CENTRAL ASIAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES

Volume: 03 Issue: 02 | Feb 2022 ISSN: 2660-5317

Основные методы и современные тенденции криптографии

асс. Шарипова У.Б. асс. П. Ф. Насриддинова

Самаркандский филиал Ташкентского университета
информационных технологий имени Мухаммада ал-Хорезми
umka_azi@mail.ru

Received 26th Jan 2022, Accepted 4th Feb 2022, Online 28rd Feb 2022

Аннотация: *Данная статья раскрывает понятие криптографии. Описывает существующие методы и проблемы криптосинтеза. Рассказывает о том, как важна криптография на сегодняшний день и как эта наука будет развиваться в дальнейшем.*

Ключевые понятия: *ключевые понятия: криптография, техника, электронная подпись, аутентификация*

На протяжении всей своей истории человечество нуждается в шифровании той или иной информации.

Из такой потребности выросла целая наука — криптография. Ранее криптография служила только интересам 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.

Криптография (с греческого —«тайнопись») — наука о защите информации с использованием математических методов. Первый труд о криптографии был написан еще до Средних век. Первые уже надежные системы защиты информации были разработаны в Китае. Чаще всего шифрование информации использовалось в военных делах.

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. Использованные шифровальные машины (немецкая «Энигма» (Рис. 1), английская «Бомба Тьюринга» (Рис. 2)) ясно показали жизненную важность информационного контроля. [1, с. 2]

В 20 в. 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:

Рис. 1. Шифровальная машина Третьего рейха «Энигма»

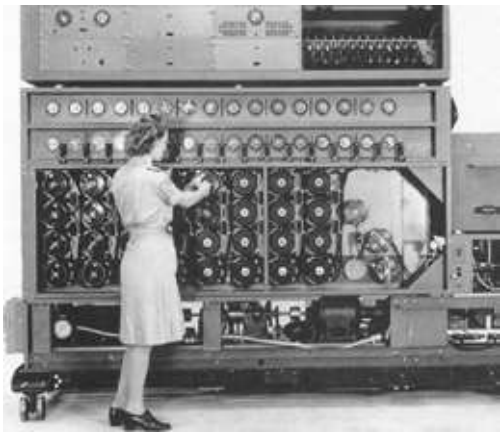

Рис. 2. Шифровальная машина «Бомба Тьюринга»

— двухключевые;

— одноключевые;

— бесключевые.

В двухключевых 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, такие как:

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 имитовставок;

ключевое и бесключевое хеширование;

использование кодов аутентификации сообщений.

Все эти методы используются в защите данных, когда нельзя использовать электронную подпись и в разных схемах аутентификации.

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

Рис. 3. Классификация криптографических методов

В алгоритме симметричного шифрования обычно и пользуется 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. [6, с. 28]

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

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

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.

«Отсутствие перспектив». В настоящее время в теории науки криптография существуют квантовые вычисления — эффективная вычислительная модель, основанная на параллелизации вычислительных процессов за счет преобразования входной информации. 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 своих слов, приведем пример. Изначально для создания криптосистемы RSA было достаточно 512 бит, а сейчас рекомендуемый объем составляет не менее 4096 бит. Аналогичная ситуация про- исходит и в других методах шифрования. В традиционной криптографии объем памяти для создания системы увеличился всего лишь в 2 раза.

«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.

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

Криптографические исследования несомненно впечатляют и являются важным вкладом в будущее. 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 исследованиями нельзя забывать и о повышении качества работы инженеров, проектирующих, разрабатывающих и внедряющих системы, использующие криптографию.

На сегодняшний день, криптография занимает в жизни каждого человека важное место. Любой человек хотя бы раз в день сталкивается с шифрованием данных. Все большее и большее количество информации передается по тем каналам связи, которые требуют особой защищенности данных. Современная криптография полностью основана на математике. Основная задача, которую преследует математика в криптографии — это криптографическая стойкость, т. е. способность противостоять теоретическому и практическому взлому. Таким образом, системы шифрования, применяющиеся в криптографических системах сети Интернет (RSA, ElGamal, Shamir и др.) используют последние достижения теории чисел и алгебры. Взломать их — значит решить сложные математические задачи.

Некоторые проблемы имеющихся методов криптографии может решить, так называемая, квантовая криптография. Квантовая криптография — это сравнительно новое направление исследований, позволяющее применять эффекты квантовой физики для создания секретных каналов передачи данных. В квантовой криптографии используется фундаментальная особенность квантовых систем, заключающаяся в принципиальной невозможности точного детектирования состояния такой системы, принимающей одно из набора нескольких неортогональных состояний. На пути практической реализации систем квантовой коммуникации возникает ряд таких технических трудностей. В настоящее время уже несколько фирм предлагают первые коммерческие системы квантовой криптографии. Очевидно, что квантовые системы еще не скоро войдут в массовое пользование, однако уже сейчас они могут найти свое применение для защиты особо важных каналов связи. [8, с. 34]

Криптографию и криптоанализ назвали наиболее важными формами разведки в современном мире. А они сводятся к математическим вычислениям. В то же время, криптография — это искусство. Иногда объекты, которые она исследует, могут не подчиняться математическим законам, и тогда на помощь приходит воображение.

Одно из новых направлений в исследовании криптографии — исследование методов защиты шифров от атак по сторонним каналам, от «нечестного» криптоанализа, который проводится на

основе «прослушивания» реализации шифра.

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.

Литература.

1. Нил Стивенсон «Криптономикон». 1999 г.
2. Партыка, Т. Л., Попов И. И. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования. — М.: ФОРУМ: ИНФРА-М, 2004.
3. Крысин, А. В. Информационная безопасность. Практическое руководство — М.: СПАРРК, К. :ВЕК+,2003.
4. Тарасюк, М. В. Защищенные информационные технологии. Проектирование и применение — М.: СОЛОН-Пресс, 2004.
5. Лукашов, И. В. Криптография? Железно! //Журнал «Мир ПК». 2003. № 3.
6. Панасенко, С. П., Защита информации в компьютерных сетях // Журнал «Мир ПК» 2002 № №2.,8.,5.
7. Бунин, О. Занимательное шифрование // Журнал «Мир ПК» 2003 № 7.
8. Lieven, M. K. et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance// Nature 414. 20–27 Dec. 2001.

