Профессиональный соперник криптографии (ПСК): модель разработки игр для изучения криптографии

С. Г. Иванов, Zahra Dorostkar
Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В.И. Ульянова (Ленина)
sg_ivanov@mail.ru, zdorostkar@stud.etu.ru

***Аннотация*. В настоящее время информационные технологии и особенно искусственный интеллект являются очень важным инструментом в различных аспектах жизни человека. Неотъемлемая часть человеческой жизни – это обучение, использующее различные методы. С самых первых дней жизни мы начинаем учиться, играя в игры. В последние годы с развитием искусственного интеллекта мы видим широкое использование его в разработке игр. С другой стороны, одна из самых важных частей информационных технологий, которую необходимо изучить, - это криптография, и необходимо найти хороший метод изучения этого. В своей работе мы предлагаем модель, которая представляет собой игру, основанную на планировании уроков и использующую искусственный интеллект. Сначала мы рассказываем о планировании уроков, затем описываем дизайн нашей игры и способы использования искусственного интеллекта.**

Ключевые слова: криптография, модель разработки игр, искусственный интеллект, обучение, планирование уроков

I. Введение

Обучение – очень важная часть жизни человека, и с развитием информационных технологий оно стало одним из важнейших средств обучения. В наши дни компьютерные игры настолько популярны, и это важный инструмент, который можно использовать в качестве обучающего устройства. Чтобы создать плодотворную игру, необходимо воспользоваться преимуществами искусственного интеллекта, чтобы иметь приемлемый и развивающийся продукт. В этой статье криптография рассматривается как тема обучения, которая должна быть разработана как игра. Была сделана попытка получить исчерпывающий взгляд на криптографию в качестве урока. Кроме того, разработанная нами игра Cryptography Professional Rival (CPR) рассматривается с точки зрения планирования урока. При проектировании искусственный интеллект используется как противник и как обучаемый.

II. Модель

A. Планирование урока

Во-первых, необходимо составить план урока, поскольку этого требует любой учебный материал. Как объяснил Стронге [1], существует семь элементов с разными собственными правами, чтобы организовать эффективный план урока и помочь нам создать его всесторонне, которые были рассмотрены в различных подходах, как следующие: Четкий урок и цели обучения (Rosenshine (1986), Джаспер (1986), Бэйн и Джейкобс (1990), Ван и др. (1993b), Захорик (2003), Джонс и др. (2011)), Создание заданий качества (Pressley и др. (1998), Wharton-McDonald (1998), Клэр (2001), Захорик (2003), Кох и Люк (2009)), Логически структурированные уроки (Rosenshine (1986), Джаспер (1986), Ван и др. (1993a), Good & Brophy (1997), Wharton-McDonald (1998), Clare (2001), Zahorik (2003), Panasuk & Todd (2005), Marzano (2007)), Стратегии обучения (Rosenshine (1986), Wang et al. (1993a), Johnson (1997)), Pressley et al. (1998), Wharton-McDonald (1998), Marzano et al. (2001)), Timing (Jasper (1986), Wang et al. (1993b), Wharton-McDonald (1998), Cameron et al. (2005), Кэмерон (2008)), Различия в обучении (Rosenshine (1986), Bain И Джейкобс (1990), Wharton-McDonald (1998), Cameron (2008), Jones et. al (2011)), Разработка соответствующих возрасту планов (Pressley et al. (1998), Wharton-McDonald (1998)).

Четкие цели урока и обучения помогают иметь четкую дорожную карту по теме, которая в основном сосредоточена на обучении учащихся, а не на их деятельности [2].

Сосредоточившись на предыдущем элементе, учителя могут организовать несколько качественных заданий, которые сделают успехи учеников возможными [3].

Планирование уроков может быть логически структурировано, если мы рассмотрим последовательность и согласование. Последовательность важна как в одном уроке, так и в серии уроков. Это позволяет учащимся объединять идеи. Согласованность помогает быть уверенным, что все части последовательности планирования урока работают вместе для достижения цели учеников, особенно цели, деятельности и оценки [4].

Когда учитель правильно использует различные учебные стратегии, уроки и задания становятся более интересными для учащихся [5]. Также он дает разные результаты [6].

Этот аспект планирования урока влияет на последовательность урока и позволяет учителям максимально использовать время учеников с материалом.

Эффективно больше времени тратится на обучение и обучение и меньше – на переход [6], [7].

Каждый человек в классе индивидуален, и учитель должен помнить об этих различиях при планировании, чтобы сделать материал значимым для каждого человека. [8] Необходимо эффективно учитывать потребности разнообразной группы учащихся [7], [8], [9]. Разработка планов уроков, соответствующих возрасту и содержанию, связана с планированием различий в обучении. Педагог должен понимать возраст детей, познавательно и с точки зрения развития, что подходит, и знать, что интересует возрастную группу. Один из способов, с помощью которого эффективные учителя разрабатывают планы, соответствующие возрасту и содержанию, учитывают различия в обучении и используют различные стратегии обучения, – это использование аутентичных занятий [7]. Кроме того, учителям нужны планы уроков, чтобы бросить вызов ученикам, находящимся за пределами их зоны комфорта, и поддержать их строительными лесами [7], [10]. Наша целевая группа – старшеклассники и студенты вузов.

Элементы, рассматриваемые в нашем подходе, подробно описаны в разделе о разработке игр.

A. Дизайн игр

В основном при проектировании учитываются два аспекта: Атрибуты обучения, которые представляют собой отношения выбранных элементов планирования урока, описанных в предыдущем разделе, с нашим предметом и их настройкой. Учитываются шесть из семи элементов планирования урока: четкие цели урока и обучения, логически структурированные уроки, стратегии обучения, время, различия в обучении, разработка планов, соответствующих возрасту. И технические атрибуты, которые представляют собой спецификации игры для реализации.

1) Атрибуты обучения

Учитывая четкий урок и цели обучения, план состоит в том, чтобы помочь игрокам начать с базовых знаний математики, алгоритмов и оптимизации, продолжить изучение различных алгоритмов и решить вопросы и, наконец, научиться создавать проблемы. Он включает в себя основные определения (алгоритм, протокол, его использование – здесь OpenSSL и TLS – большая заключительная часть. – сложность, ...), математику (матрицы, модульная арифметика, полиномы, ...), типы алгоритмов криптографии. (физический, математический, квантовый) [11]. Для типов алгоритмов криптографии, независимо от реального использования, все они определены следующим образом:

- Физический – шифр Атбаш, шифр ROT13, шифр Цезаря, аффинный шифр, шифр с ограждением рельсов, шифр Бэкона, шифр с квадратом Полибия, шифр простой подстановки, шифр кодов и номенклатур, шифр столбцового транспонирования, шифр с автоключом, шифр Бофорта, шифр Порта Ключевой шифр, шифр Виженера и Гронсфельда, шифр гомофонической замены, четырехквадратный шифр, шифр Хилла, шифр Playfair, шифр ADFGVX, шифр ADFGX, шифр Bifid, шифр Straddle Checkerboard, шифр Triherfid, шифр Basection64, шифр Basection64
- Математический – для этой группы важны три типа: хеширование, симметричный и асимметричный. Алгоритмы хеширования включают MD5, SHA-1, RIPEMD-160, Whirlpool, SHA-2, SHA-3, BLAKE2 и BLAKE3. Симметричные алгоритмы: DES, Advanced Encryption Standard (AES, Rijndael), MARS, Triple DES (3DES), Education Data Encryption Standard (E-DES), Blowfish Encryption, SEAL.
- Алгоритм, RC2, RC4, RC6, Twofish, Serpent, IDEA, CAST, HiSea и асимметричные алгоритмы включают RSA, ECC, систему шифрования ElGamal (DSA), Diffie-Hellman, XTR. На основе входных данных алгоритмы шифрования классифицируются как блочные шифры и потоковые шифры [12], [13], [14].
- Quantum

Ориентируясь на логически структурированный план, мы предлагаем три отдельных уровня: базовый, средний и продвинутый. У любого из них есть подуровни. На базовом уровне игрок изучает основы криптографии, такие как алгоритм против протокола, где и почему он используется? И математическая основа. На промежуточном уровне он или она изучает различные типы алгоритмов в реальной последовательности их улучшения и решает их проблемы. На продвинутом уровне игроки могут сами создавать вопросы, и в случае правильности, которая проверяется в игре, они могут набирать очки и повышать свой уровень.

Эти подходы позволят реализовать множество учебных стратегий:

- Игроки могут выбрать два режима: режим обучения, режим соревнования. В режиме обучения есть несколько вопросов или задач, которые нужно решать в одиночку или в группе. В режиме соревнования они могут соревноваться с реальным конкурентом-человеком или компьютерным агентом.
- В режиме обучения игроки могут выбрать время (обратный отсчет) или вневременное состояние. Вневременное состояние – это часть, которую игроки могут изучать и проверять ответы без конкуренции и стресса. В режиме обратного отсчета игроки могут объединиться в группу, чтобы решать вопросы методом мозгового штурма. Однако это не влияет на количество очков, которое игрок работает в одиночку или в группе.

Типы задач в основном похожи на соревнования Capture The Flag (CTF), чтобы быть более увлекательными и интересными для учащихся.

Поскольку было описано, что он начинается с основ, а затем появляются различные типы алгоритмов в их реальной последовательности улучшения, существует правильная последовательность.

Рассматривая любого игрока как личность, необходимо сосредоточить внимание на его слабости или силе. Чтобы достичь этой цели, в игре на любом уровне чаще появляются проблемы, более похожие на его или ее неправильные ответы.

Что касается целевой группы, которой являются учащиеся, считается, что они уже имеют знания в области базовой математики, а также могут не иметь передовых знаний в области математики или разработки алгоритмов в начале.

1) Технические характеристики

Структура: Наша игра – это онлайн-игра, в которую каждый может играть, войдя в систему с идентификатором. На любом из трех уровней есть база данных типовых вопросов, и на их основе может быть сгенерировано бесконечное количество похожих вопросов. На первом и втором уровне есть несколько подуровней по количеству предметов. И добавлен дополнительный уровень, который называется ComeBack.

Любой игрок сначала начинает с вневременного состояния режима обучения, потому что необходимо, чтобы сначала были представлены знания, а затем он или она участвует в соревновании или обратном отсчете. На одном подуровне пять вопросов на всех подуровнях базового уровня. На каждом подуровне вопросы взяты из общей темы. Когда игрок проходит подуровень, он или она может начать соревнование, связанное с этим предметом. Пройдя набор из пяти таких подуровней, игрок переходит к следующей тематической группе (набору подуровней).

Получение идей из системы Лейтнера [15], в любом наборе, если он или она не может правильно ответить на подуровень – три вопроса из пяти – этот предмет добавляется к уровню ComeBack. (Также он или она не может идти дальше, пока он или она не повторит этот подуровень столько раз, сколько он или она решит его правильно.) Каждый раз, когда уровень ComeBack включает в себя три темы, игрок должен вернуться, чтобы решить кучу вопросов о них по порядку, что может продолжить прогресс. Состояние обратного отсчета имеет различные параметры, которые настраиваются для каждого игрока в зависимости от его способностей и прогресса. Если игрок правильно отвечает во временном интервале, скорость увеличивается до предела. Если только не уменьшать его шаг за шагом, вплоть до вневременного состояния. На третьем уровне, который принадлежит ведущим профессиональным игрокам, они могут сами создавать задачи или вопросы и добавлять их в игру.

Подсчет очков: Любой подуровень с пятью вопросами имеет свой собственный счет. По количеству набранных очков различают шесть типов игроков: новичок, юниор, старший, старший старший, серебристый, золотой. С самого начала режим обучения имеет более низкий балл, чем режим соревнования, а внутри режима обучения вневременное состояние имеет самый низкий балл.

Повышая уровень на подуровнях, оценка увеличивается так же, как и за счет ускорения. Если игрок побеждает участника более низкого или того же уровня, он или она получает фиксированное количество очков в зависимости от уровня, на котором он или она соревнуется, в противном случае игрок получает фиксированное количество очков плюс бонус. После каждого набора подуровней появляется случайный вызов более высоких уровней. (Это побуждает людей учиться и идти дальше.) Если игрок может решить эту задачу, он или она, кстати, получает бонусный счет, в противном случае он не добавляется в часть ComeBack.

A. Искусственный интеллект в нашей игре

ИИ используется в двух аспектах СЛР: как противник и как обучаемый.

ИИ как противник

Это одно из старейших применений ИИ в играх любого типа. Этот шаблон используется, чтобы предоставить игроку противника, когда его не найти. Поскольку одна из частей CPR - это режим соревнования, обязательно иметь соперника. Агенты AI позволяют играть в игру в любое время и против конкурента с регулируемыми возможностями (уровнем).

ИИ как стажер

Методы машинного обучения с помощью примеров изучают новые модели поведения. В CPR основные данные – это правильные и неправильные ответы игрока как источник примеров, на которых агент ИИ может извлечь уроки. Он вращается вокруг типа проблем, связанных со знаниями любого человека. Если у игрока есть слабые места в теме, созданные проблемы в основном превращаются в эту тему. Обучение без учителя используется потому, что оно позволяет абстрагироваться от примеров без явного руководства.

Кроме того, этот шаблон используется для регулировки скорости любого игрока на любом уровне или подуровне. Скорость может меняться в течение любой части игры [16].

III. Сценарий

В качестве примера с нуля есть 10 примеров вопросов на любом подуровне в базе данных. Алекс - новый игрок. Он начинает игру. Он должен начать из вневременного состояния режима обучения. В режиме обучения он отвечает на первые 5 вопросов и дает 4 правильных ответа. Он может выбрать режим соревнования для этой части или временное состояние этого. Он решает продолжить, как начал. В следующем раунде Он проходит подуровень с 3 правильными ответами, но решает пройти его снова. Во второй попытке он дает 4 правильных ответа. Если он решит переделать этот подуровень, наша система генерирует новый набор вопросов, полученных из неправильных ответов.

Например, неправильный ответ принадлежал «Упомяните, какие типы нотации используются для временной сложности? Big O & Omega – Big Theta – Little O & Omega – Все выше», поэтому наша система генерирует связанный вопрос, например: «Какой из них не связан с временной сложностью? Big O – Big Omega – Big Theta – Little Theta».

Другой пример: Анна – игрок второго уровня. Она проходит подуровни в статусе обратного отсчета. Она проходит первый и второй подуровни второго уровня. На третьем подуровне она терпит неудачу. Эта тема добавлена в ComeBack. Во второй попытке ее скорость снижается, и она проходит мимо. На следующем подуровне и на последующем происходит то же самое. Таким образом, ее направляют к возвращению. Первые две попытки ей не удалось. В этом случае наша система генерирует больше связанных вопросов относительно ее ответов.

Например, одна из проблем, на которую был дан неправильный ответ, заключалась в следующем: «Мы знаем, что для этого сообщения используется Caesar Cipher, но мы не знаем масштабов. Найдите простой текст? TU IADXP», и наша система создает связанную задачу вроде этого: «Мы знаем, что для этого сообщения используется Caesar Cipher, но мы не знаем масштабов. Найдите простой текст? CSY ASR».

В другом случае Роя хочет начать соревнование. Она игрок уровня Top Senior. На данный момент ни один соперник не принимает ее приглашение. Таким образом, наша система создает Али, соперника старшего уровня, в качестве своего конкурента.

IV. Выводы

В этой статье обсуждалась модель игрового проектирования. Основная цель этой работы заключалась в том, чтобы представить учебный материал, который извлекает выгоду из игры, которая используется из искусственного интеллекта, чтобы помочь студентам изучить криптографию удобным и академическим способом, который также является радостным и привлекательным. Это увлекательно и может побудить людей узнать больше. Кроме того, с помощью искусственного интеллекта дизайн можно было адаптировать к любому человеку, что делало его более приемлемым для соревнований. Поскольку эта модель была обучающей, универсальной и независимой от предмета, ее можно использовать и для любых других предметов.

Список литературы

[1] J.H. Stronge, “Qualities of effective teachers” 2nd ed. Alexandria, VA: Association for Supervision and Curriculum Development, 2007.

[2] C. Danielson, “Enhancing professional practice: A framework for teaching,” 2nd ed., Alexandria, VA: Association for Supervision and Curriculum Development, 2007.

[3] L. Clare, “Exploring the technical quality of using assignments and student work as indicators of classroom practice,” Educational Assessment, 7(1), 39-59, 2001.

[4] R.M. Panasuk, J. Todd, “Effectiveness of lesson planning: Factor analysis,” Journal of Instructional Psychology, 32(2). Retrieved November 13,2010 from the Education Research Complete database, 2005.

[5] C.A. Tomlinson, J. McTighe, “Integrating differentiated instruction & understanding by design: Connecting content and kids”. ASCD; 2006.

[6] M.C. Wang, G.D. Haertel, H.J. Walberg, “What helps students learn?” Educational Leadership 51(4), 74-79, 1993b.

[7] R. Wharton-McDonald, M. Pressley, J.M. Hampston, “Literacy instruction in nine first-grade classrooms: Teacher characteristics and student achievement,” The Elementary School Journal, 99(2), 101-128, 1988.

[8] H.P. Bain, R. Jacobs, “The case for smaller classes and better teachers,” Streamlined Seminar – National Association of Elementary School Principals, 9(1), 1990.

[9] Дж. А. Дэвис, М.А. Томас, «Эффективные школы и эффективные учителя», Бостон, Массачусетс: Allyn & Bacon, 1989.

[10] М. Прессли, Р. Уортон-Макдональд, Р. Аллингтон, К.К. Блок, Л. Морроу, «Природа эффективного обучения грамоте в первом классе» (отчет № CELA-R-11007). Олбани, штат Нью-Йорк: Национальный исследовательский центр изучения английского языка и успеваемости, 1988.

[11] С.Г. Иванов, «Викторина по криптографии», СПбГЭТУ «ЛЭТИ»: Учебные материалы, не опубликовано, 2020.

[12] О. Абуд, С. Гирги, «Обзор алгоритмов криптографии», Международный научно-исследовательский журнал. 8. 495-516. 10.29322 / IJSRP.8.7.2018. p7978.

[13] М. Муштак, С. Джамель, А. Дисина, З. Пиндар, Н. Шакир, М. Мат Дерис, «Обзор алгоритмов криптографического шифрования», Международный журнал передовых компьютерных наук и приложений. 8. 333-343. 10.14569 / IJACSA.2017.081141.

[14] С.В. Свати, П.М. Лахари, Б.А. Томас ». Алгоритмы шифрования: обзор», Международный журнал перспективных исследований в области компьютерных наук и технологий (IJARCST 2016), Vol. 4, вып.2.

[15] С. Редди, И. Лабутов, С. Банерджи, Т. Йоахимс, «Неограниченное человеческое обучение: оптимальное планирование для интервального повторения», Proc. ACM SIGKDD Int., 13-17 августа 2016 г., стр. 1815–1824, 2016 г., DOI: 10.1145 / 2939672.2939850.

[16] М. Тринор и др., «Шаблоны игрового дизайна на основе ИИ». Август 2015 г.