Challenges in Teaching a Graduate Course in Applied Cryptography

Sujata Garera and **Jorge Vasconcelos**
Information Security Institute
Johns Hopkins University
3400 North Charles Street
Baltimore, Maryland 21210 USA
{sgarera, jorgev}@cs.jhu.edu

Abstract: We describe our experience in creating and teaching a graduate course in cryptography at the Johns Hopkins University. We emphasize on the importance of such a course for a graduate student in an information security program. We discuss the course implementation and discuss the challenges in teaching this course to students from varied backgrounds. Based on our observations, we suggest specific improvements that could be applied to this course in the future.

Categories and Subject Descriptors: K.3.2 [Computers and Education] Computer and Information Science Education; E.3 [Data] Data Encryption; C.2.0 Security and protection; G.2 Discrete Mathematics
General Terms: Security
Keywords: Cryptography, computer science education, security protocols

1. INTRODUCTION

Cryptography, the science of secret message writing, plays a fundamental role in safeguarding the information infrastructure that supports today's world. With the increasing dependence of industry, businesses, education, health care, and society in general, on computing and digital communications, the need for providing security through effective and efficient cryptographic algorithms has became more important than ever. Thus, a thorough understanding of modern cryptography is essential for any computer science professional focused on security.

At the Johns Hopkins University, the Information Security Institute (JHUISI) provides both, research and educational opportunities for faculty and students interested in the field of information security. Its Master of Science in Security Informatics (MSSI) program acknowledges the capital importance of cryptography and requires students pursuing this degree to take at least one course in that subject.

Traditionally, Cryptography has been taught in the Applied Mathematics and Computer Science departments, the first requiring deep knowledge of discrete mathematics and linear algebra, while the second a strong base in complexity theory. Given the fact that students enrolled in the MSSI program come from diverse educational backgrounds, and may not necessarily be mathematics or computer science majors, we observed the need for providing them with means to gather the necessary body of knowledge in cryptography.

Therefore, we chose to create an introductory course, *Basics of Applied Cryptography and Network Security*,[7] containing elements for understanding the basis of classical and modern cryptographic algorithms, as well as examples of specific applications. We expected that enrolled students would have a minimum of skills in number theory, probability and discrete mathematics. However, as we discuss in the next section, a preliminary background survey, along with students' level of comfort with mathematical topics, prompted the need for slightly restructuring the course content.

The course was constantly evolving through a continual collaborative effort throughout the semester between the authors. Sujata Garera has expertise in Computer Science with specific focus on Software and Network Security. She designed the course curriculum and assignments and delivered the lectures. Jorge Vasconcelos has expertise in Computer Science Education. His point of view helped to better shape the course according to individual needs as well as selecting reading materials for such a diverse group. After every class, the authors met to reflect on events and students responses during that particular day, assessed progress and analyzed obstacles, aiming to improve the subsequent sessions.

[7] Offered as a part of the MSSI program and taught for the very first time during the Fall of 2008.

2. GOALS, CONTENT AND POPULATION

Our broadest goal was to promote understanding of cryptographic algorithms among the MSSI students, from both, an analytical and an applied perspective, as well as providing a background that would enable our students to deal with cryptography effectively and correctly whenever necessary.

The course covered both classical and modern ciphers. Students were exposed to the analysis and design of various cryptographic primitives. We also presented various attacks against cryptographic primitives including techniques to analyze cryptographic protocols from an adversarial viewpoint. The course was conducted over a 12-week period with two lectures per week. Table 1 summarizes the core content of our course.

Table 1. Course Syllabus

Category	Topics	No.Weeks
Introduction	Basic terminology and Classical cryptography	1 ½
Block and stream ciphers	Modes of operation, DES, DES-X, AES, RC4	2 ½
Key distribution	Needham Schroeder protocol, Attacks on protocols (replay, parallel session and implementation attacks)	1
Random number generation	Randomness, HotBits, Linear congruential generators, ANSI X9.17, attacks on PRNGs	1
Hash functions	One way functions, properties of hash functions, Message authentication codes, Usage of MACs for chaffing and winnowing, authentication protocols using MACs	1 ½
Public key cryptography	Diffie Hellman, RSA, OAEP-RSA, Semantic security, Elgamal, Digital signatures, DSA, Blind signatures, Digital payment systems, Authentication protocols using signatures	3
Secret sharing	Secret sharing, Secure metering, Visual cryptography	1 ½

2.1 Demographics and Background.

Twenty-five graduate students were enrolled for the class, twenty of which stayed through the course. Nearly 60% of the students were international (mostly from India) and 40% were American. The students had undergraduate studies in Electronics Engineering, Computer Science or Information Technology.

To assess students' familiarity with foundational topics in number theory, probability, discrete mathematics and computer security, we conducted a survey on the first day of class. It consisted of a multiple-choice questionnaire[8] comprising concrete mathematical problems and self-ranking questions (in which students indicated their familiarity with specific topics). Results are shown in Tables 2 and 3.

The results in Table 2 indicate that while most students seemed familiar with popular cryptographic algorithms, more than half of the class was not familiar with fundamental concepts in number theory and algorithms. Table 3 shows the percentage of students that correctly answered the mathematical questions. It is interesting to note that while nearly 44% of the class expressed medium familiarity with the "Birthday Problem" and 20% expressed high familiarity, only 36% of students correctly answered the corresponding question.

Table 2: Students Familiarity with Topics

Topics	Familiarity (%)		
	High	Medium	None
Number Theory			
Modular arithmetic	24	28	48
Euler Phi function	12	20	68
Generator of a group	8	32	60
Galois field	0	0	100
Jacobi symbol	12	8	80
Probability & Algorithms			
Birthday problem	20	44	36
Entropy	20	40	40
Complexity classes	4	24	72
Algorithmic complexity	28	20	52
Cryptographic Algorithms			
DES	40	44	16
RSA	40	52	8
Hash functions	32	64	4
Digital signatures	20	68	12
Kerberos	8	68	24
PGP	12	60	28
SSL	44	48	8

Population: 25 MSSI graduate students.

As the semester progressed, several students became anxious about the level of mathematics required by the course. Despite a review on number theory and probability conducted at the beginning of the course, it quickly became evident that with such a heterogeneous background it would be hard, even "painful" for many people to grasp the mathematics behind every topic. This situation prompted the decision of increasing course content with respect to security protocols and applications, since most students demonstrated ability to relate to these topics and were far

[8] Available on the course web site at http://www.cs.jhu.edu/~sdoshi/crypto/crypto.html

more interactive during the class meetings. The resultant syllabus (outlined in Table 1) thus contained a reasonable amount of cryptography, security protocols and applications for a basic course in cryptography and network security. In the following sections we detail the course implementation and discuss some interesting highlights of the course.

Table 3: Correctness on Concrete Examples

Question Topics	**Correctness (%)**
Identity element	40
Permutations	36
Birthday problem	36
Primes	28
Abelian group	12

3. COURSE IMPLEMENTATION

3.1 Textbooks and Reading Material

While several textbooks on cryptography are available in the market [1-4], at the time the course was offered, we did not find one covering all the topics of our syllabus in a simple and effective manner. For example, while Stinson [1] is a popular choice in similar courses, we found it too advanced for an introductory course. Stallings [4] covered most of the cryptographic algorithms and applications at a level better suited to our class. We also used Menezes' Handbook [2] as secondary reference. Throughout the semester we guided the students on specific chapters or sections to be read.

In addition to textbook reading, we suggested several research papers [5-19], which oftentimes were the focus of discussion in class. Oftentimes, students found these papers far more interesting compared to the textbook, and these also aided for a better understanding of the course topics. In particular, we found that, for the following topics, research papers and online resources were easier to understand compared to the textbooks.

Key Distribution and Authentication Protocols:

While the book by Stallings introduces the Needham Schroeder key distribution method, a protocol that is popularly discussed in most security courses, it does not give enough insights into the design and analysis of cryptographic protocols. To promote a comprehensive understanding of this topic, we heavily referred to the paper *Prudent Engineering Practice for Cryptographic Protocols by Abadi and Needham* [12]. This paper provides a thorough discussion of how several cryptographic functions (such as encryption and signatures) must be used in a cryptographic protocol involving authentication, identification or key distribution. The paper also served as a resource for a number of assignment problems, giving the students significant experience with protocol analysis.

Random Number Generation:

Although the textbook reasonably discusses linear congruential generators and the ANSI X9.17 random number generator, it does not contain a thorough discussion regarding attacks against them. In this case, we referred to the paper *Cryptanalytic Attacks on Pseudorandom Number Generators by Kelsey, Schneier, Wagner and Hall* [8] to discuss specific attacks against the ANSI standard random number generator. In addition, to differentiate between true randomness and pseudo-randomness we referred to the online service HotBits [9]. This is a very effective way of demonstrating how radioactive decay time can be used to produce random numbers.

Furthermore, each lecture was supported by a vast set of slides which was made available beforehand through the course website. The slides were designed to be both, informative and thought provoking. In particular, we often left open questions on the slides and asked the students to think about them and publicly solve them in class. While asking students to solve questions on the board is certainly not easy, we saw how this practice not only increased self-confidence, but also helped to observe common mistakes made when solving problems [20].

3.2 Assessment

Students were evaluated based upon correctness and quality of their assignments and tests. There were five take-home assignments, two in-class assignments, one pop quiz, and midterm and final exams. Take home assignments were aiming to give students time to practice and become comfortable with the mathematics behind cryptography. The in-class assignments, quizzes and exams were designed to test if the students were able to apply their knowledge correctly within time constraints.

Students were encouraged to openly discuss ideas and do teamwork on the take home questions. We believe that such collaboration enhances the learning process and encourages students to think of the problems assigned from different points of view. While teamwork was allowed, we required each student to write down the solution in his own words, as well as explicitly give credit to other students that contributed in solving the problem. We also encouraged outside research and asked them to incorporate their findings in the solutions submitted, provided that the proper credit was given.

It is noteworthy to mention that, throughout the course, the students often referenced Wikipedia while solving the assignments. Students periodically used it to look up concepts not explicitly addressed in class, gather information aiming to gain further understanding of the

course topics, find alternative explanations, or find links to other online resources.

The questions on assignments and exams can be broadly categorized into theory, protocol analysis or rigorous cryptographic attacks. Each assignment usually comprised of five to eight questions, with the easier ones placed at the beginning and increasing difficulty towards the end. We took care that the questions were challenging enough to keep students interested in the topic and yet solvable in the time allocated. Some assignment questions are described in Table 4.

To motivate students to improve their overall performance, we gave plenty of opportunities to obtain extra-credit, by either answering optional questions or doing additional research in the mandatory ones. For each assignment we provided a detailed solution set and discussed some questions in class.

Table 4: Assignment Questions

Category	Assignment Question
Rigorous cryptographic attacks	• Given a ciphertext created by applying a substitution cipher on English text, use frequency analysis to determine the plaintext and the key. • Devise an iterative attack on the ANSI X9.17 generator based on the attack described in [8].
Protocol analysis	• Given a variation of the Needham Schroeder protocol, present an attack on a CBC implementation of the protocol.
Theory	• Compare and contrast various components of the DES and AES ciphers. • Generalize the 3-way Diffie Hellman protocol to an *N*-way protocol. • Describe semantic security proofs and proofs based on reduction. (Formal description was not required for the proofs.)

3.3 Course Highlights

As the course progressed, we learned considerably about the comfort level of the students with the subject in general. In the following sections, we highlight some key observations that were made during specific course topics.

3.3.1 Classical Cryptography and Probability

We covered several early cryptographic algorithms including the Vigenere and Vernam ciphers. We witnessed how students were definitely curious about their internals and were very motivated to suggest attacks against them.

To give a complete picture of the secrecy obtained by the Vernam cipher, we introduced the notion of perfect secrecy, which involved application of the Bayes Theorem. We found, however, that this notion was just not immediately intuitive to most students but even became a major cause of anxiety. To address this situation, we did a brief review on Bayesian Probability and had the students work out *toy examples* of perfect secrecy. Students were able to relate more to this topic whenever the discussion used trivial examples.

3.3.2 Symmetric Key Cryptography

As indicated earlier, the course included several modern symmetric key cryptographic algorithms like DES, AES and RC4. While the DES and RC4 algorithms were easy to teach, there were interesting challenges when trying to explain the internals of the AES algorithm. AES works in the Galois field $GF(2^8)$, and, as shown in Table 1, no student in the class was familiar with operations in those fields. Consequently, we devoted some time for reviewing number theory before proceeding to details of the AES algorithm.

This review involved teaching basic properties of groups, fields, and polynomial arithmetic in fields. We also discussed the Euclidean algorithm for obtaining a multiplicative inverse and had the students work out several examples. It is important to mention that while these sessions provided a minimum mathematical background to discuss AES, it certainly overwhelmed most students.

To make the students comfortable with number theory, we added several practice problems in the second assignment. In this sense, we quote Rubin [21] when claiming that number theory is quite abstract and "there is no such thing as too many examples." This situation was more than evident while covering public key algorithms, because we needed to continuously remind the students of the number theory topics related to the specific algorithm being taught. While such a "just in time" approach [22] to teaching the mathematics behind cryptography seemed to work well, we are concerned if the understanding of the algorithms was actually deep enough.

3.3.3 Key Distribution and Authentication Protocols

We discussed several cryptographic protocols during the semester. Most students seemed to relate easily to the discussions revolving around these protocols and were highly interactive during class.

We taught the Needham Schroeder symmetric key distribution protocol in an incremental manner. In particular we began with a version of the protocol without any nonces and had the students identify possible attacks against this version. Then, we incorporated the necessary nonces and had the students analyze the resultant protocol. The students were very quick to spot the possible replay attack due to the lack of timestamps in one step of the protocol. Several students were energetically arguing possible attacks against this protocol. We thoroughly enjoyed the level of excitement and interactiveness in the class during this discussion.

3.3.4 Public Key Cryptography

We spent a considerable portion of class time on the Diffie Hellman key exchange, the RSA algorithm and the Elgamal encryption algorithm. We taught both, the basics of each algorithm and the associated security proofs. In particular, we showed how to reduce the security of an algorithm to a known hard problem. For example, we described how to reduce the security of the ElGamal algorithm to the Diffie Hellman problem. Similarly, we discussed how to determine if an algorithm was semantically secure.

Pointcheval's paper [16] was particularly useful in designing problem questions for semantic security games. We developed several randomized versions of the RSA algorithm based on the Pointcheval's constructions, intentionally adding flaws from the semantic security point of view. We asked the students to work out the semantic security game and evaluate these constructions under that game. As in the case of number theory, we observed that providing several construction examples, improved the students' understanding of semantic security considerably.

4. FUTURE WORK

Teaching a course in Cryptography for the first time was a challenging and enriching experience. Since the course continuously evolved throughout the semester, we found several opportunities to alter the course content and our course delivery. We found that it not only improved our teaching abilities, but it also gave us insight into ways of improving this course in the future.

One of the aspects that we would like to incorporate in future offerings of our course is a computer project component. Other courses [21,22] have been successful in teaching through implementing projects. Although we realize this would increase the course load significantly, we feel that students could learn considerably more from implementing the algorithms taught in class. A possible approach would be to design a framework where students can implement, break and benchmark cryptographic algorithms. Similarly designing implementation assignments related to specific cryptographic applications, like encrypted file systems for example, would give the students a thorough understanding of the cryptographic primitives being used.

In addition to the project component, we also aim to provide weekly math reviews. We believe that such reviews would provide a better mathematical foundation to the students compared to the "just in time" approach [22]. Such reviews would also provide a good outlet for students to discuss example problems in number theory, probability and discrete mathematics. While the implementation component would improve the students understanding of applying cryptographic primitives, these reviews would improve their mathematical foundation for learning cryptography.

ACKNOWLEDGEMENTS

We thank Dr. Gerald Masson and Dr. Aviel D. Rubin for encouraging us to develop such a course and for writing this paper. The website we maintained throughout the semester can be found at http://www.cs.jhu.edu/~sdoshi/crypto/crypto.html.

REFERENCES

[1] Stinson, D. *Cryptography Theory and Practice*, Second *Edition*, CRC Press, February 2002.
[2] Menezes, A., et al., *Handbook of Applied Cryptography*, CRC Press, October 1996.
[3] Schneier, B., *Applied Cryptography, Second Edition*, John Wiley & Sons, 1996.
[4] Stallings, W., *Cryptography and Network Security, Fourth Edition*, Prentice Hall, 2006.
[5] Fluhrer, S., et al., "Attacks on RC4 and WEP." *Cryptobytes* 2002
[6] Rogaway, P. "The Security of DES-X." *Cryptobytes* 1996
[7] Merkle, R.C.. and Hellman, M.E., "On the security of multiple encryption." *Communications of the ACM* 1981
[8] Kelsey, J., et al., "Cryptanalytic Attacks on Pseudorandom Number Generators." *5th International Workshop on Fast Software Encryption*, 1998
[9] *HotBits*: Genuine random numbers generated by radioactive decay. http://www.fourmilab.ch/hotbits.
[10] Eastlake, D., et al., "Randomness Recommendations for Security." *IETF* Draft, 1994
[11] Callas, J., "Using and Creating Cryptographic Quality Random Numbers." http://www.merrymeet.com/jon/usingrandom.html 1996
[12] Abadi, M., and Needham, R., "Prudent Engineering Practice for Cryptographic Protocols." *IEEE Transactions on Software Engineering*, 1996
[13] Rivest, R., "Chaffing and Winnowing: Confidentiality without Encryption" http://people.csail.mit.edu/rivest/chaffing-980701.txt, 1998
[14] Difffie, W. and Hellman, M., "New Directions in Cryptography," *IEEE Transactions on Information Theory*, 1976
[15] RSA Labs., "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths." http://www.rsa.com/rsalabs/node.asp?id=2088
[16] Pointcheval, D., "New Public Key Cryptosystems based on the Dependent-RSA Problems." *Advances in Cryptology-Proceedings of EUROCRYPT* 1999
[17] Chaum, D., "Blind signatures for untraceable payments." *CRYPTO* 1998
[18] Shamir, A., "How to Share a Secret." *Communications of ACM*. 1979
[19] Stinson, D., "Visual Cryptography and Threshold Schemes" *IEEE Potentials* 1999
[20] Huggins, K. and DeCoste, R., "Reflections on Teaching Discrete Math for the First Time." *Inroads SIGCSE Bulletin*. Volume 39, Number 2, June 2007
[21] Rubin, A., "An experience teaching a graduate course in cryptography." *Cryptologia* .Volume 21, Number 2 1997
[22] McAndrew, A., "Teaching Cryptography with Open Source Software." *SIGCSE* 2008