МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«14» ноября 2017г.

ШИФРОВАНИЕ С ПОМОЩЬЮ ТАБЛИЦЫ ВИЖЕНЕРА

Методические указания по выполнению практических работ по дисциплине «Основы информационной безопасности» для студентов специальности 10.03.01

Курск 2017

УДК 004.056.55

Составители: А.Л. Марухленко

Рецензент
Кандидат технических наук, доцент *А.Г. Спеваков*

Шифрование с помощью таблицы Виженера: методические указания к выполнению практических работ / Юго-Зап. гос. ун-т; сост. А. Л. Марухленко Курск, 2017. - 9 с. Библиогр.: с. 9.

Содержат сведения по вопросам шифрования и расшифрования с помощью таблицы Виженера. Указывается порядок выполнения практической работы, пример выполнения работы, правила оформления, содержание отчета, варианты заданий.

Методические указания по выполнению практических работ соответствуют требованиям программы, утвержденной учебно-методическим объединением, предназначены для студентов направления подготовки 10.03.01 для изучения дисциплины «Основы информационной безопасности».

Текст печатается в авторской редакции

Подписано в печать 01.11.2017. Формат 60х84 1/16.
Усл.печ. л. 0,5. Уч.-изд.л. 0,5. Тираж 30 экз. Заказ _____. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Получение навыков создания зашифрованного сообщения при помощи алгоритма шифрования Виженера

2. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Шифр Виженера (фр. Chiffre de Vigenère) — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джован Баттиста Беллазо (итал. Giovan Battista Bellaso) в книге La cifra del. Sig. Giovan Battista Bellaso в 1553 году, однако в XIX веке получил имя Блеза Виженера, французкого дипломата. Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа.

История

Первое точное документированное описание многоалфавитного шифра было сформулировано Леоном Баттиста Альберти в 1467 году, для переключения между алфавитами использовался металлический шифровальный диск. Система Альберти переключает алфавиты после нескольких зашифрованных слов. Позднее, в 1518 году, Иоганн Трисемус в своей работе «Полиграфия» изобрел tabula recta — центральный компонент шифра Виженера.

То, что сейчас известно под шифром Виженера, впервые описал Джованни Батиста Беллазо в своей книге La cifra del. Sig. Giovan Battista Bellaso. Он использовал идею tabula recta Трисемуса, но добавил ключ для переключения алфавитов шифра через каждую букву. Блез Виженер представил своё описание простого, но стойкого шифра перед комиссией Генриха III во Франции в 1586 году, и позднее изобретение шифра было присвоено именно ему. Давид Кан в своей книге «Взломщики кодов» отозвался об этом осуждающе, написав, что история «проигнорировала важный факт и назвала шифр именем Виженера, несмотря на то, что он ничего не сделал для его создания».

Шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому. Известный писатель и математик Чарльз Лютвидж Доджсон (Льюис Кэрролл) назвал шифр Виженера не взламываемым в своей статье «Алфавитный шифр» англ. The Alphabet Cipher, опубликованной в детском журнале в 1868 году. В 1917 году Scientific American также отозвался о шифре Виженера, как о неподдающемся взлому. Это представление было опровергнуто после того, как Казиски полностью взломал шифр в XIX веке, хотя известны случаи взлома этого шифра некоторыми опытными криптоаналитиками ещё в XVI веке.

Шифр Виженера достаточно прост для использования в полевых условиях, особенно если применяются шифровальные диски. Например, «конфедераты» использовали медный шифровальный диск для шифра Виженера в ходе Гражданской войны. Послания Конфедерации были далеки от секретных, и их противники регулярно взламывали сообщения. Во время войны командование Конфедерации полагалось на три ключевых словосочетания: «Manchester Bluff», «Complete Victory» и — так как война подходила к концу — «Come Retribution».

Гилберт Вернам попытался улучшить взломанный шифр (он получил название шифр Вернама - Виженера в 1918 году), но, несмотря на его усовершенствования, шифр так и остался уязвимым к криптоанализу. Однако работа Вернама в конечном итоге всё же привела к получению шифра, который по-настоящему трудно взломать.

Описание

Квадрат Виженера, или таблица Виженера, также известная как tabula recta, может быть использована для шифрования и расшифрования.

В шифре Цезаря каждая буква алфавита сдвигается на несколько строк; например в шифре Цезаря при сдвиге +3, A стало бы B, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов или квадрат (таблица) Виженера. Применительно к Русскому алфавиту таблица Виженера составляется из строк по 31 символов, причём

каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 31 различных шифров Цезаря. На разных этапах кодировки шифр Виженера использует различные алфавиты из этой таблицы. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. В приложении 1 представлена таблица Виженера.

3. ВЫПОЛНЕНИЕ РАБОТЫ

Предположим, что исходный текст имеет вид:

СООБЩЕНИЕ

Человек, посылающий сообщение, записывает ключевое слово («ОКНО») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

ОКНООКНОО

Первый символ исходного текста С зашифрован последовательностью О, которая является первым символом ключа. Первый символ Я шифрованного текста находится на пересечении строки С и столбца О в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста Ш получается на пересечении строки О и столбца К. Остальная часть исходного текста шифруется подобным способом.

Исходный текст: СООБЩЕНИЕ

Ключ: ОКНООКНОО

Зашифрованный текст: ЯШЪПЖПЬЦУ

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

Если буквы А-Я соответствуют числам 0-32, то шифрование Виженера можно записать в виде формулы:

$$C_i \equiv \left(P_i + K_i\right) \bmod 32$$

Расшифровка:

$$P_i \equiv \left(C_i - K_i + 31\right) \bmod 32$$

4. ВАРИАНТЫ ЗАДАНИЙ

№	Исходный текст
1	Шумит дубравушка к непогодушке
2	Утром вороны каркают к дождю
3	Сорока на хвосте принесла
4	Снег холодный, а от мороза укрывает
5	Сирень или берёза, а всё дерево
6	Сегодня не тает, а завтра кто знает
7	Розы без шипов не бывает
8	Не высок лесок, а от ветра защищает
9	На всех и солнышко не светит
10	Красна ягодка, да на вкус горька
11	В осеннее ненастье семь погод на дворе
12	Ветром ветра не смеряешь
13	Пропущенный час годом не нагонишь
14	Счастливые часов не наблюдают
15	Друг неиспытанный, как орех не расколотый
16	Дружи с теми, кто лучше тебя самого
17	Крепкую дружбу и топором не разрубишь
18	Кто друг прямой, тот брат родной
19	лучше выслушать упрёки друга, чем потерять его
20	Одна пчела много мёду не принесёт
21	С тем не ужиться, кто любит браниться
22	Старый друг лучше новых двух
23	На чужой сторонушке рад родной воробушке
24	Народы нашей страны дружбой сильны
25	Поднявший меч от меча и погибнет
26	При солнце тепло, при Родине добро
27	Старая слава новую любит
28	Любишь кататься - люби и саночки возить
29	Кто пахать не ленится, у того хлеб родится
30	На печи не храбрись, а в поле не трусь

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1) Панасенко, С. Алгоритмы шифрования [Текст] / С. Панасенко. Спб: БХВ-Петербург, 2009, 576 стр.

2) Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография [Текст] / А.Г. Ростовцев, Е.Б. Маховенко. М: АНО НПО "Профессионал", 2005, 480 стр.

3) Рябко, Б. Я., Фионов, А. Н. Основы современной криптографии для специалистов в информационных технологиях [Текст] / Б. Я. Рябко, А. Н. Фионов. М: Научный мир, 2004, 179 стр.

4) Смарт, Н. Криптография [Текст] / Н. Смарт. М: Техносфера, 2006, 528 стр.