КАК ШИФРУЮТ МАТЕМАТИКИ?

Галеев Д.Р.

Руководитель: Вострикова О.Ю.

МБОУ Гимназия №56, 11 «б» класс, Россия, 426034, г.Ижевск, ул.Удмуртская, 230,
тел./факс (3412) 50-10-19, E-mail: danil_galeev@mail.ru

С давних времен встречалось множество проявлений шифров и криптографии в нашей жизни. Говоря о настоящем времени, область применения шифров достигла огромнейших размеров, что отчасти вызвано переходом к новому типу общества – информационному, где информация – главная ценность. А где ценность, там и стремление защитить ее от чужих рук. Вот тут-то нам и приходят на помощь шифры. Отсюда видно, что мой проект, посвященный исследованию криптографии и математики как интегрированных наук, актуален для нашего времени. Предметом исследования являются шифры и способы их создания. Рабочим материалом проекта послужили различные шифры, в том числе шифры, специально разработанные мной для этого проекта, а так же результаты проведенного эксперимента. Новизна проекта проявляется в интеграции криптографии и математики для получения новых способов шифрования и, соответственно, новых шифров. Отсюда следует, что цель данной работы – это изучение криптографии, способов создания шифров и нахождение связей между математикой и криптографией. Но основной целью я поставил исследование шифров и нахождение математических приемов в их создании, а также создание шифров, и сравнение их устойчивости. Достижение поставленных целей предполагает решение таких задач, как изучение теоретических материалов по теме и анализ их на предмет математических приемов, а также разработка алгоритмов шифрования. Методы и приемы исследования – изучение и анализ материалов строится на описательном и сопоставительном методах. Эксперимент проводится в рамках опроса. Проект реализуется в предметных рамках математики и может быть квалифицирован как исследовательский, результаты которого могут использоваться на уроках математики и информатики как учебные пособия.

Литература

1. Реальные применения мнимых чисел. М.Б. Балк, Г.Д. Балк, А.А. Полухин 1988 год
2. Краткий исторический очерк истории криптографии. В.А.Носов 2002
3. Алгебраические основы криптографии. Ростовцев А.Г. 2000