Саратовские олимпиады по криптографии SarCrypt

Абросимов М.Б.[1], Салий В. Н.[2], Жаркова А. В.[3], Лобов А. А.[4], Моденова О. В.[5], Конюшенко А. С.[6], Романов Р. А.[7]

[1]mic@rambler.ru, [2]saliivn@sgu.ru, [3]zharkovaav3@gmail.com, [4]aisanekai@mail.ru, [5]oginiel@rambler.ru, [6]aleksandrakonyshenko12@gmail.com, [7]illidann2002@mail.ru

Саратовский государственный университет имени Н.Г. Чернышевского

Аннотация. В статье рассказывается о Саратовских олимпиадах по криптографии, история которых началась с 2002 год. Олимпиады проводятся кафедрой теоретических основ компьютерной безопасности и криптографии ФГБОУ ВО Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского. Рассматриваются итоги последней олимпиады – XXI открытой олимпиады школьников и студентов по криптографии, проведённой в 2022-2023 учебном году. Даётся обзор задач, обсуждается тематика и темы, которые вызывают наибольшие затруднения. Рассматриваются аспекты подготовки и проведения соревновательных мероприятий в очно-дистанционном режиме.

Ключевые слова: олимпиада школьников, олимпиада студентов, криптография, очные соревнования, дистанционные соревнования

29 января 2023 года состоялся финальный тур XXI открытой олимпиады школьников и студентов по криптографии SarCrypt. Всего в олимпиаде приняли участие более 300 школьников и студентов из России, Республики Казахстан, Туркменистана, Республики Молдова и Республики Беларусь: 84 участника в возрастной категории 6-8 классы, 162 участника 9-11 классов, 58 студентов. Победители первого (отборочного) тура были приглашены на финальный тур, в котором приняли участие 106 школьников и студентов из России, Республики Молдова, Республики Казахстан и Туркменистана: 34 участника в категории 6-8 классы, 57 участников в категории 9-11 классы, 15 студентов.

История саратовских олимпиад по криптографии начинается с 2002 года, когда в Саратовском государственном университете имени Н.Г. Чернышевского была создана кафедра теоретических основ компьютерной безопасности и криптографии, а также открыта специальность «Компьютерная безопасность». Первая олимпиада по криптографии была проведена осенью 2002 года. Олимпиада состояла из 4 туров и проводилась для старшеклассников в заочном формате. Задания каждого тура выкладывались на сайте [1] и рассылались по школам города Саратова. Каждый тур состоял из 5 задач, на решение которых отводилось 2 недели. Все задачи олимпиады составлялись сотрудниками кафедры теоретических основ компьютерной безопасности и криптографии, а также сотрудниками лаборатории компьютерной безопасности.

Задачи, которые предлагались участникам олимпиады, имели разную направленность. Хотя криптография является одной из старейших наук, она не входит непосредственно в школьный курс. Поэтому задачи имеют разную направленность, и для успешного участия могут потребоваться знания из различных областей: информатика, математика, лингвистика. Поскольку

одной из основных задач проведения олимпиады была задача популяризации соответствующего направления, то изначально предполагалось, что участники для решения задач могут использовать любые доступные средства. Конечно, среди задач предлагаются задачи, посвященные криптографии, в которых требуется зашифровать, расшифровать или дешифровать какие-то сообщения по некоторым известным данным. Некоторые задачи имеют математическое направление, но большинство задач связанны с информатикой или программированием. Чтобы успешно справиться с заданиями олимпиады, нужно продемонстрировать не только знания по математике и информатике, навыки программирования, но и умение искать и привлекать дополнительную информацию, существенно выходящую за рамки школьной программы. Для решения задач, связанных с криптографией, желательно знакомство с классическими шифрами, которое можно получить из книг, вполне доступных школьникам [2]. Ознакомиться с заданиями олимпиад за все годы можно на сайте [1].

Многие задачи олимпиады допускают решения различными методами, как аналитическими, так и, например, с помощью программирования или поиска информации в сети Интернет. Иногда проще составить программу, иногда найти математическое решение, а иногда воспользоваться поисковыми системами. Впрочем, решения напрямую с помощью поисковых систем, скорее всего, найти не удастся.

В качестве примера приведём одну из задач отборочного тура XXI олимпиады SarCrypt 2022-2023 учебного года.

Задача. В городе Базеле рядом с домом Леонарда Эйлера была найдена загадочная записка:

Попробуйте восстановить пропуски.

В условии задачи даются подсказки, что нужно найти некоторую числовую последовательность, связанную с Леонардом Эйлером, и имеющую отношение к криптографии. Так как разрешается пользоваться поисковыми системами, а времени на решение даётся неделя, то можно было бы ожидать, что участники смогут угадать функцию Эйлера и найти пропуски. Следует отметить, что задачи, составленные в нетрадиционной форме, традиционно вызывают у участников сложности.

Так как шифрование и расшифрование можно рассматривать как частные случаи кодирования и декодирования, то почти каждый год предлагаются

задачи, в которых требуется продемонстрировать знание различных кодировок и умение с ними работать. В качестве примера приведём ещё одну из задач отборочного тура.

Задача. Перед вами записка, оставленная обмотанной бинтами женщиной с рыжими волосами. Текст в записке – это набор больших букв русского алфавита в кодировке UTF-8. На записке указаны байты:

1D 02 1C F6 19 EE 11 F0 23 EC 1F F1 14 ED 25 E4

24 F8 20 E3 23 F0 27 DF 22 F3 1D F6 1C EF 19 F3

11 FA 23 E7 1F EB 14 EA 25 EA 24 EA 20 E3 23 FF

Известно, что использовался шифр Вижинера на байтах, а в качестве ключа использовалось слово из 13 букв, представленное в кодировке ASCII. В ответе укажите, какой ключ использовался при шифровании.

В условии задачи даётся подсказка, что используется кодировка UTF-8. Несложно определить с помощью любого редактора, который позволяет показывать коды, что первый байт для русских букв всегда равен 208. Дальше можно определить ключ, даже без выполнения дешифрования.

С 2018 года олимпиада стала проводиться в два тура. Первый тур (отборочный) стал проводиться дистанционно в первую полную неделю декабря. Продолжительность отборочного тура составляет одну неделю. Задания публикуются на сайте кафедры, а для регистрации участников и ввода ответов используются возможности платформы Эрудит.Онлайн Научно-образовательного центра «Эрудит» [2]. По результатам отборочного тура все победители приглашаются на очный тур.

Второй тур (очный) проводится в последнее воскресенье января на базе факультета компьютерных наук и информационных технологий Саратовского государственного университета. Количество задач первого и второго тура одинаково, однако, если на решение задач дистанционного тура даётся одна неделя, то на решение задач очного тура отводится только 3 часа. Некоторые задачи очного тура составляются с отсылкой к задачам дистанционного тура. С одной стороны, участники подходят к этим задачам более подготовленными, с другой стороны, это позволяет оценивать самостоятельность решения задач участниками в отборочном туре.

С 2019 года олимпиада стала проводиться для участников в трёх возрастных категориях: 6-8 классы, 9-11 классы и студенты. Первой категории предлагается 6 задач, второй – 8 задач, студентам – 10 задач.

Изначально задания проверялись членами жюри в ручном режиме. С 2018 года задания стали проверяться в полуавтоматическом режиме. Сначала задания проверяются автоматически с помощью программного обеспечения платформы Эрудит.Онлайн [2]. Далее задания проверяются членами жюри в ручном режиме. В силу особенности олимпиады большинство задач составляется так, чтобы ответом было некоторое сообщение. Задачи могут иметь несколько решений, в том числе и не предусмотренных заранее

авторами заданий. Хотя процент таких решений чрезвычайно низок, для их выявления и используется ручная проверка. Таким образом, верные решения, которые не были предусмотрены авторами задач и членами жюри, при автоматической проверке оцениваются как ошибочные, однако на втором этапе, при ручной проверке, ответ оценивается как верный и участники получают полные баллы. Одна из таких задач описывалась в работе [4].

В новом формате по-прежнему предлагаются задания не только по криптографии, и для успешного решения могут потребоваться знания по информатике, программированию и математике. Многие задачи допускают различные решения: можно составить программу, а можно найти математическое решение.

Особенностью олимпиады по криптографии является то, что разрешается использовать все доступные средства: любые системы программирования, собственные или сторонние программы, справочные материалы, сеть Интернет. Обязательным условием является лишь индивидуальное участие. На дистанционном туре проверить это практически невозможно, однако на очном туре запрещается использовать мессенджеры и иные средства общения.

До 2020 года очный тур проводился на факультете компьютерных наук и информационных технологий Саратовского государственного университета имени Н.Г. Чернышевского. В 2020-2021 учебном году из-за эпидемиологических ограничений провести тур очный тур в таком виде оказалось невозможно. Было принято решение впервые очный тур провести в режиме онлайн на базе платформы ZOOM. Соблюдение регламента олимпиады контролировали сотрудники лаборатории компьютерной безопасности, что позволило считать, что все участники находятся в равных условиях и решают задания олимпиады самостоятельно. Положительным моментом такого способа проведения олимпиады стала возможность существенного увеличения географии участников очного тура: впервые в очном туре Саратовских олимпиад по криптографии приняли участие школьники из других городов России и даже из других стран – школьники из Республики Молдовы.

В 2022-2023 состоялась XXI олимпиады школьников и студентов по криптографии SarCrypt. В ней приняли участие 304 школьника и студента из России, Республики Казахстан, Туркменистана, Республики Молдова и Республики Беларусь: 84 участника 6-8 классов, 162 участника 9-11 классов, 58 студентов. География участников получилась достаточно широкой: Абакан, Балаково, Липецк, Магнитогорск, Нижний Новгород, Новосибирск, Орлов-Гай, Петропавловск (Казахстан), Пугачев, Рыбница (ПМР), Саратов, Сосногорск, Энгельс, этрапы Ак бугдай, Бабадайхан, Каака (Туркменистан) и некоторые другие населённые пункты. Отборочный тур проходил с 5 по 11 декабря 2022 года. По его результатам 106 школьников и студентов из России, Республики Молдова, Республики Казахстан и Туркменистана получили приглашение на финальный тур: 34 участника в категории 6-8 классы, 57 участников в категории 9-11 классы, 15 студентов.

Финальный тур XXI олимпиады школьников и студентов по криптографии SarCrypt проводился 29 января 2023 года в смешанном формате: участники могли решать задачи либо на факультете компьютерных наук и информационных технологий, либо дистанционно через систему Контур.Толк. Среди победителей оказались участники из России и Республики Молдова.

Следующая XXII олимпиада будет проводиться в 2023-2024 учебном году. Отборочный тур запланирован на 4-10 декабря 2023 года, а финальный тур состоится ориентировочно 28 января 2024 года.

Список литературы

[1] Олимпиады по криптографии. URL: https://www.sgu.ru/structure/computersciences/theorcompsafe/olimpiady-po-kriptografii

[2] Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. ─ М.: «Гелиос АРВ», 2002.

[3] Портал дистанционных конкурсов и олимпиад Эрудит.Онлайн. URL: https://erudit-online.ru

[4] Абросимов М.Б., Салий В.Н, Жаркова А.В., Коннова А.Д., Лобов А.А., Моденова О.В., Шабаркова А.О. Саратовская олимпиада по криптографии 2020-2021 учебного года // Информационные технологии в образовании : сборник / редакционная коллегия: С. Г. Григорьев [и др.]. ─ Саратов : Саратовский университет, 2021. ─ Вып. 4 : материалы XIII Всероссийской научно-практической конференции «Информационные технологии в образовании» (ИТО-Саратов-2021), 5-6 ноября 2021 г., г.Саратов. – С. 10–12.