Инженерный вестник Дона, №11 (2021)
ivdon.ru/ru/magazine/archive/n11y2021/7269

Программная реализация шифрования текстовых фраз

Р.Б. Адаев

Российский государственный университет им. А.Н. Косыгина, Москва

Аннотация: В статье рассматривается вопросы шифрования, использования двух различных методов шифрования текстовых фраз: шифра Цезаря и Виженера. Приводится пример использования данных шифров. На языке Java спроектирована программа, позволяющая осуществлять шифрование и дешифрование.
Ключевые слова: криптография, шифрование, дешифрование, шифр Виженера, шифр Цезаря, Java.

В современном мире часто стоит задача сохранения целостности информации и обеспечения невозможности несанкционированного доступа к ней, этими вопросами занимается наука криптография [1]. Для сохранения конфиденциальности используют шифрование — комплекс методов и способов конвертации информации с помощью шифров [2, 3]. Шифр включает набор символов для записи сообщений (алфавит), алгоритмы преобразования, определяющие перевод сообщения из зашифрованного состояния в расшифрованное и обратно, и ключ (ключи), использующиеся для выбора корректного преобразования информации из имеющейся в соответствии с алгоритмом [4].

Существуют различные алгоритмы преобразования. Один из них — шифр Цезаря, который получил название в честь Г. Ю. Цезаря. В нём каждый символ заменяется другим, удаленным от него в алфавите на определенное число позиций. Этот шифр не обладает высокой надёжностью [5, 6].

Процессы шифрования и дешифрования можно выразить в виде формулы:

$$\begin{cases} y_i = x_i + k \bmod n \\ x_i = y_i - k \bmod n \end{cases},$$

где x_i — символ искомого текста, y_i — символ зашифрованного текста, n — мощность алфавита, k — ключ (число).

Выпишем индексы российских и латинских букв (рис. 1).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я		
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								

Рис. 1. – Индексы букв

Рассмотрим пример шифрования шифром Цезаря для к=1 фраз «СЕТИ И ТЕЛЕКОММУНИКАЦИИ» и «LONDON GREAT BRITAIN».

Буква «С» имеет индекс 19, 19+1=20, первая буква зашифрованного сообщения будет иметь индекс 20, это буква «Т». Пробелы и прочие символы остаются неизменными. Шифрование представлено на рис. 2.

8	С		Е	Т	И		И		Т	Е	Л	Е	К	О	М	М	У	Н	И	К	А	Ц	И	И									
9		19	6	20	10		10		20	6	13	6	12	16	14	14	21	15	10	12	1	24	10	10									
10		20	7	21	11		11		21	7	14	7	13	17	15	15	22	16	11	13	2	25	11	11									
11	Т		Ё	У	Й		Й		У	Ё	М	Ё	Л	П	Н	Н	Ф	О	Й	Л	Б	Ч	Й	Й									
12																																	
13																																	
14	L		O	N	D	O	N		G	R	E	A	T		B	R	I	T	A	I	N												
15		12	15	14	4	15	14		7	18	5	1	20		2	18	9	20	1	9	14												
16		13	16	15	5	16	15		8	19	6	2	21		3	19	10	21	2	10	15												
17	M		P	O	E	P	O		H	S	G	B	U		C	S	J	U	B	J	O												

Рис. 2. – Шифрование фраз

Более надёжным является шифр Виженера. Ключом в этом шифре является слово. Допустим, есть некий алфавит мощностью n. Тогда шифрование можно отобразить формулой:

$C_i = (P_i + K_i) \bmod n$, а дешифрование:

$P_i = (\mathrm{C}_i - K_i + n) \bmod n$,

где Pi — символ шифруемого текста, Ci — символ шифрованного текста, Ki — символ ключевого слова [7, 8].

Для шифрования и дешифрования используют квадрат Виженера — таблицу с n строками и столбцами, содержащую буквы алфавита (рис. 3).

Рассмотрим пример шифрования фразы «СЕТИ И ТЕЛЕКОММУНИКАЦИИ», кодовое слово «ЛИСТ». Воспользуемся квадратом Виженера, выделим строки «Л», «И», «С», «Т». Запишем

шифруемую фразу, а под ней будем повторять кодовое слово (таблица №1). Пробелы не кодируются.

	А	**Б**	**В**	**Г**	**Д**	**Е**	**Ё**	**Ж**	**З**
А	А	Б	В	Г	Д	Е	Ё	Ж	З
Б	Б	В	Г	Д	Е	Ё	Ж	З	И
В	В	Г	Д	Е	Ё	Ж	З	И	Й
Г	Г	Д	Е	Ё	Ж	З	И	Й	К
Д	Д	Е	Ё	Ж	З	И	Й	К	Л
Е	Е	Ё	Ж	З	И	Й	К	Л	М
Ё	Ё	Ж	З	И	Й	К	Л	М	Н
Ж	Ж	З	И	Й	К	Л	М	Н	О
З	З	И	Й	К	Л	М	Н	О	П

Рис. 3 – Квадрат Виженера

Таблица № 1

Шифрование по алгоритму Виженера

С	Е	Т	И		И		Т	Е	Л	Е	К	О	М	М	У	Н	И	К	А	Ц	И	И
Л	И	С	Т		Л		И	С	Т	Л	И	С	Т	Л	И	С	Т	Л	И	С	Т	Л

Первая буква искомого сообщения - «С», первая буква кодовой фразы - «Л», нужно найти букву на пересечении столбца «С» и строки «Л», это буква «Э». Вторая буква фразы - «Е», находим столбец с такой буквой, этой букве соответствует буква «И» кодовой фразы, на пересечении столбца «Е» и строки «И» находится буква «Н» (рис. 4).

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

Рис. 4. – Поиск значений по квадрату Виженера

Эти буквы добавляются в качестве символов зашифрованной фразы. В результате расшифровки получилась фраза: ЭНДЫ Ф ЫЦЮРУАЯШЬЯЫЦИЗЫФ.

Программа, реализующая данные алгоритмы, написана на языке Java. В качестве обоснований данного выбора можно назвать независимость от платформы и современность языка [9]. Программная форма включает две радиокнопки для выбора алгоритма и две кнопки для шифрования и дешифрования.

В шифровании по алгоритму Цезаря для каждого символа текста определяется, к какому алфавиту он относится (русский или английский, прописные или строчные буквы), определяется длина текущего алфавита и индекс текущего символа в нём. Если символ не найден, то добавляем его в результирующую строку в неизменном виде. Символ заменяется в соответствии с ключом. Алгоритм цикличен, правее самого правого символа алфавит стоит его первый символ [10]. Выходное сообщение по длине совпадает с входным.

Для дешифрации параметр ключ задаётся отрицательным.

Для шифрования по алгоритму Виженера первоначально определяется цепочка кодового слова. Для этого определяется длина текста и кодового слова. Далее в цикле для каждого символа текста определяется, принадлежит ли он алфавиту, если да, то ему в соответствие ставится символ кодовой цепочки, иначе в кодовую цепочку попадает сам символ. Если ставится в соответствие не символ кодовой цепочки, то из счётчика вычитается 1, чтобы буква была учтена в следующий раз. Кодовая цепочка совпадает по длине с текстом. Для шифрования для каждого символа текста определяется, к какому алфавиту он относится (русский или английский, прописные или строчные буквы), определяется длина текущего алфавита и индекс текущего символа в нём. Если символ не найден, то добавляем его в неизменном виде.

Далее, если символы кодового слова и текста не совпадают по регистру, они приводятся к одному регистру. Затем происходит шифрование: по сумме индексов символа кодового слова и текста за вычетом единицы ищется индекс новой буквы.

Блок-схема алгоритма Цезаря представлена на рис. 5. Блок-схема алгоритма Виженера представлена на рис. 6.

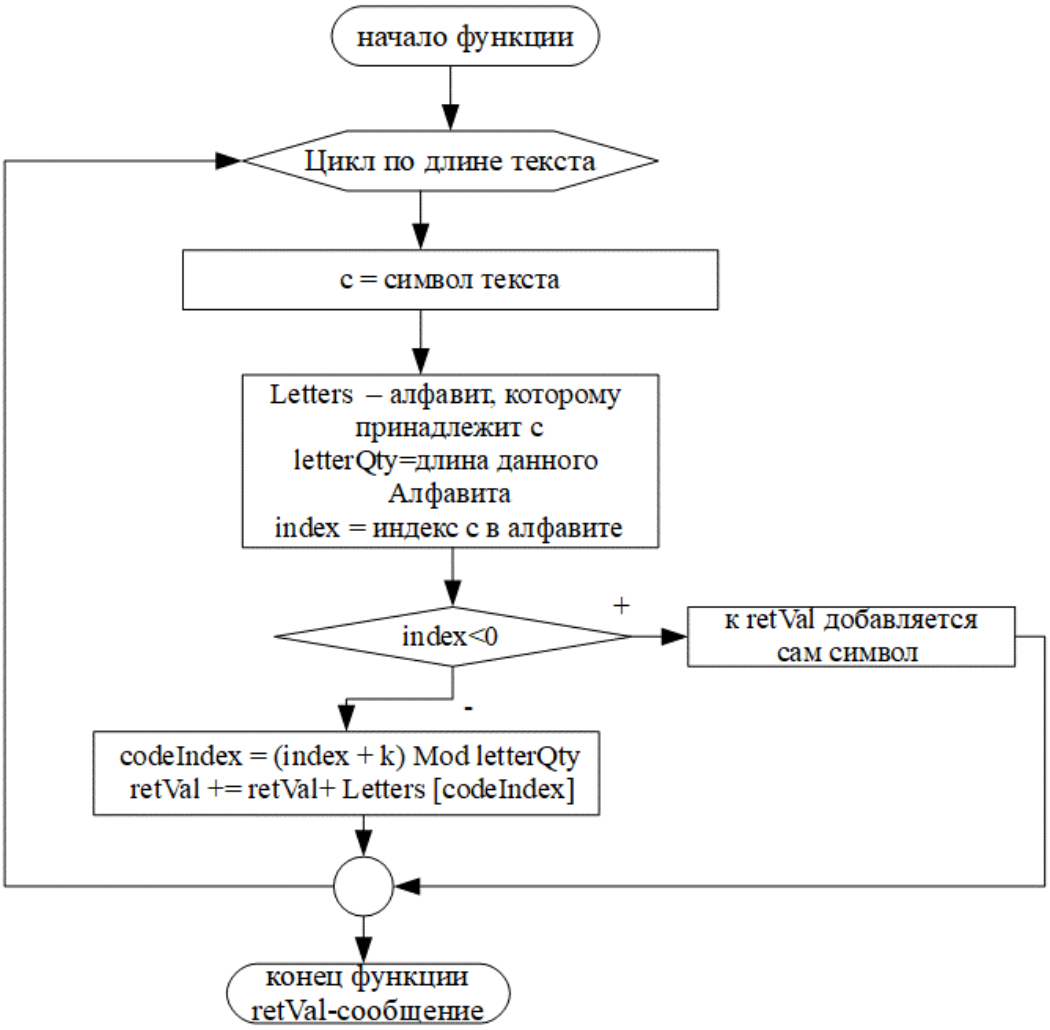

Рис. 5. – Блок-схема алгоритма Цезаря

Пример работы программы представлен на рис. 7. После введения шифруемой фразы и ключевого слова выводится зашифрованное сообщение. Его можно расшифровать кнопкой «Дешифровать».

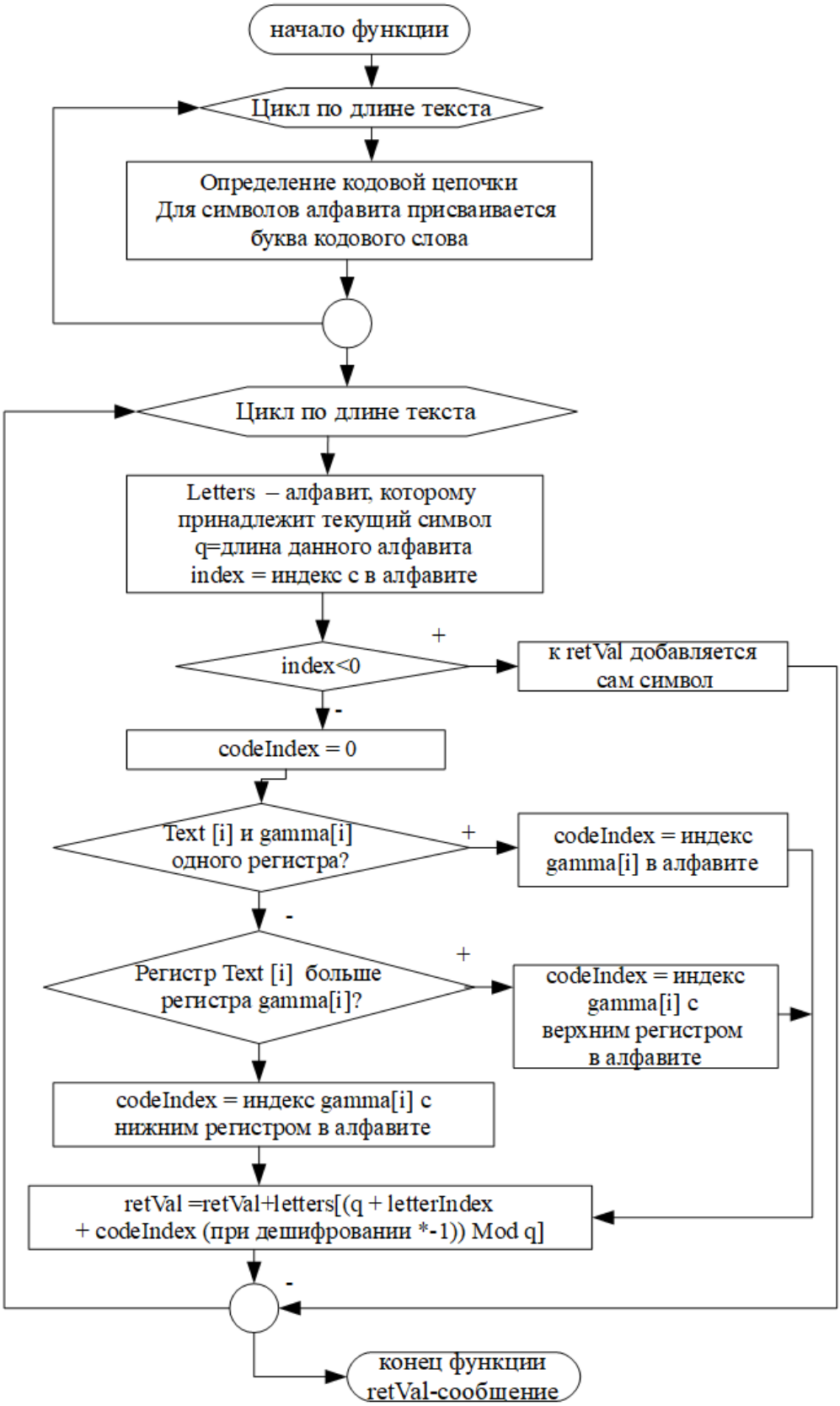

Рис. 6 – Блок-схема алгоритма Виженера

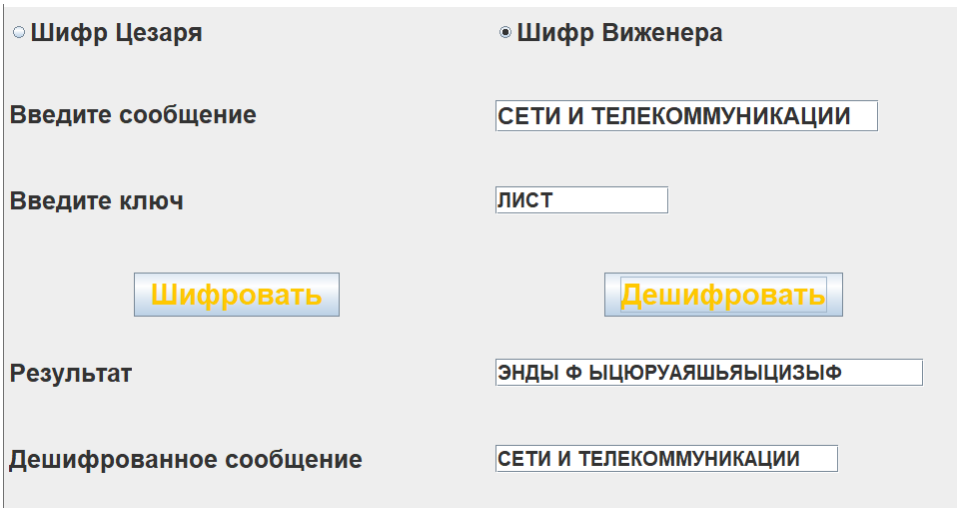

Рис. 7 – Шифрование по алгоритму Виженера

Литература

1. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации. М.: КноРус, 2020. 189 с.

2. Дмитриев А. С., Холкин Д. О., Маслова М. А. Метод передачи сообщений, с использованием лучших способов организации обмена данными и криптографических протоколов обмена мгновенными сообщениями с использованием сквозного шифрования // Инженерный вестник Дона, 2009, №6. URL: ivdon.ru/ru/magazine/archive/n6y2021/7054/.

3. Корсунов Н. И., Титов А. И. Повышение эффективности защиты информации модификацией шифра Виженера // Научные ведомости Белгородского государственного университета. 2010. №7(78). С. 171-175.

4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 816 с.

5. Фомичёв В. М. Дискретная математика и криптология: Курс лекций. М.: Диалог-МИФИ, 2013. 397 с.

6. Singh S. The Code Book, Histoire des codes secrets (англ.). США, Нью-Йорк: Doubleday, 1999. 416 с.

7. Гатченко Н. А., Исаев А. С., Яковлев А.Д. Криптографическая защита информации. СПб: НИУ ИТМО, 2012. 142 с.

8. Kochladze Z., Gelashvili G. Using Genetic Algorithm for the Breaking Vigenere Cipher // Computer Science and Telecommunications. 2017. №2(52). С. 53-56.

9. Глод О. Д., Сетраков В. В. Веб-сервис для интеграции в урбанистическую среду // Инженерный вестник Дона, 2018, №4. URL: ivdon.ru/ru/magazine/archive/n4y2018/5436/.

10. Панасенко С. Алгоритмы шифрования. СПб: БХВ-Петербург, 2009. 576 с.

References

1. Babash A. V., Baranova E. K. Kriptograficheskiye metody zashchity informatsii [Cryptographic methods of information protection]. M.: KnoRus, 2020. 189 p.

2. Dmitriyev A. S., Kholkin D. O., Maslova M. A. Inzhenernyj vestnik Dona, 2021, №6. URL: ivdon.ru/ru/magazine/archive/n6y2021/7054/.

3. Korsunov N. I., Titov A. I. Nauchnyye vedomosti Belgorodskogo gosudarstvennogo universiteta. 2010. №7. pp. 171-175.

4. Shnayyer B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnyye teksty na yazyke Si [Applied cryptography. Protocols, algorithms, source texts in C]. M.: Triumf, 2002. 816 p.

5. Fomichyov V. M. Diskretnaya matematika i kriptologiya: Kurs lektsiy [Discrete mathematics and cryptology: A course of lectures]. M.: Dialog-MIFI, 2013. 397 p.

6. Singh S. The Code Book, Histoire des codes secrets. USA, New-York: Doubleday, 1999. 416 p.

7. Gatchenko N. A., Isayev A. S., Yakovlev A .D. Kriptograficheskaya zashchita informatsii [Cryptographic protection of information]. SPb: NIU ITMO, 2012. 142 p.

8. Kochladze Z., Gelashvili G. Computer Science and Telecommunications. 2017. №2. pp. 53-56.

9. Glod O. D., Setrakov V. V. Inzhenernyj vestnik Dona. 2018. №4. URL: ivdon.ru/ru/magazine/archive/n4y2018/5436/.

10. Panasenko S. Algoritmy shifrovaniya [Encryption algorithms]. SPb: BKHV-Peterburg, 2009. 576 p.