Кібернетика та системний аналіз

УДК 34:004:[003.26+517.9]

И.А. Громыко, К.О. Швагер

Харьковский национальный университет имени В.Н. Каразина, Харьков

JAVA-РЕАЛИЗАЦИЯ ЭЛЕМЕНТОВ КРИПТОГРАФИИ СОПРЯЖЕННЫХ ДИСКРЕТ

Рассматривается вариант реализации элементов защиты информации в криптографии нового поколения с использованием математических средств непрерывного анализа для передачи дискрет (в линию связи) в виде широкополосных квазихаотических сигналов, подобных исследуемым профессором Кен Умено (Япония). Такие линии связи уже сегодня могут быть использованы для разработки систем конфиденциальной радио- и электросвязи крупных финансовых структур, коммуникаций подводных лодок и других заглублённых объектов (шахты, тоннели, разработка подземных и подводных рудников и месторождений нефти, правительственные и командные пункты, и пр.). Исследования достойны финансовой спонсорской помощи со стороны частных и государственных инвесторов.

Ключевые слова: *криптография, криптосигнал, криптостенография, хаотические сигналы, преобразования непрерывного анализа в криптографии.*

Введение

Постановка задачи в общем виде. Множество энциклопедических источников информации определяют термин «криптография», как тайнопись, систему изменения письма с целью сделать текст непонятным для непосвящённых лиц. При этом часто указывается, что в криптографии, используются математические методы, достижения науки и техники для криптографического преобразования открытой защищаемой информации в закрытую, затрудняющую восстановление открытой информации. Криптографическое преобразование – преобразование информации с целью сокрытия или восстановления ее содержания, подтверждение подлинности, целостности, авторства, определения факта неопровержимости, защиты от несанкционированного доступа и т.п., осуществляется с использованием специальных ключевых данных (ключа) [1].

Важно, что Клод Шеннон в своей базовой работе «Теория связи в секретных системах» не единожды подчеркнул дискретную направленность своих разработок в области криптографии. Тем самым Шеннон, продолжатель работ американского учёного-электронщика Ральфа Винтона Лайона Хартли, интеллигентно предупредил будущих продолжателей подобных исследований о некоторой ***специфической ограниченности*** данной ***работы*** [2]. Конечно, важно отметить, что его действия в то время были своевременны, весьма полезны и закономерны.

Несмотря на то, что приведенная выше информация не показывает криптографическое преобразование как исключительно дискретный процесс, в основе современной криптографии превалируют методы дискретной математики. В рамках её алгоритмов производятся замены символов на числа, которые в дальнейшем меняют местами, что порождает необходимость в реализации элементарных процедур на пределе технических и временных ресурсных возможностей вычислительной техники [3].

С одной стороны, в дискретности, начиная от материальных элементов и заканчивая цифрами, буквами алфавита (и пр.), заложена жизненная рациональность. С другой стороны, - работа с образами и интонацией сообщения, распознавание их и передача носят аналоговый характер, и по мере необходимости совмещаются с дискретными процессами квантования и оцифровки.

Информационные процессы, как правило, начинаются и завершаются работой АЦП и ЦАП - функциональных блоков устраняющих и/или восстанавливающих непрерывную аналоговую форму сигналов.

Всегда ли целесообразно ограничивать создание и обмен информацией исключительно рамками дискретного процесса?

По мнению авторов ряда работ, целесообразно использовать для криптографической защиты информации преобразования непрерывного анализа. В первую очередь подразумевается теория интегральных уравнений [3 – 8].

С функцией непрерывного аргумента простейшие выражения в аналитическом виде, например, из степеней $\boldsymbol{x}$, по смыслу эквивалентны перемещению на плоскости бесконечного множества точек. Причём без сколько-нибудь существенных затрат ма-

шинных ресурсов. Операции с функциями, с точки зрения преобразовательного эффекта, здесь могут оказаться уже сегодня весьма полезными и перспективными. Возникает очевидная необходимость преобразовать символы некоторого алфавита, обозначив их функциями аргумента ***x***, и изменив до неузнаваемости с использованием исключительно конструктивных, в этом отношении, средств непрерывного анализа [5].

Подразумевается, что семантический аспект сообщения может стать известным только получателю, которому источник сообщения санкционировал это действие, сообщив ключ, позволяющий дешифровать сообщение. Правонарушитель имеет возможность перехватить сообщение, но семантический аспект ему не доступен [9].

Анализ последних достижений и публикаций, связанных с решением данного вопроса. Известно, что семантическое сокрытие информации в настоящее время реализуется такими методами, как скремблирование, криптография и стеганография. *Скремблирование* позволяет скрывать разборчивость, различимость и интонацию речи т. е. скрывать аналоговую информацию, передаваемую по открытым каналам связи. *Криптография* скрывает смысл дискретных сообщений как при передаче по открытым каналам связи, так и при их хранении на потенциально доступных нарушителю носителях информации. *Стеганография* еще более разнообразна: она скрывает не только смысл сообщений (дискретных и аналоговых), но и факт их передачи и хранения (т. е. факт присутствия защищаемой информации). Причем при передаче информация может скрываться не только на энергетических (полевых), но и на вещественных носителях [10].

Таким образом, криптография предполагает защиту смысла информации после ее криптографического преобразования в дискретное сообщение, которое в процессе распространения по линии связи доступно многим пользователям. При этом смысл оказывается доступен только владельцу ключа.

Вместо громоздких действий с матрицами последнее время авторами стали осуществляться попытки применения так называемой интегральной криптографии, позволяющей использовать функции непрерывного аргумента, дифференцирование и интегрирование [3, 4, 8].

Здесь уместно привести следующее высказывание: «Аналитическое изображение функции очень удобно тем, что для тех элементарных символов, из которых она составляется, обычно разработаны удобные обозначения, установлены простые и часто очень наглядные, легко обозримые формальные правила, позволяющие осуществлять математические операции над ними чуть ли не автоматически» [5, 11].

Упрощённо, предлагается следующее.

Как и в классической криптографии, факт передачи сообщения известен: собственнику информации – Источнику (Отправителю), санкционированному Получателю, а также Оппоненту (Правонарушителю).

Получателю известна информация с ограниченным доступом (ИСОД) в виде ключа Отправителя, позволяющего дешифровать сообщение.

Оппонент имеет свободный доступ (с учётом Ремарки 1) к зашифрованному сообщению, но не имеет ключа.

> **Ремарка 1:** В дальнейшем мы увидим, что в некоторых случаях у Отправителя появляется возможность выбрать такие условия шифрования, что внешний вид сигнала, передаваемого в линию связи, становится приближённым по энергетическим и «видовым» характеристикам к форме сигнала, не содержащего семантический аспект. Например, вид амплитудно-модулированного сигнала при отсутствии модуляции (техническим языком, - присутствует только синусоида «несущей»). Это даёт повод оппонентам данного метода криптографии отрицать его, причисляя к классу методов стеганографии, скрывающей сам факт передачи сообщения. Однако такая ситуация рассматривается нами, как частный случай реализации Отправителем процесса шифрования, передачи в линию связи и частичным сокрытием от Оппонента.

Для передачи символа текста используются функции $f(x)$ и $\psi(x)$, олицетворяющие символ до и после шифрования.

С помощью уравнения Фредгольма первого рода выразим эти функции следующим образом:

$$(A\psi)(x) = \int_0^1 k(x, \xi)\psi(\xi)d\xi = f(x),\ x \in [0, 1], \quad (1)$$

где $k(x, \xi)$ – ядро;

$\psi(x)$ и $f(x)$ – функции, символа текста до и после шифрования.

Иначе говоря, шифрование осуществляется путем несложной, как правило, процедуры интегрирования $A\psi$. При этом функцию ψ выбираем по своему усмотрению. Ядро k предполагается замкнутым, вследствие чего решение однородного уравнения (1), когда $f \equiv 0$, может быть только тривиальным, $\psi = 0$.

Ситуация в отношении дешифрования, путем обращения интегрального оператора:

$$\psi(x) = \left(A^{-1}f\right)(x),\ x \in [0, 1], \quad (2)$$

кардинально сложнее, поскольку такая задача некорректна.

Иначе говоря, попытки определения функции ψ по формуле (2) предоставлены Оппоненту.

Суть в том, что если утечек ИСОД у Отправителя нет и ядро k криптоаналитикам Оппонента не известно, то они оказываются в трудном положении, что позволяет авторам предложенного метода говорить о «новой» криптографии [3-8].

Однако, авторам криптографии нового поколения до настоящего момента не удалось аргументированно доказать на практике ее жизнеспособность.

На научных семинарах авторам были противопоставлены многочисленные примеры бесперспективности данного направления работ: от «Пляшущих Человечков» Артура Конан Дойля до строгого математического обоснования иррациональности и невозможности аппаратурной реализации передачи информации с применением данного метода криптографии.

Несмотря на свыше сотни обращений к работам по данной тематике, изложенным авторами на научном сайте ResearchGate, после скрупулёзного трёхмесячного изучения работы, связанной с «Криптографией сопряжённых дискрет» харьковские рецензенты до настоящего времени не склонны считать целесообразным разрешить дальнейшую публикацию статей невысокого уровня и проведение научных работ в данном «аналоговом» направлении.

Поэтому, осознавая, с одной стороны, высокую степень кадрового риска аттестационного уровня и, с другой стороны, государственный уровень перспективности применения результатов в случае успешного исхода исследований (улучшение работы систем связи в условиях активного радиоэлектронного противодействия и кибератак противника или конкурента), авторы не прекратили научную деятельность в данном направлении, но были вынуждены осуществлять её во внеучебное и внерабочее время без привлечения каких-либо ресурсов государственных производственных и учебных учреждений.

Формулировка целей работы (постановка задачи). Целью данной статьи является рассмотрение одного из вариантов реализации криптографической защиты информации с использованием аналоговых методов.

Изложение основного материала исследования с обоснованием полученных научных результатов

Обратим внимание на то, что:

- аналоговый сигнал (сообщение, процесс), требующий криптографической защиты с целью его дальнейшей передачи в открытую линию связи, должен быть математически описан в виде зависимости $y = f(x)$;

- сигнал, несущий в себе сообщение, содержащее набор дискретных элементов, названных в данной работе «дискретами», по возможности должен быть также описан единой формулой, учитывающей их временны**ы**е и энергетические особенности.

В качестве примера выберем из алфавита четыре буквы и заменим их, как и у достопочтенного Клода Шеннона, отдельными дискретными элементами, но не нулями и единицами, а дискретами, отличающимися своей формой от общепринятых «буквенных» стандартов.

Изначально применим примитивное шифрование, устраняющее повторение и сочетание букв таким образом, чтобы подсчет частот ничего не дал или существенно осложнил работу криптоаналитика, занимающегося дешифровкой нашего сообщения.

Заменим символы на любые четыре дискреты из элементов непрерывных функций $y = f(x)$, приведенные на рис. 1:

Приведенные в качестве примера дискреты удобны для показа на экране монитора и передачи по линии связи в виде изменяющихся амплитуд (образов) напряжений. При этом распознавание образов дискрет и последующая их замена на буквы и цифры шрифта не составят труда.

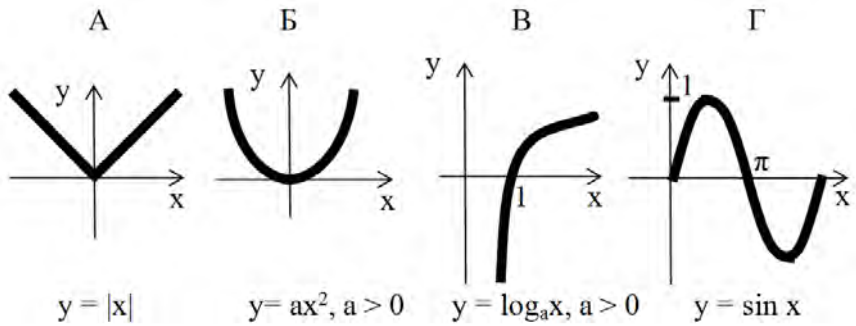

Рис. 1. Примеры графиков непрерывных функций, используемых в качестве букв алфавита

Соответственно, перемещение графиков по координатной плоскости (вправо-влево-вверх-вниз) относительно точки пересечения осей представляет собой простейшую математическую задачу.

Таким образом, наш текст отобразился в виде набора дискрет, каждая из которых имеет на координатной плоскости своё начало и свой размах (амплитудное значение) (рис. 2).

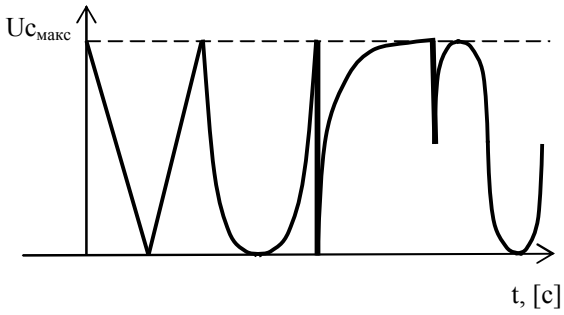

Рис. 2. Образы четырёх дискрет
на линейной оси абсцисс

Ось абсцисс X имеет аналогию с осью времени, а ось ординат Y аналогична оси таких параметров, как напряжение, мощность излучения, ток, яркость и пр.

Подобный вид шифрования, давно известен как простая замена. Он достаточно просто дешифруется путём выделения и обозначения каждого отдельного образа с последующей компьютерной обработкой повторений, сочетаний и пр.

Задача выделения каждой дискреты и последующей расшифровки текста несколько усложняется в случае преднамеренного (известного на передающей и приёмной сторонах) искажения путём изменения линейности шкал как от дискреты к дискрете, так и в процессе формирования каждого образа (рис. 3). При этом, мы не только можем изменять масштаб дискретно в момент начала формирования образа каждой дискреты, а и вмешаться в процесс формирования образа этой дискреты, изменяя масштаб по известному нам закону. И этот закон мы можем криптосигналом сообщить получателю, о чём будет сказано далее.

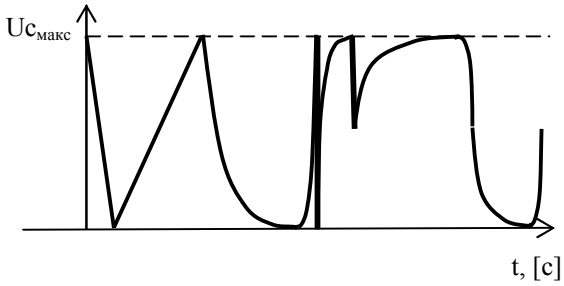

Рис. 3. Образы четырёх дискрет
на нелинейной оси абсцисс

Несмотря на искажения образов дискрет на нелинейной оси абсцисс современная вычислительная техника способна выделить отдельные дискреты, так как их характерным признаком является наличие на графиках разрывов первого или второго рода.

Если эти разрывы будут соответствовать перепадам напряжения в линии связи или мощности излучаемого сигнала, то при формировании таких перепадов спектр зашифрованного сигнала обогащается высокочастотными гармониками. А это, как минимум, демаскирует сам факт передачи, а как максимум позволяет определить периодичность следования дискрет и закономерности в искажении линейности шкал по наличию в сигнале сообщения спектра тактовой частоты.

Как известно, для определения параметров сигнала часто решают три основные задачи вычисления: тактовой частоты, несущей частоты и вида модуляции [12].

> **Ремарка 2:** Следует отметить, что таким образом сформированный сигнал по своим параметрам **приближён** к хаотическим сигналам, применяемым в перспективных системах связи. В итоге мы получили непрерывный образ сообщения в виде хаотических колебаний амплитуды непрерывного аналогового сигнала, описываемого в работах профессора Кен Умено (Япония). Хаос представляет собой апериодическое явление, обладающее свойством непредсказуемой случайности. Хаотические сигналы могут использоваться в качестве произвольных сигналов, которые представляют собой сигналы связи [13]. Следует отметить, что сформированный нами сигнал не сложно формировать и передавать в линию связи.

Избежать ситуации с появлением на стыках дискрет разрывов первого и второго рода можно путём математического (широко исследованного в аналитической геометрии) сопряжения функций.

> **Ремарка 3:** Важно определить: когда осуществлять процесс сопряжения – до шифрования (см. формулу (1)) каждой дискреты или после (?). Эту задачу ещё предстоит решить. Оказалось, что даже без применения шифрования, упомянутого выше, псевдо-аналоговая форма полученного сигнала, передаваемого в линию связи после сопряжения образов дискрет, становится существенно искаженной. Вполне понятно, что частный случай, благоприятствующий процессу криптозащиты, сообщения не является закономерным и требует дальнейших исследований. Однако видно, что мы можем сопрягать, как сглаживая стыки дискрет, уменьшая ширину спектра передаваемого сигнала, так и расширить спектр сигнала, применяя процесс обратный сглаживанию, сформировав квазихаотические сигналы. В последнем случае мы приближаемся к «управляемому хаосу».

Далее для маскировки начала и окончания каждой дискреты применим математический аппарат сопряжения функций. Для этого мы можем воспользоваться математическими достижениями аналитической геометрии [14]. Так, для известных функций $y_1 = f_1(x)$ и $y_2 = f_2(x)$, пересекающихся в точке x=a, для описания плавного перехода с одной кривой на другую в области указанной точки можно применить функцию

$$y = \left(y_1 + y_2 \cdot \left(\frac{x}{a} \right)^n \right) \Bigg/ \left(1 + \left(\frac{x}{a} \right)^n \right), \qquad (1),$$

где $n >> 1$.

Функция (1) дифференцируема и интегрируема. Например, в областях, удалённых от точки x=a, производная формируется также как и (1):

$$\frac{dy}{dx} = \left(\frac{dy_1}{dx} + \frac{dy_2}{dx} \cdot \left(\frac{x}{a} \right)^n \right) \Bigg/ \left(1 + \left(\frac{x}{a} \right)^n \right). \qquad (2).$$

Показатель степени n определяет область и скорость перехода с одной функции на другую. С ростом n область перехода сужается, а его скорость увеличивается [14].

Кроме этого можно воспользоваться готовыми разработками AutodeskInventor®, которые применяются в 3D проектировании [15].

Как было показано выше, сопряжение графиков функций как образов дискрет, позволяет скомпоновать сообщение, которое можно выразить математически - в формульном виде, и параметрически - в виде изменяющегося напряжения или плотности потока мощности выходного каскада передатчика, установленного на входе линии связи.

Для устранения возможности выделить информационные дискреты для их последующего анализа и дешифровки, осуществим сопряжение путём разрежения наиболее удобными для этой операции (дезинформационными) дискретами, которые обозначены в интервалах t_1-t_2 и t_3-t_4 (рис. 4).

При этом, не обращая внимание на некоторое увеличение избыточности, воспользуемся дискретами, которые можно описать известными непрерывными зависимостями.

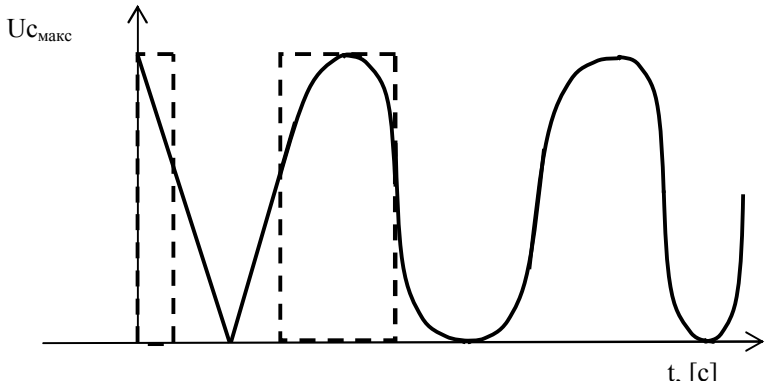

Рис. 4. Вид сигнала, содержащего дезинформационные (выделено пунктиром) дискреты

В результате мы получили сигнал, который можно подвергнуть криптоанализу лишь после предварительного исключения дезинформационных дискрет и восстановления линейного масштаба оси абсцисс. А для этого нужно знать пространственное и временное размещение информационных и дезинформационных дискрет на оси абсцисс.

Если теперь математическое выражение сообщения подвергнуть интегрированию с неизвестным ядром, то перед Оппонентом появится весьма сложная задача дешифровки сообщения.

Ключ

Для современных алгоритмов сильной криптографии утрата ключа приводит к практической невозможности расшифровать информацию.

Оппоненту неизвестен только ключ.

В нашем случае под ключом мы будем понимать переносимую основными или вспомогательными носителями [7] информацию о структурах сообщения: временной, пространственной, комбинированной и пр. Если ключ передан каким-либо сигналом, то сигнал, несущий в себе эту информацию будем называть криптосигналом.

Целесообразно применение двух видов криптосигналов – динамического и статического.

Статический криптосигнал может быть передан в любой момент времени, а использован по мере необходимости дешифровки сообщения. Динамический, как частный случай статического, передаётся по каналу связи одновременно или с некоторым опережением зашифрованного сообщения, что позволяет проводить стробирование дискрет и восстановление масштаба в реальном времени.

Практическая реализация

Целью эксперимента являлось подтверждение возможности реализации первого этапа, заключающегося в возможности получения на экране компьютера и, одновременно, на выходном разъёме (к примеру - USB) изменяющегося во времени напряжения, которое можно подать на управляющие контакты модулятора (АМ, ЧМ, и пр.).

Сам по себе язык JAVA удобен своей кроссплатформенностью, объектно-ориентированностью, гибкостью и наличием широкого спектра математических и графических библиотек.

Буквам алфавита были сопоставлены функции (рис. 5). В результате реализации мы получили изображение последовательности букв в виде графика изменения напряжения управления модулятором передатчика (рис. 6).

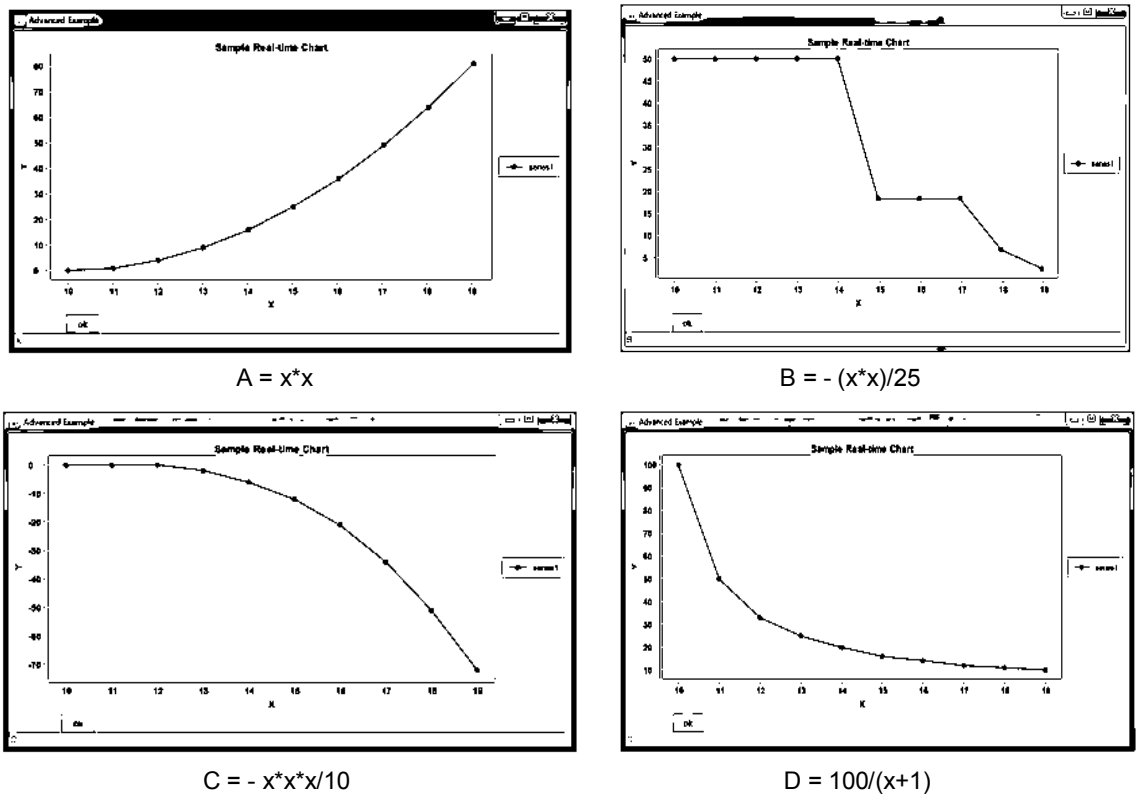

Рис. 5. Скриншоты для различных букв

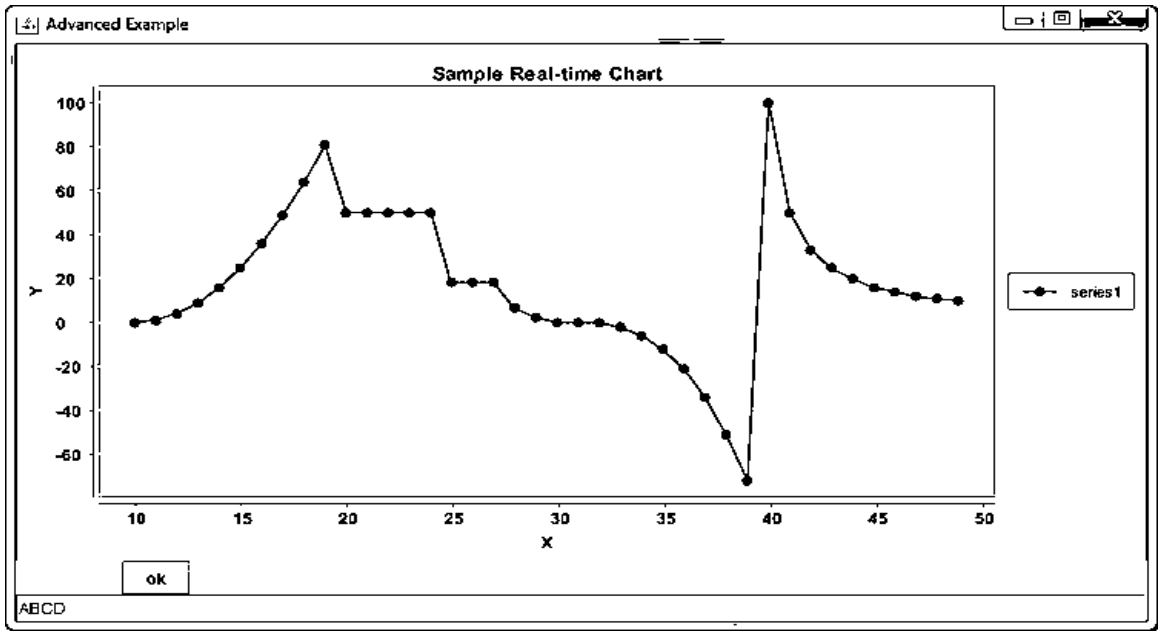

Рис. 6. Скриншот текста «ABCD», набранного на клавиатуре компьютера без сопряжения дискрет

Выводы

На практике подтверждена возможности реализации первого этапа криптографии с использованием аналоговых методов.

Ориентировочно, для полной реализации вышеизложенного на практике, требуется малый промежуток времени и минимум материальных затрат. Открывается громадное поле деятельности по созданию базы дискрет и методов их функционального сопряжения, позволяющего реализовать дальнейшее шифрование путём применения аппарата интегральной криптографии. Последовательности дискрет без сопряжения имеют образы, которые после проведения дополнительных исследований, могут оказаться весьма полезными в реальной практике для применения в качестве аналога широкополосных хаотических сигналов в информационных технологиях.

В перспективе следует рассмотреть приближение данной работы к секвентному анализу Х. Хар-

мута, позволяющее уже сегодня освоить процессы авиационной радиолокации минных полей, трасс трубопроводов, и пр.

Низкочастотные диапазоны радиоволн, позволяющие в настоящее время реализовать элементы аналоговой криптографии, применимы для разработки систем конфиденциальной радио- и электросвязи крупных финансовых структур, коммуникаций подводных лодок и других заглублённых объектов (шахты, тоннели, разработка подземных и подводных рудников и месторождений нефти, правительственные и командные пункты, и пр.).

Список литературы

1. Горбенко Ю.И. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. – Частина 1 : Методи побудування та аналізу, стандартизація та застосування криптографічних систем / Ю.И. Горбенко. – Х. :Форт, 2015 – 960 с.

2. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон. – М.: Изд-во ин. лит., 1964. – 829 с.

3. Громико І. О. Загальна парадигма захисту інформації. Математичне та комп'ютерне моделювання інформаційних процесів в складних природних та технічних системах / І.О.Громико. – Х.: ХНУ ім. В.Н.Каразіна, 2013. – 88 с.

4. Криптография нового поколения: Интегральные уравнения как альтернатива алгебраической методологии / Г.К. Броншпак, И.А. Громыко, С.И. Доценко, Е.Л. Перчик // ResearchGate: DOI: 10.13140/RG.2.1.1973.26452015-06-13 T 11:04:11 UTC. Прикладная электроника. – 2014. – Т. 13, №3. – С. 337-349.

5. Криптография нового поколения: интегральные уравнения как альтернатива алгебраической методологии (дополнение) / Г.К. Броншпак, А.Н. Ващенко, И.А. Громыко, С.И. Доценко, Е.Л. Перчик // ResearchGate: DOI: 10.13140/RG.2.1.3897.0325 2015-11-02 T 12:23:13 UTC.

6. Криптография нового поколения: Интегральные уравнения как альтернатива алгебраической методологии (мини-презентация статьи) / Г.К. Броншпак, И.А. Громыко, С.И. Доценко, Е.Л. Перчик // ResearchGate: DOI: 10.13140/RG.2.1.2497.5523 2015-06-13 T 10:54:41.

7. Громыко И.А. Общая парадигма защиты информации: проблемы защиты информации в аспектах математического моделирования: монография / И.А. Громыко. – Х.: ХНУ имени В.Н. Каразина. 2014. – 216 с.

8. Громыко И.А. Криптографиясопряженныхдискрет / И.А. Громыко, А.Д. Саханчук // ResearchGate: DOI: 10.13140/RG.2.1.2477.6722 Seediscussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/289980230.

9. Горбенко І.Д. Прикладнакриптология. Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Х.: Форт, 2012. – 868 с.

10. Основы информационной безопасности. Семантическое сокрытие информации [Электронный ресурс]. – Режим доступа: http://daxgrom.com.ua/.

11. Медведев Ф.А. Очерки истории теории функций действительного переменного / Ф.А. Медведев. – М.: Наука, 1975. – 248 с.

12. Храмов Е. Определение параметров сигнала. [Электронный ресурс] . Режим доступа: http://blog.hram0v.com/2014/03/analyzer/ .

13. Теория хаоса как решение проблемы ограниченного спектра [Электронный ресурс] // ITUnews. – 2015. - № 4 – Режим доступа: https://itunews.itu.int/ru/Note.aspx?Note=4764.

14. Александрова О.В. Сопряжение функций и переходы состояний. [Электронный ресурс] / О.В. Александрова, В.М. Маркочев. – Режим доступа : http://www.library.mephi.ru/data/scientific-sessions/2001/8/2423.htm

15. Сплайновая интерполяция. [Электронный ресурс]. – Режим доступа: http://posibnyky.vntu.edu.ua .

16. Серавкин А. Autodeskinventor 11. Шаг третий – высококачественное моделирование сложных поверхностей и тел / А. Серавкин // CADmaster. – 2006. - № 4. – С. 24-30.

Поступила в редколлегию 11.05.2016

Рецензент: д-р экон. наук, доцент С.В. Кавун, Харьковский учебно-научный институт банковского дела ГВУЗ «Университет банковского дела», Харьков.

JAVA РЕАЛІЗАЦІЯ ЕЛЕМЕНТІВ КРИПТОГРАФІЇ ЗВ'ЯЗАНИХ ДІСЬКРЕТ

І.О. Громико, К.О. Швагер

Розглядається варіант реалізації елементів захисту інформації в криптографії нового покоління з використанням математичних засобів безперервного аналізу для передачі дискрет (у лінію зв'язку) у вигляді широкосмугових квазіхаотичних сигналів, подібних досліджуваним професором Кен Умено (Японія). Такі лінії зв'язку вже сьогодні можуть бути використані для розробки систем конфіденційного радіо- і електрозв'язку крупних фінансових структур, комунікацій підводних човнів і інших заглиблених об'єктів (шахти, тунелі, розробка підземних і підводних копалень і родовищ нафти, урядові і командні пункти, і ін.). Дослідження гідні фінансової спонсорської допомоги з боку приватних і державних інвесторів.

Ключові слова: *криптографія, криптосигнал, криптостенографія, хаотичні сигнали, перетворення безперервного аналізу в криптографії.*

JAVA EMBODIMENT OF CONJUGATED DISCRETE CRYPTOGRAPHY

I.A. Gromyko, K.O. Shvager

The article considers an embodiment of the information protection elements in the cryptography of a new generation using mathematical tools for continuous analysis of the discrete transfer (within the communications line) in the form of broadband quasi-random signals similar to those explored by Professor Ken Umeno (Japan). Even today such communications can be applied in the development of systems for the purposes of confidential radio and electric communications in large financial institutions, submarines and other subsurface facilities (mines, tunnels, development of underground and underwater mines and oil fields, governmental and command centers, etc.).In the long term it is necessary to consider the connection of the presented developments with the sequential analysis of H. Hartmut allowing to master the processes of aviation radio detection and location of minefields, pipeline routes etc even at present. The level of the proposed research determines the expediency of its financial support from the point of view of both private and state investors.

Keywords: *cryptography, cryptographic signal, cryptostenography, random signals, transformation of continuous analysis in cryptography.*