УДК 004.056.55

М. А. Вареник, А. В. Корсак
Учреждение образования «Барановичский государственный университет», Барановичи

ШИФРОВАНИЕ И ДЕШИФРОВАНИЕ С ПОМОЩЬЮ АЛГОРИТМА ПОЛИАЛФАВИТНОЙ ЗАМЕНЫ

Введение. В современном мире без шифрования не обходится ни одна сфера деятельности человека. При этом сохранение конфиденциальности отправляемых данных является актуальным вопросом. Для сохранения данных используются разные методы шифровки и дешифровки.

Шифрование — это метод преобразования данных, пригодных для чтения человеком, в форму, которую человек не сможет прочитать. За счет этого данные остаются конфиденциальными и приватными.

Дешифрование — обратная операция. Преобразование нечитаемых данных в читаемые.

Цель данного исследования заключается в разработке программы шифровки и дешифровки, используя алгоритм полиалфавитной замены. Данная программа будет позволять пользователю шифровать или дешифровать заданный текст, используя ключевое слово, задуманное или известное ранее. Основная задача — разработать класс, основанный на данном алгоритме шифрования.

Основная часть. Полиалфавитные шифры состоят из нескольких шифров однозначной замены и отличаются друг от друга способом выбора варианта алфавита для зашифрования одного символа. Рассмотрим примеры алгоритмов полиалфавитной замены [1].

1. Диск Альберти. Он состоял из двух дисков — внешнего неподвижного и внутреннего подвижного, на которые были нанесены буквы алфавита. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замене ее на букву с внутреннего диска, стоящую под ней. После этого внутренний диск сдвигался на одну позицию, шифрование второй буквы производилось уже по новому шифр-алфавиту. Ключом данного шифра являлся порядок расположения букв на дисках и начальное положение внутреннего диска относительно внешнего.

2. Таблица Трисемуса — это таблица со стороной, равной n, где n — количество символов в алфавите. В первой строке матрицы записываются буквы в порядке их очередности в алфавите, во второй — та же последовательность букв, но с циклическим сдвигом на одну позицию влево, в третьей — с циклическим сдвигом на две позиции влево и т. д.

Первая строка является одновременно и алфавитом для букв открытого текста. Первая буква текста шифруется по первой строке, вторая буква — по второй и т. д. После использования последней строки вновь возвращаются к первой.

3. Система шифрования Виженера. В 1586 году французский дипломат Блез Виженер представил перед комиссией Генриха III описание простого, но довольно стойкого шифра, в основе которого лежит таблица Трисемуса.

Перед шифрованием выбирается ключ из символов алфавита. Сама процедура шифрования заключается в следующем: по i-му символу открытого сообщения в первой строке определяется столбец, а по i-му символу ключа в крайнем левом столбце — строка. На пересечении строки и столбца будет находиться i-й символ, помещаемый в шифрограмму. Если длина ключа меньше сообщения, то он используется повторно.

4. Роторные машины. Время начала создании электромеханических роторных машин относится к первой половине XX века. Некоторые из них использовались в разных странах вплоть до 1980-х годов. В большинстве из них использовались роторы (механические колеса), взаимное расположение которых определяло текущий алфавит шифрозамен, используемый для выполнения подстановки. Наиболее известной из роторных машин является немецкая машина времен Второй мировой войны «Энигма». Суть работы машины: выходные штыри одного ротора соединены со входными штырями следующего ротора, при нажатии символа исходного сообщения на клавиатуре замыкается электрическая цепь, в результате чего загорается лампочка с символом шифрозамены.

Для реализации поставленной задачи использована среда программирования Microsoft Visual Studio 2017 и язык программирования C++ [2]. Функциональные требования к разрабатываемой программе: открывать файлы с данными для дешифрования/шифрования; записывать данные в файл; генерировать ключи; шифровать данные; дешифровать данные. Нефункциональные требования: удобство использования; пользовательский интерфейс должен быть Windows-совместимым; пользовательский интерфейс системы должен быть понятным; алгоритм шифрования основан на квадрате Виженера (рисунок 1).

На рисунке 2 представлены классы, содержащие в себе выполняемые ими операции и атрибуты. Класс «Основная форма» используется для диалога с пользователем, класс «Шифровка» содержит в себе атрибуты и операции, необходимые для выполнения шифрования и дешифрования текста.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Рисунок 1 — Квадрат Виженера

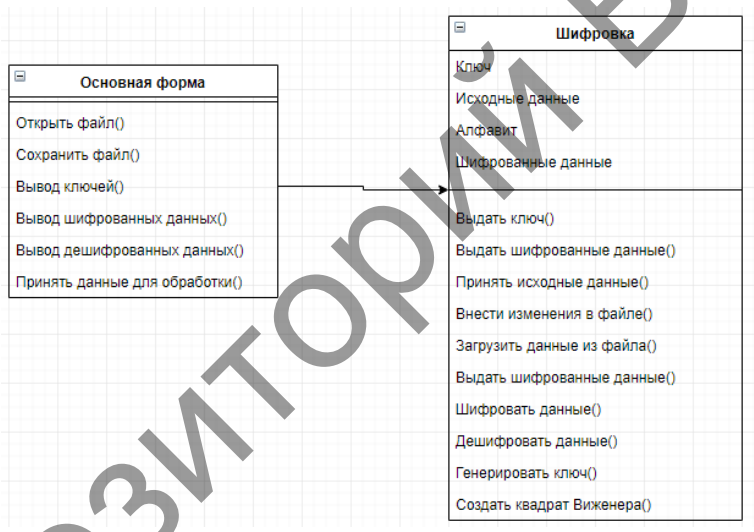

Рисунок 2 — Диаграмма классов

В ходе исследования была разработана программа шифровки и дешифровки текста.

Вводимыми данными является шифруемый или дешифруемый текст. Используя введённые данные, программа выполняет шифровку (дешифровку) введённого текста по ключевому слову.

Заключение. Программу можно использовать для шифровки (дешифровки) текста, если никто, кроме получателя, не должен знать исходный текст.

Список цитируемых источников

1. Шифры замены [Электронный ресурс]. — Режим доступа: https://sites.google.com/site/anisimovkhv/learning/krip-to/lecture/tema4#p45/ . — Дата доступа: 14.10.2019.

2. *Пахомов, Б. И.* Самоучитель C/C++ и Borland C++Builder 2006 / Б. И. Пахомов. — СПб. : БХВ-Петербург, 2006. — 576 с.