КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ ШИФРОВ ЗАМЕНЫ

Круглая А. А., Кулевич А. О.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Стройникова Е. Д. – ст. преп. кафедры информатики

В работе исследованы существующие алгоритмы шифров замены и методы их реализации. Зашифровывание и расшифровывание с использованием ряда алгоритмов продемонстрировано на примерах. Реализованы учебные программы на языке программирования C# для ознакомления и изучения студентами. Преимуществами программных кодов являются их понятность и доступность.

Современный мир очень сложно представить без интернета и социальных сетей. Основой передачи информации в интернете является шифрование, так, самое простое сообщение «Привет» успевает быстрее, чем за секунду, зашифроваться у одного пользователя и расшифроваться у другого. Изучением шифрования занимается криптография – наука и искусство передачи сообщений в таком виде, чтобы их нельзя было прочитать, не зная специального секретного ключа. В наши дни криптография характеризуется использованием открытых алгоритмов шифрования.

Шифры разделяются на два больших класса: шифры замены и шифры перестановки. Данная

работа посвящена исследованию алгоритмов шифров замены (или подстановки), разновидности которых представлены на рисунке 1.

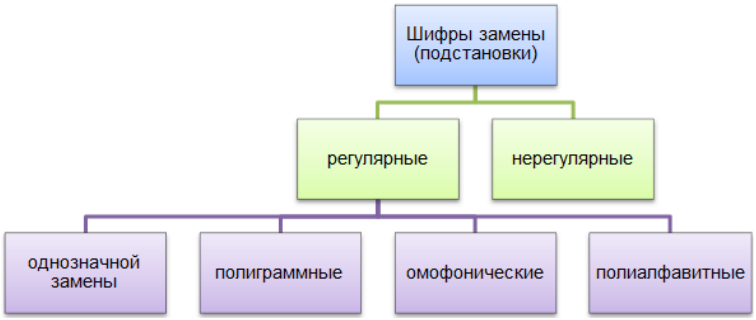

Рисунок 1 – Разновидности шифров подстановки

Принцип шифрования методом замены. Каждую букву открытого сообщения зашифровывают, сопоставляя её с каким-то множеством шифрозамен, где первой букве соответствует некоторое множество M_1, второй – M_2 и т. д. Шифрозамены выбираются таким образом, чтобы любые два множества M_i и M_j при $i \neq j$ не содержали одинаковых элементов, т. е. $M_i \cap M_j = \emptyset$.

I. Регулярные шифры – шифры, в которых шифрозамены состоят из строго определённого количества символов или в шифрограмме они отделяются друг от друга пробелом, точкой, тире и т. п.

1. Шифры однозначной замены (или моноалфавитные, простые подстановочные) характеризуются тем, что количество шифрозамен для каждого символа исходного алфавита равно 1.

Шифр **Атбаш** состоит в замене каждой буквы другой буквой, которая находится в алфавите на таком же расстоянии от конца, что и оригинальная буква от начала. Например, в английском алфавите буква «A» заменяется на «Z», буква «B» – на «Y» и т. д. Таким образом, сообщение «INFORMATICS» зашифруется в виде «RMULINZGRXH». Программа, реализующая алгоритм шифра Атбаш, доступна по ссылке: https://pastebin.com/vWG8PBR3.

Шифр Цезаря. Во время шифрования каждая буква заменяется другой, отстоящей от неё в циклически записанном алфавите на фиксированное число позиций. Программа доступна по ссылке: https://pastebin.com/ssjdMDcD. **ROT13** является современным примером шифра Цезаря. В этом шифре каждый символ английского алфавита циклически сдвигается на 13 позиций (рисунок 2). Если зашифруем сообщение «KSIS», то получим сообщение «XFVF». А если зашифруем «XFVF» (или, что то же самое, расшифруем его), то получим снова «KSIS».

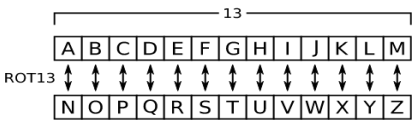

Рисунок 2 – Преобразование букв английского алфавита при помощи ROT13

2. Полиграммные шифры замены. В данном виде шифрования одной шифрозамене может соответствовать сразу несколько символов исходного текста.

Биграммный шифр Порты – первый известный биграммный шифр, который представляется в виде квадратной таблицы. Вертикально слева и горизонтально сверху находится алфавит, в самих ячейках записываются любые символы. Главное, чтобы содержимое ячеек не повторялось. Сообщение шифруется парами букв исходного текста. Первая буква указывает на строку шифрозамены, а вторая – на столбец. При нечётном количестве букв в исходном сообщении к нему добавляется вспомогательный символ. К примеру, если при помощи таблицы шифрозамен для шифра Порты, приведённой в [1], зашифруем слово «ИН ФО РМ АТ ИК А», то получим «261 603 477 018 258 031». В качестве вспомогательного символа использована буква «Я».

3. Омофонические шифры (или однозвучные, многозначной замены) характеризуются тем, что для отдельных символов исходного алфавита количество шифрозамен больше 1 ($|M_i| \geq 1$ для одного символа). Примером омофонического шифра является **книжный шифр**, в котором каждый элемент открытого текста (каждая буква или слово) заменяется на указатель (например номер страницы, строки и столбца) аналогичного элемента в дополнительном тексте-ключе.

4. Полиалфавитные шифры состоят из нескольких шифров однозначной замены и отличаются друг от друга способами выбора варианта алфавита для шифрования одного символа.

Таблица Трисемуса – многоалфавитный шифр, основанный на таблице размером $n \times n$, где n – количество символов в алфавите. В первой строке таблицы записываются буквы алфавита в порядке их очерёдности, во второй – та же последовательность букв с циклическим сдвигом на одну позицию

влево, в третьей – с циклическим сдвигом на две позиции влево и т. д. Исходный текст состоит из букв первой строки, i-я буква сообщения зашифровывается буквой, находящейся в i-й строке, в том же столбце, что и исходная буква. Если длина текста больше n, то после использования последней строки вновь возвращаются к первой и т. д. Так, используя таблицу размером 33×33 для русского алфавита, сообщение «БГУИР» зашифруется в виде «БДХЛФ».

Система шифрования Виженера основана на таблице Трисемуса, отличие от предыдущего метода шифрования заключается в том, что вначале выбирается ключ, который состоит из символов алфавита, i-я буква исходного сообщения зашифровывается буквой, находящейся в строке, начинающейся с i-й буквы ключа, в том же столбце, что и исходная буква. Если длина ключа меньше длины сообщения, то ключ используется повторно. Например, зашифровывая сообщение «ИНФОРМАТИКА» с использованием таблицы размером 33×33 для русского алфавита и ключа «КСИС», получим шифрограмму «УЯЭАЫЮИДУЬИ». Программа доступна по ссылке: https://pastebin.com/aDjc79YY.

II. Нерегулярные шифры. В шифрах данного типа шифрозамены состоят из разного количества символов и записываются в шифрограмме подряд (без отделения друг от друга), что значительно затрудняет криптоанализ.

Совмещённый шифр (или совмещённая таблица), названный так из-за необычного использования одно- и двухцифровых шифрозамен. Таблица шифрозамен содержит десять столбцов с нумерацией 0, 9, 8, 7, 6, 5, 4, 3, 2, 1. В начальной строке записано слово-ключ, исключая повторяющиеся буквы. В следующие строки вписываются по десять не вошедших в слово-ключ букв в порядке их следования в алфавите. Все строки, кроме начальной, нумеруются по порядку, начиная с 1. Во время шифрования, если буква исходного сообщения совпадает с какой-то буквой слова-ключа, то она заменяется одной цифрой – номером столбца, в противном случае – двумя – номерами строки и столбца. Так, сообщение «ИНФОРМАТИКА» зашифруется «146242028117261487» (см. рисунок 3).

	0	9	8	7	6	5	4	3	2	1
	Д	Е	К	А	Н					
1	Б	В	Г	Ё	Ж	З	И	Й	Л	М
2	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
3	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	-

Рисунок 3 – Пример таблицы шифрозамен совмещённого шифра с ключом «ДЕКАН»

Основным приёмом при вскрытии криптограмм шифров замены является анализ частоты встречаемости букв в исходном тексте. Несмотря на вытеснение шифров замены блочными шифрами, одноразовые блокноты, основанные на шифре Вернама [2], продолжают использоваться на государственном уровне в наше время для обеспечения сверхсекретных каналов связи.

Разработанные авторами на языке C# программы, реализующие ряд алгоритмов шифров замены, удобны в использовании благодаря их понятности и доступности. Для большего удобства в кодах программ присутствуют пояснения.

Список использованных источников:

1. Анисимов В. В. Криптографические методы защиты информации. Шифры замены [Электронный ресурс]. – Режим доступа : https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema4.

2. Свободная энциклопедия Википедия. Шифр Вернама [Электронный ресурс]. – Режим доступа : https://ru.wikipedia.org/wiki/Шифр_Вернама.