

На правах рукописи

Алхуссайн Аманн Хасн

**ВЕРОЯТНОСТНЫЙ АНАЛИЗ СТОЙКОСТИ ЗАЩИТЫ
ИНФОРМАЦИИ МЕТОДОМ ЦЕЛОЧИСЛЕННОГО
РАСЩЕПЛЕНИЯ СИМВОЛОВ**

Специальность 05.13.17 – «Теоретические основы информатики»

Автореферат

диссертации на соискание учёной степени
кандидата физико-математических наук

11 ИЮЛ 2018



008709237

Москва – 2018

Работа выполнена на кафедре информационных технологий факультета физико-математических и естественных наук федерального государственного автономного учреждения высшего образования - Российский университет дружбы народов (РУДН).

Научный руководитель: доктор технических наук,
профессор РУДН,
Институт проблем передачи информации РАН.
Стефанюк Вадим Львович

Официальные оппоненты: **Редько Владимир Георгиевич**
доктор физико-математических наук,
Федеральное государственное
учреждение «Федеральный научный
центр Научно-исследовательский
институт системных исследований
Российской академии наук» (ФГУ
ФНЦ НИИСИ РАН)

Аверкин Алексей Николаевич
кандидат физико-математических
наук, Федеральный исследовательский
центр "Информатика и управление"
РАН (ФИЦ ИУ РАН)

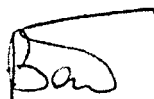
Ведущая организация: Федеральное государственное
бюджетное образовательное
учреждение высшего образования
«Тверской государственной
университет», 170100, Россия, Тверь,
ул. Желябова, 33.

Защита состоится «28» сентября 2018 г. в 15 ч. 30 мин на заседании диссертационного совета Д 212.203.28 при РУДН, расположенном по адресу: 115419, г. Москва, Орджоникидзе, д. 3, комната 110.

С диссертацией можно ознакомиться в библиотеке Российского университета дружбы народов и на официальном сайте организации

Автореферат разослан «06» 07 2018 г.

Ученый секретарь
диссертационного совета Д 212.203.28
кандидат физико-математических наук



С. А. Васильев

Общая характеристика работы

Актуальность темы диссертации. Так как в последнее время информация стала, в частности, финансовой категорией, то возникла необходимость усиления мер по её защите информации. Защита текстовой информации при передаче по каналам связи является важной задачей для бизнес-приложений и ряда других областей жизни современного общества. Исследование проблем разработки, совершенствования и применение методов и средств защиты информации в процессе передачи и хранения информации приобрело особую важность не только в государственных, дипломатических, военных сферах, но также в банковских, коммерческих и других областях, связанных с широким кругом социально-экономических проблем.

Защита текстовой информации в России имеет свою историю. Так профессиональные криптографы в России появились при Иване Грозном (1530-1584). Но в Новгороде существовала культура тайного письма с XIV века, где применяли, в основном, шифры, основанные на простой замене символов. Однако первым из российских государей, осознавшим всю важность криптографии для безопасности страны, стал Пётр I (1672—1725). Это произошло благодаря привлечению Пётром I для разработки государственного устройства России и развития образования знаменитого математика Г. В. Лейбница, задачей которого было также использование и развитие систем шифрования.

В СССР во время второй мировой войны велась разработка телефонного шифратора под руководством академика В.А. Котельникова, которому принадлежит знаменитая теорема отсчётов, лежащая в основе теории цифровой обработки сигналов.

В США К. Шеннон в 1944 г. создал основы теории секретной связи. В его работах излагается теория так называемых секретных систем, служащих, фактически, математической моделью шифров. С тех пор при разработке новых классов шифров широко используются принципы К. Шеннона рассеивания и перемешивания.

В диссертации для защиты текстовой информации предлагается воспользоваться определенным обобщением известной арифметической операции деления с остатком. Это обобщение позволяет воспользоваться аналогией с соответствующими работами К. Шеннона о стойкости¹ систем защиты. В качестве такого обобщения в диссертации предложено так называемое расщепление k -го уровня, позволяющее пользователю выбирать уровень защиты в зависимости от различных требований, предъявляемых к качеству защиты.

В работах К. Шеннона была доказана возможность метода защиты информации, обладающей свойством абсолютной стойкости, на основе метода гаммирования. Но на практике вскрылись некоторые недостатки его метода, в числе которых – необходимость использования одноразовой гаммы для каждого исходного текстового символа и необходимость указания общей длины исходного текста. Эти недостатки

¹ Термин «стойкость» – это принятый в литературе перевод термина *perfect secrecy*.

приводят, прежде всего, к сложности реализации защиты, тогда как нарушение этих требований в какой-то степени облегчает задачу злоумышленнику.

Например, абсолютно стойкий шифр, такой как алгоритм Вернама (с одноразовым блоком), является очень дорогим и непрактичным из-за условия однократности использования гаммы. Поэтому возникает необходимость создания защиты, которая возможно ли быть стойкой при менее строгих условиях.

Таким образом, изучение рассматриваемой в диссертации альтернативы в виде метода расщепления следует признать весьма актуальной задачей.

Исследование свойств предлагаемого нового метода защиты текстовой информации, чему посвящена диссертация, является актуальной задачей, возникающей как в связи с передачей по сетям связи, так и с появлением таких новых способов хранения информации, как облачная технология.

Степень разработанности темы. В основу используемого в диссертации обобщения алгоритма гаммирования были положены операции модульной арифметики, которая используются во многих известных алгоритмах, таких как метод Цезаря, Аффинная система подстановок Цезаря, метод Хилла, метод Виженера и другие методы. Однако, рассматриваемое в диссертации многократное применение операции деления нацело с остатком, ведущее к предлагаемому нами расщеплению, до настоящего времени не встречалось и не подвергалось изучению. Метод расщепления рассматривается в диссертации как один из путей повышения безопасности посредством замены каждого символа в исходном тексте на цепочку из k целых чисел. Важно отметить, что это открывает возможность выбора пользователем уровня защиты информации в зависимости от различных обстоятельств.

Согласно литературе, все известные симметричные алгоритмы, например, DES, AES, Rijndael, гаммирование, TEA, IDEA, ГОСТ28147-89, MARS, RC6, Serpent, twoFish, и др., а также ассиметричные алгоритмы, например: RSA, Рабина, Эль-Гамаль, Мак-Элиса, ГОСТ Р34.10-2001 не предусматривают возможности замены каждого передаваемого символа на строку из нескольких натуральных чисел, что требуется для повышения степени безопасности традиционных методов защиты в отношении действий интеллектуального агента, работающего в канале передачи и хранения информации. Кроме того, при этом будут скрыты сведения о длине исходного текста.

Многие из известных алгоритмов защиты данных основываются на операции деления нацело с остатком, такие как метод Цезаря, метод Виженера и другие, однако в этих методах не рассматривался вопрос многократного применения этой операции для каждого символа с целью повышения уровня безопасности и создания затруднений для анализирования передаваемых сообщений несанкционированным пользователем.

В отношении математических методов, используемых в диссертации для анализа свойств предлагаемого нового метода, следует отметить, что предлагаемый анализ является определенным развитием известных вероятностных подходов, разработанных после классических исследований К.Шеннона и других специалистов по теории информации, в таких научных учреждениях, как ИППИ РАН, ИСА РАН, ВЦ РАН, ИПУ РАН и в ряде других отечественных организаций.

Эти методы были развиты с целью обеспечения эффективного функционирования сетей и систем связи, а также обеспечения работы сложных динамических систем, в которых вставал вопрос защиты как от независимых внешних воздействий, так и от возможности вмешательства посторонних лиц и систем. В частности, вопросы защиты информации возникают в системах широкополосной мобильной коммуникации и в некоторых задачах эволюционного развития технических и биологических систем.

Среди авторов, внесших существенный вклад в эти исследования, можно отметить работы Емельянова С.В., Фомина С.В., Яблова В.В., Осипова Г.С., Редько В. Г., Стефанюк В.Л., Потапова В.Г., Алферова А.П., Зубова А.Ю., Кузьмина А.С., Черемушкина А.В., Аграновского А.В., Хаджи Р.А., Бабаша А.В., Шанкина Г.П., Баричева С.Г., Венбо Мао, Рябко Б.Я., Фионова А.Н., Червякова Н.И., Черешкина Д.С., Язенина А. В., Дудакова С. М., Аверкина А. Н., Alan G. Konheim, Menezes Alfred J., Pieprzyk J., Hardjono Th., Welsh D и др.

Цели и задачи исследования. Целью исследования в диссертации является разработка новой теоретико-методологической и практической концепции расщепления, как одной из систем защиты информации при её хранении и передаче, и получение результатов, аналогичных теореме К.Шеннона об стойкости. Достижение поставленной цели предполагает решение следующих задач:

1. Предложить новый метод – целочисленное расщепление, т.е. представление целого числа, по базе другого числа, в виде цепочки из k целых чисел (расщепление k -го уровня) и доказать необходимые строгие утверждения. Затем определить теоретическую модель защиты информации, основанную на предложенном методе расщепления.
2. Разработать метод защиты информации, позволяющий управлять уровнем защиты информации.
3. Разработать математическую модель функционирования системы защиты информации на основе расщепления, определить исходные положения самой модели и дать описание её параметров и свойств.
4. Доказать, что с ростом глубины расщепления вероятность несанкционированного восстановления символа на приёмном конце убывает по экспоненте, что позволяет говорить об асимптотической стойкости расщепления самого по себе, т.е. без использования гаммирования.
5. Показать, что процедура расщепления в значительной степени ослабляет возможность раскрытия передаваемого текста за счет учета его содержания.
6. Получить условия, при которых метод расщепления является абсолютно стойким.
7. Провести вероятностный анализ стойкости метода символического расщепления. Исследовать асимптотические свойства метода расщепления с ростом его уровня.

Научная новизна.

В процессе проведения исследований был разработан новый научный подход к защите текстовой информации и дан вероятностный анализ стойкости этого подхода:

1. Предложена новая математическая модель – целочисленное расщепление –, обобщающая известную арифметическую операцию деления с остатком (деление по модулю).
2. С учётом доказанных теорем, связанных с этой моделью, удалось построить модель системы реализующей расщепление.
3. Разработан и проанализирован новый метод защиты текста, состоящий в замене каждого символа передаваемого текста на последовательность k целых чисел (расщепление k -ого уровня). Этот метод отличается от известных способов защиты, основанных на операции модульной арифметики, тем, что он обеспечивает высокую степень безопасности, поскольку взятие модуля в системе с расщеплением делается $k-1$ раз, а не один раз, как это принято в других подходах. Важно также подчеркнуть, что параметры модуля изменяются на каждом шаге работы и, в частности, не совпадают с размером алфавита.

Теоретическая и практическая значимость работы. Теоретическая ценность полученных в диссертации результатов заключается в создании математического аппарата, основанного на использовании модульной арифметики в приложении к исследованию нового метода, названного в диссертации целочисленным расщеплением, и доказательства ряда строгих утверждений, связанных с концепцией стойкости защиты с использованием предлагаемого метода.

Метод расщепления, в силу которого целое число представляется уникальным образом в виде последовательности k целых, может иметь ценность и для других приложений, не обязательно связанных с защитой информации. В этом отношении он напоминает китайскую теорему об остатках, отличаясь от неё кардинальным образом по математическим свойствам, отмеченным в диссертации.

Практическая значимость выполненной работы обусловлена тем, что в ней построена исчерпывающая математическая схема применения метода расщепления в процессе защиты информации при её передаче и хранении, которую можно рассматривать как основу для создания действующей программной системы.

Методология и методы исследования. В диссертационной работе применяются методология и методы модульной арифметики, методы теории вероятностей и методы теории информации, связанные со стойкостью защиты информации в различных аспектах, а также методы симметричной защиты информации на основе использования генераторов псевдослучайных чисел.

Положения, выносимые на защиту.

1. Метод защиты текстовой информации путем применения целочисленного расщепления, основанного на принципах модульной арифметики, позволяющий представить целое число по базе другого целого в виде последовательности k целых чисел, построенных по определенному правилу.
2. Математическая модель указанной системы защиты текстов информации с применением генератора псевдослучайных чисел.

3. Утверждения относительно комбинаторных свойств возникающего преобразования символов и доказательство асимптотической стойкости предлагаемого метода защиты информации.

Степень достоверности и апробация результатов. Достоверность полученных в диссертации результатов вытекает из использования строгих математических методов модульной арифметики, методов теории вероятностей, методов теории информации и методов симметричной защиты информации с использованием генераторов псевдослучайных чисел.

Основные положения диссертационной работы докладывались и обсуждались: на Четырнадцатой национальной конференции по искусственному интеллекту с международным участием, Казань, 2014; На International Research Conference on Engineering, Science and Management, Dubai, 2014; На VIII Международной научной конференции «Приоритеты мировой науки: эксперимент и научная дискуссия», Южная Каролина, Северный Чарльстон, 2015; На 5й Европейской конференции по инновациям в технических и естественных науках, Австрия, Вена, 2015; На XIX Международной научно-практической конференции, Москва, 2015; На VIII Международной научно-практической конференции студентов, аспирантов и молодых учёных «Шаг в будущее: теоретические и прикладные исследования современной науки», Санкт-Петербург, 2015; На 2nd International Scientific Conference “Theoretical and Applied Sciences in the USA”, USA, New York, 2015; На First European Conference on Informational Technology and Computer Science, Austria, Vienna, 2015. На Международной научной конференции «На пути к стабильному миру: безопасность и устойчивое развитие», США, Сан-Диего, 2015; Работа автора была признана лучшей на III-й Международной летней школе-семинаре по искусственному интеллекту для студентов, аспирантов и молодых ученых “Интеллектуальные системы и технологии: современное состояние и перспективы”, Тверь, 2015;

Доклад по тематике диссертации был признан лучшим на 3rd international conference on “Engineering & Technology, Computer, Basic and Applied Sciences”, UAE, Dubai, 2016.

Другой доклад, связанный с диссертацией, был признан одним из лучших на VI Всероссийской конференции «Информационно-телекоммуникационные технологии и математическое моделирование высокотехнологичных систем», Российский университет дружбы народов, Москва, 2016.

Публикации. Основные теоретические и практические результаты диссертации опубликованы в 16 статьях и докладах, в том числе 6 работ опубликованы в рецензируемых изданиях, рекомендованных перечнем ВАК.

Соответствие паспорту специальности. Диссертационное исследование выполнено в соответствии с паспортом специальности 05.13.17 «Теоретические основы информатики» и соответствует следующим разделам паспорта специальности: п.3 (разработка и исследование моделей данных и новых принципов их проектирования), п.11 (разработка методов обеспечения высоконадежной обработки информации и обеспечения помехоустойчивости информационных коммуникаций для целей передачи, хранения и защиты информации; разработка основ теории надежности и безопасности

использования информационных технологий) и п.14 (разработка теоретических основ создания программных систем для новых информационных технологий).

Объем и структура работы. Диссертация состоит из введения, 4 глав с выводами, заключения, списка использованной литературы и приложения. Она изложена на 96 страницах машинописного текста, и включает 70 рисунка, 2 приложения, а также содержит список литературы из 173 наименований. Общий объем работы 134 страниц.

Содержание работы

Во **введении** обосновывается актуальность диссертации и перечислены основные направления исследований. Приведена общая характеристика работы. Сформулированы цель работы, решаемые задачи, определена научная новизна исследования и практическая значимость результатов.

В **первой главе** приведено описание объекта исследования, обзор проблемы и постановка задачи разработки систем защиты информации. В этой главе даются определения функции защиты информации, классы существующих систем, для которых перечисляются их основные преимущества и недостатки. Представлен обзор работ о теоретической стойкости шифров, которые были исследованы К. Шенноном, требования к таким шифрам, а также присущие им преимущества и недостатки. Кроме того, приведен обзор работ по использованию методом гаммирования и шифром Вернама, указана их применимость, перечисляются присущие им достоинства и недостатки.

Во **второй главе** объясняются теоретические основы предлагаемого в диссертации нового метода защиты информации, который получил название целочисленного расщепления. Определена математическая функция, отвечающего этому методу преобразования, и описаны ее параметры. Доказаны необходимые теоремы, связанные с этим новым методом.

Основные определения и понятия для метода целочисленного расщепления представлены в работе следующим образом:

Пусть даны два целых числа r и a , для которых выполняется неравенство $r > a > 0$.

Определение 1. Целочисленным расщеплением числа a по базе r , называется представление a в виде последовательности чисел $a_1, a_2, a_3, \dots, a_{k-1}, a_k$, в которой

$$a_1 = \delta^{(2)}, \text{ где } \delta^{(2)} = r \bmod a,$$

$$a_2 = \delta^{(3)}, \text{ где } \delta^{(3)} = r \bmod q^{(2)}, \quad q^{(2)} = \left\lfloor \frac{r}{a} \right\rfloor,$$

$$a_3 = \delta^{(4)}, \text{ где } \delta^{(4)} = r \bmod q^{(3)}, \quad q^{(3)} = \left\lfloor \frac{r}{q^{(2)}} \right\rfloor,$$

.....

$$a_{k-1} = \delta^{(k)}, \text{ где } \delta^{(k)} = r \bmod q^{(k-1)}, \quad q^{(k-1)} = \left\lfloor \frac{r}{q^{(k-2)}} \right\rfloor,$$

$$a_k = q^{(k)}, \text{ где } q^{(k)} = \left\lfloor \frac{r}{q^{(k-1)}} \right\rfloor,$$

где δ – остаток при целочисленном делении r/a , символ $\lfloor \rfloor$ означает округление до ближайшего целого в меньшую сторону, а натуральное число k назовём *уровнем расщепления*.²

Это определение является обобщением схемы математической операции деления с остатком. Блок-схема целочисленного расщепления числа a по базе r , при уровне расщепления k , показана на рис. 1.

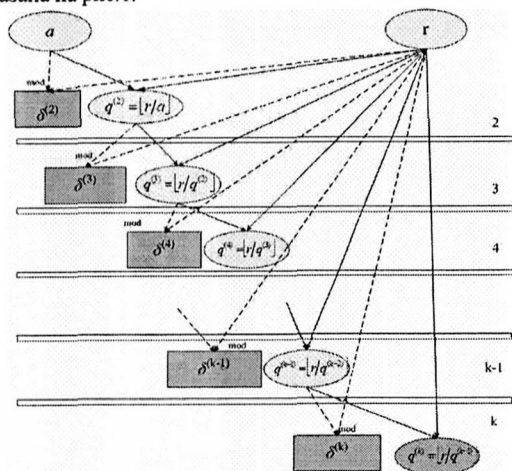


Рис. 1. Блок-схема целочисленного расщепления числа a по базе r при уровне расщепления k .

Определение 2. Функция отображения Φ_k определяется как результат целочисленного расщепления числа a по базе r , т.е. функция $\Phi_k(a)$ является отображением числа a на упорядоченную последовательность из k целых чисел $a_1, a_2, a_3, \dots, a_{k-2}, a_{k-1}, a_k$.

Тогда функция отображения $\Phi_k(a)$, при уровне расщепления равно k , задаётся следующим соотношением:

$$\Phi_k(a) = (\delta^{(2)}, \delta^{(3)}, \delta^{(4)}, \dots, \delta^{(k-1)}, \delta^{(k)}, q^{(k)}).$$

Определение 3. Расщепление по векторной базе – это обобщенное расщепление уровня k по векторной базе $\vec{r} = (r_1, r_2, \dots, r_l)$, в этом случае очередной (i -й) шаг процесса целочисленного расщепления выполняется каждый раз при новом значении базы расщепления.

Указанные выше определения позволяют сформулировать и доказать следующим теоремы:

² Отсутствие кратности r и соответствующего делителя и наличие ненулевого $q^{(i)}$ на всех этапах построения расщепления, показанного выше, гарантируется специальным дополнением к вычислениям, которое мы здесь для простоты опускаем.

Теорема 1. Целочисленное расщепление является мономорфизмом, т.е. выполняется следующее свойство: при $a \neq b \Rightarrow \Phi_k(a) \neq \Phi_k(b)$.

Теорема 2. Целочисленное расщепление является обратимым.

Теорема 3. Последовательность чисел $a_1, a_2, a_3, \dots, a_{k-1}, a_k$, возникающих при целочисленном расщеплении a , определяется единственным образом.

Доказательство приведенных выше утверждений содержится в данной главе диссертации.

В принципе, метод целочисленного расщепления, как и метод обобщенного целочисленного расщепления, весьма близок к методам эволюции, используемому в генетическом алгоритме Джона Холланда. В процессе целочисленного расщепления можно также говорить о построения новых поколений чисел, которые всё большей степени отдаляются от исходного целевого числа, что, в конечном счёте, приводит к асимптотической стойкости защиты.

Вопросу описания метода расщепления как эволюционного процесса посвящены разделы 1.9 и 2.4 диссертации, где показано, что реализация метода целочисленного расщепления по существу использует процедуру мутации, поскольку при генерации поколений применяются случайные числа.

В третьей главе рассматривается вопрос о применении целочисленного расщепления для защиты текста с заданным уровнем защиты данных. Определена математическая функция, позволяющая использовать этот метод для защиты и восстановления информации. Описана модель симметричной защиты символа и проведен вероятностный анализ стойкости предлагаемого метода.

Определение 4. Пусть r превосходить максимальное значение в выбранной кодовой таблице символов. Тогда, расщеплением уровня k для символа S с кодом a по базе r называется представление S в виде ряда целых чисел $\delta^{(2)}, \delta^{(3)}, \delta^{(4)}, \dots, \delta^{(k-1)}, \delta^{(k)}, q^{(k)}$.

Здесь число $\delta^{(i+1)}$ вычисляется по следующей формуле:

$$\delta^{(i+1)} = r \bmod q^{(i)}, \text{ где } q^{(i)} = \left\lfloor \frac{r}{q^{(i-1)}} \right\rfloor \quad (i = 2, \dots, k),$$

где число $q^{(i)}$ называется *результатом* деления нацело, а число $\delta^{(i)}$ – *остатком* от такого деления. назовём ряд целых чисел $\delta^{(2)}, \delta^{(3)}, \delta^{(4)}, \dots, \delta^{(k-1)}, \delta^{(k)}, q^{(k)}$ результатом расщепления.

Из теорем 1, 2 и 3, доказанных на главе 2, можно заключить, что если получателю известен секретный ключ, то расщепление произвольного символа S является мономорфизмом и обратимо, что открывает возможность однозначно восстановить этот символ на приёмном конце.

Метод расщепления применяется в работе к отдельным символам передаваемого текста.

В этой главе отмечается, что успех защиты символов текста зависит как от предложенного метода расщепления, так и от свойств генератора псевдослучайных чисел (ГПСЧ).

Защита текста и его восстановление происходят с помощью ГПСЧ, который считается известным и на приёмном и на передающем конце. Обычно подразумевается, что ГПСЧ представляет собой стойкий генератор псевдослучайных чисел, который создаёт непредсказуемую последовательность псевдослучайных чисел (т.е. нельзя предсказать следующий элемент гаммы) и не вызывает больших технических трудностей при технической реализации.

От источника случайных чисел (или генератора псевдослучайных чисел) поступает величина r_i , необходимая как при передаче путём расщепления, так и при восстановлении каждого символа. В результате расщепления в момент i создаются целые числа $\delta^{(2)}, \delta^{(3)}, \delta^{(4)}, \dots, \delta^{(k-1)}, \delta^{(k)}, q^{(k)}$. В нашей модели затем поступают случайные величины $r_{i,1}, r_{i,2}, \dots, r_{i,k+1}$, используемые для дополнительной защиты при передаче компонент этого символа путем гаммирования. (Предполагается, что величина $r_i > 0$ превосходит максимальное значение символов по выбранной кодовой таблице.)

Модель этапа защиты символа S с кодом a

Результат защиты при расщеплении $Y = \begin{cases} r_i \oplus a & \text{при } k=1 \\ \delta^{(2)}, \delta^{(3)}, \delta^{(4)}, \dots, \delta^{(k-1)}, \delta^{(k)}, q^{(k)} & \text{при } k>1 \end{cases}$

Результат защиты при гаммировании: $\begin{cases} \delta^{(j)} \oplus r_{i,j-1} & , \text{где } j=2,3,\dots,k \text{ при } k>1 \\ q^{(k)} \oplus r_{i,k} \end{cases}$

В диссертации приведены также методы *обобщенного расщепления*, при котором на каждом шаге формирования величин, используется новая величина $r_i > q^{(i)}$ с указанным выше свойством.

Модель этапа восстановления символа:

Результат восстановления после гаммирования $\begin{cases} \delta^{(j)} \oplus r_{i,j-1} & , \text{где } j=2,3,\dots,k \text{ при } k>1 \\ q^{(k)} \oplus r_{i,k} \end{cases}$

Результат восстановления расщеплённого символа: $\begin{cases} r_i \oplus Y & \text{при } k=1 \\ \frac{(r_i - \delta^{(j)})}{q^{(j)}} & , \text{где } j=k, k-1, \dots, 3, 2 \text{ при } k>1 \end{cases}$

Блок-схемы метода расщепления. На рис. 2.А , и рис. 2.Б показаны блок-схемы метода расщепления.

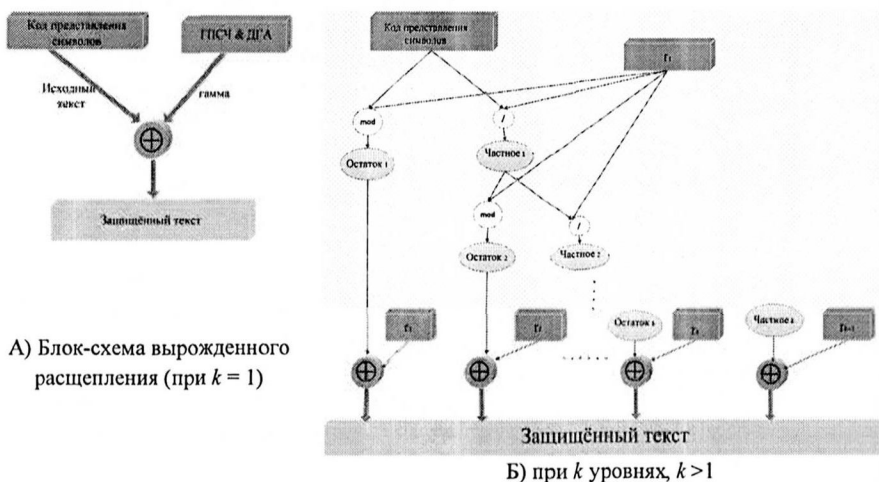


Рис.2. Блок-схема метода символического расщепления

Указанные выше определения и математические модели позволяют сформулировать и доказать следующие теоремы, связанные с вероятностным анализом математической модели символического расщепления:

Теорема 4. Элементы цепочки чисел, получаемой в случае обобщённого расщепления, в вероятностном отношении являются независимыми, при условии, что вероятностные числа \bar{r} , используемые в обобщённом расщеплении, являются независимыми.

Лемма 1. Вероятность несанкционированного восстановления символа a по результату расщепления экспоненциально быстро убывает с ростом k , согласно выражению:

$$Pr(a, k) = \frac{(N - k)!}{N!} \times \left(\frac{1}{L}\right)^{k-1}, \quad (1)$$

где N – число всех элементарных событий (исходов) в пространстве результатов расщепления, а L – число всех событий (исходов) в пространстве гаммы из случайных чисел.

Следствие 1. Из Леммы 1 следует, что вероятность несанкционированного восстановления символа a по результату расщепления экспоненциально убывает с ростом числа всех элементарных событий N в пространстве результатов расщепления, согласно выражению (1).

Следствие 2. Из Леммы 1 следует, что вероятность несанкционированного восстановления символа a по результату расщепления экспоненциально убывает с ростом числа всех событий (исходов) L в пространстве гаммы, согласно выражению (1).

Лемма 2. Вероятность несанкционированного восстановления символа a по результату обобщённого расщепления экспоненциально быстро убывает с ростом k , согласно выражению:

$$\Pr(a, k) = \frac{(N-k)!}{N!} \times \frac{(L-k-1)!}{L!}, \quad (2)$$

Где N – число всех элементарных событий в пространстве результатов обобщённого расщепления и L – размер пространства гаммы из случайных чисел.

Следствие 3. Из Леммы 2 следует, что вероятность несанкционированного восстановления символа a по результату *обобщённого расщепления* экспоненциально убывает с ростом число всех элементарных событий в пространстве результатов расщепления N , согласно выражению (2).

Следствие 4. Из Леммы 2 следует, что вероятность несанкционированного восстановления символа a по результату *обобщённого расщепления* экспоненциально убывает с ростом число всех событий (исходов) в пространстве гаммы из случайных чисел L , согласно выражению (2).

Теорема 5. Метод расщепления обладает свойством асимптотической стойкости.

Лемма 3. Метод расщепления существенно затрудняет семантическое восстановление исходного текста несанкционированным пользователем.

Приведенные выше теоремы ведут к следующему:

Следствие 5. Из Теорем 4, 5 и Леммы 3 можно сделать вывод, что защита информации методом расщепления усложнит семантическую и статистическую работу злоумышленника по сравнению с традиционными методами защиты информации, основанными на операциях модульной арифметики.

Следствие 6. Из Леммы 1 и Леммы 2 можно заключить, что, при условии $k \rightarrow \infty$, вероятность вычисления защищённого символа a при неизвестном ключе стремится к нулю. На рис. 3 показан график поведения надёжности защиты расщеплением, вытекающий из этой теоремы, т.е. вероятность несанкционированного восстановления символа при неизвестном ключе при различных значениях $k=2, 3, \dots, 8$.

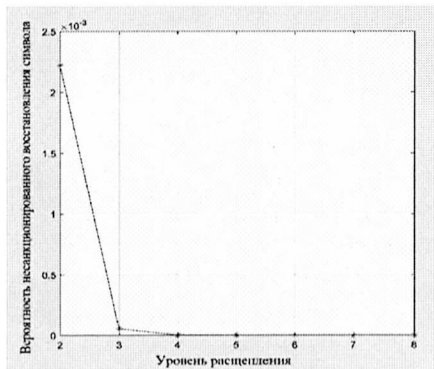


Рис. 3. Поведение вероятности несанкционированного восстановления символа при различных значениях уровней расщепления k .

Следствие 7. Пусть $\Pr(c, k)$ – вероятность результата защиты символа a расщеплением при уровне расщепления k , а величина $\Pr(c/a, k)$ – это условная вероятность возникновения защищённого текста \bar{c} если защите подвергался символ a при уровне расщепления k . Тогда из Теоремы 5 можно определить следующее соотношение: при $k \rightarrow \infty$, $\Pr(c/a, k) \approx \Pr(c, k)$, т.е. это соотношение показывает, что защищённый текст $\bar{c} = (\delta^{(2)}, \delta^{(3)}, \delta^{(4)}, \dots, \delta^{(k-1)}, \delta^{(k)}, q^{(k)})$ при уровне расщепления k не содержит для криптоаналитика никакую информацию об исходном тексте a и что метод расщепления является совершенно новым, но по смыслу полученный результат аналогичен теореме К. Шеннона об *асимптотической* стойкости.

Доказательство приведенных выше утверждений содержится в данной главе диссертации.

В четвертой главе делается сравнение метода символьного расщепления с известными схемами защиты, использующим гаммирование и со схемой Вернама, а также с указанными ранее традиционными методами защиты, применяющим операции модульной арифметики, с целью выделения достоинств предлагаемого метода защиты.

В таблице 1 представлены отличия данного метода символьного расщепления от традиционных методов защиты с использованием гаммирования и от схемы Вернама:

Таблица 1. Сравнение некоторые синхро-поточковых методов защиты с расщеплением

	Защита методом Вернама	Защита методом Гаммирования	Защита методом символьного расщепления
Период гаммы	отсутствует одноразовая гамма	имеется	существенно увеличен
Необходимость хранения гамм	Да	Нет	Нет
Необходимость доставки получателю такой же гаммы, как у отправителя	Да	Нет	Нет
Абсолютная стойкость	Да	Нет	Асимптотическая стойкость

Указанное выше сравнение позволяет сформулировать и доказать следующим теорема:

Утверждение 1. Метод расщепления решает проблему ненадёжности защиты из-за повторного использования гаммы, которая существует в поточковых методах защиты данных.

В разделе 4.3 этой главе проведено сравнение известных абсолютно стойких методов защиты с расщеплением. Есть два преимущества указанного метода символьного расщепления по сравнению с традиционными абсолютно стойкими методами защиты информации.

Первое – метод символьного расщепления является практичным и не очень дорогим по требуемым ресурсам по сравнению с другими способами обеспечения стойкости шифров, поскольку не требуется выполнения условия об использовании каждой гаммы только один раз.

Второе – метод символьного расщепления скрывает информацию о длине исходного тексте сообщения, которая определяется следующим образом: $c = k \times l$, где c – длина защищенного текста, k – уровень расщепления и l – длина исходного текста.

В разделе 4.4 отмечаются два отличия метода символьного расщепления от перечисленных традиционных методов защиты, применяющих операции модульной арифметики:

Первое – операция с применением модуля используется в традиционных методах только один раз для каждого символа. В предлагаемом методе символьного расщепления эта операция используется $k-l$ раз.

Второе – величины модулей, используемые во всех традиционных способах защиты информации (Цезарь, Вижнер, Аффинный, Хилла...), основанных на операции модульной арифметики, совпадают с размером соответствующего алфавита, тогда как в методе символьного расщепления, величина модуля изменяется на каждом шаге работы системы и не связана с общим размером алфавита. Перечисленные свойства затрудняют семантическое восстановление исходного текста несанкционированным пользователем, т.е. восстановление текста по его содержанию.

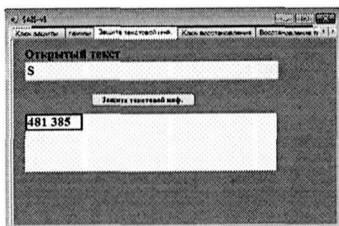
В разделе 4.5 главы представлено подробное сравнение между нашей теоремой расщепления и известной китайской теоремой об остатках, что говорит о следующем.

В отношении Китайской теоремы об остатках (КТО) следует отметить, что она используется в алгоритмах шифрования и в задачах разделённого секрета (sharing secret), основанных на использовании односторонних функций. Для вскрытия информации в таких системах требуется решения классических проблем факторизации и поиска взаимно простых чисел, на которых базируется КТО.

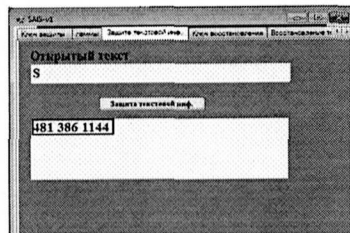
В методе расщепления, предлагаемом в диссертации, не используются взаимно простые числа, а на этапе попыток вскрытия факторизация не может быть использована в связи с особенностями предлагаемого метода.

Иллюстрацией служит пример защиты информации с использованием метода расщепления при уровне расщепления $k = 2$ показан на рис. 4.А. На этом примере видно, что защита текста расщеплением заменяет каждый символ исходного текста на два целых числа.

Если уровень расщепления $k = 3$, то мы получим защищённый текст, в котором каждый символ исходного текста заменяется на три целых числа, как показано на рис.4.Б.



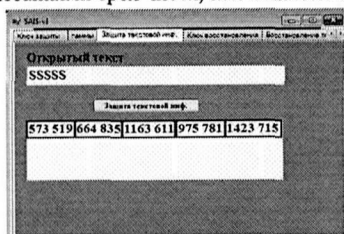
А) При уровне расщепления $k = 2$



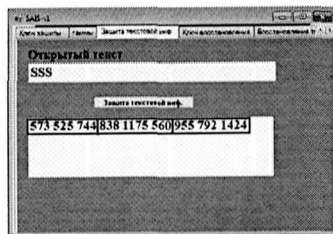
Б) При уровне расщепления $k = 3$

Рис. 4. Иллюстрация работы метода расщепления

Один символ отображается в системе с расщеплением различными сочетаниями двух чисел при $k=2$, как показано на рис. 5.А, а при $k=3$ – отображается различными сочетаниями трёх чисел, как показано на рис. 5.Б.



А) При уровне расщепления $k = 2$



Б) При уровне расщепления $k = 3$

Рис. 5. Другая иллюстрация работы метода расщепления

Если кодовая таблица символов поддерживает несколько языков, то метод работает сразу для всех этих языков.

В **заключении** к диссертации приводятся основные результаты, полученные в диссертационной работе.

Что касается приложений к диссертации, то они вызваны тем, что, как показал вероятностный анализ, проведенный в диссертации, доказательство свойств стойкости, в частности асимптотической стойкости, тесно связаны с вероятностными характеристиками вовлекаемых в рассмотрение объектов. В то же время использование генераторов псевдослучайных чисел (ГПСЧ), которое возникает в описанных в диссертации моделях использования метода расщепления при передаче и хранении текстовой информации, не гарантирует указанных выше свойств.

Известно, что только источники, использующие разнообразные физические процессы, способны порождать «истинно случайные» числа.

В **приложении А** к диссертации кратко описывается предлагаемый автором метод улучшения уровня случайности для некоторых типов генераторов псевдослучайных чисел ГПСЧ с помощью модификации генетического алгоритма, названной *детерминированным генетическим алгоритмом* (ДГА).

ДГА представляет собой эвристический алгоритм, предназначенный для улучшения вероятностных характеристик некоторых генераторов псевдослучайных

чисел. Он применялся в иллюстративных примерах, при генерации случайных чисел для гамм, используемых в методе защиты расщеплением.

В приложении В к диссертации приводятся результаты статистических тестов, которые включают частотный тест, критерий серий, коэффициент корреляции Пирсона и вычисление энтропии для трёх типов ГПСЧ. Сравнению подвергается последовательность, созданная одним из ГПСЧ без какой-либо модификации, и та же последовательность, к членам которой применяются операторы детерминированного генетического алгоритма (ДГА). Тесты осуществлялись с помощью трех пакетов программ: МАТЛАБ, Minitab и IBM SPSS Statistics.

Статистическое исследование показало, что ДГА улучшает качество случайности чисел, сгенерированных некоторыми традиционными генераторами псевдослучайных чисел (ГПСЧ) в соответствии с выбранными критериями. Эти результаты статистических тестов и сам ДГА не включены в основной состав диссертации, которая посвящена теоретическим вопросам предлагаемого в ней метода защиты информации на основе символического расщепления.

Основные результаты работы

В результате исследований были решены следующие задачи:

1. В диссертации предложен математический метод представления целого числа в виде определённой последовательности k целых чисел, названный целочисленным расщеплением.
2. Доказана единственность целочисленного расщепления и что соответствующее отображение является мономорфизмом и обратимо.
3. На основе целочисленного расщепления в диссертации предложен метод защиты информации и изучены свойства этого метода.
4. Доказано, что стойкость расщепления с ростом его глубины растёт, что позволяет говорить об асимптотической стойкости расщепления.
5. Показано, что произвольный характер порождения символов в ходе защиты затрудняет вскрытие исходного текста по его содержанию.

Публикации автора по теме диссертации

Публикации в изданиях, рекомендованных ВАК России:

1. Алхусайн А.Х. Симметричный алгоритм шифрования с помощью генетического алгоритма и генераторов псевдослучайных чисел // Естественные и технические науки .– 2015.–Т. 85, № 7.–С. 73-79.
2. Алхусайн А.Х. Детерминированный генетический алгоритм в криптографии // Естественные и технические науки .– 2016.– Т. 93, , № 3.– С.126-129.
3. Стефанюк В.Л., Алхусайн А.Х. Симметричное шифрование на основе метода расщепления // Естественные и технические науки.– 2016.– Т.93, , № 3.– С.130-133.
4. Stefanyuk V.L., Alhussain A.H. Symmetric Encryption on the Base of Splitting Method // Bulletin of PFUR, Series Mathematics. Information Sciences. Physics.– 2016.–№ 2.– P.53-61.

5. Стефанюк В.Л., Алхуссайн А.Х. Контроль степени защиты информации методом целочисленного расщепления // Искусственный интеллект и принятие решений.– 2016.– № 4.– С.86-91.
6. Алхуссайн А.Х., Стефанюк В.Л. Вероятностные свойства процедуры расщепления // Искусственный интеллект и принятие решений .– 2017.– № 3.– С.49-57.

Другие статьи и материалы конференций:

7. Стефанюк В.Л, Алхуссайн А.Х. Криптография с симметричным ключом с использованием генетического алгоритма // КИИ-2014, четырнадцатая национальная конференция по искусственному интеллекту с международным участием: РИЦ «Школа».–Казань, 2014.– Т. 1.– С. 267-275.
8. Alhussain A.H. A Literature Survey on the Usage of Genetic Algorithms in Recent cryptography Researches // International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET).–Vol.1.–Issue 3.–India, 2015.–P.22-25.
9. Alhussain A.H., Stefanuk V.L. Using deterministic genetic algorithm to increase the security level of xor encryption // VIII международной научной конференции «Приоритеты мировой науки: эксперимент и научная дискуссия.–Южная Каролина, Северный Чарльстон.– США, 2015.– С.15-18.
10. Alhussain A.H. Improving the security level of cryptographic keys of gamma cipher // VIII молодежной международной научно-практической конференции студентов, аспирантов и молодых учёных «Шаг в будущее: теоретические и прикладные исследования современной науки».– North Charleston, SC, USA, 2015.– С.12-14.
11. Alhussain A.H., Stefanuk V.L. Improvement of randomness level of pseudorandom number generators in cryptography // 2nd International Scientific Conference “Theoretical and Applied Sciences in the USA”.– New York, USA, 2015.– P. 172-177.
12. Alhussain A.H., Stefanuk V. L. Using Genetic Algorithm to improve periodic level of pseudorandom number generators // «The First European Conference on Informational Technology and Computer Science»: East West–Vienna, Austria, 2015.– P. 25-34.
13. Алхуссайн А.Х. Улучшение сгенерированного криптографического ключа с помощью генетического алгоритма // III-й Международной летней школы-семинара по искусственному интеллекту для студентов, аспирантов и молодых ученых "Интеллектуальные системы и технологии: современное состояние и перспективы" (ISyT'2015) .– Тверь, 2015.– С.107-118.
14. Alhussain A.H. A Literature Survey on the Usage of Genetic Algorithms in Key Generation // Труды конференции. The Strategies of Modern Science Development: Proceedings of the VIII International scientific–North Charleston, USA, 2015.– P. 12-14.
15. Alhussain A.H. A Literature Survey on the Usage of Genetic Algorithms in Creating New Encryption Algorithm // The Strategies of Modern Science Development: Proceedings of the VIII International scientific–North Charleston, USA, 2015.– P. 15-17.
16. Стефанюк В.Л., Алхуссайн А.Х. Криптография и кодирование как методы защиты информации // Информационно-Телекоммуникационные Технологии и Математическое моделирование высокотехнологичных систем: РУДН.– Москва,2016 .– С.181-182.

Аннотация

В диссертации предложен новый метод, названный целочисленным расщеплением, как один из способов применения модульной арифметики в области защиты информации и приведены основные определения и понятия этого метода. Описаны математические функции возникающих преобразований, исследованы их свойства и доказаны основные теоремы, оправдывающие применимость метода расщепления в задачах обеспечения стойкости защиты информации.

Определены математические функции, позволяющие использовать метод символического расщепления для защиты и восстановления информации, и описана модель симметричной защиты символа, а также проведён вероятностный анализ стойкости защиты при использовании символического расщепления.

Приведено сравнение некоторых потоковых методов защиты с расщеплением, а также сравнение известных абсолютно стойких методов защиты с расщеплением. Проведено сравнение между методами замены, основанными на операциях модульной арифметики, и методом символического расщепления. Сравнение между теоремой расщепления и китайской теоремой об остатках показано определенное преимущество использования расщепления. Кроме того, показаны, примеры иллюстрации работы теорий и метода расщепления в области защиты информации.

Abstract

In the thesis a new method, called integral splitting, is proposed, as one of the methods of applying modular arithmetic in the field of information protection, and the basic definitions and concepts of this method are presented. The mathematical functions of this method are described, their properties are investigated, and the main theorems, which justifying the applicability of the splitting method in the problems of ensuring the perfect secrecy of the information protection are proved.

The mathematical functions, which are allowing using the method of symbolic splitting to protect and restore the information, are determined, the model of symmetric symbol protection is described and a probabilistic analysis of the perfect secrecy of the mathematical model of symbolic splitting is provided.

Some of the streaming methods of protection are compared with the given splitting method, a comparison of traditional perfect secrecy methods with the proposed splitting one is presented and a comparison between the replacement protection methods based on modular arithmetic operation and the method of symbolic splitting is given. Also, the comparison between the splitting theorem and the Chinese remainder theorem shows a certain advantage of the usage of the splitting method. In addition, examples of illustrations of the splitting theories and method in the field of information protection are shown.

Подписано в печать: 04.07.2018
Объем: 1 усл.п.л.
Тираж: 150 экз. Заказ № 15
Отпечатано в типографии «Реглет»
улица Измайловский Вал, 2
(495) 971-22-77 www.reglet.ru

