УДК: 004.056

Основные положения установочной лекции для введения в криптографию и криптографические методы защиты информации

A.Yu. Shcherbakov

The Main Thesis to the Introductory Lecture in Cryptography and Cryptographic Methods of Information Security

Abstract. *This article is intended to help lecturers of cryptography and information security in the formation of an introductory lecture on cryptography for students and listeners, prepared both within the framework of university programs and additional professional education.*

The presented material is necessary for the formation of a correct conceptual and methodological view of the subject.

Keywords: *cipher, cryptanalysis, cryptographic scheme, conformance check, key, encryption algorithm, encryption system, quantum cryptography.*

А.Ю. Щербаков

Доктор технических наук, профессор кафедры комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ)имени И.М. Губкина, ведущий научный сотрудник Государственного университета управления.

E-mail: x509@ras.ru

Аннотация. *Данная статья предназначена для содействия преподавателям, читающим курсы основ криптографии и компьютерной безопасности, в подготовке вводных лекций по криптографии для обучаемых и слушателей, подготавливаемых как в рамках вузовских программ, так и дополнительного профессионального образования.*

Излагаемый материал необходим для формирования правильного понятийно-методологического взгляда на предмет.

Ключевые слова: *шифр, криптоанализ, криптографическая схема, проверка соответствия, ключ, криптографический алгоритм, система шифрования, квантовая криптография.*

ВВЕДЕНИЕ

Исторически сложилась практика, когда изучение криптографии начинается с экскурсов в историю предмета и рассмотрения сравнительно простых конструкций, связанных с подставочными (простая символьная замена) или перестановочными шифрами. Кажущаяся простота предмета внушает обучаемым ложные иллюзии, что современная криптография столь же проста и очевидна.

Однако мы полагаем, что преподаватель должен донести не только сложности современной криптографии, но также ее комплексный характер и общую зависимость предмета от установок и позиций государственных регуляторов [1].

СОДЕРЖАНИЕ ТЕРМИНОЛОГИИ И МЕТОДОЛОГИИ СОВРЕМЕННОЙ КРИПТОГРАФИИ

С точки зрения обычного восприятия криптография – это наука, изучающая процессы шифрования информации.

Основная цель шифрования – сделать содержание послания от одного воспринимающего субъекта (например, человека) к другому таким, чтобы не имеющие отношение к этой передаче субъекты не смогли его воспринять.

Эта цель позволяет более четко сформулировать или глубже прояснить, возможно, уже знакомое обучаемым понятие «нарушителя» и связать задачи криптографической защиты информации с целями и возможностями нарушителя.

Воспринимаемость – это существенное свойство для информации, поскольку, например, нарушитель древности или средних веков, не умеющий читать, не мог воспринять информацию зашифрованного послания, а позже нарушитель, не имеющий радиоприемника, не смог бы воспринять информацию в радиоканале. Таким образом, криптография с точки зрения атак – это область действия высококвалифицированных и хорошо оснащенных нарушителей.

Криптография при этом позиционируется в

классе математических наук, связанных с процессами преобразования форм информации (для передачи информация должна принять некую форму и в рамках этой формы должна быть преобразована).

С другой стороны, очевидно, что с развитием технологической цивилизации субъектами передачи и приема начинают становиться технические системы, а информация принимает существенно более разнообразные формы представления, чем текст на бумаге или свитке папируса.

Кроме того, процесс передачи становится таким, что потенциальным нарушителям гораздо проще становится не только перехватывать информацию (например, по радиоканалу), но изменять ее или целиком формировать новую, не принадлежащую отправителю.

Процессы автоматизации передачи и обработки информации обуславливают необходимость реализации математических алгоритмов преобразования в рамках технических систем, делая криптографию технической наукой.

Современная криптография в основном опирается на вычислительные алгоритмы и системы как при реализации шифров, так и при их анализе, следовательно, использует информационные и компьютерные системы.

Таким образом, криптография оказывается «встроена» в информационную технологию, когда важными являются вопросы практической реализации криптоалгоритмов в конкретной компьютерной или технической системе. Поэтому часто и обоснованно полагают, что криптография – отдельная часть компьютерной безопасности.

Самой важной задачей криптографии логично представляется создание «хороших» шифров с точки зрения их качества, чтобы их невозможно было «прочитать».

Шифр, как система преобразования информации, должен быть «устойчивым «или «стойким» в некотором математическом смысле. Кроме того, логично возникает некоторый «секретный элемент», который должен быть как у отправителя, так и у получателя.

Кроме синтеза качественных шифрующих преобразований (шифров) современная криптография изучает:

• оптимизацию криптоалгоритмов (чтобы шифрование в технических системах «работало» быстрее);

• свойства датчиков случайных чисел (чтобы получать «секретные элементы» — ключи шифра хорошего качества);

• надежность программной или аппаратной реализации шифров (чтобы ошибки разработчиков или программистов, а также сбои оборудования не приводили к снижению качества).

Предметом изучения современной криптографии также являются:

• возможности улучшения криптоанализа («взлома» шифра) с использованием побочных электромагнитных излучений или других сигналов от работы компьютерной или шифрующей техники;

• криптографические протоколы, в том числе различные алгоритмы распределения и хранения ключей, включая квантовые;

• алгоритмы авторизации и защиты целостности (электронная подпись);

• прикладное применение криптографии (банковские системы, блокчейн, голосование, интернет вещей).

Изучая основы современной криптографии, следует напомнить обучаемым, что безопасный обмен информацией является не только предметом научных изысканий, но и объектом художественного отражения в искусстве и литературе, и сопровождает человека в течение всей его осмысленной (т. е. использующей письменность) истории.

С древних времен зашифрование и стеганографирование (изготовление невидимых сообщений) представляло актуальную и интересную задачу, часто жизненно важную для судеб отдельных исторических личностей и даже государств. Соревнование и драматическая судьба шифровальщиков и дешифровальщиков не раз становились сюжетом различных произведений XX века [2], таких как «Алан Тюринг: «Энигма», «В круге первом» и другие.

Заслуживает внимания художественный фильм «Игра в имитацию» (англ. The Imitation Game) — фильм-драма, снятый по сценарию Грэма Мура, основанному на биографической книге Эндрю Ходжеса о криптографе времени Второй мировой войны Алане Тьюринге, кото-

рый «взломал» процесс шифрования немецкой шифровальной машины «Энигма». Дисковая электромеханическая шифровальная машина «Энигма» является и по сей день весьма примечательным устройством, дешифрование которого в то время явилось беспрецедентным успехом.

«В круге первом» — роман Александра Солженицына, написанный в 1955—1958 годах по его воспоминаниям о работе во время тюремного заключения на «шарашке» (спецтюрьме МВД — МГБ) в Марфино, где после Второй мировой войны работали заключённые инженеры. Этот роман является первым произведением, опубликованным в серии «Литературные памятники» при жизни автора, посвященным работам над первым в мире шифратором голосовых сообщений.

«Утоли моя печали» - заключительная книга автобиографической трилогии известного писателя, литературного критика, германиста Льва Копелева, в которой также описана «шарашка», где вместе жили и работали заключенные А. Солженицын, Л. Копелев, Д. Панин - прототипы героев романа А. Солженицына «В круге первом».

Исторические и литературные экскурсы в сложность проблем криптографии, её значимость для исторического развития народов и государств могут вызвать неформальный интерес обучаемых к предмету.

Необходимо заметить, что криптография, как никакая другая наука, отражала тенденцию ускорения обработки информации, подсознательно апеллируя к различным вычислительно трудоемким алгоритмам, являясь и фактором ускорения развития информационных технологий (пример — упомянутая выше операция «Ультра» по дешифрованию шифровальной машины «Энигма», которая, по мнению известных современников и историков существенно сократила время Второй мировой войны).

Современные шифры и их анализ — в первую очередь информатика, большие данные, новая математика и инженерные прорывы.

Понятие шифра традиционно имеет как практические, так и более «академичные» определения.

Шифр – совокупность алгоритмов или отображений открытой (общедоступной) информации, представленной в формализованном виде, в недоступный для восприятия шифрованный текст (также представленный в формализованном виде). Шифр обязательно зависит от внешнего параметра (ключа), без знания которого невозможно шифрованную информацию преобразовать в открытую. Ключ должен быть задан или сконструирован таким образом, чтобы его нельзя было определить ни по шифрованной, ни по открытой информации.

Шифрование информации – взаимноодно-значное математическое (криптографическое) преобразование, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации в некотором цифровом представлении блок шифрованной информации, также представленной в цифровом виде. Термин шифрование объединяет в себе два процесса: зашифрование и расшифрование информации.

Шифратор – аппарат или программа, реализующая шифр. В современной литературе вводится понятие “средства криптографической защиты информации” (СКЗИ), которое включает в себя шифратор, но в целом является более широким.

Альтернативным «академическим» определением шифра, приведенным в [3], является:

Шифр [cipher] — семейство обратимых отображений множества последовательностей блоков текстов (сообщений) открытых в множество последовательностей блоков текстов (сообщении) шифрованных и обратно, задаваемых функцией шифрования. Каждое из отображений определяется некоторым параметром, называемым ключом, и описывается некоторым алгоритмом шифрования, реализующим один из режимов шифрования. Математическая модель шифрования включает алгоритм зашифрования, алгоритм расшифрования, определение режима шифрования, а также модель множества текстов открытых сообщений.

В зависимости от способа представления текстов открытых (сообщений) различают блочные, поточные и другие шифры.

Основными требованиями, определяющими качество шифрования, являются: стойкость криптографическая, имитостойкость, помехо-

устойчивость шифра.

Ключ – некоторый неизвестный параметр шифра, позволяющий выбрать для шифрования и расшифрования конкретное преобразование из всего множества преобразований, составляющих шифр. Простая ассоциация – ключ от замка – во многом проясняет смысл термина. Есть много одинаковых качественно ключей, но лишь некоторые (или чаще один) откроют замок.

Шифрование – процесс получения шифрованного текста, основанный на знании ключа.

Дешифрование – восстановление открытого текста или ключа по шифрованному тексту.

Злоумышленник (нарушитель) – субъект (или физическое лицо), не знающий ключа или открытого текста и стремящийся получить его. Полагается, что нарушитель контролирует канал обмена информацией между абонентами, использующими шифрование.

Разработку и применение шифров называют криптографией, в то время как науку о раскрытии шифров — криптоанализом.

Поскольку проверка шифров на стойкость является обязательным элементом их разработки, криптоанализ также является частью процесса разработки.

Криптология — это наука, предметом которой являются математические основания как криптографии, так и криптоанализа одновременно.

Криптоаналитической атакой называют использование специальных методов для раскрытия ключа шифра и/или получения открытого текста. Предполагается, что атакующей стороне известен алгоритм шифрования, и ей требуется только найти конкретный ключ.

Другая важная концепция связана со словом «взлом». Когда говорят, что некоторый алгоритм был «взломан», это не обязательно означает, что найден практический способ раскрытия шифрованных сообщений. Здесь может иметься в виду, что найден способ существенно уменьшить ту вычислительную работу, которая требуется для раскрытия шифрованного сообщения методом «грубой силы», то есть простым перебором всех возможных ключей.

При осуществлении такого взлома практически шифр все же может оставаться стойким, поскольку требуемые вычислительные возможности будут все еще оставаться за гранью реального. При этом существование метода взлома не означает еще реальной уязвимости алгоритма, обычно такой алгоритм более не используют или модифицируют.

Понятие «нарушитель» в криптографии тесно связано с понятием “твердого незнания” им ключа. В соответствии с методологией, принятой в современной криптографии, надежность шифра определяется степенью безопасности используемых в нем ключей, поскольку все долговременные элементы криптографической системы (множество правил шифрования, его механизм) рано или поздно станут известными злоумышленнику. Этот принцип был сформулирован еще в конце XIX в. и получил название “правила Керкгоффса” (Kerckhoffs’s desiderata).

В [3] правило Керкгоффса — общепринятое в криптографии предположение проведения криптоанализа, впервые сформулированное голландским криптографом Н. Керкгоффсом («компрометация системы не должна причинять неудобств корреспондентам»). В современном понимании это правило означает, что описание криптосистемы (криптопротокола) может быть полностью известно противнику и/или нарушителю, а стойкость криптографическая основана только на том, что не известен ключ (секретный) [3].

В современной криптографии считается, что злоумышленник имеет возможность также произвольным образом изменять сообщения.

Поэтому вводится еще один термин: подлинность – принадлежность сообщения конкретному автору и неизменность содержания сообщения. Подлинность естественным образом делится на «неизменность» и «авторство».

Для описания шифра может быть использовано текстуальное или символьно-математическое описание криптографического преобразования. Кроме того, разумно представлять схему работы шифра (криптосхему) в виде конструкций одного из «общеупотребительных» языков программирования. Это весьма наглядно для программистов и специалистов в области реализации криптографических алгоритмов.

Такого рода представление ставит вопрос о проверке соответствия описания криптографи-

ческого преобразования и его реализации на языке программирования, либо в виде аппаратного изделия.

Криптографическая схема (криптосхема) – описание алгоритма криптографического преобразования в виде наглядно-графической модели, чаще всего в виде схемы или блок-схемы, в которой блоки представляют собой некоторые законченные функции, входящие в состав криптографического преобразования.

Эти функции, как правило, имеют «элементарный» характер – например, поэлементная (побайтовая) сумма двух массивов по модулю 2. В частности, такая операция используется в алгоритме шифрования «Кузнечик [4].

Несколько шире криптографической схемы формулируется система шифрования.

Система шифрования [cryptosystem, син. шифрсистема] — система криптографическая, предназначенная для защиты информации от лиц, не имеющих права доступа к ней. Защита обеспечивается путем зашифрования информации. Математическая модель системы шифрования включает способ кодирования исходной и выходной информации, шифр и систему ключевую. Основными требованиями, определяющими качество системы шифрования, являются: стойкость криптографическая, имитостойкость, помехоустойчивость шифра и др. [3].

Соответствие реализации криптографического преобразования его описанию – категория тождества, выраженная в соотнесении аналогичных или тождественных входных и выходных массивов информации, а также внутренних состояний криптографического преобразования, описанных в криптографической схеме и реализованных функционально в виде программы или аппаратного изделия.

Проверка соответствия реализации криптографического преобразования его описанию – комплекс процедур, позволяющий детерминированно или вероятностно (с высокой вероятностью) убедиться в их соответствии, и выполняемый, как правило, при помощи тестов или тестовых процедур.

С точки зрения системного анализа криптографическое преобразование (зашифрование) рассматривается в виде «белого ящика» (т. е. преобразование имеет известную структуру), на входе которого – открытый текст и ключ зашифрования, на выходе – зашифрованный текст. Такое представление соответствует принципу Керкгоффса.

При этом «белый ящик» погружен в некоторую «окружающую среду», которая представляет собой среду реализации криптографического преобразования в виде программного или аппаратного окружения.

Достаточно часто используют термин «среда функционирования криптографического средства (криптосредства)» (СФ или СФК), который также описывает окружающее «белый ящик» пространство в виде компьютерной системы, реализующее криптопреобразование и связанные процессы обработки, передачи и хранения информации. В этом случае криптографическое преобразование осуществляется в подсистеме некоторой большей с теоретико-множественной точки зрения системы.

Одной из тенденций развития современной криптографии является квантовая криптография – когда ключи в системе распределяются с использованием физических процедур обмена отдельными пакетами фотонов, которые нельзя физически перехватить, не изменив их параметры.

Вторая тенденция – исключение человека и различных программных алгоритмов из процедур обеспечения безопасности, переход к криптофизической безопасности, когда человеческий фактор по возможности исключен, а система построена на простой, надежной и доверенной платформе. Она связана также с «технической сингулярностью», когда ключи криптографического алгоритма «неизвлекаемо» хранятся в рамках некоторого замкнутого и невскрываемого изделия [5].

ЗАКЛЮЧЕНИЕ

Четкое изложение понятийных основ криптографии позволит преподавателю донести до обучаемых комплексный характер современной криптографии, ее системность, а также зависимость предмета от установок, позиций и требований государственных регуляторов в рассматриваемой области.

СПИСОК ЛИТЕРАТУРЫ

1. А.Щербаков Перспективы современной криптографии Проектирование будущего. Проблемы цифровой реальности.- 2020. № 1 (3)- С. 227-233.
2. Hodges A. Alan Turing: The Enigma. Princeton University Press; Revised edition. 2014. Pp. 768.
3. Словарь криптографических терминов под редакцией Б. А. Погорелова и В. Н. Сачкова.- Москва: М.: МЦНМО, 2006.- 91 с.
4. ГОСТ Р 34.12–2015 «Информационная технология. Криптографическая защита информации. Блочные шифры». Утвержден приказом Федерального агентства по техническому регулированию и метрологии от 19 июня 2015 г. N 749-ст: дата введения 1 января 2016 г. – Москва: Стандартинформ, 2018.
5. Гриняев С.Н., Правиков Д.И., Разгуляев К.А., Рязанова А.А., Хан Д.В., Щербаков А.Ю. Основные методологические подходы к формированию и обоснованию архитектуры и протокола квантового распределенного реестра //Научно-техническая информация, сер. 2 Информационные процессы и системы.- 2020. №1. С. 11-18.