Two Models of a Cryptography and Computer Security Class in a Liberal Arts Context

Suzanne Fox Buchele
Southwestern University
1001 East University Avenue
Georgetown, TX 78626
bucheles@southwestern.edu

ABSTRACT
The critical need for computer security concepts to be taught in the undergraduate computer science curriculum is evident from current news stories, curricular guidelines, and government initiatives. Beginning to teach a standalone computer security course can be daunting, especially for instructors with little or no background or formal education in computer security. An elective course in cryptography and computer security was developed that matched the talents of the professor and the resources and context of the two Universities and departments in which it was taught. Two models of the course evolved: an elective semester-long computer science and mathematics cross-listed course, and an elective summer computer science course with significant hands-on laboratory exercises. Either course may be used as a model for an accessible course offering involving computer security.

Categories and Subject Descriptors
K.3.2 [**Computer and Information Science Education**]: Computer Science Education.

General Terms
Experimentation, Security.

Keywords
Computer Security Education; Computer Security; Cryptography; Cryptology.

1. INTRODUCTION
There is no doubt that computer security is a requisite component of the education of modern computer scientists. Every day news stories are populated with reports of computer hacking, security breaches, malware, espionage, and/or legislative proposals related to computer, network, or information security. Several U.S. government initiatives are aimed at strengthening the security education of students [9, 17], and several NSF-funded projects have developed resources for teaching security for instructors [2, 5, 18]. In addition, the most recent computer science curriculum guideline proposal features Information Assurance and Security as a Knowledge Area that all students should cover [6]. In the introduction to the CS2013: Ironman Draft (the most recent draft of the computer science curricula available), the authors state, "When questioned about new topical areas that should be added to the Body of Knowledge, survey respondents indicated a strong need to add the topics of *Security* as well as *Parallel and Distributed Computing*" [6]. However, faculty in departments that have not to date offered a computer, network, or information security course may be concerned about the time and resources that implementing such a course would involve, especially in light of time and budget constraints, and lab configurations.

Two models of an elective course in Cryptography and Computer Security that were developed and offered at two different Universities on two different continents are presented here: one, an upper level course cross-listed as a computer science and mathematics elective at a small liberal arts college in the U.S., and the second, an upper-level computer science elective course with a combined lecture and laboratory approach at a new University with a liberal arts focus in West Africa. History, content, and outcomes of the courses follow, as well as a mapping of course topics to CS2013 Ironman Draft Knowledge Areas.

2. HISTORY OF THE COURSE DEVELOPMENT

2.1 Motivation and First Steps
The importance of computer security in modern society and the computer science industry has become more and more evident. For example, computer, network, or information security is a frequently occurring subject in the tri-weekly ACM TechNews digest [1]. However, having no formal experience with computer or information security, no support for new course development, a full curriculum, a set of "standard" electives, and a full teaching schedule meant little incentive for the author to develop a security course.

Student interest in the area led the author to oversee two independent studies involving computer security. Because studying and teaching mathematical concepts can be more straightforward than dealing with differing software and hardware configurations, topics tended toward cryptography and the knowledge-based computer security topics. However, students were also interested in doing hands-on activities that were relevant to the knowledge they were acquiring. The author was reminded of a 2006 paper presentation by Ed Crowley, and Crowley was generous enough to share many of his other resources including several full laboratory exercises using Live DVDs with a Linux distribution and several network utility tools

SIGCSE'13, March 6–9, 2013, Denver, Colorado, USA.

[3]. In addition, course content and objectives were developed and assignments were created during the independent studies, paving the way for a future course offering.

During the first independent study, the author offered to teach a summer course in Cryptography and Computer Security at Ashesi University College, a new University in Ghana, West Africa with a liberal arts focus. The department at Ashesi has a more technical and engineering focus than is typical of a liberal arts computer science department in the U.S., with an expectation of scheduled lab time in CS classes. In addition, a summer course necessitates longer contiguous contact times than a semester-long course, so a lecture-mostly format would not be suitable. Therefore, for the first formal course, a summer course offered in May-June 2010 at Ashesi University College in Ghana, the number of labs was significantly expanded. The course was offered to rising sophomores through seniors as a computer science elective, although several recent alumni working in industry also audited the course.

2.2 Two Models Emerged

In spring of 2012 a version of the course was taught at Southwestern University as an upper-level, cross-listed computer science and mathematics special topics elective. Course topics more appropriate to the mathematics majors were expanded. In addition, course topics necessitating significant computer science expertise were minimized, and explanatory material for the needed concepts was added. For several topics and assignments, differentiated learning and assignments were adopted: for mathematics majors, deep understanding of the proof and mathematical concepts behind certain algorithms was expected, and for computer science majors, the ability to implement certain algorithms was expected. An individual research, applied research, or implementation project was also added, which allowed students to select topics suited to their interest and abilities.

In the summer of 2012, an expanded version of the course was re-taught at Ashesi University College in Ghana. The course was a pilot study abroad program, with one student from Southwestern University accompanying the author to study abroad with 15 West African students for the 5 ½ week summer course. Although similar in content and structure to the initial offering in summer 2010, new material pulled from the Spring 2012 course (e.g. elliptic curve cryptography) was added, although adapted for the more applied computer science context. More labs were also added, so that most content presented now had an associated lab activity.

3. CONTENT AND STRUCTURE OF THE TWO MODELS

3.1 Prerequisites

The mathematics cross-listed course at Southwestern University required sophomore standing, CS1 (which is required of all mathematics majors), and either two mathematics courses or Computer Organization and one mathematics course. This ensured that mathematics majors had already had at least CS1, and the computer science majors had already had topics in data representation and digital logic, and some mathematical maturity; typical sophomore computer science majors had already taken either or both of Statistics or Calculus 1, although junior and senior computer science majors often had Linear Algebra and/or Discrete Mathematics as well. The only computer science course several of the mathematics majors had already taken was CS1.

The computer science summer course with a laboratory focus at Ashesi University College required at least Programming 2 (a course more like a traditional CS1 course), Statistics, a quantitative reasoning course, Calculus 1, and either Discrete Mathematics or Data Structures (CS2). Several students also had courses in Computer Organization and Architecture, Programming 3, Database Management, and Web Technologies.

3.2 Textbooks and Other Resources

Both courses began with students reading Simon Singh's *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography* [12]. Singh's book is an excellent and easy-to-read non-fiction book including stories of intrigue, espionage, mathematics, research, discovery and hard work that have characterized the development of cryptography and the algorithms and systems that employ it. Students wrote a summary of the book within the first three weeks, and in the semester-long course engaged in in-class peer review and were encouraged to re-write their papers for increased credit.

Both courses used Brett Tjaden's *Fundamentals of Secure Computing Systems*, and William Stallings, *Cryptography and Network Security* as texts [19, 16]. Tjaden's book was recommended by Crowley; the author was familiar with Stallings from using his books in other courses. Although they cover similar material, Tjaden's book is less technical and more readable by mid-level undergraduates. Stallings' book is more comprehensive and detailed, but also more terse and advanced. Mel and Baker's *Cryptography Decrypted* provides an elemental basis of the mathematical and algorithmic concepts behind many cryptographic processes, and was used as a teaching resource [8]. Their appendix, "Public Key Mathematics (and Some Words on Random Numbers)", is written at a level that is especially accessible to students with a weaker mathematics background, and was used as a roadmap for the mathematical background needed to present the RSA public key algorithm.

Other books and resources were also previewed and may be of interest to those developing a new security course or those interested in enhancing an existing one. The author attended a SWEET (Secure WEb dEvelopment Teaching) workshop at SIGCSE 2011, which proffered laboratory exercises and other resources specifically for teaching secure web development [15]. The SEED project is another NSF-funded initiative with numerous resources including 29 labs as of this writing [11]. Towson University's Security Injections provide security modules that can be injected into several courses throughout the computer science curriculum, from CS0 to a Computer Networks course [10]. Smith's *Elementary Information Security* [13] is a comprehensive text geared more toward information security than the dual cryptographic and computer/network security focus of the course presented. However, those wishing a single resource that covers the new CS2013 Information Assurance and Security Knowledge Area only may consider Smith's book. Lastly, Goodrich and Tamassia's *Introduction to Computer Security* [7] is also a comprehensive self-contained text requiring only a CS2-level background and has a broad focus on security concepts and one chapter on Cryptography. The book integrates some of the labs from the SEED project and may be considered as a lower-

level substitute to the Stallings text for a course that is not so heavily focused on Cryptography.

Both courses used Cryptool, a free and open source program originally developed as an employee education tool at a bank in Germany [4]. The Cryptool project has since evolved into a fully-functional tool that allows users to explore, practice, learn about, and/or view demos of all major historic and modern cryptographic algorithms. Originally developed as a Windows-only application, later versions included a limited web-based version called Cryptool-Online, and in 2012, a platform-independent version based on Java, called JCryptool, was released [4]. Cryptool is available in English, German, Polish, and Spanish versions.

The independent studies and the summer courses with a laboratory focus also used either Live DVDs or Virtual Machines (i.e. VMWare or Virtual Box) with Linux distributions. These were used to allow the students to experiment with OpenSSL and network utility tools to send encrypted files and view packet traffic in the local network. The semester-long mathematics cross-listed course did not utilize Linux labs, partly because of the weaker computer science skills and background of some of the students. In addition, the physical lab setup was problematic: the University-wide network does not allow any local network traffic not destined for the host to be observed or intercepted, and the departmental lab did not have enough computers to accommodate the students, even if some students brought their own laptops.

3.3 Course Structure

Both courses began with the students writing summary papers of *The Code Book*. In the semester-long mathematics cross-listed course, students engaged in in-class peer review and had the opportunity to revise their papers based on peer feedback. In the summer courses there was not enough time to accommodate a paper revision, although it would have been a valuable experience, especially since many of the students were non-native English speakers and would have benefitted from reading their peers' papers and having the opportunity for revision.

Both courses had a midterm and comprehensive final exam. In the semester-long mathematics cross-listed course, either a homework or a lab was assigned approximately every-other week. In the summer course with a laboratory focus, there were only 3 homework assignments, but labs were performed most class days (13 labs were assigned over the 5 ½ weeks of the course). In the mathematics cross-listed course, labs involved Cryptool only, while in the summer course with a laboratory focus, labs included both Cryptool and Linux-based labs. Table 1 gives a listing of the topics for both the Cryptool and Linux-based labs. Labs were typically worked on in pairs and consisted of students working through a prescribed set of applied exercises. Most labs also included an individual analysis component that was completed outside of class, which consisted of "big picture" analysis as well as questions that required more detailed work directly related to the lab exercises. Some of the labs were originally obtained from Crowley, although the majority were developed by the author as the course evolved.

Another major component of both courses was the presentation of current news articles by students at the beginning of every class. Students were instructed to choose a news article from a reputable news source from within three months of the date of their presentation that was related to cryptography or computer, network, or information security. A link to the article was posted

Table 2. Lab Topics

Cryptool Labs	Linux Labs
Monoalphabetic ciphers	Symmetric cryptography using OpenSSL
Vigenère and Enigma	
DES, AES, and CBC	Message Digests using OpenSSL
HMACs	Networked key exchange
Pseudo-random number generation	Different key exchange protocols
	Dictionary attack on passwords
RSA	Traffic/packet analysis
Digital Signatures	

or sent to students ahead of time; at the beginning of class the student gave a brief summary of the news article including its relevance to cryptography or security, and then led a brief discussion over the content of the article. Credit for news article presentations were included as part of the class participation grade.

The semester-long mathematics cross-listed class also included a research, applied research, or implementation project of the student's choosing (with the topic approved by the professor). The project included a paper or implementation and write-up, and class presentation of their work.

In addition, both courses had exposure to professionals currently working in the security industry. In the semester-long mathematics cross-listed course, an alumni working at a security division of Hewlett Packard in Austin, Texas came to guest lecture for a class. The lecture demonstrated the need for mastery of many mathematics and computer science topics and the need for continual learning, to keep up and work in the field of security. In the summer course with a laboratory focus, the class was invited by three recent alumni to a company in Accra, Ghana that develops ATM hardware, software, and services. During the field trip students were able to see the server room and learn about some of their network security issues and safeguards; see their control room and learn about the real-time tracking of ATM transactions and how they use algorithms and protocols discussed in class; and see the insides of an ATM machine and learn about many of the physical and software security mechanisms built into ATMs.

3.4 Course Content

Both courses covered similar material, although for some topics the two courses covered certain material in more or less depth. Both courses began with studying historic cryptosystems using material from the textbooks, which also overlapped material in *The Code Book*. Coverage of the more mathematical Hill cipher was included in mathematics cross-listed course but was skipped for the laboratory focused course. The modern block ciphers DES and AES, and the concept of cipher block chaining (CBC) were also discussed in both courses, with more emphasis placed on the theories of Feistel ciphers and the properties of AES in the mathematics cross-listed course. In both courses the number theory background needed to fully understand RSA public key cryptography was introduced, with more emphasis on the mathematical theory in the mathematics cross-listed course. Cryptographic hash functions, message authentication codes (MACs) and keyed-hashed MACS (HMACs) were also covered in both courses in similar depth. The Diffie-Hellman-Merkle key exchange protocol, other key exchange protocols, and different techniques for producing digital signatures were also covered in

both courses. Computer security threats (e.g. classifications of Malware) and network security threats (e.g. DDOS Attacks) were covered in similar depth, and risk analysis was discussed in both courses as well. Finally, secret key management, public key certificates and PKI infrastructure, user authentication protocols, and Kerberos were also covered in both courses.

Three topics were also covered that are not necessarily considered fundamental knowledge but that the author views as significantly important in the fields of cryptography and computer and network security: true and pseudo-random number generation, issues of passwords, and elliptic curve cryptography. True and pseudo-random number generators were discussed in somewhat more detail in the laboratory focused course, which may seem counter-intuitive; the reason is that all students in the laboratory focused course had taken an elementary statistics course and there was no guarantee that even the mathematics majors in the mathematics cross-listed course has taken any probability or statistics course. Passwords were discussed in both courses, including: hashing and storage, their use in authentication protocols, the purpose of salting passwords, and recent studies examining password qualities; in the laboratory course, a detailed Linux-based lab in which students implemented a brute-force attack on both salted and unsalted passwords was also performed. Lastly, elliptic curve cryptography, the most recent major multi-purpose cryptographic method, was also studied; not surprisingly, the mathematics cross-listed course studied this topic in more detail than the applied course.

3.5 Topics Covered and CS2013 Ironman Draft Guidelines

The Ironman Draft of the upcoming CS2013 curricular guidelines separate Information Assurance and Security (IAS) into a separate Knowledge Area, with 2 hours listed as Core-Tier1, 6 hours listed Core-Tier2, and numerous Elective topics [6]. In addition, IAS topics are distributed among other Knowledge Areas, with 23 Core-Tier1 hours and 46 Core-Tier-2 hours distributed among 8 other Knowledge Areas. There is already significant overlap between security concepts presented as the 2 Core-Tier1 and 6 Core-Tier2 IAS topics in the CS2013 Ironman Draft, and courses already taught in a typical computer science curriculum. The versions of the course presented here serve to strengthen and deepen the students' understanding of many of these core topics by providing an in-depth study of the cryptographic principles underlying the concepts and algorithms. In addition, the course expands the students' security breadth by adding other IAS Core-Tier1 and Core-Tier2 topics that are distributed in other Knowledge Areas, or that are listed as IAS Elective topics in the CS2013 Ironman Draft.

The course encompasses all of the Elective IAS/Cryptography category, all of the IAS/Network Security Core-Tier1 and most of the Core-Tier2 hours, most of the IAS/Fundamental Concepts Core-Tier1 and Core-Tier2 hours, and includes a modicum of other topics throughout the CS2013 Ironman Draft IAS Knowledge Area: topics from IAS/Risk Management, IAS/Security Architecture and Systems Administration, IAS/Security Policy and Governance, NC/Introduction, NC/Networked Applications, OS/Security and Protection, SE/Software Project Management, SF/Virtualization and Isolation, and SP/Security Policies, Laws, and Computer Crimes. In addition, discussion of current news articles gave students exposure to additional topics in: IAS/Network Security, OS/Overview of Operating Systems, OS/Operating Systems Principles, SP/Intellectual Property, SP/Professional Ethics, and SP/Security Policies, Laws, and Computer Crimes

Table 2. Course Topics and location in CS2013 Ironman.

Topic(s)	Location in CS2013 Ironman	Tier1, Tier2, or Elective
Introductory security concepts	IAS/Fundamental Concepts	Tier1 and Tier2
	IAS/Security Policy and Governance	Elective
Risk analysis	IAS/Risk Management	Elective
	SE/Software Project Management	Tier2
Classic and historic ciphers	IAS/Cryptography	Elective
Block Ciphers: DES and AES; CBC mode	IAS/Cryptography	Elective
Cryptographic hash functions, message digests, MACS, HMACs	IAS/Cryptography	Elective
True and Pseudo-random number generators	None	N/A
Number theory for RSA	IAS/Cryptography	Elective
RSA Public Key Cryptography	IAS/Cryptography	Elective
Diffie-Hellman-Merkle and other secret-key exchange protocols	IAS/Cryptography	Elective
Digital Signatures	IAS/Cryptography	Elective
Elliptic Curve Cryptography	None	N/A
Secret Key Management and Hybrid Systems	IAS/Cryptography	Elective
Public Key Infrastructure	IAS/Cryptography	Elective
User Authentication Protocols, Access Control, and Kerberos	IAS/Cryptography	Elective
	IAS/Security Arch and Systems Admin	Elective
	OS/Security and Protection	Tier2
Issues of passwords	IAS/Security Arch and Systems Admin	Elective
	SP/Security Policies, Laws, and Computer Crimes	Elective
Computer Security and Threats; Malicious Code	IAS/Fundamental Concepts	Tier2
	SF/Virtualization and Isolation	Tier2

	SP/Security Policies, Laws, and Computer Crimes	Elective
Network Security and Threats; Network Attacks	IAS/Fundamental Concepts	Tier2
	IAS/Network Security	Tier1
	NC/Introduction	Tier1
	NC/Networked Applications	Tier2
Current News Articles	IAS/Network Security	Tier1 and Tier2
	OS/Overview of OS	Tier1
	OS/OS Principles	Tier1
	SP/Intellectual Property	Tier1
	SP/Professional Ethics	Tier1 and Tier2
	SP/Security Policies, Laws, and Computer Crimes	Elective

4. OUTCOMES OF THE TWO COURSES

The course evaluations in both courses were excellent, with overall comments such as, "It inspired me!", "The course was interesting and captivating.", and "I want more." Students were clearly engaged in and excited about the course.

Students consistently reported, both via course evaluations and verbally, that they enjoyed the *The Code Book* assignment, even though it entailed reading a non-fiction book and writing a paper over it in a relatively short amount of time. *The Code Book* is engaging and easy to read, much more like a novel than a textbook, and the students agreed that it was a great way to learn the history. Although published in 1999, the material is not "dated" – it presents a comprehensive history of cryptography from the 5th century B.C. to the late 1990s, with a final chapter on quantum cryptography. Through the paper the students exercised their writing skills, and through the peer review and optional re-write for increased credit (in the semester-long mathematics cross-listed course only) students improved their writing skills as well.

The students also appreciated the daily news articles as a connection between the theory and what is happening in "real life". Sprenkle & Duvall call this the "broader issues" component of a computer science course [14]. The discussion surrounding the articles varied from forced to lively, and often connected to previous articles or previous course material. Due to the plethora of news articles related to security, students had plenty of topics to choose from, and the range of news topics presented throughout each course was largely comprehensive. Interestingly, the American students appeared to put less effort into choosing the news article they presented and preparing for the presentation than the West African students, who spent a lot of effort finding an article that was different from past articles and also relevant to the coinciding or recent course topics; the West African students also spent significant time and effort reading the background information the article referenced. Including student presentations of news articles is an aspect of the course that is highly recommended to anyone teaching a security course, because it serves to consistently highlight the relevance of security in just about every facet of our lives. For the mathematics cross-listed course, which was about ¼ mathematics majors, it also served to demonstrate the importance of security and the applicability of mathematics, and not just computer science, to the field of security. Several course evaluations commented positively on this aspect of the course, including, "The news presentation helped make a clear relationship to what happened in the real world." and "I knew nothing was secure, but Wow! All these articles about attacks is crazy!"

An added benefit of a computer security elective course that is cross-listed with mathematics is the possibility of enticing mathematics majors to take more computer science courses, and encouraging mathematics majors to take CS1 earlier rather than later in their academic careers. Most of the mathematics majors in the Southwestern University mathematics cross-listed course were either graduating seniors or rising seniors with little or no opportunity to fit "extra" CS courses in their degree plan before graduation. However, at the end of the computer security elective course, one rising senior mathematics major switched to a Computational Mathematics major, a major that incorporates much of the mathematics and computer science coursework but that is less than a full double-major. In addition, a Biology major who had taken the course in conjunction with CS 2 registered to take more CS classes the following semester. Although only two students, this points to the interest of non-CS majors desiring to take more computer science courses.

The laboratory exercises were a favorite component of each course. In both courses students commented on this in freeform responses on the course evaluations: in the semester-long mathematics cross-listed course, 7 of the 23 students said that more hands-on labs would have improved the course. A recommended future iteration of the semester-long mathematics cross-listed course would include more contact time so that more labs could be accommodated. In the summer course with a laboratory focus, almost ½ of the students commented on the labs as a strength of the course, including comments such as, "The intensive lab sessions were exciting and demystify the course", and "Labs were very helpful and questions stressed critical understanding and applied logic." Logistically, the labs in the summer course were essential since the course met 2-3 hours per day, 5 days per week; without the more applied laboratory work, students would have been too overwhelmed and/or bored in a 2-3 hour class every day. The students in the summer, laboratory focused course also greatly valued the field trip, and commented both verbally and in the course evaluations about how the trip showed the practicality and relevance of course topics and work being done in the real world.

The semester-long mathematics cross-listed course had an independent project in which students either researched theory, investigated an algorithm or application area of an algorithm not covered in class, implemented an algorithm, or performed a hands-on computer or network security investigation. Overall this was a valuable assignment, since students chose topics particularly interesting to them and further exercised their research and/or independent learning, writing and class presentation skills. However, due to the relatively large class size for the liberal arts setting (23 students), project presentations consumed the last 2 ½ weeks of the semester, which allowed less time for other class topics or labs. In the future, if enrollment in the course remains high, student in-class presentations of projects

may be eliminated so that even more time could be devoted to labs or additional topics.

Both courses are expected to continue; the semester-long mathematics cross-listed course may become one of the "standard" electives at Southwestern University. The summer course with a laboratory focus at Ashesi University College in Ghana is expected to continue and expand into a summer study abroad opportunity for American computer science students. In addition to providing an opportunity for both American and West African students to learn about cryptography and computer security, students would also learn from each other about the similar and differing issues surrounding computer and network security in two very different areas of the world.

5. CONCLUSIONS

Two models of an elective Cryptography and Computer Security course in a liberal arts context are presented, one a semester-long course taught at a traditional liberal arts college in the United States, another a summer course taught at a new University with a liberal arts focus in Ghana, West Africa. The semester-long course was cross-listed as a mathematics course and included an independent project and student presentations of their work; the summer course included about the same amount of contact time, but more time was spent in the lab and there was no individual project. Both courses were very successful and covered much of the same material. The courses provided students depth in the cryptographic principles underlying modern security algorithms, as well as background in the history of cryptography and an opportunity to discuss current news articles. In both courses, the laboratory components were considered essential and served to provide the students with opportunities for hands-on engagement with the course material. Future iterations of the semester-long mathematics cross-listed course will endeavor to include more labs. The summer course with a laboratory focus is expected to continue and expand into a summer study abroad opportunity in order for American computer science students to study in Ghana.

6. REFERENCES

[1] ACM TechNews Archive. http://technews.acm.org/archives.cfm.

[2] Chen, L., Tao, L., Li, X. and Lin, C. 2010. A Tool for Teaching Web Application Security. In *Proceedings of the 14th Colloquium for Information Systems Security Education*. CISSE, Severn, MD, 17-24.

[3] Crowley, E. 2006. Developing 'Hands-on' Security Activities with Open Source Software and Live CDs, *Journal for Computing Sciences in Colleges* 21, 4 (Apr. 2006), 139-145.

[4] Cryptool Portal, Cryptography for Everybody. http://www.cryptool.org/en/.

[5] Du, W. SEED: a suite of instructional laboratories for computer SEcurity EDucation. 2007. In *Proceedings of the 38th ACM Technical Symposium on Computer Science Education*, ACM, New York, NY, 486-490, DOI=http://doi.acm.org/10.1145/1227310.1227474.

[6] Joint Task Force on Computing Curricula (Nov. 2012). Computer Science Curricula 2013: Ironman Draft (Version 0.8). http://ai.stanford.edu/users/sahami/CS2013/ironman-draft/cs2013-ironman-v0.8.pdf.

[7] Goodrich, M.T. and Tamassia, R. 2011. *Introduction to Computer Security*. Addison-Wesley, New York.

[8] Mel, H.X. and Baker, D. 2001. *Cryptography Decrypted*. Addison-Wesley, New York.

[9] National Security Agency, Central Security Service. Information Assurance Scholarship Program (IASP). http://www.nsa.gov/careers/opportunities_4_u/students/undergraduate/iasp1.shtml.

[10] Security Injections @ Towson University. http://triton.towson.edu/~cssecinj/secinj/.

[11] SEED Project. http://www.cis.syr.edu/~wedu/seed/.

[12] Singh, S. 1999. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Doubleday, New York.

[13] Smith, R. 2011. *Elementary Information Security*. Jones and Bartlett, Burlington, MA.

[14] Sprenkle, S. and Duvall, S. 2012. Reshaping the Image of Computer Science in Only Fifteen Minutes (of Class) a Week. In *Proceedings of the 43rd ACM Technical Symposium on Computer Science Education*, ACM, New York, NY, 595-600, DOI=http://doi.acm.org/10.1145/2157136.2157308.

[15] SWEET Project. http://csis.pace.edu/~lchen/sweet/.

[16] Stallings, W. 2011. Cryptography and Network Security. Pearson- Prentice Hall, New York.

[17] U.S. Office of Personnel Management. Federal Cyber Service: Scholarship for Service. https://www.sfs.opm.gov/.

[18] Taylor, B. and Kaza, S. 2011. Security Injections: Modules to Help Students Remember, Understand, and Apply Secure Coding Techniques. In *Proceedings of the 16th Annual Joint Conference on Innovation and Technology in Computer Science Education*, ACM, New York, NY, 3-7, DOI=http://doi.acm.org/10.1145/1999747.1999752.

[19] Tjaden B.C. 2004. *Fundamentals of Secure Computer Systems*. Franklin, Beedle & Assoc., Inc. Wilsonville, OR.