Issues in Information Systems
Volume 16, Issue III, pp. 172-182, 2015

IMPOVING LEARNING OUTCOMES OF TEXTBOOK CONTENT WITH A SUPPLEMENTARY LEARNING MODULE: A CASE FOR BASIC CRYPTOLOGY

Wenli Wang, Robert Morris University, wangw@rmu.edu

ABSTRACT

The paper introduces a learning module for basic cryptology following the pedagogical recommendations for information systems security training [8], the meta-, intuition- and critical-thinking levels of teaching [6], and the "theory-algorithm-practice-application" model in cryptology education [5]. The module focuses on the fundamental concepts and logics in cryptology, supplementary to the applied techniques and tools often taught in textbooks. Data show that with the addition of the learning module students have better learning outcomes of both the relevant textbook content and the overall course. This result may extent to the education of other complex subjects.

Keywords: Cryptology, Security, IS Security Training, Case Study, CIS Curriculum, Learning Assessment

INTRODUCTION

No modern organization can survive without Information Systems (IS) security [8]; no modern IS security can be claimed strong without cryptology. Cryptology, or cryptography, is the process of encoding plaintexts into secret messages and vice versa. Cryptology is a foundational building block of secure digital communications—there is no safe digital communication that has not applied some form of cryptology. Understanding and mastering the fundamental concepts and logics as well as applied techniques and tools in cryptology are essential in implementing security by IS professionals and increasing security compliance from employees who need IS security training [8].

Modern cryptology is complex. Adamovic et al. [1] recognize that the main problem with learning cryptology is its complexity and its foundation on complex mathematical principles and formulae. Even without the deep theoretical understanding of the mathematical principles and formulae, the mere orchestration of integrated a/symmetric algorithms, uses of different keys, involvement of third-party certification, hashing, integrity checking, and the need for a proper sequence putting components together is already complex. Because of this complexity, rote memorization of cryptographic mechanisms would not last long and one-time exposure to only the textbook author's explanation may not be enough for a student to fully understand such a complexity. Therefore, iterations of the same concept but from different sets of instructions and the repeated reviews by different people—textbook author, instructor, and the students themselves—will help students with critical thinking and long-term knowledge retention.

Textbooks on IS security used in the undergraduate and graduate IS curricula do cover the topic of cryptology. However, most of them emphasize applied techniques and tools tailored to the professional certification programs such as CompTIA Security+ [3], but deemphasize the fundamental concepts and logics in cryptology. For instance, the textbook "Security+ Guide to Network Security Fundamentals" by Mark Ciampa [2] (5^{th} edition) used by most faculty in a private university for undergraduate/graduate IS security courses has two chapters—"Basic Cryptography" and "Advanced Cryptography"—but these chapters go into the details of applied techniques such as hashing without first introducing the fundamentals about why hashing is needed and what its role is in cryptography.

When a textbook chapter tries to cover many related topics in the certification programs, the breath of the content leaves insufficient rooms for the depth that explains the fundamentals. Therefore, additional learning modules are developed to establish the critical understanding of the basics to supplement the textbook content. This is important because only when critical thinking is applied can a student understand and evaluate for the long run the security level of an algorithm/protocol together with relevant key lengths verses just memorize it for a short period of time.

In addition, IS security protocols update at a fast pace, often accompanied with the changes in the *nerdy* technical names related to the "difficult and obscured" encryption algorithms. Even the technical professionals, who do not handle cryptology on a daily basis, may scratch their heads to recall the names of the algorithms. Rote memorization of the names and the security parameters affiliated with the names is not effective. Not to mention the difficulty of

discerning vender-specific products based on their myriad attributes if there is no real understanding of the qualities of these attributes. Products update frequently in the field of IS security. Rote memorization of products does not last long. Therefore, critical understanding of the foundational workings of cryptology, such as its logics and the long-lasting knowledge that is not changed with market products should be established to the students first before exposing them to the information often challenged with frequent updates.

The learning modules are supplementary to the relevant textbook content and can be integrated in any undergraduate or graduate IS security course. They provide the big picture first so that students can understand the fundamentals before the applied techniques. For instance, in contrast to how hashing is introduced mentioned above, in the learning modules hashing is not introduced until students understand the cons of computational inefficiency and the pros of strong authentication in asymmetric cryptology. Hence, students would truly understand and appreciate that hashing is an assistant step in generating strong but efficient authentication and is a solution to integrity as well.

There are two learning modules: "Cryptology I" explains the fundamentals of cryptology and is taught prior to "Basic Cryptology." "Cryptology II" demonstrates with real-world applications and is taught prior to "Advanced Cryptology." This sequence follows the "theory-algorithm-practice-application" model in cryptology education [5].

Table 1 demonstrates a sample syllabus for an eight-week course. It shows how the learning modules are integrated with the textbook content. Each learning module contains content for 1.5 contact hours in classroom and 0.5 contact hours outside classroom, same as those for a chapter's content. Each module has an assignment that is 4% of the final course grade, comparable to that of the end-of-chapter multiple choice question assignment that is 3% of the final course grade. Due to the size limitation of this paper, only "Cryptology I" is discussed.

Table 1. A Sample Course Syllabus Which Shows the Connection Between the Learning Module and the Textbook

Week	Content	Source	Assignment
1	Chapter 1: Introduction to Security Chapter 2: Malware and Social Engineering Attacks	Textbook	End of chapters multiple-choice questions (MCQs)
2	Chapter 3: Application and Networking-based Attacks Chapter 4: Host, Application, and Data Security	Textbook	End of chapters MCQs
3	Special Content: Cryptology I Chapter 5: Basic Cryptography	Learning module I Textbook	Special Assessment I End of chapter MCQs
4	Special Content: Cryptology II Chapter 6: Advanced Cryptology	Learning module II Textbook	Special Assessment II End of chapter MCQs
5	Chapter 7: Network Security Fundamentals Chapter 8: Administering a Secure Network	Textbook	End of chapters MCQs
6	Chapter 9: Wireless Network Security Chapter 10: Mobile Device Security	Textbook	End of chapters MCQs
7	Chapter 11: Access Control Fundamentals Chapter 12: Authentication and Account Management	Textbook	End of chapters MCQs
8	Chapter 13: Business Continuity Chapter 14: Risk Mitigation Chapter 15: Vulnerability Assessment	Textbook	End of chapters MCQs

The learning modules not only cover lecture content, assignments, answers, and assessment plans, but also the teaching tips on how to facilitate student learning of a seemingly difficult topic, how to make the learning fun, focused, and practical, and how to assess student learning outcomes in both theory and practice. Students are expected to be more motivated to learn, have more critical thinking, and have longer knowledge retention.

This research studies the literature guidance on security training in the design of "Cryptology I." It aims to answer the research question that "*whether or not adding a learning module on a complex subject to supplement textbook content is associated with better learning outcomes of the relevant textbook content and the overall course content*."

Section II reviews the literature on IS security training and cryptology education and discusses how "Cryptology I" is designed by following the literature guidance. Section III further presents "Cryptology I" and compares it with a relevant textbook chapter. Section IV shows the positive research results in learning outcomes. Section V concludes.

LITERATURE GUIDANCE OF THE LEARNING MODULE DESIGN

Researchers have explored various approaches to teaching cryptology. Often times, a specific practical and pedagogical tool like software [1, 9, 11, 12] or a video game such as CyberCIEGE is developed for security training and awareness [4]. Tools are helpful but using them is time-consuming and adds overhead and complexity. The total contact hours allocated to teach cryptology are often limited, which prevents the use of extensive software or gaming tools. Since only four contact hours are allocated for basic cryptography, rather than using software or video games, "Cryptology I" uses story-telling and role-playing in face-to-face instructor-to-student and student-to-student communications to mimic video game effects and to enhance effective interactive and collaborative learning, which has been shown to be effective [7, 12]. For the same reason, the effective "theory-algorithm-practice-application" model in cryptology education [5] is simplified to be "theory overview-algorithm-mental practice-application."

Karjalainen and Siponen [8] categorized 32 approaches to IS security training into 7 categories: psychological, process, computer-based, situational, security awareness program, social engineering prevention, and learning theory-based. "Crytology I" falls into the categories of process, situational, and learning theory-based.

Karjalainen and Siponen [8] further developed a meta-theory for IS security training based on Hare's theory [6] of three levels of thinking: meta-level, intuitive-level, and critical-level. The meta-level thinking recognizes the fundamental nature of IS security training to be persuasive and non-cognitive which requires more normative training than learning just about facts like in a typical textbook-based education [8]. "Cryptology I" applies story-telling and role-playing to be persuasive and non-cognitive to supplement fact-learning in textbook-based education. The intuitive-level thinking introduces the conventional practices, but the critical-level thinking questions the conventions and encourages novelty in needed situations [8]. "Cryptology I" also introduces facts and conventional IS security practices but after preparing students with why these facts are useful and important, and uses problems/solutions and questions/answers to intrigue students' critical thinking. Combinational teaching methods of instructor-led, problem-solving, critical reflections of individual and communal knowledge [8] are also applied. Combinational evaluation methods of observable performance through competence-based evaluation, adaptation of knowledge, conversational forms of evaluation of individuals and groups recommended in [10] are applied as well.

A LEARNING MODULE FOR BASIC CRYPTOLOGY

Learning Objectives

The learning objectives for "Cryptology I" and "Basic Cryptography" are listed and compared in Table 2. As stated in the textbook chapter [2], a more concise learning objective for "Basic Cryptography" is to "understand cryptography and how the encryption process can be used to protect data in term of hashing, basic a/symmetric cryptographic algorithms, file and file system cryptography." As shown in Table 2, some of the objectives in "Cryptology I" repeat those in "Basic Cryptography" and some supplement. All of these objectives are aligned with the course learning objectives, which are further in alignment with the ABET requirements. For instance, one of the BS-CIS and BS-IS program outcomes required by ABET is to cultivate students with "an ability to understand professional, ethical, legal, security and social issues and responsibilities." The learning objectives listed in Table 2 help build students' abilities to understand security and social issues and responsibilities in IS.

Table 2. Learning Objectives of the "Cryptology I" Learning Module and the "Basic Cryptography" Textbook Chapter

Learning Objectives of "Cryptology I"		**Learning Objectives of "Basic Cryptography"**	
1	Identify technical attributes of information security and explain how cryptography helps;	1	Define cryptography;
2	2.1 Understand how symmetric and asymmetric cryptograph works; 2.2 Discuss the pros and cons of symmetric and asymmetric cryptography;	2	Describe hash, symmetric, and asymmetric cryptographic algorithms;
3	Identify different roles of encryption key, message digest, and digital signature.	3	List the various ways in which cryptography is used;

Lecture Presentation

The lecture presentation content and the teaching sequences of "Cryptology I" and "Basic Cryptography" are listed in Table 3. Presentation slides have both text and graphics for easy understanding. The content of "Cryptology I" is concise and focuses on the fundamental concepts and logics behind cryptographic algorithms. The teaching sequence of "Cryptology I" aims to intrigue students' critical thinking through questions and answers. In comparison, the content of "Basic Cryptography" emphasizes diverse applied techniques and tools and provides a wider coverage of applications in cryptography. The teaching sequence of "Basic Cryptography" is topic-based rather than solution-based and does not intrigue critical thinking as much as in "Cryptology I." Both "Cryptology I" and "Basic Cryptography" are needed as they supplement each other. "Cryptology I" is taught prior to "Basic Cryptography" to build a strong foundation for critical thinking.

Table 3. Teaching Sequence and Content of "Cryptology I" and "Basic Cryptography"

"Cryptology I" Learning Module		**"Basic Cryptography" Textbook Chapter**	
Seq.	**Content**	**Seq.**	**Content**
1	learning objectives	1	learning objectives
2	five attributes of information security (*confidentiality*, *authentication*, *integrity*, *non-repudiation*, *availability*) and threats	2	definitions: cryptography, steganography history
	cryptography's role in protecting against threat and achieving desired attributes		cryptography provides five information protection
3	for *confidentiality*: encryption with symmetric cryptology	3	stream cipher, block cipher, sponge function
	disadvantages of symmetric cryptology: key management; authentication; non-repudiation	4	hashing cryptography: principle
4	asymmetric cryptology for easy key management (public key makes public)		HMAC (Hash+ symmetric cryptography)
	digital signature (for *authentication* and *non-repudiation*)		hashing provides *integrity*, e.g., file download integrity
	disadvantages of asymmetric cryptography: computationally expensive		algorithms: MD (Md2, Md4, Md5), SHA (Sha0,Sha1, Sha2, Sha3), Whirlpool, RIPEMD
5	message digest, introducing hashing to reduce computational expense	5	symmetric cryptography: principle, information protection
	hashing for i*ntegrity*		algorithms: DES, 3DES, AES, RC4, IDEA, Blowfish, Twofish, OTP
6	pros and cons of symmetric and asymmetric cryptology	6	asymmetric cryptography: principle, digital signature, practices, information protection
	comparisons of key length equivalence		algorithms: RSA, ECC, NTRUEncrypt, Quantum cryptography, DH, DHE, ECDH, perfect forward secrecy
7	combination of symmetric and asymmetric cryptology—preparing for introducing *https* in Cryptology II	7	encryption thru software, e.g., PGP, GPG, EFS, BitLocker; encryption thru hardware: USB, HDD, TPM (Trusted Platform Module), HSM

Teaching Tips

The five technical attributes of information security (*confidentiality, authentication, integrity, non-repudiation, and availability*) and how cryptology helps can be explained with the following story scenarios:

> Scenario One: If there are female students in the class, then the instructor will pick one female student as Princess (P), one male student as Poor Young Farm-boy (PYF), another male student as Rich Old Man (ROM), and the instructor plays the role of "Evil step-parent Queen or King" (EQ) who tries to break up the hidden relationship between P and PYF and fix her up with ROM by man-in-the-middle attack.
>
> Scenario Two: If there is no female student, the instructor will ask three male students to assume the roles as world leaders of communist/democratic countries. For instance, students may pick Castro (Cuban leader), Putin (Russian leader), and Obama (USA leader). The instructor plays the role of "FBI" who is the man-in-the-middle trying to break up the secret communication between Castro and Putin.

Many concepts in "Cryptology I" can be explained by playing different ways of communications in the above scenarios. Since Scenario Two is analogous to Scenario One, only Scenario One will be exemplified. For example, EQ may intercept the communication of setting up a secret date between P and PYF by modifying the message sent by P to PYF. Without encryption, EQ can do so and deliver the message to ROM instead. With encryption, EQ can no longer do so as the message will be in cipher-text. This is how "confidentiality" is achieved. Similarly, all the other four attributes can be explained.

Another example, to explain asymmetric cryptology, P, PYF and POM each generates a key pair. Then the students who assume these three roles will try out different keys to encrypt and decrypt messages. Students will be asked to choose the right key and use it in the right way when given the desired security attributes ought to be accomplished. In this way, through the story-telling and role-playing, the principles of a/symmetric cryptography are demonstrated. For instance, if P wants to deliver an encrypted message to PYF, then she should use PYF's public key. Through the trial and errors of using different keys, the students will be taught how asymmetric cryptography works and reach the conclusion that P should encrypt her secret message with PYF's public key rather than ROM's or EQ's public key, and her digital signature should be signed by her private key and then PYF decrypt with P's public key. EQ can be mischievous by mislabeling public keys with their true owners. This leads to the need of digital certification services, which will be taught in "Cryptology II."

It is important to provide sufficient theoretic and practical knowledge to the students without further complicating their learning. Since there are only 1.5 contact hours to cover the key knowledge points in "Cryptology I," there should be discretion over what knowledge points have to be explained thoroughly such as message digest and digital signature and what knowledge points can simply be touched upon such as the mathematical principles and formulae. Some levels of complexity can be avoided so that students do not get confused or lose interests. Retainable key knowledge is the focal point of effective teaching. The instructor needs to think how it is possible to leave strong impressions to the students of key knowledge points that students not only understand the knowledge with their true understanding and critical thinking but also retain the knowledge in the future.

For instance, the basic mathematics of Rivest-Shamir-Adleman (RSA) is demonstrated to the extent that students would know its theory, what public key/private key are, how these two keys are connected, and how a plaintext is encrypted to a cipher-text and vice versa. The instructor can go over the mathematics once in class but should not require the students to fully understand the details or to be tested upon the details. Students only need to know that RSA is based on the difficulty of prime factorization of a very large number, but do not need to know how to do prime factorization or modular arithmetic. It also depends on each class and the real-time feedback from the students. The instructor should observe students' facial expressions when reaching this topic and then decide how much depth the explanations should involve. In general, it is recommended not to delve into this topic for too long for undergraduate students but could be explored more for graduate students. See sample slides on RSA below:

- Choose two random large prime numbers: p, q and n=pq
- Randomly choose the encryption key **e** (i.e., encrypt), such that e and (p-1)(q-1) are relatively prime.
- Compute **d** (i.e., decrypt). where **ed** = 1 mod (p-1)(q-1)

- Public key: **e and n**; Private key: **d and n**;
- m–message/plaintext, c–ciphertext
- $c = m^e \bmod n$; $m = c^d \bmod n$
- $c^d=(m^e)^d=m^{ed}=m^{k(p-1)(q-1)+1}= mm^{k(p-1)(q-1)}= m*1(\text{mod } n) = m \text{ (mod } n)$

It is important to point out to the students that the security strength of a particular kind of cryptography depends on two aspects: algorithm and key length. Based on the current computation power, the requirement for key length may change. Students can easily have the misconception that asymmetric cryptography is better than symmetric cryptography, and a longer key length is better than shorter ones without first considering the key length is for which algorithm and the algorithm belongs to what kind of cryptography. By providing the strength comparison between symmetric and asymmetric cryptography, students' misconceptions can be reduced. Therefore, after explaining the above theory about RSA and showing how a RSA key looks like in a hexadecimal form, the following practical information is given to the students:

- Symmetric cryptography:
  - Strong security: 128 bits or longer; US government requires 192 or 256-bit AES key for high sensitive data.
  - For AES-128, there is no known attack which is faster than the 2^{128} complexity of exhaustive search. AES-192 and AES-256 breakable by attacks of 2^{176} and 2^{119}, faster than exhaustive search but non-practical and pose no real threat.
- Asymmetric cryptography:
  - Strong security: 1024 bits or longer;
  - RSA Laboratories recommends 1024 bits for corporate use, 2048 bits for extremely valuable keys like the root key pair used by a certifying authority;
  - 2048-bit keys sufficient until 2030. 3072-bit keys should be used if security is required beyond 2030.
- Compare in strength:
  - 1024-bit RSA keys = 80-bit AES; 2048 RSA =112 AES; 3072=128 AES, 15360 RSA=256 AES

Hashing, message digest, and digital signature are other key knowledge points. Figures are helpful visual tools to show the one-way function of a hashing algorithm, the size limitation of a message digest, digital signature as a message digest digitally signed with the sender's private key, a message sent together with its message digest created by the sender, and a second message digest regenerated by the receiver to verify integrity, etc.

After teaching "Cryptology I" in depth in 1.5 contact hours in the classroom, the content from the relevant textbook chapter (such as "Basic Cryptography") can be taught in the second remaining 1.5 contact hours. The textbook reiterates what a/symmetric cryptography and hashing are, etc., but in different ways of explaining and illustrating. The textbook chapter also covers in breath some applied techniques and tools, which are lacking in "Cryptology I."

In the next class meeting, before teaching "Cryptology II," students are asked to explain the key knowledge points learned in "Cryptology I." If there are students missing in "Cryptology I" class but show up in "Cryptology II," then students who were present in "Cryptology I" assume the role of the instructor and demonstrate their understandings with the story-telling and role-playing in either Scenario One or Two. Students are encouraged to avoid technical jargons and to pretend explaining cryptology to non-technical people. With the story-telling, role-playing, and the reinforcement of using non-tech plain languages, students' critical thinking and long-term knowledge retention are challenged the second time. The review helps ensure all students are on the same page with "Cryptology I" before moving onto "Cryptology II." The instructor helps reinforcing students' understanding by correcting their mistakes.

Assignment, Answer, and Learning Outcome Assessment Plan

The assignment (see Appendix A) assesses student learning according to the learning objectives. The answer and the learning outcome assessment plan, which shows how questions are graded are demonstrated in Appendix B.

LEARNING OUTCOMES AND RESEARCH RESULTS

Table 4 shows the data on learning outcomes of "Cryptology I," "Basic Cryptography," and the overall course from four semesters in 2013-2015 and from a total of sixty students. The average assignment grades in percentile demonstrate the learning outcomes of the learning module and the textbook chapter. The average exam grades only pertaining to the exam questions in "Basic-" and "Advanced cryptography" further demonstrate the learning outcomes on cryptology. The average midterm and final exam grades show the overall course performance. Data are from four semesters—one semester without the additional learning module and three semesters with the addition.

Examining on "Cryptology I" only, the learning outcomes of its assignment satisfy the ABET requirement of above 80%. In the Fall 2014 on-ground undergraduate course, the average assignment grade for "Cryptology I" was 84% (3.36 out of 4) with the highest grade of 3.8 and the lowest of 2.1. In the Spring 2015 on-ground graduate course, the average grade was 89% (3.56 out of 4) with the highest grade of 4 (3 students got the full marks) and the lowest of 2.5 (2 students). In the Summer 2015 online graduate course, the average grade was 86.5% (3.46 out of 4) with the highest grade of 4 (1 student) and the lowest of 2.7. The completion rates were all 100%.

Table 4. Student Learning Outcomes: Without vs. with the Supplementary Learning Module of "Cryptology I"

IS Security	**Without "Crypto I"**	**With "Cryptology I" Learning Module**						
Level	Undergraduate	Undergraduate		Graduate		Graduate		Average
Style	on-ground	on-ground with story-telling/role-playing		on-ground with story-telling/role-playing		online without story-telling/role-playing		
# of students	10	11		23		16		17
Term	spring 2013	fall 2014		spring 2015		summer 2015		—
Content	Basic Crypto	Crypto I	Basic Crypto	Crypto I	Basic Crypto	Crypto I	Basic Crypto	Basic Crypto
Completion rate	100%	100%	100%	100%	100%	100%	100%	100%
Average assignment grade	**85.5%**	84%	95%	89%	94%	86.5%	95%	**94.7%**
Average exam grade (Basic & Advanced Crypto chapters only)	N/A	89.7%		89.6%		90.8%		**90%**
Average midterm grade	**85.9%**	95.1%		92.3%		94.1%		**93.8%**
Average final grade	**84.0%**	95.8%		93.3%		97.4%		**95.5%**

Table 4 also shows that with the addition of "Cryptology I"—either on-ground with the instructor's explanations, story-telling and role-playing, or online self-studied by students—student learning outcomes of the relevant textbook chapter and the overall course (indicated in midterm and final exam average grades) were better than those in a session without the addition of "Cryptology I."

The average assignment grade for "Basic Cryptography" was only 85.5% without "Cryptology I" whereas the average grade for the same chapter assignment increased to 94.7% with "Cryptology I." One possible reason for the

differences maybe also due to the differences in incentives—in Spring 2013 students were only graded based on their submissions of the assignment rather than the quality of their submissions in 2014 and 2015. If the average chapter grade is not a good basis for comparison, the average midterm and final exam grades are because the exams were using the same format of multiple-choice questions and were similar in content. The average midterm grade in a session without "Cryptology I" was only 85.9% whereas the average of the averages of the three sessions with "Cryptology I" was 93.8%. The average final exam grade without "Cryptology I" was 84% whereas the average of the averages of the three sessions with "Cryptology I" was 95.5%.

The midterm and final exams included questions from all chapters other than just cryptography. For exam questions only related the two chapters of "Basic-" and "Advanced Cryptography," the average grade can be assumed to be 85% (average of midterm and final exam) for the session without "Cryptology I" (note: the individual student exam record is no longer accessible for the Spring 2013 semester) whereas the average of the averages of the three sessions was 90%.

The improvements in student learning outcomes in all the dimensions are not due to the different levels of graduate vs. undergraduate courses. Table 4 shows that the learning outcomes of the three sessions with added "Cryptology I" indicated in the average assignment grades of the relevant textbook chapter and of the exams are comparable regardless if a session is for undergraduate or graduate students. Comparing only between undergraduate sessions, the average grades were higher in the session with added "Cryptology I" than those without "Cryptology I."

Hence, the data show that adding the learning module of "Cryptology I" has improved the learning outcomes of textbook's chapter on "Basic Cryptography" as well as the overall course. The reason is due to the fact that cryptology is an essential building block for later content in the course such as network security, wireless security, authentication, etc. The textbook used in 2013 was the 4th edition, in which the two chapters on cryptography were later in the course in chapters 11 and 12. But the textbook used in 2014 and 2015 was the 5th edition, in which the author has moved the two chapters to chapters 5 and 6. The chapter content in the two editions remains almost the same. It cannot be ruled out that such a change in sequence actually helps strengthening students' learning in this fundamental building block and improving their course performance. Even though adding a supplementary learning module may not be the only reason for the improvements, it definitely has helped student learning as well.

The average assignment grades on "Cryptology I" show that graduate students have better critical thinking and a higher average grade (89%) than undergraduates (84%), given that the two sessions in comparison were both on-ground with story-telling/role-playing in class. The story-telling/role-playing helped with student learning outcomes of "Cryptology I" as the graduate on-ground with story-telling/role-playing has a higher average grade of 89% for this assignment than that of 86.5% in the graduate online session without story-telling/role-playing.

Students typically have difficulty in answering what keys to use to "Send an encrypted message + signature with AES" or to "Decrypt an encrypted message + signature with AES." The key knowledge point tested here is not stated explicitly on purpose. Students need to know AES is a symmetric algorithm; hence the key is a shared key. These two questions are to test students' recognition and proper categorization of cryptographic algorithms.

CONCLUSIONS

The learning module for basic cryptology is designed following the theories and pedagogy recommendations for IS security training [8] and other practical teaching methodologies in cryptology in the literature [5, 6, 7, 12]. The module encourages a teaching method that allows students to first focus on the fundamental concepts and logics before exposing them to various applied techniques and tools often taught in a relevant textbook chapter.

Data from four sessions of IS security courses with a total of sixty students show that adding the learning module of "Cryptology I" has not only improved the learning outcome of the relevant textbook chapter such as "Basic Cryptography" but also of the overall course. Since cryptology is such an essential building block for various areas in security such as network security, wireless security, authentication, etc., adding a supplementary learning module that is complete with its own objectives, presentation, assignment, assessment plan, and teaching tips, etc. has helped students to build a strong foundation in their learnings in security. For a complex topic such as cryptology, the additional efforts have led to the good result. This result may extent to the education of other complex subjects.

It has hoped that the training in students' critical thinking and conversational expression would have a long lasting effect on students' comprehension of the subject matter beyond satisfying the within-semester evaluation of their learning outcomes. Measuring such long-term effects requires longitudinal studies of students' understanding on the related topics, which could be a future research extension.

REFERENCES

1. Adamovic, S., Sarac, M., Veinovic, M., Milosavljevic, M., & Jevremovic, A. (2014). An interactive and collaborative approach to teaching cryptology. *Educational Technology & Society*, 17(1), 197–205.
2. Ciampa, M. (2015). *Security+ Guide to Network Security Fundamentals*.
3. CompTIA. (2015). CompTIA Security + certification designates knowledgeable professionals in the field of security. Available at: http://certification.comptia.org/getCertified/certifications/security.aspx
4. Cone, B., Irvine, C., Thompson, M . F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers and Security*, 26(1), 63–72.
5. Feng Y., Cheng Z., MengXiao Y., & YiRan H. (2009). Teaching cryptology course based on theory-algorithm-practice-application mode. *Proceeding of the First International Workshop on Education Technology and Computer Science*, Wuhan, China.
6. Hare, R. M. (1981). *Moral thinking: its levels, method, and point*. Oxford: Clarendon Press.
7. Jingtao L., Yiming Z., & Lei S. (2009). Interactive teaching methods in information security course. *Proceeding of the Eighth International Conference on Embedded Computing*, Dalian, China.
8. Karjalainen, M., & Siponen, M., (2011). Towards a new meta-theory of designing information systems (IS) security training approaches. *Journal of the Association of Information Systems*, 12(8), 518–555.
9. Matthaus W., Arno W., & Torben W. (2010). Towards peer-to-peer-based cryptanalysis. *Proceeding of the 35th Annual IEEE Conference on Local Computer Networks*, Denver, Colorado, USA.
10. Miller, J. (2007). *The holistic curriculum.* 2nd edition. Toronto: OISE Press.
11. Rachid A., Kevin P., & Georgios T. (2008). An animated cryptographic learning object. *Proceeding of the Fifth International Conference on Computer Graphics, Imaging and Visualization: Modern Techniques and Applications*, Penang, Malaysia.
12. Xiulli, S., & Hongyao, D. (2009). Taking flexible and diverse approaches to get undergraduate students interested in cryptography course. *Proceeding of the First International Workshop on Education Technology and Computer Science*, Wuhan, China.

APPENDIX A

"Cryptology I" Assignment

1. Please fill in the blanks below (*6pts, with each question 1pt*)

Action	**Use whose and what key**
Create a signature	Use _____'s_____ key to encrypt _____
Decrypt a signature to authenticate sender	Use _____'s _____key to decrypt _____
Send an encrypted message (such as a session key) with RSA	Use _____'s _____key
Decrypt an encrypted message (such as a session key) with RSA	Use _____'s _____key
Send an encrypted message+signature with AES	Use _____ key
Decrypt an encrypted message+signature with AES	Use _____ key

2. Please address the learning objectives (one to two paragraphs for each objective) (*4pts, each question 1pt*)

1) Identify technical attributes of information security and explain how cryptography helps.

2) Understand how symmetric and asymmetric cryptograph works.
3) Discuss the pros and cons of symmetric and asymmetric cryptography.
4) Identify different roles of encryption key, message digest, and digital signature.

APPENDIX B

"Cryptology I" Answer and Learning Outcome Assessment Plan

1. Please fill in the blanks below (*6pts, with each question 1pt*)

Action	**Use whose and what key**
Create a signature	Use __sender__'s _private__ key to encrypt _message digest__
Decrypt a signature to authenticate sender	Use __sender___'s _public___key to decrypt _digital signature_
Send an encrypted message (such as a session key) with RSA	Use _receiver___'s _public__ key
Decrypt an encrypted message (such as a session key) with RSA	Use _receiver___'s _private_ key
Send an encrypted message+signature with AES	Use _sender/receiver shared session_ key
Decrypt an encrypted message+signature with AES	Use _sender/receiver shared session__ key

2. Please address the learning objectives (one to two paragraphs for each objective) (*4pts, each question 1pt*)

1) Identify technical attributes of information security and explain how cryptography helps.
Technical attributes: Confidentiality (*0.1pt*), Authentication (*0.1pt*), Integrity (*0.1pt*), Non-repudiation (*0.1pt*), Availability (*0.1pt*)
How cryptography helps:
Confidentiality – encryption (*0.1pt*)
Authentication – digital signature/digital certificate (*0.1pt*)
Integrity – message digest (*0.1pt*)
Non-repudiation – digital signature (*0.1pt*)
Availability – authentication via encryption reduces denial of service attack (*0.1pt*)

2) Understand how symmetric and asymmetric cryptograph works.
Symmetric cryptography encrypts and decrypts a message with the same shared key. The sender encrypts, and the receiver decrypts. Before a secure session, the sender and the receiver need to share a symmetric key that is common to both the sender and the receiver. Key distribution is a challenge. (*0.5pt*)
Asymmetric cryptography uses a pair of keys – private and public keys. If a message is encrypted with a public key, then it will be decrypted with the matching private key. If a message is encrypted with a private key, then it will be decrypted with the matching public key. (*0.5pt*)

3) Discuss the pros and cons of symmetric and asymmetric cryptography.
Symmetric cryptography has cost-effective encryption/decryption. Asymmetric cryptography has relatively more computationally demanding encryption/decryption, hence not as cost effective as symmetric cryptography. (*0.5pt*)
Key management is problematic for symmetric cryptograph as the sender and receiver need to share the same symmetric key before a secure communication can take place. Key management in asymmetric cryptography

is easier. Each party keeps one's own private key secure, but publicizes one's public key. Public key distribution is managed by the Public Key Infrastructure (PKI), within which structure Certification Authority certifies the binding of an identity with the identity's public key, and hence facilitates the trust-worthy distribution of public keys. (*0.5pt*)

4) Identify different roles of encryption key, message digest, and digital signature.
   Encryption key – confidentiality (*0.33pt*)
   Message digest – integrity (*0.33pt*)
   Digital signature – authentication (*0.33pt)*