УДК: 003.26(076.1)

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ

Дегтярева Анна Александровна

студент

Пчелинцева Наталия Владимировна

старший преподаватель

natas79@mail.ru

Макова Наталья Евгеньевна

доцент

nemakova@mail.ru

Мичуринский государственный аграрный университет

г. Мичуринск, Россия

Аннотация: в статье речь идет о криптологии как одной из областей применения математики.

Ключевые слова: криптология, шифры, шифрование, расшифрование, задачи криптографии.

Одной из важнейших областей применений математики является криптография — наука о шифрах, т. е. способах преобразования информации, позволяющих скрывать её содержание от посторонних.

С развитием электронных коммуникаций криптография стала предметом интереса более широкого круга потребителей: возникла необходимость защиты технических, коммерческих, персональных и других данных, передаваемых негосударственными организациями по общедоступным каналам связи [1-4].

Основы современной теории секретной связи были разработаны Клодом Шенноном во время Второй мировой войны. Им была теоретически обоснована возможность построения совершенного шифра — такого способа шифрования, что у перехватившего преобразованное сообщение злоумышленника не будет ни одной «зацепки» для выделения исходного сообщения [5].

«Все любят разгадывать других, но никто не любит быть разгаданным», — эти слова французского писателя-моралиста Ларошфуко как нельзя лучше отражают сущность современной криптологии как соревнования методов криптографии и криптоанализа [1, 6].

Безусловно, древние криптосистемы не используются сегодня на практике. Мы не преувеличим, сказав, что криптография является ровесницей письменности: простейшей криптосистемой явилась сама возможность сохранения информации в виде надписи, недоступной для непосвящённых - не владеющих чтением. В дальнейшем, чтобы скрыть смысл написанного от нежелательных получателей, приходилось придумывать более сложные методы преобразования текста: использование нестандартных обозначений для букв (иероглифов, клинописных знаков), употребление чисел вместо некоторых слов и т.п.

Стоит отметить, что для многих древних цивилизаций криптография не была чем-то экзотическим. Так, в Древней Индии было известно порядка 60 способов письма (считалось, что большинством из них владел в своё время и сам Будда), а в Кама-сутре среди искусств, которыми должна была в обязательном порядке владеть женщина, упоминается и криптография. Древнееврейский шифр «Атбаш» (ивр. известен с VI века до н.э.) [2, 6, 7]

Известен также шифр, называемый «квадрат Полибия» (II век до н.э.). Весь алфавит греческий или латинский помещался в квадрат 5×5, столбцы и строки которого нумеровали цифрами от 1 до 5. В каждую клетку вписывали одну букву. В греческом варианте одна клетка оставалась пустой, а в латинском, наоборот, в одну из клеток вписывались две буквы. В результате

каждой букве соответствовала пара цифр и шифрованное сообщение представляло последовательность пар цифр.

В I веке н.э. Юлий Цезарь пользовался шифром, в котором каждая буква открытого текста заменяется третьей после нее буквой в алфавите, который считается написанным по кругу, т.е. после буквы «я» следует буква «а». Можно было заменять и не только третьей, главное, чтобы тот, кому посылается зашифрованное сообщение, знал эту величину. Понятно, что применять подобные шифры при больших объёмах переписки неудобно. Как правило, для шифрования используют электронные устройства или компьютерные программы, реализующие сложные алгоритмы преобразования сколь угодно длинных сообщений с помощью секретных ключей [1, 3, 8]. Таким образом, при выбранном алгоритме зашифрованное сообщение является функцией от исходного сообщения и ключа. Эту связь можно рассматривать как уравнение относительно ключа, если известны алгоритм, исходное и зашифрованное сообщения. Чтобы обеспечить практическую невозможность решения таких уравнений перебором всех возможных ключей, множество этих ключей должно быть астрономически велико.

В последние десятилетия в криптографии стали появляться шифры, стойкость которых обосновывается сложностью решения чисто математических задач: разложения больших чисел на множители, решения показательных сравнений в целых числах и других. Стойкость шифров зависит также и от качества генераторов случайных чисел, порождающих ключи.

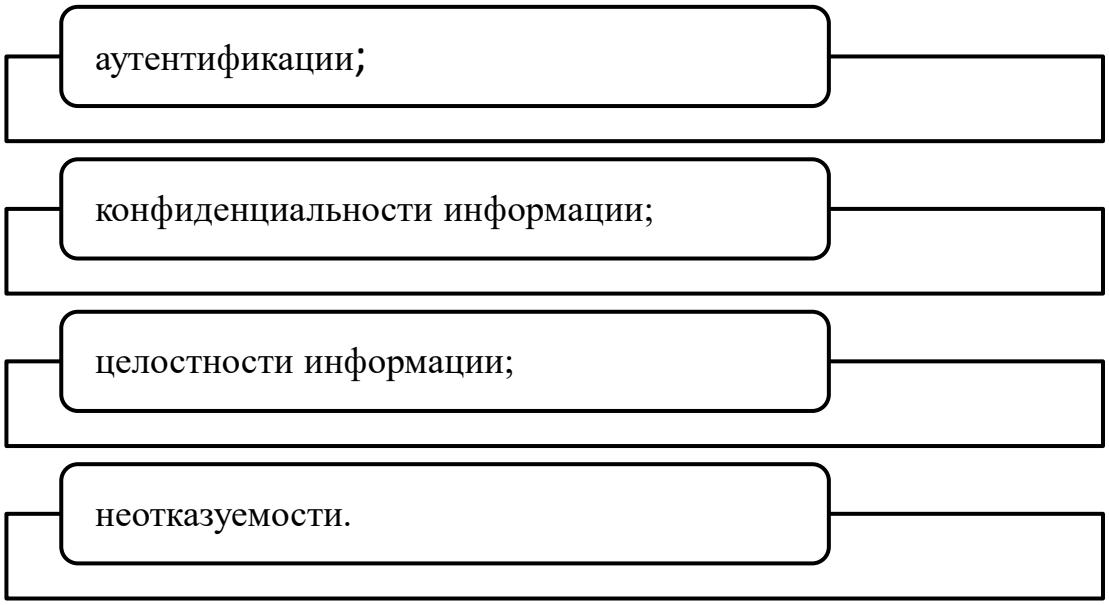
Методы и результаты различных разделов математики (в частности, алгебры, комбинаторики, теории чисел, теории алгоритмов, теории вероятностей и математической статистики) используются как при разработке шифров, так и при их исследованиях, в частности, при поиске методов вскрытия шифров. Шифр можно считать стойким, пока при его исследовании не выявляются особенности, которые потенциально можно

использовать для вскрытия шифра. Для пользователей шифра очень важно узнать, что он ненадёжен, раньше, чем этим смогут воспользоваться злоумышленники.

В настоящее время криптология− это наука, содержащая две взаимосвязанные части, а именно, криптографию, изучающую различные методы шифрования текстов и их расшифрования, и криптоанализ, изучающий методы, позволяющие расшифровать перехваченное сообщение, не зная самого ключа для расшифрования.

Криптография используется в таких отраслях как электронная коммерция, телекоммуникация, интернет и др..

Итак, изначально криптография (cryptography) возникла как наука, изучающая методы преобразования информации с целью сокрытия её смысла от нежелательных получателей. Сейчас задачи криптографии значительно шире, как минимум можно говорить о том, что она является основой для обеспечения:



Конфиденциальность информации (confidentiality) означает, что она остаётся недоступной для всех, кроме легальных пользователей. Конфиденциальность достигается за счёт использования симметричных и асимметричных криптосистем

Целостность информации (integrity) [9] рассматривается как подтверждение её неизменности при хранении или передачи. Механизмы контроля целостности позволяют получателю сообщения убедиться в том, что оно осталось неизменным в процессе передачи. Контроль целостности реализуется с использованием криптографических хэш-функций и цифровых подписей.

Аутентификация (authentication) [8, 9] представляет собой процесс подтверждения подлинности предъявленного идентификатора и используется преимущественно для обеспечения контроля доступа к определённым ресурсам или сервисам. В протоколах аутентификации используются все без исключения криптографические примитивы.

Неотказуемость (nonrepudiation) защищает получателя сообщения от возможной попытки отравителя отказаться от авторства отправленного ранее сообщения. Неотказуемость может быть реализована только средствами криптографии с открытым ключом.

Криптография является богатым источником трудных математических задач, а математика — одной из основ криптографии. История показывает, что рано или поздно развитие математических методов и техники приводит к тому, что задачи, казавшиеся неразрешимыми, находят решение. Отставание в творческом соревновании математиков разных стран может привести к поражениям в экономике, дипломатии и военных операциях.

Список литературы:

1. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва : Издательство Юрайт, 2020;

2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для академического

бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2019;

3. Петрушин В.Н. Нормальное и бета-распределение а оценке ограниченных случайных величин / В.Н. Петрушин, Н.В. Картечина // Вестник МГУП имени Ивана Федорова. – 2007. – № 3. – С. 63-70;

4. Пчелинцева Н.В. Методические аспекты количественной оценки риска в аграрной сфере производства / Н.В. Пчелинцева // Наука и Образование. – 2019. – № 3. – С. 37.

5. Кузнецов П.Н. Информационное обеспечение техники в Тамбовской области / П.Н. Кузнецов, В.В. Хатунцев, А.П. Кузнецова //Наука и Образование. – 2019. – № 4. – С. 263.

6. Кузнецов П.Н. Информационно-техническое обеспечение проведения процессов технического сервиса техники / П.Н. Кузнецов, В.В. Хатунцев, А.П. Кузнецова // Наука и Образование. – 2019. – № 2. – С. 216.

7. Абалуев Р.Н. Машинное обучение в среде СУБД MS SQL SERVER / Р.Н. Абалуев, А.А. Крумкаченко // Наука и Образование – 2019. – №4. – С. 52.

8. Сравнение нормального распределения и эмпирической функции распределения при статистической обработке результатов измерений / Н.В. Картечина, Л.В. Бобрович, Н.В. Пчелинцева, О.С. Картечина // Наука и Образование. – 2019. – № 3. – С. 20.

9. Коротков А.А., Автоматизированные системы контроля в сельском хозяйстве в контексте реализации концепта IoTAGRO / А.А. Коротков, И.П. Криволапов // Наука и образование. – 2019. – № 2

MATHEMATICAL FOUNDATIONS OF CRYPTOLOGY

Degtyareva Anna Aleksandrovna
student
Pchelintseva Natalia Vladimirovna
senior lecturer
natas79@mail.ru
Makova Natalya Evgenievna
Associate Professor
nemakova@mail.ru
Michurinsk State Agrarian University
Michurinsk, Russia

Abstract: the article deals with cryptology as one of the areas of application of mathematics.

Keywords: cryptology, ciphers, encryption, decryption, cryptography tasks.