УДК 519.7 DOI 10.17223/2226308X/8/27

NSUCRYPTO — СТУДЕНЧЕСКАЯ ОЛИМПИАДА ПО КРИПТОГРАФИИ: ИДЕЯ, ВОПЛОЩЕНИЕ, РЕЗУЛЬТАТ[1]

Н. Н. Токарева

Кратко представлен опыт проведения первой международной студенческой олимпиады по криптографии NSUCRYPTO. Рассмотрены принципы её организации и математические задачи, предложенные участникам.

Ключевые слова: *NSUCRYPTO, олимпиада, криптография, булевы функции.*

Идея провести студенческую олимпиаду по криптографии появилась несколько лет назад в Новосибирске. К тому времени существовало несколько школьных олимпиад по криптографии и информационной безопасности, вызывающих большой интерес. В первую очередь среди них стоит отметить олимпиаду по математике и криптографии, успешно проводимую ИКСИ уже более 20 лет подряд. Но студенческой олимпиады по криптографии не было, в том числе и за рубежом. Новая олимпиада сразу задумывалась как международная, поэтому её официальным языком стал английский. Чтобы максимально расширить географию участников, было принято решение проводить её дистанционно, через интернет. Ещё одной ключевой идеей стала идея о том, что в целом задачи олимпиады должны быть сложными (не игровыми), а часть из них и вовсе нерешёнными. Вместе с коллегами мы не ставили перед собой задачу популяризации криптографии как таковой; нам хотелось привлечь внимание студентов и молодых исследователей к современным математическим вопросам криптографии, возбудить научный интерес к криптографии.

В 2014 г., заручившись активной поддержкой руководства мехмата НГУ и Института математики СО РАН, обсудив формат олимпиады с нашими коллегами-криптографами из Томского и Белорусского университетов, лаборатории COSIC университета г. Лёвена (Бельгия), мы занялись её организацией. В программный комитет олимпиады NSUCRYPTO-2014 вошли: Г. П. Агибалов (профессор, заведующий кафедрой защиты информации и криптографии ТГУ); С. В. Агиевич (заведующий НИЛ проблем безопасности информационных технологий НИИ прикладных проблем математики и информатики, БГУ); Н. А. Коломеец (н.с. ИМ СО РАН, преподаватель НГУ); И. А. Панкратова (доцент кафедры защиты информации и криптографии ТГУ); Н. Н. Токарева (с.н.с. ИМ СО РАН, доцент НГУ); S. Nikova (сотрудник лаборатории COSIC университета г. Лёвена); B. Preneel (профессор лаборатории COSIC университета г. Лёвена, президент Международной ассоциации криптографических исследований (IACR)), V. Rijmen (сотрудник лаборатории COSIC университета г. Лёвена, один из двух создателей шифра AES). Организационный комитет олимпиады представили преподаватели и студенты НГУ: В. А. Виткуп, А. А. Городилова, Г. И. Шушуев, Д. П. Покрасенко и С. Ю. Филюзин.

Олимпиада NSUCRYPTO-2014 состояла из двух независимых интернет-туров: индивидуального (школьная и студенческая секции) и командного. Для участия достаточно было зарегистрироваться на сайте `www.nsucrypto.nsu.ru`, при этом стать участником мог каждый. Было зарегистрировано более 450 участников из 12 стран — России, Австрии, Бельгии, Белоруссии, Болгарии, Германии, Дании, Индии, Италии, Ка-

[1]Работа поддержана Новосибирским государственным университетом, грантами РФФИ № 15-07-01328 и НШ-1939.2014.1 Президента России для ведущих научных школ.

захстана, Сингапура, Украины. Более 280 участников — студенты, около 120 — школьники, остальные участники — любители криптографии и профессионалы.

Участникам олимпиады было предложено 15 задач. Математические задачи олимпиады посвящены вопросам исследования дифференциальных характеристик S-блоков; взаимосвязи простейших операций, использующихся для построения шифра: циклического сдвига и сложения по модулю 2^k; построению специальных линейных подпространств в $\mathbb{F}_2^n$; поиску числа решений уравнения $F(x)+F(x+a)=b$ над конечным полем $\mathbb{F}_{2^n}$ и APN-функциям. Были и игровые задачи, такие, как крипто-квест, дешифрование секретных сообщений, анализ музыкального шифра. Детально задачи и их решения обсуждаются в [1, 2]. При этом работа [2] содержит не только разбор всех задач, но и комментарии к решениям участников, организационные моменты олимпиады, списки призёров.

Победителями олимпиады стали участники из Новосибирска, Омска, Москвы, Санкт-Петербурга, Саратова, Минска (Беларусь) и Лёвена (Бельгия): 15 участников в первом туре и 11 команд-победительниц во втором туре. Награждение призёров состоялось в Новосибирском государственном университете в декабре.

NSUCRYPTO задумана как ежегодное мероприятие. В следующий раз она пройдёт в ноябре 2015 г. (см. `www.nsucrypto.nsu.ru`). Приглашаем всех желающих принять в ней участие! Например, участники конференции Sibecrypt могут выбрать категорию «любитель/профессионал».

ЛИТЕРАТУРА

1. *Agievich S., Gorodilova A., Kolomeec N., Nikova S., et al.* Mathematical problems of the First international student's Olympiad in cryptography NSUCRYPTO // IV Симпозиум «Современные тенденции в криптографии» CTCrypt'15, Казань, 3–5 июня 2015 г.
2. *Agievich S., Gorodilova A., Kolomeec N., Nikova S., et al.* Problems, solutions and experience of the first international student's Olympiad in cryptography // Прикладная дискретная математика. 2015. № 3(29).

УДК 519.95 DOI 10.17223/2226308X/8/28

АТАКА ПО ШИФРТЕКСТАМ НА ОДНУ ЛИНЕЙНУЮ ПОЛНОСТЬЮ ГОМОМОРФНУЮ КРИПТОСИСТЕМУ[1]

А. В. Трепачева

Описывается новая стратегия атаки по шифртекстам на одну линейную полностью гомоморфную криптосистему, чья защищённость обосновывается с привлечением сложности задачи факторизации больших чисел. Приводятся теоретические и практические оценки вероятности раскрытия секретного ключа с использованием данной атаки. Проводится анализ связи трудности факторизации чисел и защищённости криптосистемы против атаки по шифртекстам, на основе которого предлагается более эффективная модификация криптосистемы.

Ключевые слова: *полностью гомоморфное шифрование, задача факторизации чисел, атака по шифртекстам.*

Введение

В связи с распространением облачных сервисов задача построения полностью гомоморфных криптосистем (ПГК), позволяющих проводить произвольные вычисления

[1]Работа поддержана грантом РФФИ № 15-07-00597-а.