УДК 51

МАТЕМАТИКА В КРИПТОГРАФИИ

Шелковников Д.В., студент гр. ПИб-192, II курс
Ковшов А.В., студент гр. ПИб-192, II курс
Гутова Е.В., ст. преподаватель кафедры математики
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово

В современном мире информационные технологии развиваются очень быстро и довольно сложно представить сферу жизнедеятельности человека, в которой не было бы косвенное или прямое соприкосновение с новыми технологиями. Информационные технологии заветно сильно уменьшают расход времени за счет вычисления математических операций буквально за секунды, но у всех новых технологий есть уязвимость в безопасности и криптография позволяет данную уязвимость защитить с помощью шифров. Например, с помощью мессенджеров мы можем совершать отправление сообщения из одной точки света в другую, но стоит понимать, что если бы наши сообщения не шифровались от других пользователей, то к данному сообщению имели доступ все пользователи, а не конкретный получатель, к которому мы направили сообщение. Поэтому средствами криптографии часто используются государства, организации, частные лица, из-за того, что большой обмен информации происходит в цифровом виде через открытые каналы связи и по отношению данной информации возможна применение какого-либо рода угрозы – подмены, фальсификации, утечки и т.п. И так с помощью алгебраических структур, таких как группы, кольца и поля невозможно изучения криптографии.

Вернемся к примеру, с сообщением и разберем более подробнее. Сообщение должно быть обязательно зашифровано и передано конкретному пользователю. В первую очередь сообщение проходит через такой процесс, когда записывается длина двоичной последовательности, включающего в себя 0 и 1, после построения данной длины сообщение называется оцифрованным. Также зная ограничение знаков двоичной последовательности, то можно заранее знать способы шифрования и расшифровки. Как создается данная длина N можно легко понять на примере с идеальной монетой. Монета подбрасывается N раз, при этом, при приземлении, на монете указывается «орел» или «решка», в двоичном коде «орел» будет являться единицей, а «решка» нулем. После шифровки сообщения данным образом сообщение передается получателю, при этом чтобы доступ был только у отправителя и получателя. Доступ к данному сообщению они получают с помощью «ключа», который создается при отправлении. Так, в данном примере используется ключ «сложение по

модулю 2» (то есть: 0+0=0; 0+1=1; 1+0=1; 1+1=0), по которому зашифрован каждый символ сообщения. И так полученная последовательность будет зашифрованным сообщением.

Подобное шифрование называется совершенным, из-за невозможности декодировки без ключа, ведь прибавление различных двоичных длин N не дает изначальное сообщение. Шифр утратит совершенность в тот момент, когда будет неоднократное использование.

В последнее время подобные шифры считаются не актуальные, потому что доступ к их декодировки имеют все и для этого создание новых шифров выступают различные разделы математики, в частности, алгебры, комбинаторики, теории чисел, теории алгоритмов, теории вероятности и математической статистики). Так появилось понятие «стойкий шифр». Данное понятие заключается в том, что при исследовании данного шифра злоумышленники не могут получить особенности, которые могут вскрыть ключ шифра.

Для защиты любых данных в глобальной паутине используются разные способы шифрования, но существуют два основных вида, на которых опирается основа шифрования:

1) Симметричный. Одинаковый ключ используется как для шифрования, так и для расшифрования сообщения;
2) Ассиметричный. Разные ключи используются для шифрования и расшифрования сообщения.

Симметричное шифрование заключается в перестановке букв на определённую позицию, так называемый ключ, в котором хранится тот самый сдвиг относительно других букв в алфавите. Данные способ применяется в банковских платежах, переводах, онлайн переводах, замки дверей. Но у данного способа есть и свой минус: можно легко разгадать код с помощью повторяющих букв и поэтому создали критерии, под который зашифрованный код должен попадать:

1) Наиболее частотные символы исходного текста не должны соответствовать наиболее частотным символам шифра;
2) В шифровании не должно быть закономерности, благодаря которому будет возможность отследить текст и разгадать шифр.

Ассиметричное шифрование заключается в паре чисел, одно из которых находится в открытом доступе и благодаря нему любой пользователь может зашифровать сообщение, а второй, закрытый, и является ключом, благодаря которому происходит расшифровка сообщения. Но закрытый ключ связан с открытым с помощью алгоритмов, а внутри этого алгоритма находится третье, секретное число, которое связано и с закрытом, и с открытом ключом. Например, если взять два больших простых числа и между собой перемножить, то получится число больше этих двух, данное число и будет лежать в основе алгоритма, а внутри этого алгоритма будет лежать такая математика, зависимая от разложения чисел на множители. И если же не

знать одно из первоначальных двух чисел, то разложить на множители умноженное число будет практически невозможной задачей.

Кроме основных шифров есть множество других, основанных на различных разделах математики. Например, благодаря геометрическим фигурам были придуманы такие шифры:

1) Шифр цезаря, линейка Энея – Отрезок
2) Шифр Сцитала – Цилиндр
3) Шифр Уилкинса – Трегольник
4) «Магический квадрат» - Квадрат
5) Шифр перестановки по группам, шифр Чейза – прямоугольник.

Шифр Цезаря один из самых древних шифров. Данный шифр относится к разделу замены, в свою очередь одними из простыми в понимании шифровки. Суть шифра заключается в сдвиге буквы относительно текущей позиции в алфавите на определённую другую позицию. Например, с помощью данного шифра можно зашифровать слово «Тайнопись» с помощью изменения каждой буквы на 3 позиции относительно текущей в алфавите и в результате получится слово «Хгмрстлфя».

П	Э	Ж	К	Л	М	Ё	О	Щ
Р	Ю	З	Л	М	Н	Ж	П	Ъ
С	Я	И	М	Н	О	З	Р	Ы
Т	А	Й	Н	О	П	И	С	Ь
У	Б	К	О	П	Р	Й	Т	Э
Ф	В	Л	П	Р	С	К	У	Ю
Х	Г	М	Р	С	Т	Л	Ф	Я

Рисунок 1. Варианты шифровки.

Если присмотреться на рисунок 1, то можно заметить, что на четвертой строчке находится изначальное слово, а на седьмой строчке слово после применения шифра и этому есть объяснение с точки зрения математики. Пусть множество всех символов (весь алфавит и символы, такие как точка и запятая) $A = \{a_1, a_2, a_3, \dots, a_n\}$, а множество знаков шифра $B = \{b_1, b_2, b_3, \dots, b_{35}\}$. Пусть f: $A \to B$, где выбирается определенная буква «a_x» алфавита A, которая сопоставляется с определенной буквой «b_x» алфавита B. Тогда буквы исходного текста $a_1, a_2, a_3, \dots, a_n$ можно зашифровать и само слово будет в виде: $f(x_1), f(x_2), \dots, f(x_n)$. Данное объяснение можно применить ко всем словам русского языка, так как генерация ключа может состоять из 35 позиций и таким образом будет $1 \cdot 2 \cdot 3 \cdot \dots \cdot 35 = 35!$ возможных отображений. Запомнить данное отображение практически невозможно, а хранить при себе всегда таблицу «ключ» шифра нецелесообразно, так как ее могут перехватить в любой момент времени.

Поэтому математический метод, позволяющий найти $f(x)$ по x намного эффективнее в применении.