CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
http://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 02 Issue: 11 | Nov 2021 ISSN: 2660-5309

Исследование Вопросов Необходимых Условий Идеально Стойких Алгоритмов Шифрования

Д. Е. Акбаров[1], О. Э.Кушматов[2], Ш.А. Умаров[3], Б. С.Далиев[4]

[1]*д.физ.-мат. н., Какандский государственный педагогический институт, Каканд, Узбекистан*

[2]*к.физ.-мат. н., Ферганский филиал Ташкентского университета информационных технологий, Фергана, Узбекистан*

[3]*исследователь, Ферганский филиал Ташкентского университета информационных технологий, Фергана, Узбекистан*

[4]*ст. Преподаватель, Ферганский политехнический институт, Фергана, Узбекистан*

Аннотатсия:

В статье исследованы особенности необходимых условий идеально стойких алгоритмов шифрования. Выявлены общие свойства моделей классов идеально стойких алгоритмов шифрования. На их основе сформулированы соответствующие требования в виде критериев, определяющих необходимые условия криптографической стойкости. Совокупность этих критериев сформулированы как утверждение.

ARTICLEINFO

Article history:
Received 30 Sep 2021
Revised form 22 Oct 2021
Accepted 17 Nov 2021

Ключевые слова: классы алгоритмов шифрования, идеально стойкий алгоритм, критерий, криптостойкость, необходимое условие, математическая модель, преобразование распространения, преобразование перемешивания, коллизия, длина ключа, шифр обозначение, шифр величина, мощность алфавита, открытое сообщение, шифрованное сообщение, микропроцессор, нелинейность, односторонность, равновесие, регулярность, лавинный эффект, гибкость относительно корреляции.

Введение. Смысл шифрования заключается в преобразовании некоторого сообщения так, чтобы его истинный смысл был скрыт. При этом алфавиты открытого сообщения перестановят или символы алфавита поменяются на другие символы по смыслу. При этом используются некоторые операции, табличные замены, перемешивания и распространения символов. Эти процедуры все же непроизвольные [1-4]. Они должны обладать теми свойствами, чтобы были легко выполняемые с вычислительной точки зрения, удобно реализуемыми в аппаратных средствах микропроцессоров и микроконтроллеров [5-6]. Об особенностях конструкции разных типов алгоритмов шифрования подробно можно познакомиться во многих научных и учебных источниках, в том числе [1-16].

Постановка задачи. В предлагаемой статье исследуются вопросы необходимых условий идеально стойких алгоритмов шифрования. Выявляются общие особенности свойства

моделей классов идеально стойких алгоритмов шифрования и систематизированном виде формулируются необходимые требования – критерии относительно конструкции алгоритма в виде утверждения.

Решение задачи. Шеннон исследовал вопросы стойкости криптографической системы с двух точек зрения: *теоретической* и *практической.* В оценке теоретической стойкости предполагается, что специалист криптографического анализа заинтересованной стороны имеет всевозможные теоретические, технические и другие необходимые средства, кроме того время криптоанализа неограниченно. А в оценке практической стойкости предполагается, что для криптоанализа не имеются достаточных необходимых средств и времени [3,4]. На основе анализа использованных литературных источников [17-25] и совокупности многих других работ в этой области осознана необходимость формулировки условий идеально стойких алгоритмов шифрования. Опираясь на эти обоснования и из личного опыта исследования авторов предлагаемой статьи можно сформулировать следующее утверждение.

Утверждение. *Для того чтобы алгоритм шифрования был идеально стойким необходимо выполнения следующих условий:*

1) *Алгоритм должен относится к типу шифрования много алфатиной замены , т.е. в процессе шифрования символы открытого сообщения на символы шифр величин по этапу изменяется в таблице замены;*
2) *Длина ключа или мощность множества шифробозначений достаточно большое;*
3) *В большенстве случаях один символ открытого сообщения преобразуется в один символ шифробозначения на основе процедуры замены;*
4) *X– символы открытого сообщения и Y –символы шифробозначений шифрованного сообщения статистически независимы, т.е. для $\forall x$ -открытого сообщения и $\forall y$ – шифрованного сообщения имеет место вероятное равенство $P(X=x/Y=y)=P(X=x)$;*
5) *Длина ключа K не меньше относительно длины открытого сообщения M, т.е. $K \geq M$;*
6) *Ключ шифрования используется один раз.*

Доказательство. Сущности необходимых условий заключается в том, что если алгоритм относится к типу шифрования идеальной стойкости, то должны выполнятся требования–критерии утверждения.

Отметим, что криптографический анализ каждого конкретного нового разработанного алгоритма является новой задачей для исследования. Потому, что каждый новый алоритм имеет свои новые базовые преобразования и их комбинации собственной конструкции. Криптоаналитиком исследуется криптографические свойства базовых преобразований и конструкция алгоритма относительно существующих методов криптоатак. При этом исследуются свойства: односторонности преобразования, эффективного распространения и рассеивания, лавинного эффекта и многих других особенностей криптостойкости. Для этого проводятся численные эксперименты для установления прицельных закономерностей, проверяется возможности/невозможности полного выбора всех вариантов, определяются степени корреляции и случайности, делаются попытки разработки возможных математических моделей для раскрытия слабостей криптографических свойств стойкости и др.

Ниже обосновываются необходимые критерии (условия), приведенные в утверждении идеально стойкого алгоритма шифрования.

1. Идеально стойкий алгоритм шифрования относится к типу многозначной замены: в процессе шифрования правила таблицы замены символов открытого текста на символы шифрованного текста периодически изменяются. Здесь отмечается, что правило табличной замены является ключом алгоритма шифрования [26-30]. При этом совокупность элементов символов шифробозначений должны иметь, достаточно большую мощность, в настоящее время этот показатель не меньшее 256 символов.

Иначе, если алгоритм относится к типу однозначной замены, частотные характеристики открытого сообщения переходят к шифрованному сообщению. Такое обстоятельство криптоаналитику позволяет определять нужную стратегию и тактику для моделирования криптоатак.

Если алгоритм шифрования многозначный, совокупность символов шифр величин обозначить $\{x_1, x_2, ..., x_N\}$, а совокупность символов шифр обозначений обозначить $\{y_1, y_2, ..., y_M\}$, то ключ алгоритма идеального шифрования можно выражать следующей таблицей

Таблица 1.

Символы открытого сообщения	x_1	x_2	**...**	**...**	x_N
Символы шифрованного сообщения 1-этапа	$y_{i_1}^1$	$y_{i_2}^1$	**...**	**...**	$y_{i_N}^1$
Символы шифрованного сообщения 2-этапа	$y_{i_1}^2$	$y_{i_2}^2$	**...**	**...**	$y_{i_N}^2$
...	**...**	**...**	**...**	**...**	**...**
...	**...**	**...**	**...**	**...**	**...**
Символы шифрованного сообщения *w*-этапа	$y_{i_1}^w$	$y_{i_2}^w$	**...**	**...**	$y_{i_N}^w$

Здесь шифр обозначения $y_l^d \in \{y_1, y_2, ..., y_M\}$ по строке и столбцу таблицы многозначной замены попарно разные.

Действительно, если полагать символы открытого сообщения $\{x_1, x_2, ..., x_N\}$ и шифрованного сообщения $\{y_1, y_2, ..., y_M\}$, то модель процесса шифрования многозначной замены с некоторой операцией ($*$) и ключевым блоком $k = k_1 k_2 ... k_i ... k_m$ выражается: $x_i * k_i = y_i$. При известном x_i и y_i однозначно определяется k_i, поэтому появляется возможность восстановления таблицы многозначной замены. Следовательно, требуется условие использования ключа один раз.

Опираясь на вышеприведенные соображения можно утвердать, что при известной паре открытого и соответствующего шифрованного сообщения можно создать средство криптоатак для определения таблицы замены

2. Проверка обеспеченности достаточности длины ключа и определение мощности алфавита совокупности шифробозначений осуществляется в следующем виде.

Развитие вычислительной техники и технологии естественным образом требует модернизации преобразования существующих алгоритмов, в том числе и длины ключа.

Не выполнения условие 2), может быть основой для определения алфавита шифробозначений и осуществить полный выбор всевозможных ключей. Кроме того, при не достаточной мощности алфавита шифробозначений для шифрования коротких сообщений неудобно с точки зрения осуществления криптоатаки выбора возможных открытых сообщений.

Современная минимальная длина исходного ключа, из которого образуются промежуточные и этапные ключи, криптоалгоритмов должна быть не меньше 256 символов. Длина ключа определяется с алфавитом ключа исходя из свойства преобразований алгоритма шифрования.

Если преобразования осуществляются над битами, то алфавит ключа выражается в битах, следовательно, длина исходного ключа должна быть не меньше 256 битов.

Если преобразования осуществляются над полубайтами или байтами, то алфавит ключа выражается в полубайтах или байтах, следовательно, длина исходного ключа должна быть не меньше 256 полубайтов или байтов соответственно.

Таким образом, исходя из правила использования символов ключа в преобразованиях определяется его алфавит. По определённому алфавиту длина исходного ключа должна быть не меньше 256 символов

3. В третьем требовании утверждения отмечается, что базовые преобразования алгоритма осуществляются над каждыми символами ключевого блока и шифруемого сообщения.

При нарушении этого условия, имея пару открытого и соответствующего ему шифрованного сообщения некоторого источника, появляется основа для получения информации, и возможность создать модели криптоатак на другие криптограммы.

Выполнение этого критерия выражается в общем аналитическом виде $x_i * k_i = y_i$, где $*$ –некоторая операция базового преобразования, x_i –символ открытого сообщения, k_i –символ ключевого блока, одно равенство имеет два неизвестных, что не даёт однозначного решения.

4. В четвертом требовании утверждения отмечается, что X – открытое сообщение и Y – шифрованное сообщение статистически независимы , т. е. сообщения $\forall x \in X$ и $\forall y \in Y$ статистически независимы. Это высказанное в общем математическом виде выражается моделью условной вероятности: $P(X=x/Y=y)=P(X=x)$.

В случае нарушения условия статистической независимости, для некоторого x –открытого сообщения и соответствующего ему y–шифрованного сообщения, или их некоторых частей имеет место неравенство: $P(X=x/Y=y) \neq P(X=x)$.

Выполнения критериев 3) и 6) в утверждении будет основой обеспечения требования–критерия 4), т. е. равенство условной вероятности.

5. В пятом требовании-критерии утверждения отмечается, что длина ключа K не меньше длины открытого сообщения M , т.е. $K \geq M$.

Не выполнение этого условия, т.е. выполнение условия $K<M$, может позволить определить периодичность использования ключа, который может быть маловажным для криптоаналитика в определенных случаях раскрытия криптограмм.

6. Сущность требования выполнения критерий 6) была изложена выше в пункте 4

Анализ полученных результатов. Отмечается, что изложенные выше факты являются общими для алгоритмов класса идеального шифрования. Как вначале отмечалось, что для

каждого алгоритма этого класса проверка приведённых критериев утверждения требует тщательного научного исследования. Проверка каждого условия утверждения для алгоритмов конкретными новыми базовыми преобразованиями требуют свои соответствующие методы достижения цели возникающих задач.

Отмечается, что приведённые критерии в утверждении, с развитем вычислительной техники и технологии, соответствующим образом дополняется и модернизируется.

Возникающие отрицательные последствия при нарушении этих необходимых условий криптостойкости обоснованы соответствующими примерами.

Заключение. Определены критерии, которые позволяют проверить особенности криптографической стойкости алгоритмов идеального стойкого шифрования, и оно выражено в виде утверждение. В научно обоснованном виде исследованы и изложены сущности критериев утверждения необходимых условий стойкости. Приведённые в утверждении необходимые критерии являются общими и указывают обоснованный путь к оценке криптостойкости класса алгоритмов идеального шифрования.

ИСПОЛЬЗОВАННЫЕ ЛИТЕРАТУРЫ

1. Шнайер, Б. (2002). Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. *М.: Триумф*, *816*, 3.
2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. (2002). Основы криптографии: Учебное пособие, 2-е изд. –М.: Гелиос АРВ,.с. 480.
3. Шеннон, К. (1963). Теория связи в секретных системах. *Работы по теории информации и кибернетике. М.: ИЛ*, 333-369.
4. Merkle, R. C. (1978). Secure communications over insecure channels. *Communications of the ACM*, *21*(4), 294-299.
5. Харин, Ю. С., Берник, В. И., Матвеев, Г. В., & Агиевич, С. В. (2003). Математические и компьютерные основы криптологии.
6. Ростовцев А. Г., Маховенко Е. Б., (2004). Теоретическая криптография. НПО «Профессионал», Санкт-Петербург. С. 478.
7. Молдовян А. А., Молдовян Н. А., Советов Б. Я. (2001). Криптография. – Санкт-Петербург, Изд. «Лань»,.с. 224.
8. Акбаров, Д. Е., & Умаров, Ш. А. (2020). Анализ приложения логических операций к криптографическим преобразованиям средств обеспечения информационной безопасности. *Universum: технические науки*, (2-1 (71)).
9. Akbarov, D. E., & Umarov, S. A. (2021). Mathematical characteristics of application of logical operations and table substitution in cryptographic transformations. *Scientific-technical journal*, *4*(2), 6-14.
10. Akbarov D. E., Umarov Sh. A. (2020). Applying Logical Operations and table replacements in modeling basic transformations of Symmetric block encryption algorithms. International Journal of Mechanical and Production Engineering Research and Development, Vol. 10, Issue. 3, Jun, 15041-15046.
11. Умаров, Ш. А., & Акбаров, Д. Е. (2016). Разработка нового алгоритма шифрования данных с симметричным ключом. *Журнал Сибирского федерального университета. Техника и технологии*, *9*(2).
12. Акбаров, Д. Е., Умаров, Ш. А., & Акбаров, Д. Є. (2016). Новый алгоритм блочного шифрования данных с симметричным ключом.

13. Akbarov D. E. (2009). Cryptographic methods of ensuring information security and their application. Tashkent. p. 432.
14. Молдовян, Н. А. (2004). *Криптография: от примитивов к синтезу алгоритмов*. БХВ-Петербург.
15. Молдовян, А. А. (2002). *Криптография. Скоростные шифры*. БХВ-Петербург.
16. Туктамышева, Л. М. (2018). Математические модели регионального рынка труда: оперативный мониторинг и прогнозирование. *Азимут научных исследований: экономика и управление*, *7*(2 (23)).
17. Хавинсон, М. Ю. (2016). Моделирование динамики численности занятых, безработных и экономически неактивного населения в регионе с учетом социальных связей. *Вестник Воронежского государственного университета. Серия: Экономика и управление*, (4), 178-188.
18. Холмуминов Ш.Р. (2014). Формирование и развитие сельского рынка труда а также их прогнозирование. Монография. Ташкент: “Fan va texnologiya”, 232 p.
19. Abdurazakov, A., Makhmudova, N., & Mirzamakhmudova, N. (2021). On one method for solving degenerating parabolic systems by the direct line method with an appendix in the theory of filration.
20. Абдуразаков, А., Махмудова, Н., & Мирзамахмудова, Н. (2020). Численное решение методом прямых интеграла дифференцирования уравнений, связанных с задачами фильтрации газа. *Universum: технические науки*, (7-1 (76)), 32-35.
21. Абдуразаков, А., Махмудова, Н., & Мирзамахмудова, Н. (2019). Решения многоточечной краевой задачи фильтрации газа в многослойных пластах с учетом релаксации. *Universum: технические науки*, (11-1 (68)).
22. Shadimetov, K., & Daliyev, B. (2021, July). Composite optimal formulas for approximate integration of weight integrals. In *AIP Conference Proceedings* (Vol. 2365, No. 1, p. 020025). AIP Publishing LLC.
23. Шадиметов, Х. М., & Далиев, Б. С. (2020). Коэффициенты оптимальных квадратурных формул для приближенного решения общего интегрального уравнения Абеля. *Проблемы вычислительной и прикладной математики*, (2 (26)), 24-31.
24. Hayotov, A. R., Bozarov, B. I., & Abduganiev, A. (2018). Optimal formula for numerical integration on two dimensional sphere. *Uzbek Mathematical Journal*, *3*, 80-89.
25. Bozarov, B. I. (2019). An optimal quadrature formula with sinx weight function in the Sobolev space. *Uzbekistan academy of sciences vi romanovskiy institute of mathematics*, 47.
26. Hayotov, A., & Bozarov, B. (2021, July). Optimal quadrature formulas with the trigonometric weight in the Sobolev space. In *AIP Conference Proceedings* (Vol. 2365, No. 1, p. 020022). AIP Publishing LLC.
27. Alimjonova, G. (2021). Modern competencies in the techno-culture of future technical specialists. *Current research journal of pedagogics (2767-3278)*, *2*(06), 78-84.
28. Каримов, Ш. Т., & Хожиакбарова, Г. (2017). Аналог задачи гурса для одного неклассического уравнения третьего порядка с сингулярным коэффициентом. *Toshkent shahridagi turin politexnika universiteti*, 121.
29. Tillabayev, B., & Bahodirov, N. (2021). Solving the boundary problem by the method of green's function for the simple differential equation of the second order linear. *ACADEMICIA: An International Multidisciplinary Research Journal*, *11*(6), 301-304.
30. Kosimov, H., & Tillabaev, B. (2018). Mixed fractional order integral and derivatives for functions of many variables. *Scientific journal of the Fergana State University*, *1*(2), 5-11.