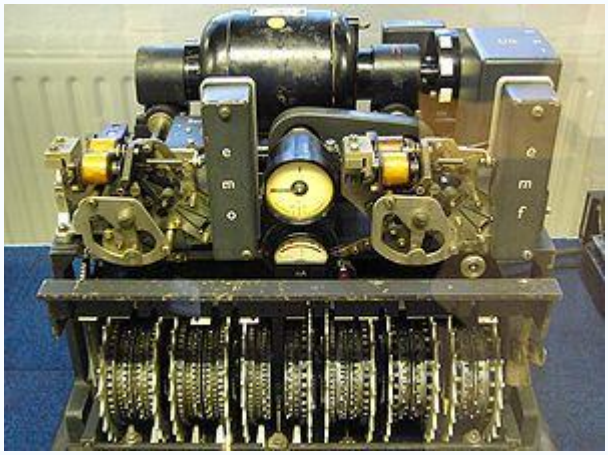
Криптография

Материал из Википедии — свободной энциклопедии



Немецкая криптомашина Lorenz, использовалась во время Второй мировой войны для шифрования самых секретных сообщений

Криптогра́фия (от греч. κρυπτός — скрытый и γράφω — пишу) — 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 и/или ключа в шифрованный текст (шифртекст). 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 асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Криптография не занимается: защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищенных системах передачи данных.

Криптография — одна из старейших наук, ее история насчитывает несколько тысяч лет.

Содержание

Терминология

- **Открытый (исходный) текст** — данные (не обязательно текстовые), передаваемые без использования криптографии.
- **Шифрованный (закрытый) текст** — данные, полученные после применения криптосистемы с указанным ключом.
- **Криптосистема** — семейство обратимых преобразований открытого текста в шифрованный.
- **Ключ** — параметр шифра, определяющий выбор конкретного преобразования данного текста. В современных шифрах *алгоритм шифрования* известен, и криптографическая стойкость шифра целиком определяется секретностью ключа (Принцип Керкгоффса).
- **Криптоанализ** — наука, изучающая математические методы нарушения конфиденциальности и целостности информации.
- **Криптоаналитик** — человек, создающий и применяющий методы криптоанализа.
- Криптография и криптоанализ составляют **криптологию**, как единую науку о создании и взломе шифров (*такое деление привнесено с запада, до этого в СССР и России не применялось специального деления*).
- **Криптографическая атака** — попытка криптоаналитика вызвать отклонения в атакуемой защищенной системе обмена информацией. Успешную криптографическую атаку называют **взлом** или **вскрытие**.
- **Шифрование** — процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.
- **Расшифровывание** — процесс нормального применения криптографического преобразования шифрованного текста в открытый.
- **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, вообще говоря, может заключаться и в анализе шифросистемы, а не только зашифрованного ею открытого сообщения).
- **Криптографическая стойкость** — способность криптографического алгоритма противостоять криптоанализу.
- **Имитозащита** — защита от навязывания ложной информации. Имитозащита достигается обычно за счет включения в пакет передаваемых данных имитовставки.
- **Имитовставка** — блок информации, применяемый для имитозащиты, зависящий от ключа и данных. В частном случае обеспечивается ЭЦП.
- **Асимметричный шифр** - шифр, являющийся асимметричной криптографической системой.

История криптографии и криптоанализа

Использовавшийся в Древней Греции шифр «скитала», чья современная реконструкция показана на фото, вероятно был первым устройством для шифрования.

До нашего времени криптография занималась исключительно конфиденциальностью сообщений (то есть зашифровкой) — преобразованием сообщений из понятной формы в непонятную и обратное восстановление на стороне получателя, делая его нечитаемым для перехватившего или подслушавшего без секретного знания (а именно ключа, необходимого для дешифровки сообщения). В последние десятилетия область применения криптографии расширилась и включает не только тайную передачу сообщений, но и методы проверки целостности сообщений, идентификации получателя/отправителя сообщения, цифровую подпись, интерактивную проверку, защищённые вычисления и другие.

Основные классические виды шифрования — это перестановочное шифрование, при котором буквы сообщения переставляются (например «помоги мне» превращается в «опомиг нме» при простейшей схеме перестановки) и замещающий шифр, когда буквы или группы букв по определённому правилу заменяются на другие буквы или группы букв (например «fly at once» становится «gmz bu podf» при замене каждой буквы следующей за ней в алфавите). Простейшие версии обоих шифров — не более чем небольшая защита от любопытных. Первым замещающим шифром был шифр Цезаря, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите. Назван этот шифр в честь Юлия Цезаря, который, как сообщается, использовал шифр со смещением 3 при связи со своими полководцами во время военных кампаний.

Шифрованием пытались достичь гарантированной секретной связи в первую очередь в таких областях, как шпионаж, военное дело и дипломатия. Так, существуют древние еврейские зашифрованные тексты. Криптография рекомендуется к применению в индийской Камасутре как средство для связи любовников.[1] Стеганография (то есть сокрытие самого факта передачи сообщения) также появилась в античные времена. Первый пример передачи скрытого сообщения из Геродота — татуировка, сделанная на обритой голове раба, скрытая под отросшими волосами.[2] Более современные примеры стеганографии состоят в использовании симпатических чернил, микроточек и цифровых водяных знаков для сокрытия информации.

Шифротексты, получающиеся после применения классических шифров (а также и некоторых современных), всегда выдают статистическую информацию об исходном тексте, которая может быть использована для их взлома. После разработки частотного анализа (возможно арабским энциклопедистом ал-Кинди) в IX веке, практически все такие шифры стали взламываемыми достаточно квалифицированным взломщиком. Однако классические шифры до сих пор пользуются популярностью, правда больше как головоломки. По существу, все шифры оставались уязвимы для криптоанализа с

использованием этой техники до изобретения полиалфавитных шифров наиболее вероятно Леоном Баттистой Альберти около 1467 года (есть некоторые указания на то, что они были известны арабам несколько ранее). Нововведение Альберти состояло в том, чтобы использовать различные шифры (то есть замещающие алфавиты) для разных частей сообщения (возможно, для каждого последовательного исходного текста в некотором наборе). Он также изобрёл, вероятно, первую автоматическую шифровальную машину — колесо, которое осуществляло частичную реализацию его изобретения. В полиалфавитном шифре Вигнера для шифрования используется *ключевое слово*, которое контролировало замену буквы в зависимости от того, какая использовалась буква ключевого слова. В середине 1800-х годов Бэббидж показал, что полиалфавитные шифры этого типа содержат частичную уязвимость к технике частотного анализа.[2]

Роторная шифровальная машина Энигма, разные модификации которой использовались германскими войсками с конца 1920-х годов до конца Второй мировой войны[3], осуществляла сложное электро-механическое полиалфавитное шифрование. Взлом шифра Энигмы Biuro Szyfrów и последующая широкомасштабная дешифровка сообщений Энигмы в Блетчли Парк (Bletchley Park) были важным вкладом в победу союзников во Второй мировой войне.[2]

Хотя частотный анализ является мощным средством, шифрование до сих пор остаётся эффективным на практике, так как многие потенциальные криптоаналитики не знакомы с этой техникой. Взлом сообщения без частотного анализа обычно требует знания используемого шифра, то есть является следствием шпионажа, взятки, кражи или измены для его определения. В XIX веке стало окончательно ясно, что секретность алгоритма шифрования не является гарантией от взлома, более того в дальнейшем было понято, что адекватная крипографическая схема (включая шифр) должна оставаться защищённой даже, если противник полностью узнал алгоритм шифрования. Секретность ключа должна быть достаточна для хорошего шифра, чтобы сохранить стойкость к попыткам взлома. Этот фундаментальный принцип впервые ясно сформулировал в 1883 Огюстом Керкгоффсом и обычно называется Принципом Керкгоффса; альтернативно и более прямо принцип был также сформулирован Клодом Шенноном как *Максима Шеннона* — «враг знает нашу систему».

Для облегчения шифрования были разработаны различные вспомогательные устройства. Одним из самых первых является скитала, придуманная в Древней Греции,

представляющая собой простую палочку. Придумано оно было предположительно в Спарте для осуществления перестановочного шифрования. В средние века были придуманы другие вспомогательные средства, такие как решётка для шифрования, использовавшаяся для различных видов стеганографии. С появлением полиалфавитных шифров вспомогательные устройства стали усложняться, как, например, диск с шифротекстом Альберти, квадратная доска (tabula recta) Тритемиуса и дисковый шифр Томаса Джефферсона (переоткрытый независимо Этьеном Базери около 1900). Различные механические шифраторы/дешифраторы были разработаны уже в XX веке. Принцип действия многих из них был запатентован (например, роторная машина).

Развитие компьютерной техники и электроники после Второй мировой сделало возможным использование более сложных шифров. Более того, компьютеры позволили шифровать любые данные, которые представимы в цифровом бинарном виде, в отличие от классических шифров, которые предназначались только для шифрования написанных текстов. Это привело к непригодности лингвистических методов криптоанализа для большинства случаев, так как многие компьютерные шифры характеризуются работой с последовательностями битов (возможно сгруппированных в блоки), в то время как классические и механические схемы обычно манипулировали традиционными знаками (буквами и цифрами). С другой стороны, компьютеры помогают криптоанализу, что может компенсировать усложнение шифров. Однако, несмотря на это, хорошие современные шифры идут впереди криптоанализа, обычно использование качественного шифра очень эффективно (то есть осуществляется быстро и с минимальными ресурсами), в то время как взлом требует усилий на много порядков больше как по времени, так и по ресурсам, делая криптоанализ настолько неэффективным и непрактичным, что можно считать его невозможным за разумное время или с разумными ресурсами.

Развитие академических криптографических исследований началось относительно недавно — начиная примерно с середины 1970-х годов с открытой публикации спецификации стандарта шифрования DES от NBS в статье Диффи — Хеллмана [4] и открытия алгоритма RSA. После этого криптография начинает широко использоваться в коммуникациях, компьютерных сетях и вообще компьютерной безопасности.

На данный момент секретность большинства современных методов криптографии базируется на вычислительной сложности таких проблем, как факторизация больших целых чисел или проблема дискретного логарифма. В большинстве случаев существуют доказательства, что методики шифрования являются надёжными, *если* соответствующая вычислительная проблема не может быть эффективно решена.[5] Единственное существенное исключение из этого правила — метод одноразового блокнота, который работает каждый раз с новыми значениями и имеет абсолютную криптографическую стойкость.

Как не раз показала мировая история криптографии, разработчики криптографических алгоритмов и систем должны очень серьёзно подходить к возможности разработки в будущем более мощных средств дешифровки. Например, продолжающееся развитие компьютерной техники постоянно увеличивает длину ключа шифрования, который может быть взломан методом грубой силы. Возможное использование квантовых вычислений также учитывается при проектировании некоторых криптографических систем: необходимо учитывать потенциальную опасность применения таких устройств[6].

До XX века криптография имела дело только с языковедческими образцами. С тех пор акцент сместился, и теперь в криптографии активно используются математика, включая теорию информации, теорию сложности вычислений, статистику, комбинаторику,

абстрактную алгебру и теорию чисел. Криптография также стала частью инженерного дела (см. Криптографическое инженерное дело и security engineering). Также активно развиваются исследования по применению в криптографии квантовой физики (см. квантовая криптография и квантовый компьютер).

Современная криптография

Для современной криптографии характерно использование открытых алгоритмов шифрования, предполагающих использование вычислительных средств. Известно более десятка проверенных алгоритмов шифрования, которые при использовании ключа достаточной длины и корректной реализации алгоритма криптографически стойки. Распространенные алгоритмы:

- симметричные DES, AES, ГОСТ 28147-89, Camellia, Twofish, Blowfish, IDEA, RC4 и др.;
- асимметричные RSA и Elgamal (*Эль-Гамаль*);
- хэш-функций MD4, MD5, SHA-1, ГОСТ Р 34.11-94.

Во многих странах приняты национальные стандарты шифрования. В 2001 году в США принят стандарт симметричного шифрования AES на основе алгоритма Rijndael с длиной ключа 128, 192 и 256 бит. Алгоритм AES пришёл на смену прежнему алгоритму DES, который теперь рекомендовано использовать только в режиме Triple DES. В Российской Федерации действует стандарт ГОСТ 28147-89, описывающий алгоритм блочного шифрования с длиной ключа 256 бит, а также алгоритм цифровой подписи ГОСТ Р 34.10-2001.

Криптография с симметричным ключом

Основная статья: ***Алгоритм с симметричным ключом***

Криптография с открытым ключом

Основная статья: ***Криптосистема с открытым ключом***

Криптоанализ

Основная статья: ***Криптоанализ***

Криптографические примитивы

Построение криптостойких систем может быть осуществлено путём многократного применения относительно простых криптографических преобразований (примитивов). В качестве таких примитивов Клод Шеннон предложил использовать подстановки (substitution) и перестановки (permutation). Схемы, реализующие эти преобразования, называются SP-сетями. Часто используемыми криптографическими примитивами являются также преобразования типа циклический сдвиг или гаммирование.

Криптографические протоколы

Основная статья: ***Криптографический протокол***

Примеры криптографических протоколов: доказательство с нулевым разглашением, забывчивая передача, протокол конфиденциального вычисления.

Управление ключами

Основная статья: ***Управление ключами***

Государство, законодательство, философия и криптография

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:

- распространению шифровальных (криптографических) средств
- техническому обслуживанию шифровальных (криптографических) средств
- предоставлению услуг в области шифрования информации
- 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 соискателя … следующего квалифицированного персонала: руководитель и (или) лицо, уполномоченное руководить работами по лицензируемой деятельности, имеющие высшее профессиональное образование и (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)»[7], 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» [8].

Относительно юридических лиц и предпринимателей, желающих разрабатывать либо реализовывать криптосистемы, существуют п. 5—11 ст. 17 Федерального Закона от 08.08.2001 N 128-ФЗ «О лицензировании отдельных видов деятельности»

> *5) деятельность по распространению шифровальных (криптографических) средств;*
> *6) деятельность по техническому обслуживанию шифровальных (криптографических) средств;*
> *7) предоставление услуг в области шифрования информации;*
> *8) разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;*
> *10) деятельность по разработке и (или) производству средств защиты конфиденциальной информации;*
> *11) деятельность по технической защите конфиденциальной информации;*

Экспортный контроль

Основная статья: ***Экспорт криптографии***

Управление цифровыми правами

Основная статья: ***Технические средства защиты авторских прав***

Философии

Основная статья: ***Криптоанархизм***

См. также

- Информационная безопасность
- Конфиденциальность
- Получение скрытой информации

Примечания

1. ↑ *Kama Sutra*, Sir Richard F. Burton, translator, Part I, Chapter III, 44th and 45th arts.

2. ↑ [1] [2] [3] David Kahn, The Codebreakers, 1967, ISBN 0-684-83130-9.
3. ↑ *Joy Hakim A History of Us: War, Peace and all that Jazz. — New York: Oxford University Press. — ISBN 0-19-509514-6*
4. ↑ Whitfield Diffie and Martin Hellman, «New Directions in Cryptography», IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp: 644—654. (pdf)
5. ↑ Oded Goldreich, *Foundations of Cryptography*, *Volume 1: Basic Tools*, Cambridge University Press, 2001, ISBN 0-521-79172-3
6. ↑ *A. Menezes, P. van Oorschot, S. Vanstone.* Handbook of Applied Cryptography. — CRC-Press, 1996. — 816 p. — (Discrete Mathematics and Its Applications). — ISBN 0-8493-8523-7
7. ↑ Приказ ФСБ РФ от 09.02.2009 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение пкз-2005)»
8. ↑ Указ президента РФ от 03.04.1995 № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»

Ссылки

- Юрий Лифшиц. Курс лекций Современные задачи криптографии
- Информационная безопасность и шифрование
- Криптографический ликбез
- Криптографический справочник
- Библиотека научных статей по криптографической защите информации
- Криптолог-блог
- Сборник статей по криптографии
- Подборка статей об истории криптографии
- А.В. Синельников «Шифры и революционеры России (Криптография конца XIX - начала XX вв.)

Литература

- Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. М.: Научный мир, 2004. ISBN 5-89176-233-1.
- *Баричев С.Г., Гончаров В.В., Серов Р.Е.* Основы современной криптографии. — М.: Горячая линия — Телеком, 2002. — 175 с. — (Специальность. Для высших учебных заведений). — 3000 экз. — ISBN 5-93517-075-2
- Варфоломеев А. А., Жуков А. Е., Пудовкина М. А. Поточные криптосистемы. Основные свойства и методы анализа стойкости. М.: ПАИМС, 2000.
- Ященко В. В. Введение в криптографию. СПб.: Питер, 2001. ISBN 5-318-00443-1.
- Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.:Триумф, 2002. ISBN 5-89392-055-4, ISBN 0-471-11709-9.
- Вильям Столлингс. Криптография и защита сетей: принципы и практика. М.: Вильямс, 2001. ISBN 5-8459-0185-5.
- *Венбо Мао* Современная криптография: теория и практика = Modern Cryptography: Theory and Practice. — М.: «Вильямс», 2005. — С. 768. — ISBN 0-13-066943-1
- Герасименко В. А. Защита информации в автоматизированных системах обработки данных., кн. 1, 2. М.: Энергоатомиздат, 1994.
- ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: ГК СССР по стандартам, 1989.
- ГОСТ Р 34.10-94.Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асиметричного криптографического алгоритма. М., 1995.

- ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования. М., 1995.
- ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М., 2001.
- *Нильс Фергюсон, Брюс Шнайер* Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М.: «Диалектика», 2004. — С. 432. — ISBN 0-471-22357-3
- Конхейм А. Г. Основы криптографии. М.: Радио и связь, 1987.
- Мафтик С. Механизмы защиты в сетях ЭВМ. М.: Мир, 1993.
- Мельников В. В. Защита информации в компьютерных системах. М.: Финансы и статистика, 1997.
- Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография. СПб.: «Лань», 2000.
- Молдовян Н. А. Скоростные блочные шифры. СПб.: Издательство СПбГУ, 1998.
- Нечаев В. И. Элементы криптографии (Основы теории защиты информации). М.: Высшая школа, 1999.
- Основы криптозащиты АСУ. Под ред. Б. П. Козлова. М.: МО, 1996.
- Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.
- Ухлинов А. М. Управление безопасностью информации в автоматизированных системах. М.: МИФИ, 1996.
- Жельников В. Криптография от папируса до компьютера. М.: АВР,1996.

Источник — «http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F»

Категории: Хеш-функции | Криптография | Информационная безопасность