ПОДГОТОВКА УЧАЩИХСЯ СРЕДНЕЙ ШКОЛЫ К РЕШЕНИЮ КРИПТОГРАФИЧЕСКИХ ЗАДАЧ

Отрыванкина Т.М.
Оренбургский государственный университет, г. Оренбург

В последние десятилетия во всем мире, в том числе и в России, криптография получила интенсивное развитие не только как прикладная, но и как фундаментальная наука, лежащая в основе научно-технических методов обеспечения безопасности государственных, экономических и военных информационных ресурсов. Всестороннее развитие криптографии на основе тесного взаимодействия со смежными областями науки и техники требует постоянного притока талантливой молодежи, проявляющей интерес к точным наукам и имеющей хорошие знания в математике, физике, информатике. [1]

Стало традицией ежегодное проведение в России Межрегиональной олимпиады школьников по математике и криптографии. Ее организаторами являются Академия ФСБ России, Академия криптографии Российской Федерации, Учебно-методическое объединение высших учебных заведений России по образованию в области информационной безопасности (УМО ИБ) при участии входящих в состав УМО ИБ вузов. Координацию организационного обеспечения проведения Олимпиады осуществляет Институт криптографии, связи и информатики Академии ФСБ России. Председатель оргкомитета Олимпиады – вице-президент Академии криптографии Российской Федерации В.Н. Сачков. Председатель методической комиссии олимпиады – вице-президент РАН В.В. Козлов. Олимпиада проводится для школьников 8-11 классов учреждений общего среднего образования и соответствующих категорий обучающихся начального и среднего профессионального образования на основе общеобразовательных программ соответствующих ступеней обучения. Олимпиада проходит в два тура – отборочный (в дистанционной форме) и заключительный (в очной форме). [2] В настоящее время подводятся итоги очного финального тура 24-ой олимпиады.

Впервые Оренбургский государственный университет выступал региональной площадкой этого математического соревнования школьников. Это очень важно, так как Межрегиональная олимпиада школьников по математике и криптографии входит в Перечень олимпиад школьников, и успешное участие в ней дает льготы победителям и призерам при поступлении в государственные и муниципальные учреждения высшего профессионального образования. [2]

В некоторых регионах России проведение олимпиад в области информационной безопасности имеет относительно давнюю историю. Следует, отметить, что лидерами по подготовке школьников к олимпиадам по математике и криптографии выступают не только школы Москвы и Санкт-Петербурга. Так, на Дальнем Востоке еще в 2002 году был создан Дальневосточный региональный учебно-научный центр по проблемам информационной безопасности (ДВРУНЦ), который проводит региональные

конференции, семинары и совещания, олимпиады и конкурсы по тематике информационной безопасности. [3] С 2009 года ДВРУНЦ выступает организатором в Приморье Межрегиональной олимпиады школьников по математике и криптографии. За прошедшее время ведущие школы Владивостока достигли больших успехов в подготовке призеров Олимпиады.

В рамках XV Всероссийского Симпозиума по прикладной и промышленной математике в октябре 2014 года прошёл ежегодный круглый стол «Интеллектуальные соревнования для студентов и школьников в области информационной безопасности». По итогам активной дискуссии её участники пришли к общему выводу о системном влиянии интеллектуальных соревнований школьников и студентов на формирование регионального кадрового потенциала в сфере информационной безопасности.[3]

В Оренбурге систематическая работа по подготовке школьников к подобным соревнованиям пока не ведется. Сама Олимпиада не на слуху у педагогов школ и преподавателей вузов. Только некоторые школьники знают о ней из интернет-источников. Появление ОГУ среди ВУЗов-участников позволяет активно приглашать школьников для участия в отборочном туре и требует организации подготовительной работы. С одной стороны, в олимпиаде большая доля просто математических знаний, логики, интуиции, есть возможность анализа задач прошлых лет, доступных в архиве на сайте, с другой стороны – постановка задач специфическая, поэтому их нужно обсуждать с учащимися.

В этом учебном году в МОБУ «Лицей №8» начал работу кружок по криптографии для учеников 7-9 классов. На нем обсуждаются исторические шифры, решаются задачи шифрования-дешифрования и простейшего криптоанализа. Предметом обсуждения стали и некоторые задачи прошедшего в ноябре 2014 года отборочного тура XXIV Межрегиональной олимпиады школьников по математике и криптографии.

Приведем примеры заданий первого занятия, посвященного основным понятиям криптографии, ее задачам и шифру Цезаря – простейшему, но важному шифру наивного периода.

1) Напишите свое имя и зашифруйте со сдвигом на 3 элемента алфавита.

2) Напишите слово cryprography и зашифруйте его со сдвигом 5.

3) Получено сообщение ЩЧХЛ УХЙЪЩ ШХЬЧЖФПЩГ ШЛСЧЛЩ, ЛШТП КИХЛ ПО ФПЬ УЛЧЩИВ. Найдите величину сдвига, который использовался при шифровании, и восстановите исходный текст.

4) Ученики получили криптограмму:

«Шсёйзбдяб зёымяцвтдезия «Бегётфиыждцх чыюеёцздезит» хшвхыизх зёымяцвязиег ёе юцпяиы ядкежгцмяя ъезициенде ояжебеще ёжекявх (дызгеижх дц ие, ние ш ъяёвегы шсёйзбдябц чйъыи юцёязцдц бшцвякябцмях «Гциыгцияб»). Ед юцдягцыи дц ёжыъёжяхияя ёжегыэйиендеы ёевеэыдяы гыэъй жйбешеъзишег ёжыъёжяхиях, з еъдеа зиежедс, еиъывцгя цшиегцияюцмяя (ядкежгцмяеддсл иылдевещяа, ядкежгцияюцмяя) ёжыъёжяхияа, з ъжйщеа зиежедс, ц ицбэы звйэчеа чыюеёцздезия ёжыъёжяхиях, з ижыитыа зиежедс.»

Каким было исходное послание?

5) Расшифруйте: fipygyuhmhypylbupchanimussio'lymillscmuwunw bjblumyvumyxihufchyzlignbyhipyfuhx1970zcfgfipymnilsmnullchaufcguwaluquhxl.

Задача упомянутого отборочного тура имела следующее содержание: «Исходный текст разбивается на блоки длины 16, и к каждому блоку применяется перестановка вида

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
7	11	15	9	14	3	5	1	13	12	8	6	10	2	16	4

После ее применения 2015 раз получилась криптограмма:

КЛБЗЬМЯЗСАААОАЕОЛМУШЫЕШИЛАМТЕДЬЬЕ.

Найдите первое слово исходного текста.»

Задача хорошо дополнила материал кружка, посвященный перестановкам как способу шифрования, и позволила в очередной раз напомнить об олимпиаде по криптографии.

Поскольку решение даже самых простых криптографических задач требует справочного и вспомогательного инструментария, то его нужно разрабатывать. Такая работа может стать предметом учебно-исследовательского проекта, в котором самостоятельность школьника проявится в выявлении информации, необходимой для криптоанализа того или иного шифра, и составлении и оформлении ее в виде таблиц.

Учебное исследование по теме «Математические методы анализа исторических шифров» было выполнено одной из учениц лицея и представлено на конференциях школьников, прошедших в декабре 2014 года в Оренбурге. Материал, подготовленный в работе, был апробирован на занятиях кружка и помог его участникам справиться с предложенными заданиями.

Отметим, что организация олимпиад по криптографии становится важным направлением работы в разных вузах. Например, Саратовский университет организовал собственную заочную олимпиаду по криптографии, которую уже в 13-ый раз проводит кафедра теоретических основ компьютерной безопасности и криптографии СГУ. Задачи тематически связаны как непосредственно с шифрами, так и с широко применяемыми в современной криптографии разделами алгебры, теории чисел, дискретной математики и лингвистики. [4]

Список литературы

1. *Сачков, В. Спрос на таланты в математике и криптографии будет только расти [Электронный ресурс]// «BIS Journal» № 3(14)/2014. –Режим доступа: http://journal.ib-bank.ru/pub/314 . –22.10.2014.*
2. *Межрегиональная олимпиада школьников по математике и криптографии [Электронный ресурс]. – Режим доступа: http://www.cryptolymp.ru*
3. *Коротышев, П. Путь в повелители чисел [Электронный ресурс]// «BIS Journal» № 4(15)/2014. – Режим доступа: http://www.journal.ib-bank.ru/pub/330. – 22.12.2014.*
4. *Олимпиады по криптографии. Тринадцатая заочная олимпиада по криптографии [Электронный ресурс]. – Режим доступа*

http://www.sgu.ru/structure/computersciences/theorcompsafe/olimpiady-po-kriptografii. – 23.12.2014.