СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

А.Б. Левина

Криптография и криптографические протоколы

Криптоанализ и криптостойкость

СПбГЭТУ «ЛЭТИ», 2022 г.

1. ВВЕДЕНИЕ

Сегодня мы немного поговорим о криптоанализе и криптостойкости. На этой лекции мы повторим те криптоатаки, которые успели изучить во время этого курса, рассмотрим также дифференциальный и линейный криптоанализ и поговорим об основном виде современного криптоанализа – атаках по сторонним каналам.

Сегодня на лекции будут рассмотрены:

- Базовые понятия, используемые в криптоанализе;
- Основные виды криптоанализа (линейный и дифференциальный);
- Атаки по сторонним каналам.

2. БАЗОВЫЕ ПОНЯТИЯ

2.1 КРИПТОАНАЛИЗ

На первой лекции мы говорили, что криптоанализ является неотъемлемой частью криптографии, несмотря на то, что многие криптографы рассматривают его как отдельное направление, но без тщательного криптоанализа создать криптостойкий алгоритм невозможно. Вспомним ряд определений.

Определение 2.1.1 *Криптоанализ — наука о методах расшифровки зашифрованной информации без предназначенного для такой расшифрофки ключа.*

Криптоанализ предполагает выявление ключа или нахождение уязвимостей алгоритма, дающих возможность получить секретную информацию, не имея на это прав.

Определение 2.1.2 *Криптографическая атака - попытка раскрытия конкретного шифра с применением методов криптоанализа.*

Определение 2.1.3 *Взлом (вскрытие) - криптографическая атака, в ходе которой удалось раскрыть шифр (получить секретный ключ)*

Мы помним, что основные принципы криптоанализа сформулировал Огюст Кергхофф в 1883 году, в своем труде «Военная криптография». Проговорим их еще раз:

1. Система должна быть физически, если не математически, невскрываемой.
2. Нужно, чтобы не требовалось сохранение системы в тайне; попадание системы в руки врага не должно причинять неудобств (*принцип Кергоффса*).
3. Хранение и передача ключа должны быть осуществимы без помощи бумажных записей; корреспонденты должны располагать возможностью менять ключ по своему усмотрению.
4. Система должна быть пригодной для сообщения через телеграф.
5. Система должна быть легко переносимой, работа с ней не должна требовать участия нескольких лиц одновременно.
6. От системы требуется, учитывая возможные обстоятельства её применения, чтобы она была проста в использовании, не требовала значительного умственного напряжения или соблюдения большого количества правил.

Мы также помним, что в 1949 году Клод Шеннон в статье «Теория связи в секретных системах», переформулировал принцип Керкгоффса следующим образом: «Враг знает систему».

В настоящее время, это является основным принципом криптонализа. Наш противник – Ева знает о системе шифрования всё, кроме применяемых ключей.

Чем меньше секретов содержит система, тем выше её безопасность. Мы рассматривали несколько алгоритмов, нарушивших этот принцип. Это алгоритм ГОСТ - 28147-89 и стандарты шифрования GSM.

Алгоритмы A3/A8 и A5 были взломаны менее, чем за год после их попадания в

общественность (1997-1998).

Поговорим теперь немного о криптостйкости.

2.2 КРИПТОСТЙКОСТЬ

Определение 2.2.1 *Криптостойкость - способность криптографического алгоритма противостоять криптоанализу.*

Мы понимаем, что вскрыть можно любую систему с помощью полного перебора, потому взлом должен требовать слишком много ресурсов:

1. Времени (актуальность информации);
2. Открытых текстов (недостижимость перехвата);
3. Памяти (вычислительные ресурсы).

Рассмотрим один из подходов к анализу криптостойкости -

1.1 информационно-теоретический подход.

Согласно данному подходу криптосистемы можно разделить на:

- Абсолютно стойкие;
- Условно стойкие.

Клод Шеннон в работе «Теория связи в секретных системах» в 1949, ввел определение абсолютно стойкой системы, которое мы рассматривали на второй лекции.

Условно стойкие криптосистемы с помощью сложностно-теоретического подхода можно разделить на:

- Вычислительно стойкие;
- Предположительно стойкие;
- Вычислительно нестойкие.

Брюс Шнайер выделил 4 основных метода криптоанализа:

- Атака на основе шифротекста (Ciphertext-only attack). Атакующему известен только шифротекст.
- Атака на основе открытых текстов (Known-plaintext attack). У атакующего на руках есть и шифротексты и открытые тексты, необходимо найти ключ.
- Атака на основе подобранного открытого текста (Chosen-plaintext attack). Атакующий делает так, что законные пользователи шифруют необходимый ему открытый текст и у него есть пара – нужный ему открытый текст – шифротекст. Данную атаку мы разбирали, когда изучали перестановочные шифры.
- Атака на основе адаптивно подобранного открытого текста (Adaptive chosen-plaintext attack). Данная атака более сильная, чем атака на основе подобранного открытого, так как атакующий меняет открытый текст, отталкиваясь от полученных ранее вариантов.

Так же Шнайер выделил дополнительные методы криптоанализа:

- Атака на основе связанных ключей ($K_B = F(K_A)$). Когда открытые тексты шифруются ключами имеющими некую взаимосвязь.
- Атака на основе подобранного шифротекста (lunchtime attack или midnight attack).
- «Бандитский» криптоанализ.

С некоторыми методами криптоанализа мы уже познакомились:

- Полный перебор (brute force) – шифр Цезаря;
- Частотный анализ (IX век) – шифры замены;
- Метод Касиски (1863) – шифр Виженера;

- Атака «дней рождения» - хэш-функции;
- Атака «человек посередине» (Man in the middle) - протокол Диффи- Хеллмана.

Вспомним пройденные нами методы криптоанализа более подробно.

2.3 АТАКИ, РАССМОТРЕННЫЕ РАНЕЕ

Начнем мы по порядку. Первые атаки, известные нам, это атаки на моноалфавитные шифры, они основывались на **частотном анализе**.

Зная частоту появления букв в тексте и видя шифротекст, полученный с помощью моноалфавитного алгоритма шифрования, можно сразу догадаться, какая буква открытого текста соответствует какой букве шифротекста.

Метод Касиски. Мы помним, что на смену моноалфавитным шифром, пришли полиафавитные шифры (шифр Вижнера) и для его взлома использовался тест Касиски.

Тест Касиски основан на нахождении длины секретного слова – ключа, так как если мы сможем найти длину ключа, то, соответственно, будем знать сколько шифрующих алфавитов использовалось. Тогда, зная количество этих алфавитов, будет известно на каких позициях используются одинаковые шифрующие алфавиты и, соответственно, на этих позициях статистика языка будет оставаться.

Следующие атаки, с которыми мы познакомились, это были **атаки на RSA**

1.1 Атака «раздельный модуль».

В системе используется общий модуль N.

Тогда есть две атаки на систему – атака внутреннего пользователя и внешнего атакующего.

Атака ***внутреннего пользователя***.

Лемма 2.3.1 *Если известна дешифрующая экспонента d алгоритма RSA, соответствующая открытому ключу (N, E), то число N можно эффективно разложить на множители.*

Так как Алиса знает свое d_1, соответственно согласно Лемме, она сможет

разложить число N на сомножители и найти $\phi(N)$. Тогда она может посчитать d_2 Боба по формуле $d_2 = 1/E_2(mod\ \phi(N))$.

И у Алисы теперь есть секретный ключ Боба.

Внешний атакующий может тоже произвести атаку, если используется общий модуль N.

Ева видит два шифротекста C_1 и C_2 и знает, что модуль у них один, тогда она вычисляет $T_1 = {E_1}^{-1}(mod\ E_2)$, и $T_2 = (T_1E_1\text{-}1)/E_2$.

После этого она возводит в степень T_1 и $-T_2$ соответственно C_1 и C_2 и получает:

$$C^{T_1}C^{-T_2} = m^{(E_1)\cdot(T_1)}m^{(-E_2)\cdot(T_2)} = m^{1+E_2T_2}m^{-E_2T_2} = m.$$

1.2 Атака "малые экспоненты"

Пусть у нас есть три пользователя с тремя различными модулями N_1, N_2, N_3 и они все используют $E = 3$.

Предположим, что им всем было послано одно и тоже сообщение m, тогда мы получаем три разных шифротекста C_1, C_2, C_3 такие, что:

$C_1 = m^3(mod\ N_1),\ C_2 = m^3(mod\ N_2),\ C_3 = m^3(mod\ N_3)$.

Ева видит все эти три шифротекста и, с помощью Китайской Теоремы об остатках, решает систему уравнений $X = C_i(mod\ N_i)\ i = 1, 2, 3$.

$X = m^3(mod\ N_1N_2N_3)$, так как $m^3 < N_1N_2N_3$ следовательно целые числа X и m^3 должны совпадать. Извлекая кубический корень из X мы находим m.

Вспомним еще одну атаку - **атака на алгоритм Диффи-Хеллмана**.

1. Алиса договаривается с Евой, думая, что она общается с Бобом;
2. Боб также ведет переговоры с Евой, считая, что это Алиса;
3. Ева читает все сообщения, так как они проходят через нее как через коммутатор. При этом она может их менять, или не менять по своему усмотрению. Если Ева не

вносит изменений в сообщения, то обнаружить ее невозможно.

После того как мы вспомнили пройденные атаки, давайте познакомимся с основными видами криптоанализа – линейным и дифференциальным криптоанализом.

3 ЛИНЕЙНЫЙ И ДИФФЕРЕНЦИАЛЬНЫЙ КРИПТОАНАЛИЗ

3.1 ЛИНЕЙНЫЙ КРИПТОАНАЛИЗ

Линейный криптоанализ был предложен японским криптографом Мицуру Мацуи в 1993 году и является одним из основных видов криптоанализа, которому подвержены симметричные шифры.

Он направлен на восстановление неизвестного ключа шифрования, по известным открытым сообщениям и соответствующим им шифртекстам.

Для проведения линейного криптоанализа атакующему необходимо обладать большим количеством пар открытый/зашифрованный текст, полученных с использованием одного и того же ключа шифрования. Цель атакующего – восстановить ключ, частично или полностью.

Сама атака сводится к двум шагам:

- Построение соотношений между открытым текстом, шифротекстом и ключом, которые справедливы с высокой долей вероятности;
- Применение этих вероятностей к известным открытым текстам и шифротекстам для вычисления битов ключа.

В данном курсе мы не будем подробно рассматривать линейный крипто- анализ, но для взлома алгоритма DES были получены следующие результаты:

- для взлома 8 раундов алгоритма необходимо 2^{21} пар открытый текст/ шифротекст, примерное время атаки 40 секунд;
- для взлома 12 раундов алгоритма необходимо 2^{33} пар открытый текст/ шифротекст,

примерное время атаки 50 часов;

- для взлома 16 раундов алгоритма необходимо 2^{47} пар открытый текст/ шифротекст, примерное время атаки 50 дней.

3.2 ДИФФЕРЕНЦИАЛЬНЫЙ КРИПТОАНАЛИЗ

Дифференциальный криптоанализ был предложен израильскими криптографами Эли Бихамом и Ади Шамиром в 1990 году, с их работами мы уже хорошо знакомыми.

Основной идей дифференциального криптоанализа является изучение разностей (вернее сказать результатов операции XOR) между шифруемыми значениями на различных раундах шифрования.

Дифференциальный криптоанализ является атакой на основе адаптивно подобранных открытых текстов, но также может проводится на основе только открытых текстов. Для атаки необходимы пары открытых текстов, связанных определенной разницей.

Исследуя разницу входных и выходных значений раунда восстанавливается (или частично восстанавливается) ключ раунда, а далее проходясь по каждому раунда восстанавливается полный ключ.

С увеличением числа раундов сложность криптоанализа увеличивается. На данной картинке представлена сложность взлома DES, в зависимости от количества раундов.

Число раундов	Трудоёмкость атаки
4	2^4
6	2^8
8	2^{16}
9	2^{26}
10	2^{35}
11	2^{36}
12	2^{43}
13	2^{44}
14	2^{51}
15	2^{52}
16	2^{58}

Рис. 1: Зависимость трудоемкости атаки от количества раундов алгоритма DES

При проведении дифференциального криптоанализа атакуемой частью криптоалгоритма являются S-блоки.

Несмотря на важность линейного и дифференциального криптоанализа, оба они являются теоретическими способами проведения криптоатак. Давайте познакомимся с более применяемыми на практике, и действительно представляющим угрозу, видом криптоанализа – атаками по сторонним каналам.

4 АТАКИ ПО СТОРОННИМ КАНАЛАМ

В настоящее время, **атаки по сторонним каналам** являются наиболее широко применяемым и наиболее опасным видом криптоатак.

Они нацелены на нахождение уязвимостей – «сторонних каналов», при реализации криптоалгоритмов. Огромную популярность они получили в 1996 году после публикации Пола Кохера «Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems». В данной работе Кохер предло- жил использовать один из «сторонних каналов», а именно время выполнения различных операций, для проведения атаки и нахождения ключа.

Определение 4.0.1 *Атака по сторонним (или побочным) каналам (Side-channel attack) — класс атак, направленный на уязвимости в практической реализации криптосистемы.*

Позже было выявлено несколько наиболее успешных «сторонних каналов»:

- Время выполнения криптографических операций;
- Потребляемая мощность;
- Электромагнитное излучение;
- Издаваемые процессором звуки;
- Излучение от экрана.

Атаки по сторонним каналам классифицируются по следующим трём типам:

1. По контролю над вычислительным процессом: *пассивные* и *активные*.
2. По способу доступа к модулю: *агрессивные (invasive), полуагрессивные (semi-invasive)* и *неагрессивные (non-invasive)*.
3. По методу, применяемому в процессе анализа: *простые - simple side channel attack (SSCA)* и *разностные - differential side channel attack (DSCA)*.

Выделим основные атаки, известные в настоящее время:

- Атака по времени (Timing attacks).
- Атака зондированием (Probing attack).
- Атаки по энергопотреблению (Power Analysis Attack).
- Атаки по ошибкам вычислений (Fault Attacks).
- Атаки по электромагнитному излучению (Electro Magnetic Analysis).
- Атака по видимому излучению (Visible Light Attacks).
- Акустическая атака (Acoustic Attacks).
- Атаки на кэш (Cache-based Attacks).

Давайте разберем каждую из этих атак более подробно.

4.1 Атака по времени.

Атака по времени (Timing attack) основана на анализе времени, затрачиваемого на исполнение логических операций, проводимых криптографическим алгоритмом. В основном, данной атаке подвержены алгоритмы асимметричного шифрования, использующие такие операции как возведение в степень (алгоритмы Диффи-Хеллмана и RSA), использующие для проведения операций китайскую теорему об остатках (алгоритм RSA).

Данная атака относится к пассивным атакам, так как не вмешивается в

вычислительный процесс, а по способу доступа к модулю - не агрессивной, так как во время атаки производится только замер времени, без какого либо вмешательства.

Как раз атака по времени и была предложена Полом Кохером в его работе «Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems», которая стала началом данного направления.

4.2 Атака зондированием.

Атака зондированием (Probing Attack) является агрессивной пассивной атакой. При проведении атаки устройство, содержащее криптомодуль, вскрывается, и с помощью оптического микроскопа исследуется печатная плата. Для проведения исследования на проводники, по которым идут сигналы, устанавливаются щупы, далее сигнал записывается и анализируется. Так же во время проведения атаки исследуется состояние ячеек памяти.

Наиболее известные атаки в этой области были проведены Сергеем Скоробогатовым. В 2011 году он представил саму идею и первые успешные атаки зондирования в статье «Side-channel attacks: new directions and horizons».

4.3 Атаки по энергопотреблению.

Атака по энергопотреблению (Power Analysis Attack) является одной из самых распространенных атак по сторонним каналам, так как без потребления энергии криптомодуль работать не сможет. Данная атака является пассивной атакой, и тоже была предложена Полом Кохером.

Существует две разновидности атак по энергопотреблению:

- Простая атака по энергопотреблению (Simple Power Analysis).
- Разностная атака по энергопотреблению (Differential Power Analysis).

При проведении **простой атаки по энергопотреблению** атакующий производит анализ зависимости потребляемых устройством тока/мощности от времени. При выполнении криптомодулем разных операций происходят колебания потребляемой мощности, так как разные инструкции, исполняемые микропроцессором, оказывают разное

влияние на энергопотребление.

Данная атака очень чувствительна к реализации криптоалгоритма.

Дифференциальная/разностная атака по энергопотреблению проводит статистический анализ данных измерений энергопотребления криптосистемы. В отличие от простой атаки, дифференциальная атака не существенно зависит от реализации криптосистемы и есть возможность автоматизации процесса атаки.

4.4 Атака по ошибкам вычислений.

Атака по ошибкам вычислений (Fault–Induction Attack) является активной атакой. Суть атаки - осуществление различных воздействий на крипто- модуль с целью возникновения искажения информации на некоторых этапах шифрования. В дальнейшем анализ результатов, полученных после искажения информации, помогает восстановить исходный ключ. Наиболее распространенными вносимыми ошибками является:

- Изменение напряжения питания криптосистемы.
- Изменение конструкции шифратора (нарушение электрических контактов).
- Изменение тактовой частоты шифрующего устройства.
- Воздействие лазерным лучом или сфокусированным световым пучком.
- Воздействие переменным магнитным полем.
- Помещение устройства в сильное электромагнитное поле.
- Повышение температур некоторых частей криптомодулей.

Наиболее известные и интересные разработки в этой области были получены Сергеем Скоробогатовым, и были представлены в его работе ”Optical Fault Induction Attacks”.

4.5 Атаки по электромагнитному излучению.

Атака по электромагнитному излучению (Electromagnetic Analysis Attacks) является пассивной атакой. Во время работы криптомодули производят электромагнитное излучение. Связывая спектральные компоненты излучения с операциями, выполняемыми в устройстве, можно получить достаточно информации для определения секретного ключа или самой обрабатываемой информации.

Ряд успешных атак было произведено на:

1. DES и RSA;
2. AES и криптосистемы на эллиптических кривых реализованных на FPGA;
3. Криптографических хэш-функции.

4.6 Атака по видимому излучению.

Атака по видимому излучению (Visible Light Attack) является пассивной атакой, была предложенна Маркусом Куном в 2002 году и состоит в анализе излучения, производимого монитором.

4.7 Акустическая атака.

Акустическая атака (Acoustic cryptanalysis) разновидность пассивной атаки, направленная на получение информации из звуков, производимых компьютером, или иными шифрующими устройствами.

Данная атака была предложена Ади Шамиром и его командой в 2004 году в работе «RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis».

4.8 Атака на кэш.

Атака на кэш (Cache-Based Attacks) является одной из разновидностей атак по времени. Данный тип атак основывается на измерениях времени и частоты промахов в кэш процессора. Предложена данная атака была в 2003 году Yukiyasu Tsunoo, Teruo Saito, Tomoyasu Suzaki, Maki Shigeri
«Cryptanalysis of DES implemented on computers with cache».

Представленные выше атаки являются основными атаками по сторонним каналам.

Есть еще ряд очень интересных работ, одна из таких атак - атака по разности потенциалов Daniel Genkin, Itamar Pipman, Eran Tromer: “Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs”. Данный метод основан на том, что при выполнении различных операций энергопотребление меняется, данные колебания гасятся схемами регулирования напряжения, которые пытаются поддерживать постоянное напряжение, но колебания разности потенциалов отражаются во всех цепях подачи напряжения. Измерить колебания разности потенциалов можно через организацию физического контакта с нулевой фазой - «землей», например, подключив датчик к корпусу ноутбука. При данной атаке, криптографы смогли успешно подобрать 4096-разрядный ключ RSA.

Атаки по сторонним каналам являются наиболее перспективным и значимым направлением в современной криптографии. Они дают возможность получить информацию при относительно небольших временных и мощностных затратах, но у атак по сторонним каналам есть свой минус – для каждой реализации криптоалгоритма атака должна быть своя, универсальных атак, проводящих анализ в автоматическом режиме, пока не существует.

5.ЗАКЛЮЧЕНИЕ

На данной лекции мы познакомились с основными принципами криптоанализа. Вспомнили атаки, которые прошли во время нашего курса, рассмотрели идеи дифференциального и линейного криптоанализа. Узнали об основном виде современного криптоанализа – атакам по сторонним каналам, посмотрели какие атаки бывают и какие идеи они используют.