УДК 378.147:003.26

Использование элементов интерактивного обучения на занятиях по криптографии

Вильданов Алмаз Нафкатович
Нефтекамский филиал «Башкирский государственный университет»
к.ф.-м.н., доцент

Хузин Ильнар Фидарисович
Нефтекамский филиал «Башкирский государственный университет»
студент

Аннотация
Предлагаются сценарии проведения интерактивных занятий, посвященных математическим основам криптографии. Обучающимся предлагается «смоделировать» процесс создания электронной цифровой подписи и ее проверки, создать общий ключ по алгоритму Диффи-Хеллмана и обменяться сообщениями, используя алгоритм RSA. Предполагается, что такие занятия помогут студентам лучше освоить приемы шифровки-дешифровки и понять особенности применения цифровой подписи и решения проблемы распределения ключей.
Ключевые слова: интерактивные методы обучения, криптография, RSA, электронная цифровая подпись, протокол Диффи-Хеллмана

Using interactive learning elements in training on cryptography

Vildanov Almaz Nafkatovich
Neftekamsk branch of Bashkir State University
Candidate of physico-mathematical sciences, associate professor

Khuzin Ilnar Fidarisovich
Neftekamsk branch of Bashkir State University
student

Abstract
Described are offered interactive methods of the training devoted to the mathematical foundations of cryptography. Students are encouraged to "simulate" the process of creating an electronic digital signature and its verification, create a common Diffie-Hellman key and exchange messages using the RSA algorithm. It is supposed that such interactive games will help students to master the methods of encryption-decryption and understand the features of using digital signature and solving the problem of key distribution.
Keywords: interactive methods of the training, cryptography, RSA, digital signature, Diffie–Hellman key exchange

Предмет криптографии сам по себе достаточно сложен для освоения, и не исключением является та ее часть, которая связана с теорией чисел. Делимость чисел, решение сравнений и пр. могут показаться студенту скучными и неинтересными. Сегодня требовательный студент может прямо спросить: а какое отношение имеет данный материал к моей будущей профессиональной деятельности? Поэтому в преподавании математических основ криптографии важно, кроме используемого математического аппарата теории чисел, объяснить и показать обучающимся модели применения на практике изучаемого теоретического материала. Несомненно, это поможет повысить интерес студентов к материалу и поднимет качество его усвоения.

В настоящее время в учебных заведениях активно разрабатываются, применяются и совершенствуются новые методики обучения для повышения эффективности образовательного процесса. Одной из таких методик стало внедрение интерактивного обучения.

В отличие от традиционных методов, интерактивные ориентированы на более широкое взаимодействие студентов, как с преподавателем, так и друг с другом, на доминирование активности последних в процессе обучения [1].

Интерактивное обучение – это специальная форма организации познавательной деятельности, в которую вовлечены все участники учебного процесса, созданы комфортные условия для обучения [2]. Интерактивное обучение подразумевает продуктивный диалог, работу в малых группах, кейсовые задания, ролевые игры, и пр.

В данной работе предлагаются сценарии проведения интерактивных игр, которые нацелены помочь студентам глубже проникнуться исследуемой проблематикой. Предполагается, что студент уже освоил необходимый материал по теории чисел, умеет решать сравнения с помощью цепных дробей и знает алгоритм RSA.

Рассмотрим сценарий с имитированием электронной подписи. Поскольку алгоритм RSA работает с целыми числами, сначала нужно договориться о правилах перевода текста в число и наоборот. Например, можно каждой букве сопоставить ее номер в алфавите. Таким образом, букве «к» будет соответствовать число 12, букве «т» – 20 и т.д. Для первых девяти букв можно добавлять нолик в записи внутри слова. Например, слово «сон» преобразуется в следующее число – 191615, слово «бал» преобразуется в число 20113, и т.д. Следует помнить, что полученное число не должно превышать значения числа n в RSA, и поэтому желательно либо ограничиться словами из двух букв, либо зашифровывать каждую букву слова отдельно.

Студенты разбиваются на пары. Первый студент, «владелец» будущей электронной подписи, должен создать ее и подписать какое-нибудь свое сообщение, например, «уж». Ход работы этого студента будет состоять из следующих шагов [3]:

– выбор двух простых чисел, например, $p = 101$ и $q = 211$;

– нахождение числа $n = p \cdot q = 21311$;

– определение функции Эйлера $phi\_n = (p - 1) \cdot (q - 1) = 21000$;

– выбор простого числа e, например, $e = 31$, с учетом того, что числа e и phi_n должны быть взаимно простыми;

– нахождение числа d из уравнения

$$e \cdot d \equiv 1 \pmod{phi\_n},$$

отсюда $d = 12871$.

После проведения вычислений у первого студента на руках будет открытый ключ (e,n) и закрытый ключ (d,n). Теперь ему нужно зашифровать сообщение. В алгоритме RSA шифрование обычно происходит с помощью закрытого ключа d, расшифровка – с помощью открытого ключа e. В режиме цифровой подписи все наоборот. Этапы зашифровки:

– слово «уж» переводится в числовой формат по раннее предложенному алгоритму: «уж» → 2108;

– зашифровывается число 2108 согласно формуле

$$C = M^d \ (mod\ n),$$
$$C = 2108^{12871} \ (mod\ 21311) = 7350.$$

Сообщение C рассматривается как подпись первого студента, поэтому оно вычисляется с помощью закрытого ключа d, который должен быть известен только ему. Теперь первый студент записывает на бумажке значения e, n, слово «уж», и подпись (рисунок 1), и передает преподавателю. Преподаватель проверяет отсутствие избыточных данных, и передает записку второму студенту.

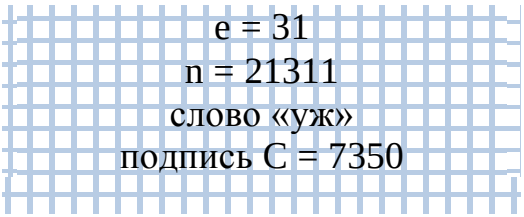

Рисунок 1

Второй студент выполняет проверку подписанного сообщения. Его ход шагов [3]:

– расшифровка сообщения C = 7350 с помощью открытого ключа:

$$M_1 = C^e \ (mod\ n),$$
$$M_1 = 7350^{31} \ (mod\ 21311) = 2108$$

– число 2108 переводится в текстовый формат: 2108 → «уж».

Если все вычисления проведены правильно, то второй студент получит то же самое слово, что написано на бумажке. Потом студенты меняются ролями.

Для уменьшения вычислений можно добавить промежуточное хэширование сообщений, и шифровать не само сообщение, а его хэш (что и происходит на практике). Например, хэш-сумма может вычисляться по простому правилу:

$$h(M) = M \ (mod\ 13)$$

Следующий сценарий игры предполагает создание и применение общего ключа с использованием алгоритма Диффи-Хеллмана.

Алгоритм Диффи-Хеллмана позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищённый от подмены канал связи. Полученный ключ можно использовать для обмена сообщениями с помощью симметричного шифрования.

Снова группа разбивается на пары. Теперь действия внутри пар почти идентичны. Сначала студенты сообща выбирают два простых числа, например, n = 67 и q = 11; эти числа может предложить и сам преподаватель. Теперь первый студент

– выбирает себе число – свой секретный ключ, например, α = 47;
– вычисляет число $A = q^{\alpha}\ (mod\ n)$:

$$A = 11^{47}\ (mod\ 67) = 2$$

Он записывает числа на бумажке, и передает записку второму студенту (рисунок 2):

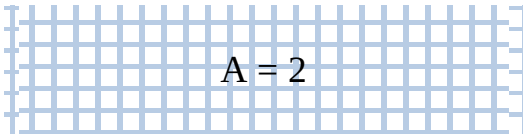

Рисунок 2

Действия второго студента:

– выбирает себе число – свой секретный ключ, например, β = 51;
– вычисляет число $B = q^{\beta}\ (mod\ n)$:

$$B = 11^{51}\ (mod\ 67) = 3$$

Он также записывает числа на бумажке, и передает записку первому студенту (рисунок 3):

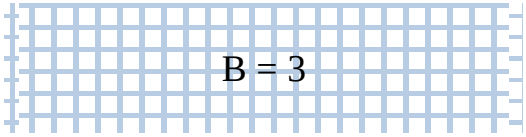

Рисунок 3

Студенты записывают числа на бумажках, и обмениваются между

собой. Теперь оба студента вычисляют общий ключ. Первый студент:

$$K = 3^{\alpha}\ (mod\ n) = 3^{47}\ (mod\ 67) = 27$$

Действия второго студента:

$$K = 2^{\beta}\ (mod\ n) = 2^{51}\ (mod\ 67) = 27$$

Если студенты все сделали правильно, то ключи совпадают, и пара может эффективно обмениваться сообщениями. Данный метод можно совместить с шифром Цезаря, для определения шага сдвига алфавита. Студенты шифруют слова полученными шифрами, и передают криптотексты друг другу для расшифровки. Если ключи совпадают, то оба студента могут успешно расшифровать тексты друг друга.

Итак, по итогам занятий, студенты «смоделировали» процесс создания электронной цифровой подписи и ее проверки, создали общий ключ по алгоритму Диффи-Хеллмана и обменялись сообщениями. Такие занятия помогут студентам закрепить материал по RSA-шифрованию, понять особенности применения цифровой подписи и решения проблемы распределения ключей. Студенты действовали парами, но ничто не мешает создать команды и провести данные мероприятия в виде соревнований.

Библиографический список

1. Королева Н.М., Костерина И.В. Роль интерактивного обучения в современном образовании // Ученые записки. Электронный научный журнал Курского государственного университета 2015. № 1(33). С. 128-132.
2. Кашлев С.С. Технология интерактивного обучения: учеб.-метод. пособие. М.: Тетрасистемс, 2005. 35 с.
3. Кнауб Л.В. Новиков Е.А., Шитов Ю.А. Теоретико-численные методы в криптографии: учебное пособие. Красноярск: Сибирский федеральный университет, 2011. 160 с.