Литература

1. Кругликов, С.В. Методика решения задачи многофакторного целераспределения в автоматизированной системе управления / С.В. Кругликов // Доклады БГУИР. – 2013. – № 5. – С 93–99.

2. Липлянин, А.Ю. Методика учета важности цели при решении задачи распределения летательных аппаратов между огневыми средствами / А.Ю. Липлянин, А.С. Шеин, А.В. Хижняк // Доклады БГУИР. – 2017. – № 2. – С 77–84.

3. Городецкий, В.И.Методы и алгоритмы коллективного распознавания: обзор / В.И. Городецкий, С.В. Серебряков // Труды СПИИРАН. – 2006. – Вып. 3, т. 1. – С. 139 – 171.

АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ В АЛГОРИТМАХ ЗАЩИТЫ ИНФОРМАЦИИ

В.А. Липницкий, Л.В. Михайловская

Различные аспекты, связанные с решением алгебраических уравнений, часто и довольно неожиданно возникают при практической реализации тех или иных криптографических систем. Так, криптосистема Рабина своим базовым алгоритмом дешифрования ставит проблему решения квадратного уравнения в кольце классов вычетов по составному модулю – произведению двух простых нечетных чисел. Как ни странно, такие квадратные уравнения в общем случае имеют четыре, а не два корня.

Решение уравнения легальными пользователями сводит задачу по китайской теореме об остатках в минимальных полях Z/pZ и Z/qZ. Если p и q относятся к классу простых чисел Блюма, т.е. имеют вид $4t+3$, t – натуральное число, то задача легко решается возведением дискриминанта в строго определенную степень. Если же $p = 4t+1$, то при нечетных t существуют аналогичные формулы, а при четных t поиск квадратных корней осуществляется процедурой перебора, хотя и достаточно ограниченного перебора. Поэтому реальные пользователи криптосистемы Рабина стараются брать простые числа вида, рассмотренного в первом случае. Хакер вынужден вначале факторизовать модуль n в произведение простых множителей, т.е. решить ту же проблему, что и в криптосистеме *RSA*. Глубокое владение теорией чисел позволяет строить совершенные криптографические системы, удобные и практичные в применении.

ГРУППА АВТОМОРФИЗМОВ БЧХ-КОДА И ЕЕ ПОЛИНОМИАЛЬНЫЕ ИНВАРИАНТЫ

В.А. Липницкий, Е.В. Середа

По сути дела, группа автоморфизмов G любого БЧХ-кода порождена циклической и циклотомической подстановками, а потому является некоммутативной. Нормы синдромов – основной объект, разработанный белорусскими кодировщиками ТНС – теории норм синдромов – явились эффективными инвариантами группы Γ циклических сдвигов: норма синдрома так специфично определена через компоненты синдрома, что является одинаковой для всех векторов каждой Γ-орбиты ошибок, поэтому данный уникальный параметр и назван нормой Γ-орбиты. Выяснялось, что нормы Γ-орбит любой корректируемой совокупности векторов-ошибок попарно различны. Практическим следствием данной теории явилось семейство перестановочных норменных методов и алгоритмов коррекции ошибок БЧХ-кодами, на порядок ускоряющих работу декодеров по сравнению с традиционными синдромными алгоритмами.

В докладе рассматриваются полиномиальные инварианты всей группы G автоморфизмов БЧХ-кодов. Каждая G-орбита представляет собой объединение строго определенного ряда Γ-орбит, связанных друг с другом посредством циклотомической подстановки и ее степеней. Нормы циклотомически связанных Γ-орбит являются сопряженными элементами в конечном поле – поле определения соответствующего БЧХ-кода. Семейство взаимно сопряженных элементов поля Галуа составляет полную группу корней неприводимого полинома любого из элементов этого семейства. Согласно формулам Виета, всякий полином однозначно определяется своими корнями. Таким образом, полное семейство попарно сопряженных норм Γ-орбит, составляющих данную G-орбиту, задают однозначно определенный полином, корнями которого они являются. Это и есть полиномиальный