ПРАКТИЧЕСКАЯ КРИПТОЛОГИЯ
ЛЕКЦИЯ 1
Лектор: Сушко С.А.
Специальность: 6.170101 – Бсіт

§1. Основные определения

Криптология – наука, которая делится на криптографию и криптоанализ.

Предметом изучения ***криптографии*** есть шифрование информации с целью ее защиты от несанкционированного доступа. Из оригинального документа (обычный текст, цифровое изображение, звуковой сигнал и др.), который называют ***открытым текстом***, при шифровании образуется его зашифрованная версия, которую называют ***шифротекстом***, ***закрытым текстом***, ***криптограммой***. Если шифрование текста – прямая задача, то дешифрование, т.е. превращение шифрованного текста в открытый, – обратная задача.

криптография от древнегреческого κρυπτός — скрытый и γράφω — пишу.

Основные задачи (сервисы) криптографии:

1). ***Обеспечение конфиденциальности*** – защита информации от ознакомления с ней со стороны лиц, не имеющих доступа к ней (конфиденциальная информация = секретная, ограниченного доступа информация);

2). ***Аутентификация*** – это подтверждение подлинности сторон (идентификация) и самой информации в процессе информационного обмена (получатель сообщения хочет убедиться, что сообщение пришло именно от определенного лица, а не от кого-либо другого, даже если это лицо захочет это отрицать).

3) ***Обеспечение целостности*** – гарантирование, что информация при хранении или передаче не изменилась.

4) ***Обеспечение невозможности отказаться от авторства*** – предотвращение отказа субъектов от факта передачи сообщения и других совершенных ими действий. Когда сообщение отправлено, получатель может убедиться, что это сделал легальный отправитель. Аналогично, когда сообщение пришло, отправитель может убедиться, что оно получено легальным получателем.

5) ***Контроль доступа*** – возможность ограничить и контролировать доступ к системам и приложениям по коммуникационным линиям.

Практическое применение криптографии стало неотъемлемой частью жизни современного общества — её используют в таких отраслях как электронная коммерция, электронный документооборот (включая цифровые подписи), телекоммуникации и др.

Например, Интернет трафик защищен с помощью протокола HTTPS, беспроводной трафик, например, Wi-Fi трафик защищен с помощью WPA2 протокола, который является частью стандарта 802.11i, трафик сотовых телефонов защищен с помощью шифровального механизма GSM, Bluetooth трафик также защищен с помощью криптографии, и т.д. Криптография широко используется для защиты файлов, хранящиеся на диске путем их шифрования. Даже если диск будет украден, файлы не будут скомпрометированы. Когда вы покупаете DVD или Blu-Ray диски, фильмы на этих дисках записаны в зашифрованном виде, в частности, DVD использует систему под названием CSS (Contents Scrambling System), а Blu-Ray диски использует систему, называемую AACS.

Введем следующие понятия и обозначения:

1) алфавит A, с помощью которого записываются открытые тексты. Количество букв алфавита, называют его ***мощностью*** (обозн. $|A|$). Любой открытый текст – это упорядоченный набор слов, состоящих из букв алфавита.

2) Алфавит B для записи шифротекстов. Любой шифротекст – это слово в алфавите B, $|B|$ – мощность алфавита B (число его букв).

3) m – открытый текст, который необходимо зашифровать (обозначение от слова message – сообщение). Другие часто используемый обозначения открытого текста – M, x, p (от слова plaintext – открытый текст). Множества всех возможных открытых текстов или ***пространство открытых текстов*** обозначается также через M (или X).

4) c – шифротекст (закрытый текст, криптограмма), который получен в результате зашифрования (обозначение от слова cryptograma). Другие часто используемые обозначения шифротекста – C, y. Множества всех возможных шифротекстов или ***пространство шифротекстов*** обозначается также через C (или Y).

5) ***Зашифрование*** – процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа. ***Расшифрование*** – процесс нормального применения криптографического преобразования шифротекста в открытый. ***Дешифрование*** – процесс извлечения открытого текста без знания криптографического ключа на основе известного шифротекста.

6) ***Ключ*** k – сменный параметр шифра, определяющий выбор конкретного преобразования данного текста. k_1 ***– ключ зашифрования,*** k_2 ***– ключ зашифрования.*** Множество всех возможных ключей или пространство ключей обозначается K (от слова key – ключ). Иногда мы будем через K_1 и K_2 обозначать ***множества ключей зашифрования и расшифрования*** соответственно.

7) ***Криптоалгоритм зашифрования/расшифрования*** – это математически связанные функции, используемые для шифрования и расшифрования. ***Уравнение зашифрования***

$$c = E_{k_1}(m), \text{ где } c \in C,\ m \in M,$$

уравнение расшифрования

$$m = D_{k_2}(c)$$

(или в др. обозначениях $y = E_{k_1}(x)$, $x = D_{k_2}(y)$). Использованные символы E и D для функции зашифрования и расшифрования происходят от англ. слов encryption – шифрование, decryption – расшифрование.

8) ***Криптосистема*** или ***шифр*** – множество обратимых функций отображения множества открытых текстов M во множество шифротекстов C, зависящих от ключа. Другими словами, это алгоритм преобразования обратимых преобразований открытого текста в шифротекст и наоборот. Каждое конкретное отображение отвечает шифрованию с одним конкретным ключом (на сленге – шифрование на ключе). Для задания криптосистемы (шифра) надо указать:

- множество M открытых текстов;
- множество C шифротекстов;
- множества K_1 и K_2 ключей зашифрования и расшифрования соответственно;
- алгоритм генерации ключей;
- криптоалгоритм зашифрования $C = E_{K_1}(M)$;
- криптоалгоритм расшифрования $M = D_{K_2}(C)$.

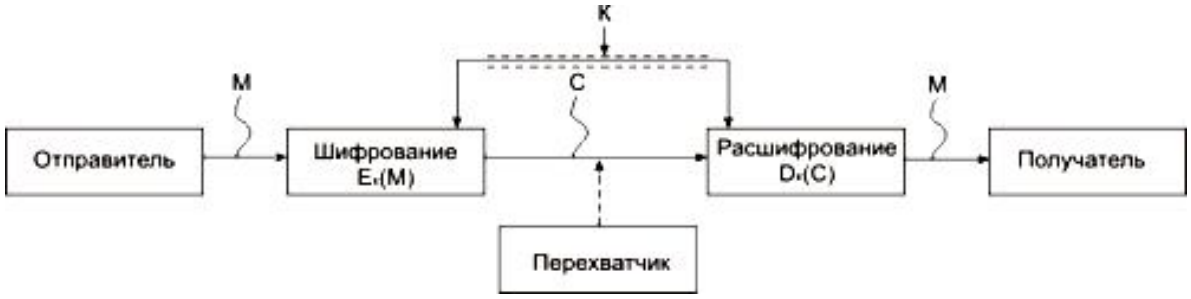
Для каждого ключа зашифрования k_1 функция $c = E_{k_1}(m)$ должна быть обратимой:

$$D_{k_2}(E_{k_1}(m)) = m, \text{ т.е. } \quad D = E^{-1}$$

Обратимость – основное условие шифрования, по которому каждому зашифрованному сообщению c ставится одно исходное сообщение m.

Обобщенная схема криптографической системы, обеспечивающей шифрование передаваемой информации, показана на рисунке. Отправитель генерирует открытый текст исходного сообщения M, которое должно быть передано законному получателю по незащищенному каналу. За каналом следит перехватчик с целью перехватить и раскрыть передаваемое сообщение. Для того чтобы перехватчик не смог узнать содержание сообщения M, отправитель шифрует его с помощью обратимого преобразования $E_{k_1}(M)$ и получает шифртекст $C = E_{k_1}(M)$, который отправляет получателю.

Законный получатель, приняв шифртекст C, расшифровывает его с помощью обратного преобразования $D = E^{-1}$ и получает исходное сообщение ввиде открытого текста M:



Раскрытие (***взлом***) ***шифра***, ***атака на шифр*** – это действия противника с целью получить открытый текст из шифрованного текста без знания шифра или ключа.

Методы вскрытия шифров, их применение изучает вторая часть криптологии – ***криптоанализ***.

Термин «криптоанализ» впервые ввел в криптологию Вильям Фридман в 1920 г. [14].

Если криптография – наука о создании шифров, то криптоанализ – искусство их взлома.

§2. Различные классификации криптоалгоритмов

- По секретности алгоритма:
  - ***ограниченные криптосистемы***, когда надо сберегать в тайне сам алгоритм шифрования.
  - ***криптосистемы общего использования,*** основанные на правиле Керкгоффса. ***Правило Керкгоффса –*** это фундаментальное допущение криптоанализа, о том, что секретность сообщения всецело зависит от ключа, т.е. весь механизм шифрования, кроме значения ключа, известен противнику. Как бы то ни было, секретность алгоритма не является большим препятствием: например, для

определения типа программно реализованного криптографического алгоритма требуется лишь несколько дней анализа исполняемого кода. Таким образом, далее принимаем, что ***секретность шифра обеспечена секретностью ключа шифрования, а не секретностью алгоритма***. (*Правило сформулировано в книге «La Cryptographie militare» в конце XIX ст. голландцем Огюстом Керкгоффсом, преподававшим немецкий язык в Париже*).

- По типу организации секретной связи:
  - ***симметричные криптосистемы***, в которых ключи для шифрования и дешифрования совпадают или могут легко вычисляться один из другого. Здесь защита информации обеспечена секретностью ключей (нужен тайный канал обмена ключами). Ключи шифрования и расшифрования должны быть известны легальным пользователям и храниться в секрете от злоумышленника (криптоаналитика). Если есть n группа людей, в которой каждый должен иметь связь друг с другом, то для организации связи необходимо $\frac{n(n-1)}{2}$ ключей, так как каждому надо $n-1$ ключ, чтобы связаться с остальной частью группы, но ключ между А и В может использоваться в обоих направлениях. Поэтому для симметричных криптосистем возникает ***задача распределения секретных ключей*** между легальными пользователями – надежное создание и доставка уникальных секретных ключей для всех пар пользователей.
  - асимметричные криптосистемы или криптосистемы с открытым ключом позволяют организовать секретную связь без предварительного секретного обмена ключами. Криптосистема называется ***криптосистемой с открытым ключом (асимметричной криптосистемой)***, если один из ключей (ключ шифрования), называемый ***открытым ключом***, известен всем пользователям, включая криптоаналитика, а другой ключ известен только передающей или принимающей стороне. Этот сберегаемый в тайне ключ (для расшифрования) называется ***секретным (закрытым)***. Считают, что такие криптосистемы родились в 1976 г., когда была опубликована статья американских математиков Вайтфилда Диффи и Мартина Хеллмана «Новые направления в криптографии», где они ввели понятие односторонней функции с лазейкой. На сегодняшний день

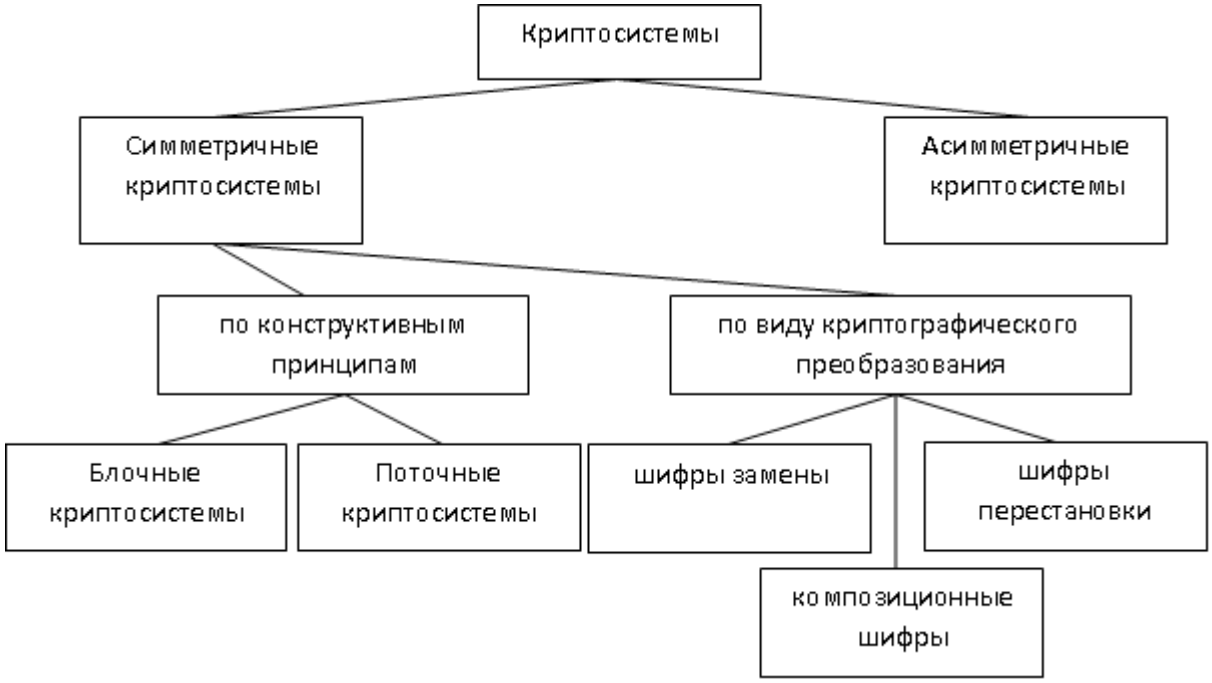
симметричные криптосистемы обладают высокой скоростью шифрования данных (десятки мегабайт в секунду на ПК), а известные криптосистемы с открытым ключом – низкой скоростью (килобайты в секунду на ПК). В то же время общедоступность открытого ключа для всех пользователей в асимметричной криптосистеме позволяет строить удобные системы аутентификации пользователей и последующего распределения ключей, так как нет необходимости держать открытый ключ в секрете. Поэтому симметричные криптосистемы из-за высокой скорости используют для шифрования данных, в то время как асимметричные – для аутентификации и создания секретных сеансовых ключей для симметричного шифрования данных.

Два основных типа симметричных шифров:

- ***блоковые шифры***, которые шифруют открытый текст, разбивая его на блоки. Один и тот же блок данных в любом месте открытого текста переходит в одинаковый блок криптограммы.
- ***потоковые шифры*** оперируют бытовыми или байтовыми потоками открытых текстов и при шифровании один и тот же бит может перейти в разные биты криптограммы.

❖ По используемым средствам шифрования:

- программные
- аппаратные (все процедуры шифрования и расшифрования выполняются специальными электронными схемами по определенным логическим правилам).
- программно-аппаратные (см. Приложение 1).



- По виду криптографических преобразований:
  - Перестановочные – блоки информации (байты, биты, более крупные единицы) не изменяются сами по себе, но изменяется их порядок следования, что делает информацию недоступной стороннему наблюдателю
  - Подстановочные (замены). Эти шифры заменяют символы открытого текста или их группы на другие, но сохраняющие приэтом их положение в тексте

История криптографии насчитывает около 4 тысяч лет. Как основной критерий ее периодизации используют технологические характеристики используемых методов шифрования:

I период – приблизительно с 3-го тысячелетия до н. э. – характеризуется господством моноалфавитных шифров (основной принцип — замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами).

II период – с IX века на Ближнем Востоке и с XV в. в Европе до начала XX века – ознаменовался введением в обиход полиалфавитных шифров.

III период – с начала и до середины XX века – характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.

IV период – с середины до 70-х годов XX века — период перехода к математической криптографии, когда в работе Клода Шеннона

появляются строгие математические определения количества информации, энтропии, функции шифрования.

Однако до 1975 года криптография оставалась «классической», или же, более корректно, криптографией с секретным ключом.

Современный период развития криптографии (с конца 1970-х годов по настоящее время) отличается зарождением и развитием нового направления — криптография с открытым ключом. Её появление знаменуется не только новыми техническими возможностями, но и сравнительно широким распространением криптографии для использования частными лицами.

Современная криптография образует отдельное научное направление на стыке математики и информатики — работы в этой области публикуются в научных журналах, организуются регулярные конференции.

Потоковым шифрам отдают предпочтение военные организации всего мира, а банковские структуры – блоковым шифрам, так как потоковые шифры малопригодны для программной реализации из-за побитового шифрования и расшифрования. Программная реализация блоковых шифров проще, так как вместо манипулирования с битами они оперируют с большими блоками данных.

§3. Основные параметры шифров

1). ***Криптографическая стойкость шифра*** – способность шифра противостоять атакам на него. Для современных симметричных алгоритмов основной характеристикой криптостойкости является длина ключа. Шифрование с ключами длиной 128 бит и выше считается сильным, так как для расшифровки информации без ключа требуются годы работы мощных суперкомпьютеров. Для асимметричных алгоритмов, основанных на проблемах теории чисел (проблема факторизации в RSA, проблема дискретного логирифмирования в системе Эль-Гамаля) в силу их особенностей минимальная надёжная длина ключа в настоящее время — 1024 бит. Для асимметричных алгоритмов, основанных на теории эллиптических кривых, минимальной надёжной длиной ключа считается 163 бит, но рекомендуются длины от 191 бит и выше.

Криптостойкость обычно оценивают одной из следующих величин:

− количеством всех возможных ключей (если длина ключа равна N бит, то число всех возможных ключей составляет 2^N).

− количеством операций или временем (с заданными ресурсами), необходимым для взлома шифра с заданной вероятностью и т. д.

2). ***Отсутствие статистической зависимости между открытым текстом и криптограммой*** (криптограмма не должна отличаться от истинно случайной последовательности символов, изменение любого бита ключа при неизменном открытом тексте должно менять 50% битов криптограммы, а изменение любого быта открытого текста при неизменном ключе – 50% криптограммы).

3). ***Сложность вскрытия шифра*** – современных криптографов интересуют шифры, которые сложно сломать доступными компьютерными средствами. Оценивают объем информации, нужный для вскрытия, время обработки, быстродействие и память компьютера.

4). ***Сложность операций шифрования и расшифрования*** – предпочтение отдают шифрам с более простыми операциями.

5). ***Разрастание количества ошибок –*** у некоторых шифров ошибка в одной букве при шифровании вызывает большое количество ошибок в криптограмме.

6). ***Имитостойкость –*** способность противостоять попыткам навязать законному пользователю неправильную информацию путем искажения или подмены криптограммы на другую.

7). ***Помехоустойчивость –*** способность шифра противостоять помехам в канале связи при передаче шифрованных сообщений.

8). ***Увеличение длины сообщения*** – некоторые шифры значительно увеличивают длину криптограммы по сравнению с длиной открытого текста. Такой нежелательный эффект наблюдается например при попытках замаскировать статистику повторений букв текста с помощью введения в криптограмму вспомогательных символов («пустышек»).

§4. Типы криптоаналитических атак

Действия криптоаналитика (злоумышленника) восстановить из шифротекста открытый текст без знания ключа или шифра называется ***атакой***. Успешную криптоаналитическую атаку называют ***взломом шифра*** или ***вскрытием***.

Атаки могут быть пассивными и активными. **Пассивной** называется атака, при которой противник не имеет возможности изменять передаваемые сообщения. При пассивной атаке возможно лишь прослушивание передаваемых сообщений, их дешифрование и анализ трафика. При **активной** атаке противник может модифицировать передаваемые сообщения и даже добавлять свои сообщения.

- ***классификация атак по доступу к открытому и зашифрованному текстам***

1. **Атака на основе только известного шифротекста.** Криптоаналитик имеет только шифротексты $C_1, C_2, ..., C_i$ сообщений, зашифрованные на одном ключе одним алгоритмом E_k. Задача криптоаналитика – раскрыть исходные открытые тексты $M_1, M_2, ..., M_i$ или, еще лучше, вычислить ключ k шифрования, чтобы расшифровать потом и другие сообщения. Этот вариант соответствует модели внешнего нарушителя, который имеет физический доступ к линии связи, но не имеет доступ к аппаратуре шифрования и расшифрования.

2. **Атака на основе известного открытого текста.** Криптоаналитик имеет доступ не только к шифротекстам $C_1, C_2, ..., C_i$ сообщений, но также к открытым текстам $M_1, M_2, ..., M_i$ этих сообщений. Задача криптоаналитика – найти ключ k, используемый для шифрования или способ дешифрования новых шифротекстов, полученных на том же ключе. Возможность проведения такой атаки складывается при шифровании стандартных документов, подготавливаемых по стандартным формам, когда определенные блоки данных повторяются и известны. Он также применим при использовании режима глобального шифрования, когда вся информация на встроенном магнитном носителе записывается в виде шифротекста, включая главную корневую запись, загрузочный сектор, системные программы и пр. При хищении этого носителя (или компьютера) легко установить, какая часть криптограммы соответствует системной информации, и получить большой объем известного исходного текста для выполнения криптоанализа.

3. **Атака с выбором известного открытого текста**. Криптоаналитик не только имеет доступ к шифротекстам $C_1, C_2, ..., C_i$ и соответствующих им открытым текстам $M_1, M_2, ..., M_i$, но и может по желанию выбирать открытые тексты, которые затем получает в зашифрованном виде. Такой криптоанализ получается более мощным по сравнению с криптоанализом с известным открытым текстом, потому что криптоаналитик может выбрать для шифрования такие блоки открытого текста, которые дадут больше информации о ключе. Задача криптоаналитика – поиск ключа k шифрования или способ дешифрования новых шифротекстов, полученных на том же ключе. Этот вариант атаки соответствует модели внутреннего нарушителя. На практике такая ситуация может возникнуть при вовлечении в криптоатаку лиц, которые не знают секретного ключа, но в силу своих служебных полномочий имеют доступ к шифратору.

4. **Атака с выбором известного шифротекста**. Криптоаналитик может выбирать для расшифрования различные шифротексты

$C_1, C_2, ..., C_i$ и получить соответствующие им открытые тексты $M_1, M_2, ..., M_i$. Задача криптоаналитика – поиск ключа k, использованного для шифрования. Этот тип криптоатак представляет особый интерес для алгоритмов с открытым ключом.

Отдельно отметим **атаки по побочным каналам** – так называют атаки, основанные на информации, которую можно получить из устройства для шифрования и которая не является ни открытым текстом, ни шифротекстом (время выполнения операций шифрования, потребленная при этом мощность и др., электромагнитное излучение, анализ кеш-памяти). Задача криптоаналитика – определение ключа шифрования и восстановление открытых текстов из шифротекстов.

Эффективность защиты данных зависит от сопутствующей информации, известной криптоаналитику. Так, стандартные тексты в начале и конце сообщения («Здравствуйте», «До свидания»; если источник сообщения есть президент, то он может закончиться его подписью). Кроме того, противник может убедить владельца секретного ключа переслать криптограмму определенного открытого текста. Как пример этого, приведем прием, использованный командованием военно-морским флотом США во Второй мировой войне перед битвой на Мидуэе. Чтобы удостовериться в правильности взлома японского военного шифра, криптоаналитики США попросили американский гарнизон, дислоцированный на Мидуэе, проинформировать открытым незащищенным о недостатке пресной воды. Через два дня было перехвачено секретное сообщение, в котором японцы, следившие за каналом, сообщили о проблеме с водою в некотором районе «AF». Благодаря этому американцы узнали, что «AF» – кодовое обозначение Мидуэи в криптограммах противника. Сопутствующая информация может содержаться также с переданными данными – запись файла по сбыту нередко организован таким образом: фамилия и адрес клиента внесены в один сегмент, условия продажи – в другой, дата – в третий. Как уже отмечалось, небезопасны и шифрованные коды программ из-за частого использования ключевых слов (в языках программирования C та C++ – for, while, if, else, return). Все это – дополнительный фактаж для криптоаналитика.

Поэтому атаки с использованием известного или подобранного открытого текста встречаются чаще, чем можно думать. Необходимое требование к современному хорошему криптоалгоритму: он должен противостоять атакам на основе выбранных открытых текстов. Это означает, что все предыдущие дешифрования любой информации не

облегчают дешифровку новых криптограмм, полученных на одном ключе.

❖ *Классификация атак по объему ресурсов, необходимых для их осуществления*

• по памяти – объем памяти, требуемый для реализации атаки;

• по времени – количество элементарных операций, которые необходимо выполнить для проведения атаки. К примеру, если атака имеет сложность 2^{128}, то это значит, что для взлома шифра требуется выполнить 2^{128} операций;

• по объему данных – необходимый объём открытых и соответствующим им зашифрованных текстов, необходимых для проведения атаки. В некоторых случаях эти параметры являются взаимозависимыми: например, за счет увеличения памяти можно сократить время атаки.

Взлом ключа шифра без применения криптоанализа (например, подкуп, воровство) называют ***компрометацией ключа***.

Криптографическая стойкость криптосистемы – свойство криптосистемы (криптопротокола), характеризующее её (его) способность противостоять атакам злоумышленника, с целью получить ключ секретный или открытое сообщение. Стойкость криптосистемы – фундаментальное понятие криптографии. Стойким считается шифр, который для успешной атаки требует от противника недостижимых вычислительных ресурсов, недостижимого объёма перехваченных открытых и зашифрованных сообщений или же такого времени раскрытия, что по его истечению защищенная информация будет уже не актуальна, и т. д.

§5. Полный перебор

Другие названия метода полного перебора – ***проба на ключ***, ***систематический поиск***, ***грязная атака***, ***лобовой взлом, метод «грубой силы»*** (от англ. brute force).

Полный перебор – универсальный метод криптоанализа, суть которого в испытании всех возможных ключей ключевого пространства.

1-ый вариант: перехватив пару «шифротекст – соответствующий открытый текст», криптоаналитик дешифрует шифротекст на всех допустимых ключах поочередно, пока не получит совпадения с открытым текстом.

2-ый вариант: криптоаналитик осуществляет атаку на основе только шифротекста. Как в этом случае определить правильность дешифрования? Если шифровался графический файл или программа, то задача определения «осмысленности» выходных данных становится очень трудной. В более простом случае, когда известно, что открытый текст есть предложение на естественном языке, проанализировать результат и опознать успешный исход дешифрования сравнительно несложно, тем более что нередко криптоаналитик располагает некоторой априорной информацией о содержании сообщения. Требуется по небольшому отрезку текста решить, что собой представляет дешифрованный текст: осмысленное сообщение или набор случайных символов. Однако вручную выполнить анализ множества фрагментов дешифрированных текстов невозможно. Поэтому задачу выделения осмысленного текста (то есть обнаружение правильно дешифрированного текста) решают с помощью ЭВМ. В этом случае используют теоретические положения, разработанные в конце XIX века петербургским математиком Марковым А.А., - так называемые цепи Маркова.

Устойчивость к brute-force атаке определяет используемый в криптосистеме ключ шифрования. С увеличением длины ключа сложность взлома этим методом возрастает экспоненциально. В простейшем случае шифр длиной в N битов взламывается, в наихудшем случае, за время, пропорциональное 2^N.

Скорость определяется двумя факторами: 1) скоростью тестирования одного ключа; 2) количеством всех ключей. Если пространство решений очень велико, то полный перебор может не дать результатов в течение нескольких лет или даже столетий.

Пусть пространство ключей насчитывает $|K|$ ключей, проверка одного ключа состоит из одной операции. Тогда полный перебор всех $|K|$ ключей требует $|K|$ операций. Если все ключи равновероятны, то вероятность правильно угадать ключ с первого раза равна $\frac{1}{|K|}$. В качестве оценки трудоемкости метода перебора выбирают математическое ожидание $M(\alpha)$, где α – количество уже проверенных ключей до момента нахождения правильного ключа. Случайная величина α распределена равномерно, поэтому $M(\alpha) = \frac{|K|}{2}$. Например, если длина ключа шифра 8 битов, то общее количество ключей равно $|K| = 2^8 = 256$ и тогда с вероятностью $1/2$ ключ будет определен после

половины всех проверок. Если ж длина ключа 56 битов, то существует 2^{56} разных ключей. Если за 1 секунду компьютер перебирает 1 миллион ключей, то поиск правильного ключа в среднем будет длиться 2285 лет.

В таблице представлено оценочное время полного перебора паролей в зависимости от их длины. Предполагается, что в пароле могут использоваться 36 различных символов (латинские буквы одного регистра + цифры), а скорость перебора составляет 100 000 паролей в секунду.

Кол-во знаков	***Кол-во вариантов***	***Время перебора***
1	*36*	*менее секунды*
2	*1296*	*менее секунды*
3	*46 656*	*менее секунды*
4	*1 679 616*	*17 секунд*
5	*60 466 176*	*10 минут*
6	*2 176 782 336*	*6 часов*
7	*78 364 164 096*	*9 дней*
8	*2,821 109 9x10^{12}*	*11 месяцев*
9	*1,015 599 5x10^{14}*	*32 года*
10	*3,656 158 4x10^{15}*	*1162 года*
11	*1,316 217 0x10^{17}*	*41 823 года*
12	*4,738 381 3x10^{18}*	*1 505 615 лет*

Видно, что пароли длиной до 6 символов в общем случае не являются надежными.

Алгоритмы полного перебора допускает ***распараллеливание***, что ускоряет поиск правильного ключа. Существует два способа распараллеливания: 1) ***построение конвейера***, когда каждый процессор выполняет часть операций по восстановлению ключа и передает свои данные другому процессору; 2) ***разбиение пространства ключей*** K на непересекающиеся подмножества с последующим перебором одним процессором одного подмножества.

В криптографии на вычислительной сложности перебора основывается оценка криптостойкости шифров. В частности, шифр считается криптостойким, если не существует метода «взлома», существенно более быстрого, чем полный перебор ключей. Метод полного перебора – универсальная атака (применим ко всем шифрам), но и самая долгая.

Заметим, что в криптоанализе раскрытие шифра – это необязательно полное восстановления ключа и текста по перехваченной криптограмме. Шифр считают сломанным, если в криптосистеме найдена слабость, которую можно использовать для более

эффективного взлома, нежели, метод полного перебора. Например, если для дешифровки криптограммы полным перебором надо перебрать 2^{128} возможных ключей, то дешифровка, которая выполняется за 2^{110} операций, уже будет считаться вскрытием шифра.

Оценим минимальную битовую длину ключа для защиты криптосистемы от атаки полным перебором всех возможных секретных ключей. Сделаем такие предположения:

· одно ядро процессора выполняет $R = 10^7 \approx 2^{23}$ шифрований и расшифрований в секунду;

· вычислительная сеть состоит из $n = 10^3 \approx 2^{10}$ узлов;

· в каждом узле имеется $C = 16 = 2^4$ ядер процессора;

· нужно обеспечить защиту данных на $T = 100$ лет $\approx 2^{32}$ с;

· выполняется закон Мура: удвоение вычислительной производительности на единицу стоимости каждые 2 года, то есть за 100 лет производительность вырастет в $M = 2^{T/2} \approx 2^{50}$ раз.

Число переборов N примерно равно

$$N \approx RnCTM \quad N \approx 2^{23}2^{10}2^{4}2^{32}2^{50} = 2^{119}.$$

Следовательно, минимально допустимая длина ключа для защиты от атаки перебором на 100 лет составляет $\log_2 N \approx 119$ бит.

ПРИЛОЖНИЕ 1

Что такое закон Мура?

Закон Мура (Moore) оценивает развитие вычислительной техники во времени. В базовом варианте он гласит, что для заданной стоимости (в широком смысле, включая энергопотребление, производство оборудования, износ, стоимость хранения, и т.д.) вычислительная мощность увеличивается в 8 раз каждые 3 года. Говоря более точно, можно сказать, что через каждые три года, технологические достижения позволяют разместить в 4 раза больше логических элементов в микросхеме заданной стоимости, одновременно ускоряя ее быстродействие в 2 раза.

Этот закон замечательно подтверждался в течение последних 15 лет. Следует отметить, что центральные микропроцессоры компьютеров общего назначения не полностью следуют этому закону, потому что они не могут так же быстро увеличить размер шины данных (по соображениям обратной совместимости кода, а также потому, что вычисления, которые эти процессоры обычно производят, имеют дополнительные ограничения, делающие бесполезным использование слишком больших регистров).

Это касается, таким образом, систем, описываемых в терминах логических элементов, специализированных на конкретном алгоритме. Таким образом, это по сути ASIC (Application Specific Integrated Circuit - специализированные микросхемы) и FPGA (Field Programmable Gate Arrays - программируемые логические интегральные схемы); то есть перепрограммируемые цепи, выполняющие те же задачи, что и ASIC, но вдвое более дорогие при заданной мощности, однако являющиеся многоцелевыми).

Какова предполагаемая стоимость полного перебора с использованием специализированного оборудования?

Если закон Мура будет продолжать выполняться (и не имеется веских оснований для обратного, так как он учитывает качественные достижения, а не только увеличение точности обработки кремния), можно достичь машины EFF (четверть миллиона долларов, для 56 бит за 3 дня) и добавлять 3 бита каждые 3 года (3 бита = 2^3 = 8; что дает в 8 раз больше возможных вариантов ключей).

Заметим, что для сохранения закон Мура, качественные достижения должны происходить достаточно быстро, так как имеются пределы в увеличении плотности элементов на кристалле кремния (замедление вследствие туннельного эффекта). В ряде разрабатываемых методов предполагается осуществить замену кремния на арсенид галлия, что позволит достичь более высокой плотности элементов, замену алюминия медью, которая позволяет работать гораздо более быстро, построение оптической логики (оптический элемент переключается приблизительно в 100 раз быстрее электронного, но его стоимость выше более чем в 100 раз).

Таким образом, можно считать, подобрать полным перебором 128-битный ключ так же "легко", как сейчас 56-битный, станет возможным через 72 года. Эта оценка является "наилучшей", в то время как многие исследователи этой тематики полагают, что закон Мура будет выполняться в лучшем случае еще несколько лет (действительно, все качественные изменения, привнесенные за последних 15 лет, были просто нереализованными, известными с 1975 года, и их запас почти исчерпан в настоящее время).

Физическая аналогия	**Число**
Время, оставшееся до наступления следующего ледникового периода	$16\text{-}10^{3}$ (2^{14}) лет
Время, оставшееся до превращения Солнца в новую звезду	10^{9} (2^{30}) лет
Возраст Земли	10^{9} (2^{30}) лет
Возраст Вселенной	10^{10} (2^{32}) лет

Количество атомов, из которых состоит Земля	$10^{51}(2^{170})$
Количество атомов, из которых состоит Солнце	$10^{57}(2^{190})$
Количество атомов, из которых состоит наша Галактика	$10^{67}(2^{223})$
Количество атомов, из которых состоит Вселенная	$10^{77}(2^{265})$
Объем Вселенной	$10^{84}(2^{280})см^{3}$

ПРИЛОЖЕНИЕ 2

Аппаратная реализация операций шифрования и расшифрования

До недавних пор алгоритмы шифрования реализовывались в виде отдельных устройств, что обусловливалось использованием криптографии для засекречивания различных видов передачи информации (телеграф, телефон, радиосвязь). С развитием средств вычислительной техники и общедоступных сетей передачи данных появились новые возможности применения криптографических алгоритмов. Однако аппаратная реализация до сих пор широко используется не только в военной сфере, но и в коммерческих организациях. Подобная «живучесть» аппаратных средств криптографической защиты информации объясняется рядом факторов:

1) аппаратная реализация обладает лучшими скоростными характеристиками, нежели программно реализуемые алгоритмы шифрования. В отличие от процессоров общего назначения использование специальных чипов, адаптированных к зашифрованию/ расшифрованию, оптимизирует математические операции, применяемые в алгоритмах шифрования.

2) аппаратные средства защиты информации обладают большей защищенностью как от побочных электромагнитных излучений, возникающих в ходе работы аппаратуры, так и от непосредственного физического воздействия на устройства для шифрования и хранение ключевой информации (в случае обнаружения несанкционированного доступа к современной микросхеме она саморазрушается).

3) аппаратные средства более удобны в эксплуатации (зашифрование/расшифрование происходит для пользователя в прозрачном режиме), легко инсталлируются.

Программная реализация операций шифрования и расшифрования

Достоинства программной реализации:

1) гибкость и переносимость (программу, написанную под одну операционную систему, можно модифицировать под любой тип ОС).

2) современные разработки в области криптографических протоколов недоступны для реализации в виде аппаратных средств.

Недостаток программной реализации – возможно вмешательство в действие алгоритмов шифрования и получения доступа к ключевой информации, хранящейся в общедоступной памяти.

Программно-аппаратная реализация операций шифрования и расшифрования

Основная функция аппаратной части программно-аппаратного комплекса криптографической защиты информации – генерация ключей и их хранение в устройствах, защищенных от несанкционированного доступа. Это позволяет идентифицировать пользователей с помощью паролей (фиксированных или однократных, которые могут храниться на различных носителях ключевой информации - смарт-карты,etoken и т.д.) либо на основе уникальных для каждого пользователя биометрических характеристик. Устройства считывания подобных сведений могут входить в состав программно-аппаратной реализации средств защиты информации.

Обычно криптографические алгоритмы реализуют в программном виде для выполнения на микропроцессорах общего назначения. В последнее время все большее распространение получает разработка аппаратных вариантов алгоритмов на базе:

- ***интегральных схем ASIC*** (*application-specific integrated circuit*) , специализированные для решения одной конкретной задачи. ASIC обычно содержат 32-битный процессор, блоки памяти и другие крупные блоки. Такие ASIC часто называют системой на кристалле (*System-on-a-Chip*). ASIC-чипы хороши только для строго конкретных задач, под которые они и изготовлены, обладая при этом наилучшими показателями в сравнении с другими возможными решениями; имеют наименьшее энергопотребление и наибольшее быстродействие. Отметим низкую себестоимость.готовых ASIC-чипов и астрономическую дороговизну самой разработки.
- ***программируемых пользователем вентильных матриц FPGA*** (Field-Programmable Gate Array). Это архитектурная разновидность микросхем программируемой логики. Такая матрица может быть сконфигурирована производителем или разработчиком уже после изготовления путём изменения логики работы схемы с помощью языка проектирования. Если в схемах ASIC используются логические матрицы, которые конфигурируются один раз в процессе производства, то FPGA можно постоянно перепрограммировать и менять топологию

соединений в процессе использования. FPGA могут быть легко и быстро адаптированы под выполнение почти любой криптографической задачи или алгоритма. FPGA применяются также, как ускорители универсальных процессоров в суперкомпьютерах. С практической точки зрения, целесообразность использования FPGA в аппаратных устройствах обоснована резким уменшением временных затрат на выполненин многих арифметических и логических операций.

С другой стороны, описанные технологии одновременно усиливают и возможности криптоанализа. Сегодня на рынке можно найти FPGA-чипы стоимостью 200**$**, способные перебирать до 30 миллионов ключей в секунду, и ASIC-чипы за 10**$**, анализирующие 200 миллионов ключей в секунду.