Cryptography Professional Rival(CPR) : A Game Designing Model to Learn Cryptography

Sergey G. Ivanov
Department of Algorithmic Mathematics
Saint Petersburg Electrotechnical University
Saint Petersburg,Russia
sg_ivanov@mail.ru

Zahra Dorostkar
Department of Computer Science and Engineering
Saint Petersburg Electrotechnical University
Saint Petersburg,Russia
zdorostkar@stud.etu.ru

***Abstract*—Nowadays information technology and particularly artificial intelligence is a very vital tool in different aspects of human life. One inseparable part of human life is learning which has diverse methods. From the very first days of our life we start to learn by playing games in different ways. In recent years with growth of artificial intelligence we see widespread usage of it in game designing. On the other hand, one of the most important parts of information technology to be learned is cryptography, there is a need to find a good method of learning that. In our work we propose a model which is a game, based on lesson planning and utilizes artificial intelligence. Firstly, we explain about lesson planning then describe our game design and how artificial intelligence is used.**

Keywords—Cryptography, Game Designing Model, Artificial Intelligence, Learning, Lesson Planning

I. Introduction

Learning is a very important part of human life and with the growth of information technology it has benefitted from it as one of the most vital devices of learning. Nowadays computer games are so popular and it is a considerable tool to be utilized as a learning device. In order to create a fruitful game it is necessary to take advantage of artificial intelligence to have an acceptable and developing product. In this article, cryptography is considered as the topic of learning to be designed as a game. An attempt has been made to have a comprehensive view of cryptography as a lesson. In addition, our designed game, Cryptography Professional Rival(CPR), is considered from a lesson planning aspect. In designing, artificial intelligence is used as an adversary and as trainee.

II. Model

A. Lesson Planning

First, it is necessary to create a lesson plan as any teaching material requires that. As Stronge explained there exist seven elements with different own rights in order to organize an effective lesson plan and help us to create it comprehensively, which have been considered in different approaches as following: *Clear Lesson & Learning Objectives* (Rosenshine(1986), Jasper(1986), Bain & Jacobs(1990), Wang et al.(1993b), Zahorik(2003), Jones et. al(2011)), *Creating Quality Assignments* (Pressley et al.(1998), Wharton-McDonald(1998), Clare (2001), Zahorik(2003), Koh & Luke(2009)), *Logically Structured Lessons* (Rosenshine(1986), Jasper (1986), Wang et al.(1993a), Good & Brophy (1997), Wharton-McDonald (1998), Clare(2001), Zahorik(2003), Panasuk & Todd(2005), Marzano(2007)), *Instructional Strategies* (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), Cameron (2008)), *Learning Differences* (Rosenshine (1986), Bain & Jacobs (1990), Wharton-McDonald (1998), Cameron (2008), Jones et. al (2011)), *Developing Age Appropriate Plans* (Pressley et al.(1998), Wharton-McDonald(1998)).

Clear lesson and learning objectives help to have a clear road map of the topic which mostly focus on students' learning rather than their activities [1].

Focusing on the previous element, teachers can organize some quality assignments that make the students' progress and achievement become possible [2].

Lesson planning can be logically structured if we consider sequencing and alignment. Sequentiality is important in one single lesson and also in a set of lessons. It enables learners to connect ideas. Alignment helps to be sure that all the parts of the lesson planning sequence are working together toward the goal of student achievement, especially the objective, activity, and evaluation[3].

When a teacher correctly uses a variety of instructional strategies, lessons and tasks become more engaging to learners[4]. Also it generates diverse outcomes [5].

This aspect of lesson planning impacts the sequencing of the lesson and allows teachers to maximize students' time with the material. In an effective way more time is spent on teaching and learning and less time on transitioning [5][6]

Each person in the class is an individual and the teacher must mind about these differences in planning to make the material meaningful for each person.[7] In effective ways the needs of a diverse group of learners must be considered.[6][7][8].

Developing age and content appropriate lesson plans relates to planning for learning differences. The teacher must understand the age of the children, know cognitively and developmentally what is appropriate, and know what interests the age group. One way effective teachers develop age and content appropriate plans, while meeting learning differences, and using varied instructional strategies, is through the use of authentic activities [6]. Additionally, teachers need lesson plans to challenge students just outside their comfort zone and support them by scaffolding [6][9].

Our goal group are senior high school students and university students.

The elements considered in our approach are explained in the game designing section in detail.

B. Game Designing

Basically two aspects are considered in designing: *Learning Attributes* which are the relations of the chosen elements of lesson planning explained in the previous section with our subject and customization of them. Six out of seven of lesson planning elements are considered: Clear Lesson & Learning Objectives, Logically Structured Lessons, Instructional Strategies, Timing, Learning Differences, Developing Age Appropriate Plans. And *Technical Attributes* which are specifications of the game for implementing.

1) Learning Attributes

Considering clear lesson and learning objectives, the plan is to help players start with the basic knowledge of mathematics and algorithms and optimization, continue with knowing different algorithms and solve the questions and finally to be able to create problems. It includes main definitions(algorithm, protocol, usage of it -Here OpenSSL and TLS is a big concluded part.-, complexity,...), mathematics(matrices, modular arithmetic, polynomials,...), types of cryptography algorithms(physical, mathematical, quantum).[10] For types of cryptography algorithms regardless the real usage, all are defined as following:

- Physical - Atbash cipher, ROT13 cipher, Caesar cipher, Affine cipher, Rail-fence cipher, Baconian cipher, Polybius Square cipher, Simple Substitution cipher, Codes and Nomenclators cipher, Columnar Transposition cipher, Autokey cipher, Beaufort cipher, Porta cipher, Running Key cipher, Vigenère and Gronsfeld cipher, Homophonic Substitution cipher, Four-Square cipher, Hill cipher, Playfair cipher, ADFGVX cipher, ADFGX cipher, Bifid cipher, Straddle Checkerboard cipher, Trifid cipher, Base64 cipher, Fractionated Morse cipher
- Mathematical - Three types for this group are considerable: Hashing, Symmetric and Asymmetric. Hashing algorithms include MD5, SHA-1, RIPEMD-160, Whirlpool, SHA-2, SHA-3, BLAKE2 and BLAKE3. Symmetric algorithms are DES, Advanced Encryption Standard (AES, Rijndael), MARS, Triple DES (3DES), Educational Data Encryption Standard (E-DES), Blowfish Encryption, SEAL Algorithm, RC2, RC4, RC6, Twofish, Serpent, IDEA, CAST, HiSea and asymmetric algorithms include RSA, ECC, ElGamal Encryption System(DSA), Diffie-Hellman, XTR. On the basis of the input data, encryption algorithms are classified as block ciphers, and stream ciphers.[11][12][13]
- Quantum

Focusing on a logically structured plan, we suggest three separated levels: *Basic, Intermediate, Advance*. Any of them has sub-levels. For the basic level the player learns fundamentals of cryptography such as algorithm vs protocol, where and why it is used? And mathematical foundation. In the intermediate level he or she learns different types of algorithms in the real improvement sequence of them and answers the problems of them. In the advance level players can create questions themselves and in case of correctness which is checked in game, they can gain scores and level up.

Variety of instructional strategies, would be possible by these approaches:

- ➢ Two modes can be chosen by the players : Learning mode, Competition mode. In learning mode there are some questions or challenges to be solved solo. In competition mode they can compete with a real human competitor or a computer agent.
- ➢ In learning mode, the players can select timing(countdown) or timeless state.

The challenges' types are mostly similar to Capture The Flag(CTF) competitions in order to be more engaging and interesting for students.

Since it has been described that it is started from fundamentals and then different types of algorithms appear in the real improvement sequence of them, there is a proper sequence.

Considering any player as an individual, it is needed to focus on that person's weakness or strength. In order to reach this aim, in the game in any level challenges more similar to his or her wrong answers appear more commonly.

Regarding the goal group which is students, it is considered that they already have knowledge of basic mathematics also they may don't have advanced knowledge in mathematics or algorithm design at the beginning.

2) Technical Attributes

Structure: Our game is an online game that everybody can play by login with an Id. In any level of three levels, there is a database of sample questions and based on them an infinite number of similar questions can be generated.In first and second level there are some sublevels regarding the number of subjects. And an extra level which is called *ComeBack* is added.

Any player firstly starts from *Timeless* state of *Learning mode*, because it is necessary that knowledge be presented first and later he or she enters the competition or countdown. In a single sub-level there are five questions in all sublevels of the basic level. In each sub-level the questions are from a common topic. When the player passes a sublevel, they can join a competition related to that subject. After passing a set of five of these sublevels, the player goes to the next subject group(set of sublevels).

Getting ideas from the Leithner System,[14] in any set if he or she can not answer a sublevel correctly - three questions out of five- this subject is added to the ComeBack level. (Also they can not go further until they repeat this sublevel as many times as they solve it correctly.) Whenever the ComeBack level includes three subjects the player must come back to solve a bunch of questions about them in order that they can continue the progress. The CountDown state has different options which are customized for any single player regarding their ability and progress. If the player answers correctly in a time slot, the speed is increased up to a limit. Unless it is decreased step by step, down to timeless state. In the third level which belong to top professional

players, they can create challenges or questions themselves and add it to the game.

Scoring: Any five-questioned sublevel has its own score. Regarding the gained score there are six types of players: newbee, junior, senior, top senior, silvery, golden. From the beginning, Learning mode has a lower score than Competition mode and inside the Learning mode the timeless state has the lowest score.

By leveling up in the sublevels the score is increased as well as by speeding up. If the player wins a lower or same level competitor he or she gains a fixed score regarding the level they compete on, otherwise the player earns a fixed score plus a bonus. After every set of sublevels, a random challenge of higher levels is appeared. (It encourages people to learn and go further.) In case the player can solve it, they gain a bonus score, by the way, otherwise it is not added to the ComeBack part.

C. Artificial Intelligence in our game

AI is used in two aspects of CPR: as Adversary and as Trainee.

- AI as Adversary

This is one of the oldest uses of AI in any types of games. This pattern is used to provide the player with a competitor when none (or few) may be found. Since one part of CPR is Competition mode it is necessary to have an opponent for sure. AI agents make it possible to play the game at any time and against a competitor with adjustable capabilities(level).

- AI as Trainee

Machine learning techniques by means of using examples learn new behaviours. In CPR the main data is right and wrong answers of the player as a source of examples which the AI agent can learn from. It revolves around the type of generating challenges regarding any individual's knowledge. If the player has weakness in a topic, the generated challenges mostly turn into that topic. Unsupervised learning is used because it can abstracts from examples without explicit guidance.

Additionally, this pattern is used for adjusting the speed of any player in any level or sublevel. The speed can change during any part of the game. [15]

III. Conclusion

In this article a game designing model was discussed. The main aim of this work was presenting a learning material which benefits from a game that is utilized from AI to help students learn cryptography in a convenient and academic way which is also joyable and attractive. It is engaging and can encourage people to learn more. In addition, using AI, the design could be adjustable to any individual, plus, made it more acceptable in the competition aspect. Since this model is teaching-based, universal and independent from the subject, it is possible to be used for any other subjects as well.

References

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

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

[3] 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.

[4] CA. Tomlinson, J.McTighe, "Integrating differentiated instruction & understanding by design: Connecting content and kids". ASCD; 2006.

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

[6] 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.

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

[8] G. A. Davis, M. A. Thomas, "Effective schools and effective teachers," Boston, MA: Allyn & Bacon, 1989.

[9] M. Pressley, R.Wharton-McDonald, R. Allington, C. C. Block, L. Morrow, "The nature of effective first-grade literacy instruction" (Report No. CELA-R- 11007). Albany, NY: National Research Center on English Learning and Achievement, 1988.

[10] S. G. Ivanov, "Quiz on cryptography," Saint Petersburg State Electrotechnical University(LETI), Teaching material, Unpublished, 2020.

[11] Abood, Omar & Guirguis, Shawkat. (2018). A Survey on Cryptography Algorithms. International Journal of Scientific and Research Publications. 8. 495-516. 10.29322/IJSRP.8.7.2018.p7978.

[12] Mushtaq, Muhammad & Jamel, Sapiee & Disina, Abdulkadir & Pindar, Zahraddeen & Shakir, Nur & Mat Deris, Mustafa. (2017). A Survey on the Cryptographic Encryption Algorithms. International Journal of Advanced Computer Science and Applications. 8. 333-343. 10.14569/IJACSA.2017.081141.

[13] S.V. Swathi, P.M. Lahari, B.A. Thomas. 2016. Encryption Algorithms: A Survey, International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016), Vol. 4, Issue 2.

[14] S. Reddy, I. Labutov, S. Banerjee, and T. Joachims, "Unbounded human learning: Optimal scheduling for spaced repetition," Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min., vol. 13-17-August-2016, pp. 1815–1824, 2016, doi: 10.1145/2939672.2939850.

[15] M. Treanor *et al.*, "AI-Based Game Design Patterns AI-Based Game Design Patterns," no. August, 2015.