© Borysenko O., Horiachev O., Serdiuk V., Yermakov M. Protection of information based on factorial numbers // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 3, pp. 169-174.

DOI: 10.18372/2225-5036.24.13069

ФАКТОРИАЛЬНЫЕ ЧИСЛА В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

Алексей Борисенко, Алексей Горячев, Виктор Сердюк, Максим Ермаков

Сумский государственный университет, Украина

БОРИСЕНКО Алексей Андреевич, д.т.н., профессор

Год и место рождения: 1946, Сумская область
Образование: Харьковский национальный университет радиоэлектроники
Должность: профессор кафедры электроники и компьютерной техники Сумского государственного университета
Научные интересы: теория и кодирование информации
Публикации: более 200 научных публикаций
E-mail: 5352008@ukr.net

ГОРЯЧЕВ Алексей Евгеньевич, к.т.н.

Год и место рождения: 1985 год, г. Сумы, Украина
Образование: Сумский государственный университет, 2007 год
Должность: Старший преподаватель кафедры электроники и компьютерной техники Сумского государственного университета
Научные интересы: кодирование информации
Публикации: более 50 научных публикаций
E-mail: alevgor@gmail.com

СЕРДЮК Виктор Васильевич

Год и место рождения: 1995 год, г. Сумы, Украина
Образование: Сумский государственный университет, 2017 год
Должность: Аспирант кафедры электроники и компьютерной техники Сумского государственного университета
Научные интересы: теория и кодирование информации
E-mail: viktman2012@gmail.com

ЕРМАКОВ Максим Сергеевич

Год и место рождения: 1998 год, г. Белополье, Сумская обл., Украина
Образование: Сумский государственный университет
Должность: Студент кафедры электроники и компьютерной техники Сумского государственного университета
Научные интересы: теория и кодирование информации
E-mail: ermakov.maksim@gmail.com

Аннотация. *В статье рассматривается метод защиты данных на перестановках для одновременной защиты данных от несанкционированного доступа и помех, использующий в качестве промежуточного носителя информации факториальные числа. Они формируют промежуточный шаги преобразования исходных сообщений в перестановки. При этом время генерирования перестановок по сравнению с другими методами генерирования перестановок уменьшается, а реализация соответствующих алгоритмов и устройств упрощается.*

Ключевые слова: *защита информации, шифр, перестановки, системы счисления, факториальные числа, , помехоустойчивое кодирование, статистика.*

Введение

В классических задачах защиты информации одним из основных вопросов является снижение влияния на шифры статистики символов исходных сообщений. Для этого достаточно часто применяются перемешивание входящих в них символов или их групп [1-5]. Существуют также методы, снижающие статистику символов сообщений путем преобразования последних в другие сообщения, в которых исходная статистика в определенной мере выравнивается [5]. В результате скрывается исходная информация и устраняется, хотя бы частично, влияние на зашифрованные сообщения статистика символов, которая может быть использована для вскрытия шифров.

Идя по этому пути, Шеннон предложил концепцию построения идеальных шифров, путем устранения с них избыточности, а с ней и статистики символов, что приводит к равной вероятности символов в сообщениях и взаимной их независимости. Он писал: «Для того, чтобы приблизиться к идеальной ненадежности можно преобразовать сообщения с помощью устройств, которые устраняют эту избыточность. После этого достаточно применить любой шифр – подстановку, транспозицию, шифр Виженера и т. д.» [5, стр. 383].

К таким методам построения шифров, близких к идеальным шифрам, относятся методы, основанные на сжатии исходных сообщений. В них после сжатия появляются новые символы с распределением вероятностей близким к равновероятному распределению. Но в этом случае требуется применение методов сжатия сообщений, снижающие быстродействие шифрования, которые к тому ж вследствие отсутствия избыточности в сжатых сообщениях не защищены от воздействия помех. Аппаратурная реализация методов сжатия также не всегда достаточно эффективна как с точки зрения разработки аппаратуры, так и ее помехозащищенности.

Задача работы

Поэтому наряду с методами сжатия шифруемых сообщений следует рассмотреть и другие методы их защиты, обеспечивающие статистику получаемых символов близкую к равновероятной статистике. При этом важно, чтобы искомый метод шифрования давал возможность обнаруживать ошибки в шифрах и соответственно позволял строить помехоустойчивые шифры. Кроме того, он должен обеспечить достаточное быстродействие шифрования сообщений. Поиск такого метода и составляет задачу данной статьи.

Таким образом, задачей статьи является разработка метода получения помехоустойчивого шифра близкого к идеальному шифру с достаточным для решаемых практических задач быстродействием его работы.

Идея работы

В данной работе для решения указанной задачи избран подход, состоящий в преобразовании исходных сообщений в перестановки. В нем каждому шифруемому сообщению ставится в соответствие перестановка, состоящая из n элементов, которые по определению встречаются в ней один раз. Эти элементы представляются номерами 1, 2, …, n. Тогда, например, для n = 3 будет получено 6 перестановок: 123, 132, 213, 231, 312, 321, содержащих по 3 элементы. При шифровании сообщений элементы перестановок 1, 2, 3 преобразуются в соответствующие им двоичные номера 001, 010, 011. В результате перестановки преобразуются в двоично-кодированные формы 001 010 011, …, 011 010 001. каждая из которых кодирует одно из 6 шифруемых сообщений. Минимальная длина этих сообщений равна 3 битам, а максимальная теоретически не ограничена.

Если нужно зашифровать 100 различных двоичных сообщений любой длины, то следует взять перестановки, содержащие n = 5 элементов, так как тогда их количество 5! = 1×2×3×4×5 = 120 будет больше 100, что дает возможность преобразовать каждое из сообщений в одну из 120 двоично-кодированных перестановок. В этом случае каждая из 100 перестановок будет содержать 5 × 3 = 15 бит двоичной информации. Минимальная длина шифруемых сообщений при этом, очевидно, будет равна 7 битам. Поэтому избыточность перестановок, взятая по отношению к этой длине, составит 8 бит. Она может быть использована для обнаружения и исправления ошибок в перестановках, а значит и в зашифрованных сообщениях.

Однако избыточность реальных исходных сообщений может быть значительно больше избыточности перестановок и тогда для преобразования ее в перестановки потребуется уменьшить избыточность путем сжатия до минимальной величины. Можно пойти и по другому пути, разбивая исходные шифруемые двоичные сообщения на участки, соответствующие минимальной длине, и каждый раз представляя их перестановками. Однако в последнем случае исходная избыточность шифруемых сообщений никуда не исчезает и соответственно облегчает дешифрацию зашифрованных сообщений. Только в случае минимальной длины шифруемых двоичных последовательностей можно гарантировано прийти к шифру близкому к идеальному.

Однако и без сжатия шифры на перестановках будут обладать большей стойкостью, чем обычные шифры, в силу сложности получения статистики шифруемых сообщений и соответствующих им перестановок. Поэтому на практике можно использовать два методы построения шифров на перестановках: с минимальной длиной и без нее. В первом случае шифрование будет ближе к идеальному, но потребует большего времени и аппаратных и программных ресурсов, а во втором менее затратное, но есть риск раскрытия шифра из-за избыточности шифруемых сообщений и появления из-за этого статистики перестановок и их элементов. Однако этот риск значительно меньше, чем при шифровании обычными методами, в которых присутствует статистика символов. В любом случае шифры будут помехоустойчивыми, что придает им новый качественный эффект, который отсутствует в большинстве известных шифров.

Очевидно, что исходная статистика, которая присутствует в двоичных шифруемых сообщениях, может проявиться в статистике непосредственно перестановок. Но ее, получить значительно сложнее, чем статистику символов, в силу того, что количество перестановок при n равном или большем 5 значительно превосходит их алфавит. Чтобы заметить ее проявление, необходим статистический анализ элементов большого количества перестановок, число которых будет сильно увеличиваться с ростом длины сообщений. Правда, всегда могут появиться устойчивые и поэтому часто встречаемые словосочетания, которые могут облегчить вскрытие шифра. Такие словосочетания надо учитывать при построении рассматриваемых шифров на перестановках.

Но в любом случае статистика символов защищаемых сообщений практически не влияет на эффективность шифров на длинных перестановках. В них элементы формируются независимо друг от друга и при шифрах длины уже более 30 элементов (150 бит) их вероятности можно принять равными между собой. В результате могут быть получены шифры близкие к идеальным шифрам.

Однако если для шифрования используется только алгоритм преобразования исходного сообщения в перестановку, то такая перестановка еще не представляет шифра, так как для восстановления сообщения достаточно будет перейти от перестановки к исходному сообщению, что при известном алгоритме преобразования решается довольно просто. Поэтому нужен еще ключ, который собственно и образует в конечном итоге шифр на перестановках.

Разработка такого ключа не представляет особой трудности, так как практически любой классический шифр можно получить на перестановках, как на обычных сообщениях, например, шифр Цезаря. Но в большинстве случаев в таких шифрах нет необходимости, так как многие из них создавались с целью рассеяния статистики символов, а в данном случае эта статистика устраняется изначально при преобразовании шифруемого сообщения в перестановку.

В качестве ключей на перестановках можно использовать перестановки всех, или некоторых их элементов, выбираемых по определенным правилам из исходной перестановки, полученной в результате преобразования в нее шифруемого сообщения. Это позволяет уже при небольших длинах исходных перестановок, получаемых из шифруемых сообщений, например, длиной в 30 элементов (150 бит), образовывать шифры, практически не раскрываемые простым перебором ключей, так как в этом случае их количество будет примерно равно 30! [6]. Перебрать такое количество ключей сегодня на обычных ЭВМ практически невозможно. При этом нужно учесть, что для каждого перебираемого ключа нужно еще перейти от перестановки к генерируемому им сообщению. В результате процедура раскрытия шифра существенно усложняется. Это значит, что предлагаемый метод шифрования позволяет строить довольно надежные даже по современным меркам шифры. Следует отметить, что речь идет не о каком-то одном конкретном шифре на перестановках, а о возможности построения множества различных шифров со своими ключами.

Достоинством данного метода защиты, кроме высокой стойкости порождаемых им шифров, является также еще и то, что он одновременно позволяет совместить шифрование с помощью перестановок с помехоустойчивым кодированием. Благодаря своей помехоустойчивости перестановки относительно легко обнаруживают и исправляют ошибки в передаваемых с их помощью сообщениях, что в ряде случаев не менее важно, чем защита непосредственно сообщений от нежелательного доступа. Такое помехоустойчивое кодирование с помощью перестановок уже применялось ранее, однако оно не совмещалось с шифрованием информации [7].

Помехоустойчивость перестановок связана с тем, что они содержат структурную избыточную информацию, вызванную отсутствия повторяемости ее элементов. Поэтому эта избыточность другой природы, чем избыточность, содержащаяся в шифруемых сообщениях, связанная со статистической избыточностью символов исходных сообщений, которая автоматически исчезает при их преобразовании в перестановки. Учитывая, что большинство существующих шифров не могут это делать, то этот факт является немаловажным достоинством предлагаемого метода построения шифров на перестановках.

Однако статистика непосредственно самих сообщений все же проявляется в соответствующей статистике перестановок и их элементов, что может помочь в раскрытии шифра. Чтобы окончательно исключить и эту возможность дешифрации нужно предварительно перед преобразованием шифруемых сообщений в перестановки произвести их сжатие. Только тогда можно говорить о идеальных шифрах на перестановках.

Шифрование преобразованием в перестановки

Идеальные шифры на перестановках нельзя получить без алгоритмов перевода в них шифруемых сообщений. Небольшие сообщения позволяют организовать их перевод в перестановки с помощью таблиц соответствия, но при этом в силу малой длины перестановок образуются статистические связи между ними и сообщениями, что облегчает их дешифрацию. Эти связи уменьшаются при увеличении количества шифруемых сообщений, но тогда их преобразование в перестановки с помощью таблиц становится затруднительным из-за большой требуемой емкости памяти. Поэтому для преобразования длинных сообщений в соответствующие перестановки потребовался специальный метод преобразования. Причем он должен быть регулярным и в достаточной мере быстродействующим, иначе эффективность шифров будет падать.

Существует ряд методов построения перестановок с регулярной структурой, среди которых имеется поиск с возвращением, вложенных циклов, транспозиции смежных элементов [12]. В этих методах используются непосредственно действия над элементами перестановок, в результате чего одни

перестановки преобразуется в другие. Эти методы обладают невысокой скоростью порождения перестановок, снижающейся с ростом числа содержащихся в них элементов.

Главный недостаток этих методов, что они не преобразовывают напрямую исходные сообщения в перестановки, так как могут только их перебирать или порождать случайным образом. Из-за этого на сегодня продолжается поиск быстрых алгоритмов преобразования сообщений в перестановки.

Таким методом формирования перестановок, предложенный авторами, есть метод их порождения с помощью факториальных чисел [8, 9, 12]. Их особенность состоит в том, что они имеют структуру, соответствующую структуре перестановок [8, 9].

Для получения перестановки берется исходное двоичное число и преобразовывается по специальному алгоритму в факториальное. Это первый шаг формирования перестановок. Затем на втором шаге происходит по специальному алгоритму переход от факториального числа к перестановке. Факториальные числа дают возможность не только формировать перестановки, а и выполнять над ними определенные арифметических операций, что можно применить для дальнейшего скрытия шифруемой информации [10, 11].

Поэтому разработка метода ускоренного формирования перестановок с повышенным количеством элементов на основе факториальных чисел, для защиты от помех и скрытия информации, решает поставленную в работе задачу.

Схема системы защиты информации на перестановках, формируемых факториальными числами, дана на рис. 1. Ее эффективность можно оценить на основе обобщенного критерия, одновременно анализирующего эффект от защиты сообщений и от помехоустойчивого кодирования [13].

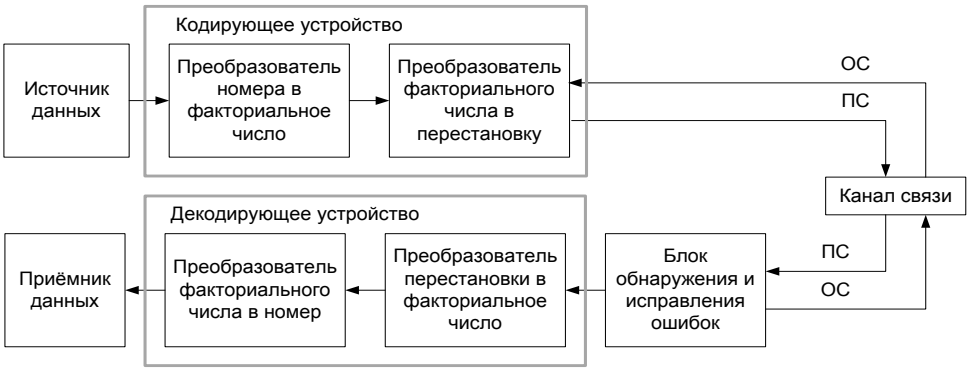

Рис. 1. Структура системы помехоустойчивой передачи и защиты данных на перестановках

Теоретические предпосылки метода

Весовыми факториальными коэффициентами в факториальных числах берутся цифры $i = 0,1, \ldots, n - 1$. Отсюда факториальная функция приобретает форму:

$$N = x_{n-1} \times (n-1)! + x_{n-2} \times (n-2)! + \ldots + x_i \times i! + \ldots + 1 \times 1! + 0 \times 0!, \quad (1)$$
$$0 \le xi \le i, \; 0 \le i \le n-1.$$

Так, факториальное число 2 3 0 1 1 0 будет записано как

$$N = 2\times5! + 3\times4! + 0\times3! + 1\times2! + 1\times1! + 0\times0! = 240 + 72 + 2 + 1 = 315.$$

Максимальная факториальная цифра в старшем разряде равна $n - 1$. Соответственно максимальное число

$$N_{\max} = (n-1)\times(n-1)! + (n-2)\times(n-2)! + \ldots + 1\times1! + 0\times0! = n! - 1, \quad (2)$$

а диапазон факториальных чисел

$$P = n! = N_{\max} + 1. \quad (3)$$

Метод получения перестановок

Метод преобразования шифруемого числа в перестановку, как отмечалось выше, состоит из 2 шагов: сначала происходит переход шифруемого числа в факториальное число и далее переход его в перестановку. Рассмотрим эти шаги по отдельности.

Переход от шифруемого сообщения к факториальному числу

Для перевода шифруемого сообщения в факториальное число оно, представленное в двоичном виде, последовательно делится на числа – 1, 2, … . После первого деления на 1 будет получен остаток 0. Частное при этом будет оставаться неизменным. Если это число равно 1, то первый разряд равен 1. Результат перевода 10. Если частное от деления на 1 больше 1, то дальше происходит деление на 2. Остаток от деления будет представлять собой цифру первого разряда, которая равна 0 или 1. Затем происходит анализ полученного частного. При его значении меньшем 3, цифра второго разряда факториального числа получена. При значении большем 3 происходит третий шаг, по которому полученное частное делится на 3. Аналогично выполняются следующие шаги. – Последний результат деления представляет собой старшую цифру.

Пример. Преобразовать десятичное число D = 50 в соответствующее факториальное число F.

Решение:

1. 50/1 = 50, остаток равен 0.
2. 50/2 = 25, остаток равен 0.
3. 25/3 = 8, остаток равен 1.
4. 8/4 = 2, остаток равен 0.

Ответ: F = 2 0 1 0 0.

Переход от факториального числа к перестановке

Переход от факториальных чисел к перестановкам имеет следующий вид. Факториальная цифра, старшего разряда записывается в перестановке без изменений в виде ее 1-го элемента. Факториальная цифра следующего разряда сравнивается в перестановке с первым ее элементом. Если она меньше его, то не меняется. Если равняется или больше, то прирастает на 1. В том и другом случае появляется второй элемент перестановки. Аналогично процедура идет далее.

Алгоритм замены факториального числа перестановкой проиллюстрирован на следующем примере.

Пример. Перевести пятиразрядное факториальное число *F* = 2 0 1 0 0 в перестановку P.

Решение:

Цифра 2 переводимого факториального числа 2 0 1 0 0 выбирается в качестве первого элемента перестановки. Следующая слева направо цифра 0 меньше ее и поэтому входит в перестановку без изменений, образуя второй элемент. Третья цифра 1 числа больше элемента перестановки 0, поэтому увеличивается на 1. Полученная при этом цифра 2 равна элементу 2, поэтому снова увеличивается на 1. Это значит, что третий элемент перестановки будет равен 3. Следующая четвертая цифра числа 0 равна предшествующему элементу 0. Соответственно ее значение будет увеличено на 1. Оно меньше полученных элементов перестановки 2 и 3. Поэтому останется неизменным, то есть 1. Последняя пятая цифра факториального числа со значением 0 будет увеличиваться до тех пор, пока не станет равной 4. На этом процедура перевода факториального числа в перестановку заканчивается.

Результат P = 2 0 3 1 4.

Оценка быстродействия метода

Предлагаемый метод получения перестановок характеризуется тем, что в нем нужно переходить от сообщений к перестановкам, а это задача значительно более сложная, чем перебор перестановок или их случайное генерирование. Поэтому в литературе практически отсутствуют методы преобразования перестановок из двоичных сообщений. Лишь в [12] говорится о существовании такого метода и дается оценка его быстродействия в виде количества операций n^2. В рассматриваемом методе количество операций будет равно $2n$, из которых n операций получено во время преобразования исходного шифруемого сообщения в факториальное число во время деления на основания. Еще n операций будет получено в процессе перехода от факториального числа к перестановке. Тогда можно сделать вывод, что предлагаемый метод более быстродействующий по сравнению с предложенным в [12] в $n/2$ раза.

Перспективы развитие метода шифрования на перестановках

Рассмотренная в статье факториальная система счисления порождает все возможные перестановки. Но могут быть получены и другие, более сложные факториальные системы счисления, порождающие факториальные числа с более сложной структурой, которые дадут возможность на их основе строить перестановки с ограничениями, то есть получать только часть из общего количества перестановок. Тем самым появится возможность усложнить шифры и сделать их более стойкими и помехоустойчивыми.

Выводы

Предложенные в работе алгоритмы преобразования шифруемых сообщений в перестановки на базе факториальных систем счисления позволяют их применять для построения как известных, так и новых более эффективных шифров, обладающих высокой стойкостью и хорошей помехоустойчивостью. Они также относительно легко реализуются в виде помехоустойчивых цифровых устройств с однородной структурой. Наиболее близко к идеальным шифрам подходят шифры с преобразованием исходных сообщений в перестановки, использующие предварительное сжатие исходных сообщений. Однако их применение на практике усложняет шифры, делая их более дорогими.

Литература

[1]. R. Girija, H. Singh, "A new substitution-permutation network cipher using Walsh Hadamard Transform", I*nternational Conference on Computing and Communication Technologies for Smart Nation (IC3TSN),* pp. 168-172, 2017.

[2]. A. Aryal, S. Imaizumi, T. Horiuchi, H. Kiya, "Integrated algorithm for block-permutation-based encryption with reversible data hiding", *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC),* pp. 203-208, 2017.

[3]. D. Smith, R. Montemanni, "A new table of permutation code", *Designs, Codes and Cryptography*, vol. 63, pp. 241-253, 2012.

[4]. I. Janiszczak, R. Staszewski, *An improved bound for permutation arrays of length 10*. [Electronic resource]. Online: http:// www. iem. uni-due. de/ preprints/IJRS.pdf

[5]. К. Шеннон, *Работы по теории информации и кибернетике*, М.: Иностранная литература, 1963, 832 с.

[6]. В. Столлингс, *Криптография и защита сетей: принципы и практика*, 2-е изд. М.: Вильямс, 2001, 672 с.

[7]. А. Борисенко, А. Горячев, М. Ермаков, Я. Ярошенко, Б. Артюх, "Формирование помехоустойчивых перестановочных кодов на основе факториальных чисел", *II Міжнародна конференція "Комп'ютерна алгебра та інформаційні технології", CAIT-Odessa-2018*, С. 129-132.

[8]. А. Горячев, "Обнаружение ошибок в перестановках", *Вісник СумДУ. Технічні науки*, №3, С. 169-174, 2009.

[9]. А. Борисенко, А. Горячев, Е. Онанченко, "Обнаружение и исправление ошибок в перестановках", *Міжнародна науково-практична конференція "Інформаційні технології та комп'ютерна інженерія"*, Вінниця: ВНТУ, С. 348-349, 2010.

[10]. О. Борисенко, І. Кулик, О. Горячев, "Електронна система генерації перестановок на базі факторіальних чисел", *Вісник СумДУ. Технічні науки*, №1, С. 183-188, 2007.

[11]. A. Borisenko, V. Kalashnikov, I. Kulik, A. Goryachev, "Generation of Permutations Based Upon Factorial Numbers", *Eighth International Conference on Intelligent Systems Design and Applications*. Kaohiung, Taiwan, pp. 57-61, 2008.

[12]. Ю. Рейнгольд, Н. Део, *Комбинаторные алгоритмы: теория и практика*, М.: Мир, 1980, 477 с.

[13]. A. Borisenko, V. Kalashnikov, N. Kalashnykova, A. Goryachev, «Chapter 11: A Generalized Criterion of Efficiency for Telecommunication Systems», M. Favorskaya, L. Jain, "Computer Vision in Advanced Control Systems Using Conventional and Intelligent Paradigms", *Springer Series: Intelligent Systems Reference Library, ISSN 1868-4394*, Springer-Verlag, Alemania, vol. 1, pp. 353-373, 2014. [Electronic resource]. Online: http://www.springer.com/series/8578Э.

УДК 621.3.037.37

Борисенко О.А., Горячев О.Є., Сердюк В.В., Єрмаков М.С. Захист інформації на основі факторіальних чисел

Анотація. *У статті розглядається метод захисту даних на перестановках для одночасного захисту даних від несанкціонованого доступу і перешкод. Пропонується кожному повідомленню ставити у відповідність перестановку, в якій елементи незалежні один від одного і при великих довжинах шифрів близькі до рівноімовірних. В цьому випадку статистика повідомлень, що захищаються, не буде впливати на шифр, що ускладнить їх дешифрування. Перевагою запропонованого методу також є те, що він дозволяє поєднувати захист інформації від несанкціонованого доступу з її перешкодостійким кодуванням. Це пояснюється тим, що перестановки містять надлишкову інформацію, яка дозволяє виявляти і виправляти помилки в повідомленнях. Запропонований метод для своєї реалізації вимагає перетворення вихідного повідомлення в відповідну йому перестановку символів. В роботі для такого перетворення використовуються факторіальні числа. Формування перестановок на основі факторіальних чисел дає можливість не тільки отримувати перестановки, а й виконувати над ними різні арифметичні операції. Зазначені перетворення роблять шифри, що розглядаються, повторюваними і однорідними, тим самим досягається однорідність і стійкість шифрувальних пристроїв. Показана структура системи передачі даних на перестановках, одержуваних за допомогою факторіальних систем числення, в якій вирішуються поставлені в роботі завдання. Перераховані основні властивості і характеристики факторіальних систем числення. Приведено докладний опис етапів методу шифрування повідомлення перестановками. Показано, що для підвищення ефективності розглянутого методу необхідно ввести спеціальний ключ, який би не залежав від алгоритму перетворення. В якості такого ключа може виступити друге факторіальне число, з яким буде складатися число, отримане після перетворення вихідного повідомлення. Якщо даний ключ буде динамічним, у вигляді псевдовипадкового факторіального числа, то розшифрувати такий шифр буде набагато складніше, особливо з ростом довжини перестановок. Таким чином, метою статті є розробка перешкодостійкого методу ідеального шифрування з достатньою для практичних завдань швидкодією роботи. Новизна роботи полягає в методі ідеального шифрування по Шеннону на основі платформи перестановок з використанням для їх отримання факторіальних чисел.*

Ключові слова: *захист інформації, перестановки, системи числення, факторіальні числа, нероздільні коди, завадостійке кодування.*

Borysenko O., Horiachev O., Serdiuk V., Yermakov M. Protection of information based on factorial numbers

Abstract. *The article discusses the method of protecting data based on permutations for the simultaneous protection of data from unauthorized access and interference. Assigning a permutation, in which the elements are independent of each other and with large cipher lengths are close to equiprobable, is proposed for each message. In this case, the statistics of the protected messages will not affect the cipher, which will complicate their decryption. Another advantage of the proposed method is possibility to combine the protection of information from unauthorized access with its noise-resistant coding. This is due to the fact that permutations contain redundant information that makes possible to detect and correct errors in the transmitted messages. For implementation of the proposed method the conversion of the original message to the corresponding permutation of characters is required. In the work factorial numbers are used for this conversion. Forming permutations based on the factorial numbers makes it possible not only to obtain permutations, but also to perform various arithmetic operations on them. These transformations make the ciphers considered repeatable and homogeneous, thereby achieving homogeneity and noise immunity of encryption devices. The structure of the data transmission system on permutations obtained using factorial number systems, in which the problems posed in the work are solved, is shown. The main properties and characteristics of factorial number systems are listed. A detailed description of the method steps for message encryption with permutations is given. It is shown that in order to increase the efficiency of the considered method, it is necessary to introduce a special key that would not depend on the transformation algorithm. Such a key can be the second factorial number that will be added to the number obtained after converting the original message. If this key is dynamic, in the form of a pseudo-random factorial number, then deciphering such a cipher will be much more difficult, especially with increasing permutation length. It is harder, especially with increasing length of permutations. Thus, the purpose of the article is to develop a noise-resistant method of perfect encryption with a high-speed operation that is sufficient for practical tasks. The novelty of the work lies in the method of perfect Shannon-based encryption based on the platform of permutations using factorial numbers to obtain them.*

Keywords: *information protection, permutations, number systems, factorial numbers, inseparable codes, error-correcting coding.*

Отримано 20 *листопада 2018 року*, затверджено редколегією *15 грудня 2018 року*