# Information Security Lab Development with Free and Open Source Software: Applied Cryptology and Secure Communications

**Edward Crowley**
Information and Logistics Department
University of Houston

## Abstract

Several current trends are making the securing of an enterprise's informational assets increasingly challenging. Three significant trends are that enterprises are increasingly:

1. Becoming more dependent on digital information and related systems that process, store, and transport that information.
2. Connecting their internal networks to other external enterprise networks as well as to public networks.
3. Employing portable storage devices, including portable computers and USB storage devices.

Left uncontrolled, each of these trends can decrease enterprise security.

Fortunately, use of appropriate cryptographic services can mitigate current and future risks. Specific enterprise issues positively impacted by cryptographic services include secure communications and secure data storage. The increased need for enterprise cryptographic security services has also increased the need for security professionals that can assess, evaluate, and implement cryptographic security solutions.

The increased need for skilled enterprise professionals presents the curriculum developer, with several challenges. These challenges include defining the applied cryptography course with respect to course goals, scope, content, and organization. While there are well-established cryptography courses offered in the Computer Science and Mathematics disciplines, these classes tend to focus on mathematical foundations rather than services and applications. Consequently, the developer of such courses finds that resources particularly those relating to "hands-on" activities are lacking.

For a lab module designer, creating modules that support an applied cryptography class presents several unique challenges. For example, the choice of laboratory software presents a unique challenge. This is especially true since most commercial cryptographic software is designed to shield the user from operational details. This makes most commercial cryptographic software packages unsuitable for use in our lab modules.

Fortunately, there are also Open Source Cryptographic Toolkits that have worked well in our lab environment.

This paper presents the author's experience in the development of laboratory modules for an applied cryptography and secure communications course. These laboratory modules utilize Free and Open Source Software (FOSS) in a networked computer lab environment. In addition to conventional utilities, the lab modules utilize two FOSS cryptographic toolkits. One toolkit, OpenSSL, is available for both Linux and Windows environments. The other toolkit, CryptTool, was originally available exclusively for Windows though there is also a Linux version available.

## Introduction

As enterprises become increasingly dependent on digital information and related digital systems, the protection of information while in transport and in storage becomes increasingly important. This means that the supporting cryptographic security applications and services also become increasingly important.

As more commerce becomes Internet enabled, we can expect more enterprise data and communication system attacks. Figure 1 models this expectation. In this model, risk is proportional to the area of the triangle. And as any of the sides of the triangle increases, enterprise risk increases.

As the Internet expands, it creates more opportunity for nefarious behavior. And as more sites that distribute malware come online, the required skills to create an online enterprise attack expands. Consequently, we expect that as Internet use expands, enterprise risk will increase.

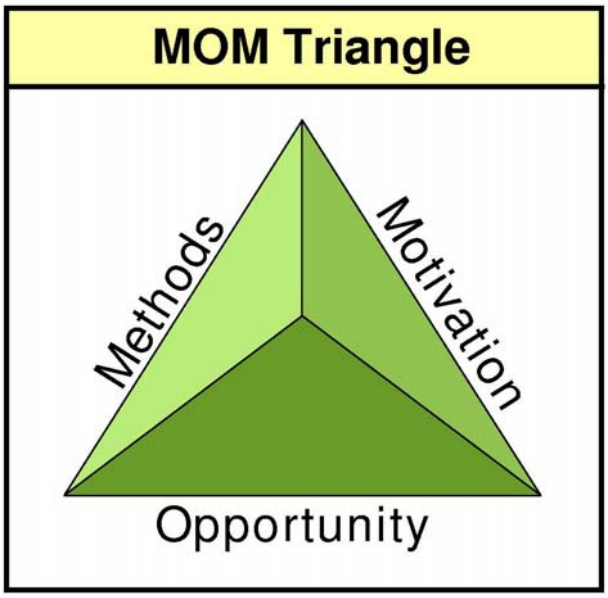


Figure 1. Risk Triangle Model

Some of these attacks may lead directly to financial losses. Other attacks may negatively impact the availability of critical services. And still other attacks may greatly reduce public confidence in specific enterprises. In addition to the need to defend against technical attacks, cryptography is becoming increasingly utilized to demonstrate regulatory compliance. For example, California SB 1386 excludes encrypted data from its provisions.

Consequently, for many enterprises, managing risks as well as ensuring regulatory compliance has become increasingly important. And while risks may exist within people, process, or technical domains, cryptographic applications can offer many innovative solutions. Though, care needs to be exercised that the cryptographic application and the environment in which it is implemented is appropriately assessed and evaluated.

Another one of the challenges of developing an applied cryptography and secure communications course is that "Although the cryptology is a unique science based on exact mathematical apparatus, there is not any unique method how to teach it" [6]. For example, a cryptology course may be classically orientated, emphasizing mathematical and complexity aspects or it may be practically oriented emphasizing the applications of algorithms and protocols. While there is an established history of theoretically oriented courses, applied courses are still being developed.

Part of the development process then is deciding what applied content to include and what learning activities will reinforce that content best. A brief examination of the history of cryptography will help to illuminate this issue.

## Historical Development

From a broad historical perspective, cryptography can be considered to have progressed through three distinct generations. Each generation can be distinguished by the unique encryption/decryption method that it utilized. For example, in the first generation, encryption was done by hand. In the second generation, encryption was done by machine. And in the third generation, encryption was done by computers.

As cryptography evolved through each generation, the definition of cryptography also evolved. For example during the Roman Empire, Caesar, invented the mono-alphabetic cipher that bears his name. During this first cryptographic generation, the meaning of the term "cryptography" was derived from the original Greek. That is, from "cryptos-" meaning hidden and "-graphy" meaning writing. Consequently, cryptography was originally defined as "hidden writing".

As cryptography continued to evolve, algorithms became more complex. Rather than monoalphabetical schemes, such as the Caesar Cipher, polyalphabetical schemes such as the Vigenère cipher were developed. While these were initially implemented by hand, to facilitate the implementation of more complex polyalphabetical ciphers, machines, typically rotary type, were employed.

For example in WW II, the Germans employed a three rotor cipher machine called the Enigma. At the same time, the Americans employed a fifteen rotor cipher machine called the SIGABA. The SIGABA, also known as the ECM Mark II, was used through the 1950s. An appropriate second generation definition of cryptography can be taken from U.S. Army Field Manual FM 34-40-2 which defines cryptography as "… the branch of knowledge which concerns secret communications in all its aspects."

Over time, digital networks became the preeminent means of communications. At the same time, computers facilitated the development of even more complex algorithms such as DES, 3DES, and AES. This was also the era when asymmetrical cryptography, with its longer key lengths, was developed. An appropriate third generation definition of cryptography comes from the National Institute for Standards and Technology (NIST) which defines cryptography as "… a branch of mathematics that is based on the transformation of data and can be used to provide several security services: confidentiality, data integrity, authentication, authorization and non-repudiation."

Properly implemented, third generation cryptographic applications provide the foundation for many critical enterprise security services. Included in these services are confidentiality, integrity, authentication, and non repudiation. Related security mechanisms include identity management, secure networking, as well as mechanisms such as authentication and non repudiation.

## Curriculum Development Context

Prior to enrolling in our applied cryptography and secure communications course, a student must meet several prerequisites. For example, to be admitted to our program, a student is expected to have already earned a technical undergraduate degree, or have earned a non-technical undergraduate degree coupled with appropriate experience. Specific skills that students entering this course are expected to possess include a basic understanding of computer and network systems as well as a familiarity with network protocols and applications including SSL, TCP, IP, ICMP, and DNS.

The class focuses on learning cryptographic principles, procedures, mechanisms, and techniques as well as applications for secure communications and secure storage. In the lab modules, students apply cryptology tools that demonstrate and reinforce enterprise cryptographic principles and services including confidentiality, integrity, and nonrepudation.

## Laboratory Module Development

Before selecting course goals and content, the author worked with an informal advisory board to answer three specific questions.

1. What contribution should an applied cryptography and secure communications class make to our program goals?
2. What aspects of cryptology and secure networking should be taught?

3. How should this class be taught?

Our published program goals can provide insight concerning these questions.

## Program Goals

Core Information Assurance skills our graduates bring to an organization are the ability to assess, evaluate, and improve an organization's security posture. Assessment focuses on organizational issues including, information criticality, security policy, vulnerability, threat, and risk analysis. It also includes the recommendation of appropriate, cost effective, technical and administrative countermeasures. Evaluation focuses on technical issues including the ability to evaluate existing technical infrastructure in terms of effectiveness and congruency with organization policy. [2]

### Class Goals

Another challenge concerns the class goals i.e. what specific applied cryptographic knowledge and skills that a successful student will need. One source for such information is the National Security Agency (NSA). Through its Information Assurance Directorate, the NSA manages the Information Assurance Courseware Evaluation (IACE) program.[3] Under this program, several hundred schools have had their courseware evaluated.

The IACE Program "… implements a process to systematically assess the degree to which the courseware from commercial, government, and academic sources maps to the national standards set by the Committee on National Security Systems (CNSS). "CNSS publishes instructions intended to provide guidance and establish technical criteria for specific national security systems. "These instructions include technical or implementation guidelines, restrictions, doctrines, and procedures applicable to information assurance."

Table 1 presents the cryptology related goals defined by the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4011. [5] Note that the Committee on National Security Systems (CNSS) was reestablished (formerly NSTISSI) by Executive Order (E.O.) 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age.

| Domain | Knowledge Area |
|---|---|
| Cryptography | Encryption (e.g., point-to-point, network, link)<br>Key management (to include electronic key)<br>Strength (e.g., complexity, secrecy, characteristics of the key)<br>Application of cryptographic systems |
| Cryptosecurity | Cryptovariable or key electronic key management system<br>Encryption/decryption method, procedure, algorithm |
| Key Management | Access, control and storage of COMSEC material<br>Destruction procedures for COMSEC material |

| | |
|---|---|
| | Identify and inventory COMSEC material<br>Key management protocols (electronic key, over-the-air rekeying)<br>Report COMSEC incidents |

Table 1. Information Systems Security (INFOSEC) Professionals, NSTISSI 4011

The following Table 2 presents knowledges specified in the Information Systems Security Officers Standard (CNSS 4014). [4] Specifically, it presents knowledges that security professionals should be able to define, explain, and, where relevant,make recommendations concerning the topics in Table 2.

| Information Systems Security Officers, CNSS 4014 |
|---|
| Cryptanalytic techniques<br>Cryptographic concepts<br>Digital signatures/non-repudiation<br>Key management<br>Message digests (e.g., md5, sha, hmac)<br>Methods of encryption |

Table 2. Information Systems Security Officers, CNSS 4014

For our most recent Applied Security Course, Table 3 presents selected course goals.

| Expected Class Outcomes |
|---|
| Upon completion of this course, students will be able to:<br>1. Define basic cryptographic terms including: random number, private key, public key, algorithm, trusted third party, hybrid cryptosystem and cryptanalysis.<br>2. List, define, and demonstrate cryptographic algorithms including MD5, SHA1, DES, 3DES, AES, and RSA.<br>3. Compare and contrast symmetric, asymmetric, and one-way cryptography.<br>4. Implement and demonstrate secure key exchange with certificates.<br>5. Create and demonstrate relevant cryptographic mechanisms including digital signatures, and message authentication codes (MAC).<br>6. Define, explain, and demonstrate Public Key Infrastructure (PKI) principles and components.<br>7. Define and demonstrate steganography.<br>8. Define, explain, and demonstrate secure protocols including Secure Socket Layer (SSL) and IPSec.<br>9. Define and demonstrate a Virtual Private Network.<br>10. List, define, and explain major cryptographic vulnerabilities and their related threats.<br>11. List and explain major computer and network system threats. |

Table 3. Expected Class Outcomes

## Course Scope and Content

Olejar and Standk [6] have published a cryptographic taxonomy that organizes the cryptology domain into seventeen sub topics. Along with the taxonomy, they proposed a

course content selection tool that, depending upon the audience, would specify different subsets of their original seventeen topics. They further proposed three "rings" or sets of topics for three separate audiences. Defined audiences were cryptologists, programmers, security managers, and users.

For our class, we selected a simplified eight-topic version of Olejar and Standk's security manager's ring. Table 4 presents these eight topics.

| # | Topic | Description |
|---|---|---|
| 1. | Basics | Definitions and terminology. Security goals. Practical cryptology. Historical context. |
| 2. | Classical Cryptography | Historical systems. Ciphers mono and poly-alphabetic. Transposition and substitution. One-time pad. |
| 2A. | Block ciphers | Design principles (Feistel networks etc.), randomness, and algorithms |
| 2B. | Stream ciphers | Design principles and algorithms |
| 2C. | Random Number Generators | Classical, requirements. Modern generators. |
| 3. | Hash Functions | Requirements, one way, collision intractable, etc.. Message authentication codes. SHA and other algorithms. |
| 4. | Public key Cryptography | Theory and model (one-way and trapdoor functions)<br>Big number arithmetic, advantages and disadvantages.<br>Hybrid cryptosystems |
| 5. | Digital Signatures | Signature schemes. Digital Signature Standard. (DSS) |
| 6. | Practical Cryptographic Protocols | Authentication. Key distribution/agreement. Identification schemes. Kerberos. Certificates. |
| 6A. | Security of Cryptographic Protocols | Cryptographic protocol attacks. Secure protocol analysis. |
| 7. | Classical Cryptanalysis | Brute force attacks and complexity issues. Simple/historical system attacks. Kinds of attacks, ciphertext only, chosen plaintext, etc. |
| 8. | Other Cryptology Issues | Quantum cryptology, steganography, legal issues. NIST and FIPs standards… |

Table 4. Recommended Cryptology Class Content for Security Managers

## Class Organization

Our Applied Cryptography Course is taught in a non-traditional format. By design it consists of 10 lecture modules and 10 activity modules. Table 5 presents the lecture modules in the order of their presentation.

| Lecture Modules | Topics |
|---|---|
| Cryptography Evolution | Hand Ciphers<br>Machine Ciphers<br>Computer Ciphers |

| | |
|---|---|
| | Related Topics, Steganography, Digital Watermarking |
| Classic (Secret Key) Cryptography | Substitution and Transposition<br>Mono/poly alphabetical ciphers<br>Block and Stream Ciphers<br>Caesar, Vernam, DES, and AES algorithms<br>Key Exchange Problems |
| Cryptanalysis | Attack Types<br>Frequency analysis<br>Brute Force<br>Implementation vulnerabilities |
| One Way Functions | Hash Functions, MD5, SHA1<br>Message Authentication Codes, HMAC<br>Hard one-way problems |
| Public Key (Asymmetric) Cryptography | Diffie Helman<br>RSA<br>Elliptic Curve<br>Hybrid Cryptosystems<br>Digital Signatures<br>Digital Signature Standard |
| Public Key Infrastructure | Key Distribution<br>Certificates<br>Infrastructure Components |
| Digital System Security Threats | Network Security Testing<br>Network Security and Threats<br>Man in the Middle Attacks<br>Replay Attacks |
| Secure Networks (VPNs) | TCP/IP Review<br>Protocol Analysis<br>SSL & IPSec |
| Secure Applications | E-mail<br>WWW Security and Threats<br>Real World Systems<br>Electronic Commerce |
| Intrusion Detection | Snort and Network Security Monitoring |

Table 5. Lecture Topics and Descriptions

## Lab Modules

Each of the ten lecture modules has a corresponding activity module. Table 6 lists and describes these laboratory modules. The primary cryptographic toolkits employed in our labs are OpenSSL and Cryptool.

The OpenSSL crypto toolkit is available for Linux and Windows platforms. Because OpenSSL is available on the Knoppix LiveCD, it is especially easy to incorporate into laboratory modules. The OpenSSL Project defines itself as "… a collaborative effort to

develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library…" [7] OpenSLL is freely available under an Apache style license.

CrypTool, an educational tool, was developed at University of Darmstadt.[1] With a Windows interface, CrypTool contains numerous cryptographic and cryptoanlynitic methods and mechanisms. Cryptool also contains interactive demonstrations and visualizations that illustrate a number of cryptographic methods and mechanisms such as Digital Signature creation and hybrid encryption. CrypTool source code is distributed under the GNU General Public License (GPL).

In addition to OpenSSL and Cryptool, our laboratory modules utilize a variety of other FOSS tools including Ethereal (WireShark), net cat, and Apache. In addition, a variety of Live Linux CDs are utilized in the lab modules.

Lab Topics

| | Topics | Tools/Comments |
|---|---|---|
| Lab 1 | Monoalphabetical ciphers<br>Caeser cipher<br>Cryptanlysis, Frequency analysis | Prelab monalphabetical cryptanalysis problem. Cryptool orientation and frequency analysis. |
| Lab 2 | Introduction to OpenSSL<br>Introduction to Federal Information Processing Standards (FIPs) | OpenSSL toolkit command line orientation (Knoppix LiveCD). FIPS 140-2 intro. |
| Lab 3 | Symmetric Key Cryptography<br>Pseudo random number generation<br>DES key creation<br>Encryption and decryption with DES<br>File integrity with MD5 hash | Create DES keys with the OpenSSL toolkit. Use DES key to encrypt and decrypt text file. Employ one way hash to demonstrate integrity. |
| Lab 4 | Symmetric Key Distribution<br>With NetCat<br>With Apache<br>Key compromise by protocol analysis (Wireshark) | Tools, NetCat, Apache, and Wireshark, available on the Knoppix LiveCD are used to illustrate key management problems. |
| Lab 5 | Asymmetric Key Cryptography<br>RSA key pair generation<br>Public key distribution with Apache<br>File Integrity with MD5 | OpenSSL toolkit is used to generate an RSA key pair while the Apache Web Server is used for key distribution and MD5 for integrity. |
| Lab 6 | Message Authentication Codes | Using the Knoppix LiveCD, a student appends their DES key to a text file and then hashes the file. After exchanging the text file and the MAC, recreation of the MAC establishes authentication and nonrepudiation. |
| Lab 7 | Digital Signature Generation | Cryptool provides a step by step tutorial and OpenSSL provides the |

| | | |
|---|---|---|
| | | means to create a digital signature. |
| Lab 8 | Password Auditing/Cracking | Students create a series of Windows user accounts with passwords of various strengths. Then, they use the Ophcrack LiveCD to crack the passwords. |
| Lab 9 | Intrusion Detection with Snort | Students work in two person teams. One person utilizes Knoppix, the other person utilizes Knoppix-NSM (Network Security Monitor). |
| Lab 10 | Steganography | Students choose Windows or Linux based tools to demonstrate steganography. |

Table 6. Laboratory Modules

## Conclusions and Future Directions

Antidotal student lab module response has been enthusiastic. Because the labs are open source and LiveCD based, students can repeat and/or verify their labs at home or at work. Students can also freely distribute lab software. Open source software also makes it easy for professors, in related programs to select and adopt existing lab modules.

Much remains to be done. One obvious goal would be the creation of a custom LiveCD containing lab modules and related class materials. Class scope could be extended by adding new modules. For example, TrueCrypt could be employed to demonstrate volume and file encryption applications. Other projects could include a more formal evaluation the effectiveness of existing modules.

## References


1. Cryptool http://www.cryptool.com/ Accessed on 8 Feb 08.

2. Crowley, E,. “Information System Security Curricula Development”, Proceedings of the 4th conference on Information technology curriculum, October 16-18, 2003, Lafayette, Indiana, USA

3. IA Courseware Evaluation Program, http://www.nsa.gov/ia/academia/iace.cfm, Accessed on 8 Feb 08.

4. National Information Assurance Training Standard For Information Systems Security Officers, CNSSI 4014, Retrieved 8 Feb 08 from http://www.cnss.gov/Assets/pdf/cnssi_4014.pdf.

5. National Training Standard For Information Systems Security (Infosec) Professionals, NSTISSI No. 4011, Retrieved 8 Feb 08 from http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf.

6. Olejar, D., and Stanek, M., "Some Aspects of Cryptology Teaching," IFIP WG 11.8 1st World Conference on Information Security Education WISE1, 17-19 June 1999

7. OpenSSL http://www.openssl.org/ Accessed on 8 Feb 08.

Edward Crowley
Ed Crowley is an Instructional Associate Professor at the University of Houston. There, he has obtained NSA/CNSS certification for their Security Specialization. He holds multiple NSA security certifications. He has also earned the Certified Information Systems Professional (CISSP) certification. He is a graduate of the U.S. Army's Military Police Academy and is interested in security curriculum development.