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

N E W S

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

SERIES
PHYSICO-MATHEMATICAL

5 (339)

SEPTEMBER – OKTOBER 2021

PUBLISHED SINCE JANUARY 1963

PUBLISHED 6 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. Физикалық-математикалық 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 физико-математическая» 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: *математика, информатика, механика, физика, ғарыштық зерттеулер, астрономия, ионосфера.*
Мерзімділігі: жылына 6 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: *математика, информатика, механика, физика, космические исследования, астрономия, ионосфера.*
Периодичность: 6 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. Physical-mathematical series.
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: *mathematics, computer science, mechanics, physics, space research, astronomy, ionosphere.*
Periodicity: 6 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 5, Number 339 (2021), 100–110 ***https://doi.org/10.32014/2021.2518-1726.90***

УДК 004.056.5
МРНТИ 81.93.29

Усатова О.А.[1,2], Бегимбаева Е.Е.[1,2], Нысанбаева С.Е.[1], Усатов Н.С.[3]

[1]Институт информационных и вычислительных технологий КН МОН РК, Алматы, Казахстан;
[2]Казахский Национальный Университет им. аль-Фараби, Алматы, Казахстан;
[3]Университет «Туран», Алматы, Казахстан.
E-mail: uoa_olga@mail.ru

АНАЛИЗ МЕТОДОВ И ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ХЕШ-ФУНКЦИЙ

Аннотация. На сегодняшний день область применения хеш-функций чрезвычайно широка. Функции хеширования успешно применяются при решении задач защиты компьютерной информации, включая аутентификацию субъектов и объектов информационного взаимодействия до внесения неопределенности в работу средств и объектов защиты. В последние годы отмечается чрезвычайный рост необходимости использования безопасных хеш-функций. К тому же функция хеширования играют особенную и главную роль в современной криптографии. Криптографические хеш-функции, также могут использоваться для защиты от фальсификации передаваемой информации. Существует большое количество алгоритмов хеширования, которые отличаются криптографической стойкостью, сложностью, разрядностью и другими свойствами. Криптографическая хеш-функция является математическим алгоритмом, который преобразовывает массив входных данных произвольной длины в выходную битовую строку фиксированной длины. Вне зависимости от объема вводных данных, при условии использования того же типа хеша длина будет оставаться неизменной.

В криптографических приложениях к функциям хеширования предъявляются ряд требовании, которые описаны в статье. Помимо существования определенных требований и свойств, в разных странах имеются национальные стандарты криптографической защиты информации для хеш-функций. В статье предлагается анализ современного состояния безопасности и структур криптографических хеш-функций. Приводятся результаты практического применения алгоритмов криптографических хеш-функций и их реализации на различных платформах. Во многих языках программирования, а также серверных языках используются специальные классы и функции, которые без затруднений вычисляют хеш-функции, и при этом используют стандартные алгоритмы. Алгоритмы хеширования применяются в системных, объектно-ориентированных, web приложениях, системы управления базами данных, архивации, технологии блокчейн и криптовалютах. Показаны особенности использования хеш-функций по областям применения.

Ключевые слова: защита данных, хеш-функция, криптография, алгоритмы хеширования, информационная безопасность.

Введение. Область применения хеш-функций чрезвычайно широка, они успешно решают практически все задачи защиты компьютерной информации от обеспечения аутентичности субъектов и объектов информационного взаимодействия до внесения неопределенности в работу средств и объектов защиты.

Хеширование используется для выполнения целого ряда задач, таких как аутентификация, осуществление проверки целостности информации, защита файлов, включая, в некоторых случаях, определение вредоносного программного обеспечения и многие другие функции. Хеширование решает проблему по объему поступающих данных, именно поэтому алгоритмы, способные оперировать лаконичными значениями, весьма востребованы в современном мире цифровых технологий. Механизм хеш-функций применяется для уменьшения времени, необходимого для генерации и проверки подписи,

а также для сокращения ее длины. Хеширование применяется для сравнения данных. Хорошая хеш-функция – это та функция, которая с вычислительной точки зрения проста, равномерно распределяет ключи в хеш-таблице и уменьшает число коллизий. Хеш-функции строятся по итеративной схеме, когда исходное сообщение разбивается на блоки определенного размера, и над ними выполняются ряд преобразований с использованием как обратимых, так и необратимых операций. Как правило, в состав хеширующего преобразования включается сжимающая функция, поскольку его выход зачастую по размеру меньше блока, подаваемого на вход. На вход каждого цикла хеширования подается выход предыдущего цикла, а также очередной блок сообщения.

Материалы и методы. В международном стандарте ИСО/МЭК 14888-1-2008 хеш-функция определена как функция, отображающая строки бит в строки бит фиксированной длины [1]. Для практического взаимодействия в той или иной области хеш-функции имеют ряд требований и свойств [2-4]:

− алгоритм должен характеризоваться чувствительностью к изменениям во внутренней структуре хешируемых документов. Любые изменения входных данных должны влиять на выходные биты, т.е. входные и выходные данные хеш-функции не должны быть статистически коррелированы. Данное явление называется лавинным эффектом.

− алгоритм должен преобразовывать данные так, чтобы обратная операция (превращение хеша в изначальный документ) была на практике невозможна, то есть для хеш-функции «H», устойчивой к прообразу, при заданном хеш-значении «H(M)» конкретного сообщения «M» должно быть вычислительно невозможно извлечь исходное сообщение «M» или действительно невозможно сгенерировать любое сообщение $M' \neq M$ такое, что H (M') = H (M):

$$Adv_H^{pre[m]}(A) = \Pr\left[M \xleftarrow{\$} \{0,1\}^m; Y \leftarrow H(M); M' \xleftarrow{\$} A(Y): H(M') = Y\right] \quad (1)$$

− алгоритм, который практически исключает вероятность формирования одинаковой последовательности символов в виде хеш, то есть появление коллизий. Формально преимущество противника «A» в обнаружении коллизии в хеш-функции «H» определяется следующим образом:

$$Adv_H^{cr}(A) = \Pr\left[(M,M') \xleftarrow{\$} A : M \neq M' \wedge (M) = H(M')\right] \quad (2)$$

−частичное сопротивление прообразу: также иногда называемое локальной односторонностью, утверждает, что извлечение части исходного сообщения из его хеш-значения должно быть столь же трудным, как и получение всего сообщения, даже если часть сообщения уже известна.

Помимо существования определенных требований и свойств, в разных странах имеются национальные стандарты криптографической защиты информации для хеш - функций.

В Южной Кореесть собственный стандарт хеширования LSH, разработанный в 2014 году. LSH - один из криптографических алгоритмов, одобренных Корейской программой проверки криптографических модулей (KCMVP). Преимущество данного алгоритма в том, что он более чем в два раза превышает производительность международных стандартов (SHA2 / 3) в различных средах программного обеспечения.

Основные характеристики хеш-функций: длина вывода: 224 бит, 256 бит, 384 бит или 512 бит; конструкция: LSH имеет широкую структуру Меркла - Дамгарда с заполнением одним нулем.

LSH до сих пор защищен от известных атак на хеш-функции. LSH устойчив к столкновениям для $q<2^{n/2}$ и имеет устойчивость к прообразу и устойчивость к второму прообразу для $q<2^n$ в идеальной модели шифра, где q - количество запросов для конструкции LSH [5].

В Японии действует стандарт «JISX 5057-2: 2003 (ISO/IEC 10118-2:2000) Информационные технологии. Методы безопасности. Хеш-функции. Часть 2. Хеш-функции с использованием n-битного блочного шифра» [6]. Использование SHA-1 обозначено как стандартная хеш-функция JIS с 2018 года.

В Индии нет специальных положений закона о шифровании. Однако ряд отраслевых нормативных актов, в том числе в банковской, финансовой и телекоммуникационной отраслях, содержат такие положения, как минимальные стандарты шифрования, которые могут использоваться для обеспечения безопасности транзакций. Условия лицензионного соглашения между Министерством телекоммуникаций (DoT) и поставщиками интернет-услуг разрешают использование технологий шифрования только до 40 бит с алгоритмами RSA или их эквивалентами без предварительного одобрения DoT. Для лучшего шифрования стандарт может использоваться только с разрешения и

передачи ключа дешифрования, разделенного на две части, в DoT. Более того, существует полный запрет на использование массового шифрования интернет-провайдерами в соответствии с этими условиями лицензии (пункт 2.2 (vii) Лицензионного соглашения между DoT и ISP, январь 2010 г.) [7].

В Китае есть ряд стандартов: «GM/T 0002-2012 SM4 BlockCipherAlgorithm (Алгоритм блочного шифрования SM4)», «GB/T 32905-2016 InformationsecuritytechnologySM3 cryptographichashalgorithm (Технология защиты информации Криптографический алгоритм хеширования SM3)», «GB/T 18238.2-2002 Informationtechnology - Securitytechniques - Hash-functions - Part 2: Hash-functionsusingann-bitblockcipher Информационные технологии. Методы безопасности. Хеш-функции. Часть 2. Хеш-функции с использованием n-битного блочного шифра.)», «GB/T 18238.3-2002 Informationtechnology - Securitytechniques - Hash-functions - Part 3: Dedicatedhash-functions (Информационные технологии. Методы безопасности. Хеш-функции. Часть 3. Выделенные хеш-функции), «GB/T 18238.1-2000 Information technology – Security techniques-Hash-function - Part 1: General (Информационные технологии. Методы безопасности. Хеш-функция. Часть 1. Общие положения), «GB/T 32905-2016 InformationsecuritytechnologySM3 cryptographichashalgorithm (Технология защиты информации Криптографический алгоритм хеширования SM3)» [8].

Система хеширования может рассматривать несколько типов:

1. Алгоритм для аудита целостности информации. При передачи электронных документов выполняется вычисления хеш-кода, результат будет передаваться вместе с документами. При приеме передаваемой информации происходит повторное вычисление хеш-кода с последующим сравнением, полученным значением. Если вычисленные результаты не совпадают, то это является ошибкой. Данный алгоритм обладает высокими скоростными показателями при вычислении, но отличается нестабильностью и малым значением хеш-функции.

2. Криптографический алгоритм. Используется в качестве защиты от несанкционированного доступа в момент передачи файлов по сети, проверяя систему на предмет модификации информации. В этом случае хеш имеет свободный доступ, а ключ, полученного документа, вычисляется при помощи разнообразных программ.

3. Алгоритм для создания эффективной информационной конструкции. Определяющей задачей которой является структурирование информации в хеш-таблицы, которая делает возможным добавление/удаление, нахождение нужных данных с высокой скоростью.

В эпоху информатизации мы не представляем нашу жизнь без Интернета. При скачивании файлов пользователи сети сталкиваются с хеш-функциями сами того не осознавая, так как не обращают внимание на череду непонятных цифр и латинских букв, это и есть хеш или контрольные суммы. В начале последовательности указано название используемого протокола хеширования. Для проверки подлинности и выявления ошибок используются специальные утилиты.

Хеш – функцииреализуют:

1. Создание и проверку электронных цифровых подписей;
2. Системы аутентификации, где используются для хеширования паролей.
3. Хранение паролей в базах данных систем безопасности;
4. Проверка подлинности и целостности элементов файловой системы ПК;
5. В рамках современной криптографии для создания уникальных ключей онлайн.

Для защиты данных применяют многоярусный комплексный криптографический алгоритм и дополнительные меры безопасности защиты канала связей. Хеш-функция в ЭЦП служит для сжатия исходного подписываемого текста в дайджест(хеш-код) (относительно короткое число), состоящее из фиксированного небольшого числа битов и характеризующее весь текст в целом.

Анализ современных алгоритмов хеширования данных. Впервые важность криптографических хеш-функций была отмечена с изобретением нового типа криптографической системы, системы с открытым ключом (СОК) У. Диффи и М. Хеллманом [9] в 1976 году, и с тех пор хеш-функций стали неотъемлемой частью СОК. К сожалению, недавние достижения в области криптоанализа выявили недостатки, присущие большинству популярных хеш-функций. В связи с этим были приняты два основных подхода: исправление существующих конструкций путем их небольшого изменения с учетом определенного набора слабых мест и разработка новых хеш-функций с нуля. Существующие конструкции хеш-функции имеют преимущество, что они были тщательно изучены и проанализированы с течением времени, таким образом, если не спроектированы очень тщательно, структурно новые хеш-функции могут быть подвержены большему количеству атак, чем те, которым они сопротивляются.

Первая хеш-функция была основана на блочном шифре DES. Со времен их эволюции опубликованы сотни новых хеш-функций и предложены их модификации. Широко используются хеш-функции семейства MD5 и SHA-1. NIST объявил конкурс SHA-3 на выбор безопасной и эффективной хеш-функции. В 2012 году конструкция на основе губки Keccak была выбрана в качестве стандарта SHA-3. По структуре хеш-функций можно разделить на три категории: хеш-функция, основанная на блочных шифрах, хеш-функция, основанная на арифметических функциях, и специализированные хеш-функции. Большинство криптографических хеш-функций относится к категории специализированных хеш-функций.

Существуют два основных типа хеш-функций: ориентированные на данные; (используются в системах, работающих с большими объемами данных для ускорения их поиска, сравнения и выдачи) и ориентированные на безопасность.

Алгоритмы MD5, SHA-1, SHA-256, а в России ГОСТ Р 34.11-2012 имеют применение в большинстве решений связанные с преобразованием данных.

В Массачусетском университете профессором Рональдом Ривестом в 1990 году была описана хеш-функция MD4, которая была взломана в 1993 году. MD 5 является наиболее распространенная из семейства MD-функций на сегодняшний день.

В 2006 году Властимил Клима опубликовал алгоритм [10], позволяющий обнаруживать коллизии за несколько часов. Исследователь обнародовал алгоритм, находящий коллизии за одну минуту, который позднее получил название «туннелирование». На сегодняшний день MD5 не рекомендована для использования в реальных приложениях.

SHA1 (Secure Hashing Algorithm) является алгоритмом, созданный Агентством национальной безопасности (NSA). На выходе которого создается 160-битное хеш сообщения фиксированной длины. Для распознавания исходного сообщения для алгоритма SHA1 потребуется 2^{160} операции, тогда как в MD5 2^{128} операции.

SHA3 принципиально отличается по архитектуре SHA1 и является частью большой схемы алгоритмов хеширования Keccak. Во внутреннем механизме SHA3 используются случайные перестановки при обработке данных, называемыеконструкцией «губки»: «впитывание данных» и «выжимание», где P_i – входные блоки, Z_j – блоки на выходе, r- скорость, размер части состояния (записывается и считывается), c – емкость, размер части, которая нетронута вводом / выводом. На рисунке 1 показана принцип работы функции губки.

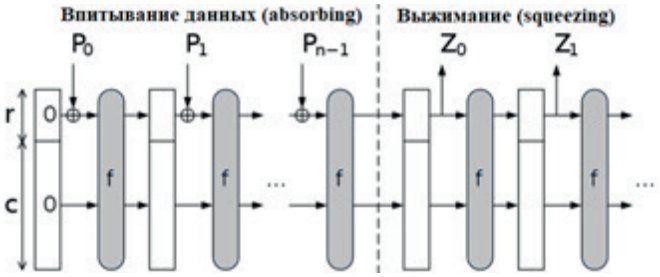

Рисунок 1 – Конструкция функции губки.

В работе [11] предложен алгоритм хеширования, который основан на комбинации некоторых функций SHA-256 и модификацией расширения сообщений - и MD5 на основе двойной схемы Дэвиса-Майера.

Хеш-сумма сообщения (MD) описывает математическую функцию, которая может выполняться в строке переменной длины. MD5 - это хеш-функция, разработанная Роном Ривестом как усиленная версия MD4 [12]. Он может сжимать данные любой длины в информационную хеш-сумму размером 128 бит, в то время как эта сегментная хеш-сумма сообщения часто претендует на роль цифрового отпечатка данных [13]. В 1993 г. B. Den Boer и A. Bosselaers обнаружили своего рода псевдо коллизию для MD5, состоящую из одного и того же сообщения с двумя разными наборами начальных значений. Эта атака обнаруживает слабую лавину в наиболее значимом бите для всех цепочечных переменных в MD5 [12]. В 2002 году Национальный институт стандартов и технологий (НИСТ) выпустил пересмотренную версию стандарта FIPS 180-2, в которой определены три новые версии SHA с длинами хеш-значений 256, 384 и 512 бит. Эти версии известны как SHA-256, SHA-384, SHA-512. Данные алгоритмы имеют ту же базовую структуру и используют те же типы модульных арифметических

и логических бинарных операций, что и SHA-1. В 2005 году НИСТ-омбыло объявленооб отказе от утверждения SHA-1 и переходе к использованию других версий SHA к 2010 году. Вскоре после этого исследовательская группа описала атаку, где указывалось о возможности нахождения двух отдельных сообщении, доставляющих один и тот же хешSHA-1 с использованием 2^{69} операций. Это намного меньше, чем считалось ранее 2^{80} операций, необходимых для обнаружения коллизии с хешем SHA-1. SHA-256 также недостаточно безопасен, поскольку он имеет атаку на 46 (из 64) шагов функции сжатия с практической сложностью [14] и атаки на прообраз на 41 шаге SHA-256 [15]. В 2007 году это была комбинация MD5 и SHA-1 с длиной хеш-кода 160 бит [16], в 2012 году это была комбинация MD5 и SHA-1 с длиной хеш-кода 256 бит [17].

Результаты. Практическое применение хеш-функций. Во многих языках программирования, а также серверных языках используются специальные классы и функции, которые без затруднений вычисляют хеши, и при этом используют стандартные алгоритмы. Алгоритмы хеширования применяются в системных, объектно-ориентированных, web приложениях, системы управления базами данных (СУБД), архивации, технологии блокчейн и крипто валютах. Рассмотрим практическое применение алгоритмов хеширования SHA2 и MD5 для Web-приложений.

MD5 является одним из алгоритмов хеширования на 128-битной основе. Этот стандарт кодирования является одним из самых распространенных методов защиты данных не только в прикладном, но и в веб-программировании [18].

Реализации алгоритмов хеширования MD5 и SHA256 на языке программирования Python представлена на рисунке 2.

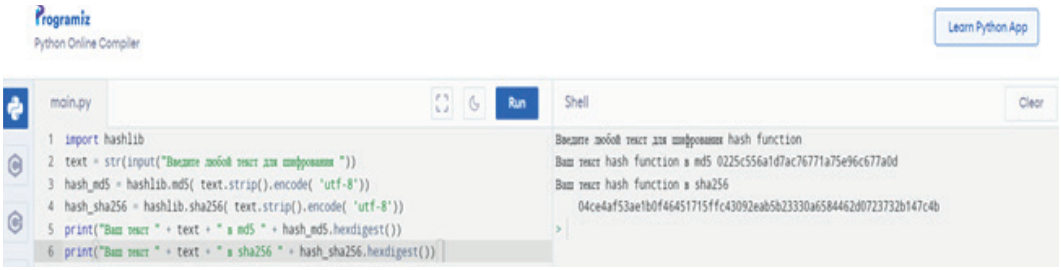

Рисунок 2 – Реализации алгоритмов хеширования на языке программирования Python.

Основным способом, гарантирующим безопасность хеша вашего пароля, является использование «соли». Он основан на добавлении к паролю нескольких случайных символов и последующем хешировании результата. Для примера рассмотрим создание хеш-кода на основе алгоритма MD5, в качестве одного из параметров принимает значение «соли», на языке программирования PHP (рисунок 3).

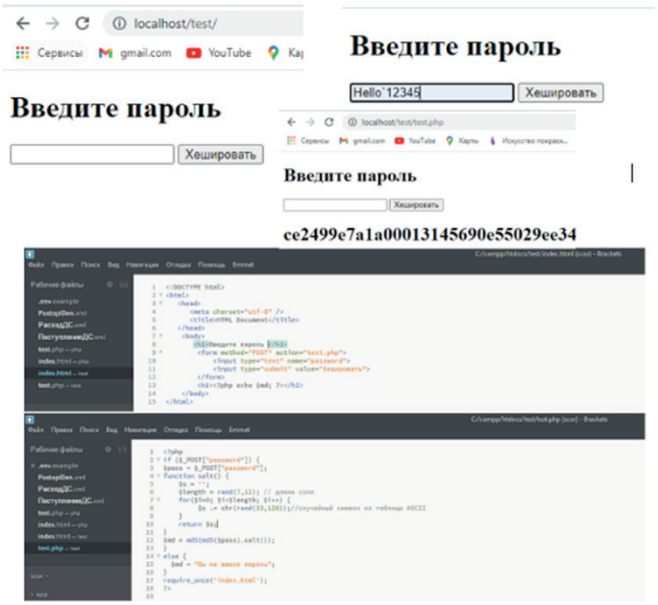

Рисунок 3 – Реализации алгоритмов хеширования на языке программирования PHP.

Рассмотрим пример SHA256 в алгоритме двухфакторной аутентификации.Выбор тригонометрической функции для вычисления одноразового пароля осуществляется в соответствии с результатом полученной хеш – функции стандартов SHA256, где используются первые символы, которые будут являться индексами в таблице размерностью 256x256 представленный на рисунке 4. По данному индексу будет выбрана функция и определены её параметры. По итогам вычисления в качестве одноразового временного пароля берутся цифры после запятой, начиная с 5 – й позиции и длиною в 6 цифр. Полученное число и будет временным паролем, которое необходимо ввести в приложение [19-20].

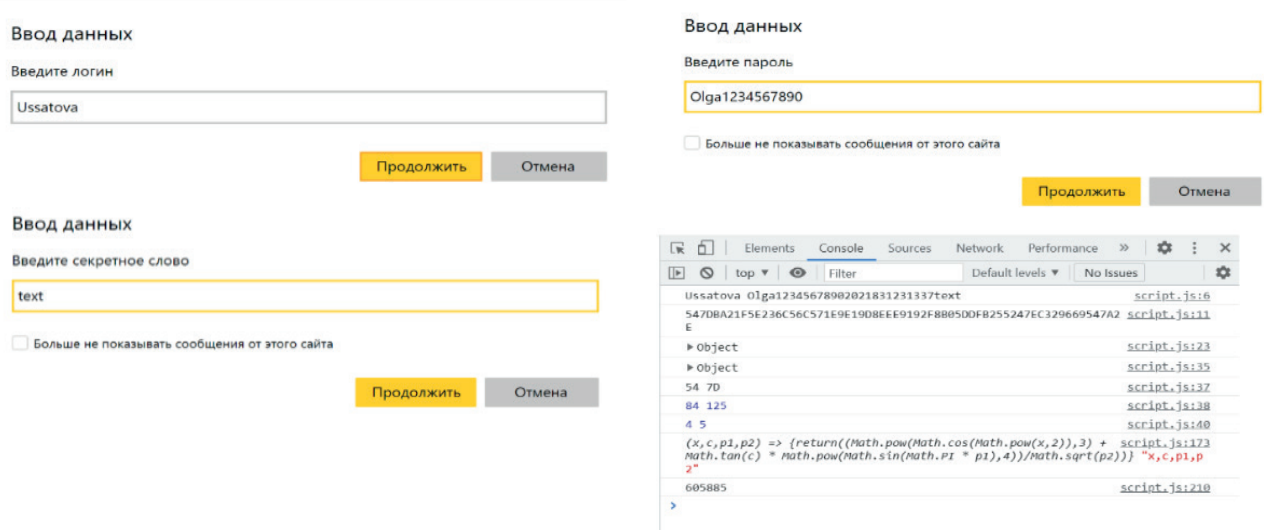

Рисунок 4 – SHA256 в алгоритме двухфакторной аутентификации.

Обсуждение. Особенности использования хеш-функций по областям применения представлены в таблице 1.

Таблица 1 - Использование хеш-функций

Область применения	Особенности использования хеш-функций
Системное ПО	В операционных системах (ОС) хеш - функции используются для хранения паролей. Полномочия пользователей и способ их аутентификации заложен на уровне системы. В ОС Linux список пользователей хранится в файле /etc/passwd, который можно открыть его и посмотреть, пароли же выделены в отдельный файл - /etc/shadow. Этот файл можно открыть только с правами суперпользователя, и, более того, пароли здесь хранятся в зашифрованном виде, в связи с этим узнать пароль Linux будет невозможно. Смена пароля выполняется с помощью утилиты passwd, которая позволяет не только менять пароль, но и управлять сроком его жизни. В ОС Windows пароли пользователей хранятся в hives реестре в файлах SYSTEM и SAM в виде хешей. В ОС Linux файл *.iso и ОС Windows *.exe запускаются с помощью хеш-функций, что подтверждает оригинальность файла и целостность в процессе загрузки.
Блокчейн и Криптовалюта	Хеши в блокчейнах гарантируют «необратимость» всей цепочки транзакций. Дело в том, что каждый новый блок транзакций ссылается на хеш предыдущего блока в реестре. Хеш самого блока зависит от всех транзакций в блоке, но вместо того, чтобы последовательно передавать транзакции хеш-функции, они собираются в одно хеш-значение при помощи двоичного дерева с хешами (дерево Меркла). Таким образом, хеши используются как замена указателям в обычных структурах данных: связанных списках и двоичных деревьях.

	В блокчейне биткоина осуществляется несколько операций, которые включают себя хеширование, большая часть которого заключается в майнинге. Практически все криптовалютные протоколы полагаются на хеширование для связывания и сжатия групп транзакций в блоки, а также для создания криптографической взаимосвязи и эффективного построения цепочки из блоков.Когда речь заходит о биткоине, криптографические хеш-функции являются неотъемлемой частью в процессе майнинга, а также занимают основную роль в генерации новых ключей и адресов.
Архивация	При архивации файлов добавляются хеши. Для расчета хеша используют специальные программы, такие как HashTab. Она добавляет соответствующие функции в меню свойств файлов.
Приложения и СУБД	1. Структуры данных - языки программирования содержат структуры данных, основанные на хеше. 2. Дайджест сообщения - алгоритм используется при проверке целостности данных. Примеры алгоритмов дайджеста сообщений включают MD2, MD4, MD5 и MD6. 3. Безопасный алгоритм хеширования - используется для защиты данных в приложениях и протоколах, таких как Secure Socket Layer. 4. Проверка и хранение пароля - при вводе пароля для аутентификации пользователя вычисляется хеш-значение введенного пароля и отправляется по сети на сервер, где хранится хеш-код оригинала. 5. Работа компилятора - в языках программирования используются разные ключевые слова, чтобы различать ключевые слова и идентификаторы, компилятор использует хеш-набор, который реализован с использованием хеш-таблицы для хранения ключевых слов и идентификаторов. 6. Алгоритм Рабина-Карпа - использует хеширование для поиска одного или нескольких шаблонов в заданной строке. 7. Сопоставимые и компараторские интерфейсы - содержат функции, которые используются для сравнения двух объектов одновременно. Внутренне компаратор и сопоставимые интерфейсы используют хеш-функцию для сравнения объектов друг с другом.

При практическом применение хеш-функции важным является вопросом производительности. Более стойкие алгоритмы потребляют больше ресурсов, для использования хеш-функций необходимо протестировать систему рассчитав скорость перебора в секунду. В качестве примера на рисунке 5 графически представлена скорость перебора хеш-функций картыGeForce GTX 1060 (единицы измерения – мегахеши в секунду):

- MD5: 11560,2 MH/ s (95,88ms);
- SHA-1: 4428.1 MH/s (96.34ms);
- SHA256:1478.3 MH/s (95.92ms);
- SHA512: 552.3 MH/s (95.92ms);
- NTLM: 19204.1 MH/s (97.03ms).

Рисунок 5 – Скорость перебора хеш-функций карточки GeForce GTX 1060.

Заключение. Функции хеширования данных считаются относительно случайными. Безопасные криптографические хеш-функций имеют основные требования, такие как: невозможность генерации сообщения, соответствующее определенному хеш-значению и невозможность создания два сообщения, которые производят одно и то же значение хеш. На сегодняшний день MD5 не рекомендована для использования в реальных приложениях, поскольку исследовательские атаки предоставили достаточные основания для исключения использования алгоритма в приложениях, которым требуется устойчивость к различного рода коллизиям.

Статья подготовлена в рамках проекта № OR11465439 «Разработка и исследование алгоритмов хеширования произвольной длины для цифровых подписей и оценка их стойкости».

Усатова О.А.[1,2], Бегимбаева Е.Е.[1,2], Нысанбаева С.Е.[1], Усатов Н.С.[3]

[1]Ақпараттық және есептеуіш технологиялар институты ҚР БҒМ ҒК, Алматы, Қазахстан;
[2]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан;
[3] «Тұран» университеті, Алматы, Қазақстан.
E-mail: uoa_olga@mail.ru

ХЕШ ФУНКЦИЯ ӘДІСТЕРІН ТАЛДАУ ЖӘНЕ ПРАКТИКАЛЫҚ ҚОЛДАНУ

Аннотация. Бүгінгі таңда хеш-функцияларын қолдану аясы өте кең. Хештеу функциялары компьютерлік ақпаратты қорғау мәселелерін шешуде, ақпараттық өзара әрекеттесу субъектілері мен объектілерін аутентификациялауды қоса алғаннан бастап қауіпсіздік объектілері мен құралдарының жұмысына белгісіздік енгізуге дейін сәтті қолданылады. Соңғы жылдары қауіпсіз хеш-функцияларын пайдалану қажеттілігінің өсуі байқалады. Сонымен қатар, хештеу функциялары қазіргі криптографияда ерекше және басты рөлді атқарады. Криптографиялық хеш-функциялары, сондай-ақ, жіберілетін ақпаратты фальсификациядан қорғау үшін пайдаланылуы мүмкін. Криптографиялық беріктігімен, күрделілігімен, бит разрядтылығымен және басқа да қасиеттерімен ерекшеленетін көптеген хеш алгоритмдері бар. Криптографиялық хеш-функциялары - бұл еркін ұзындықтағы кіріс массив деректерін тұрақты ұзындықтағы шығыс бит жолына түрлендіретін математикалық алгоритм болып табылады. Еңгізу деректерінің көлеміне қарамастан, хештің белгілі бір түрін қолданған жағдайда, шығыс деректерінің ұзындығы өзгеріссіз қалады.

Криптографиялық қосымшаларда хеш функцияларына бірқатар талаптар қойылады, ол талаптар мақалада сипатталған. Белгілі бір талаптар мен қасиеттердің болуымен қатар, әртүрлі елдерде хеш-функциялары үшін ақпаратты криптографиялық қорғаудың ұлттық стандарттары бар. Мақалада қазіргі қауіпсіздік жағдай мен криптографиялық хеш-функцияларының құрылымына жасалған талдау ұсынылады. Криптографиялық хеш-функцияларының алгоритмдерін тәжірибеде қолдану және оларды әртүрлі платформаларда жүзеге асыру нәтижелері келтірілген. Көптеген бағдарламалау тілдерінде, сондай-ақ серверлік тілдерде хеш-функцияны стандартты алгоритмдерді қолдана отырып, оңай есептейтін арнайы класстар мен функциялар пайдаланылады. Хештеу алгоритмдері жүйелік, объектіге бағытталған, веб-қосымшаларда, дерекқорды басқару жүйелерінде, мұрағаттауда, блокчейн технологиясында және криптовалюталарда қолданылады. Қолдану салалары бойынша хеш-функцияларды пайдалану ерекшеліктері көрсетілген.

Түйінді сөздер: мәліметтерді қорғау, хеш функция, криптография, хештеу алгоритмдері, ақпараттық қауіпсіздік.

Ussatova O.[1,2], Begimbayeva Ye.[1,2], Nyssanbayeva S.[1], Ussatov N.[3]

[1]Institute of Information and Computational Technologies CS MES RK, Almaty, Kazakhstan;
[2]Kazakh National University named after al-Farabi, Almaty, Kazakhstan;
[3]«Turan» University, Almaty, Kazakhstan.
E-mail: uoa_olga@mail.ru

ANALYSIS OF METHODS AND PRACTICAL APPLICATION OF HASH FUNCTIONS

Abstract. Today, the field of application of hash functions is extremely broad. Hash functions are successfully used in solving problems of protecting computer information, including the authentication of subjects and objects of information interaction before introducing uncertainty into the operation of the means and objects of protection.In recent years, there has been an extraordinary increase in the need for secure hash functions. In addition, hashing functions plays a special and central role in modern cryptography. Cryptographic hash functions can also be used to protect against falsification of transmitted information. There are a large number of hashing algorithms that differ in cryptographic strength, complexity, bit depth, and other properties. A cryptographic hash function is a mathematical algorithm that converts an arbitrary length of input data into a fixed length of output bit string.Regardless of the amount of the input data, provided that the same type of hash is used, the length will remain unchanged.

In cryptographic applications, hashing functions have a number of requirements that are described in the article.In addition to the existence of certain requirements and properties, different countries have national standards for the cryptographic protection of information for hash functions.The article an analysis of the current state of security and structures of cryptographic hash functions are proposes.The results of practical application of algorithms for cryptographic hash functions and their implementation on various platforms are presented.Many programming languages, as well as server-side languages, use special classes and functions that calculate the hash function without difficulty, and at the same time use standard algorithms.Hashing algorithms are used in system, object-oriented, web applications, database management systems, archiving, blockchain technology and cryptocurrencies. The features of the use of hash functions by areas of application are shown.

Key words*:* data protection, hash function, cryptography, hashing algorithms, information security.

Information about authors:

Ussatova Olga – PhD, Senior Researcher, Institute of Information and Computing Technologies, Kazakh National University named after al-Farabi, Kazakhstan. uoa_olga@mail.ru, https://orcid.org/0000-0002-5276-6118;

Begimbayeva Yenlik – PhD, Senior Researcher, Institute of Information and Computing Technologies, Kazakh National University named after al-Farabi, Kazakhstan. enlik_89@mail.ru, https://orcid.org/0000-0002-4907-3345;

Nyssanbayeva Saule – Doctor of technical science, Chief Researcher, Institute of Information and Computing Technologies, Kazakhstan. sultasha1@mail.ru, https://orcid.org/0000-0002-5835-4958;

Ussatov Nikita – student, University «Turan», Almaty. usatov.nikita2242@gmail.com, *https://orcid.org/0000-0002-5034-0682*.

ЛИТЕРАТУРА

[1] Международный стандарт ИСО/МЭК 14888-1-2008 «Информационная технология. Методы защиты. Цифровые подписи с приложением» [электронный ресурс]. URL https://www.iso.org/obp/ui/#iso:std:iso-iec:14888:-1:ed-2:v1:en (06.07.2021).

[2] Ivan Damgaard. Collision Free Hash Functions and Public Key Signature Schemes. In Eurocrypt ‘87, volume 304 of LNCS, p. 203-216. Springer-Verlag, 1987.

[3] Alfred Menezes, Paul Oorschot, and Scott Vanstone. Handbook of Applied Cryptography, chapter Hash Functions and Data Integrity, pages 321{384. CRCPress, 1996. 6, 27.

[4] John Kelsey and Tadayoshi Kohno. Herding Hash Functions and the Nostradamus Attack. In Eurocrypt ‘06, volume 4004 of LNCS, p. 183-200. Springer-Verlag, 2006.

[5] Kim, Dong-Chan; Hong, Deukjo; Lee, Jung-Keun; Kim, Woo-Hwan; Kwon, Daesung (2015). LSH:

A New Fast Secure Hash Function Family. Springer International Publishing. pp. 286–313. ISBN 978-3-319-15943-0.

[6] X 5057-2:2003 (ISO/IEC 10118-2:2000) *http://kikakurui.com/x5/X5057-2-2003-01.html* [электронный ресурс]. URL*http://kikakurui.com/x5/X5057-2-2003-01.html (05.02.2021)*.

[7] Sakshar Law Associates Explained: Anti Encryption Laws in India [электронный ресурс]. URL https: //www.lexology.com/library/detail.aspx?g = af33ffb9-66b8-4d04-a9ff-0c5a4668a5fd #:~:text = Securit (06.07.2021).

[8] Chinese National Standard List: Data encryption [электронный ресурс]. URL *http://www.codeofchina.com/national_list/L80.html.ies%20and%20Exchange%20Board%20of,all%20transactions%20and%20online%20trading (16.07.2021)*.

[9] Whiteld Die and Martin Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6):644-654, 1976.

[10] Vlastimil Klima. Tunnels in Hash Functions: MD5 Collisions Within a Minute. Cryptology e Print Archive, Report 2006/105, 2006 [электронный ресурс]. URL eprint.iacr.org/2006/105 (16.07.2021).

[11] Roshdy R., Fouad M., Aboul-Dahab M. Design and implementation a new security hash algorithm based on MD5 and SHA-256 // International Journal of Engineering Sciences & Emerging Technologies, 2013. Volume 6, Issue 1, pp: 29-36.

[12] Wang X., Yu H., "How to Break MD5 and Other Hash Functions", Advances in Cryptology, proceedings of EUROCRYPT 2005, Lecture Notes in Computer Science 3494, pp. 19–35, 2005.

[13] Rivest R.L. The MD5 Message Digest Algorithm. RFC 1321, 1992.

[14] Lamberger M. and Mendel F., "Higher-order differential attack on reduced SHA-256", Cryptology ePrint Archive, Report 2011/037, 2011.

[15] Sasaki Y., Wang L., and Aoki K., "Preimage Attacks on 41-Step SHA-256 and 46-Step SHA-512", IACR Cryptology e Print Archive, Vol. 2009.

[16] Mirvaziri H., Jumari K. and Ismail M. "A new Hash Function Based on Combination of Existing Digest Algorithms", The 5th Student Conference on Research and Development, SCOReD 2007, December 2007.

[17] kasgar A., Agrawal J. and Sahu S. "New Modified 256-bit MD5 Algorithm with SHA Compression Function", International Journal of Computer Applications (0975 – 8887), Vol.42, No.12, March 2012. [10] NIST, "Secure Hash Standard (SHS)", FIPS PUB 180-2, 2002.

[18] Kioon M.C., Wang Z.S., Shubra D.D. Security Analysis of MD5 Algorithm in Password Storage // Scientific.Net. 2013. C. 2706-2711.

[19] Baisholan N., Kubayev K.E., Baisholanov T.S. Modern tools for information security systems // News of the National Academy of sciences of the Republic of Kazakhstan, Phy.-Math ser., Volume 1, Number 335 (2021), 14 – 18 https://doi.org/10.32014/2021.2518-1726.2.

[20] Begimbayeva Yenlik, Ussatova Olga, Biyashev Rustem, Nyssanbayeva Saule «Development of an automated system model of information protection in the cross-border exchange» // Cogent Engineering Journal, Birmingham, UK, №7, 2020 г. ISSN: 2331-1916, P.1-13.https://doi.org/10.1080/23311916.2020.1724597.

REFERENCES

[1] International standard ISO / IEC 14888-1-2008 "Information technology. Protection methods. Digital signatures with an application" [Electronic resource]. URL https://www.iso.org/obp/ui/#iso:std:iso-iec:14888:-1:ed-2:v1:en (06.07.2021).

[2] Ivan Damgaard. Collision Free Hash Functions and Public Key Signature Schemes. In Eurocrypt '87, volume 304 of LNCS, p. 203-216. Springer-Verlag, 1987.

[3] Alfred Menezes, Paul Oorschot, and Scott Vanstone. Handbook of Applied Cryptography, chapter Hash Functions and Data Integrity, pages 321-384. CRC Press, 1996. 6, 27.

[4] John Kelsey and Tadayoshi Kohno. Herding Hash Functions and the Nostradamus Attack. In Eurocrypt '06, volume 4004 of LNCS, p. 183-200. Springer-Verlag, 2006.

[5] Kim, Dong-Chan; Hong, Deukjo; Lee, Jung-Keun; Kim, Woo-Hwan; Kwon, Daesung (2015). LSH: A New Fast Secure Hash Function Family. Springer International Publishing. pp. 286–313. ISBN 978-3-319-15943-0.

[6] X 5057-2:2003 (ISO/IEC 10118-2:2000) [Electronic resource]. URL *http: //kikakurui.com/x5/X5057-2-2003-01. html (05.02.2021)*.

[7] Sakshar Law Associates Explained: Anti Encryption Laws in India [Electronic resource]. URL, https: //www.lexology.com /library /detail.aspx?g = af33ffb9 - 66b8 - 4d04 - a9ff - 0c5a4668a5fd#:~:text = Securit (06.07.2021).

[8] Chinese National Standard List: Data encryption [Electronic resource]. URL *http://www.codeofchina.com/national_list/L80.html.ies%20and%20Exchange%20Board%20of,all%20transactions%20and%20online%20trading (16.07.2021)*.

[9] Whiteld Die and Martin Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6):644-654, 1976.

[10] Vlastimil Klima. Tunnels in Hash Functions: MD5 Collisions Within a Minute. Cryptology ePrint Archive, Report 2006/105, 2006 [Electronic resource]. URL eprint.iacr.org/2006/105 (16.07.2021).

[11] Roshdy R., Fouad M., Aboul-Dahab M. Design and implementation a new security hash algorithm based on MD5 and SHA-256 // International Journal of Engineering Sciences & Emerging Technologies, 2013. Volume 6, Issue 1, pp: 29-36.

[12] Wang X., Yu H., "How to Break MD5 and Other Hash Functions", Advances in Cryptology, proceedings of EUROCRYPT 2005, Lecture Notes in Computer Science 3494, pp. 19–35, 2005.

[13] Rivest R.L.The MD5 Message Digest Algorithm. RFC 1321, 1992.

[14] Lamberger M. and Mendel F., "Higher-order differential attack on reduced SHA-256", Cryptology e Print Archive, Report 2011/037, 2011.

[15] Sasaki Y., Wang L., and Aoki K., "Preimage Attacks on 41-Step SHA-256 and 46-Step SHA-512", IACR Cryptology e Print Archive, Vol. 2009.

[16] Mirvaziri H., Jumari K. and Ismail M. "A new Hash Function Based on Combination of Existing Digest Algorithms", The 5th Student Conference on Research and Development, SCOReD 2007, December 2007.

[17] Kasgar A., Agrawal J. and Sahu S. "New Modified 256-bit MD5 Algorithm with SHA Compression Function", International Journal of Computer Applications (0975 – 8887), Vol.42, No.12, March 2012. [10] NIST, "Secure Hash Standard (SHS)", FIPS PUB 180-2, 2002.

[18] Kioon M.C., Wang Z.S., Shubra D.D. Security Analysis of MD5 Algorithm in Password Storage // Scientific. Net. 2013. C. 2706-2711.

[19] Baisholan N., Kubayev K.E., Baisholanov T.S. Modern tools for information security systems // News of the National Academy of sciences of the Republic of Kazakhstan, Phy.-Math ser., Volume 1, Number 335 (2021), 14 – 18 https://doi.org/10.32014/2021.2518-1726.2.

[20] Begimbayeva Yenlik, Ussatova Olga, Biyashev Rustem, Nyssanbayeva Saule «Development of an automated system model of information protection in the cross-border exchange» // Cogent Engineering Journal, Birmingham, UK, №7, 2020 г. ISSN: 2331-1916, P.1-13.https://doi.org/10.1080/23311916.2020.1724597.

МАЗМҰНЫ

ФИЗИКА

ИНФОРМАТИКА

МАТЕМАТИКА

СОДЕРЖАНИЕ

ФИЗИКА

ИНФОРМАТИКА

МАТЕМАТИКА

CONTENTS

PHYSICS

COMPUTER SCIENCE

MATHEMATICS

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 15.10.2021.
Формат 60x881/8. Бумага офсетная. Печать –ризограф.
4,6 п.л. Тираж 300. Заказ 5.

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