УДК *003.26*

Г.Н. Шурховецкий [1]

[1] *Иркутский государственный университет путей и сообщений, г. Иркутск, Российская Федерация*

КРИПТОСТОЙКОСТЬ АЛГОРИТМОВ ШИФРОВАНИЯ

Аннотация. *В работе дается обзор методов оценки стойкости криптографических алгоритмов, шифров, кодов. Дается понятие криптографической стойкости. Обсуждаются различные единицы её измерения, факторы и методы оценки. Единицами измерения стойкости могут являться затраты времени на взлом ключа, включая разработку соответствующей вычислительной модели; необходимый объём памяти для взлома ключа; стоимостные затраты на взлом ключа; количество необходимой энергии, затрачиваемой на взлом ключа; временная сложность наилучшего из известных алгоритмов, нарушающих безопасность; физический объём вычислительной модели для взлома ключа.*

Обсуждаются понятия вычислительной стойкости, информационно-теоретической стойкости, доказуемой стойкости. Приводятся классические результаты К.Шеннона и примеры стойких и нестойких алгоритмов. Рассматриваются подходы к оценке стойкости криптографических методов и алгоритмов.

Отмечается, что необходимость усложнения алгоритмов шифрования увеличивает сложность вычислений, что приводит к уменьшению их практической полезности. Делается вывод об актуальности некриптографических методов защиты информации: стеганографии и др.

Ключевые слова: *криптографическая стойкость, криптоанализ, криптоаналитическое вскрытие, алгоритм.*

G. N. Surchovetcky [1]

[1] *Irkutsk State University of Railways and Communications, Irkutsk, Russian Federation*

CRYPTIC RESISTANCE OF ENCRYPTION ALGORITHMS

Abstract. *The paper gives an overview of methods for assessing the strength of cryptographic algorithms, ciphers, codes. The concept of cryptographic stability is given. Various units of its measurement, factors and methods of evaluation are discussed. The units of resistance measurement can be the time required to crack a key, including the development of an appropriate computational model; the amount of memory required to crack the key; the cost of hacking the key; the amount of energy required to crack the key; the time complexity of the best known algorithms that violate security; the physical volume of the computational model to crack the key.*

Discuss the notions of computational durability, information and the theoretical resistance, provable resistance. Classical results of K. Shannon and examples of persistent and unstable algorithms are given. Approaches to the evaluation of cryptographic methods and algorithms stability are considered.

It is noted that the need to complicate encryption algorithms increases the complexity of calculations, which leads to a decrease in their practical usefulness. The conclusion is made about the relevance of non-cryptographic methods of information protection: steganography, etc..

Keywords: *cryptographic stability, cryptanalysis, cryptanalytic dissection, algorithm.*

Введение

Криптографическая стойкость (или криптостойкость) – это умение криптографического алгоритма быть устойчивым к криптографическому анализу. Устойчивым называется тот алгоритмический код, успешное криптоаналитическое вскрытие которого предписывает заинтересованному лицу иметь в своём распоряжении настолько колоссальные вычислительно-алгоритмические или временные ресурсы на дешифровку перехваченных сообщений, что задачу решить либо практически невозможно, либо к тому времени, когда она будет решена, засекреченная информация утратит свою ценность для злоумышленников. Очень часто устойчивость криптографического алгоритма не может быть доказана как теорема. Существует лишь возможность оценить риск успешного вскрытия криптографического алгоритма, либо (в том случае, если криптографическая система имеет открытый ключ) показать, что взлом алгоритмического кода не проще решения задачи, которая является вычислительно и алгоритмически крайне сложной [4].

Методы установки криптографической стойкости алгоритмов

Криптостойкость алгоритма можно определять с помощью специальных единиц измерения стойкости, таких как:

- затраты времени на взлом ключа, включая разработку соответствующей вычислительной модели;
- необходимый объём памяти для взлома ключа;
- стоимостные затраты на взлом ключа;
- количество необходимой энергии, затрачиваемой на взлом ключа;
- временная сложность наилучшего из известных алгоритмов, нарушающих безопасность;
- физический объём вычислительной модели для взлома ключа.

Время, на протяжении которого, обеспечивается сохранение конфиденциальности зашифрованной информации, определяется совокупностью различных факторов, включающих в себя:

- производительность вычислительной модели, находящейся в распоряжении взломщика;
- объём памяти вычислительной модели;
- скорость роста производительности вычислительной модели взлома со временем при её совершенствовании;
- сложность наилучшего из известных алгоритмов, решающего задачу вскрытия конфиденциальности;
- возможностью создания новых математических методов, создающих более эффективные алгоритмы решения задачи дешифровки;
- вероятность успешного решения задачи данным алгоритмом;
- возможность получения дополнительной информации об используемом ключе, например, наличие открытых и соответствующих зашифрованных текстов, возможность зашифровывания или расшифровывания специальным образом подобранных текстов [1].

Алгоритмы в криптографии можно отнести к трём типам по уровню криптографической стойкости:

I. Вычислительная стойкость – это возможность потенциального криптоаналитическо вскрытия шифра, когда при всех заданных параметрах и ключах алгоритма шифрования на современной стадии развития криптографического анализа у злоумышленника не существует необходимых вычислительно-алгоритмических и временных ресурсов, чтобы реализовать вскрытие. Считается, что если алгоритм, который осуществляет вскрытие шифра должен выполнить больше или порядка 2^{80} операций, шифр является вычислительно стойким. Не являются вычислительно стойкими: шифры сдвига, замены, Виженера. К вычислительно стойким шифрам относятся DES, AES, RSA, шифр Эль-Гамаля;

II. Информационно-теоретическая стойкость (или абсолютная стойкость) – это ситуация, когда криптоаналитик не способен вскрыть криптосистему ни теоретически, ни практически, даже если он имеет бесконечно большие вычислительно-алгоритмические ресурсы. Доказательства криптографической стойкости в модели такого типа выводятся из теории информации;

III. Доказуемая стойкость – при которой доказательство алгоритмической стойкости криптографической системы представляется в виде решения вполне конкретной трудно решаемой математической проблемы, положенной в основу алгоритмического кода [8].

Среди методов анализа на криптографическую стойкость нужно обратить внимание в первую очередь на полный перебор всех ключей (или метод «грубой силы»), т.к. криптоаналитическое вскрытие данным методом возможна для всех типов криптографических алгоритмов, кроме абсолютно стойких «по Шеннону». Для вновь созданного алгоритма данный метод криптографического анализа часто является единственно возможным. Методы их анализа в значительной степени зависят от трудностей вычисления алгоритмической сложности

кода, которая потом выражается в объёмах затрачиваемого времени, а также в деньгах, необходимой производительности аппаратуры и её вычислительно-алгоритмических ресурсах. В частности, алгоритмический код можно обозначить как криптографически стойкий, если нет способа его «взлома» значительно более быстрого, чем метод полного перебора всех ключей. Криптографические атаки, в основе которых лежит метод полного перебора или «грубой силы», представляют собой на данный момент времени самые универсальный способы взлома алгоритмического кода, но при этом они же являются и самыми продолжительными по времени. Метод «грубой силы» является самым лучшим вариантом вскрытия криптографического алгоритма, если нет или не удаётся найти уязвимостей в системе шифрования, либо же в данной системе шифрования слабых мест нет. Если же такие уязвимости будут найдены, то злоумышленниками разрабатывается методики криптографического анализа с учётом выявленных особенностей системы, что значительно повышает вероятность вскрытия [1].

Во вторую очередь, для последующего изучения алгоритма с целью нахождения его слабостей (уязвимостей), нужно оценить его стойкость в отношении других известных методов установки криптостойкости, таких как линейный криптоанализ, дифференциальный криптоанализ и более специфические, которые должны снизить существующую стойкость [6].

Например, для большого количества симметричных шифров имеются ненадёжные ключи и *S*-блоки, использование которых уменьшает криптографическую стойкость [11].

Важно обратить внимание на то, что особым методом осуществления криптографической стойкости представляют собой атаки на реализацию, которые используются специально для конкретного программно-аппаратно-человеческого комплекса. Они образуют особый тип атак, которые нацелены на уязвимые места в практически эксплуатации криптографической системы. Это значительно отличается от теоретического криптографического анализа, т.к. атаки по сторонним каналам реализуют информацию о физических процессах в вычислительной технике, которые не подвержены рассмотрению в теоретической основе криптографического алгоритма [13].

Также важно подчеркнуть значимость длительной проверки и открытого обсуждения криптографических методов и алгоритмов. Продолжительный анализ и высокая квалификация экспертов при изучении алгоритма и его реализаций порождают уверенность в криптографической стойкости, если попытки взлома не дали результатов. Существуют примеры, когда длительный и внимательный анализ приводил к уменьшению криптографической стойкости ниже приемлемого уровня (например, в черновых версиях FEAL). Известно, что недостаточная проверка (по мнению многих криптографов – искусственное ослабление) алгоритма потокового шифрования A5/1 привела к успешной атаке на него [7].

Алгоритмы абсолютно стойкие «по Шеннону»

Исследования по теоретической составляющей стойкости алгоритмов впервые были проведены К. Шенноном. В своих публикациях (см. напр. [13, 16, 17]) он, применяя вероятностную модель алгоритма, впервые сформулировал определение совершенно стойкого алгоритма и доказал, что такой алгоритм действительно существует. Это известный среди специалистов шифр Вернама, который также называется одноразовым блокнотом. Данный алгоритм был представлен американским инженером из компании AT&T Джилбертом Вернамом еще в 1917 г. для шифрования телеграфных сообщений. Суть алгоритма шифрования Вернама заключался в том, что представленная в двоичном коде последовательность открытого текста побитово складывалась с ключом – случайной двоичной последовательностью с длиной, превышающей или равной длине исходного сообщения [3]. Сложение осуществлялось по схеме исключающего ИЛИ. Важной особенностью шифра также является одноразовость ключа.

Теоремы Шеннона

Предположим, что открытая информация – это слова, представленные длиной n в алфавите Z_m. Пусть имеется множество информационных сообщений, представленных открытыми текстами X и шифрованными текстами Y, помещенными в пространство V всех возмож-

ных последовательностей длины n в алфавите Z_m [10]. Как отмечено в [10], действия по дешифровке можно изобразить графически в виде группы линий, которые выходят из всех шифрованных текстов $y \in Y$ к разным $x \in V$. Каждый $y \in Y_n$ связан с k открытыми текстами $x \in V$ (причём, $k = r$, где здесь r – число значений гаммы шифра) Их можно выразить как $x^{(1)},\ldots,x^{(k)}$. Линии, которые идут от y к $x^{(1)},\ldots,x^{(k)}$, могут иметь в своём составе в том числе и искомый текст x_0. Если исследователь знает необходимые признаки, присущие открытому тексту (например, читаемость), и в наборе $x^{(1)},\ldots,x^{(k)}$ хотя бы один текст x отвечает заданным признакам, то можно считать, что процедура дешифрирования считается завершённой. Однако возможна ситуация, когда признаками открытого текста обладает более одного элемента из набора $x^{(1)},\ldots,x^{(k)}$. Тогда цель дешифровки, т.е. извлечение достоверной информации не может считаться достигнутой. Из этого следует чёткое понимание того, что на вероятностный результат дешифрования совершенно определённо влияет число линий r. Если $r = 1$, то от y проходит одна единственная линия к x и, следовательно, по условию, этот текст и будет являться искомым. Проблемы неоднозначности здесь нет. Если же $r = m$, то это значит, что от y проходит m разнообразных линий ко всем существующим элементам V. Из этого условия можно сделать вывод, что любой текст из X может считаться вероятностно-предопределённо открытым текстом, что в свою очередь не даст никакой возможности для достижения цели дешифрования и именно этот случай обязательно порождает неоднозначность прочтения криптограммы. Для понимания того, какие значения r вероятностно-предопределяют однозначное дешифрование, а какие r допускают его невозможность, необходимо рассмотреть следующую модель. На множестве ключей задаётся равномерная мера, т.е. любая допустимая гамма может быть представлена с вероятностью $1/|K|$. Также можно предположить, что для абсолютно любого задаваемого шифротекста y, который получен из открытого текста x, все линии, связывающие y с $x^{(1)},\ldots,x^{(k)}$ за исключением (y, x), получаются случайным и равновероятным выбором с возвращением из $(m-1)$ возможностей. Это предположение Шеннон впервые ввёл при определении «случайного шифра» (фактически здесь был рассмотрен частный случай «случайного шифра»). Если модель, основанная на этих и последующих предположениях, позволяет оценить r, при котором выполняется дешифрование, и эта оценка подтверждается экспериментом, то можно говорить о том, что теория правильно выражает сущность вопроса [16].

Искомая строка x может выделиться совершенно определённо и с большой вероятностью, если вероятность появления ошибочных открытых текстов низкая. Для последующего изучения соответствия между заданными параметрами нужна оценка $|X|$.

На данный момент вся совокупность открытых текстов x представляются как подмножество множества V_n всех слов, имеющих длину n. Однако нет никаких обоснованных предположений для того, чтобы считать, что какая-либо последовательность не может стать сообщением. Стоит отметить, что вероятность найти в качестве сообщения одни слова может быть намного больше, чем найти другие. Поэтому можно предположить, что все последовательности длины n могут быть упорядочены в соответствии с их возможными появлениями при общении, происходящем на данном языке. Тогда и только тогда собственно осмысленные (в бытовом понимании этого слова) выражения можно отнести к наиболее вероятностным, в отличие от тех последовательностей, которые имеют значение для нас непонятное (трудно представить общение при помощи труднопроизносимых буквосочетаний) [17].

Так как значения k, m, n и $|X|$ велики, то оценочную характеристику $|X|$ можно дать асимптотически, если предположить, что n большое. Данные оценки были разработаны Шенноном и представлены в его работе «Математическая теория связи» и др. (см. напр. [16, 17]).

Пусть даны $p(a_1),\ldots,p(a_m)$, которые представляют собой вероятности появления букв в заданном месте i в сообщении x длиной n $(1 \le i \le n)$. Предположим, что все буквы в открытом сообщении возникают независимо друг от друга равновероятным образом. Подобная модель открытых сообщений может представляться грубой, но оценка для r, которая доста-

точно близка к экспериментальной, должна показать, что данный способ анализа отображает суть проблемы.

Обозначим через v_i, $i = 1,...,m$, частоты появления букв $a_1,...,a_m$ в последовательности x. Тогда вероятность появления сообщения x равна [10]:

$$P(x) = p^{v_1}(a_1)\cdots p^{v_m}(a_m).$$

Если считать, что

$$p(a_i) > 0, H = -\sum_{i=1}^{m} p(a_i)\log_2 p(a_i),$$

то можно сформулировать следующую теорему.

Теорема 1 (К. Шеннон). Для любых $\varepsilon > 0$ и $\delta > 0$ существует возможность нахождения такого n_0 (число «нужных» событий), что для любой $n > n_0$ последовательности из V делятся на два непересекающихся класса B и $\overline{B}$ так, что

1) $P(\overline{B}) < \varepsilon$, где P - вероятность наступления определенных событий
2) $\forall x \in B$ выполняется неравенство (3)

$$\left|\frac{\log_2 P^{-1}(x)}{n} - H\right| < \delta,$$

где H – энтропия Шеннона.

Считаем, что $0 < \varepsilon < 1$ является произвольным малым числом. Последовательности длины n расположим в порядке убывания вероятностей их появления (при этом очевидно, что множество осмысленных сообщений размещается на начальном участке этого набора). Пусть, далее, $\beta(\varepsilon)$ – количество наиболее вероятностных последовательностей так, что сумма вероятностей их появления больше или равна $1-\varepsilon$, а сумма вероятностей появления любого набора из оставшихся меньше, чем $1-\varepsilon$. Как доказал Шеннон, при $n \to \infty$ множество последовательностей, которые представлена в нашей модели открытыми текстами, не зависит от ε.

Теорема 2 (К. Шеннон). Для любого $\varepsilon > 0$

$$\lim_{n\to\infty} \frac{\log_2 \beta_n(\varepsilon)}{n} = H,$$

где ε не равно 0 или 1.

Дополнительные материалы по этому вопросу можно найти в [3, 12].

Подходы к оценке стойкости шифров

В криптографии были разработаны два основополагающих подхода к оценке стойкости шифров. Первый подход (совершенная секретность) был разработан К. Шенноном в 1948 г. Им была предложена следующая модель обращения с параметрами, которые предоставляют характеристику шифрованию и действиям противника [5]. Пусть

$$\pi \leftarrow \mathrm{Prove}(\sigma, y, w)$$

– множества открытых сообщений и возможных шифротекстов. Открытый текст, для произведения передачи в шифрованном виде, выбирается случайным образом в соответствии с распределением π.

Сразу после этого, при решении задачи по вскрытию x по известному y, противник способен вычислить апостериорные вероятности посланных сообщений: $Verify(\sigma, y, \pi) = accept$, $s=1,...,n$. Если задача дешифрования решена и открытый текст найден, то апостериорное распределение выглядит как [5]:

$$P(x_i|y_j) = 1, P(x_s|y_j) = 0, \text{ при } s \neq i$$

В таком случае в апостериорных вероятностях $\{P(x|y), x \in X\}$ происходит отображение даже частичных сведений об открытом тексте, которые получены при перехвате шифрованного сообщения. Шенноном совершенная секретность (стойкость) шифра была определенна следующим условием: апостериорные распределения на открытых текстах при любом $y \in Y$ оказываются одинаковым с априорным распределением на X, т.е. $P(x|y) = P(x)$ для любых $x \in X$, $y \in Y$ [5].

Дальнейший шаг в теоретическом подходе по оценочной характеристике стойкости шифров служит дача оценки числа открытых текстов, которые можно получить при применении всевозможных способов трансформации текстов, которые имеются в наличии, при неизвестном заблаговременно ключе. Суть этого подхода раскрывается далее на примере, не относящемся к криптографии [15].

Пример. Пусть мы играем в игру: необходимо определить слово по имеющимся в порядке их следования некоторым буквам этого слова (пример – телеигра «Поле чудес»). Предположим, в слове имеется буква «п». Но существует множество слов, которые имеют букву «п», и поэтому мы не способны даже приблизительно указать заданное слово. Иначе говоря, у нас нет в наличии достаточной информации, чтобы отгадать слово. Более того, возможно мы не сможем восстановить слово, даже если будем знать несколько букв. Например, мы заведомо обладаем информацией, что первые три буквы в слове - это «при». Не зная других ограничений, мы не сможем указать множество различных по смыслу слов, которые имеют данную приставку «при». Поэтому это буквосочетание почти что ничего не предоставляет для общего осмысления неизвестного слова [9].

Аналогично, если при проведении дешифрования уравнение $T(x, k) = y$ имеет множество решений x, а ключ способен принимать все допустимые значения, то соответственно возможно множество смысловых текстов x, которые подходят по описанию под существующие наши ограничения и имеют приблизительно равную возможность их возникновения в качестве открытых текстов. После этого не существует алгоритма, который решает данную задачу дешифрования (в смысле однозначного нахождения открытого текста и ключа). Наоборот, во многих моделях шифров можно доказать, что такое решение единственно [9].

Другой подход к определению стойкости алгоритма берет своё начало так же в работе Шеннона и называется практической стойкостью или сложностный подход к стойкости. Рассмотрим выражение $T(x, k) = y$ как уравнение относительно x и k. Тогда решение этого уравнения предполагает наличие алгоритма, для которого в математике существует понятие сложности. Сложность определяется двумя параметрами: число операций для вычисления результата (трудоемкость алгоритма) и объем необходимой памяти [17].

Число операций взаимосвязано со временем работы алгоритма. Отсюда следует, что стойкость может быть выражена в терминах времени работы алгоритма дешифрования. В связи с этим, естественное требование надежности шифра – высокая сложность любых вероятностных алгоритмов дешифрования [16].

Замечание 1. Можно повысить сложность дешифрования за счёт повышения сложности преобразования $T(x, \kappa) = y$. Но если сложность вычисления $T(x, k)$ и $(y, w) \in R\sigma(y, k)$ при известном k будут велики, то практически данный шифр будет трудно использовать. Поэтому наряду с требованием сложности решения уравнения $T(x, k) = y$ при неизвестном k, привлекают естественное требование простоты вычисления $T(x, k)$ и $(y, w) \in R\sigma(y, k)$ при известном k [2].

Замечание 2. Требование высокой сложности при любых возможных алгоритмах дешифрования не конструктивно. Это связано с тем, что оно опирается на необходимость перебора всех таких алгоритмов, что, вообще говоря, немыслимо. На практике это требование заменяется на вполне реализуемое – условие высокой трудоемкости при всех известных на сегодня методах дешифрования [14].

Заключение

Как можно видеть из представленного материала, существуют самые различные подходы к оценке криптостойкости. Специалистами предложены единицы измерения криптостойкости, определены характеризующие её факторы. Предложены методы оценки. Для создания более совершенных алгоритмов шифрования необходимо учитывать и все возможные алгоритмы дешифрования. Необходимость усложнять алгоритмы шифрования увеличивает сложность вычисления, но при этом уменьшается практическая полезность в использовании. Также важно отметить, что рассмотренные методы оценки криптостойкости во многом свя-

заны со стойкостью алгоритмов шифрования. В связи с этим актуальны некриптографические методы защиты информации: стеганография и др.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гатченко Н.А., Исаев А.С., Яковлев А.Д. Криптографическая защита информации. СПб: НИУ ИТМО, 2012. 142 с.
2. Грушо А.А, Применко Э.А, Тимонина Е.Е. Анализ и синтез криптоалгоритмов. Курс Лекций, Йошкар-Ола: Изд-во Марийского филиала Московского открытого социального университета, 2000г. 110 с.
3. Зубов А.Ю. Совершенные шифры – М.: Гелиос АРВ, 2003. 160 с.
4. Криптографическая стойкость. – https://ru.wikipedia.org/wiki/ Криптографическая_стойкость (Дата обращения 18.10.2018).
5. Логачёв О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. М.: Московский центр непрерывного математического образования, 2004. 470 с.
6. Мао В. Современная криптография: Теория и практик. М.: Вильямс, 2005. 768 с.
7. Найджел С. Криптография. Москва: Техносфера, 2005. 528 с.
8. ПРАКТИЧЕСКАЯ КРИПТОЛОГИЯ ЛЕКЦИЯ 3 Специальность: 6.170101 – Бсіт Лектор: Сушко С.А. – http://bit.nmu.org.ua/ua/student/metod/cryptology/лекция 3.pdf (Дата обращения 18.10.2018).
9. Совершенно секретные шифры и теория Шеннона. http://cryptowiki.net/index.php?title=Совершенно_секретные_шифры_и_теория_Шеннона (Дата обращения 18.10.2018).
10. Теоремы Шеннона. – http://cryptowiki.net/index.php?title=Теоремы_Шеннона (Дата обращения 18.10.2018).
11. Фергюсон Н, Шнайер Б. Практическая криптография: Пер. с англ. М.: Издательский дом “Вильямс”, 2004. 432 с.
12. Фомичев В.М. Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
13. Шеннон К. Теория связи в секретных системах / пер. с англ. В. Ф. Писаренко // Работы по теории информации и кибернетике / Под редакцией Р. Л. Добрушина и О. Б. Лупанова. М.: Издательство иностранной литературы, 1963. 829 с.
14. Thomas W. Cusick and Pantelimon Stanica. Cryptographic Boolean Functions and Applications. Academic Press, 2009. 248 p.
15. van Tilborg, Henk C.A., Jajodia, Sushil (Eds.). Encyclopedia of Cryptography and Security. Springer, 2011. 1416 p.
16. Shannon C.E. A mathematical theory of communication. Bell system technical journal, 27, 1948. pp 379-423.
17. Shannon C.E. Communication theory of secrecy systems. Bell system technical journal, 28, 1949. pp. 656-715.

REFERENCES

1. Gatchenko N.A., Isaev A.S., Yakovlev A.D. Cryptographic protection of information. SPb: NIU ITMO, 2012. 142 p.
2. Grusho A.A., Applied E.A., Timonina E.E. Analysis and synthesis of cryptographic algorithms. Course of Lectures, Yoshkar-Ola: Publishing house of the Mari branch of Moscow Open Social University, 2000. 110 p.
3. Zubov A.Yu. Perfect Ciphers. M.: Helios ARV, 2003. 160 p.
4. Cryptographic firmness. – https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%81%D1%82%D0%BE%D0%B9%D0%BA%D0%BE%D1%81%D1%82%D1%8C [Accessed 18/10/2018]

5. Logachev OA, Salnikov A.A., Yashchenko V.V. Boolean functions in coding theory and cryptology. Moscow: Moscow Center for Continuous Mathematical Education, 2004. 470 p.
6. Mao V. Modern cryptography: Theory and practice. M.: Williams, 2005. 768 p.
7. Nigel S.t Cryptography. Moscow: Technosphere, 2005. 528 p.
8. PRACTICAL CRYPTOLOGY LECTURE 3 Specialty: 6.170101 – BSIT Lecturer: Sushko S.A. – http://bit.nmu.org.ua/ua/student/metod/cryptology/%D0%BB%D0%B5%D0%BA%D1%86%D0%B8%D1%8F%203.pdf [Accessed 18/10/2018]
9. Top Secret Ciphers and Shannon's Theory. – http://cryptowiki.net/index.php?title=%D0%A1%D0%BE%D0%B2%D0%B5%D1%80%D1%88%D0%B5%D0%BD%D0%BD%D0%BE_%D1%81%D0%B5%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D1%8B%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D1%8B_%D0%B8_%D1%82%D0%B5%D0%BE%D1%80%D0%B8%D1%8F_%D0%A8%D0%B5%D0%BD%D0%BD%D0%BE%D0%BD%D0%B0 [Accessed 18/10/2018]
10. Shannon's theorems. – http://cryptowiki.net/index.php?title=%D0%A2%D0%B5%D0%BE%D1%80%D0%B5%D0%BC%D1%8B_%D0%A8%D0%B5%D0%BD%D0%BD%D0%BE%D0%BD%D0%B0 [Accessed 18/10/2018]
11. Ferguson N., Schneier B. Practical cryptography: Trans. from English. M.: Publishing house “Williams”, 2004. 432 p.
12. Fomichev V.M. Methods of discrete mathematics in cryptology. M.: Dialogue-MIPI, 2010. 424 p.
13. Shannon C. Communication theory in secret systems / Per. from English VF Pisarenko // Works on Information Theory and Cybernetics / Edited by R. L. Dobrushushin and O. B. Lupanova. M.: Publishing House of Foreign Literature, 1963. 829 p.
14. Thomas W. Susic and Runtelon Street. Syrtograrhis Boolean Functions and Arplications. Academis Press, 2009. 248 p.
15. van Tilborg, Henk C.A., Jajodia, Sushil (Eds.). Encyclopedia of Cryptography and Security. Springer, 2011. 1416 p.
16. Shannon C.E. A mathematical theory of communication. Bell system technical journal, 27, 1948. pp. 379-423.
17. Shannon C.E. Communication theory of secrecy systems. Bell system technical journal, 28, 1949. pp 656-715.

Информация об авторах

Шурховецкий Георгий Николаевич – аспирант, аспирант кафедры «Информационные системы и защита информации», Иркутский государственный университет путей и сообщений, г. Иркутск, e-mail: gshn5@yandex.ru

Authors

Surchovetcky George Nikolaevich – Postgraduate Student, Postgraduate Student of the Department "Informatics Systems and Information Security ", Irkutsk State University of Railways and Communications, Irkutsk, e-mail: gshn5@yandex.ru

Для цитирования

Шурховецкий Г.Н. Криптостойкость алгоритмов шифрования [Электронный ресурс] / Г.Н. Шурховецкий // Молодая наука Сибири: электрон. науч. журн. – 2018. – №2. – Режим доступа: http://mnv.irgups.ru/toma/22-2018, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 17.12.2018)

For citation

Surchovetcky G.N. *Cryptic resistance of encryption algorithms* [Cryptographic strength of encryption algorithms]. *Molodaya nauka Sibiri: ehlektronnyj nauchnyj zhurnal* [Young science of Siberia: electronic scientific journal], 2018, no. 2. [Accessed 17/12/18]