РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

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

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

болады. Бірақ сипатталған байланыс тәуекелдердің мөлшерін азайтады. Яғни, сканер мен жүйе екеуін бірге қолданған дұрыс болып табылады.

Қорытындылай келе, бұл жүйенің көмегімен көптеген жұмыстарды жасай алатынымызды білдік. Осы жүйені елімізге толығымен енгізіп, әрбір ұйымның немесе кәсіпорынның ақпараттарын ғана емес, мемлекеттегі маңызды жасырын құпия ақпараттарды қорғауға мүмкіндік алу. Жүйе тек қана қауіп төндіріп тұрғаны туралы ақпарат беретін болғандықтан, оны ары қарай дамытып, сол қауіптерді жоя алатындай жаңа бір жүйе ойлап табу қажет.

Пайдаланылған әдебиеттер тізім:

1. Котенко И. В., И. Б. Саенко, О. В. Полубелова. Перспективные системы хранения данных для мониторинга и управления безопасностью информации, Тр. СПИИРАН. 2013. № 25. С. 113-134.

2. Karlzen H. An Analysis of Security Information and Event Management: The Use of SIEMs for Log Collection, Management and Analysis. Department of Computer Science and Engineering, University of Gothenburg. 2009.

3. Kotenko I.V., Chechulin A.A. A Cyber Attack Modeling and Impact Assessment Framework // Proceedings of 5th International Conference on Cyber Conflict 2013 (CyCon 2013). 2013. pp. 119–142.

4. Файзуллин Р. Р., Васильев В. И. Метод оценки защищенности сети передачи данных в системе мониторинга и управления событиями информационной

УДК 519.713

АВТОМАТЫ БЕЗ ВЫХОДА В КРИПТОГРАФИИ

Шахметова Гульмира Балтабаевна
Евразийский национальный университет им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – Шарипбай А.А.

Еще с древних времен человечество интересовало обеспечение секретности передаваемой информации. Создавались различные виды кодирования информации, изобретались новые устройства для создания стойких шифров и легкого шифрования сообщений. Долгое время криптографические методы шифрования были засекречены, и применялась только с целью обеспечения секретности военных и государственных тайн. Ситуация кардинально поменялась в XX веке с появлением персональных компьютеров, тогда возникла естественная потребность в защите персональных данных. С развитием информационных технологий, на замену старых шифров приходили усовершенствованные и более стойкие алгоритмы шифрования/дешифрования, и как следствие интерес к такой науке, как криптография стремительно возрос. Основная цель криптографии – это обеспечить целостность, конфиденциальность, аутентификацию данных и неотказуемость авторства [1]. Достигаются эти задачи путем преобразования (шифрование) пересылаемого открытого текста в непонятный зашифрованный текст, а затем дешифрования этого сообщения обратно в его первоначальную форму.

Первое время широкую известность имела симметричная криптография, а позже и асимметричная. Симметричная криптография включает в себя криптографический алгоритм с использованием одного секретного ключа, в то время как асимметричное шифрование представляет собой криптосистему с двумя ключами: открытым и закрытым. В симметричной криптосистеме при шифровании и дешифровании пересылаемого сообщения используется один ключ, известный как отправителю, так и получателю и передаваемому по засекреченному каналу. В асимметричной криптосистеме передаваемое сообщение шифруется с помощью открытого общедоступного ключа, а для дешифрования данных

используется хранящийся в секрете закрытый ключ. Так же криптосистемы классифицируются на поточное и блочное шифрование. Основная идея блочного шифрования заключается в следующем: открытый текст разбивается на блоки одной длины и каждый блок шифруется отдельно. В поточном шифровании поток открытого текста шифруется побитно или побайтно с использованием последовательности ключей [2].

Каждая криптосистема имеет свои недостатки и преимущества. Симметричные криптосистемы в отличие от асимметричных легки в аппаратной реализации и быстры в исполнении, но имеют трудности в распространении ключей и не имеют цифровой подписи. Асимметричные криптосистемы, не смотря на то, что затрачивают больше вычислительных мощностей, могут обеспечить целостность и невозможность отказа от авторства, благодаря цифровой подписи. Различия так же просматриваются и в размерах ключей, в симметричном шифровании ключ относительно мал по сравнению с ключом асимметричного шифрования. Именно недостатки многих криптографических алгоритмов подталкивают к созданию радикально новых шифров, или усовершенствованию уже существующих. Как альтернативный метод проектирования криптосистем предлагается теория формальных языков и автоматов. На основе различных типов автоматов и грамматик, таких как автоматы Мили, клеточные автоматы, системы Линденмайера и другие, были созданы некоторые криптосистемы.

Теория формальных языков и автоматов, являясь фундаментальным направлением науки информатики, занимается исследованием порождающих и распознающих механизмов языков. Понятие автомата может служить модельным объектом в самых разнообразных задачах, благодаря чему возможно применение теории автоматов в различных научных и прикладных исследованиях. Это привело к широкому использованию теории языков и автоматов в физике и кибернетике, химии и биологии, экономике и статистике, в криптографии и других науках. Конечный автомат представляет собой абстрактное математическое устройство, работающее в дискретном времени. По способу работы автоматы можно разделить на два вида [3]: автомат-распознаватель и автомат-преобразователь. Автомат-распознаватель (или конечный автомат без выхода) распознает входные слова, т.е. отвечает на вопрос, принадлежит ли входное слово данному множеству. Автомат-преобразователь преобразует входные слова в выходные, т.е. реализует автоматное отображение. Два эти вида конечных автоматов нашли свое применение в реализации криптографических системах.

Автомат-преобразователь, а именно машина Мили, в 1985 году был впервые использован в создании криптосистемы с открытым ключом на основе конечных автоматов. Основоположником применения теории автоматов в криптографии был китайский профессор Tao Renji [4]. Данная криптосистема была названа FAPKC – Finite Automata Public Key Cryptosystem. Основная идея ее заключается в использовании слабо обратимого автомата. Слабо обратимый автомат – это автомат, который по начальному состоянию и выходной последовательности может восстановить входную последовательность [5]. В основе алгоритма лежит композиция двух конечных автоматов с памятью и некоторыми начальными и обратимыми состояниями. Задача разложения композиции конечных автоматов на составляющие компоненты является такой же трудной задачей, как и разложение на множители произведения двух больших чисел [6].

Не меньший интерес для ученных-криптологов представляли автоматы без выходов. В 2008 году P. Dömösi [7] спроектировал симметричную криптосистему, основанную на Rabin-Scott модели конечного автомата, в которой детерминированный автомат без выхода работает как ключ для шифрования открытого текста и дешифрования зашифрованного. В представленной системе для шифрования и дешифрования используется один и тот же секретный ключ, который состоит из матрицы переходов ключа-автомата без выхода, начального и конечных состояний. Каждому символу в наборе символов открытого текста присваивается одно или несколько конечных состояний ключа-автомата. Во время шифрования открытый текст читается последовательно символ за символом, и ключ-

автомат присваивает каждому текстовому символу символьную строку, длина которой регулируется в пределах заданного диапазона длины. Создается зашифрованный текст, связывая эти символьные строки вместе. Во время расшифровки ключ-автомат, начиная с начального состояния, считывает зашифрованный символ посимвольно, а расшифровка осуществляется путем связывания между собой текстовых символов, связанных с определенными конечными состояниями, что обеспечивает приведению открытого текста в его исходный вид [8].

В криптосистемах Dömösi применяется модифицированный конечный автомат без выхода $A = < Q, T, q_0, \delta, K, F >$, где

Q – конечное множество состояний,

T – входной алфавит,

q_0 – начальное состояние, $q_0 \in Q$,

δ – функция переходов: $Q \times T \to Q$,

F – множество кодирующих состояний, $F \subseteq Q$,

K – кодовый алфавит (здесь существует взаимно однозначное отображение между состояниями кода и буквами кодового алфавита) [9].

Рассмотрим небольшой пример шифрования и дешифрования с помощью метода Dömösi.

Пусть дан автомат A = ({a, b, c},{0,1},δ, a,{a, b},{0,1})

Функция перехода:

δ(a,0)=c, δ(a,1)=b,

δ(b,0)=a, δ(b,1)=c,

δ(c,0)=b, δ(c,1)=a.

Для удобства запишем переходы автомата в табличном виде:

	0	1	
δ	a	b	c
0	c	a	b
1	b	c	a

Открытый текст: ”10011”

Шифрование проходит следующим способом:

Символам открытого текста присваивается одно конечное состояние ключа-автомата 0=a и 1=b.

Генерируется случайная строка из символов алфавита состояний, фиксированной длины: abacabcb.

	1	0		0	1		1
a	b	a	c	a	b	c	b
	1	**0**	**0**	**1**	**1**	**1**	**0**

Получаем зашифрованный текст: “1001110”.

Дешифрование:

1	0	0	1	1	1	0	
a	b	a	c	a	b	c	b
	1	**0**		**0**	**1**		**1**

Получаем исходный текст: “10011”

Данная симметричная криптосистема имеет свои преимущества [10]:

- Генератор случайных чисел не зависит от ключа.

- Слабая обратимость автоматов не влияет на криптосистему, поэтому эта система не может быть атакована методами, используемыми для взлома криптосистем FAPKC.

- Ключ-автомат выбирается случайным образом из большого набора автоматов с более чем 256 состояниями и более чем 256 входными сигналами, т. е. более 256 (256!) возможные ключевые автоматы генерируются случайным образом.

К недостаткам можно отнести то, что шифрованный текст получается в много раз длиннее открытого текста.

Рассмотренная в статье криптосистема не являются единственно возможной сферой применения автомата без выхода в криптографии. К примеру, в работе [11] расскрывается особенность работы нового блочного шифра на основе автоматов Глушкова (перестановочных автоматов). Криптосистема состоит из двух основных частей: генератора псевдослучайных чисел и набора автоматов перестановок. Авторы G. Khaleel и др. [12, 13] предложили усовершенствованный алгоритм шифрования Dömösi, в которой используется дополнительная система управления. Предложенная система управления предотвращает обратный поиск в алгоритме шифрования Dömösi, генерируя два вектора в соответствии с текущим состоянием, входными символами и конечными состояниями. Система управления состоит из этапа инициализации и этапа эксплуатации. Модифицированная криптосистема имеет такую же криптостойкость к взломам как и первоначальная система шифрования Dömösi.

Список использованных источников:

1. Шнайер Б. Прикладная криптография: протоколы, алгоритмы и исходные тексты на языке С. 2-е издание. – Москва: Триумф, 2002. -816 с.
2. Бабенко Л.К., Ищукова А.Е., Сидоров И.Д. Параллельные алгоритмы для решения задач защиты информации. - Горячая линия-Телеком, 2014. – 299 с.
3. Лупал М.А. Теория автоматов. Учебное пособие. – СПб., 2000. – 119 с.
4. Dai Z.D., Ye D.F., Lam K.Y. Weak Invertability of Finite Automata and Cryptanalysis on FAPKC // LNCS. – 1998. – № 1514. – P 227-241.
5. Катеринский Д.А. Об обратимости конечных автоматов с конечной задержкой // Прикладная дискретная математика. Приложение Математические методы криптографии. – 2013. – №6. – С 35-36.
6. Сатыбалдина Д.Ж. Разработка методов и алгоритмов криптографической защиты информации. Доклад научной работы на соискание академической степени доктора философии (PhD). – Астана, 2011. – 17 с.
7. KhaleelG., TuraevS., I. Al-Shaikhli, M.I. Mohd Tamrin. An overview of cryptosystems based on finite automata // Journal of Advanced Review on Scientific Research. –2016. –V.27, Issue 1. – С 1-7.
8. Dömösi P. A novel cryptosystem based on finite automata without outputs // M. Ito, Y. Koboyashi, and K. Shoji (eds.), Automata, Formal Languages and Algebraic Systems, World Scientific, - 2008. P. 23-32,
9. Dömösi P., Horváth G. A Novel Stream Cipher Based on Deterministic Finite Automaton. Lecture note. - NCMA, 2017. – 37 p.
10. Khaleel G., Turaev, S., Zhukabayeva T. A novel stream cipher based on nondeterministic finite automata // Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSSM 2016). - Tomsk, Russia, 2016. – P. 110-191.
11. Dömösi P., Horváth G. A Novel Cryptosystem Based on Gluskov Product of Automata // Acta Cybernetica. – 2015. – P. 359–371.
12. Khaleel Gh., Turaev Sh, Zhukabayeva T. A Novel Stream Cipher Based on Nondeterministic Finite Automata // AIP Conference Proceedings 1705, 020007, 2016.
13. Khaleel Gh., Turaev Sh, M. Izzuddin M. Tamrin, Imad F. Al-Shaikhli. Performance and Security Improvements of Dömösi's Cryptosystem // International Journal of Applied Mathematics and Statistics. – V.55, № 2. – 2016. – P. 32-45.