МЕТОДЫ РЕШЕНИЯ ПРОБЛЕМЫ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ В ЛАБОРАТОРНОМ КОМПЛЕКСЕ ВОЕННОГО ВУЗА

В.А. Липницкий, Е.В. Жалобкевич

Современные методы криптографической защиты информации основаны на методах современной математики в сочетании с мощными компьютерными средствами.

В основе используемых асимметричных алгоритмов шифрования лежат односторонние функции. В роли таких функций могут выступать умножение и факторизация целых чисел, возведение в квадрат и извлечение квадратного корня по заданному модулю, а также логарифмирование в кольцах классов вычетов по большому модулю.

Рассмотрим проблему дискретного логарифмирования в контексте криптосистемы Эль-Гамаля, модификации которой долгое время были в основе российского и белорусского стандартов шифрования [1].

Априорное решение уравнения $\bar{g}^x = \bar{h}$ в кольце Z / pZ с простым p осуществляется единственным способом – последовательным перебором степеней $\bar{g}$.

Для криптограмм с шестью и более десятичными знаками требуется применение иных, менее переборных методов. Так, использование алгоритма «Baby step giant step» сокращает время вычисления секретного ключа более чем в 7 раз [2]. Данный метод доступен студентам, хотя и требует от них определенных интеллектуальных усилий.

Метод Полига-Хеллмана вызывает интерес и практическое применение у специалистов, но требует у обучаемых дальнейшего погружения в глубины теории групп [3]. Уравнение $\bar{g}^x = \bar{h}$ распадается на n уравнений. Используя китайскую теорему об остатках, искомый секретный ключ восстанавливается по формулам Гарнера. Данный метод весьма эффективен в случаях, когда p является большим числом, а множители p –1 — малыми числами.

Использование алгоритма Полига-Хеллмана в реальных криптосистемах сокращает время решения задачи дискретного логарифмирования примерно в 6 раз по сравнению с алгоритмом «Baby step giant step». Это возможно благодаря тому, что в данном алгоритме используются, преимущественно, операции умножения, выполнение которых происходит значительно быстрее, и как следствие, возрастает скорость выполнения всей операции дискретного логарифмирования.

Литература

1. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. М., 2003.

2. *Липницкий В.А.* Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа: учеб. метод. пособие. Минск, 2006.

3. *Pohlig S.C., Hellman M.E.* An Improved Algorithm for Computing Logarithms Over GF(p) and its Cryptographic Significance // IEEE Transactions on Information Theory. 1978. Т. 1. № 24. С. 106–110.

ОЦЕНКА ПЕРСПЕКТИВ ПОДГОТОВКИ КАДРОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЗАОЧНОЙ ФОРМЕ ПОЛУЧЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ

А.В. Ломако

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» (БГУИР) обеспечивает получение высшего образования первой ступени в заочной форме по двум специальностям, имеющим непосредственное отношение к информационной безопасности: 1-38 02 03 «Техническое обеспечение безопасности» (ТОБ) и 1-39 03 01 «Электронные системы безопасности» (ЭСБ). В настоящее время по специальности ТОБ заочное обучение ведется на 5-м и 6-м курсах, а по специальности ЭСБ — с 1-го по 4-й курс. Всего за все годы обучения по специальности ТОБ в рамках заочной формы обучения подготовлено 210 дипломированных специалистов (первый выпуск состоялся в 2009 г.), выпуск 2016 г. составит 32 человека, а 2017 г. — 40 человек. С 2012 г. набор на специальность ТОБ прекращен и начат набор на специальность ЭСБ.

Практика набора абитуриентов на указанные специальности показала ежегодное наличие конкурса (от 1,5 до 2 человек на место), причем конкурс наблюдался при наборе и на обучение за счет средств бюджета, и на платное обучение. В период обучения примерно половина студентов (от 40 до 60%) работает по профилю избранной специальности. После окончания обучения практически все выпускники начинают работать по полученной специальности. Проблемы с трудоустройством, как правило, отсутствуют.