, 0000000016) с вероятностью 1. [Рисунок б](https://www.intuit.ru/studies/professional_retraining/940/courses/409/lecture/17871?page=1#image.N.2) показывает ту же самую характеристику, как [рисунок а](https://www.intuit.ru/studies/professional_retraining/940/courses/409/lecture/17871?page=1#image.N.2), за исключением того, что левые и правые вход и выход поменялись местами; вероятность изменится чрезвычайно. Рисунок в показывает, что входная разность (4008000016, 0400000016) дает разность выхода (0000000016, 040000016) с вероятностью 1/4. Наконец, [рисунок г](https://www.intuit.ru/studies/professional_retraining/940/courses/409/lecture/17871?page=1#image.N.2) показывает, что входная разность (0000000016, 6000000016) дает разность выхода (0080820016 600000016) с вероятностью 14/64.

Слайд 7:

После создания и хранения однораундных характеристик анализатор может комбинировать различное количество раундов, чтобы создать множественную характеристику раунда. Рисунок показывает случай трехраундной DES. На рисунке мы использовали три смесителя и только два устройства замены, потому что последний раунд не нуждается ни в каком устройстве замены. Характеристики, показанные в смесителях первых и третьих раундов, те же самые, как и на [рисунке b](https://www.intuit.ru/studies/professional_retraining/940/courses/409/lecture/17871?page=1#image.N.2) с прошлого слайда. Характеристика смесителя во втором раунде - та же самая, что и на [рисунке a](https://www.intuit.ru/studies/professional_retraining/940/courses/409/lecture/17871?page=1#image.N.2), тоже с прошлого слайда. Очень интересно отметить, что точки, в этом конкретном случае, разности входа и выхода - те же самые

Слайд 8:

Для шифра с шестнадцатью раундами можно скомпилировать много различных характеристик. Рисунок справа показывает подобный пример. На этом рисунке шифр DES состоит из восьми секций с двумя раундами. Каждая секция использует характеристики *а*и *б*на рисунке с позапрошлого слайда (где 4 секции). Ясно, что если последние раунды не имеют устройства замены, вход (x, 0) создает выход (0, x) с вероятностью (1/234)8.

Слайд 9:

Подытожим вышесказанное касательно разностного криптоанализа DES.

#### Атака

Для примера предположим, что Ева использует характеристику, чтобы напасть на DES с шестнадцатью раундами. Ева каким-то способом провоцирует Алису, чтобы зашифровать много исходных текстов в форме (x, 0), в которой левая половина - x (различные значения) и правая половина - 0. Ева затем сохраняет все зашифрованные тексты, полученные от Алисы, в форме (0, x). Обратите внимание, что 0 здесь означает 0000000016.

#### Нахождение ключа шифра

Окончательная цель злоумышленника в дифференциальном криптоанализе состоит в том, чтобы найти ключ шифра. Для этого нужно найти ключи каждого раунда от основания до вершины (K16K1).

##### Нахождение последних ключей раунда

Если злоумышленник имеет достаточно много пар исходного текста / зашифрованного текста (каждый с различными значениями. x ), он может использовать отношения в последнем раунде, 0 = f(K16,x) и найти некоторые из битов в K16. Это можно сделать, выбирая самые вероятные значения.

##### Нахождение других ключей раунда

Ключи для других раундов можно найти, используя другие характеристики или применяя атаки грубой силы.

##### Безопасность

В целом что можно сказать по безопасности? Известно, что необходимы 247 выборки пар исходного текста / зашифрованного текста, чтобы напасть на DES с 16 раундами. Найти такое огромное число выбранных пар чрезвычайно трудно в ситуациях реальной жизни. Это означает, что DES неуязвимы для этого типа атаки.

Слайд 10:

*Линейный криптоанализ* для *DES* был разработан Матцуи. Это - *атака знания исходного текста*. *Анализ* использует распространение конкретного набора битов через устройство шифрования.

*Линейный криптоанализ* основан на отношениях линейности. В этом типе криптоанализа представляют интерес два набора отношений: линейные профайлы и характеристики раунда, как показано на рисунке.

Линейный профайл показывает уровень линейности между входом и выходом S-блока. Мы видели, что в S-блоке каждый бит выхода - функция всех входных битов. Желательное свойство в S-блоке достигнуто, если каждый бит выхода - нелинейная функция всех входных битов. К сожалению, эта идеальная ситуация не существует в DES; некоторые биты выхода - линейная функция некоторых комбинаций входных битов. Другими словами, можно найти, что некоторые комбинации битов входа-выхода могут быть отображены между собой, используя линейную функцию. Линейный профайл показывает уровень линейности (или нелинейности) между входом и выходом. Криптоанализ может создать восемь различных таблиц, по одной для каждого S-блока, в которых первый столбец показывает возможные комбинации входов по шесть бит, 0016 до 3F16. Первая строка показывает возможные комбинации выходов по четыре бита, 016 до F16. Входы показывают уровень линейности (или нелинейности) данного проекта. Мы не можем углубляться в детали того, как измеряется уровень линейности, но входы с высокого уровня из линейности интересны для криптоанализа.

Слайд 11:

Характеристика раунда в линейном криптоанализе показывает комбинации входных битов, битов ключей раунда и битов выхода для того, чтобы определить линейное отношение. Рисунок изображает две различные характеристики раунда. Система обозначений, используемая для каждого случая, определяет биты, которые складываются по модулю два. Например, О (7, 8, 24, 29) означает операцию исключающее ИЛИ 7-х, 8-х, 24-х и 29-х битов, выходящих из функции; K (22) означает 22-й бит в ключе раунда; I (15) означает 15-й бит, входящий в функцию.

Слайд 12:

После создания и хранения однораундных характеристик анализатор может комбинировать различные раунды, чтобы создать множественную характеристику раунда. Рисунок показывает случай трехраундной DES, в которой раунды 1 и 3 используют одну и ту же характеристику, как это изображено на прошлом рисунке, а в раунде 2 использована произвольная характеристика.

1) Цель линейного криптоанализа состоит в том, чтобы найти линейное отношение между некоторыми битами в паре "исходный текст / зашифрованный текст" и ключ. Давайте посмотрим, можем ли мы установить такое отношение для DES с 3-мя раундами, изображенной на рисунке снизу.

2) Но L2 - тот же самый, что и R1, и R2 - тот же самый, что и R3. После замены L2 на R1 и R2 на R3 во втором отношении мы получим:

3) Мы можем заменить R1 на его эквивалентное значение в раунде 1, в результате имеем

4) Это отношения между битами входа и выхода для всей системы из трех раундов после преобразований:

5) Другими словами, мы имеем:

Слайд 13:

Один интересный вопрос: как найти вероятность трехраундных (или n -раундных) DES. Матцуи (Matsui) показал, что вероятность в этом случае определяется по формуле выше, где n является числом раундов,. P.- вероятность каждой характеристики раунда и P - полная вероятность. Например, полная вероятность для трехраундного анализа для нашего примера будет рассчитана, как показано на рисунке ниже.

Слайд 14:

16-раундовая характеристика может также быть скомпилирована, чтобы обеспечить линейные отношения между некоторыми битами исходного текста, некоторыми битами зашифрованного текста и некоторыми битами в ключах раунда.

Слайд 15:

После нахождения и сохранения многих отношений между некоторыми битами исходного текста, битами зашифрованного текста и битами ключей раунда Ева может обратиться к некоторым парам исходного текста / зашифрованного текста (атака знания исходного текста) и использовать соответствующие биты из сохраненных характеристик, чтобы найти биты в ключах раунда.

Что можно сказать в плане безопасности? Известно, что для того чтобы напасть на 16-раундовый DES, необходимы 243 известных пар исходного текста / зашифрованного текста. *Линейный криптоанализ* выглядит более вероятным, чем *дифференциальный криптоанализ*, по двум причинам. Первая: число шагов у него меньше. Вторая: он более прост для атаки знания исходного текста, чем для атаки с выборкой исходного текста. Однако и такая атака все еще далека от того, чтобы ее серьезно опасаться тем, кто работает с DES.

Слайд 16:

На этом все, ваши вопросы…?