УДК 004.056.55, 003.26.09

Н.Г. КАНАКИ, И.Л. АФОНИН, П.А. БУГАЁВ
ФГАОУ ВО «Севастопольский государственный университет»
Pasha_ba@mail.ru

СПОСОБ ШИФРОВАНИЯ СООБЩЕНИЙ

Предлагается способ шифрования сообщений, который имеет несколько ключей, применяемых одновременно, связанных между собою арифметическими операциями. Кроме того он имеет несомненные преимущества, по сравнению с известными способами шифрования, в результате применения арифметических операций вычитания между различными элементами различных ключей и одновременного использования различных ключей, известных только конфиденциальным корреспондентам. Даются практические рекомендации.

Ключевые слова: информация, шифрование, дешифрование, ключ, конфиденциальность.

N.G. KANAKI, I.L. AFONIN, P.A. BUGAYOV
Sevastopol State University
Pasha_ba@mail.ru

METHOD ENCRYPT MESSAGES

Annotation — Message encryption method is proposed, which has several keys used at the same time, interconnected arithmetic operations. Moreover, it has undoubted advantages compared with known methods of encryption, a result of subtraction arithmetic operations between the different elements of various keys and the simultaneous use of different keys known only sensitive reporters. Practical recommendations.

Keywords: information, encryption, decryption, key confidentiality.

Информация — одно из общин понятий, связанных с материей [1]. Информация существует в любом материальном объекте в виде многообразия его состояний и передаётся от объекта к субъекту в процессе их взаимодействия. Существование информации как объективного свойства материи логически вытекает из известных фундаментальных свойств материи: структурности, непрерывного изменения и взаимодействия материальных объектов. Множество состояний материальной системы и всех её подсистем представляет информацию о системе. Необходимость утаивать информацию о системе, скрывать содержание важных сообщений существует уже тысячи лет. В военном деле, где особенно важно утаивание своих действий от противника. И в повседневной, невоенной, жизни приходилось «прятать» содержание передаваемых «депеш». Обострившиеся в наше время проблемы безопасности мореплавания, в частности, пиратские нападения на беззащитные мирные суда, предъявляют новые требования к предохранению от несанкционированного проникновения в информацию, например: о цели движения судна, номенклатуре, количестве, цене товаров на борту. Люди искали все более и более сложные способы кодирования сообщений, поскольку простые способы кодировки декодируются с большей легкостью. Известен класс шифров, называемых шифрами перестановки, например, «Сцитала» — шифр, примененный во времена войн Спарты против Афин в V веке до нашей эры [1]. В том способе шифрования на специальный жезл, имеющий форму цилиндра, виток к витку, без просветов и нахлестов наматывалась узкая папирусная лента, а затем вдоль оси «сциталы» записывался открытый текст. Лента разматывалась, поперек ленты оставались в беспорядке записанные буквы, эту ленту отправляли адресату, который таким же образом наматывал ленту на такую же «сциталу» и читал сообщение вдоль оси «сциталы». Известен шифр Цезаря, где каждая из букв открытого текста заменялась третьей после неё буквой в алфавите, который считается написанным по кругу, т.е., после «Я» следует «А». Безопасность записанной информации определялась, в первую очередь, ключом, при этом, законные пользователи тайно обменивались ключами перед обменом шифрованными сообщениями. Если противник перехватывал криптограмму, не зная секретного ключа $K1$, то он пытался найти сообщение m, где $d = EK1(m)$. Поскольку алгоритм шифрования общеизвестен, то противник мог просто перебрать все возможные сообщения длины n, вычислить для каждого такого сообщения m_i криптограммы $d_i = Ek1(m_i)$ и сравнить d_i с d, то сообщение, для которого $d_i = d$ и будет искомым открытым текстом. Перебор будет выполнен за время, порядка $2nT(n)$, где $T(n)$ — время, требуемое для вычисления функции EK, от сообщений длины n. Если сообщения имеют длину порядка 1000 бит, то такой перебор неосуществим на практике ни на каких самых мощных компьютерах. Шифрами замены называют такие шифры, преобразования из которых приводят к замене каждого символа открытого сообщения на другие символы — шифрообозначения, совпадающие с порядком следования соответствующих им символов открытого сообщения. На день нынешний в мире насчитывается тысячи способов сокрытия сообщений. Проанализируем некоторые из них.

Код Морзе (азбука Морзе). Несмотря на свое название, код Морзе не является кодом — это шифр. Каждая буква алфавита, цифры от 0 до 9 и некоторые символы пунктуации заменены на последовательность коротких и длинных звуковых сигналов, которые часто называют «точка» — «•» и «тире» — «—». А становится «• —», Б становится «— • • •» и так далее (рис. 1). В отличие от большинства других шифров, код Морзе не используется для сокрытия сообщений.

Таблица 1

Азбука Морзе

А	● —	П	● — — ●	Ь	— ● ● —
Б	— ● ● ●	Р	● — ●	Ы	— ● — —
В	● — —	С	● ● ●	Й	● — — —
Г	— — ●	Т	—	Ъ	— — ● — —
Д	— ● ●	У	● ● —	1	● — — — —
Е	●	Ф	● ● — ●	2	● ● — — —
Ж	● ● ● —	Х	● ● ● ●	3	● ● ● — —
З	— — ● ●	Ц	— ● — ●	4	● ● ● ● —
И	● ●	Ч	— — —●	5	● ● ● ● ●
К	— ● — ●	Ш	— — — —	6	● ● ● ●
Л	● — ● ●	Щ	— —● —	7	— ● ● ●
М	— —	Э	● ● — ● ●	8	— — —● ●
Н	— ●	Ю	● ● — —	9	— — — — ●
О	— — —	Я	● — ● —	0	— — — — —

Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Этот метод является простой формой многоалфавитной замены. 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.

Шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому. Известный писатель и математик Чарльз Лютвидж Доджсон (Льюис Кэрролл) назвал шифр Виженера невзламываемым 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 Касиски 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. 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 действительно невозможно взломать.

	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

Рис. 1. Таблица Виженера

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

Предложенный способ шифрования сообщений, имеет несколько ключей, применяемых одновременно, связанных между собою арифметическими операциями. Кроме того он имеет несомненные преимущества, по сравнению с известной тысячью способов шифрования, в результате применения арифметических операций вычитания между различными элементами различных ключей и одновременного использования различных ключей, известных только конфиденциальным корреспондентам. При этом выполняют следующие технологические переходы, которые не применялись совместно при известных способах шифрования:

1) В качестве первого ключа шифра, конфиденциальные корреспонденты между собою заранее

согласовывают определённый текст, называемый, в дальнейшем, ключевым фрагментом шифра, например, С. Есенин, «Пороша», 1914:

А.) «Еду. Тихо. Слышны звоны под копытом на снегу, только серые вороны расшумелись на лугу. Заколдован невидимкой, дремлет лес под сказку сна, словно белою косынкой подвязалася сосна. Понагнулась, как старушка, оперлася на клюку, а над самою макушкой долбит дятел на суку. Скачет конь, простору много, валит снег и стелет шаль. Бесконечная дорога убегает лентой вдаль». [2] В отличие от шифра Виженера [1], в приведенном способе ключевой фрагмент шифра используют для арифметических операций, что снижает вероятность несанкционированного дешифрования.

2) Для введения противника в заблуждение, для изменения статистики появления в тексте слов определённой длины, для усложнения анализа частотности букв, вводим второй ключ, изменяя длину каждого слова в ключевом фрагменте шифра*,* нумеруя по порядку слова в нём:

1« **2**Еду **3**. **4**Тихо **5**. **6**Слышны **7**звоны **8**под **9**копытом **10**на **11**снегу **12**, **13**только **14**серые **15**вороны **16**расшумелись **17**на **18**лугу **19**. **20**Заколдован **21**невидимкой **22**, **23**дремлет **24**лес **25**под **26**сказку **27**сна **28**, **29**словно **30**белою **31**косынкой **32**подвязалася **33**сосна **34**. **35**Понагнулась **36**, **37**как **38**старушка **39**, **40**оперлася **41**на **42**клюку **43**, **44**а **45**над **46**самою **47**макушкой **48**долбит **49**дятел **50**на **51**суку **52**. **53**Скачет **54**конь **55**, **56**простору **57**много **58**, **59**валит **60**снег **61**и **62**стелет **63**шаль **64**. **65**Бесконечная **66**дорога **67**убегает **68**лентой **69**вдаль **70**. **71**»

3) Ключевой фрагмент шифра может состоять из любого количества знаков, причём, сложность дешифрования возрастает с увеличением этого количества. Если количество знаков в ключевом фрагменте шифра меньше, чем количество знаков в самом шифруемом конфиденциальном сообщении, то ключевой фрагмент шифра записывают «по кругу», т.е., после его конечного знака записывают вновь весь ключевой фрагмент шифра, и так делают несколько раз, покуда количество знаков записанного таким образом ключевого фрагмента шифра совпадёт с количеством знаков шифруемого сообщения, и это есть третий ключ шифра.

4) В качестве четвёртого ключа шифра, по предварительной договорённости между двумя конфиденциальными корреспондентами, в шифруемом сообщении буквы и знаки также нумеруют по порядку, приписывая, например, в конце каждого слова его порядковый номер, причём, нумерацию, для противодействия противнику, можно производить от последнего слова шифруемого текста к первому. Эта избыточность поможет проверить правильность расшифровки при санкционированном дешифровании и затруднит раскрытие шифра нежелательному читателю.

5) В качестве пятого ключа шифра, по предварительной договорённости между двумя конфиденциальными корреспондентами, в шифруемом, конфиденциальном сообщении буквы и знаки заменяют числами, по согласованному закону, в пределах, например, от 1 до 250: А=2, Б=1, В=94, Г=63, …, Э=31, Ю=133, Я=32, «точка»=74, «запятая»=35, «тире»=250, «двоеточие»=128, «восклицательный знак»=211, «пробел»=99, «точка с запятой»=40, «вопросительный знак»=141, «скобки»=206, «кавычки»=43, цифры: 1=144, 2=205, 3=246, 4=27, 5=8, 6=49, 7=150, 8=151, 9=52, 0=93 — в результате чего вместо шифруемого сообщения получают недетерминированную, на первый взгляд, но назначенную шифруемым конфиденциальным сообщением, последовательность чисел в пределах от 1 до 250;

6) В качестве шестого ключа шифра в заранее согласованном тексте, в ключевом фрагменте шифра по п.п. 1,2,3, все буквы и знаки также заменяют числами, но в пределах от 251 до 500, включительно, по другому согласованному закону, например: А=251, Б=255, В=256, Г=359, Д=358, … , Э=484, Ю=385, Я=286, «точка»=487, «запятая»=488, «тире»=489, «двоеточие»=290, «восклицательный знак»=291, «пробел»=392, «точка с запятой»=493, «вопросительный знак»=294, «скобки»=495, 1=306, 2=405, 3=304, 4=403, 5=322, 6=301, 7=500 8=499, 9=298,…, 0=500 — в результате чего вместо шифруемого сообщения получают, похожую на случайную, недетерминированную, последовательность чисел в пределах от 251 до 500;

7) Полученную по п.п. 1, 2, 3 и 6, первую последовательность чисел, соответствующую ключевому фрагменту шифра, записывают над второй последовательностью чисел, полученной по п.п. 4 и 5, и соответствующей шифруемому сообщению, затем вычитают из каждого верхнего числа нижнее число, поэлементно, при этом, в качестве седьмого ключа шифра, согласно предварительной договорённости между конфиденциальными корреспондентами, первую последовательность чисел, полученную по п.п. 1, 2, 3 и 6, располагают, относительно второй числовой последовательности, полученной, согласно п.п. 4 и 5, в соответствии с одним из заранее оговоренных вариантов, например: в обратном порядке, т.е., первое число первой последовательности чисел, полученной, согласно п.п. 1, 2, 3 и 6, и соответствующей ключевому фрагменту шифра, располагают над последним числом второй последовательности чисел, полученной, согласно п.п. 4 и 5, и соответствующей шифруемому сообщению, второе число первой последовательности чисел, полученной, согласно п.п. 1, 2, 3 и 6, располагают над предпоследним числом второй последовательности чисел, полученной, согласно п.п. 4 и 5, и так далее, последнее число первой последовательности чисел, полученной, согласно п.п. 1, 2, 3 и 6, располагают над первым числом второй последовательности чисел, полученной, согласно п.п. 4 и 5. Или все числа располагают со сдвигом на одну или несколько позиций по порядку — в результате вычитания получают третью последовательность чисел, в пределах от 1 до 500;

8) В качестве восьмого ключа шифра в полученной по п. 7 последовательности чисел каждое число, от 1 до 500, включительно, заменяют символом, взятым, например, из латинского, греческого алфавитов,

знаков языка иврит, иероглифов, например: 1=А, 2=Б, 3=В, 4=Г, …, 31=Э, 32=Ю, 33=Я, 34=Q, 35=W, 36=R, 37=Y, 38=U, 39=S;40=D; 41=F, 42=G;1=A, 2=Б, 3=В, 4=Г, …, 31=Э, 32=Ю, 33=Я, 34=Q, 35=W, 36=R, 37=Y, 38=U, 39=S, 40=D, 41=F, 42=G, 43=N, 44=V, 45=J, 46=L, 47=Z, 48=α, 49=β, 50=γ, 51=δ, 52=ω, 53=λ, 113=ש,…,470= ص, 500 = ؤ, причём, замену чисел на символы нескольких алфавитов заранее оговаривают между собой только конфиденциальные корреспонденты;

9) Полученную по п. 8 последовательность символов, взятых из разных алфавитов, отправляют открытым каналом связи от одного конфиденциального корреспондента к другому конфиденциальному корреспонденту, который, получив сообщение, преобразовывает, в обратном порядке, используя восьмой ключ шифра, символы нескольких алфавитов — в числа, согласно п. 8, получает при этом третью последовательность чисел, от 1 до 500, соответствующую п. 7, и являющуюся последовательностью чисел, каждое из которых является разностью от вычитания каждого числа, соответствующего каждому знаку шифруемого сообщения, из каждого числа, соответствующего ключевому фрагменту шифра;

10) Полученную по п. 9 третью последовательность чисел, соответствующую последовательности чисел, полученных по п. 7, записывают, в порядке, оговоренном седьмым ключом шифра, под второй последовательностью чисел, полученной по п.п. 3 и 6, соответствующей ключевому фрагменту шифра, и вычитают из каждого верхнего числа нижнее число, поэлементно, в результате вычитания получают четвёртую последовательность чисел, соответствующую первой последовательности чисел, представляющей шифруемое, конфиденциальное сообщение, по п. 5, в пределах от 1 до 250;

11) В полученной по п. 10 последовательности чисел, применяя шестой ключ, каждое число заменяют буквенным символом, согласно п. 4, в результате чего получают первоначальное, расшифрованное сообщение.

Таким образом, предложен новый подход к шифрованию текстов, который имеет несомненные преимущества, по сравнению с известной тысячью способов шифрования, в результате применения арифметических операций вычитания между различными элементами различных ключей и одновременного использования различных ключей, известных только конфиденциальным корреспондентам, обозначим эти ключи:

- в качестве первого ключа заложен ключевой фрагмент шифра**,** скрываемый от несанкционированного дешифровальщика в арифметических операциях вычитания чисел. При этом, для усложнения недопустимого дешифрования, можно взять несколько ключевых фрагментов шифра, например: А) обозначенный в п.п. 1 и 2; и, дополнительно, Б): *«В те дни, когда в садах Лицея я безмятежно процветал, читал охотно Апулея, а Цицерона не читал, в те дни в таинственных долинах, весной, при кликах лебединых, близ вод, сиявших в тишине, являться муза стала мне. Моя студенческая келья вдруг озарилась: муза в ней открыла мир младых затей, воспела детские веселья, и славу нашей старины, и сердца трепетные сны.»* [3];
- в качестве второго ключа шифра, в котором произведена нумерация слов в ключевом фрагменте шифра, причём, во втором ключевом фрагменте шифра, обозначенном здесь буквой **Б)**, нумерацию слов можно производить, например, от последнего знака ключевого фрагмента шифра к первому: **76**«**75**В **74**те **73**дни**72**, **71**когда **70**в **69**садах **68**Лицея **67**я **66**безмятежно **65**процветал**64**, **63**читал **62**охотно **61**Апулея**60**, **59**а **58**Цицерона **57**не **56**читал**55**, **54**в **53**те **52**дни **51**в **50**таинственных **49**долинах**48**, **47**весной**46**, **45**при **44**кликах **43**лебединых**42**, **41**близ **40**вод**39**, **38**сиявших **37**в **36**тишине**35**, **34**являться **33**муза **32**стала **31**мне**30**. **29**Моя **28**студенческая **27**келья **26**вдруг **25**озарилась**24**: **23**муза **22**в **21**ней **20**открыла **19**мир **18**младых **17**затей**16**, **15**воспела **14**детские **13**веселья**12**, **11**и **10**славу **9**нашей **8**старины**7**, **6**и **5**сердца **4**трепетные **3**сны **2**. **1**»;
- как третий ключ, производят запись ключевого фрагмента шифра в виде кольца, т.е., после завершающего знака ключевого фрагмента шифра записывают вновь весь ключевой фрагмент шифра, и так — до совпадения количества знаков ключевого фрагмента шифра и шифруемого конфиденциального сообщения;
- в качестве четвёртого ключа шифра, производят нумерацию слов в шифруемом сообщении;
- в соответствии с пятым ключом, производят, по согласованному только между конфиденциальными корреспондентами порядку, замены символов текста конфиденциального сообщения цифрами;
- в соответствии с шестым ключом, выбирают один из нескольких, заранее согласованных, порядков замены символов ключевого фрагмента шифра цифрами;
- в соответствии с седьмым ключом, конфиденциальные корреспонденты заранее оговаривают порядок вычитания каждого числа одной числовой последовательности, изображающей конфиденциальное сообщение, из каждого числа другой числовой последовательности, изображающей ключевой фрагмент шифра;
- в соответствии с восьмым ключом, конфиденциальные корреспонденты заранее согласовывают порядок замены результатов вычитания чисел символами, взятыми из нескольких алфавитов;
- девятым ключом в разработанном способе шифрования текстов, производят обратные преобразования, с одновременным применением восьми шифровальных ключей, каждый из которых подразумевает выбор одного варианта ключа из нескольких вариантов, оговоренных между конфиденциальными корреспондентами. Для усложнения дешифровки недопустимыми читателями конфиденциальные корреспонденты могут согласовать между собою несколько различных вариантов замен

знаков шифруемого сообщения и знаков ключевого фрагмента шифра и изменять их, согласно отдельной договорённости, от сообщения к сообщению, и даже внутри одного сообщения можно применять эти различные варианты, например: после 25-го знака использовать заранее согласованный ключевой фрагмент шифра, обозначенный выше как Б), потом после 57-го использовать заранее согласованный ключевой фрагмент шифра, обозначенный выше как А), после 114 — вновь Б) и т.д. — но не произвольно, а по взаимной договорённости.

Использование одновременно большого количества ключей, согласованных между конфиденциальными корреспондентами, а самое главное: применение арифметической операции вычитания чисел, изображающих шифруемое сообщение, из чисел, изображающих ключевой фрагмент шифра, делает для субъектов, не обладающих ключами, время несанкционированного дешифрования зашифрованного сообщения неприемлемо большим, стремящимся к бесконечности, а зашифрованное сообщение становится доступным только конфиденциальным корреспондентам, имеющим полные наборы ключей представленного в этой статье способа шифрования текстов. И этот факт существен, особенно в военном деле. Одинаковые слова шифруемого сообщения в приведенном способе изображены совершенно различными последовательностями чисел, являющихся результатами вычитаний чисел, представляющих собою ключевой фрагмент шифра и фрагмент конфиденциального сообщения, и это нейтрализует тесты Касиски и Фридмана [1]. Вследствие обозначений различными числами пробела между словами, (в шифруемом конфиденциальном сообщении — одним числом, а в ключевом фрагменте шифра — иным числом), полученные последовательности чисел становятся непрерывными, что не позволит, при несанкционированном дешифровании анализировать вероятности появления в тексте слов определенных длин.

Литература

1. Ященко, В. В. Введение в криптографию / Под общей редакцией В. В. Ященко. — М. : МЦНМО, 2000. — 386 с.

2. Есенин, С. Собрание сочинений в одной книге / С. Есенин. — Харьков, Белгород : Клуб семейного досуга, 2012. — 960с.

3. Пушкин, А. С. Сочинения. В 3-х томах. Т. 2. Поэмы ; Евгений Онегин; Драматические произведения / А. С. Пушкин — М. : Худож. Лит., 1986. — 527 с.

References

1. Jashhenko, V. V. Vvedenie v kriptografiju / Pod obshhej redakciej V. V. Jashhenko. — M. : MCNMO, 2000. — 386 s.

2. Esenin, S. Sobranie sochinenij v odnoj knige / S. Esenin. — Har'kov, Belgorod : Klub semejnogo dosuga, 2012. — 960 s.

3. Pushkin, A. S. Sochinenija. V 3-h tomah. T. 2. Pojemy; Evgenij Onegin ; Dramaticheskie proizvedenija / A. S. Pushkin — M. : Hudozh. Lit., 1986. — 527 s.

Рецензія/Peer review : 24.5.2016 р. Надрукована/Printed :27.6.2016 р.
Стаття рецензована редакційною колегією