DOI: 10.17805/ggz.2021.5.2

Модификация исторического шифра «двойной квадрат» Уитстона в учебном процессе как составляющая ответа на глобальные вызовы информатизации*

М. В. Шептунов
Российский государственный гуманитарный университет;
Московский гуманитарный университет;
Московский государственный лингвистический университет

В статье один из вариантов модернизации давно известного исторического шифра «двойной квадрат» Чарльза Уитстона 1854 г. предложен в качестве составляющей ответа высшего образования в сфере международной информационной безопасности, в том числе развития социотехнических систем. Он строится на операциях «max» и «min», введение которых в шифр направлено на повышение стойкости криптографического преобразования благодаря управляемым перестановкам, которые осуществляются по отличающемуся принципу подстановкам.

Ключевые слова: *шифр сложной замены; управляемые подстановки; управляемые перестановки; шифр Уитстона; шифр двойного квадрата; шифрование; эволюционный процесс развития; эволюционный процесс стандартизации; информационные риски социотехнических систем*

Modification of Long-Standing Wheatstone's Two-Square Cipher in the Educational Process as a Part of the Response to Global Challenges of Informatization

M. V. Sheptunov
Russian State University for the Humanities;
Moscow University for the Humanities;
Moscow State Linguistic University

The author proposes one of the variants of modernization of the well-known traditional two-square cipher invented by Charles Wheatstone in 1854 as a component of the response of higher education in the field of international information security, including the development of sociotechnical systems. It is based on the

* Статья подготовлена на основе доклада, представленного на XVII Международной научной конференции «Высшее образование для XXI века. Ответы на глобальные вызовы» (25–27 ноября 2021 г., Московский гуманитарный университет).

max and min operations. Their introduction into the cipher is aimed at increasing the strength of the cryptographic transformation due to controlled permutations that are carried out on a different principle of substitutions.

Keywords: complex substitution cipher; controlled substitutions; controlled permutations; Wheatstone's cipher; two-square cipher; evolutionary process of development; evolutionary process of standardization; information risks of socio-otechnical systems

ВВЕДЕНИЕ

Одной из проблем XXI в. является устойчивость международной информационной безопасности к глобальным вызовам как для Российской Федерации, так и для мира в целом. Приоритетную роль в ее решении играет высшее образование, в том числе в ракурсе развития умений выпускников защищать конфиденциальную информацию различными доступными и допустимыми способами и средствами.

ШИФР УИТСТОНА: НОВЫЕ ВОЗМОЖНОСТИ МОДЕРНИЗАЦИИ

Давно известен и хорошо зарекомендовал себя в различные исторические периоды шифр «двойной квадрат» англичанина Чарльза Уитстона, использовавшийся Германией даже в годы Второй мировой войны (Романец, Тимофеев, Шаньгин, 1999). Однако в упомянутые периоды еще отсутствовали достаточно мощные ЭВМ, задействование которых могло бы существенно упростить и ускорить взлом данного шифра.

Также известно, что одним из подходов к повышению стойкости криптографического преобразования — особенно к частотному криптоанализу — является использование, вообще говоря, в произвольном шифре управляемых подстановок и перестановок (Молдовян, А., Молдовян, Н., Советов, 2000). Для шифра «двойной квадрат» 1854 г., относящегося к шифрам сложной замены (подстановки), не обнаружено (насколько известно автору на дату написания статьи) предложенного ранее усовершенствования, в точности соответствующего предмету данной работы, строящегося на введении определенным образом в известный шифр операций «max» и «min», на основе которых возможны варианты рассматриваемой модификации.

Известно и то, что с целью затруднения анализа алгоритма шифрования можно использовать различные операции преобразований, зависящие от преобразуемых данных, причем в качестве таковых могут применяться как операция подстановки, так и операция перестановки. Управляемые подстановки могут быть заданы (в общем случае) как множество «различных таблиц подстановок, каждой из которых присвоен порядковый номер» (Молдовян, А., Молдовян, Н., 1999: 7). Относительно же управляемой операции перестанов-

ки отметим, что обычно ее использование для преобразования подблоков предполагает, что один из них используется как управляющий (Молдовян, А., Молдовян, Н., Советов, 2000).

Цель статьи — показать преимущественно для студентов и абитуриентов уровня магистратуры некоторые возможности модификации шифра «двойной квадрат» Уитстона 1854 г., предложив отдельные, но далеко не единственно возможные пути либо приемы его модернизации.

Отметим, что еще рано говорить не только о рабочих качествах предложенного в статье А. Б. Симона подхода (Симон, 2020), но и возможностях продемонстрированного, описанного и модифицированного в настоящей работе шифра. Однако и этот подход к задаче может оказаться интересным. При этом укажем, что в отличие от А. Б. Симона (там же) мы вовсе не предполагаем отказываться от таблицы замен.

Опираясь на раскрытие сущности исходного шифра «двойной квадрат» в работе «Защита информации в компьютерных системах и сетях», поясним процедуру криптографического преобразования усовершенствованным шифром на приведенном в ней примере (Романец, Тимофеев, Шаньгин, 1999).

Проясним на указанном примере случай шифрования блоков той же размерности (биграмм), задействуя управляемые подстановки и перестановки на основе операций «max» и / или «min». Предварительно сформируем составную таблицу 1, как бы объединяющую, но при этом также и обособляющую ее левую половину как таблицу I и правую половину как таблицу II. Как и в оригинальном шифре Уитстона, в рассматриваемом случае усовершенствования исходное сообщение разбивают на биграммы, каждая из которых шифруется отдельно. Первый символ биграммы отыскиваем в левой половине таблицы 1, т. е. в таблице I, а 2-й символ — в правой половине таблицы 1, т. е. в таблице II. Затем, действуя как в исходном шифре, мысленно строят прямоугольник так, чтобы символы биграммы лежали в его противоположных вершинах; тогда другие две вершины этого прямоугольника представляют собой символы биграммы шифртекста.

После этого «достраивают» прямоугольник до большего его размера при наличии достаточного пространства в рамках таблицы, увеличив высоту прямоугольника на то же количество строк, какое имеется между верхней и нижней образующими его строками. (Отметим, что если преобразуемый прямоугольник состоит из более чем одной строки (вполне возможная ситуация), то число строк получаемого таким образом вновь прямоугольника всегда должно быть нечетным, в чем нетрудно убедиться непосредственно.) Такое увеличение высоты прямоугольника выполняют в направлении (вверх либо вниз), в котором для этого достаточно пространства в пределах высоты таблицы. Если пространства для указанного «допостроения» достаточно в

обоих направлениях, то выбирают то из них, при котором возможно избежать неполного зашифрования (либо полного незашифрования) биграммы; если же в любом из двух направлений при «допостроении» биграмма шифруется полностью отличающимися (от соответствующей биграммы открытого текста) символами, то выбор направления увеличения высоты прямоугольника (по сути управляемую подстановку) осуществляют для определенности в сторону увеличения координаты по высоте. В любом случае в расчет принимаются координаты интересующих символов в таблице 1; в рамках нее координаты обозначены арабскими цифрами. Если же для упомянутого выше «допостроения» в рамках таблицы 1 по высоте пространства недостаточно, то для соответствующей биграммы данное увеличение прямоугольника не производят, оставляя его на данном этапе (в ракурсе управляемой подстановки) неизменным, производя только для таких не подвергшихся управляемой подстановке биграмм, управляемые перестановки внутри каждой из этих биграмм — что будет показано далее.

Для ситуации, когда оба символа биграммы открытого сообщения расположены в одной и той же строке, символы шифртекста — как и в первичном варианте шифра Уитстона — берут и в усовершенствованном варианте из этой же строки. А именно: 1-й символ биграммы шифртекста берут из левой половины таблицы 1 (т. е. таблицы I) в столбце, соответствующем второму символу биграммы сообщения, а второй символ биграммы шифртекста считывают из правой половины таблицы 1 (т. е. таблицы II) в столбце, соответствующем первому символу биграммы сообщения. Поэтому, например, рассмотренная Ю. В. Романцом, П. А. Тимофеевым и В. Ф. Шаньгиным биграмма «ТО» сообщения «ПР ИЛ ЕТ АЮ _Ш ЕС ТО ГО», разбитого на биграммы, преобразуется в биграмму шифртекста «БЖ». Пусть, например, как и в их работе, шифруется биграмма исходного текста ИЛ (Романец, Тимофеев, Шаньгин, 1999). Отмечаем (мысленно или в таблице), что символ И находится в первом столбце и во второй строке левой половины таблицы 1 (т. е. табл. I), а символ Л расположен в пятом столбце и четвертой строке правой половины таблицы 1 (т. е. табл. II). Это указывает на то, что первый («недостроенный») прямоугольник образован второй и четвертой строками, а также первым столбцом левой половины таблицы 1 (т. е. табл. I) и пятым столбцом правой половины табл. 1 (т. е. табл. II). Поэтому входящим в биграмму шифртекста является символ О, расположенный в десятом столбце (т. е. в пятом столбце правой половины таблицы 1 — табл. II) и во второй строке, и также непременно символ В, расположенный в первом столбце левой половины таблицы 1 (т. е. табл. I) и четвертой строке. Таким образом вырисовывается сначала биграмма шифртекста ОВ.

Таблица 1 (табл. I — левая и табл. II — правая)
Table 1 (table I — the left one and table II — the right one)

	I	II	III	IV	V	I	II	III	IV	V	
1	Ж	Щ	Н	Ю	Р	И	Ч	Г	Я	Т	1
2	И	Т	Ь	Ц	Б	,	Ж	Ь	М	О	2
3	Я	М	Е	.	С	З	Ю	Р	В	Щ	3
4	В	Ы	П	Ч	_	Ц	:	П	Е	Л	4
5	:	Д	У	О	К	Ъ	А	Н	.	Х	5
6	З	Э	Ф	Г	Ш	Э	К	С	Ш	Д	6
7	Х	А	,	Л	Ъ	Б	Ф	У	Ы	_	7
	1	2	3	4	5	6	7	8	9	10	

Суть управляемой именно подстановки в предлагаемом варианте усовершенствования состоит в том, что упомянутое «допостроение» прямоугольника зависит от преобразуемых данных в виде биграмм, выполняясь избирательно, в зависимости от наличия либо отсутствия достаточного для него дополнительного пространства по высоте в рамках таблицы, причем соответствующий символ биграммы из модифицированного прямоугольника используется лишь при его несовпадении с таким же символом биграммы открытого текста. В случае же управляемых именно перестановок применяются (в данном усовершенствовании) операции «max» и «min».

Обозначим (в общем случае) $\alpha(x_1; y_1)$ — 1-й символ биграммы открытого текста (здесь и далее обе координаты соответствующего символа подразумеваются именно арабскими цифрами, также фигурирующими в табл. 1), $\beta(x_2, y_2)$ — 2-й символ биграммы открытого текста с соответствующими координатами, $\alpha'\left(x_1'; y_1'\right)$ — 1-й символ биграммы шифртекста с соответствующими координатами, $\beta'\left(x_2'; y_2'\right)$ — 2-й символ биграммы шифртекста с соответствующими координатами, Δh — разность между номерами верхней и нижней граничных строк исходного (меньшего) прямоугольника, ΔH — разность между номерами верхней и нижней граничных строк большего «допостроенного» прямоугольника, $\alpha''\left(x_1''; y_1''\right)$ и $\beta''\left(x_2''; y_2''\right)$ — 1-й и 2-й символы биграммы шифртекста с соответствующими координатами, полученными при формировании прямоугольника в предлагаемом усовершенствовании шифра.

К примеру, для вышеупомянутой биграммы ИЛ открытого текста, которой соответствует биграмма ОВ шифртекста в первоначальном варианте шифра Уитстона, имеем $\Delta h = 2$, $\Delta H = 4$, и именно при подстановке в резуль-

тате предлагаемого усовершенствования получается биграмма ДВ шифртекста.

Если же, например, необходимо зашифровать биграмму АЮ, где $A(2;7)=\alpha(x_1;y_1)$, $Ю(7;3)=\beta(x_2;y_2)$, то действуют так: поскольку видно, что недостаточно (дополнительного) пространства для модифицированного «достраиваемого» прямоугольника, используют только полученную при помощи подстановки из первоначально полученного прямоугольника биграмму шифртекста, но затем применяют *управляемую перестановку*, задействуя *условие*: если $\max\left(y_1^{'},y_2^{'}\right)=y_1^{'}$, то $\alpha^{'}\overset{\mapsto\downarrow}{\Uparrow}\beta^{'}$, т. е. тогда $\alpha^{''}\equiv\beta^{'}$ и $\beta^{''}\equiv\alpha^{'}$, $y_1^{''}=y_2^{'}$ и $y_2^{''}=y_1^{'}$.

Поэтому для полученной сначала конкретной биграммы шифртекста, например, ФМ, где $\Phi(3;6)\equiv\alpha^{'}\left(x_1^{'};y_1^{'}\right)$, $M(9;2)\equiv\beta^{'}\left(x_2^{'};y_2^{'}\right)$, за счет управляемой перестановки, так как $\max(6;2)=6\equiv y_1^{'}$, получается биграмма МФ. В плане же именно управляемых подстановок важно, что 1-й (2-й) символ вновь образованной («допостроением» прямоугольника) биграммы шифртекста, лежащий в точке пересечения двух «половинок» большего прямоугольника должен быть также первым (вторым) символом биграммы, сформированной по первоначальному шифру Уитстона.

Таким образом, вырисовывается следующий результат при предлагаемом варианте:

сообщение:	ПР	ИЛ	ЕТ	АЮ	_Ш	ЕС	ТО	ГО
шифртекст:	ЬЕ	ДВ	ЩУ	МФ	БЕ	РФ	БЖ	ЦД

Для сравнения обратим внимание, что для первичного варианта шифра Уитстона для того же открытого текста имеют место:

сообщение:	ПР	ИЛ	ЕТ	АЮ	_Ш	ЕС	ТО	ГО
шифртекст:	ПЕ	ОВ	ЩН	ФМ	ЕШ	РФ	БЖ	ДЦ

При сравнении данного результата криптографического преобразования из книги «Защита информации в компьютерных системах и сетях» (Романец, Тимофеев, Шаньгин, 1999) с полученным в данной статье видно (глядя в данном случае на первую и пятую биграммы), что при предлагаемом усовершенствовании шифра достижимо большее количество несовпадающих символов между открытым сообщением и шифртекстом.

Отметим, что при расшифровке считывание начинают с первого символа биграмм шифртекста в правой половине таблицы 1 (т. е. табл. II). Если обнаруживают, что недостаточно по высоте пространства в рамках табл. 1 для «допостроения» прямоугольника и для расшифровки соответствующей биграммы шифртекста, и при этом для координат ее символов $\min\left(y_1^{''},y_2^{''}\right)=y_1^{''}$, то, как в первоначальном шифре Уитстона, отыскивают соответствующую ей биграмму шифртекста, причем при выполнении данного соотношения пред-

варительно переставляют местами символы биграммы, а после этой перестановки действуют, как в первоначальном шифре Уитстона. При расшифровке именно при подстановке «допостроение» прямоугольника ведут в обратном направлении (уменьшения координаты по высоте), но при необходимости с его корректировкой — при соответствующем расположении совпадающих (его) символов(а) шифртекста и сообщения в данной биграмме.

ЗАКЛЮЧЕНИЕ

Предложенный вариант видится более выигрышным, хотя строгие оценки стойкости здесь рассмотренного еще предстоит получить, что могло бы послужить темой отдельного исследования. Заметим, однако, что и для сильно отличающейся модификации шифра «двойной квадрат» Уитстона, описанной в статье А. Б. Симона (Симон, 2020), такие оценки еще не были получены.

Примечательно также, что и после революционного изобретения в конце 1970-х гг. двухключевых криптосистем с открытым ключом имеют место, как отмечают исследователи, инновационные принципы управляемых операций для одноключевых криптосистем (Молдовян А., Молдовян Н., Советов, 2000), а в разносторонне аудируемых социотехнических системах обработки дискретных данных идет и эволюционный процесс развития и стандартизации, в том числе и в комплексной защите информации. Цель затруднения криптологического анализа алгоритма шифрования, т. е. управление эффективностью (в том числе экономической — в случае проецирования на современные криптосистемы) процесса работы криптоаналитиков, информационными рисками социотехнических систем, видится достижимой даже для исторических шифров (по крайней мере, схожих с шифром «двойной квадрат»). И это видится актуальным в ракурсе глобальных вызовов XXI в. и формирования ответа на них.

Отметим .что пользователи для большей защищенности могут менять местами (в том числе периодически) вертикальную координату с горизонтальной согласно предварительной договоренности между ними. При этом «в плане обеспечения помехоустойчивой передачи сообщений эффективным является применение ортогональных сигналов, представляющих частный случай наиболее помехоустойчивых кодов — кодов с ортогональными признаками» (Афонин, 2008: 166; см. также: Макаров, Нечаев, 2011).

Основная часть работы выполнена автором в Финансовом университете после аттестации в должности доцента и продолжена им, будучи слушателем курсов повышения квалификации НИУ «Высшая школа экономики», в той же должности в ФГБОУ ВО «Российский государственный гуманитарный университет», работая по совместительству в ФГБОУ ВО

«Московский государственный лингвистический университет» и АНО ВО «Московский гуманитарный университет».

СПИСОК ЛИТЕРАТУРЫ

Афонин, В. Н. (2008) Повышение достоверности обработки информации в информационно-телекоммуникационных системах с использованием специальных функций преобразования сигналов // Информатизация и информационная безопасность правоохранительных органов : XVII Международная научная конференция, 20–21 мая 2008 г. : сборник трудов / [редкол.: В. В. Гордиенко и др.]. М. : Акад. упр. МВД России. 523 с. С. 163–167.

Макаров, В. Ф., Нечаев, Д. Ю. (2011) Методы защиты информационной инфраструктуры экономических систем. М. : Изд-во Российского гос. торгово-экономического ун-та. 195 с.

Молдовян, А. А., Молдовян, Н. А. (1999) Способ криптографического преобразования блоков цифровых данных : патент на изобретение № RU 2140709 C1, 27.10.1999. Заявка 97120853/09 от 16.12.1997.

Молдовян, А. А., Молдовян, Н. А., Советов, Б. Я. (2000) Криптография. СПб. : Лань. 224 с.

Романец, Ю. В., Тимофеев, П. А., Шаньгин, В. Ф. (1999) Защита информации в компьютерных системах и сетях. М. : Радио и связь. 328 с.

Симон, А. Б. (2020) Новое о шифре Уитстона // Вопросы защиты информации. № 2 (129). С. 8–13.

Дата поступления: 29.11.2021 г.

REFERENCES

Afonin, V. N. (2008) Povyshenie dostovernosti obrabotki informatsii v informatsionno-telekommunikatsionnykh sistemakh s ispol'zovaniem spetsial'nykh funktsii preobrazovaniia signalov [Improving the reliability of information processing in information and telecommunication systems using special signal conversion functions]. In: *Informatizatsiia i informatsionnaia bezopasnost' pravookhranitel'nykh organov [Informatization and information security of law enforcement agencies]* : The 17th International scientific conference, May 20–21, 2008 : Proceedings / editorial board: V. V. Gordienko et al. Moscow : Administration Academy of the Ministry of Internal Affairs of Russia. 523 p. P. 163–167. (In Russ.).

Makarov, V. F. and Nechaev, D. Yu. (2011) *Metody zashchity informatsionnoi infrastruktury ekonomicheskikh system [Methods of protecting the information infrastructure of economic systems].* Moscow : Russian State University of Trade and Economics Publ. 195 p. (In Russ.).

Moldovian, A. A. and Moldovian, N. A. (1999) *Sposob kriptograficheskogo preobrazovaniia blokov tsifrovykh dannykh [A method for cryptographic transformation of digital data blocks]* : A patent of invention, no. RU 2140709 C1, 27.10.1999. Application for an invention 97120853/09 of 16.12.1997. (In Russ.).

Moldovian, A. A., Moldovian, N. A. and Sovetov, B. Ya. (2000) *Kriptografiia [Cryptography].* St. Petersburg : Lan' Publ. 224 p. (In Russ.).

Romanets, Yu. V., Timofeev, P. A. and Shangin, V. F. (1999) *Zashchita informatsii v komp'iuternykh sistemakh i setiakh [Information protection in computer systems and networks].* Moscow : Radio i sviaz' Publ. 328 p. (In Russ.).

Simon, A. B. (2020) Novoe o shifre Uitstona [New about the Wheatstone cipher]. *Voprosy zashchity in-formatsii*, no. 2 (129), pp. 8–13. (In Russ.).

Submission date: 29.11.2021.

Шептунов Максим Валерьевич — кандидат технических наук, доцент; доцент кафедры комплексной защиты информации Российского государственного гуманитарного университета; доцент кафедры прикладной информатики Московского гуманитарного университета; доцент кафедры международной информационной безопасности Московского государственного лингвистического университета. Адрес: ГСП-3, 125993, Россия, г. Москва, Миусская пл., д. 6. Тел.: +7 (915) 297-22-75. Эл. адрес: triumf403@yandex.ru

SHEPTUNOV Maxim Valerievich, Candidate of Technical Sciences, Associate Professor, Department of Information Security, Russian State University for the Humanities; Associate Professor, Department of Applied Informatics, Moscow University for the Humanities; Associate Professor, Department of International Information Security, Moscow State Linguistic University. Postal address: 6 Miusskaya Sq., GSP-3, 125993 Moscow, Russian Federation. Tel.: +7 (915) 297-22-75. E-mail: triumf403@yandex.ru

SPIN-код РИНЦ: 8279-7422

Для цитирования:

Шептунов М. В. Модификация исторического шифра «двойной квадрат» Уитстона в учебном процессе как составляющая ответа на глобальные вызовы информатизации [Электронный ресурс] // Горизонты гуманитарного знания. 2021. № 5. С. 10–18. URL: https://journals.mosgu.ru/ggz/article/view/1550 (дата обращения: дд.мм.гггг). DOI: 10.17805/ggz.2021.5.2