ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ
әл-Фараби атындағы Қазақ ұлттық университетінің

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный университет
имени аль-Фараби

NEWS

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
al-Farabi Kazakh National University

SERIES
PHYSICO-MATHEMATICAL

1 (341)

JANUARY – MARCH 2022

PUBLISHED SINCE JANUARY 1963

PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

NAS RK is pleased to announce that News of NAS RK. Series physico-mathematical journal has been accepted for indexing in the Emerging Sources Citation Index, a new edition of Web of Science. Content in this index is under consideration by Clarivate Analytics to be accepted in the Science Citation Index Expanded, the Social Sciences Citation Index, and the Arts & Humanities Citation Index. The quality and depth of content Web of Science offers to researchers, authors, publishers, and institutions sets it apart from other research databases. The inclusion of News of NAS RK. Series of chemistry and technologies in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential content of chemical sciences to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы «ҚР ҰҒА Хабарлары. Физика және информатика сериясы» ғылыми журналының Web of Science-тің жаңаланған нұсқасы Emerging Sources Citation Index-те индекстелуге қабылданғанын хабарлайды. Бұл индекстелу барысында Clarivate Analytics компаниясы журналды одан әрі the Science Citation Index Expanded, the Social Sciences Citation Index және the Arts & Humanities Citation Index-ке қабылдау мәселесін қарастыруда. Webof Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын усынады. ҚР ҰҒА Хабарлары. Химия және технология сериясы Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді химиялық ғылымдар бойынша контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Известия НАН РК. Серия физика и информационные технологии» был принят для индексирования в Emerging Sources Citation Index, обновленной версии Web of Science. Содержание в этом индексировании находится в стадии рассмотрения компанией Clarivate Analytics для дальнейшего принятия журнала в the Science Citation Index Expanded, the Social Sciences Citation Index и the Arts & Humanities Citation Index. Web of Science предлагает качество и глубину контента для исследователей, авторов, издателей и учреждений. Включение Известия НАН РК в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному контенту по химическим наукам для нашего сообщества.

«ҚР ҰҒА Хабарлары. Физика-математикалық сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

«Известия НАН РК. Серия физика-математическая».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика и информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series physico-mathematical.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 1, Number 341 (2022), 26–33 https://doi.org/10.32014/2022.2518-1726.113

МРНТИ 81.93.29
УДК 004.056

Т.С. Байшоланов*, Ж.М. Алимжанова, Н. Байшолан, К.Е. Кубаев, К.С. Байшоланова

Казахский национальный университет имени аль-Фараби, Алматы, Казахстан.
E-mail: btstalgat@mail.ru

ОЦЕНКА СТОЙКОСТИ КРИПТОГРАФИЧЕСКИХ ШИФРОВ С ПОМОЩЬЮ АНАЛИЗА ШИФРТЕКСТОВ

Аннотация. В статье рассматривается один из критериев, влияющих на стойкость криптографических алгоритмов шифрования. Одним из основных условий устойчивости алгоритмов шифрования является равновероятное распределение шифртекста. Случайное распределение шифртекста не дает злоумышленнику определить какой-либо информации, применяемой для вскрытия шифртекста или ключа. Таким образом, применяя оценочные модели на предмет повышения уровня случайности шифртекста, повышается стойкость и самого криптографического алгоритма шифрования. На практике для определения меры случайности шифртекста используется различные тестовые статистические алгоритмы.

В данной работе для анализа случайности данных шифртекста применяются математические аппараты теории вероятностей и математической статистики: математическое ожидание, дисперсия и коэффициенты автокорреляции. Приведенные методы, в котором, вычисляя математическое ожидание, дисперсию и коэффициенты автокорреляции от шифртекстов дают определение случайности последовательностей данных шифртекста.

Применение этих способов для известных криптографических алгоритмов шифрования Шифра Виженера, Упрощенный алгоритм S-DES, Triple DES и AES показали, что полученные результаты действительно согласуется с ожидаемыми. Тем самым показано применяемость данного метода для установления случайности данных шифртекстов.

Метод можно использовать как вспомогательный для анализа стойкости алгоритмов шифрования, например, для исследования качество выхода зашифрованных текстов при разработке криптографических алгоритмов шифрования.

Математическое моделирование вероятностно-статистических алгоритмов для оценки стойкости криптографических алгоритмов шифрования, методом исследования уровня случайности шифртекста позволяет повысить аналитическую базу оценки стойкости криптографических шифров, а также позволяет разработать методику их тестирования.

Ключевые слова: математическое ожидание, дисперсия, коэффициенты автокорреляции, статистический тест, криптостойкость алгоритмов шифрования, тестирование псевдослучайных последовательностей, шифртекст.

Т.С. Байшоланов*, Ж.М. Алимжанова, Н. Байшолан, К.Е. Кубаев, К.С. Байшоланова

Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан.
E-mail: btstalgat@mail.ru

ШИФРМӘТІНДІ ТАЛДАУ АРҚЫЛЫ КРИПТОГРАФИЯЛЫҚ ШИФРЛАРДЫҢ ТҰРАҚТЫЛЫҒЫН БАҒАЛАУ

Аннотация. Мақалада криптографиялық шифрлау алгоритмдерінің тұрақтылығына әсер ететін критерийлердің бірі қарастырылады. Шифрлау объектілерінің тұрақтылығының негізгі

шарттарының бірі - шифрмәтіннің тең ықтималды таратылуы болуы. Шифрмәтіннің кездейсоқ тең ықтималды таратымды болуы шабуылдаушыға шифрмәтінді немесе кілтті ашу үшін пайдаланатын қандай да бір ақпаратты анықтауға мүмкіндік бермейді. Осылайша, шифрмәтіннің кездейсоқтық деңгейін жоғарылату үшін бағалау модельдерін қолдана отырып, криптографиялық шифрлау алгоритмінің тұрақтылығы артады. Іс жүзінде шифрмәтіннің кездейсоқтық өлшемін анықтау үшін әртүрлі статистикалық алгоритмдер қолданылады.

Бұл жұмыста шифрмәтін деректерінің кездейсоқтығына талдау жасау үшін ықтималдық теориясы мен математикалық статистиканың математикалық аппараттары қолданылады: математикалық болжам, дисперсия және автокорреляция коэффициенттері. Шифрмәтіндердің математикалық болжамын, дисперсиясын және автокорреляция коэффициенттерін есептеу арқылы шифрмәтіннің кездейсоқтығы анықталады.

Бұл әдістерді шифрлаудың белгілі криптографиялық алгоритмдеріне Виженер шифріне, S-DES, Triple DES және AES алгоритмдеріне қолдану нәтижелері күткеніміздей болып шықты. Осылайша, осы шифрмәтіндердің кездейсоқтығын анықтау үшін осы әдісті қолдану көрсетілген.

Бұл әдісті шифрлау алгоритмдерінің тұрақтылығына талдау жасау үшін көмекші ретінде пайдалануға болады, мысалы, криптографиялық шифрлау алгоритмдерін жасау кезінде шифрланған мәтіндердің сапасын зерттеу кезінде.

Шифрмәтіннің кездейсоқтық деңгейін зерттеу әдісімен криптографиялық шифрлау алгоритмдерінің тұрақтылығын бағалаудың ықтималдық-статистикалық алгоритмдерін математикалық модельдеу, криптографиялық шифрлардың тұрақтылығын бағалаудың аналитикалық базасын арттыруға, сонымен қатар оларды тестілеу әдістемесін жасауға мүмкіндік береді.

Түйін сөздер: математикалық болжам, дисперсия, автокорреляция коэффициенттері, статистикалық тест, шифрлау алгоритмдерінің криптографиялық тұрақтылығы, кездейсоқ тізбекті тестілеу, шифрмәтін.

T.S. Baisholanov*, Zh.M. Alimzhanova, N. Baisholan, K.E. Kubayev, K.S. Baisholanova

Al-Farabi Kazakh National University, Almaty, Kazakhstan.
E-mail: btstalgat@mail.ru

EVALUATION OF THE STRENGTH OF CRYPTOGRAPHIC CIPHERS USING CIPHERTEXT ANALYSIS

Abstract. This article discusses one of the criteria affecting to the strength of cryptographic encryption algorithms. One of the main conditions for the stability of encryption algorithms is an equally probable distribution of the ciphertext. The random distribution of the ciphertext does not allow the attacker to determine any information that can be used to open the ciphertext or key. Therefore, the cryptographic encryption algorithm increases automatically by applying evaluation models to increase the level of randomness of the encoded text. In practice, various statistical test algorithms are used to determine the measure of randomness of the ciphertext.

In this paper, mathematical tools of probability theory and mathematical statistics are used to analyse the randomness of ciphertext data: mathematical expectation, variance and autocorrelation coefficients. The given methods determine the randomness of encoded text data sequences by calculating the mathematical expectation, variance and autocorrelation coefficients from ciphertexts.

The use of these methods for the well-known cryptographic algorithms such as Vigener Cipher, the Simplified algorithm S-DES, Triple DES and AES showed that the results obtained are consistent with the expected ones. Accordingly, the applicability of this method to establish the randomness of ciphertext data is proven.

The method can be used as an auxiliary for analysing the strength of encryption algorithms. For instance, to study the quality of the output of encrypted texts in the development of cryptographic encryption algorithms.

Mathematical modelling of probabilistic-statistical algorithms for assessing the strength of cryptographic encryption algorithms, by studying the randomness of the ciphertext level allows to increase the analytical base for assessing the strength of cryptographic ciphers, and allows developing a methodology for testing them.

Key words: mathematical expectation, variance, autocorrelation coefficients, statistical test, cryptographic stability of encryption algorithms, pseudo-random sequence testing, ciphertext.

Введение. В условиях цифровой глобализации безопасность информационной системы и защита сетевых данных стало более актульным для любой сферы деятельности. Криптологическая наука, применяя различных криптографических методов и в том числе криптостойкого шифрования, вносит свой вклад для надежности защиты информации от криптоаналитических атак. Действительно, «современная криптография – соревнование методов шифрования и криптоанализа» [1], к тому же криптоаналитик на основе различных алгоритмов шифрования может атаковать различных стойких систем.

Возможности методов криптоанализа начиная с различных математических методов до вычислительных техники позволяет определить наличия и оценить уязвимости или ненадежности в криптосистемах.

На сегодняшний день существует различные виды криптоаналитических атак и продолжает расти их количество. С ростом криптоаналитических атак, соответственно, создаются методы их обнаружения и защиты.

Существуют различные способы криптоанализа алгоритмов шифрования целью которого является дешифрование шифрованной информаций без знания ключа. Одним из них является анализ зашифрованных текстов для выявления слабостей в алгоритмах шифрования. Защитным средством от этой атаки является равновероятное распределение составляющих шифртекста.

Существуют различные статистические тесты для определения случайности шифртекста. Например, в литературе [2] описаны пятнадцать тестов для определения случайности заданной последовательности бинарных данных.

В данной статье приведена вероятностно-статистический способ определения случайности последовательности бинарных данных. Основанный на вычислениях математического ожидания, дисперсии и коэффициентов автокорреляции при возрастающей длине выборки и их анализе.

Материалы и методы. В целях анализа криптографических шифров принимается гипотеза пропорциональной зависимости распределения случайной величины к равномерному распределению шифртекста. Проведено исследование свойства выхода некоторых алгоритмов шифрования – шифртексты. Для получения шифртекста в качестве открытого текста взяты тексты на английском языке объемом 1,5 Мб, около 450 страниц на редакторе Word. Для сравнения результатов анализа зашифрованы один и тот же текст на разных алгоримах шифрования. Алгоритмы шифрования были реализованы на языке программирования Python в режиме Cipher Block Chaining (CBC). Для анализа выбраны следующие алгоритмы шифрования: шифр Виженера, Упрощенный алгоритм S-DES, 3DES и AES [3, 4, 5].

Для проведения анализа шифртекстов используется математические аппараты из теории вероятностей и математической статистики, такие как: математическое ожидание, дисперсия и коэффициенты автокорреляции, а также статистические тесты, используемые для проверки случайности двоичных последовательностей. Для определения параметров, характеризующих аналитическую оценку при особенностях колебания шифртекстов, выявляются закономерности, сопоставимые со статистической последовательностью, дающей численные отклонения.

Из курса теории вероятности известно, что математическое ожидание приближенно равно среднему значению случайной величины [6].

$$M(x) = \bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i = \frac{x_1+x_2+\cdots+x_n}{n}. \quad (1)$$

Дисперсия случайной величины – это мера разброса значений случайной величины относительно её математического ожидания [4]:

$$D(x) = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2. \quad (2)$$

Если для временного ряда коэффициенты автокорреляции приближенно равно к нулю, тогда ряд является случайно распределенным [7,8,14]. Коэффициент корреляции характеризует существование линейной зависимости между двумя величинами.

Пусть даны две выборкиб, $x^m = (x_1, \dots, x_m), y^m = (y_1, \dots, y_m)$, коэффициент корреляции рассчитывается по формуле [8,15]:

$$r_{xy} = \frac{\sum_{i=1}^{m}(x_i-\overline{x})(y_i-\overline{y})}{\sqrt{\sum_{i=1}^{m}(x_i-\overline{x})^2\sum_{i=1}^{m}(y_i-\overline{y})^2}}, \quad (3)$$

где $\overline{x}, \overline{y}$, – выборочные средние.

Для оценки силы связи по таблице 1 используется шкала Чеддока [8].

Таблица 1 - Шкала Чеддока

Коэффициент	0,1 – 0,3	0,3 – 0,5	0,5 – 0,7	0,7 – 0,9	0,9 – 0,99
Характеристика зависимости	Слабая	Умеренная	Заметная	Высокая	Весьма высокая

Описание метода и результаты исследования. Для подтверждения гипотезы о случайности шифртекста принимаются числовые статистические характеристики. При определении математического ожидания, дисперсии и коэффициентов автокорреляции, шифртексты были разделены на интервалы равные длине выборки. Для корректности оценочных характеристик, с учётом особенностей формирования алгоритмов блочных шифров, длина выборки определена по мощности кратной длине блоков алгоритмов шифрования: 16, 32, 64, … и т.д. Вычисляется математическое ожидание от последовательностей байтов шифртекста приравненные к их числовым эквивалентам от длины равных к длине выборки. Вычисляется средние отклонения от нуля математических ожиданий. Ниже приведена таблица 2 со средними отклонениями от нуля математического ожидания для шифртекстов при возрастающей длине выборки.

Анализ данных, отраженных в таблице 2, позволяет определить следующую закономерность: для алгоритмов шифрования S-DES, 3DES и AES, с ростом выборки математические ожидания от шифртекста стремятся к нулю. В силу случайности шифртекста вероятность того, что случайная величина во временном ряду примет определенное значение, равна нулю [5]. Как видно из анализа поведения криптографических шифров, на предмет исследования прогноза методом определения математического ожидания, при достаточно стойком шифре с ростом размера выборки математическое ожидание должно стремиться к нулю. Таким образом, ряд представляет собой случайную последовательность, если математическое ожидание будет стремится к нулю.

Также из полученных в таблице 2 данных можно заметить: для шифра Виженера с ростом выборки математическое ожидание не меняется, т.е. остается постоянным и равняется около значения 57. Это означает, что шифртекст полученный методом криптографического шифра Виженера имеет наибольший постоянный показатель, и как следствие, не является равновероятно распределенным, т.е. значения ряда не случайны. Этот эффект, позволяет понизить его оценочную характеристику на предмет стойкости криптошифров, методом прогнозирования среднего статистического значения.

Таблица 2 - Среднее отклонение от нуля математических ожиданий по шифртексту при возрастающей длине выборки

Длина выборки (в байтах)	Шифр Виженера	S-DES	3DES	AES
16	57.65	14.52	14.64	14.88
32	57.61	10.17	10.05	10.97
64	57.64	7.56	7.85	7.58
128	57.74	5.74	5.28	5.33
256	57.63	3.89	3.50	3.88
512	57.62	2.66	2.53	2.59
1024	57.93	1.84	1.77	1.85
2048	58.14	1.41	1.32	1.29
4096	58.07	1.05	0.93	0.95
8192	58.11	0.77	0.78	0.67
16348	58.19	0.59	0.60	0.59

Следующим шагом в получении оценочной характеристики определено среднеквадратичное отклонение. Вычислены дисперсии от шифртекстов, полученных на базе определенных выше

криптографических алгоритмов. Ниже приведена таблица 3 со значениями, показывающими разницу между минимальными и максимальными дисперсиями, вычисленных от интервалов по шифртексту, равные к длине выборки. Эта разница показывает насколько отличаются значения дисперсии друг от друга, при разных интервалах.

Анализ данных, отражённых в таблице 3, позволяет определить следующую закономерность: с ростом выборки, разница между минимальными и максимальными дисперсиями монотонно уменьшается, кроме шифра Виженера. Это означает, что с ростом размера выборки значение дисперсии стремится к некоторому постоянному значению. Это происходит в силу случайности последовательности шифртекста. Таким образом, если временной ряд представляет собой случайную последовательность, тогда дисперсия не меняется.

Таблица 3. Разница между минимальными и максимальными дисперсиями шифртекста

Длина выборки (в байтах)	Шифр Виженера	S-DES	3DES	AES
16	3158	6394	5747	6505
32	1942	4067	3711	4892
64	1340	2877	2846	2935
128	926	2044	2193	2799
256	832	1490	1493	1738
512	804	1200	1068	1310
1024	543	1034	793	765
2048	410	621	612	597
4096	362	479	390	413
8192	486	345	284	260
16384	365	209	163	205

Также, вычислены коэффициенты автокорреляции от шифртекстов. Ниже приведена таблица 4 с коэффициентами автокорреляции вычисленных от интервалов по шифртексту, которые равны длине выборки. Лаг равно к 16 байтам.

Лагом считаем величину сдвига между рядами наблюдений. Лаг с величиной 16, был специально выбран равному к длине блоку алгоритмов шифрования, с целью максимально корректного отображения поведенческих характеристик криптографических шифров. Размерность лага при данной методике исключает помехи при оценке шифртекста.

Из таблицы 4 видно, что для всех алгоритмов шифрования Шифра Виженера, S-DES, 3DES и AES с ростом выборки коэффициенты автокорреляции стремятся к нулю. Согласно шкале Чеддока имеет место очень слабой зависимости между числами в шифртекстах [9,13]. Это означает, что по этому способу последовательность данных шифртекста являются случайными.

Таблица 4 - Коэффициенты автокорреляции для различных алгоритмов шифрования

Лаг	Длина выборки (в байтах)	Шифр Виженера	S-DES	3DES	AES
16	**16**	0.212019	0.208718	0.214384	0.208593
16	**32**	0.143279	0.143555	0.149660	0.143274
16	**64**	0.101883	0.099025	0.102893	0.096751
16	**128**	0.068487	0.072161	0.074431	0.067515
16	**256**	0.048940	0.051886	0.051052	0.048301
16	**512**	0.034098	0.040014	0.036014	0.034312
16	**1024**	0.023074	0.031361	0.027001	0.021264
16	**2048**	0.016320	0.024233	0.019917	0.014016
16	**4096**	0.009521	0.015116	0.017046	0.011027
16	**8192**	0.007060	0.010508	0.014764	0.005420
16	**16384**	0.004778	0.004066	0.008181	0.002320

Итак, временной ряд представляет собой случайную последовательность [10], если переменные независимы и одинаково распределены с математическим ожиданием, равным нулю, имеют одинаковую дисперсию и каждое значение имеет нулевую корреляцию со всеми другими значениями в ряду.

Математический временной ряд является случайным, если выполняется одно или несколько следующих условий:

1) с ростом размерности выборки математическое ожидание стремится к нулю;

2) с ростом размерности выборки дисперсия не меняется;

3) с ростом размерности выборки коэффициент автокорреляции между запаздывающими переменными стремится к нулю.

Метод статистического анализа. Для проведения статистических тестов шифротекстов криптографического алгоритма используется средство тестирования NIST_STS [2,11]. Исполняемый файл nist_sts.exe запускается из командной строки, и задаётся длина исследуемой последовательности равное 1000000 [12].

Статистический тест в таблице 5 включает набор пятнадцати тестов Национального института стандартов и технологий США (NIST).

Таблица 5 - Результаты статистических тестов на случайность по nist_sts.exe

№	Статистический тест	Шифр Виженера	S-DES	3DES	AES
1	Frequency	Failure	Success	Success	Success
2	BlockFrequency	Failure	Success	Success	Success
3	CumulativeSums	Failure	Success	Success	Success
4	Runs	Failure	Success	Success	Success
5	LongestRun	Failure	Failure	Success	Success
6	Rank	Failure	Success	Success	Success
7	FFT	Failure	Success	Success	Success
8	NonOverlappingTemplate	Failure	Failure	Success	Success
9	OverlappingTemplate	Failure	Failure	Success	Success
10	Universal	Failure	Success	Success	Success
11	ApproximateEntropy	Failure	Failure	Success	Success
12	RandomExcursions	Failure	Success	Success	Success
13	RandomExcursionsVariant	Failure	Success	Success	Success
14	Serial	Failure	Failure	Success	Success
15	LinearComplexity	Success	Success	Success	Success

По результатам статистического теста NIST не прошли тест Шифр Виженера и S-DES. Успешно прошли тест 3DES и AES (таблица 6).

Таблица 6 - Итоговая таблица по результатам всех тестов

№ таблицы	Признаки	Шифр Виженера	S-DES	3DES	AES
1	Математическое ожидание	−	+	+	+
2	Дисперсия	−	+	+	+
3	Автокорреляция	+	+	+	+
4	Статистические тесты NIST	−	−	+	+

Из таблицы 6 видно, что шифр Виженера не прошел статистический тест NIST, математического ожидания и дисперсии. Алгоритм S-DES не прошел статистический тест NIST. Все тесты успешно прошли алгоритмы криптографического преобразования 3DES и AES. По результатам всех тестов алгоритмы 3DES и AES можно отнести к устойчивым алгоритмам по результатам анализа их шифртекста.

Заключение. В данной работе проведены статистические тесты для шифртекстов алгоритмов шифрования Виженера, S-DES, 3DES и AES. Осуществлена проверка статистических характеристик шифртекста на случайность и линейную независимость.

Шифр Виженера не прошел тест математического ожидания, дисперсии и статистический тест на случайность, так как математические ожидания по шифртексту постоянны, не стремятся к нулю. Также нарушается монотонность убывания дисперсии. Алгоритм S-DES не прошел статистический тест NIST на случайность. По результатам анализа алгоритмы 3DES и AES являются устойчивыми алгоритмами к атакам осуществляемых на основе периодичности по шифртексту, так как успешно прошли все тесты.

Данный метод можно использовать как вспомогательный для анализа стойкости алгоритмов шифрования по шифртексту, а также описанную в этой статье теорию можно продолжить исследовать в заданном направлении и формировать в виде статистического теста для определения случайности заданных данных.

Information about authors:

Kubayev K.E. – Dr. Sci. Economy, professor Al-Farabi Kazakh National University, +7 7026159530, kubaev.k@mail.ru, https://orcid.org/0000-0002-9083-4257;

Baisholanova K.S. – Dr. Sci. Economy, associate professor Al-Farabi Kazakh National University, +7 7026159530, baisholanova.k@gmail.com, https://orcid.org/0000-0001-7375-5998;

Alimzhanova Zh.M. – Cand. sci. of phys. and math., senior lecturer, Al-Farabi Kazakh National University, +7 747 9574800, zhannamen@mail.ru, https://orcid.org/0000-0001-6282-5356;

Baisholan N. – PhD Student of the Al-Farabi Kazakh National University, +7 771 4164017, baisholan@gmail.com, https://orcid.org/0000-0002-8134-0466;

Baisholanov T.S. – Master's degree student of the Al-Farabi Kazakh National University, + 7 777 2644070, btstalgat@mail.ru, https://orcid.org/0000-0002-3413-0087.

ЛИТЕРАТУРЫ

[1] Авдошин С.М., Савельева А.А., Криптоанализ: современное состояние и перспективы развития. Режим доступа: https://www.hse.ru/data/712/315/1234/Авдошин.Савельева_Криптоанализ.pdf.

[2] NIST SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number, Generators for Cryptographic Applications / [A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo]. National Institute of Standards and Technology, 2010.

[3] ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197, November 26, 2001.

[4] Federal Information, Processing Standards Publication 46-3, Announcing the DATA ENCRYPTION STANDARD, 1999 October 25.

[5] Dr. K.S. Ooi, Brain Chin Vito, Cryptanalysis of S-DES, University of Sheffield Centre, Taylor's College, 2002. p.8, https://eprint.iacr.org/2002/045.pdf

[6] Гмурман В.Е. Теория вероятностей и математическая статистика. - М.: Юрайт, 2016. - 479 с. ISBN 978-5-9916-4997-1

[7] Трофимова Е.А., Кисляк Н.В., Гилёв Д.В. Теория вероятностей и математическая статистика, М-во образования и науки Рос. Федерации, Урал. федер. ун-т. – Екатеринбург: Изд-во Урал. ун-та, 2018. - 160 с. ISBN 978-5-7996-2317-3.

[8] Ковалев Е.А., Медведев Г.А. Теория вероятностей и математическая статистика для экономистов, М.: Издательство Юрайт, 2017. - 284 с. ISBN 978-5-9916-5950-5.

[9] Демин С.Е., Демина Е.Л. Математическая статистика, Нижний Тагил: НТИ УрФУ, 2017. - 240 с. ISBN 978-5-9544-0079-3

[10] Слеповичев И.И. Генераторы псевдослучайных чисел. Учебное пособие. Саратов: СГУ, - 118 с. 2017.

[11] S. Kim, K, Umeno, and A. Hasegawa, Corrections of the NIST Statistical Test Suite for Randomness, Cryptology ePrint Archive, Report 2004/018, 2004.

[12] Ковтун. В. Разработка и исследование генератора псевдослучайных чисел. [Электронный ресурс]. Режим доступа: https://www.nrjetix.com/fileadmin/doc/publications/labs_security/Lab2.pdf.

[13] Романьков В.А. Введение в криптографию. Курс лекций, 2012. - 240 с. https://itsecforu.ru/wp-content/uploads/2018/02/V_A_Romankov_Vvedenie_v_kriptografiyu_2-e_izdanie.pdf

[14] Werner Linde. Probability Theory. A First Course in Probability Theory and Statistics. 2016. p. 200, 237. Walter de Gruyter GmbH, Berlin/Boston, ISBN 978-3-11-046617-1.

[15] Oliver Knill. Probability Theory and Stochastic Processes with Applications. Overseas Press, (India) PVT. LTD. 2009. p. 25. ISBN: 978 - 81 - 89938 - 40 - 6.

REFERENCES

[1] Avdoshin S.M., Savelyeva A.A., Cryptanalysis: Current State and Prospects of Development. [Electronic resource]. Access mode: https://www.hse.ru/data/712/315/1234/Авдошин.Савельева_Криптоанализ.pdf (in Russ.).

[2] NIST SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number, Generators for Cryptographic Applications / [A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo]. National Institute of Standards and Technology, 2010. (in Eng.).

[3] ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197, November 26, 2001 (in Eng.).

[4] Federal Information, Processing Standards Publication 46-3, Announcing the DATA ENCRYPTION STANDARD, 1999 October 25. (in Eng.).

[5] Dr. K.S. Ooi, Brain Chin Vito, Cryptanalysis of S-DES, University of Sheffield Centre, Taylor's College, 2002. https://eprint.iacr.org/2002/045.pdf (in Eng.).

[6] Gmurman V.E. Probability Theory and Mathematical Statistics. - Moscow: Yurait, 2016. – p. 479. ISBN 978-5-9916-4997-1 (in Russ.).

[7] Trofimova E.A., Kislyak N.V., Gilyov D.V. Probability Theory and Mathematical Statistics, Ministry of Education and Science of the Russian Federation. Federation, Ural Federal University. - Ekaterinburg: Izd vo Ural. Un., 2018. – 160 c. ISBN 978-5-7996-2317-3 (in Russ.).

[8] Kovalev E.A., Medvedev G.A. Probability Theory and Mathematical Statistics for Economists, Moscow: Yurait, 2017. – 284 c. ISBN 978-5-9916-5950-5 (in Russ.).

[9] Demin S.E.E., Demina E.L. Mathematical Statistics, Nizhny Tagil: NTI UrFU, 2017. – 240 c. ISBN 978-5-9544-0079-3 (in Russ.).

[10] Slepovichev I.I. Pseudorandom number generators. Study guide. Saratov: SGU, – 118 c. 2017. (in Russ.).

[11] S. Kim, K, Umeno, and A. Hasegawa, Corrections of the NIST Statistical Test Suite for Randomness, Cryptology ePrint Archive, Report 2004/018, 2004. (in Eng.).

[12] Kovtun. B. Development and research of a pseudorandom number generator. [Electronic resource]. Access mode: https://www.nrjetix.com/fileadmin/doc/publications/labs_security/Lab2.pdf (in Russ.).

[13] Romankov V.A. Introduction to Cryptography. Course of lectures, 2012. – 240 c. https://itsecforu.ru/wp-content/uploads/2018/02/V_A_Romankov_Vvedenie_v_kriptografiyu_2-e_izdanie.pdf (in Russ.).

[14] Werner Linde. Probability Theory. A First Course in Probability Theory and Statistics. 2016. p. 200,237. Walter de Gruyter GmbH, Berlin/Boston, ISBN 978-3-11-046617-1. (in Eng.).

[15] Oliver Knill. Probability Theory and Stochastic Processes with Applications. Overseas Press, (India) PVT. LTD. 2009. p. 25. ISBN: 978 - 81 - 89938 - 40 - 6. (in Eng.).

СОДЕРЖАНИЕ

ИНФОРМАТИКА

ФИЗИКА

МАЗМҰНЫ

ИНФОРМАТИКА

ФИЗИКА

CONTENTS

COMPUTER SCIENCE

PHYSICS

Publication Ethics and Publication Malpracticein
the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:

www:nauka-nanrk.kz

http://physics-mathematics.kz/index.php/en/archive

ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Редакторы: *М.С. Ахметова, А. Ботанқызы, Д.С. Аленов, Р.Ж. Мрзабаева*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 10.03.2022.
Формат 60x881/8. Бумага офсетная. Печать –ризограф.
9,0 п.л. Тираж 300. Заказ 1.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19