

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л. Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМ. Л. Н. ГУМИЛЕВА

THE MINISTRY OF EDUCATION AND SCIENCES OF REPUBLIC KAZAKHSTAN
L.N. GUMILYOV EURASIAN NATIONAL UNIVERSITY



Л.Н. Гумилев 100 жылдығына арналған Қоғамды ақпараттандыру
III Халықаралық ғылыми-практикалық конференция
ЕҢБЕКТЕРІ

ТРУДЫ

III Международной научно-практической конференции
Информатизация общества, посвященной 100-летию Л.Н. Гумилева

PROCEEDINGS

the III International scientific and practical conference
Informatization of society dedicated to the century of L.N. Gumilev



АСТАНА 2012

УДК 002

Қ 54

ҚОҒАМДЫ АҚПАРАТТАНДЫРУ: Үшінші халықаралық ғылыми-практикалық конференция: Баяндамалар мен хабарламалар тезистері
ИНФОРМАТИЗАЦИЯ ОБЩЕСТВА. Третья международная научно-практическая конференция: Труды конференции.

ISBN9965-718-56-3

Редакционная коллегия: Шарипбаев А.А., Байбеков С.Н., Нурбекова Ж.К., Ниязбекова Р.К., Адамов А.А., Тусупов Д. А., Боранбаев С.Н., Бекманова Г.Т., Жалгасбекова Ж.К., Иманкул М.Н., Бекенов М.И., Андасова Б.З., Альжанов А.К., Ниязова Р.С., Сагнаева С.К., Жумадилаева А.К., Сексенбаева А.К., Разахова Б.Ш., Зулпыхар Ж.Е., Омарбекова А.С., Ташенова Ж.М.

Техническая редакция: Исайнова А.С., Сатбаев С.Б.

© Л.Н.Гумилев атындағы Еуразия ұлттық университеті, 2012
Евразийский национальный университет им. Л.Н. Гумилева, 2012

ISBN 9965-718-56-3

Спонсоры:

- Компания EPAM Systems
- ТОО «Казахский институт интеллектуальных систем и высоких технологий»

СЕКЦИЯ 7

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ СИГНАЛДАРДЫ САНДЫҚ ӨНДЕУ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЦИФРОВАЯ ОБРАБОТКА СИГНАЛОВ INFORMATION SECURITY AND DIGITAL SIGNAL PROCESSING

1. A.N. Issainova, G.B. Shakhmetova, S.A. Askarova - Sales network risk management system 328
2. T. Kartbayev, R. Uskenbayeva, M. Mussaif - Effective algorithms of multimedia data processing 331
3. D. OSIPOV - Blind detection in a noncoherent asynchronous DHA FH OFDMA system 333
4. N.N. Tashatov, Z.S. Sautbekova - Representation of state of simple encoders of the convolutional encoder and the diagram of states 336
5. Абдибеков А.У., Жакебаев Д.Б.- Создания казахской кодировки в консоли LINUX на примере KOI8-RK 339
6. Абдулин Д.А., Ибрашева Ш.С. - Обеспечение целостности и неотслеживаемости информации с использованием криптографических протоколов 342
7. Бапанов А.А. - Применение стохастических дифференциальных уравнений в криптографической защите информации 343
8. Бейбітхан Е. - Оценка стойкости криптосистем 347
9. БОКАЕВ Н.А., МУКАНОВ Ж.Б., АХАЖАНОВ Т.Б. - О некоторых свойствах сигналов с финитным спектром Фурье-Уолша 350
10. Боранбаев С.Н., Тулебаев Е.Б. - Модификация алгоритма шифрования RC6 и его программная реализация 351
11. Галамагин А.В. - О перспективных методах обеспечения информационной безопасности 354
12. Ержан А.А., Куралбаев З.К. - Опыт применения средств защиты от шума в беспроводных каналах передачи данных 355
13. Ефимов Д. А. - Практическая реализация турбокодов на примере клиент-серверного приложения 357
14. Ибрашева Ш.С., Абдулин Д.А. - Линейные конечные автоматы в криптографии 360
15. Казиев Г.З., Адильбекова А.К. - Размещение средств защиты информационных ресурсов в узлах вычислительных сетей 363
16. Курманова Е.Н., Себельдин А.М. - Определяемость прямых сумм рациональных групп с точностью до равенства и приложения в информатике 365
17. Медетбаева С.А., Сейтбекова Г.О. - Возможные последствия атак на информацию и модели защиты информации в области информационной безопасности 366
18. Муратхан Р., Сатыбалдина Д.Ж. - Методы обработки экспертных оценок 368
19. Назаров В., Сатыбалдина Д.Ж. - Оптимизация метода сжатия изображений 372
20. Назаров В., Сатыбалдина Д.Ж. - Реализация алгоритма сжатия jpeg 2000 376
21. Панченко Е.А. - Обзор программной реализации алгоритма кодирования и декодирования кодами Рида-Соломона 379
22. Панченко Е.А., Ташатов Н.Н. - Реализация систематического алгоритма кодирования кодами Рида-Соломона 382
23. Сембекова А.Е. - Обзор методов обнаружения ошибок с помощью циклических кодов 385
24. Тайлак Б.Е., Бейсенби М.А. - Генерация псевдослучайных чисел на основе 388

БЕЙБІТХАН Е.

Евразийский национальный университет им. Л.Н. Гумилева, КазУТБ Астана, Казахстан

ОЦЕНКА СТОЙКОСТИ КРИПТОСИСТЕМ

Эффективность современных шифровальных систем и их устойчивость к дешифровке настолько высока, что в некоторых странах использование мощных алгоритмов запрещено, так как оно делает дешифровку информации невозможной даже для органов власти, что может быть использовано в преступных целях. Ограничениям, накладываемым на возможности шифровальных систем, сопротивляются деловые круги – в самом деле, кому нужны шифры, которые с легкостью могут быть взломаны конкурентами?

При оценке стойкости произвольных криптографических систем защиты информации обычно придерживаются принципа Керкхоффа: стойкость криптосистемы должна быть обеспечена и тогда, когда нарушителю известно полное ее описание. Поэтому при анализе стойкости криптографической системы будем предполагать, что противоборствующей стороне известно детальное описание системы, статистические характеристики используемого языка сообщений, пространства возможных ключей и криптограмм; она может иметь некоторую информацию о контексте сообщения и т.п. Единственное, чего не должен знать нарушитель – секретный криптографический ключ, используемый пользователями криптографической системы защиты информации.

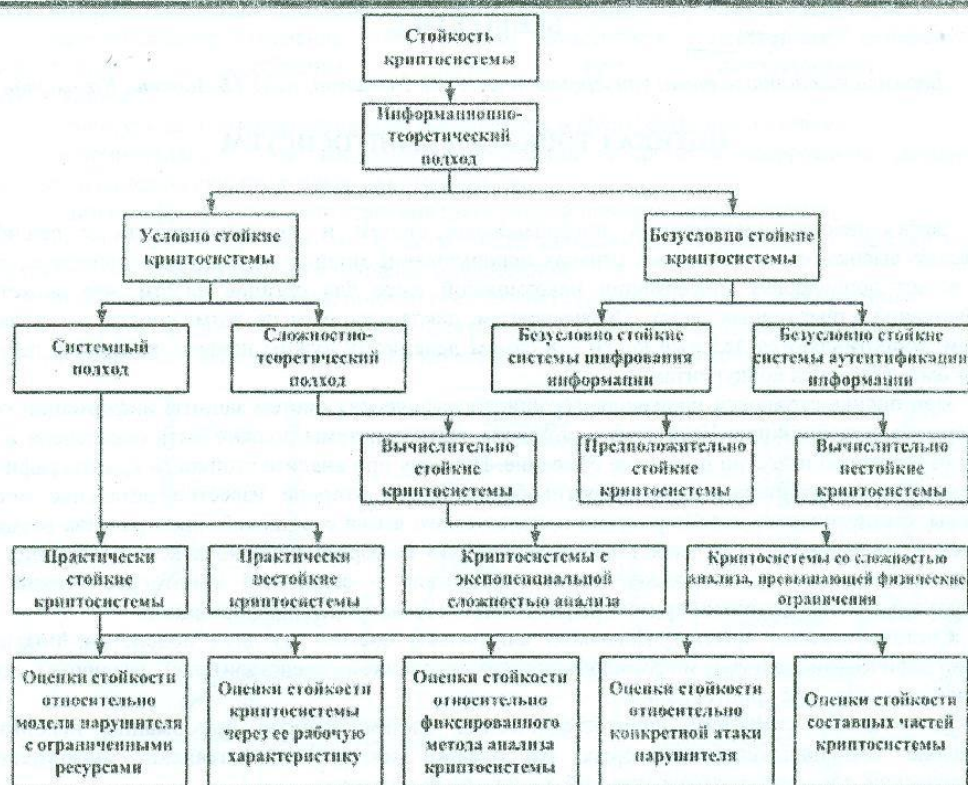
Система анализа криптографических алгоритмов состоит из двух подсистем: подсистемы криптографической защиты информации с использованием представителей различных классов шифров и подсистемы криптоанализа.

Для оценки стойкости криптографических систем защиты информации используются различные подходы, среди которых наибольший интерес представляют информационно-теоретический, сложностно-теоретический и системный подходы.

В соответствии с информационно-теоретическим подходом к оценке стойкости криптографических систем они могут быть разделены на, безусловно стойкие и на условно стойкие криптосистемы. Стойкость безусловно стойких криптографических систем не зависит ни от каких возможностей нарушителя и условий ее определения и не может быть уменьшена ни при каких обстоятельствах.

Стойкость условно стойких криптографических систем зависит от возможностей противоборствующей стороны и условий ее определения, и ее оценки могут меняться в зависимости от многих факторов.

Выяснение вопроса, является ли криптосистема безусловно или условно стойкой, составляет важную задачу информационно-теоретического подхода к оценке стойкости произвольных криптографических систем защиты информации. Если в рамках информационно-теоретического подхода криптосистема признана условно стойкой, то уточнить степень ее стойкости можно с использованием сложностно-теоретического и системного подходов. В научно-технической литературе информационно-теоретический подход иногда относят к классу теоретических подходов к оценке стойкости криптосистем, а остальные – к классу практических подходов. На рис. 1. приведена классификационная схема оценок стойкости криптографических систем защиты информации.



1. Классификационная схема оценок стойкости криптографических систем защиты информации

Среди средств защиты информации от возможных атак нарушителя выделяются средства криптографической защиты информации. На них могут возлагаться следующие основные задачи:

- обеспечение секретности (конфиденциальности) передаваемой, обрабатываемой и хранимой информации;
- обеспечение целостности передаваемой, обрабатываемой и хранимой информации;
- обеспечение подлинности сообщений и корреспондентов (пользователей), а также подлинности взаимодействующих сетей и систем;
- установление авторства передаваемых и хранимых сообщений;
- обеспечение доступности для законных корреспондентов (пользователей) информации, ресурсов и услуг;
- обеспечение целостности самих средств криптографической защиты информации.

Функции, используемые в криптографических системах

Принципы построения криптографических систем защиты информации основаны на использовании математических функций специального вида, которые должны легко вычисляться законными пользователями, знающими «ключ», и очень сложно для всех не обладающих ключом.

Общее описание функций, используемых в криптографических системах

Рассмотрим пример произвольной функции $y = f(x)$, которую зададим графически (рис.2). Пусть задано множество $X = \{a, b, c, d, e\}$ и множество $Y = \{1, 2, 3, 4, 5\}$. Напомним, что функция определяется двумя множествами X и Y , и правилом f , которое назначает каждому элементу из множества X один элемент из множества Y . Множество X называется областью определения функции, а множество Y областью ее значений.



Рис. 2 Биъективная функция f и обратная к ней $g = f^{-1}$

Элемент y из множества Y является образом элемента x , а элемент x является прообразом y . Отображение элементов из множества X в множество Y записывают так: $f: X \rightarrow Y$.

Множество всех элементов y , имеющих хотя бы один прообраз, называется образом функции f и обозначается $\text{Im}(f)$.

Функция называется однозначной (отображением один в один), если каждый элемент из множества Y является образом не более одного элемента из множества X . Функция f называется биекцией, если она является однозначной и $\text{Im}(f) = Y$. Функция вида $g = f^{-1}$ называется обратной к f .

Среди биъективных функций есть класс функций называемых инволюциями, которые наиболее часто используются для построения симметричных криптографических систем защиты информация.

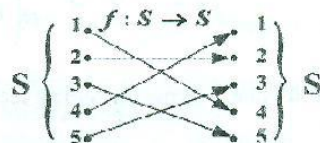


Рис. 3 Инволюция f для множества $S = \{1, 2, 3, 4, 5\}$

Биъективная функция называется инволюцией, если у функции совпадает область определения и область ее значений, т.е. $X = Y = S$, а также обратная функция с прямой $f = f^{-1}$. Пример инволюции для множества $S = \{1, 2, 3, 4, 5\}$ показан на рис. 3.

Существование обратной функции является основой построения систем шифрования информации, с помощью которой можно однозначно дешифровать криптограммы в сообщения.

Последовательное применение сначала функции шифрования, а затем функции дешифрования к произвольному сообщению $x \in S$ однозначно восстанавливает данное сообщение: $f(f(x)) = x$.

В Казахстане и ряде других стран существуют строгие ограничения на использование криптографии. Практически все виды деятельности, связанные с шифрованием информации, требуют получения государственной лицензии. Доступность стойких ко взлому криптографических систем, однако, является одним из важных факторов для развития электронного бизнеса. Хочется верить, что со временем ситуация в Казахстане позволит свободную разработку и использование стойких криптографических систем, что несомненно окажет положительное влияние на электронный рынок страны.

Литература

1. Теория электрической связи: учебное пособие / К.К. Васильев, В.А. Глушков, А.В. Дормидонтов, А.Г. Нестеренко; под общ. ред. К.К. Васильева. – Ульяновск: УлГТУ, 2008. – 452 с.
2. Брюс Шнайдер Прикладная криптография 2-е изд. М: 2000 г.
3. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии - М.: Издательство Московского центра непрерывного математического образования, 2000 г. С. 194-203.
4. Writing Secure Code / Michael Howard, David LeBlanc.: Microsoft Press 2002 г.
5. Дорогов А.Ю., Алексеев А.А. Математические модели быстрых нейронных сетей. В сб. научн. тр. СПбГЭТУ «Системы управления и обработки информации». Вып.490, 1996, с.79-84.