DOI 10.37882/2223–2966.2023.04–2.22

ШИФРОВАНИЕ В СРЕДЕ MS EXCEL ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ И ХРАНЕНИЯ ДАННЫХ

ENCRYPTION IN MS EXCEL ENVIRONMENT FOR SECURE DATA TRANSMISSION AND STORAGE

V. Mikhaelis
S. Mikhaelis

Summary. The paper provides an example of implementation of encryption algorithm based on Caesar and Vigenere ciphers as well as XOR operation in MS Excel 2019 spreadsheet environment, which has a number of features suitable for implementation of cryptographic transformation. The paper shows the use of standard MS Excel functions for message encryption and de-encryption.

Keywords: Caesar cipher, Vigenere cipher, cipher modification, XOR, MS Excel.

Михаэлис Владимир Вячеславович
Кандидат педагогических наук, доцент, ФГБОУ ВО «Иркутский государственный университет путей сообщения»
mvv_1967@mail.ru
Михаэлис Светлана Ивановна
Кандидат педагогических наук, доцент, ФГБОУ ВО «Иркутский государственный университет путей сообщения»
msibgu@rambler.ru

Аннотация. В статье приведен пример реализации алгоритма шифрования на основе шифров Цезаря и Виженера, а также операции XOR в среде табличного процессора MS Excel 2019, который имеет ряд особенностей, подходящих для реализации криптографических преобразований. Показано использование стандартных функций MS Excel для шифрования и расшифрования сообщений.

Ключевые слова: шифр Цезаря, шифр Виженера, модификация шифра, XOR, MS Excel.

В настоящее время такие исторические шифры, как шифры Цезаря и Виженера, не используются в чистом виде, но их рациональные идеи применяются в ряде современных криптографических алгоритмов. Циклический сдвиг в алфавитном порядке в кодах Цезаря и Виженера представляет собой модульное суммирование, которое используется в современных симметричных кодах. Было выполнено много работ по усилению классических шифров, значительно укрепивших их. Однако по-прежнему существует потребность в улучшении их криптостойкости, поскольку преимущества криптографии заключаются в том, что она предлагает в том числе личную конфиденциальность (в англоязычных источниках обозначается термином individual privacy).

Принимая во внимание простоту этих шифров, как российские, так и зарубежные исследователи приходят к различным вариантам их модификации [1–4], и совместное использование этих алгоритмов позволяет повысить уровень защиты. Также существуют различные средства реализации криптографических алгоритмов (C++, Java, Python и др.), однако MS Excel — наиболее доступный инструмент для решения таких задач, позволяющий наглядно продемонстрировать весь процесс шифрования или криптоанализа информации [8, 10, 11, 12].

Основной целью статьи является разработка гибрида шифров Цезаря и Виженера, который может предотвратить несанкционированный доступ к конфиденциальной информации или ее модификацию, и реализация алгоритма шифрования с использованием Excel.

Опишем процесс шифрования, используемый для достижения целей и задач исследования.

Важное значение имеет длина ключа, т.к. она является основной характеристикой криптостойкости. Для симметричного шифрования надежным считается ключ длиной от 128 бит. В нашем примере используется ключ меньшей длины для удобства восприятия представленного материала. В Excel не составляет труда увеличить длину ключа различными способами.

Вначале выполняется подготовительный этап, заключающийся в удалении из исходного текста пробелов, знаков препинания с использованием функции ПОДСТАВИТЬ (рис. 1) .

Шаг алгоритма	Пояснение	Результат
подготовительный	открытый текст	кодсимвола
1	ключ_1	7
2	ключ_2	семь
3	текст_1	схкшпуихтж
4	ключ_2_1	шлуг
5	текст_2	йбюызяьшкт

Рис. 1. Шаги 1–5 алгоритма

Шаг алгоритма	Пояснение	Результат					
6	побуквенное разбиение текста_2	й	б	ю	ы	з	я
7	двоичная форма букв текста_2	11101001	11100001	11111110	11111011	11100111	11111111
	двоичная форма ключа_1	110111					
8	посимвольное разбиение ключа_1	0					
		0					
		1					
		1					
		0					
		1					
		1					
		1					
9	посимвольное разбиение текста_2	1	1	1	1	1	1
		1	1	1	1	1	1
		1	1	1	1	1	1
		0	0	1	1	0	1
		1	0	1	1	0	1
		0	0	1	0	1	1
		0	0	1	1	1	1
		1	1	0	1	1	1

Рис. 2. Шаги 6–9 алгоритма

Шаг алгоритма	Пояснение	Результат					
10, 11	XOR	1	0	1	0	1	0
		1	0	1	0	1	0
		0	1	0	1	0	1
		1	1	1	0	1	1
		1	0	0	1	0	0
		1	1	1	0	0	1
		1	1	1	0	1	0
		0	1	0	0	1	0
12	объединение	11011110	00110111	11010110	00101000	11010011	00110100
13	десятичная форма	222	55	214	40	211	52
14	символьное представление	Ю	7	Ц	(	У	4
15	объединение	Ю7Ц(У4Л7П%					

Рис. 3. Шаги 10–15 алгоритма

Для реализации алгоритма шифрования в таблицах Excel необходимы следующие шаги:

1. Берется произвольный числовой *ключ_1* длиной в зависимости от мощности алфавита, для чего используется функция СЛУЧМЕЖДУ.
2. Числовой *ключ_1* переводится в буквенный эквивалент. Таким образом получаем *ключ_2* по методике, описанной в работе [14] .
3. *Ключом_1* шифруется методом Цезаря открытый текст, в результате чего получается *текст_1* по методике, описанной в работах [8, 10].
4. *Ключом_1* шифруется методом Цезаря *ключ_2_1*.
5. *Ключом_2_1* шифруется *текст_1* методом Виженера, в результате чего получается *текст_2* (рис.1) .
6. *Текст_2* разбивается побуквенно с размещением каждой буквы в отдельные ячейки (функции СТОЛБЕЦ, ПСТР) .
7. Производится перевод *текста_2* и *ключа_1* в код ASCII (функция КОДСИМВ), затем перевод полученного результата в двоичную форму (функция ДЕС.В.ДВ) .
8. Применяется посимвольное разбиение *ключа_1* (функции СТОЛБЕЦ, ПСТР) .
9. Применяется посимвольное разбиение *текста_2* (функции СТОЛБЕЦ, ПСТР) (часть таблицы представлена на рис.2) .
10. Применяется операция XOR к *ключу_1* и первой букве *текста_2* (функции ИСКЛИЛИ, ЕСЛИ) .
11. Применяется операция XOR к результату п. 10 и второй букве *текста_2*, затем результат к третьей и т.д. Таким образом получили блок цифр.
12. Ячейки с полученными на предыдущем шаге цифрами объединяются (функция СЦЕПИТЬ), в результате чего получается двоичное представление каждой буквы шифротекста.
13. Полученные двоичные числа преобразуются в десятичные числа (функция ДВ.В.ДЕС) .
14. Десятичные числа переводятся в буквы (функция СИМВОЛ).
15. Буквы, разнесенные по ячейкам, сцепляются для получения шифротекста (функция СЦЕПИТЬ) (часть таблицы представлена на рис. 3) .

Таким образом, выполнив описанные выше шаги, был получен шифротекст. Процесс дешифрования происходит в обратном порядке с использованием тех же функций.

В заключение отметим, что в определенные исторические периоды представленные классические алгоритмы использовались достаточно успешно. Появление новых научных инструментов (в том числе развитие вычислительной техники) позволило создать методы их расшифровки в разумные сроки.

Анализ недостатков некриптостойких шифров помогает создавать новые, более мощные средства криптографической защиты. На смену некриптостойким алгоритмам приходят новые.

Как показано, MS Excel предоставляет возможности реализации методов шифрования как известных алгоритмов, так и их модификаций. Представленная работа может быть использована для обучения и проведения экспериментов в криптографии. Дальнейшим развитием данной работы будет являться изучение возможностей криптоанализа средствами MS Excel. Представленная работа может быть использована для обучения и проведения экспериментов в криптографии. Дальнейшим развитием данной работы будет являться изучение возможностей криптоанализа средствами MS Excel.

ЛИТЕРАТУРА

1. Omolara O.E., Oludare A.I., Abdulahi S.E. Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication // Computer Engineering and Intelligent Systems.— 2014.— Vol. 5.— No. 5.
2. Purnama B. A New Modified Caesar Cipher Cryptography Method with LegibleCiphertext From a Message to Be Encrypted / B. Purnama, H. Rohayani// Procedia Computer Science.— 2015.— № 59.— P. 195–204.
3. Siregar S.J. Application and Manual Encryption Process with The Combination Algorithm of One Time Padand Vigenere Cipher / S.J. Siregar, M. Zarlis, Z. Situmorang // Journal of Physics: Conference Series.— 2020.— Vol. 1641. International Conference on Advanced Information Scientific Development (ICAISD) 2020 6–7 August 2020, West Java, Indonesia.
4. Tan C.M.S. A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher / C. M.S. Tan, G.P. Arada, A.C. Abad, E.R. Magsino // Journal of Physics: Conference Series.— 2021.— Vol. 1997. Asian Conference on Intelligent Computing and Data Sciences (ACIDS) 2021 24–25 May 2021, Perlis, Malaysia.
5. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения.— М.: Стандартинформ, 2008.
6. Зеленорицкая А.В. Модификации поточного шифра RC4 / А.В. Зеленорицкая, М.А. Иванов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки.— 2019.— № 3–2.— С. 56–61.
7. Михайлец А.Н. Углубленное изучение алгоритмов шифрования с использованием базового программного обеспечения / А.Н. Михайлец, Д.Н. Михайлец, А.А. Калинин // I-methods.— 2021.— Т. 13.— № 2.
8. Михайлов Д. Криптография и криптоанализ с MS Excel / Д. Михайлов // Математика и информатика.— 2022.— Vol. 65.— No 1.— P. 53–71.
9. Михаэлис В.В. Защита беспроводных сетей / В.В. Михаэлис, С.И. Михаэлис // Информационные технологии и проблемы математического моделирования сложных систем.— 2015.— № 14.— С. 4–10.
10. Паршукова Н.Б. Криптографические алгоритмы в среде электронных таблиц /Н.Б. Паршукова // Информатика в школе.— 2019.— № 8 (151) .— С. 51–55.
11. Сдвижков О.А. Основы математической логики и криптографии. Практикум в Excel: уч. пос. для направлений бакалавриата «Математика и компьютерные науки» / О.А. Сдвижков.— М.: КноРус, 2022.— 358 с.
12. Сдвижков О.А. Применение Excel в криптографии / О.А. Сдвижков, Н.П. Мацнев // Международный научно-исследовательский журнал.— 2020.— № 7–1 (97) .— С. 87–95.
13. Справка по функциям Excel [Электронный ресурс] .— URL: https://msoffice-prowork.com/ref/excel/excelfunc/ (дата обращения: 1.02.2023) .
14. Числа прописью — Эффективнее! Bill K.xlsx [Электронный ресурс] .— URL: https://drive.google.com/file/d/1h8DYksxslB8zQ0dgi2gL–LG_zr2iKzDy/view (дата обращения: 1.02.2023) .
15. Шурховецкий Г.Н. Криптостойкость алгоритмов шифрования / Г.Н. Шурховецкий // Молодая наука Сибири.— 2018.— № 2 (2) .— С. 84–91.