УДК 004.056.5
МРНТИ 81.93.29

К ВОПРОСУ О ПРОБЛЕМЕ СОВРЕМЕННЫХ ТЕНДЕНЦИЙ КРИПТОГРАФИИ

Н.А. КАПАЛОВА[1,2], ANDRZEJ KOTYRA[3], А.Ж. АБИШЕВА[1,2]

[1]Институт информационных и вычислительных технологий КН МОН РК
[2]Казахский Национальный университет имени аль-Фараби
[3]Люблинский технический университет, Польша

Аннотация: *Данная статья раскрывает понятие криптографии. Описывает существующие методы и проблемы криптосинтеза. Криптографические исследования несомненно впечатляют и являются важным вкладом в будущее. В данной работе рассматриваются криптографические алгоритмы, т.е. строительные блоки, используемые для разработки систем и протоколов. Проведен анализ в распространенных криптосистемах, которые связаны именно с недостатками проектирования и реализации. Пока нет оснований полагать, что этот тренд в ближайшее время изменится, поэтому наравне с теоретическими исследованиями нельзя забывать и о повышении качества работы инженеров, проектирующих, разрабатывающих и внедряющих системы, использующие криптографию. Приведенные различные примеры показывают как важна криптография на сегодняшний день и как эта наука будет развиваться в дальнейшем.*

Ключевые слова: *шифрование, криптография, ключевое и бесключевое хеширование, аутентификация, сертификат открытого ключа*

TO THE QUESTION OF THE PROBLEM OF MODERN TRENDS OF CRYPTOGRAPHY

Abstract: *This article reveals the concept of cryptography. Describes existing methods and problems of cryptosynthesis. Cryptographic research is undoubtedly impressive and an important contribution to the future. In this paper, cryptographic algorithms are considered, i.e. building blocks used to develop systems and protocols. An analysis is made in common cryptosystems that are associated precisely with design and implementation flaws. While there is no reason to believe that this trend will change in the near future, therefore, along with theoretical research, one should not forget about improving the quality of work of engineers who design, develop and implement systems using cryptography. The various different examples show how important cryptography is today and how this science will develop in the future.*

Keywords: *encryption, cryptography, key and keyless hashing, authentication, public key certificate*

ЗАМАНАУИ КРИПТОГРАФИЯЛЫҚ ТЕНДЕНЦИЯЛАРДЫҢ МӘСЕЛЕЛЕРІ ТУРАЛЫ

Аңдатпа: *Бұл мақалада криптография ұғымы ашылады. Криптосинтездің қолданыстағы әдістері мен мәселелерін сипаттайды. Бүгінгі криптографияның маңыздылығы және болашақта бұл ғылымның даму барысы жайлы айтылады. Аталған еңбекте жүйелер мен хаттамаларды жасау үшін пайдаланылатын құрылыс блоктары, яғни криптографиялық алгоритмдер қарастырылған. Талдау дәл жобалау мен іске асырудағы қателіктермен байланысты жалпы криптожүйелерде жасалады. Бұл тенденция жақын арада өзгереді деп айтуға негіз жоқ, сондықтан теориялық зерттеулермен қатар криптографияны қолдана отырып, жүйелерді жобалау, әзірлеу және енгізу инженерлердің жұмыс сапасын жақсарту туралы ұмытпау керек. Әртүрлі мысалдар криптографияның бүгінгі күннің қаншалықты маңызды екендігін және болашақта бұл ғылымның қалай дамитынын көрсетеді.*

Түйінді сөздер: *шифрлау, криптография, кілттік және кілтсіз хэштер, аутентификация, ашық кілт сертификаттары*

ВВЕДЕНИЕ

В настоящее время, например, средства электронной почты используются не только для общения между людьми, но и для передачи контрактов и конфиденциальной финансовой информации. Web-сервера используются не только для рекламных целей, но и для распространения программного обеспечения и электронной коммерции. Электронная почта, доступ к Web-серверу, электронная коммерция, VPN требуют применения дополнительных средств для обеспечения конфиденциальности, аутентификации, контроля доступа, целостности и идентификации [2]. В настоящее время в качестве таких средств используется стойкая криптография.

На протяжении всей своей истории человечество нуждается в шифровании той или иной информации. Из такой потребности выросла целая наука – ***криптография***. Ранее криптография служила только интерресам государства, но с появлением интернета ее методы стали интересовать и частных лиц. На сегодняшний день криптография широко используется хакерами, борцами за свободу информации и простыми пользователями, желающими защитить свои данные в сети.

Чтобы понять, как развивалась наука криптография, обратимся к ее истории. ***Криптография*** (с греческого – «тайнопись») – наука о защите информации с использованием математических методов. Первый труд о криптографии был написан еще до Рождества Христова. Первые уже надежные системы защиты информации были разработаны в Китае. Чаще всего шифрование информации использовалось в военных делах [3].

Криптография активно развивалась в Средние века, шифрованием сообщений часто пользовались дипломаты и купцы. Одним из самых известных шифров Средних веков называют кодекс Copiale – изящно оформленную рукопись с водяными знаками, не расшифрованную до сих пор. Во времена Эпохи Возрождения Френсис Бэкон описал 7 методов скрытого текста, а также он предложил двоичный метод шифрования. Во время Первой мировой войны криптография стала признанным боевым инструментом. Вторая мировая война послужила своеобразным катализатором развития компьютерных систем – через криптографию [6]. Использованные шифровальные машины (немецкая «Энигма» (рис. 1), английская «Бомба Тьюринга» (рис. 2)) ясно показали жизненную важность информационного контроля [1, с. 2].

В XX веке сформировался современный подход к криптографии. Эта наука была разделена на две части: криптосинтез и криптоанализ. Криптосинтез обеспечивал защиту информации, а криптоанализ ищет пути взлома системы. Как упоминалось ранее, в криптографии определены некоторые методы. Их можно подразделить в зависимости от количества ключей, которые используются в соответствующих алгоритмах [4]:

- двухключевые;
- одноключевые;
- бесключевые.

МЕТОДЫ ИССЛЕДОВАНИЯ

В двух ключевых алгоритмах используется два ключа: открытый и секретный. В одноключевом используется обычный секретный ключ. И в бесключевом алгоритме не используются какие-либо ключи вообще. Следует также отметить и остальные криптографические методы.

Электронная подпись, где алгоритм использует два вида ключей: секретный и открытый. Используется для подтверждения целостности данных и авторства.

Аутентификация. Данный метод позволяет определить действительно ли пользователь является тем, за кого себя выдает.

Методы криптографического контрольного суммирования:

- вычисление имитоприставок;
- ключевое и бесключевое хеширование;
- использование кодов аутентификации сообщений.

Рис. 1 – Шифровальная машина Третьего рейха «Энигма»

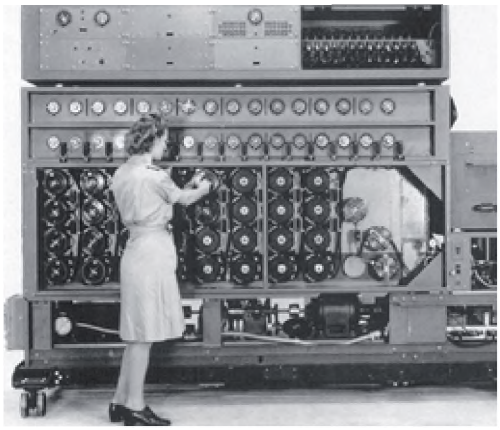

Рис. 2 – Шифровальная машина «Бомба Тьюринга»

Все эти методы применяются в защите данных, когда нельзя использовать электронную подпись, и в разных схемах аутентификации [5].

Генераторы случайных и псевдослучайных используются в криптографии, в частности:

- для генерации секретных ключей;
- в большинстве алгоритмов электронной подписи;
- в большинстве схемах аутентификации.

Как видно из рис. 3 алгоритмы шифрования можно разделить на две категории:

- алгоритмы асимметричного шифрования;
- алгоритмы симметричного шифрования.

Криптография с открытым ключом представляет собой форму обеспечения конфиденциальности сообщений, подразумевающую создание *открытого* и *закрытого* ключей. Закрытый ключ хранится в секрете, а открытый ключ передается другим лицам. Хотя ключи математически связаны, закрытый ключ нельзя легко вычислить с помощью открытого ключа. Открытый ключ можно использовать для шифрования данных, которые сможет расшифровать только соответствующий закрытый ключ. Это может использоваться для шифрования сообщений для владельца закрытого ключа.

Аналогичным образом владелец закрытого ключа может шифровать данные, которые могут быть расшифрованы только с помощью открытого ключа. Такое использование – это основа цифровых сертификатов, в которых сведения, содержащиеся в сертификате, зашифрованы владельцем закрытого ключа, подразумеваемым автором содержимого. Поскольку ключи шифрования и расшифровки разные, они называются *асимметричными* ключами [7].

Как сертификаты, так и асимметричные ключи представляют собой способы асимметричного шифрования. Сертификаты часто используются как контейнеры для асимметричных ключей, так как они могут содержать дополнительные данные, например, о датах окончания действия и поставщиках. Не существует различий между двумя механизмами для алгоритма шифрования, равно как и различий в надежности при одинаковой длине ключа. Как правило, сертификат используется для шифрования других типов ключей шифрования в базе данных или подписи программных модулей [8].

Сертификаты и асимметричные ключи можно применять для расшифровки данных, зашифрованных другим способом. Обычно асимметричный ключ используется для шифрования симметричного ключа перед его сохранением в базе данных. В отличие от сертификата открытый ключ не имеет определенного формата, и его нельзя экспортировать в файл.

Несомненно, криптография будет развиваться дальше весьма активно. Одна из ее

задач на будущее – разработка скоростных методов шифрования с высоким уровнем секретности. Эта задача обусловлена большим количеством каналов связи (беспроводные сети, сотовая связь), по которым передаются очень большие объемы информации.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

В алгоритме симметричного шифрования обычно используется тот же самый ключ, которым зашифровывали данные, или используют другой ключ, который связан с основным ключом простым соотношением. А в алгоритме ассиметричного шифрования используется ключ зашифрования k1, который легко вычисляется из ключа k2 таким образом, что обратное вычисление невозможно [9, с. 28].

Несмотря на новизну криптографии как науки, у нее уже имеются нерешенные проблемы. На сегодняшний день специалисты выделяют несколько проблем в криптографии [10]. К ним относят:

- ограниченность рабочих схем с открытым ключом;
- отсутствие перспектив;
- увеличение размера шифрируемых блоков данных и ключей к ним;
- ненадежность фундамента шифрования.

ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Рассмотрим каждую из них в отдельности.

Ограниченность рабочих схем с открытым ключом. Несмотря на то, что в криптографии существует множество алгоритмов для шифрования данных, о чем говорилось ранее, которые могут быть получены путем комбинации разных простых изменений, каждая схема основывается на, так называемой, «нерешаемой» задаче. Таким образом, мы понимаем, что количество криптографических схем крайне ограничено [11].

Отсутствие перспектив. В настоящее время в теории науки криптография существуют *квантовые вычисления* – эффективная вычислительная модель, основанная на параллелизации вычислительных процессов за счет преобразования входной инфор-

Рис. 3 – Классификация криптографических методов

мации. Это значит, что можно одновременно вычислить значение функции для всех её аргументов за один вызов функции. Такие вычисления позволят в будущем решать задачи гораздо быстрее, чем на обычных компьютерах, а значит будущее криптографии весьма туманно.

Увеличение размера шифрируемых блоков данных и ключей. Быстрые темпы развития вычислительной техники приводят к увеличению размеров блоков, данных и их ключей. В доказательство приведем пример. Изначально для создания криптосистемы RSA было достаточно 512 бит, а сейчас рекомендуемый объем составляет не менее 4096 бит. Аналогичная ситуация происходит и в других методах шифрования. В традиционной криптографии объем памяти для создания системы увеличился всего лишь в 2 раза [12].

Ненадежность фундамента шифрования. В рамках теории вычислительной сложности доказана связь между сложновычисляемыми задачами и их аналогами. Это значит, что, если будет подобран ключ к одной криптосистеме, то откроются и остальные, так как аналогичные задачи имеют одинаковую или весьма похожую основу.

ВЫВОДЫ

Из вышесказанного можно сделать вывод о том, что сейчас в криптографии актуальны проблемы усложнения криптосистем, повышение стойкости алгоритмов, а также уменьшение размеров блоков данных.

Но следует помнить о том, что криптографические алгоритмы – это всего лишь строительные блоки, используемые для разработки систем и протоколов. Почти все самые громкие уязвимости в распространенных криптосистемах связаны именно с недостатками проектирования и реализации. Пока нет оснований полагать, что этот тренд в ближайшее время изменится, поэтому наравне с теоретическими иссследованиями нельзя забывать и о повышении качества работы инженеров, проектирующих, разрабатывающих и внедряющих системы, использующие криптографию.

Работа выполнена за счет средств программно-целевого финансирования научных исследований на 2018-2020 годы по проекту «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения».

ЛИТЕРАТУРА

1. Нил Стивенсон. Криптономикон. – Нью-Йорк, 1999. – 928 с.
2. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования. – М.: ФОРУМ: ИНФРА-М, 2002. – 243 с.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: изд.-во ТРИУМФ, 2002. – 816 с.
4. Введение в криптографию / Под. общей ред. В.В. Ященко. – 3-е изд. – М.: МЦНМО, 2000. – 288 с.
5. Столлингс В. Криптография и защита сетей. Принципы и практика. – М.: «Вильямс», 2001. – 698 с.
6. Бабаш А.В., Шанкин Г.П. История криптографии. Часть 1. – М.: Гелиос АРВ, 2002. – 240 с.
7. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. 2-е изд. – М.: Гелиос АРВ, 2002. – 480 с.
8. James M. Stewart, Mike Chapple, Darril Gibson. CISSP: Certifi ed Information Systems Security Professional Study Guide, 6th Edition. - Sybex, 2012. 936 p.
9. Shon Harris, CISSP All-in-One Exam Guide, 6th Edition -McGrawHill, 2012. 1216 p.
10. Бунин О. Занимательное шифрование // Журнал «Мир ПК». – 2003. – № 7.
11. Панасенко С.П., Ракитин В.В. Аппаратные шифраторы // Журнал «Мир ПК». – 2002. – № 8.
12. Lieven, M.K. et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance // Nature 414. 20–27 Dec. 2001.