Journal of Engg. Research Vol. 9 No. (3A) September 2021 pp. 143-152 DOI : 10.36909/jer.v9i3A.10943

The use of computer games for teaching and learning cybersecurity in higher education institutions

Mohammed Yahya Alghamdi* and Younis A. Younis**

**Assistant Professor, Department of Computer Science, Faculty of Science & Arts of Baljurshi AL-Baha University, Baha, Saudi Arabia*
***Assistant Professor, Department of Computer Science, Faculty of Information Technology, University of Benghazi, Benghazi, Libya*
**Corresponding Author: Myahya@bu.edu.sa*

Submitted: 26/06/2020
Revised: 03/12/2020
Accepted: 08/12/2020

ABSTRACT

In higher education, teaching cybersecurity concepts to students such as encryption-based security protocols is a challenging task, but it is fundamental for personal and national security. One of the reasons for this is related to the inadequate mathematical knowledge of students, which limits their understanding of the cryptographic algorithms underlying the protocols. Therefore, higher education institutions are seeking out engaging and effective strategies for developing students' skills in this area. The aim of this research is to explore the use and potential effectiveness of game-based learning to assist in the teaching and learning of cybersecurity concepts in higher education. It contributes to the literature by raising public interest in cybersecurity and helping learners to understand suitable and safe behaviors online. It also offers a systematic overview of game-based learning tools that have been used in previous studies to improve students' understanding of cryptographic algorithms. This research also presents a framework for the effective teaching of cryptography in higher education, relying on animation and gamification.

Keywords: Computer game-based learning; Interactive learning environment; Technology-enhanced learning; Digital games; Cybersecurity education; Cryptography.

INTRODUCTION

Historically, the purpose of games was predominantly for entertainment, but researchers are increasingly recognizing the value of game-based learning (Mayer, 2019) (Boghian et al., 2019). The current generation of learners are digital natives who have grown up in an environment replete with technology-based games (Chaudhry, 2019) (Putri et al., 2016). Furthermore, young people's extensive use of the Internet and their engagement with other types of digital communications have influenced their use of information and their learning.

The number of people using games exclusively for learning purposes has increased significantly in recent years (Gumusgul, 2019). Therefore, this study focuses on the use and potential value associated with computer game-based learning in higher education for cryptography. The field of cryptography is concerned with safeguarding information and communications using codes, and it serves as the foundation of today's secure network infrastructures. Cryptography is also a central research area in data security and an essential element of information assurance. For these reasons, the teaching and learning of cryptography is important for all information assurance courses, with key concepts being encryption, decryption, and cryptanalysis.

Due to the involvement of mathematical concepts from probability and abstract algebra in cryptography, students often suffer from a knowledge gap in this area (especially those with limited mathematical backgrounds), or suffer from

special difficulties when pursuing studies in this field (de Castro et al., 2019) (Chang & Yang, 2016; Hsiao et al., 2016). Therefore, various pedagogical strategies have been devised to support students in understanding the mathematical elements of cryptographic algorithms, including both practical and theoretical approaches. An important limitation of theoretical approaches, which often rely on textbooks, is that students with limited knowledge of mathematical notation experience difficulties when attempting to make progress.

Diverse approaches have been developed in the literature to improve cryptography teaching and learning in higher education, particularly in terms of advancing students' understanding of cryptographic algorithms. A well-known approach involves the use of visualization tools, which relies on the conversion of mathematical notation and expressions into attractive and understandable diagrams (Dixit et al., 2018; Epishkina et al., 2016; Hu et al., 2018; Liu & Cheng, 2017; Liu, 2018; Parakh et al., 2017; Rahaman et al., 2018; Rao & Dave, 2019; Rass & Winkler, 2017; Salib & Hobar, 2018; Xu et al., 2016; Zhu et al., 2019).

With the above considerations in mind, this research presents a framework for enhancing the teaching and learning of cryptography in the context of higher education. The framework uses an interactive delivery model consisting of animation videos to simplify the delivery of knowledge about cryptographic protocols, along with gamification to assess the knowledge delivered to students.

The rest of this paper is structured as follows: Section 2 overviews web-based games; Section 3 examines existing visualization tools for cryptography teaching; Section 4 illustrates several proposed games for teaching specific cryptographic protocols; Section 5 presents the proposed framework; and finally, Section 6 offers concluding remarks.

AN OVERVIEW OF WEB-BASED GAMES

The scope of virtual games is broader than many individuals recognize. They incorporate easy-going games, advergames, and genuine games. Each is planned with an alternate expectation. To represent this, an easy-going game is simply used for entertainment purposes, while advergames are intended to showcase advertisements and publicize a product or service (Derryberry & Serious, 2007). The most relevant types of games to the present research are genuine games, which are defined based on their main role being something other than entertainment (Susi et al., 2007). One of the main purposes of genuine games is to train the user in a new skill or knowledge, but entertainment is also a key feature of these games (Susi et al., 2007).

Researchers have examined the distinction between genuine games and different types of Internet games, and it has been noted that genuine games are more centered around teaching and learning compared to other purposes (e.g., excitement or entertainment) (Michael & Chen, 2006). Furthermore, genuine games contrast with other web-based games in terms of their central goal, as they center around exact, intentional learning to achieve quantifiable goals (Derryberry & Serious, 2007). It has been reported that McDonald's uses genuine games to prepare store workers in client administration, store activities, and supervision (Derryberry & Serious, 2007).

The use of genuine games has many advantages for students. Maintenance increments when using PC games contrasted with other customary showing strategies (Egenfeldt-Nielsen, 2006). They give students the opportunity to encounter a situation that is difficult to recreate in reality due to factors such as security, time, and cost (Corti, 2006). Notably, a user preference survey conducted in a sample of students at Malaysia's Institute of Higher Learning revealed that 60% of the participants preferred playing games using their smartphones (Hashim et al., 2007).

Furthermore, there are opportunities for students to learn efficiently and effectively in the context of collaborative game-based learning, as reflected in the collaborative digital history game proposed by (Shiue et al. 2017).

In the Taiwan-based study of (Li et al. 2012), game-based learning (GBL), in the form of the so-called "Millionaire Language Game", was used to teach the Chinese language to primary school students. The researchers reported that

GBL improved learning attitudes in both male and female students. (Chen & Chan's 2010) research highlighted the importance of using game quests for educational purposes to address the limitations of traditional teaching methods, and the researchers demonstrated how digital games can be made compatible with school curriculums. Other studies have implemented the productive failure teaching concept with interactive learning games as a way to cultivate innovative teaching and learning. For example, (Kannappan et al. 2019) developed a 2D bridge building puzzle game to teach students about the linked list, and also to stimulate students to begin exploring the applications of this data structure.

Genuine games can be used in various aspects of teaching and learning, including military affairs, promoting health and well-being, and primary to tertiary education. This research focuses on the use and value of genuine games in the context of teaching and learning in higher education. More specifically, this research seeks to improve the teaching and learning of fundamental concepts and practices in the field of cryptography.

GAME-BASED TEACHING AND LEARNING FOR CYBERSECURITY

Today, cybersecurity is one of the most vital practices that underpins stable global functioning, and so it has become an essential module on most computer science courses in higher education. The most common methods used to teach cybersecurity are traditional lectures, textbooks, and academic papers, which often fail to engage students adequately and needlessly complicate the process of learning cybersecurity concepts such as cryptographic protocols. Hence, researchers and lecturers around the world have explored novel approaches to the teaching of cybersecurity, including the use of interactive visualization techniques such as games. Cybersecurity games can simplify and emulate cybersecurity protocols and algorithms. They also can engage students, encouraging them to interact with simulated or real-world cybersecurity challenges and devise creative ways to tackle them.

Jordan et al. (2011) proposed and designed a game called "CounterMeasures", which enables students to learn and practice cybersecurity skills by pursuing and achieving guided objectives. The game provides students with an opportunity to practice cybersecurity techniques in a virtual environment, thereby introducing them, in an engaging and entertaining way, to the repertoire of complex techniques used by cybersecurity experts. The game relies on the use of a real server to offer students with an environment resembling real-world security systems. The researchers formulated two hypotheses: firstly, that game-based learning would engage students to a greater degree compared to traditional textbook learning; and secondly, that the emulation of really existing systems would be a more effective platform for learning security concepts compared to reading technical documents. To test the hypotheses, a series of missions were assigned to students in the game to teach them security knowledge and skills. The missions assisted a student in security fundamentals while teaching and testing individual security skills. The authors used three training missions to teach students about exploits, scanning, and buffer overflows, and one live mission tested the use of the three previously learned skills. The game was developed using Flex/Flash running in an Adobe Air client. The authors evaluated the game by running it over 3 days with 20 participants. Two groups were used: an experimental group, consisting of students who played the game; and a control group, consisting of students who read from a packet of condensed computer security information. The results illustrated that the control group took approximately twice as long as the experimental group to finish the mission even though both groups showed approximately the same level of learning.

(Irvine et al. 2005) designed the CyberCIEGE video game to enhance cybersecurity education by illustrating the abstract functions and limitations of security mechanisms. The game is a construction and management resource simulation that resembles the Tycoon series of video games (Adams & Rollings, 2006). The game had over 20 scenarios that confronted students with a series of choices influencing the security of an enterprise's assets, which covered a range of computer and network security principles. Students had to make decisions within a three-dimensional office environment populated by game characters who needed to access the enterprise's assets to achieve predefined goals. Students identified vulnerabilities such as Trojan horses, trapdoors, insiders, configuration errors, and unpatched

software flaws, and they mitigated them via the deployment and configuration of simulated protection mechanisms (e.g., operating system access controls, user authentication mechanisms, firewalls, and biometric devices). The game was used by the Naval Postgraduate School for teaching its introductory course on computer security, and students' assessments were based on log generation, collection, and analysis.

(Labuschagne et al. 2011) developed an interactive game hosted by social networking sites to raise awareness of cybersecurity threats and vulnerabilities. The game applied the concept of informing the students about potential security threats and vulnerabilities, and then assessing the students. It applied principles such as comprehension or projection, decisions over hypermedia, hypertext, and multimedia to achieve perception, an extensive catalogue of questions, and user acceptance. Once a student logged on to the game, they were presented with a topic tree showing core topics graphically, along with the student's most recent achievement. When a topic was selected by a student, they had three options to choose from: a video, a slideshow, or a quiz. However, the game was not implemented on or added to social networking sites, and it was not been tested or validated. Finally, the game's contribution to enhancing the teaching and learning of cybersecurity is questionable, given that it only consisted of an interface for watching videos, looking at slides, and recording quiz answers.

GAMES AND APPLICATIONS FOR TEACHING SPECIFIC CRYPTOGRAPHIC PROTOCOLS

Varied approaches are used to teach information security, in general, and cryptographic ciphers, in particular, including traditional lectures, tutorials, and the attack/defend isolated laboratory approach (Yurcik & Doss, 2001). These approaches can be used individually or in combination to teach a small or large number of students. They can lessen the difficulties that students may experience in learning about cryptographic protocols, which are a crucial part of information protection and security. Although these approaches have been known and used for some time, they are not effective ways to teach cryptographic protocols to students who lack a strong mathematical background. Therefore, new and enhanced teaching and learning approaches, including interactive visualization, should be used to improve the teaching of specific cryptographic protocols.

In cryptography, interactive demonstrations and visualizations are not a new concept. In fact, several websites and programs already exist that offer diverse approaches to learning about cryptography protocols and ciphers. Moreover, there are several visual applications, including (CrypTool 2019), that illustrate the steps involved in an algorithm, while others allow users to type in text information to perform encryption/decryption, such as Cryptoy (GCHQ, 2014).

The US Air Force Academy undertook a project to create a set of cipher visualizations to support an undergraduate course in cryptography taken primarily by computer science and mathematics students (Schweitzer & Baird, 2006). The core aim of the project was to produce interactive demonstrations of different encryption algorithms to support lectures. The project supports various cryptographic algorithms, including Shift Cipher, Simple Substitution Cipher, Affine Cipher, Vigenère Cipher, RC4 Stream Cipher, RSA Cipher, and DES Cipher. Moreover, every cipher visualization tool is implemented as an applet in Java.

Other work has been undertaken to teach cryptography using open-source software, such as CrypTool, in order to lower the cost of using other paid software (e.g., Maple) (McAndrew, 2008; Adamović et al., 2011). The mentioned works give students the ability to explore several cryptographic algorithms, including symmetric algorithms, asymmetric algorithms, hash functions, and digital signatures. In McAndrew's research, open-source software was used to teach cryptography formally to 32 students at Victoria University in Australia. Focusing on the fundamentals of breaking and designing cryptosystems, the researcher reported that there appeared to be no reduction in student satisfaction or learning outcomes between those who used open-source software (Maxima or Axiom) and those who had used Maple. In formal questionnaires and informal discussions, all 32 students preferred using software with an unrestricted license and enjoyed the freedom to use it.

At Guangzhou University, Yi & Quan (2009) designed a cryptography-based software development course intended for senior students preparing for occupations in IT-related industries. The researchers used the open-source project OpenSSL to teach the students how to design and implement a cryptographic utility tool. Furthermore, the software enabled the students to learn about popular structural programming styles, as well as techniques for implementing cryptographic algorithms. The students were asked to extract specific codes from cryptographic routines and to incorporate them into an independently-designed cryptographic utility tool. The results indicated that the experience was largely positive for the students.

Adamović et al. (2011) taught a cryptography course using the open-source CrypTool software, the purpose of which was to expose students to all classical and modern cryptographic algorithms and protocols. As a free, open-source learning application, CrypTool is used worldwide in the analysis and implementation of cryptographic algorithms. The introduction of an interactive approach, based on CrypTool, was intended to fill the gap caused by the use of a textbook-theoretical approach to teach cryptography, and thereby to improve the students' learning outcomes. It was noted that the CrypTool software was effective at demonstrating the inner workings of cryptography algorithms in a user-friendly way, which was beneficial for students who lacked a strong mathematical background. For example, students simulated RSA key generation and encryption. Positive feedback received from students and comparative analyses of students' attendance (grades) confirmed the effectiveness of CrypTool and the advantages of the adopted approach compared to traditional teaching strategies.

Another study conducted by Tao et al. (2011) targets a specific cryptographic algorithm, namely, DESvisual. The researchers implemented a visualization tool for DESvisual that could help instructors to teach the building blocks of DES symmetric encryption algorithms, and also advance students' understanding. Their tool simulated the fundamental operations needed to perform the first DES permutation with an 8-bit or 16-bit input. Additionally, the tool improved students' abilities in terms of computing the output of each operation utilized by the tool and following through the encryption operation. By using the tool, students gained insights into the functions of primitive operations and investigated how they are composed in the DES algorithm.

Mathematical operations used within cryptography are also implemented and visualized for teaching cryptographic algorithms and protocols, with a case in point being ECvisual (Tao et al., 2012). The ECvisual visualization tool, which is compatible with Linux, macOS, and Windows, helps students to learn about ciphers based on elliptic curves, offering an opportunity to visualize elliptic curves over finite and real fields of prime order. The tool also assists students in mapping points to an elliptic curve, undertaking arithmetic operations, and facilitating decryption and encryption. ECvisual was developed to improve learning about the ElGamal encryption system, and it incorporates the following operation modes: demo and practice. ECvisual also contains a subsystem over the real field and another subsystem over a finite field of order. ECvisual was employed in an undergraduate cryptography introduction course with mixed results, where only 9 students felt that the tool was valuable for their learning.

Gaffer & Alghazzawi (2012) used a virtual security lab to teach cryptography and conduct hands-on information security laboratory exercises. Their lab was based on the Secure WEb dEvelopment Teaching (SWEET) project (SWEET, n.d.) and the Department of Defense Information Assurance Scholarship Project. Moreover, the SWEET project features six project modules, a virtualized platform for web development, and eight modules for teaching, enabling instructors to undertake practical laboratory exercises. Students were exposed to the use of MD5 and SHA-1 hash functions, as well as the concepts of digital signatures, symmetric-key ciphers, and public keys. Based on the results, it appears that most students benefitted from the virtual lab in terms of their learning outcomes.

Table 1. Comparing the proposed games for teaching cybersecurity against four important factors.

	Interactive demonstrations and visualization	Cryptographic algorithm development	Simulates various types of cryptographic protocols	Simplify mathematical notations and expressions
CounterMeasures game (Jordan et al., 2011)	Yes	No	No	No
CyberCIEGE video game (Irvine et al., 2005)	Yes	No	Yes	No
Interactive game hosted by social networking sites (Labuschagne et al., 2011)	Yes	No	No	No
CrypTool (CrypTool, 2019)	Yes	No	No	No
Cryptoy (GCHQ, 2014)	Yes	No	Yes	No
The US Air Force Academy project (Schweitzer & Baird, 2006)	Yes	No	Yes	No
Open-source software for teaching formal cryptography (McAndrew, 2008)	Yes	No	No	No
Cryptography-based software development (Yi & Quan, 2009)	Yes	No	Yes	No
Cryptography course using open-source CrypTool (Adamović et al., 2011)	Yes	No	No	No
DESvisual, a visualization tool (Tao et al., 2011)	Yes	No	No	No
Implementing mathematical operations in cryptography, for example, ECvisual (Tao et al., 2012)	Yes	No	No	Yes
Virtual security lab for cryptography teaching (Gaffer & Alghazzawi, 2012)	Yes	No	Yes	No

DISCUSSION

Even with all the efforts illustrated in Table 1 to improve and simplify the teaching of cryptography, there is still a lack of interactive demonstrations and visualizations that can be used to facilitate effective learning of cryptographic algorithms and protocols. Moreover, most of the proposed or used techniques do not simplify mathematical notations and expressions in a way that can help students to understand cryptographic algorithms and protocols. Thus, there is a need to devise interactive and novel methods for delivering learning content, including the use of visualization and animation, for widely used cryptographic algorithms and protocols, which appeal to various types of learners. Therefore, the author intends to develop a novel framework to enhance teaching and learning cryptographic protocols.

In terms of the research methodology used for the present study, electronic databases, including Scopus and Web of Science, were used to search for research articles addressing the topic of game-based learning for cybersecurity. Web of Science is a comprehensive repository of research articles from high-quality and reputable journals covering multiple subjects, including science education and educational technology. To use Web of Science, journals indexed in the Social Sciences Citation Index and the Science Citation Index Expanded were used to identify relevant articles. As for Scopus, this is the most sizeable abstract and citation database for peer-reviewed articles and high-quality web sources. To ensure that studies of satisfactory methodological quality were included in this research, articles were excluded if they were not published in reputable journals. Additionally, articles written in languages other than English were excluded from the literature search in order to avoid difficulties arising from translation.

The literature search strategy involved entering the same keywords on both Web of Science and Scopus. A collection of keywords related to the cybersecurity education was strung together using Boolean operators. After search hits were returned by the electronic databases, the researcher reviewed article titles and abstracts to find relevant articles that satisfied the following criteria: firstly, the researchers needed to have implemented a minimum of one digital game related to cybersecurity education; secondly, the digital game needed to have been evaluated by the researchers in terms of students' learning outcomes or process; and thirdly, the full-text version of the research article needed to be available, whether electronically or in hardcopy. If article titles and abstracts did not offer enough information to decide about eligibility for inclusion, the researcher analyzed each article's methodology and results to draw a conclusion.

A task that will be undertaken in the future as part of this research relates to the research methodology. In particular, it has been identified that a mixed methods research project, consisting of both quantitative and qualitative methods, will enable a comprehensive investigation to be undertaken into the use of gamification and animation in the teaching and learning of cybersecurity. Using the proposed framework, which is shown in Figure 1, final-year students in the IT department of two Arabic universities will be taught a cybersecurity course. A questionnaire and written assessment will be given to the students when the course has been finished, and the outcomes of these students will be compared to the outcomes of students from the previous three years. The researcher anticipates that challenges may be faced in terms of creating an engaging, entertaining, and effective game for teaching cybersecurity protocols.

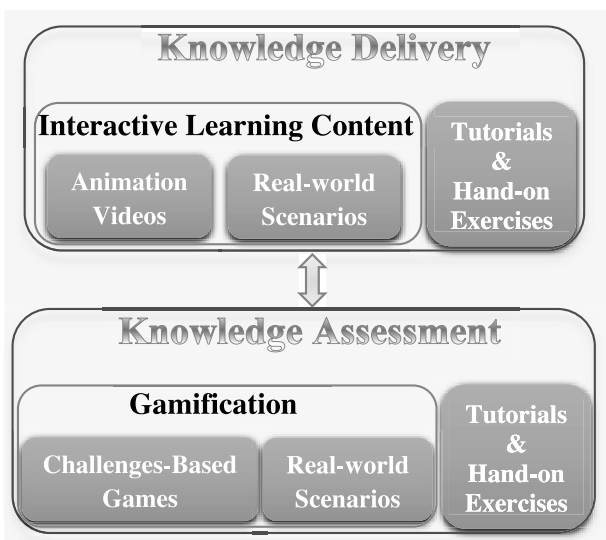

Figure 1. The proposed framework.

As illustrated in Figure 1, the proposed framework aims to leverage interactive approaches to the delivery of learning content (e.g., animation and visualization) relating to widely used cryptographic protocols. It will enhance students' knowledge by offering a more engaging, effective, and motivating way of learning compared to the presentation- and

video-based approaches that predominate in many higher education institutions. Furthermore, students who use the proposed framework will be exposed to various levels of explanatory detail (e.g., mathematical notation or flowcharts) to improve and complement their existing knowledge. The framework will use various strategies for assessing the knowledge delivered by the visualization and animation methods, including gamification. It could be used to deliver differentiated and informative games that are based on real-world issues, which is expected to increase the students' problem-solving abilities. In addition, gamification will be exploited as an aid to teaching by developing students' capabilities in terms of building and validating protocols, enabling them to gain greater insight into their weaknesses and how to address them. In addition, the framework will be implemented and applied in two Arabic universities, which are willing to enhance their ways of teaching cybersecurity in general and cryptography in particular.

CONCLUSION

Learners today receive education using various digital modalities, and various aspects of their lives, ranging from email to social communication, rely on the use of computers and other digital devices. Versatility is another key feature. Students advance in a continual way, whether at work or in lessons, and they tend to prefer learning in practical rather than theoretical ways. The use of portable games in education is associated with remarkable effects in terms of student engagement and learning outcomes. With these considerations in mind, a viable way to increase the effectiveness of existing teaching and learning practices is to integrate digital modalities, including PC games, into existing processes.

This research article focused on the teaching and learning of cryptography in higher education using game-based learning. Several game-based tools were identified that have enhanced students' understanding of cryptographic algorithms and protocols, including visualization tools, which can be exploited to translate mathematical notation and expressions into easily comprehensible and interactive diagrams. This research also presented a framework to simplify the teaching and learning of cryptographic protocols and to make them more straightforward to comprehend. The framework will use animated videos to deliver learning content relating to cryptographic protocols, and gamification will be used for assessment purposes.

In future research, the author will focus on implementing and evaluating the proposed framework. In particular, the author intends to investigate the effectiveness of animation and gamification in improving the learning outcomes of students in Arabic universities regarding their understanding of cryptographic protocols, as well as their ability to apply their knowledge.

REFERENCES

Adamović, S., Branović, I., Živković, D., Tomašević, V., & Milosavljević, M. (2011). Teaching interactive cryptography: the case for CrypTool. IEEE Conference, ICEST, 1(44006), 3-5. https://doi.org/10.13140/2.1.1065.0564

Adams, E., & Rollings, A. (2006). Fundamentals of Game Design. In Design. Prentice Hall. https://doi.org/10.1017/CBO9781107415324.004

Boghian, Ioana; Cojocariu, Venera-Mihaela; Popescu, Carmen Violeta; Mâţă, L. (2019). Game-based learning. Using board games in adult education. Journal of Educational Sciences & Psychology, **9**(1): 51-57.

Chang, R., & Yang, C. (2016). Developing a mobile app for game-based learning in middle school mathematics course. 2016 International Conference on Applied System Innovation (ICASI), 1-2. https://doi.org/10.1109/ICASI.2016.7539807

Chaudhry, S. (2019). Impact of Computer Based Educational Games on Cognitive Performance of SCHOOL CHILDREN IN LAHORE, PAKISTAN. The Shield-Research Journal of Physical Education & Sports Science, **51**(3): 9.

Chen, Z., & Chan, T. (2010). Using Game Quests to Incorporate Learning Tasks within a Virtual World. 2010 10th IEEE International Conference on Advanced Learning Technologies, 750-751. https://doi.org/10.1109/ICALT.2010.221

Corti, K. (2006). Games-based Learning; a serious business application. Informe de PixelLearning, 1-20.

CrypTool. (2019). https://www.cryptool.org/en/

de Castro, J.H.C.C., Divino, R.J.Z., Cambe, W.J., Lati, B.T., Fabito, B.S., & Jamis, M.N. (2019). ALGEbright: Design of an Avatar Customization Game-Based Learning for Algebra. 2019 IEEE Student Conference on Research and Development (SCOReD), 49-52. https://doi.org/10.1109/SCORED.2019.8896229

Derryberry, A., & Serious, I. (2007). Serious games : online games for learning. Serious Games, 9, 1–15. http://www.adobe.com/resources/elearning/pdfs/serious_games_wp.pdf

Dixit, R., Nirgude, M., & Yalagi, P. (2018). Gamification: An Instructional Strategy to Engage Learner. 2018 IEEE Tenth International Conference on Technology for Education (T4E), 138-141. https://doi.org/10.1109/T4E.2018.00037

Epishkina, A., Kogos, K., & Nikiforova, N. (2016). A course of Mathematical Logic and Theory of Algorithms as a mathematical background of modern cryptology. 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC), 200-204. https://doi.org/10.1109/DIPDMWC.2016.7529389

Gaffer, S.M., & Alghazzawi, D.M. (2012). Using Virtual Security Lab in Teaching Cryptography. International Journal of Modern Education and Computer Science, **4**(1): 26-32. https://doi.org/10.5815/ijmecs.2012.01.04

GCHQ. (2014). Cryptoy. https://play.google.com/store/apps/details?id=com.hmg.cryptoy/

Gumusgul, O. (2019). Investigation of University Students' Attitudes to Play Educational Games and Games Consisting of Physical Activity. World Journal of Education, **9**(2): 31. https://doi.org/10.5430/wje.v9n2p31

Hashim, H.A., Hamid, S.H.A., & Rozali, W.A.W. (2007). A Survey on Mobile Games Usage among the Institute of Higher Learning (IHL) Students in Malaysia. 2007 First IEEE International Symposium on Information Technologies and Applications in Education, 40-44. https://doi.org/10.1109/ISITAE.2007.4409233

Hsiao, I.Y.T., Yang, S.J.H., Chang, T., Wei, Y., & Lan, Y. (2016). Creating a 3D Game-Based Learning System in a Virtual World for Low-Achieving Students in Mathematics. 2016 IEEE 16th International Conference on Advanced Learning Technologies (ICALT), 518-519. https://doi.org/10.1109/ICALT.2016.37

Hu, X., Jiang, W., Ma, C., & Yu, C. (2018). Security and Design Analysis of Certificateless Signature Schemes as Teaching Cases of Cryptography and Security Course Education. 2018 9th International Conference on Information Technology in Medicine and Education (ITME), 601-605. https://doi.org/10.1109/ITME.2018.00138

Irvine, C., Thompson, M., & Allen, K. (2005). Active Learning with the CyberCIEGE Video Game. Federal Information Systems Security Educators' Association Conference, 1-10.

Jordan, C., Knapp, M., Mitchell, D., Claypool, M., & Fisler, K. (2011). CounterMeasures: A game for teaching computer security. Annual Workshop on Network and Systems Support for Games, 6. https://doi.org/10.1109/NetGames.2011.6080983

Kannappan, V.T., Fernando, O.N.N., Chattopadhyay, A., Tan, X., Hong, J.Y.J., Seah, H.S., & Lye, H.E. (2019). La Petite Fee Cosmo: Learning Data Structures Through Game-Based Learning. 2019 International Conference on Cyberworlds (CW), 207-210. https://doi.org/10.1109/CW.2019.00041

Labuschagne, W.A., Burke, I., Veerasamy, N., & Eloff, M.M. (2011). Design of cyber security awareness game utilizing a social media framework. 2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference. https://doi.org/10.1109/ISSA.2011.6027538

Li, K.H., Lou, S., Cheng, T., & Tsai, H. (2012). Application of Game-based Learning (GBL) on Chinese Language Learning in Elementary School. 2012 IEEE Fourth International Conference On Digital Game And Intelligent Toy Enhanced Learning, 226-230. https://doi.org/10.1109/DIGITEL.2012.61

Liu, J., & Cheng, Y. (2017). The Design and Simulation of Real-Time Encryption Algorithm for Mobile Terminal Voice Source. 2017 International Conference on Computer Systems, Electronics and Control (ICCSEC), 1016-1021. https://doi.org/10.1109/ICCSEC.2017.8446839

Liu, X. (2018). A Small Java Application for Learning Blockchain. 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 1271-1275. https://doi.org/10.1109/IEMCON.2018.8614961

Mayer, R.E. (2019). Computer Games in Education. Annual Review of Psychology, **70**(1): 531-549. https://doi.org/10.1146/annurev-psych-010418-102744

McAndrew, A. (2008). Teaching cryptography with open-source software. ACM SIGCSE Bulletin, **40**(1): 325. https://doi.org/10.1145/1352322.1352247

Michael, D.R., & Chen, S. (2006). Serious games [electronic resource] : games that educate, train, and inform (p. 287).

Parakh, A., Subramaniam, M., & Ostler, E. (2017). QuaSim: A virtual quantum cryptography educator. 2017 IEEE International Conference on Electro Information Technology (EIT), 600-605. https://doi.org/10.1109/EIT.2017.8053434

Putri, R.A.A.K., Moniaga, J.V, & Wijaya, Y. (2016). A design model for digital game-based learning in the study of international relations: Developing an innovative learning method for a defense strategy course at Bina Nusantara University. 2016 1st International Conference on Game, Game Art, and Gamification (ICGGAG), 1-6. https://doi.org/10.1109/ICGGAG.2016.8052636

Rahaman, S., Meng, N., & Yao, D. (2018). Tutorial: Principles and Practices of Secure Crypto Coding in Java. 2018 IEEE Cybersecurity Development (SecDev), 122-123. https://doi.org/10.1109/SecDev.2018.00024

Rao, A.R., & Dave, R. (2019). Developing hands-on laboratory exercises for teaching STEM students the internet-of-things, cloud computing and blockchain applications. 2019 IEEE Integrated STEM Education Conference (ISEC), 191-198. https://doi.org/10.1109/ISECon.2019.8882068

Rass, S., & Winkler, J. (2017). Learning pairing-based cryptography by hands-on exercises. 2017 IEEE 6th International Conference on Teaching, Assessment, and Learning for Engineering (TALE), 186-191. https://doi.org/10.1109/TALE.2017.8252329

Salib, E.H., & Hobar, G. (2018). Platform for Teaching Hands-on End-to-End Anonymity Algorithms. 2018 IEEE Frontiers in Education Conference (FIE), 1-9. https://doi.org/10.1109/FIE.2018.8658575

Schweitzer, D., & Baird, L. (2006). The design and use of interactive visualization applets for teaching ciphers. Proceedings of the 2006 IEEE Workshop on Information Assurance, 2006(June), 69-75. https://doi.org/10.1109/iaw.2006.1652079

Shiue, Y., Hsu, Y., & Liang, Y. (2017). Modeling the continuance usage intention of game-based learning in the context of collaborative learning. 2017 International Conference on Applied System Innovation (ICASI), 1106-1109. https://doi.org/10.1109/ICASI.2017.7988196

Simon Egenfeldt - Nielsen. (2006). Overview of research on the edducational use of video games. Digital Kompetanse, **1**(3): 184-213.

Susi, T., Johannesson, M., & Backlund, P. (2007). Serious Games - An Overview. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017, 1-24. https://doi.org/10.1109/UEMCON.2017.8249059

SWEET. (n.d.). http://csis.pace.edu/~lchen/sweet/.

Tao, J., Ma, J., & Keranen, M. (2012). ECvisual: a visualization tool for elliptic curve based ciphers. Proceedings of the 43rd ACM Technical Symposium on Computer Science Education, 571-576. https://doi.org/10.1145/2157136.2157298

Tao, J., Ma, J., Mayo, J., & Shene, C.K. (2011). DESvisual: A VISUALIZATION TOOL FOR THE DES CIPHER. Journal of Computing Sciences in Colleges, **27**(1): 81-89. https://doi.org/10.1145/2729094.2742589

Xu, J., Yuan, X., Yu, A., Jung Hee Kim, Taehee Kim, & Jinghua Zhang. (2016). Developing and evaluating a hands-on lab for teaching local area network vulnerabilities. 2016 IEEE Frontiers in Education Conference (FIE), 1-4. https://doi.org/10.1109/FIE.2016.7757364

Yi, T., & Quan, Z. (2009). Teaching cryptography-based software developing with open-source software. Proceedings of 2009 4th International Conference on Computer Science and Education, ICCSE 2009, 1604-1608. https://doi.org/10.1109/ICCSE.2009.5228308

Yurcik, W., & Doss, D. (2001). Different approaches in the teaching of information systems security. Proceedings of the Information Systems Education Conference.

Zhu, D., Zhang, D., He, B., Zhao, C., & Chen, X. (2019). Design and Implementation of an Experimental Teaching Scheme for the Development of SDN Northbound Applications. 2019 14th International Conference on Computer Science Education (ICCSE), 731-736. https://doi.org/10.1109/ICCSE.2019.8845443