GJEE Xtea

by Irfan Syamsuddin

Submission date: 30-Jun-2022 06:26AM (UTC-0700)
Submission ID: 1865010563
File name: cryptography_learning_module_GJEE_2018_-_G06-Syamsuddin-I-XX.pdf (183.94K)
Word count: 2228
Character count: 11706

Volume 20, Number 3, 2018

Global Journal of Engineering Education

Evaluation of NgeXTEA - a cryptography learning module

Irfan Syamsuddin

State Polytechnic of Ujung Pandang
Makassar, Indonesia

ABSTRACT: A new cryptography learning module, NgeXTEA, has been developed and applied to enhance teaching on the Information Security course. The module, NgeXTEA, is intended to deal with the lack of easy-to-understand teaching aids particularly for symmetric cryptography, which requires students to have extensive mathematical skills. The module was assessed by experts in terms of the validity of the learning module and the validity of the associated manual. In addition, the module was also measured in terms of ease of use from the student perspective. Overall, both evaluations show that NgeXTEA meets standard requirements as an appropriate learning module and it is found useful in enhancing students' understanding of symmetric cryptography.

Keywords: Extended tiny encryption algorithm (XTEA), symmetric cryptography, evaluation

INTRODUCTION

The Information Security course is offered in the sixth semester to students majoring in Computer and Network Engineering in the School of Electrical Engineering at the State Polytechnic of Ujung Pandang, Indonesia. One of the topics in the course is symmetric cryptography, where a lecturer introduces several cryptography algorithms that use the same key for both encryption and decryption.

There are several issues faced by the lecturer in teaching cryptography, such as the unavailability of appropriate tools to visualise how the algorithm works; in addition, there is the lack of mathematical ability of the students. This is in line with previous studies that highlighted three main problems in teaching cryptography at a higher educational institution, viz. limited class hours, low mathematical ability of the students and the lack of tools to help students obtain hands-on practice in cryptography [1][2].

To tackle this issue, a new learning module to assist in learning symmetric cryptography, called NgeXTEA, has been developed and used by students majoring in Computer and Network Engineering at the State Polytechnic of Ujung Pandang. NgeXTEA, which stands for Ngerti XTEA, is a learning module to enable the understanding of how an extended tiny encryption algorithm (XTEA) works. It also simulates the encryption and decryption processes based on XTEA in different modes. The development of NgeXTEA as a learning module is intended to address the complexity of teaching cryptography algorithms from the lecturer's perspective, as well as to help reduce the mathematical barriers to learning from the student's perspective [3]. It comes with an adequate graphical user interface (GUI) equipped with well-documented practical guidance, which makes it a self-explanatory learning guide for students.

NgeXTEA simulates XTEA, a relatively simple algorithm compared to other symmetric cryptography algorithms, such as the data encryption standard (DES) and the advanced encryption standard (AES). The XTEA algorithm [4] is derived from the tiny encryption algorithm (TEA) introduced by Wheeler and Needham [5]. The strength of XTEA lies in its lightweight size with few lines of code that makes it fast in operation [4]. It has a stronger encryption mechanism than other symmetric cryptography algorithms, as argued in several reviews [6][7].

Several approaches are seen in the literature regarding a pedagogic tool for symmetric cryptography. Chok, and Herath used a spreadsheet to explain a simple DES algorithm, with examples [8]. Another approach is where a computer

program is applied to calculate the result of the AES algorithm [9]. In other studies Java programming is applied to provide DES and AES algorithms, with several short examples [10]. However, such programming approaches are considered too complicated and difficult for students who require learning that is easy to follow and presented in an attractive way. To the best of the author's knowledge, NgeXTEA is the first learning module to support students with hands-on practice of symmetric cryptography using XTEA.

Reported in this article is the evaluation of NgeXTEA from the viewpoint of educational experts and students. While the experts assess NgeXTEA in terms of its validity for the learning module, the students evaluate the impact on their course of using NgeXTEA.

METHOD

The development of NgeXTEA followed the analysis, design, development, implementation, evaluation (ADDIE) model [11]. The five stage model of ADDIE offers a dynamic and flexible guideline by which to realise an effective development [12].

In the first stage, the developer conducted a requirements analysis provided by the lecturer and students. In this stage, a manual XTEA procedure was used, and linked with perceptions from both students and lecturer. This was followed by the design stage informed by the findings derived from the first stage. The development of the module was through PHP and JavaScript (see Figure 1). The implementation stage was conducted in class by the lecturer with the students. The last stage, evaluation, is the core of this study.

Figure 1: NgeXTEA learning module.

NgeXTEA resembles the manual process that was previously undertaken by students in class. The module is supported by practical guidelines within NgeXTEA. Both the learning module and guidelines for the use of NgeXTEA require comprehensive evaluation in order to ensure that NgeXTEA, as a new learning module, will enhance students' understanding of the topic.

The evaluation involved two types of user, viz. experts in higher education and students. The experts evaluated the validity of the learning module and the validity of the module guidelines [13]. Students were asked to evaluate the ease of use of the learning module [14].

RESULTS AND DISCUSSION

The first evaluation was to measure how valid NgeXTEA was as a learning module in terms of five validity criteria [13]. First, is the connection of the learning to the course topic, in this case, symmetric cryptography. Second, is the learning module educationally appropriate. Third, tool usability in terms of user interface design and interactivity. Fourth, practicability of the module. Finally, the learning module as a whole was evaluated.

Three experts were involved using values from 1 (represents worst) to 5 (represents best). The results of the validity survey are presented in Table 1 (see Figure 2).

Once the results from all experts were obtained for each validity criterion, the mean score of each criterion was calculated. The mean scores for the five criteria were 4.13, 4.43, 3.8, 4.27 and 3.7, respectively. These yield the validity score of 4.06 for the learning module.

Table 1: Validity of the NgeXTEA learning module.

No.	Validity criteria	E1	E2	E3	M
1	Connection with the topic	4.3	3.9	4.4	4.13
2	Educational aspects	4.5	4.5	4.5	4.43
3	Tool usability	3.6	3.8	4.0	3.8
4	Practicality of the module	4.0	4.2	4.6	4.27
5	Learning module value	3.4	3.8	3.9	3.7
				Validity score (VS)	4.06

Note: E - expert, M - mean score, VS - validity score ($\Sigma M/n$ - VS)

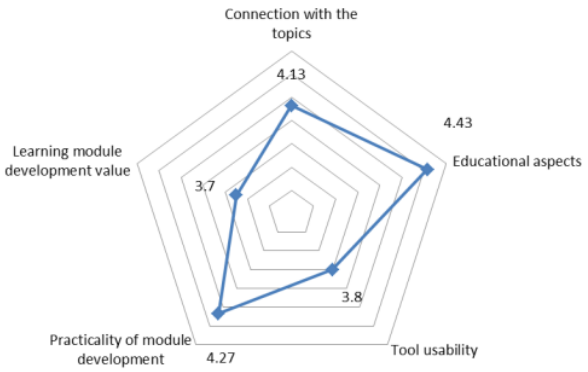

Figure 2: Validity of the NgeXTEA learning module.

The second evaluation was to measure how valid were the practical guidelines included within NgeXTEA. The same three experts determined four aspects of validity; namely, the content, language, layout and learning. Values from 1 (represents worst) to 5 (represents best) were chosen by the experts to represent their opinions on each aspect of validity. Table 2 shows the validity results for the NgeXTEA guidelines (please see Figure 3).

Table 2: Validity of the NgeXTEA guidelines.

No.	Aspects	E1	E2	E3	M
1	Content	4.2	4.1	4.4	4.233333
2	Language	4.2	4.2	4.1	4.166667
3	Layout	3.8	3.7	3.8	3.766667
4	Learning	4	4.5	4.3	4.266667
				Validity score (VS)	4.11

Note: E - expert, M - mean score, VS - validity score ($\Sigma M/n$ - VS)

The mean scores from the four criteria were 4.23, 4.16, 3.76 and 4.26, respectively. These yielded the validity score of 4.11 for the guidelines.

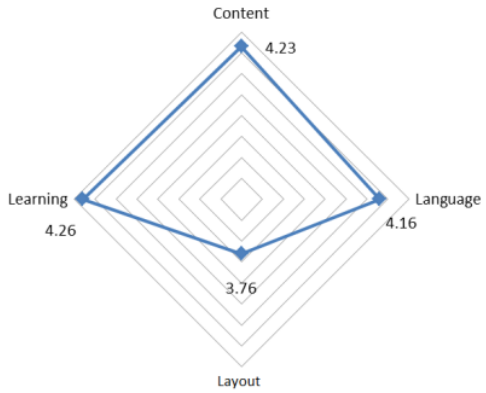

Figure 3: Validity of the NgeXTEA guidelines.

Results from the Experts' Assessments

Based on the experts' assessments through the first and second evaluations, several interesting findings emerged. Having a validity score of 4.06 for the NgeXTEA learning module indicates that the experts agree that it is an appropriate learning module to be used in supporting teaching.

In the second evaluation of the NgeXTEA guidelines, the experts also gave a positive result of 4.11 for validity. This means they agreed that the guidelines are clear and easy to understand. This is particularly true for the three criteria of *content, language and learning aspects,* with mean scores of more than 4.0, and *layout* a little lower at 3.76.

Overall, the experts agreed that NgeXTEA, as a new learning module, is valid to be applied to enhance the teaching of symmetric cryptography in the Information Security course.

Results from the Students' Assessments

The last evaluation was carried out to measure the student perceptions of using NgeXTEA. The survey consisted of five questions using a 1 to 5 Likert scale, viz. strongly disagree (SD), disagree (D), neutral (N), agree (A) and strongly agree (SA). The results of the student survey are presented in Table 3.

Table 3: Student survey of NgeXTEA.

No.	Survey question	SD	D	N	A	SA
1	NgeXTEA clearly explains how symmetric cryptography works	0	0	0	16	29
2	NgeXTEA shows encryption visualisation in stages and is easy to understand	0	0	1	12	32
3	Practical guidelines for NgeXTEA are similar to the manual book	0	0	0	22	23
4	NgeXTEA facilitates the laboratory practical process	0	0	2	10	33
5	NgeXTEA saves time in learning	0	1	4	10	30

The results show that most of the students gave a positive response to the NgeXTEA learning module. In detail, the results are, 100% of respondents stated agree (A) and strongly agree (SA) on the first and the third questions, while 97% of respondents stated A and SA on the second question. Approximately 95% of the respondents stated A and SA in the fourth question, and finally 88% of the respondents stated A and SA on the last question.

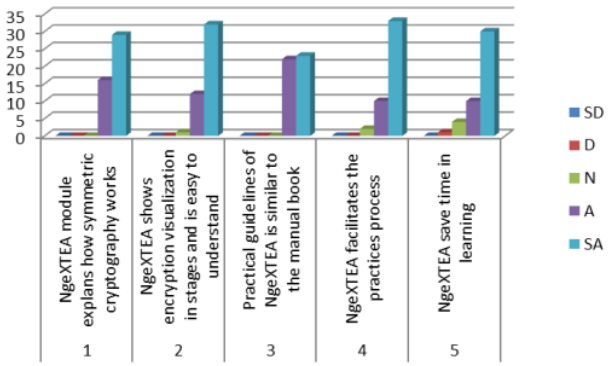

Figure 4: Student survey results.

Overall, it is clearly shown that most of the students felt significant benefits were obtained in their learning through the use of NgeXTEA. This is illustrated in Figure 4.

CONCLUSIONS

A new learning module, called NgeXTEA, has been developed and introduced to help students understand symmetric cryptography within the Information Security course. The study carried out is a description of the evaluation of the learning module from experts' and students' perspectives.

Two evaluations were made by the experts, i.e. the validity of the learning module and the validity of the guidelines. The validity of learning module was rated 4.06, and the validity of learning module guidelines was 4.11, both indicating high validity.

The final evaluation was made by the students in the form of a survey, which consisted of five questions. This indicated that the NgeXTEA learning module was useful in enhancing student knowledge in symmetric cryptography.

ACKNOWLEDGEMENTS

This study was financially supported by the Ministry of Research and Higher Education in Indonesia.

REFERENCES

1. Olejar, D. and Stanek, M., Some aspects of cryptology teaching. *Proc. WISE1-IFIP WG 11.8 1st World Conf. on Infor. Security Educ.,* Stockholm, Sweden, 1-9 (1999).
2. Song, X. and Deng, H., Taking flexible and diverse approaches to get undergraduate students interested in the importance of the using software tools for learning modern cryptography. *Proc. First Inter. Workshop on Educ. Technol. and Computer Science*, 490-494 (2009).
3. Adamovic, S., Sarac, M., Stamenkovic, D. and Radovanovic, D., The importance of the using software tools for learning modern cryptography. *Inter. J. of Engng. Educ.*, 34, **1**, 256-262 (2018).
4. Needham, R.M. and Wheeler, D.J., Tea Extensions. Report. Cambridge University (1997).
5. Wheeler, D.J. and Needham, R.M., TEA, a tiny encryption algorithm. *Inter. Workshop on Fast Software Encryption,* 363-366 (1994).
6. Ballal, V., Kumar, K., Meghan, V. and Rai, S.R., A study and comparison of lightweight cryptographic algorithm. *IJSR J. of Electronics and Communic. Engng.*, 12, **4**, 20-25 (2017).
7. Ebrahim, M., Khan, S. and Khalid, U., Symmetric algorithm survey: a comparative analysis. *Inter. J. of Computer Applications,* 61, **20**, 12-19 (2013).
8. Chok, O.S. and Herath, S., Computer security learning laboratory: implementation of des and AES algorithms using spreadsheets. *Proc. Midwest Instruction and Computing Symp.* (2004).
9. McAndrew, A., Teaching cryptography with open-source software. *Proc. ACM 39th SIGCSE Technical Symp.*, 325-329 (2008).
10. Schneier, B., *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. (2nd Edn), Wiley (1995).
11. Kali, Y. and Tamar, R.F., Teaching to design educational technologies. *Inter. J. of Learning Technol.,* 6, **1**, 4-23 (2011).
12. Allen, W.C., Overview and evolution of the ADDIE training system. *Advances in Developing Human Resources,* 8, **4**, 430-441 (2006).
13. Muharram, Adnan and Sudding, The development of an enzyme catalase kit for engineering students at technical-vocational schools. *Global J. of Engng. Educ.*, 19, **2**, 168-172 (2017).
14. Lin, Y-C, Chen, Y-C. and Yeh, R-C., Understanding college students' continuing intentions to use multimedia e-learning systems. *World Trans. on Engng. and Technol. Educ.*, 8, **4**, 488-493 (2010).

BIOGRAPHY

Dr Irfan Syamsuddin is a lecturer in the School of Electrical Engineering at the State Polytechnic of Ujung Pandang (PNUP), Makassar, Indonesia. His research areas are information technology, information security, e-learning, e-government and human computer interaction. He is the Head of the Centre for Applied ICT Research (CAIR) at PNUP in Indonesia.

GJEE Xtea

ORIGINALITY REPORT

16%	14%	11%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	accentsjournals.org Internet Source	2%
2	www.wiete.com.au Internet Source	2%
3	www.researchgate.net Internet Source	2%
4	lib.buet.ac.bd:8080 Internet Source	1%
5	www.springerprofessional.de Internet Source	1%
6	"Security in Computing and Communications", Springer Science and Business Media LLC, 2015 Publication	1%
7	Neeraj Chandnani, Chandrakant N. Khairnar. "Bio-Inspired Multilevel Security Protocol for Data Aggregation and Routing in IoT WSNs", Mobile Networks and Applications, 2022 Publication	1%

8	acet.ecs.baylor.edu Internet Source	1 %
9	Alaaeldin A. Aly. "Cryptography and security protocols course for undergraduate IT students", ACM SIGCSE Bulletin, 6/1/2004 Publication	1 %
10	ujcontent.uj.ac.za Internet Source	1 %
11	Boryczka, Urszula, and Kamil Dworak. "Genetic Transformation Techniques in Cryptanalysis", Lecture Notes in Computer Science, 2014. Publication	1 %
12	Submitted to University Tun Hussein Onn Malaysia Student Paper	1 %
13	Irfan Syamsuddin, Junseok Hwang. "The Application of AHP Model to Guide Decision Makers: A Case Study of E-banking Security", 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology, 2009 Publication	<1 %
14	www.mcgill.ca Internet Source	<1 %

15	C.E. Landwehr, D.M. Goldschlag. "Security issues in networks with Internet access", Proceedings of the IEEE, 1997 Publication	<1%
16	Janet Burge. "Exploiting Multiplicity to Teach Reliability and Maintainability in a Capstone Project", 20th Conference on Software Engineering Education & Training (CSEET'07), 2007 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		