МИНИСТЕРСТВО РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИИ И КОМУНИКАЦИИ РЕСПУБЛИКИ УЗБЕКИТСАН

НУКУССКИЙ ФИЛИАЛ ТАШКЕНСТКОГО УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИИ

Факультет: Компьютерный инжиниринг
Группа: 201-15 КИ рус (2в КИ)

Самостоятельная работа

По предмету: _____

На тему: Криптография

Сдал : _____

Принял(а) : _____

Содержание

Введение

1. Криптография
2. История криптографии
3. Терминология
4. Запреты
5. Криптоанализ
6. Основные методы криптоанализа
7. Криптографические генераторы случайных чисел

Список литературы.

Введение

Разные люди понимают под шифрованием разные вещи. Дети играют в игрушечные шифры и секретные языки. Это, однако, не имеет ничего общего с настоящей криптографией. Настоящая криптография должна обеспечивать такой уровень секретности, чтобы можно было надежно защитить критическую информацию от расшифровки крупными организациями - такими как мафия, транснациональные корпорации и крупные государства. Настоящая криптография в прошлом использовалась лишь в военных целях. Однако сейчас, со становлением информационного общества, она становится центральным инструментом для обеспечения конфиденциальности.

По мере образования информационного общества, крупным государствам становятся доступны технологические средства тотального надзора за миллионами людей. Поэтому криптография становится одним из основных инструментов обеспечивающих конфиденциальность, доверие, авторизацию, электронные платежи, корпоративную безопасность и бесчисленное множество других важных вещей.

Криптография не является более придумкой военных, с которой не стоит связываться. Настала пора снять с криптографии покровы таинственности и использовать все ее возможности на пользу современному обществу. Широкое распространение криптографии является одним из немногих способов защитить человека от ситуации, когда он вдруг обнаруживает, что живет в тоталитарном государстве, которое может контролировать каждый его шаг.

Криптография

Криптография – это одна из старейших наук, ее история насчитывает несколько тысяч лет, наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Изначально криптография изучала методы шифрования информации - обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

История криптографии

История криптографии насчитывает около 4 тысяч лет. В качестве основного критерия периодизации криптографии, возможно, использовать технологические характеристики используемых методов шифрования.

Первый 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).

Второй период (хронологические рамки - с IX века на Ближнем Востоке и с XV века в Европе - до начала XX века) ознаменовался введением в обиход полиалфавитных шифров.

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

Четвертый период (с середины до 70-х годов XX века), период перехода к математической криптографии. Появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования. 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 (в предыдущие эпохи использование криптографии было исключительной прерогативой государства). Правовое регулирование использования криптографии частными лицами в разных странах сильно различается - от разрешения до полного запрета.

Современная криптография образует отдельное научное направление на стыке математики и информатики - работы в этой области публикуются в научных журналах, организуются регулярные конференции. Практическое применение криптографии стало неотъемлемой частью жизни современного общества - её используют в таких отраслях как электронная коммерция, электронный документооборот (включая цифровые подписи), телекоммуникации и других.

Терминология

Открытый текст - в криптографии исходный текст, подлежащий шифрованию, либо получившийся в результате расшифрования. Может быть

прочитан без дополнительной обработки. Открытый текст часто является читабельным текстом на одном из человеческих языков, в связи, с чем перед шифрованием (с использованием современной вычислительной техники) его сжимают с целями увеличения производительности и уменьшения избыточности, свойственной человеческим языкам.

Открытым текстом будет называться информация даже в том случае, если она сохранена в нетекстовом виде - например, музыка или звук. Главное, чтобы для использования данной информации не требовалось производить дешифрование.

Шифротекст - результат операции шифрования. Часто также используется вместо термина «криптограмма», хотя последний подчёркивает сам факт передачи сообщения, а не шифрования. Процесс применения операции шифрования к шифротексту называется перешифровкой.

Ключ - секретная информация, используемая криптографическим алгоритмом при шифровке или расшифровке сообщений, постановке и проверке цифровой подписи, вычислении кодов аутентичности. При использовании одного и того же алгоритма результат шифрования зависит от ключа. Для современных алгоритмов сильной криптографии утрата ключа приводит к практической невозможности расшифровать информацию.

Шифр - какая-либо система преобразования текста (код) для обеспечения секретности передаваемой информации. Шифры применяются для тайной переписки дипломатических представителей со своими правительствами, а также в вооруженных силах для передачи текста секретных документов по техническим средствам связи.

Шифр может представлять собой совокупность условных знаков (условная азбука из цифр или букв) либо алгоритм кодирования с использованием обычных цифр и букв. Процесс засекречивания сообщения с помощью шифра называется шифрованием.

Код - совокупность алгоритмов криптографических преобразований (шифрования), отображающих множество возможных открытых данных на

множество возможных зашифрованных данных, и обратных им преобразований. Важным параметром любого шифра является ключ - параметр криптографического алгоритма, обеспечивающий выбор одного преобразования из совокупности преобразований, возможных для этого алгоритма.

Шифрование - способ преобразования открытой информации в закрытую и обратно. Применяется для хранения важной информации в ненадёжных источниках или передачи её по незащищённым каналам связи.

Криптоанализ - наука о методах получения исходного значения зашифрованной информации, не имея доступа к секретной информации (ключу), необходимой для этого. В большинстве случаев под этим подразумевается нахождение ключа. В нетехнических терминах, криптоанализ есть взлом шифра (кода). Термин был введён американским криптографом Уильямом Фридманом в 1920 году.

Под термином «криптоанализ» также понимается попытка найти уязвимость в криптографическом алгоритме или протоколе. Хотя основная цель осталась неизменной с течением времени, методы криптоанализа претерпели значительные изменения, эволюционировав от использования лишь ручки и бумаги до широкого применения вычислительных мощностей специализированных криптоаналитических компьютеров в наши дни. Если раньше криптоаналитиками были большей частью лингвисты, то в наше время это удел «чистых» математиков.

Криптоаналитик - специалист по криптоанализу. Одним из первых криптоаналитиков был Аристотель, криптографически вскрывший скиталу - одно из первых известных криптографических устройств. Современный криптоаналитик должен иметь познания в области математики и теории алгоритмов. Часто также является криптографом - специалистом по созданию и использованию средств шифрования.

Дешифрование (дешифровка) - процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного.

Термин дешифрование обычно применяют по отношению к процессу криптоанализа шифротекста (криптоанализ сам по себе, может заключаться и в анализе шифросистемы, а не только зашифрованного ею открытого сообщения).

Криптографическая стойкость (или криптостойкость) - способность криптографического алгоритма противостоять возможным атакам на него или оценка алгоритма, способного взломать шифр. Атакующие криптографический алгоритм используют методы криптоанализа. Стойким считается алгоритм, 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.

Имитозащита - защита системы шифровальной связи или другой криптосистемы от навязывания ложных данных. Реализуется с помощью добавления к сообщению дополнительного кода, имитовставки, зависящей от содержания сообщения и секретного элемента, известного только отправителю и получателю (ключа). Закладка избыточности позволяет обнаружить внесённые в сообщение несанкционированные изменения.

Запреты

В Российской Федерации коммерческая деятельность, связанная с использованием криптографических средств, подлежит обязательному лицензированию. С 22 января 2008 года действует Постановление Правительства РФ от 29 декабря 2007 N 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами», которым приняты Положения о лицензировании деятельности по:

1. Распространению шифровальных (криптографических) средств;

2. Техническому обслуживанию шифровальных (криптографических) средств;

3. Предоставлению услуг в области шифрования информации;

4. Разработке, производству шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

Следует отметить, что приложения к данному Постановлению содержат жёсткие требования к лицу-соискателю лицензии, включая его образование, квалификацию, стаж, требования к помещению, охране, информационной и эксплуатационной безопасности при разработке и реализации средств. К примеру, требуется «наличие в штате у следующего квалифицированного персонала: руководитель или лицо, уполномоченное руководить работами по лицензируемой деятельности, имеющие высшее профессиональное образование или профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области не менее 5 лет; инженерно-технические работники, имеющие высшее профессиональное образование или прошедшие переподготовку в области информационной безопасности с получением специализации, необходимой для работы с шифровальными (криптографическими) средствами».

В настоящее время действует также Приказ ФСБ России от 9 февраля 2005 г. N 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение пкз-2005)», который определяет порядок разработки и эксплуатации криптографических средств.

В частности, согласно приказу, средства криптографии реализуются «юридическим лицом или индивидуальным предпринимателем, имеющим право на осуществление данного вида деятельности, связанного с шифровальными (криптографическими) средствами вместе с правилами пользования ими, согласованными с ФСБ России».

Ранее был издан Указ Президента РФ от 3 апреля 1995 N 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», постановивший «Запретить использование государственными организациями и предприятиями в информационно-телекоммуникационных системах шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись), и защищенных технических средств хранения, обработки и передачи информации, не имеющих сертификата Федерального агентства правительственной связи и информации при Президенте Российской Федерации, а также размещение государственных заказов на предприятиях, в организациях, использующих указанные технические и шифровальные средства, не имеющие сертификата Федерального агентства правительственной связи и информации при Президенте Российской Федерации».

Криптоанализ

Криптоанализ - наука о методах получения исходного значения зашифрованной информации, не имея доступа к секретной информации (ключу), необходимой для этого. В большинстве случаев под этим подразумевается нахождение ключа. В нетехнических терминах, криптоанализ есть взлом шифра (кода). Термин был введён американским криптографом Уильямом Ф. Фридманом в 1920 году.

Под термином «криптоанализ» также понимается попытка найти уязвимость в криптографическом алгоритме или протоколе. Хотя основная цель осталась неизменной с течением времени, методы криптоанализа претерпели значительные изменения, эволюционировав от использования лишь ручки и бумаги до широкого применения вычислительных мощностей специализированных криптоаналитических компьютеров в наши дни. Если

раньше криптоаналитиками были большей частью лингвисты, то в наше время это удел «чистых» математиков.

Результаты криптоанализа конкретного шифра называют криптографической атакой на этот шифр. Успешную криптографическую атаку, дискредитирующую атакуемый шифр, называют взломом или вскрытием.

Классический криптоанализ. Хотя понятие криптоанализ было введено сравнительно недавно, некоторые методы взлома были изобретены десятки веков назад. Первым известным письменным упоминанием о криптоанализе является «Манускрипт о дешифровке криптографических сообщений», написанный арабским учёным Ал-Кинди ещё в 9 веке. В этом научном труде содержится описание метода частотного анализа.

Частотный анализ - основной инструмент для взлома большинства классических шифров перестановки или замены. Данный метод основывается на предположении о существовании нетривиального статистического распределения символов, а также их последовательностей одновременно и в открытом тексте, и в шифротексте. Причём данное распределение будет сохраняться с точностью до замены символов как в процессе шифрования, так и в процессе дешифрования. Стоит отметить, что при условии достаточно большой длины шифрованного сообщения моноалфавитные шифры легко поддаются частотному анализу: если частота появления буквы в языке и частота появления некоторого присутствующего в шифротексте символа приблизительно равны, то в этом случае с большой долей вероятности можно предположить, что данный символ и будет этой самой буквой. Самым простым примером частотного анализа может служить банальный подсчёт количества каждого из встречающихся символов, затем следуют процедуры деления полученного числа символов на количество всех символов в тексте и умножение результата на сто, чтобы представить окончательный ответ в процентах. Далее полученные процентные значения сравниваются с

таблицей вероятностного распределения букв для предполагаемого языка оригинала.

Современный криптоанализ. По мере развития новых методов шифрования математика становилась всё более и более значимой. Так, например, при частотном анализе криптоаналитик должен обладать знаниями и в лингвистике, и в статистике. В то время как теоретические работы по криптоанализу Энигмы выполнялись преимущественно математиками, например, Аланом Матисоном Тьюрингом. Тем не менее благодаря всё той же математике криптография достигла такого развития, что количество необходимых для взлома элементарных математических операций стало достигать астрономических значений. Современная криптография стала гораздо более устойчивой к криптоанализу, чем некогда используемые, устаревшие методики, для взлома которых было достаточно ручки и листа бумаги. Может показаться, что чистый теоретический криптоанализ не способен более эффективно взламывать современные шифры.

Бандитский криптоанализ. Криптоаналитик может использовать так называемый «человеческий фактор», т.е. пытаться с помощью шантажа, подкупа, пыток или иных способов получить информацию о системе шифрования или даже сам ключ шифрования. Например, дача взятки, как одна из разновидностей бандитского криптоанализа, может носить название «Вскрытие с покупкой ключа». Таким образом методика вскрытия построена на слабости людей как составной части системы защиты информации.

Бандитский криптоанализ считается очень мощным способом взлома системы, а зачастую и наилучшим путём вскрытия шифров.

Основные методы криптоанализа

Атака на основе шифротекста. Допустим, криптоаналитик обладает некоторым числом шифротекстов, полученных в результате использования одного и того же алгоритма шифрования. В этом случае криптоаналитик

может совершить только атаку на основе шифротекста. Целью криптографической атаки в этом случае является нахождение как можно большего числа открытых текстов, соответствующих имеющимся шифротекстам, или, что ещё лучше, нахождение используемого при шифровании ключа.

Входные данные для подобного типа атак криптоаналитик может получить в результате простого перехвата зашифрованных сообщений. Если передача осуществляется по открытому каналу, то реализация задачи по сбору данных сравнительно легка и тривиальна. Атаки на основе шифротекста являются самыми слабыми и неудобными.

Атака на основе адаптивно подобранного шифротекста. Атака такого типа является более удобным частным случаем атаки на основе подобранного открытого текста. Удобство атаки на основе адаптивно подобранного шифротекста состоит в том, что помимо возможности выбирать шифруемый текст, криптоаналитик может принять решение о шифровании того или иного открытого текста на основе уже полученных результатов операций шифрования. Другими словами, при осуществлении атаки на основе подобранного открытого текста криптоаналитик выбирает всего один большой блок открытого текста для последующего шифрования, а потом на основе этих данных начинает взламывать систему. В случае организации адаптивной атаки криптоаналитик может получать результаты шифрования любых блоков открытого текста, чтобы собрать интересующие его данные, которые будут учтены при выборе следующих отправляемых на шифрование блоков открытого текста и так далее. Наличие обратной связи даёт атаке на основе адаптивно подобранного шифротекста преимущество перед всеми вышеперечисленными типами атак.

Атака на основе подобранного ключа. Вопреки своему названию атака на основе подобранного ключа не подразумевает под собой того, что криптоаналитик занимается простым перебором ключей в надежде найти нужный. Атака такого типа строится на том, что криптоаналитик может

наблюдать за работой алгоритма шифрования, в котором используются несколько ключей. Криптоаналитик изначально ничего не знает о точном значении ключей, зато ему известно некоторое математическое отношение, связывающее между собой ключи. Примером тому может служить ситуация, когда криптоаналитик выяснил, что последние 80 битов у всех ключей одинаковы, хотя сами значения битов могут быть неизвестными.

Атака на основе подобранного открытого текста. Для осуществления такого типа атаки криптоаналитику необходимо иметь не только какое-то количество открытых текстов и полученных на их основе шифротекстов. Помимо прочего в данном случае криптоаналитик должен обладать возможностью подобрать несколько открытых текстов и получить результат их шифрования. Задачи криптоаналитика повторяют задачи для атаки на основе открытого текста, то есть получить ключ шифрования, либо создать дешифрующий алгоритм для данного ключа.

Получить входные данные для такого вида атаки можно, например, следующим образом:

1.Создать и отправить поддельное не зашифрованное сообщение якобы от одного из пользователей, которые обычно пользуются шифрованием.

2.В некоторых случаях можно получить ответ, в котором будет содержится зашифрованный текст, цитирующий содержание поддельного сообщения.

При осуществлении атаки подобного типа криптоаналитик имеет возможность подбирать блоки открытого текста, что при определённых условиях может позволить получить больше информации о ключе шифрования.

Атака на основе открытых текстов и соответствующих шифротекстов. Пусть в распоряжении криптоаналитика есть не только шифротексты, но и соответствующие им открытые тексты.

Тогда существуют два варианта постановки задачи:

1.Найти ключ, использованный для преобразования открытого текста в шифротекст

2.Создать алгоритм, способный дешифровать любое сообщение, закодированное с помощью этого ключа

Получение открытых текстов играет решающую роль в осуществлении этой атаки. Открытые тексты извлекают из самых различных источников. Так, например, можно догадаться о содержимом файла по его расширению.

В случае взлома переписки можно сделать предположение, что письмо имеет структуру типа:

- «Приветствие»
- «Основной текст»
- «Заключительная форма вежливости»
- «Подпись»

Следовательно, атака может быть организована путём подбора различных видов «Приветствия» (например, «Здравствуйте!», «Добрый день» и т. д.) или «Заключительной формы вежливости» (таких как «С уважением», «Искренне Ваш» и т. п.). Легко заметить, что данная атака сильнее атаки на основе одного лишь шифротекста.

Атака на основе подобранного шифротекста. Допустим, что у криптоаналитика имеется временный доступ к дешифрующему средству или устройству. В таком случае за ограниченный промежуток времени криптоаналитик может получить из известных ему шифротекстов соответствующие им открытые тексты, после чего криптоаналитику нужно будет приступать к взлому системы. При осуществлении подобного типа атаки цель взлома - получить ключ шифрования.

Криптографические генераторы случайных чисел

Криптографические генераторы случайных чисел производят случайные числа, которые используются в криптографических приложениях,

например - для генерации ключей. Обычные генераторы случайных чисел, имеющиеся во многих языках программирования и программных средах, не подходят для нужд криптографии (они создавались с целью получить статистически случайное распределение, криптоаналитики могут предсказать поведение таких случайных генераторов).

В идеале случайные числа должны основываться на настоящем физическом источнике случайной информации, которую невозможно предсказать. Примеры таких источников включают шумящие полупроводниковые приборы, младшие биты оцифрованного звука, интервалы между прерываниями устройств или нажатиями клавиш. Полученный от физического источника шум затем "дистиллируется" криптографической хэш-функцией так, чтобы каждый бит зависел от каждого бита. Достаточно часто для хранения случайной информации используется довольно большой пул (несколько тысяч бит) и каждый бит пула делается зависимым от каждого бита шумовой информаци и каждого другого бита пула криптографически надежным (strong) способом.

Когда нет настоящего физического источника шума, приходится пользоваться псевдослучайными числами. Такая ситуация нежелательна, но часто возникает на компьютерах общего назначения. Всегда желательно получить некий шум окружения --- скажем от величины задержек в устройствах, цифры статистики использования ресурсов, сетевой статистики, прерываний от клавиатуры или чего-то иного. Задачей является получить данные, непредсказуемые для внешнего наблюдателя. Для достижения этого случайный пул должен содержать как минимум 128 бит настоящей энтропии.

Список литературы.

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных кн. 1.-М.: Энергоатомиздат. -1994.-400с.

2. Вербицкий О.В.Вступление к криптологии.- Львов.: Издательство науково- техничной литературы.-1998.-300с.

3. Диффи У. Первые десять лет криптографии с открытым ключом //ТИИЭР, т. 76(1988)б Т5б с. 54-74.

4. Герасименко В.А., Скворцов А.А., Харитонов И.Е. Новые направления применения криптографических методов защиты информации.- М.: Радио и связь.-1989.-360с.

5. Миллер В. Использования эллиптических кривых в криптографии .: -1986.-417-426с.

6. Галатенко В.А. Информационная безопасность. –М.: Финансы и статистика, 1997. –158 с.

7. Грегори С. Смит. Программы шифрования данных // Мир ПК –1997. -№3. -С.58 - 68.

8. Ростовцев А. Г., Михайлова Н. В. Методы криптоанализа классических шифров. –М.: Наука, 1995. –208 с.