УДК 519.1:003.26

КАК ДИСКРЕТНАЯ МАТЕМАТИКА СВЯЗАНА С КРИПТОГРАФИЕЙ?

Ложкин П.А.

ФГБОУ ВО «Ставропольский государственный аграрный университет», Ставрополь, e-mail: pasha26rusk@gmail.com

Криптография включает в себя создание письменных или сгенерированных кодов, которые позволяют хранить информацию в секрете. Криптография преобразует данные в формат, который не читается для неавторизованного пользователя, что позволяет передавать его без возможности его декодирования обратно в читаемый формат, тем самым компрометируя данные. Криптография опирается многие понятия математики и дискретной математики такие, как абстрактная алгебра, теория чисел, множества, линейная алгебра, комбинаторика, теория вероятностей. Примером связи криптографии и дискретной математики может служить известный алгоритм RSA, который позволяет использовать систему шифрования с открытым ключом, используя понятие наибольшего общего делителя чисел, теорему Ферма, теорию конгруэнции и расширенный алгоритм Евклида. Криптография способствует развитию математики, а математика предоставляет базу для решения задач криптографии.

Ключевые слова: безопасность, дискретная математика, криптография

HOW IS DISCRETE MATHEMATICS CONNECTED WITH CRYPTOGRAPHY?

Lozhkin P.A.

Stavropol State Agrarian University, Stavropol, e-mail: pasha26rusk@gmail.com

Cryptography includes the creation of written or generated codes that allow you to store information in secret. Cryptography converts data into a format that is not readable for an unauthorized user, which allows it to be transmitted without the possibility of decoding it back into a readable format, thereby compromising data. Cryptography is based on many concepts of mathematics and discrete mathematics, such as abstract algebra, number theory, sets, linear algebra, combinatorics, probability theory. An example of the connection between cryptography and discrete mathematics is the well-known RSA algorithm that allows the use of a public key encryption system using the concept of the greatest common number divisor, Fermat's theorem, congruence theory, and the extended Euclidean algorithm. Cryptography promotes the development of mathematics, and mathematics provides a basis for solving cryptography problems.

Keywords: security, discrete mathematics, cryptography

Криптография – один из наиболее распространённых способов защиты информации. Суть этого способа заключается в преобразовании текста программы / данных в шифрованный текст [1, 3].

Шифрование/кодирование данных является одним из самых древних способов защиты информации и применялось ещё задолго до появления первых ЭВМ и электронных носителей информации. Древние люди шифровали свою информацию перестановкой слов /фраз/ чисел в тексте, тем самым получая возможность передавать кому-либо конфиденциальную информацию с малой вероятностью её расшифровки в дальнейшем. Однако такие методы шифрования были не слишком надёжны, и подбор ключа для расшифровки требовал не слишком много времени. С тех пор методы шифрования значительно шагнули вперед, и существует огромное количество программ, генерирующих сложные и длинные ключи и шифрующих данные всё надёжнее. Подобные ключи человеку запомнить не под силу и потому для расшифровки кодированных файлов используются заранее установленные пароли, которые прописываются в зашифрованный файл программой его зашифровывающей. Для декодирования подобного файла требуется лишь программа-дешифратор (обычно таковой является та же самая программа, что и шифровала файл(-ы) и знание пароля) [2].

Минимально безопасным паролем, на данный момент, считается пароль от 12 знаков – подбор такого пароля методом брутфорса (автоматического перебора пароля по определённому словарю) является продолжительным и, на одном персональном компьютере, может занять годы, если не века. Тем не менее, на производительном оборудовании подбор подобных паролей уже отнимает гораздо меньше времени, особенно если ведётся сразу с большого числа компьютеров. Зачастую злоумышленники взламывают компьютеры пользователей, устанавливают вредоносное программное обеспечение и создают сеть ботнет – множество заражённых персональных компьютеров, образующих единую сеть, чаще всего предназначенную для DDoS-атак или же брутфорса, то есть перебора ключей

для расшифровки закодированного файла. Такие сети могут вовлекать в себя миллионы компьютеров, тем самым подвергая огромной угрозе безопасность криптованных данных.

Для большей безопасности криптованных данных нередко применяются способы их маскировки под текстовые документы, аудио и видео файлы путём «склейки» зашифрованного файла/контейнера с обычным файлом/программой, содержащим любую информацию. Запустив такой файл, злоумышленник увидит лишь информацию подставного файла и, с высокой вероятностью, даже не станет пытаться его расшифровывать. То есть, чтобы никто не нашёл чёрную кошку в тёмной комнате, желательно, чтобы никто о ней и не знал – тогда не будет желающих искать [8].

Таким образом, можно сказать, что криптография являлась на протяжении всей истории человечества и продолжает являться поныне наиболее гарантированным способом защиты и сокрытия важной информации, особенно той, что находится в открытом доступе или потенциально может быть украдена. В совокупности с некоторыми хитростями такой метод становится ещё более надёжным.

Как связана криптография и математика?

Шифрование данных использует множество инструментов из абстрактной алгебры, теории чисел, линейной алгебры, включающих такие разделы, как конгруэнции, квадратичную теорию вычетов, теорию поля, матрицы, некоммутативные группы, комбинаторику, теорию вероятностей, различные математические алгоритмы, хэш-функции и квантовые алгоритмы. Все эти математические инструменты являются частью дискретной математики [4, 6, 7, 10].

Криптография о.пирается на такие понятия математики и дискретной математики, как множество, отношения и операции над множествами, мощность множества, эквивалентность множеств, функции, целые и действительные числа, простые числа, НОД, НОК числа и алгоритмы их нахождения, многочлены и разложение их на множители, действия над матрицами, алгоритмы применения матриц. Используются системы аксиом для основных алгебраических структур: группоид, моноид, полугруппы, группы, частичные порядки, кольца, поля [5, 9].

В криптологии до сих пор существует проблема разложения больших чисел (целых) на множители.

Примером связи криптографии и дискретной математики может служить известный алгоритм RSA, который позволяет использовать систему шифрования с открытым ключом, в которой каждый знает, как шифровать, но может расшифровать только тот, у кого есть специальный закрытый ключ. Вместе они называются открытым ключом. Одним из этих чисел является произведение pq двух простых чисел, а другое – число мы будем называть «E», которое по техническим причинам должно быть относительно простым с $(p–1)$ $(q–1)$. То есть наибольший общий делитель (НОД) E и $(p–1)$ $(q–1)$ должен быть равен 1. Например, мы можем выбрать $p = 5$, $q = 11$ и $E = 21$.

Заметим, что (5–1) (11–1) = 40 и что НОД (21, 40) = 1. Чтобы зашифровать сообщение, сначала нужно конвертировать его в последовательность целых чисел. Есть много способов сделать это – некоторые лучше, некоторые хуже. Затем, один за другим, необходимо зашифровать целые числа. Чтобы зашифровать целое число x, вычисляется $x \wedge E \ mod \ pq$, где *mod* – (вычисление остатка от целочисленного деления).

Числа pq и E являются общедоступными, так что каждый может зашифровать любое целое число. Например, для шифрования числа 6 мы вычисляем $6 \wedge 21 \ mod \ 55 = 46$.

Не очевидно, как это сделать в голове, но дискретная математика обеспечивает быстрые (эффективные) алгоритмы модульного возведения в степень. Плюсом этой схемы является то, что очевидный способ расшифровки 46 заключается в «грубой силе». Эта идея «грубой силы» слишком медленная, потому что, когда используются очень большие p и q, результирующее число всевозможных x слишком велико для эффективного управления.

Однако, используя средства еще одной части дискретной математики, а именно теорему Ферма, теорию конгруэнции и расширенный алгоритм Евклида, мы можем эффективно вычислить показатель магического декодирования d, который будет занимать 46, и вернуть его обратно к 6.

Задача применения разделов дискретной математики состоит в том, чтобы найти d такое, что $Ed = 1 \ mod \ (p–1) \ (q–1)$. (Обнаружение этого магического дешифрующего экспонента). Средства дискретной математики позволяют нам задействовать такой эффективный алгоритм, что для этого, нам необходимо знать только $(p–1) \ (q–1)$.

В нашем случае показатель магического декодирования случайно совпадает с 9 (обычно это не одинаковое число), поэтому для дешифровки 46 нам нужно вычислить

$$46 \text{ ^ } 9 \; mod \; 55 = 6.$$

Таким образом, единственное, что препятствует расшифровке публично кодированного сообщения RSA, заключается в том, что они не знают (p–1) (q–1). И единственный способ узнать это число – получить его от числа pq, что потребует факторинга pq, и никто не знает, как это сделать эффективно. Поэтому единственными людьми, которые могут расшифровать публично закодированные сообщения RSA, являются люди, которые создали pq, в первую очередь, потому что только они знают p и q. Существует много примеров, но этот единственный пример, который объясняет, как дискретная математика неразрывно связана с криптографией.

Криптография порождает новые трудные математические задачи, при этом математика является каркасом, основой криптографии. По мере развития общества, его научных достижений разрабатываются новые математические методы, приводящие к разрешению задач, ранее считавшихся неразрешимыми.

Список литературы

1. Авдошин С.М., Набебин А.А. Дискретная математика. Модулярная алгебра, криптография, кодирование. – М.: ДМК Пресс, 2017.

2. Вихляева В.В., Попова С.В. Вероятность как инструмент поиска оптимального решения в условиях неопределённости // Современные наукоемкие технологии. – 2014. – № 5–2. – С. 146 – 148.

3. Гулай Т.А., Долгополовой А.Ф., Мелешко С.В. Математические методы исследования экономических процессов // Международный журнал экспериментального образования. – 2016. – № 12–1. – С. 116–117.

4. Линейная алгебра (учебное пособие) / Крон Р.В., Попова С.В., Долгих Е.В., Смирнова Н.Б. // Международный журнал экспериментального образования. – 2014. – № 11–1. – С. 115.

5. Линейная алгебра: учебное пособие для студентов вузов сельскохозяйственных, инженерно-технических и экономических направлений/ Р.В. Крон, С.В. Попова, Н.Б. Смирнова, Е.В. Долгихю – М., 2015.

6. Мелешко С.В., Попова С.В., Цыплакова О.Н. Элементы комбинаторики: Учебно-методическое указание. – Ставрополь, 2012.

7. Попова С.В. Формирование алгоритмической культуры у студентов на занятиях по математике // Экономика регионов России: анализ современного состояния и перспективы развития: Сборник научных трудов по материалам ежегодной 68-й научно-практической конференции / Ответственный редактор Н.В. Кулиш, 2004. – С. 423–426.

8. Попова С.В., Колодяжная Т.А. Применение алгоритмов при обучении математике в вузе // Моделирование производственных процессов и развитие информационных систем: Даугавпилсский университет, Латвия, Европейский Союз Белорусский государственный университет, Беларусь Днепропетровский университет экономики и права, Украина Московский государственный университет им. М.В. Ломоносова, Россия Санкт-Петербургский государственный политехнический университет Северо-Кавказский государственный технический университет Ставропольский государственный университет Ставропольский государственный аграрный университет. Ставрополь, 2011. – С. 278–281.

9. Попова С.В., Смирнова Н.Б. Элементы алгоритмизации в процессе обучения математике в высшей школе // Современные проблемы развития экономики и социальной сферы: сборник материалов Международной научно-практической конференции, посвященной 75-летию Ставропольского государственного аграрного университета / Ответственный редактор: Н.В. Кулиш, 2005. – С. 526–531.

10. Смирнова Н.Б., Попова С.В. Основные принципы проектирования компьютерной математической модели // Сборник научных трудов по материалам Ежегодной 69-й научно-практической конференции, посвященной 75–летию СтГАУ / Ответственный редактор: Н.В. Кулиш, 2005. – С. 185–189.