https://doi.org/10.48009/4_iis_2016_98-108

*Issues in Information Systems*
*Volume 17, Issue IV, pp. 98-108, 2016*

# A LEARNING MODULE FOR ADVANCED CRYPTOLOGY

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

## ABSTRACT

*This paper introduces a learning module for advanced cryptology subsequent to the learning module for basic cryptology (Wang, 2015). The module focuses on the concepts and logics in digital certificate and certificate authority. It is also designed following the pedagogical recommendations for information systems security training (Karjalainen & Siponen, 2011) and the meta-, intuition- and critical-thinking levels of teaching (Hare, 1981). However, it introduces the new "application-theory-algorithm-practice" model in cryptology education. It starts with real-world applications to catch students' attention and ends with practical assignments that assess students' independent and critical evaluations of security strengths of selected websites. Answers to the assignments evolve with the security updates in the industry. Students' performances from eight sessions in four years show that the "cryptology II" module helps improve students' learning outcomes in the subject of advanced cryptology and in the overall security course. Story-telling and role-playing also help students' critical thinking.*

**Keywords:** Cryptology, Security, IS Security Training, CIS Curriculum, Learning Assessment

## INTRODUCTION

Education of information system (IS) security is essential not only to the security professionals, but also to the common IS users. Cryptology, or cryptography, which encodes plaintexts to secret messages and vice versa, is a critical engine for modern IS security. But it is difficult to teach student cryptology due to its complexity and its frequent updates needed in the digital world.

Wang (2015) has stated that textbooks on IS security covering the topic of cryptology have their limitations in theory, practicality, and the cultivation of students' critical thinking. Most of the textbooks are tailored to the professional certification programs such as CompTIA Security+ (CompTIA, 2016) by covering a long lists of facts and de-emphasizing the learning processes of the students. Learning modules demonstrating both the teaching and learning processes of cryptology are lacking. There is a need for learning modules with teaching tips showing how to teach the subject matter in a fun, focused, and practical manner, how to facilitate students' learnings of such a complex topic, and how to assess students' learning outcomes from both theory and practice.

Wang (2015) introduced a learning module for basic cryptology for educating students the foundational concepts and logics of cryptology. This paper introduces a subsequent learning module "Cryptology II" for advanced cryptology. The module is also designed following the pedagogical recommendations for IS security training (Karjalainen & Siponen, 2011) and the meta-, intuition- and critical-thinking levels of teaching (Hare, 1981).

The "Cryptology II" learning module also has content for one and half (1.5) hour in-classroom contact and half (0.5) an hour outside-classroom study. It is supplementary to textbook coverage of related knowledge points in advanced cryptography and can be integrated in any undergraduate or graduate IS security course. For instance, the textbook "Security+ Guide to Network Security Fundamentals" (Ciampa, 2015) used for undergraduate and graduate IS students in a private university by most faculty has two chapters on cryptology–"Basic Cryptography" and "Advanced Cryptography." The "Cryptology I" learning module supplements "Basic Cryptography" in the fundamentals of algorithms and theories and will be taught prior to "Basic Cryptography." Similarly, "Cryptology II" supplements "Advanced Cryptography" and will be taught prior to the textbook chapter. The sequence of "Cryptology I" to "Cryptology II" follows the "theory-algorithm-practice-application" model in cryptology education (Yang et al., 2009). However, within the "Cryptology II" learning module itself, it introduces the new "application-theory-algorithm-practice" model to catch students' attention with real-world applications as "hooks" and to tailor the need of the subject matter (i.e., digital certificate and certificate authority). Some of the assignments

in "Cryptology II" assess students' critical evaluations of real-world applications of cryptology. By demonstrating and challenging students with real-world applications, students are expected to have more motivations and critical thinking, longer knowledge retention, and better learning outcomes.
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 has a special assessment designed to contribute to 4% of the final course grade, comparable to that (3%) the end-of-chapter multiple-choice questions assignment.

**Table 1.** A Sample Course Syllabus that Embeds the Learning Module "Cryptology II" within the Content of a Sample Textbook (Ciampa, 2015)

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

## LITERATURE REVIEW

The challenges of information system security education are due to the complexity and the need for knowledge updates in subject matters like cryptology. Adamovic et al. (2014) stated that one of the main problems with learning cryptology is its complexity and its foundation on complex mathematical principles and formulae. Even without requiring students to understand deeply the theoretical foundations of mathematical principles and formulae, the mere practical orchestration of integrated a/symmetric algorithms, integrated use of different keys/message digest/digital signature, and the involvement of third-party certification still challenges many students. Due to such complexity, rote memorization of cryptographic mechanisms would not last long. And one-time exposure to the textbook author's explanation only may not be enough for a student to really understand such complex knowledge (Wang, 2015). Therefore, iterations of the same concepts but from different sets of instructions will help; so will the repeated reviews of the same concept by different people—textbook author, instructor and the students themselves. It has been shown that the use of supplementary materials as additions to textbook content has improved students' learning outcomes in the study of basic cryptology (Wang, 2015).

In addition, IS security protocols and their parameters used to satisfy the market needs update at a fast pace, often accompanied with the changes in the technical names or terms. It is already difficulty for the security professionals to keep updated with these names and terms. Rote memorization of the names and the terms by either the security professionals or the common IS users is ineffective and does not last long. Not to mention the difficulty of window-shopping and selecting vender-specific products with the appropriate attributes to satisfy the present market needs. Therefore, critical understanding of the foundational workings of cryptology (Wang, 2015), such as its logic and non-changing knowledge should first be established before its variations in key length and other changing techniques are to be taught. And such critical understanding can be accomplished through the demonstrations of current industrial practices following the rules-of-the-thumbs. Only when critical thinking is applied, a student can

understand and evaluate, not just memorize for a short period of time, the security levels that an algorithm/protocol and its relevant security parameters can provide based on the present market needs.

Researchers have explored different approaches to teaching cryptology (Wang, 2015). Pedagogical tool like software or video game is sometimes developed (Adamovic et al., 2014; Cone et al., 2007; Matthaus et al., 2010; Rachid et al., 2008; Song & Deng, 2009). Software and video games are helpful, but it takes time to install them and train students how to use them. Depending on the total contact hours allocated to teach cryptology, adding such a pedagogical tool may add more complexity and time requirement (Wang, 2015). Because of the limited contact hours allocated in the classroom, even the effective model of "theory-algorithm-practice-application" model to teach cryptology (Yang el al., 2009) was simplified to "theory overview-algorithm-mental practice-real-world application" in teaching "Cryptology I" (Wang, 2015). Story-telling and role-playing in face-to-face instructor-to-student and student-to-student communications (Wang, 2015) are used for efficient interactive and collaborative learning (Li et al., 2009; Song & Deng, 2009). For "Cryptology II," the model of "application-theory-algorithm-practice" is introduced to catch students' attention with real-world applications as "hooks" and to tailor the need of the subject matter of digital certificate and certificate authority. Since students have already learned some theories and algorithms in basic cryptology, they have built the foundation to take on the challenge of real-world security applications with critical thinking. These applications help engage students in further inquiries to self-discover the need of trusted third parties who issue digital certificates to assist in the verification of digital signatures.

Karjalainen and Siponen (2011) summarized 32 approaches to IS security training in organizations and categorized them into seven major categories: psychological training approaches, process approaches, computer-based training approaches, situational approaches, security awareness program approaches, social engineering preventive approaches, and training approaches based on learning theories. Furthermore, a meta-theory was developed based on Hare's theory of three levels of thinking: meta-level, critical thinking-level, and intuitive-level thinking (Hare, 1981). The design principles of the "Cryptology II" learning module touches upon the meta- and intuitive-level thinking but focus mainly on the critical thinking-level. Teaching methods of problem-solving and critical reflections of individual and communal knowledge are applied (Miller, 2007). Evaluation involves observable performance and the adaptation of knowledge (Miller, 2007). The training approach of this learning module also takes the experiential learning pedagogy suggested for IS security training (Karjalainen & Siponen, 2011) with: 1) students' concrete experiences with online banking (most of them do); 2) their engaged reflective observation with evaluating security parameters of their own websites and comparing those with the examples given; 3) their formations of abstract concepts and generalization through answering general conceptual questions; and 4) their enabling of active experimentation with the active evaluation of the websites of their own choice.

## A LEARNING MODULE FOR ADVANCED CRYPTOLOGY

### Learning Objectives

**Table 2.** Learning Objectives of "Cryptology II" and "Advanced Cryptography"

| **Learning Objectives of "Cryptology II"** | | **Learning Objectives of "Advanced Cryptography"** | |
|---|---|---|---|
| 1 | Identify different roles of digital certificate and certification authority; | 1 | Define digital certificates; |
| | | 2 | List various types of digital certificates & how they are used; |
| | | 3 | Describe components of Public Key Infrastructure (PKI); |
| 2 | Discuss how combined a/symmetric cryptography takes advantages of both; | 4 | List tasks associated with key management; |
| 3 | Explain how SSL/TLS works; | 5 | Describe different transport encryption algorithms. |
| 4 | Apply the understanding of cryptography to assess website security strength. | | |

The learning objectives for the supplementary "Cryptology II" and the textbook chapter of "Advanced Cryptography" are listed and compared in Table 2 below. Some of the objectives in "Cryptology II" repeat those in "Advanced Cryptography" and others supplement. "Cryptology II" emphasizes the content and the learning process

leading to the application of assessing the real-world website security strength. Since "Cryptology II" is taught ahead of "Advanced Cryptography" as shown in Table 1, "Cryptology II" first provides the general information a security consumer needs to understand such as the necessity of a certificate authority and a public-key infrastructure, and then "Advanced Cryptology" introduces content that a security specialist needs to know such as the details of the different types of digital certificates and the architectural of the public-key infrastructure.

**Lecture Presentation**

The lecture presentation content and the teaching sequences of "Cryptology II" and "Advanced Cryptography" are listed in Table 3. The PowerPoint slides show the outlines and teaching materials, which can be followed in the general teaching manner. Both text and graphics are used for easy understanding in "Cryptology II." The content focuses on the essential concepts and theories behind the algorithms and is designed to fit with the background and capacity of undergraduate/graduate information systems students.

The content of "Cryptology II" is concise and focuses on the use of the real-world applications of digital certificate and certificate authorities in daily Internet activities to catch students' initial attentions to the topic. The fundamental concepts and logics behind cryptographic algorithms are explained in conjunction to the real-world applications. The teaching sequence of "Cryptology II" aims to intrigue students' critical thinking through relevant questions and answers to their daily activities. In comparison, the textbook content of "Advanced Cryptography" often starts directly with the theory and logic of cryptography and then with some screen shots of relevant Internet browser information. The teaching sequence of "Advanced Cryptography" is topic-based rather that solution-based and does not consider the psychological perceptions of the students or immediately intrigue students' critical thinking as "Cryptology II" does. Both "Cryptology II" and "Advanced Cryptography" are needed as they supplement each other. For instance, because "Advanced Cryptography" covers certain content such as trust models, "Cryptology II" omits the coverage on this topic.

After explaining "Cryptology II" in one and half (1.5) contact hours, the content and presentation from the related textbook chapter (such as the "Advanced Cryptography" chapter in the above mentioned textbook) can be taught in the remaining one and half (1.5) contact hour. "Cryptology II" is taught prior to "Advanced Cryptography" to build a strong foundation for students' critical thinking.

**Table 3.** Teaching Sequence and Content of "Cryptology II" and "Advanced Cryptography"

| **"Cryptology II" Learning Module** | | **"Advance Cryptography" Textbook Chapter** | |
|---|---|---|---|
| **Seq.** | **Content** | **Seq.** | **Content** |
| 1 | Explain learning objectives. | 1 | Learning objectives |
| 2 | Recapture knowledge learned in "Cryptology I." | 2 | Digital certificates definition and management, etc. |
| 3 | Raise the question of how to evaluate website security? Demonstrate multiple websites and the information related to the https padlock. | 3 | The roles of certificate authority, registration authority. The roles of certificate repository and certificate revocation list. |
| 4 | Demonstrate website certificate information and explain the fundamental concepts of digital certificate. | 4 | Types of digital certificates. |
| 5 | Demonstrate website certificate authority information including certification path and explain the fundamental concepts of certificate authority. | 5 | Public key infrastructure and public-key cryptographic standards. |
| 6 | Demonstrate website certificate detailed information and review again the concepts of message digest, digital signature, asymmetric and symmetric cryptography learned before but put them in the context of digital certificate. | 6 | Trust models of certificate authorities. |
| 7 | Discuss certificate and key management issues. | 7 | Public key infrastructure management and key management. |

| | | | |
|---|---|---|---|
| 8 | Explain why and how to combine a/symmetric cryptography to take advantages of both. | 8 | SSL/TLS. |
| 9 | Explain the operations of secure socket layer (SSL)/Transport layer security (TLS) protocols. | 9 | SSH, SCP, etc. |
| 10 | Explain other security protocols like SSH, PGP, etc. | 10 | HTTPS, SHTTP, etc. |
| 11 | Raise the awareness of security protection via cryptography vs. social engineering to bring the application of cryptography in the social context. | 11 | IPSec. |

**Teaching Tips**

In a similar manner, the story in "Cryptology I" can be extended to explain "Cryptology II", which focuses on how digital certificate and certificate authority work, how asymmetric and symmetric cryptography work complementarily, and how SSL/TLS/ and https work.

First of all, before going into "Cryptology II", students are asked to explain the knowledge points learned in "Cryptology I". If there were students missing in "Cryptology I" but showed up in "Cryptology II", then students who were presented in "Cryptology I" to assume the role of instructors and demonstrate their understandings with the story of either Scenario One or Two. Students are encouraged to avoid technical jargons and to pretend to explain to grandmothers how cryptology works. With the role playing and the reinforcement of using simple non-tech plain language, students' critical thinking is challenged the second time. With this review, it is ensured that all students now are on the same page with sufficient understanding of the knowledge points in "Cryptology I". The instructor will help in correcting the mistakes of the students and reinforcing their right understandings.

The stories in "Cryptology I" are discussed in details in (Wang, 2015). In sum, the following story scenarios were introduced to help demonstrate the technical attributes of information security and basic cryptology:

> 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 Boyfriend (PYB), another male student as Rich Old Man (ROM), and the instructor plays the role of "Evil Queen" or "Evil King" (E) who tries to break up the hidden relationship between P and PYB 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, student one may pick Castro (Cuban leader), student two may pick Putin (Russian leader), student three may pick Obama (USA leader), and 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. (Since Scenario Two is analogous to Scenario One, only Scenario One will be explained below.)

For instance, E wants to intercept the communication of setting up a secret date between P and PYB by modifying the message sent by P to PYB. Without encryption, E can do so and deliver the message to ROM instead. However, with encryption, E can no longer do so as the message will be in cipher-text. This is how "confidentiality" attribute is achieved. Similarly, all the other four attributes can be explained to the students in the context of Scenario One. Many concepts in "Cryptology I" can be explained by playing different ways of communications in Scenario One. Another example, to explain asymmetric cryptology, P, PYB and POM are each given a key pair. Then the students who assume these three roles will try out different keys to encrypt and decrypt messages, and 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 and role-playing, the principles of symmetric/asymmetric cryptography are demonstrated. For instance, if P wants to deliver an encrypted message to PYB, then she should use PYB'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 PYB's public key rather than ROM's public key, and her digital signature should be signed by her private key and then decrypted with her public key by PYB. E can be mischievous by mislabeling public keys with their true owners. This leads to the need of digital certification service, which is taught in "Cryptology II."

After qualitatively assessing students' learning outcomes in "Cryptology I" to be satisfactory, the instructor moves onto "Cryptology II." One student will take the role of a Certificate Authority (CA) who has a pair of keys different from those of other three students. Again, along the storyline, the bond between PYB and his public key is established by a CA so that ROM cannot claim PYB's public key. In this way, the function of a digital certificate and how a CA signs with the CA' digital signature onto an issued digital certificate would be explained.

Following the story of Scenario One or Two, students would be asked to tell a different story on their own, in a similar manner, and to play the roles of a web server of a bank and a web browser through which a bank client accessing to bank account information from the bank's web server. From this story, the instructor explains how Secure Socket Layer/Transport Layer Security (SSL/TLS) and https work. Before the story, the instructor actually has already clicked on the "https:" on a bank's webpage to show the content of SSL/TLS in a connection between a web browser and the certified web server of the bank to trigger the students' interests in truly understanding the students' role play in browser and server. Also through this story, students will learn that in the virtual world, an identity does not have to be a person but can be a virtual object such as a web server or a java applet.

**Assignment, Answer, and Learning Outcome Assessment Plan**

The assignment assesses student learning outcome according to the respective learning objective stated in the presentation of "Cryptology II" as well as assesses student's understanding of: how CA, SSL/TLS, https work and how to evaluate the security strengths of a/symmetric algorithms used in https. The content of the assignment can be seen in the Appendix. Note that there is an additional row in the table of Question #1 which asks a student to evaluate the security parameters of a website of his/her own choice. The grading of it can be flexible.

**Discussions**

The biggest difficulty for implementing the "application-theory-algorithm-practice" model is the need for frequent updates because both the application and practice in the field of security in the industry change quite often. As seen from the sample answers in the Appendix, the answers especially for those of Question #1 are linked to the real-world applications in the industry. Since the web servers' security parameters are often updated; these answers are in need of frequent updates as well. As a matter of fact, the answers have been updated four times during the period between Fall 2013 and Spring 2016 because many security parameters for various online businesses have been changed. This is a challenge for an instructor to assign homework to evaluate real-world industrial applications because the instructor needs to keep the answers updated almost on a semester basis. These changes are beneficial to students' learning as well. Students are provided with the answers not only for their current semesters but also from the previous semesters. In this way, students will learn the importance of always keeping updated in the field of security—they learn from the fact that the security parameters of real-world applications change more frequently than they have thought.

Another major difficulty for implementing the "application-theory-algorithm-practice" model is the need for working with diverse computing environment. The instructor needs to frequently review different web browsers' settings prior to a class meeting to ensure the smooth demonstrations in the classroom. Students who bring their own laptops to class are welcome to report the results from their computers. Students' home computing environment for doing their homework is quite diverse with various operating systems and/or browsers. Since some of the security parameters are the results of "handshaking" between a web browser and a web server, there may not be fixed answers that fit for all. Students are given additional "voice" to show how they reach their answers and in what computing environment in case they have shown the correct understanding of the theory, algorithms, and procedures to do the homework but their answers are somewhat deviated from the main standard answers.

A minor difficulty for implementing the "application-theory-algorithm-practice" model is the need for working with students' perceptions and assumptions. Since the examples used in Question #1 are mostly financial institutions, many students naturally chose to evaluate their own financial institutions such as their own banks. Evaluating a website "close to home" helps raise students' curiosities and promotes engaged reflective observation (Karjalainen & Siponen, 2011). However, students' attachment to their own "turfs" have caused them to give higher security ratings than they should have. Another common mistake from the students is that they fail to give Google a low

rating in its security just because Google is so popular and is an industrial leader in web presence. But the reality is that security rating of Google email should be low because it uses its own in-house certification services rather than uses a *trusted third* party. Many students do not get this knowledge point by themselves first time. Their mistakes encourage more critical thinking and leave stronger impressions for long-term knowledge retention. It also challenges the typical assumption of students that a large well-known technology company must have a high level of security. In addition, classroom discussions can be brought up to see whether or not certain applications like email need the highest level of security. Cost-benefit analysis provides students with an additional perspective.

## LEARNING OUTCOMES AND RESEARCH RESULTS

Table 4 shows the data on learning outcomes of "Cryptology II," "Advanced Cryptography," and the overall course from eight semesters in 2013-2016 and from a total of 124 students. The average assignment grades in percentile demonstrate the learning outcomes of the learning module and the textbook chapter. The average exam grades pertaining to the exam questions in "Basic-" and "Advanced cryptography" only further demonstrate the learning outcomes on cryptology. The average midterm and final exam grades show the overall course performance. Among the eight semesters, six semester are with the additional learning module and two semesters are without.

Examining on "Cryptology II" only, the learning outcomes of its assignment satisfy the ABET requirement of above or equal to 80%. In the Fall 2014 and Fall 2015 on-ground undergraduate courses, the average assignment grade for "Cryptology II" was 83.6% (3.34 out of 4) with the highest grade of 3.9 and the lowest of 2.3. In the Spring 2015 and Fall 2015 on-ground graduate courses, the average grade was 82.4% (3.3 out of 4) with the highest grade of 3.9 (two students with one in each class) and the lowest of 2.15. In the Summer 2015 and Spring 2016 online graduate courses, the average grade was 80% (3.2 out of 4) with the highest grade of 4 (1 student) and the lowest of 1.0. The completion rates for cryptology II were on average 98.8%.

Table 4 also shows that student learning outcomes of the relevant textbook chapter and the overall course (indicated in midterm and final exam average grades), with the addition of "Cryptology II" either on-ground with the instructor's explanations, story-telling and role-playing, or online self-studied by students, were better than those in two sessions without the addition of "Cryptology II." The average assignment grade for "Advanced Cryptography" was 92% without "Cryptology II" whereas the average grade for the same chapter assignment increased to 94.7% with the supplementary "Cryptology II." If the average chapter grade may not be significantly different for the comparison purpose, 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 sessions without "Cryptology II" was only 89.4% whereas the average of the averages of the six sessions with "Cryptology II" was 93.4%. The average final exam grade without "Cryptology II" was 88.6% whereas the average of the averages of the six sessions with "Cryptology II" was 94.1%.

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 was not available and can possibly be assumed to be 89% (the average of average midterm and final exam grades) for the sessions without "Cryptology II" (note: the individual student exam record is no longer accessible for the Spring 2013 semester) whereas the average exam grade for these two chapters of the averages of the six sessions with "Cryptology II" was 91.2%, higher than that without "Cryptology II."

Surprisingly, with "Cryptology II," the student learning outcomes at the undergraduate level in almost all dimensions (Crypto II assignment grade and average exam grades except for chapter assignment grade for textbook "advanced cryptography") are better than those at the graduate level consistently. However, without "Cryptology II," the student learning outcomes at the undergraduate level (only the average midterm and final exam grades are available for comparison) are lower than those at the graduate level. Comparing only between undergraduate sessions, the average midterm and final exam grades were much higher in the sessions with added "Cryptology II" than those without "Cryptology II." These results indicate that undergraduate students can improve their learning outcomes with the story-telling and role-playing.

But such a positive effect of story-telling and role-playing on the learning outcomes does not show strongly at the graduate level although the average assignment grade for "Cryptology II" is higher for on-ground graduate students than online graduate students. Even though graduate students already have strong critical and logical thinking capabilities, additional guidance facilitating more abstract and critical thinking would still help. However, the average exam grades for on-ground graduate students are quite lower than those of online graduate students. This may due to the reason that graduate students taking online courses could be just better students than those taking on-ground courses. It is possible that online graduate students could have more technical background and working experiences. Graduate students taking on-ground courses could be students directly from undergraduate programs and do not have much working experiences in the field. Nevertheless, if comparing online graduate students with and without the added "Cryptology II," online graduate students with "Cryptology II" have better average midterm and final exam grades (e.g., 94.9% and 97%) than those without "Cryptology II" (e.g., 92.8% and 93.1%).

In summary, for the overall the undergraduate/graduate and on-ground/online students, the data in Table 4 show that adding the learning module of "Cryptology II" has improved the learning outcomes of textbook's chapter on "Advanced Cryptography" as well as the overall course. As having explained in (Wang, 2015), 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.

**Table 4**. Student Learning Outcomes: Without vs. With the Supplementary Learning Module of "Cryptology II"

| **IS Security** | **Without "Crypto II"** | | | **With "Cryptology II" Learning Module** | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Level | **under-grad** | **grad** | **Ave.** | **undergraduate** | | **graduate** | | | | **Ave.** |
| Style | on-ground | online | | on-ground with story-telling/role-playing | | on-ground with story-telling/role-playing | | online without story-telling/role-playing | | |
| # students | 10 | 13 | 12.5 | 20 | | 49 | | 32 | | 16.8 |
| Term | spring 2013 | summer 2014 | — | fall 2014 & fall 2015 | | spring & fall 2015 | | summer 2015 & spring 2016 | | — |
| Content | Adv. Crypto | N/A | Adv. Crypto | Crypto II | Adv. Crypto | Crypto II | Adv. Crypto | Crypto II | Adv. Crypto | Adv. Crypto |
| Completion rate | 100% | N/A | **100%** | 95% | 100% | 98% | 100% | 100% | 100% | **98.8%** |
| Average assignment grade | 92% | N/A | **92%** | 83.6% | 89.5% | 82.4% | 97.5% | 80% | 97.1% | **94.7%** |
| Ave. exam grade (Basic & Adv. Crypto) | N/A | N/A | **N/A** | 92.7% | | 87.5% | | 93.3% | | **91.2%** |
| Ave. midterm grade | 85.9% | 92.8% | **89.4%** | 97.1% | | 88.3% | | 94.9% | | **93.4%** |
| Average final grade | 84.0% | 93.1% | **88.6%** | 95.4% | | 89.9% | | 97% | | **94.1%** |

## CONCLUSIONS

The learning module for advanced cryptology is designed following the theories and pedagogy recommendations for IS security training (Karjalainen & Siponen, 2011) and other practical teaching methodologies in cryptology in the literature (Yang et al., 2009; Li et al., 2009; Song & Deng, 2009). The module introduces the new "application-theory-algorithm-practice" model in cryptology education and encourages students to first focus on the practical inquiries pertaining to their daily Internet needs before their exposures to various applied techniques and tools such as digital certificate and certificate authority. The learning outcome assessment is practical and personal, as well as abstract and conceptual. Moreover, the answers to the practical investigation evolve with the security updates of the real-world applications—the update itself teaches students one fundamental trait of the information security field: it requires change frequently. Students' performances from eight sessions in four years show that the added "cryptology II" module helps improve students' learning outcomes in the subject of advanced cryptology and the overall security course. Story-telling and role-playing also help students to understand advanced cryptology concepts. It has hoped that the training in students' hands-on investigation, critical thinking, and conversational expression of difficult technical and practical knowledge would have a long lasting effect on students' comprehension of the subject matter beyond simply satisfying the within-semester evaluation of their learning outcomes. Future research work needs to empirically study such long-term effects.

## REFERENCES

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.

Ciampa, M. (2015). *Security+ Guide to Network Security Fundamentals*, 5th edition, Course Technology.

CompTIA. (2016). CompTIA Security + certification designates knowledgeable professionals in the field of security. Retrieved on May 15th, 2016 at: http://certification.comptia.org/getCertified/certifications/security.aspx

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.

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.

Li, J. T., Zhao, Y. M., & Shi, L. (2009). Interactive teaching methods in information security course. *Proceeding of the Eighth International Conference on Embedded Computing*, Dalian, China.

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.

Miller, J. (2007). *The holistic curriculum*. 2nd edition. Toronto: OISE Press.

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.

Song, X. L. & Deng, H. Y. (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.

Wang, W. (2015). Improving Learning Outcomes of Textbook Content with a Supplementary Learning Module: A Case for Basic Cryptology. *Issues of Information Systems*, 16(3), 172-182.

Yang, F., Zhong, C., Yin, M. X., & Huang, Y. R. (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.

## APPENDIX
## SAMPLE "CRYPTOLOGY II" ANSWERS AND LEARNING OUTCOME ASSESSMENT PLANS

Note that the answers to Question #1 evolved together with the security updates of the real-world applications. The following answers are for Fall 2013 semester only.

1. Please fill in the blanks below (6pts, with each column 1pt, evaluation of self-chosen website 1pt)

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

| **Web Servers** | **CA Name/ Class** | **Asymmetric Algorithm/ Key length** | **Symmetric Algorithm/ Key length** | **Hash Algorithm** | **Your Rating of Security (1-5)** |
|---|---|---|---|---|---|
| **Fidelity** | COMODO CA 2 | RSA 2048bits | TLS1.0, RC4_128bits | Sha1 | 4 |
| **Scottrade** | VeriSign Class 3 | RSA 2048bits | TLS1.2, RC4_128bits | Sha1 | 4.5 |
| **PNC** | VeriSign Class 3 | RSA 2048bits | TLS1.0, AES_128bits | Sha1 | 4 |
| **Chase** | VeriSign Class 3 | RSA 2048bits | TLS1.0, RC4_128bits | Sha1 | 4 |
| **Gmail** | Google Internet Authority G2 | ECDH 256bits | TLS1.2 AES_128_GCM | Sha1 | 2 |
| **Yahoo! Mail** | None | None | None | None | 1 |
| **Website of your choice** | | | | | |

1) Identify different roles of digital certificate and certification authority.
   Digital certificate certifies the binding between a digital identity and its public key. Digital certificate is issued by a certificate authority and is digital signed by the certificate authority. (*0.5pt*)
   Certificate authority is a trusted third party issuing digital certificates. (*0.5pt*)
2) Discuss how combined a/symmetric cryptography takes advantages of both cryptography.
   Asymmetric cryptography can be first used to authenticate the two communication parties and securely exchange a symmetric key between the two parties. (*0.5pt*)

Once both parties have the same symmetric key, their communications can be secured by encrypting the messages with the shared symmetric key. Once the communication ends, both parties no longer need the shared symmetric key. (*0.5pt*)

3) Explain how SSL/TLS works.
   SSL refers to Secure Sockets Layer, which is the predecessor of TLS – Transport Layer Security. (*0.2pt*)
   In a web communication session, both web server and client browser first negotiate security parameters, such as common algorithms for key exchange, symmetric cryptography, hash, digital signature, etc. and their corresponding key lengths. (*0.2pt*)
   Webserver authenticates itself through digital certificate and digital signature of the server. Browser may authenticate itself, but mostly optional. (*0.2pt*)
   Browser selects a single key for the session. Securely deliver the session key to the webserver by encrypting it in using webserver's public key, obtained from the digital certificate issued by a certificate authority but sent by web server. Session key established. (*0.2pt*)
   Encrypt all transmissions during the session with this session key until the web session ends. (*0.2pt*)
4) Apply the understanding of cryptography to assess website security strength.
   If https rather than http is the protocol used in a web session, that implies the application of cryptography is the web session. Click on lock icon in https. Click on "Connection," it shows which version of SSL/TLS is applied and what the algorithm is for session key encryption and its key length, as well as what the algorithm is for session key exchange. (*0.5pt*)
   Further click on "certificate information", it shows the certificate authority issuing the certificate and which level of certificate it is, as well as the key parameters in secured connection, such as hash algorithm, digital signature algorithm, asymmetric cryptography algorithm and key length, etc. (*0.5pt*)