УДК 004.056+003.26

Студ. Д.А. Тарасевич
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

ОСОБЕННОСТИ ДИФФЕРЕНЦИАЛЬНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА

Криптоанализ – это наука, изучающая математические методы нарушения конфиденциальности и целостности информации, также включает методы выявления уязвимости криптографических алгоритмов и протоколов. На практике криптоанализ основан на 3 вещах:

- изучение системы шифрования в целом,
- изучение особенностей исходного текста,
- изучение особенностей ключевой системы.

Рассмотрим основные виды атак [1,2].

Пассивная атака – это перехват и прослушивание передаваемых по сети данных, т.к. атакующий не воздействует на протокол, алгоритм, ключ, само сообщение, какие-либо части системы шифрования.

Активная атака – это изменение сообщений, изменение системных файлов, попытки выдать себя за другого человека. К основным видам атак относятся следующие.

1) Атака «только шифротекст» (cipher-only attack): при выполнении атаки этого типа, атакующий имеет шифротекст нескольких сообщений. Каждое из сообщений зашифровано одним и тем же алгоритмом.

2) При выполнении атаки типа «известный открытый текст» (known-plaintext attack), у атакующего есть открытый текст и соответствующий ему шифротекст одного или нескольких сообщений.

3) При выполнении атаки типа «выбранный открытый текст» (chosen-plaintext attack), у атакующего также есть открытый текст и соответствующий ему шифротекст, но он имеет возможность самостоятельно выбирать открытый текст и получать его в зашифрованном виде.

4) При выполнении атаки типа «выбранный шифротекст» (chosen-ciphertext attack), атакующий может выбирать шифротекст для расшифрования и имеет доступ к получаемому в результате открытому тексту.

Дифференциальный криптоанализ разработан в 1990 году израильскими криптографами Э. Бихамом (E. Biham) и А. Шамиром (A. Shamir) [3]. Первая такая атака была проведена в 1990 году против алгоритма DES. Дифференциальный криптоанализ — атака с подобранным открытым текстом. Это означает, что для применения ДК вы должны иметь возможность зашифровать абсолютно любые тексты в абсолютно любом количестве.

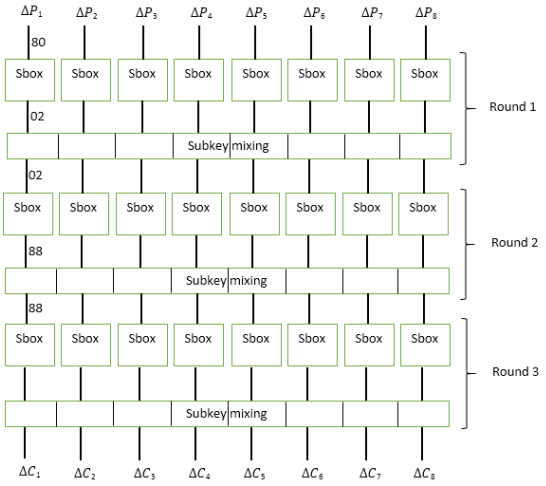
Проанализируем данный криптоанализ на примере трехраундового блочного шифра, представленного на рис. 1. Для двух заранее подобранных шифротекстов P1 и P2 злоумышленником вычисляется «дифференциал» ΔP=P1⊕P2. И с помощью ΔP пытается определить каким должен быть «дифференциал» шифротекстов ΔC=C1⊕C2.

Данный шифр имеет 64 битный размер блока и 128 битный ключ. На каждом раунде входной блок делится на 8 байт, каждый из которых проходит через функцию подстановки Sbox. После этого данные перемешиваются с 64 битным подключом Subkey. Функция перемешивания представляет собой XOR операцию.

Предположим, что злоумышленник решил проверить дифференциал 0x80. Для этого он генерирует произвольный байт X1, и вычисляет X2=X1⊕80. Далее атакующий прогоняет X1 и X2 через функцию Sbox и получает значения Y1 и Y2. Для каждой такой пары X1 и X2, дифференциал которых равен 80, атакующий в состоянии получить дифференциал ΔY. Анализируя полученные значения, атакующий выбирает такое значение ΔY, которое имеет большую вероятность возникновения.

Возвращаясь к нашему примеру, предположим, что из всех 256 пар X1 и X2, в 192 случаях Y1⊕Y2=02. Таким образом, вероятность того, что при заданном ΔX=80, значение ΔY=02, составляет 192/256=3/4. Это в свою очередь означает, что при заданном ΔX=80, с вероятность P1=3/4 на вход второго раунда попадут два значения U1 и U2, такие, что ΔU=02.

Рисунок 1 – Трехраундовый блочный шифр [4]



Ключ не влияет на значение дифференциалов. Так как при шифровании разных текстов ключ не изменяется и перемешивание с ключевой последовательностью осуществляется с помощью XOR, то при вычислении ΔU байты ключа взаимно исключаются. Для раскрытия свойств второго раунда, злоумышленник генерирует новые 256 пар

входных байт X1 и X2, таких, что X1⊕X2=02. Произведя вычисление функции Sbox для каждой пары X1 и X2, атакующий замечает, что в 64 случаях из 256 ΔY=88. Т.е. вероятность того, что ΔY=88, для заданного ΔX=02, составляет P2=64/256=1/4. Таким образом, произведя нехитрый подсчет вероятностей, атакующий понимает, что для указанного шифра для каждой пары байт X1 и X2, таких, что ΔX=80, с вероятность P= P1P2=3/4*1/4=3/16, дифференциал внутреннего состояния шифра перед последним раундом составляет ΔY=88. Обладая этим знанием, атакующий генерирует несколько пар текстов таких, что ΔP=808080808080 и приступает к побайтовому подбору подключа третьего раунда.

Покажем, каким образом осуществляется вскрытие первого байта подключа. Для каждого из 256 возможных вариантов первого байта Subkey [0] и для каждой пары шифротекстов {C1, C2}, злоумышленник вычисляет U1=Sbox (C1⊕Subkey [0]) и U2=Sbox (C2⊕Subkey [0]).

Если Subkey[0] угадан правильно, то приблизительно 3 из каждых 16 пар U1 и U2 при вычислении ΔU будут равны 88. Подобрав таким образом наиболее вероятный первый байт подключа Subkey, атакующий может перейти ко второму байту и действуя аналогичным образом вскрыть весь ключ третьего раунда.

После того, как ключ последнего раунда будет раскрыт, злоумышленник может приступить к атаке на предпоследний раунд и действуя подобным образом в конечном итоге получит информацию о всех раундовых ключах шифра.

Недостатки метода:

- высокие требования к времени и объему данных (на практике),
- chosen plaintext attack,
- необходим большой объем памяти для хранения возможных ключей,
- может быть использован только для вскрытия с известным открытым текстом,
- для 16-этапного DES этот метод менее эффективен, чем вскрытие грубой силой.

Линейный криптоанализ разработан М. Мацуи (M. Matsui) в 1993 г. [4]. Является вариантом атаки, направленным на выявление наиболее вероятного значения ключа, использованного в процессе шифрования блочным алгоритмом. Атакующий выполняет атаку «известный открытый текст» на несколько различных сообщений, зашифрованных на одном и том же ключе. Атакующий анализирует входящие и исходящие значения для каждого S-бокса. Он анализирует вероятность того, что определенные входящие значения дают в ре-

зультате определенную комбинацию. Выявление таких результирующих комбинаций позволяет ему оценивать вероятность для различных значений ключа, пока он не найдет повторяющийся шаблон, имеющий высокую вероятность.

Алгоритм заключается в следующем [4]:

1) пусть T — количество текстов, для которых левая часть уравнения (ф.1) равняется 0, тогда *если* T>N/2, где N — число известных открытых текстов,

2) предположить, что $K_{I1} \oplus K_{I2} \oplus \ldots \oplus K_{Ic} = 0$ (когда P>1/2) или 1 (когда P<1/2), *иначе,*

3) предположить, что $K_{I1} \oplus K_{I2} \oplus \ldots \oplus K_{Ic} = 1$ (когда P>1/2) или 0 (когда P<1/2).

Из анализа алгоритма можно сделать вывод, что успех алгоритма напрямую зависит от значения |P-1/2| и от количества доступных пар открытый/закрытый текст N.

Защита от линейного криптоанализа:

1) минимизирование вероятностных смещений,

2) выбор высоко нелинейных S-блоков и усиление диффузии,

3) учитывать эффект линейных оболочек,

4) применение бент-функций в построении стойких S-блоков.

Проанализировав два примера, можно сделать вывод, что дифференциальный криптоанализ не подходит для применения на практике из-за того, что для него существуют высокие требования ко времени и объему данных, и подходит только для атаки типа «выбранный открытый текст». Линейный криптоанализ подходит только для атаки типа «известный открытый текст», из чего можно вывести зависимость чем больше вероятность P равенства (ф.1) отличается от 1/2, тем меньшее количество открытых текстов N необходимо для атаки.

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации / П.П. Урбанович. – Минск: БГТУ, 2016.

2. Heys, H. M. A Tutorial on Linear and Differential Cryptanalysis/ H.M. Heys. [Электронный ресурс]. – Режим доступа: http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf. – Дата доступа: 15.04.2019.

3. Biham, E. Differential cryptoanalysis of the Data Encription Standard/E. Biham, A. Shamir. [Электронный ресурс]. – Режим доступа: http://bookre.org/reader?file=1242706. – Дата доступа: 15.04.2019.

4. Matsui, M. Linear Cryptanalysis method of DES cipher/ M. Matsui. [Электронный ресурс]. – Режим доступа: https://www.cs.bgu.ac.il/~beimel/Courses/crypto2001/ Matsui.pdf. – Дата доступа: 15.04.2019.