ПЕРЕСТАНОВОЧНЫЕ МЕТОДЫ В ЗАЩИТЕ ИНФОРМАЦИИ

В.А. Липницкий, М.Н. Королева
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектороники
Кафедра высшей математики №3, Белорусский национальный технический университет
Минск, Республика Беларусь
E-mail: margo010172@ramblerl.ru

Глобализация современного общества ведет к тому, что проблемы защиты, передачи и хранения информации приобретают статус ключевых в XXI веке, а применение сложныных математических структур будет способствовать наиболее успешному решению этой задачи
Ключевые слова: защита информации от несанкционированного доступа, защита инфор- мации от помех, перестановочные методы, теория групп, группы подстановок.

ВВЕДЕНИЕ

Современные научные исследователи склоняются к той парадигме, что человеческое общество переживает эпоху, которую следует назвать информационной. И действительно, любой военный конфликт сейчас начинается, прежде всего, с информационной войны. Работа воздушного и наземного транспорта, сложные индустриальные технологические процессы (АЭС, мартены, прокатные станы и многое другое) невозможны без соответствующей грамотной информационной поддержки. Любая чрезвычайная ситуация в жизни общества требует достоверной, надежной и точной информации обо всех обстоятельствах возникшей проблемы для выработки быстрого, мотивированного решения и адекватного выхода из этой ситуации. Именно в наши дни правдивая и своевременная информация приобретает, зачастую, бесценное или неоценимое значение. Поэтому совершенно естественно, что защита информации приобрела столь высокое значение и неослабевающий интерес государственных органов, бизнеса, коммерческих и производственных фирм, науки и производства, практически всех слоев общества. Многие международные научные конференции по защите информации тонут в рассмотрении широчайшего многообразия ее различных аспектов - компьютерных, технических, технологических, аппаратных, организационных, лингвистических, правовых, социальнопсихологических и т. д. При этом научные, алгоритмические аспекты становятся какбы вторичными, уходят на дальний план. Как известно, остановка прогресса в любой области жизни общества чревата серьезными негативными последствиями для всего человечества.

Основная часть

Несмотря на отмеченные выше тенденции, защита информации как современный раздел науки переживает период бурного развития и перестройки. Хотя некоторые науковеды относят ее к своего рода современной религии (надежность многих крипто- систем, фактически, приходится принимать на веру), на самом деле защита информации - это очень наукоемкая сфера, захватывающая в свой оборот все новые и новые разделы математики, напоминая известный тезис: "Наука становится подлинной только тогда, когда начинает опираться на математический аппарат". Основным направлениям защиты информации - защите от помех и защите от несанкционированного доступа - приходится иметь дело с похожими друг на друга объектами, хотя и рассматривающими их с разных, почти противоположных сторон. Так, проблемы защиты информации от помех решает помехоустойчивое кодирование. Основная проблема, которую оно решает - быстро, со скоростью передачи информации, синхронно отбирать и однозначно определять возникающие в передаваемых блоках информации разного рода ошибки из-за неизбежных шумов и помех в каналах передачи этой информации. Приходится скрупулезно и тщательно искать в огромной совокупности возможных ошибок ту единственную, которая и произошла в данной конкретной ситуации. Попытки преодоления проблемы перебора здесь довольно часто приводят, к примеру, к решению алгебраических уравнений или их систем над полями Галуа [1, 2]. Как выяснилось, теория здесь слабо разработана, а предлагаемые рекомендации плохо поддаются алгоритмизации [2 - 4].

В защите информации от несанкционированного доступа почти противоположная ситуация. Практически бесконечное количество слов претендует быть передаваемым и зашифрованным сообщением. А надо из этого комплекса выбрать единственное, истинное. Как правило, названная проблема решается сложными алгоритмизированными вычислениями, требующими серьезной компьютерной поддержки [5], зачастую придающими ложную психологическую уверенность в наличии какой-то хитрой и простой отмычки. В обоих случаях проблему перебора можно существенно упростить посредством применения алгебраических средств - теории групп автоморфизмов сложных систем или применением тех или иных групп преобразований - под-

становок. Действие групп на исследуемых объектах позволяет структурировать их содержимое, предварительно разбив исследуемое множество на куски - групповые орбиты. Тем самым перебирается не все рассматриваемое многообразие, а в несколько итераций перебор быстро сужается практически до искомого элемента. Подобный метод применения автоморфизмов кодов успешно реализован на рубеже XX и XXI веков белорусской школой помехоустойчивого кодирования для решения проблем борьбы с помехами широким классом линейных кодов в созданной ими "теории норм синдромов"[2, 6]. Теория групп подстановок успешно применяется и в криптографии - при создании высокоскоростных шифров и методов работы с ними [7]. Обширный список из 27 открытых проблем Кэмерона о свойствах и приложениях групп подстановок [8] свидетельствует о нераскрытых еще возможностях этих групп, в частности, в решении проблем защиты информации. Существенное продвижение в решении только одной третьей проблемы Кэмерона [9] явилось одновременно и продвижением в классификации реперных множеств, важной для обеих ветвей защиты информации.

1. Мак-Вильямс Ф.Дж. Теория кодов, исправ- ляющих ошибки / Ф.Дж. Мак-Вильямс, Сло- эн Н.Дж.А. // М.: Связь, 1979. - 744.
2. Липницкий В.А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения / В.А. Липницкий, В.К. Коно- пелько // Мн.: БГУ, 2007. - 214.
3. Муттер В.М. Основы помехоустойчивой те- лепередачи информации / В.М. Муттер // Л.: Энергоатом издат, 1990. - 286.
4. Липницкий В.А. Современная прикладная алгебра. Математические основы защиты ин- формации от помех и несанкционированного доступа / В.А.Липницкий // Мн.: БГУИР, 2005. - 88; 2-е издание: Мн.: БГУИР, 2006. - 88.
5. Смарт Н. Криптография / Н. Смарт // М.: Техносфера, 2005. - 528.
6. Липницкий В.А. Теория норм синдромов / В.А.Липницкий // Мн.: БГУИР, 2010. - 108.
7. Молдовян А.А. Криптография: Скоростные ключи / А.А. Молдовян и др. // СПб, "БХВ- Петербург, 2002. - 496.
8. Cameron P., Problems on permutation groups // доступно по адресу http://www.maths.qmul.ac.uk/pjc/pgprob.html
9. Цветков В.Ю. Предсказание, распознавание и формирование образов многоракурсных изображений с подвижных объектов / В.Ю. Цветков, В.К. Конопелько, В.А. Липницкий // Мн.: Издательский центр БГУ, 2014. - 220.