СЕКЦИЯ 6. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ЗАШИФРОВАННАЯ ПЕРЕПИСКА

И. Д. Гордынец,
студент факультета международных экономических отношений и менеджмента
Учреждение образования Федерации профсоюзов Беларуси
«Международный университет «МИТСО», г. Минск
Научный руководитель:
Е. И. Шутько,
старший преподаватель кафедры информационных технологий
Учреждение образования Федерации профсоюзов Беларуси
«Международный университет «МИТСО», г. Минск

Испокон веков не было ценности большей, чем информация. Конец XX в. – это время информатики и информатизации. Технологии позволили передавать и хранить огромные объемы информации. Начало XXI в. – время логинов, паролей, аккаунтов, кодов, ключей и вместе с тем их взлом и дешифровка. Поэтому все большую важность приобретает **проблема защиты информации** от несанкционированного доступа при передаче и хранении.

Связывание проблемы безопасности общества с сохранностью данных исследований, разработок и стратегической управляющей информации в компьютерных системах, перемещение экономических преступлений в область электронной обработки данных, повсеместное взламывание электронных ящиков – это наиболее яркие подтверждения тому, насколько актуальным является использование криптографии в современном обществе.

В последнее время наряду со словом «криптография» часто встречается и слово «криптология», но соотношение между ними не всегда понимается правильно.

Криптология – наука, состоящая из двух ветвей: криптографии и криптоанализа.

Криптография – наука о способах шифрования информации с целью ее защиты от незаконных пользователей.

Криптоанализ – наука о методах и способах вскрытия шифров.

Исторически в криптографии закрепились некоторые военные слова, например криптография – защита, то есть разработка шифров, криптоанализ – нападение, то есть атака на шифры. Однако следует заметить, что не бывает хороших криптографов, не владеющих методами криптоанализа, то есть эти две науки тесно связаны между собой [1].

Методы.

Выбор шифра зависит от характера защищаемых секретов или тайны. Некоторые тайны (например, государственные, военные и другие) должны сохраняться десятилетиями, а некоторые (например, биржевые) – уже через несколько часов можно разгласить. Необходимо учитывать также и возможности того противника, от которого защищается данная информация.

Анализ взламывания электронных писем позволил сделать вывод о том, что наилучшим способом защиты электронной переписки является **зашифрованная переписка**, то есть преобразование смыслового текста в некий набор хаотических знаков (или букв алфавита). Такой способ защиты информации получил название **криптографический.** Криптография – слово греческое и в переводе означает «тайнопись». По утверждению ряда специалистов криптография – ровесник египетских пирамид.

Основное понятие криптографии – **шифр** (от арабского «цифра»; арабы первыми стали заменять буквы на цифры с целью защиты исходного текста). Секретный элемент шифра, недоступный посторонним, называется **ключом шифра**. Как правило, в древние времена использовались так называемые шифры замены и шифры перестановки.

Историческим примером **шифра замены** является **шифр Цезаря** (I в. до н. э.). Гай Юлий Цезарь использовал в своей переписке шифр собственного изобретения. Применительно к современному русскому языку он состоял в следующем. Выписывался алфавит: А, Б, В, Г, Д, Е...; затем под ним выписывался тот же алфавит, но со сдвигом на 3 буквы влево:

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х…

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х…

При зашифровке буква А заменялась буквой Г, Б заменялась на Д, и так далее. Так, например, слово «РИМ» превращалось в слово «УЛП». Получатель сообщения «УЛП» искал эти буквы в нижней строке и по буквам над ними восстанавливал исходное слово «РИМ». Ключом в шифре Цезаря является величина сдвига 3-й нижней строки алфавита. Преемник Юлия Цезаря – Цезарь Август использовал тот же шифр, но с ключом – сдвиг 4. Слово «РИМ» он в этом случае зашифровал бы в буквосочетание «ФМР».

Для примера **шифра перестановки** выберем целое положительное число, скажем, 5; расположим числа от 1 до 5 в двустрочной записи:

1	2	3	4	5
3	2	5	1	4

Зашифруем фразу «КОНСТИТУЦИЯ». В этой фразе 11 букв. Выпишем эту дополненную фразу без пропусков, одновременно разбив ее на пятизначные группы:

КОНСТ ИТУЦИ Я

Буквы каждой группы переставим в соответствии с указанной двухстрочной записью по следующему правилу: первая буква встает на третье место, вторая – на второе, третья – на пятое, четвертая – на первое и пятая – на четвертое. Оставшаяся одна буква запишется последней. Полученный текст выписывается без пропусков:

СОКТНЦТИИУЯ

При расшифровании текст 1 разбивается на группы по 5 букв и буквы переставляются в обратном порядке: первая – на 4-е место, вторая – на 2-е место, третья – на 1-е место, четвертая – на 5-е место и пятая – на 3-е место. Ключом шифра является выбранное число 5 и порядок расположения чисел в нижнем ряду двухстрочной записи [2].

Многие выдающиеся математики начиная с тех времен стали привлекаться к криптографической службе. В России великому Леонарду Эйлеру при Анне Иоанновне, кроме математики, приходилось заниматься еще и криптографией и астрологией. Именно ему историки приписывают знаменитый гороскоп Ивана VI.

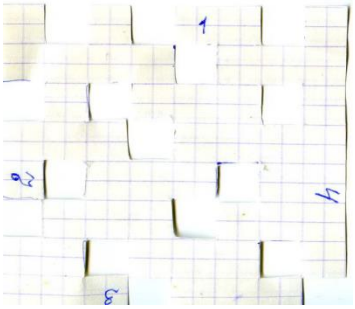
Во Франции таким математиком был Франсуа Виет, основатель современной элементарной алгебры. Его теорему о корнях и коэффициентах квадратных уравнений до сих пор изучают в школе. Описывая времена Генриха IV, даже видные литераторы Мериме и Цвейг делают явный промах: увлеченно повествуя, как перехватываются и читаются тайные послания, они забывают главное, что искусство криптографии тогда было необычайно высоко развито и сообщения, зашифрованные Франсуа Виетом, сеньором Биготьерским, вскрыть никто из современников не мог. В то же самое время он легко читал все шифровки испанского двора, а это, говорят, вызвало жалобу Филиппа II папе римскому на использование французами черной магии или нечистой силы.

Тем не менее, папы римские сами не чуждались услуг криптографов. Выдающийся итальянский математик Джероламо Кардано, имя которого дошло до нас благодаря изобретенному им шарнирному механизму и первой публикации о методе решения уравнений третьей степени, состоял у них на службе. Его перу принадлежит несколько книг по криптографии и описание метода трафаретов.

Жизнь и смерть Джероламо полны легенд. Больше всего современников Кардано поражал дар предвидения, благодаря которому он безмятежно перенес казнь своего сына и потерю крупного состояния. Вероятно, хотя бы отчасти его мистический талант знать

будущее объясняется принадлежностью к криптографической службе, знающей все, что можно узнать. Но вот предсказав продолжительность своей жизни в 75 лет, он в назначенный год покончил самоубийством, оставив записку: «Если и неверно, то неплохо придумано».

Увлечение теорией магических квадратов привело Кардано к открытию нового класса шифров перестановок, названных решетками или трафаретами. Они представляют собой квадратные таблицы, где четверть ячеек прорезана так, что при четырех поворотах они покрывают весь квадрат. Вписывание в прорезанные ячейки текста и повороты решетки продолжаются до тех пор, пока весь квадрат не будет заполнен. На рис. 1 показана решетка 4×4 и повороты по часовой стрелке на указанный ниже угол.



0' 90' 180' 270'

Рисунок 1 – Решетка Кардано

Число подобных решеток быстро растет с их размером. Так, решетка 2×2 единственна, решеток 4×4 уже 256, а решеток размером 6×6 свыше ста тысяч. Несмотря на кажущуюся сложность, шифры типа решеток довольно просто вскрываются и не могут использоваться в виде самостоятельного шифра. Однако они очень удобны и еще долго использовались в практике для усиления шифров замены [3].

Интересно использование шифров, подобных решеткам Кардано, в письмах Грибоедова к своей жене из Персии. Уже в советское время некоторых его биографов смутил тот факт, что в отдельных письмах из Персии жене нарушается характерный стиль, и замечательный писатель не похож сам на себя. При исследовании, сделанном криптоаналитиками, оказалось, что эти письма содержали дипломатические послания Александра Сергеевича. Они были сделаны через накладываемый на лист бумаги трафарет, в котором были вырезаны отдельные окошки под буквы. Написав донесение через трафарет, Грибоедов дописывал разбросанные по листу буквы в связный текст так, чтобы он содержал письмо жене, и отправлял его с обычной почтой. Российские секретные службы перехватывали это письмо, или, как принято говорить, перлюстрировали, расшифровывали, а затем доставляли адресату. По-видимому, жена его не догадывалась о двойном назначении этих посланий. Отметим большое остроумие примененного шифра и хорошую надежность; имея отдельное письмо, вскрыть шифр практически невозможно, а переписывание текста от руки разрушало шифровку, поскольку буквы неизбежно сдвигались по месту расположения [4].

Результаты.

Описанные выше способы шифровки текста легли в основу компьютерной программы, разработанной в рамках проекта «Зашифрованная переписка», представленного на III Внутривузовской студенческой научно-практической конференции «Правовые и социально-экономические аспекты становления Республики Беларусь (к 25-летию Конституции Республики Беларусь)».

Целесообразность выбора именно этих способов шифровки электронных писем связана прежде всего с тем, что шифровать необходимо исключительно текстовые

сообщения. Использование при этом естественных языков повышает степень защиты шифра в силу их огромной избыточности.

Однако с высоты достижения современной криптографии, шифр Цезаря предельно примитивен. Для более полной защиты электронного письма автором предусмотрено усиление шифра Цезаря.

Шифрование текста с помощью решеток Кардано связано прежде всего с уникальностью разрабатываемого фрагмента программы. Кропотливый анализ существующих аналогов программ позволил сделать вывод о том, что разработанный автором алгоритм шифрования текста с помощью решеток Кардано является единственным.

Шифровка текста с помощью решеток Кардано усиливает шифры замены.

Программа является открытой для дальнейшего усовершенствования. В частности, предполагается формировать решетки Кардано случайным образом.

Для увеличения объема шифруемых писем планируется организовать их ввод и вывод из файлов.

Компьютерная реализация методов.

В 2019 году исполнится 65 лет со дня смерти создателя идеально простого теоретического компьютера Алана Тьюринга. Благодаря работам Тьюринга и его коллег была создана одна из первых ЭВМ в мире, получившая название «Колосс». Эта машина взломала код «Лоренц», что позволило союзникам быть в курсе переписки высших руководителей гитлеровской Германии и **сократило длительность войны как минимум на несколько месяцев**. Сама машина представляла собой бесконечную ленту и автомат, который видел и мог заменить на ленте только один символ, а также двигался влево и вправо. Решетка Кардано тоже позволяет записывать в клетку символ, только не перемещается, а поворачивается. По мнению автора, **шифрование с помощью решеток Кардано также идеально просто,** а значит, надежно. Выбор этого метода и его программная реализация – это дань памяти создателю первого компьютера Алану Тьюрингу.

При слове «шифровка» у каждого возникает в голове образ Штирлица. Бесстрашный разведчик в известном культовом сериале «Семнадцать мгновений весны» использовал относительно эффективный ручной (то есть без применения компьютеров или специальных шифровальных машин) шифр, который дожил почти до наших дней с незапамятных времен – это шифровка сообщения по тексту книги. В этом шифре сообщение состоит из чисел. В качестве ключа получателю сообщения указывается страница, строка и буква в определенном издании, о котором уславливаются заранее. Начиная с этой буквы, он должен отсчитать количество знаков, равное очередному числу в сообщении, и подставить полученную букву в текст.

В перспективе планируется **шифровку сообщения по тексту книги** перевести в программный код. Таким образом, проект «Зашифрованная переписка» обогатится еще на один **алгоритм Штирлица.**

Слова **«война закончилась на несколько месяцев раньше»** благодаря компьютерной расшифровке вражеских радиограмм означают, что **сохранены тысячи человеческих жизней**. Во Второй мировой войне погиб каждый третий житель Беларуси. Накануне 75-й годовщины освобождения нашей страны от немецко-фашистских захватчиков эти слова становятся главными, а тема шифровки и дешифровки приобретает особую значимость.

Список использованных источников

1. Абельсон, Х. Атака битов: твоя жизнь, свобода и благополучие в цифровую эпоху / Х. Абельсон, К. Ледин, Г. Льюис. – М. : Символ-Плюс, 2009. – 392 с.

2. Арутюнов, В. В. Защита информации / В. В. Арутюнов. – М. : Либерея-Бибинформ, 2008. – 56 с.
3. Панасенко, С. П. Алгоритмы шифрования / С. П. Панасенко. – СПб. : BHV, 2009. – 576 с.
4. Кузнецов, А. А. Защита деловой переписки (секреты безопасности) / А. А. Кузнецов. – М. : Экзамен, 2018. – 239 с.