В. Е. Писпанен, А. С. Поздняков, А. Ф. Васильев
(ГГУ им. Ф. Скорины, Гомель)

ТЕОРИЯ ГРУПП В КРИПТОГРАФИИ

Криптография – наука о методах обеспечения конфиденциальности, целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства [1].

Криптография требует, чтобы были заданы множества целых чисел и операции, определенные для них. Комбинация множеств и операций, которые могут быть применены к элементам множества, называются алгебраической структурой.

Клод Шеннон предложил рассматривать блочные шифры как наиболее перспективное средство обеспечения конфиденциальности сообщений в системах секретной связи. Он построил свою первую модель секретной системы с помощью алгебры шифров, введя понятия их суммы и произведения [2].

Современные симметрично-ключевые блочные шифры выполняют операции с n-битовыми словами. Понимание этих шифров требуют знания разделов современной алгебры, называемых алгебраическими структурами. Одной из таких структур являются группы.

Группа (G) – набор элементов с бинарной операцией «*» обладает следующими свойствами: замкнутость, ассоциативность, коммутативность, существование нейтрального элемента и существование инверсии.

Хотя группа включает единственный оператор, свойства, присущие каждой операции, позволяют использование пары операций, если они – инверсии друг друга. Если оператор – сложение, то группа поддерживает и сложение, и вычитание как аддитивно инверсные операции. Это

также верно для умножения и деления. Однако группа может поддержать только сложение/вычитание или умножение/деление, но не оба сочетания одновременно.

Литература

1 Ляховский, В. Д. Группы симметрии и элементарные частицы / В. Д. Ляховский, А. А. Болохов. – Изд-во ЛГУ, 1983. – 336 с.

2 Аграновский, А. В. Практическая криптография / А. В. Аграновский, Р. А. Хади. – М. : Солон-Пресс, 2009. – 258 с.