Cyber Missions
Annotated Bibliography

PROFESSIONAL LEVEL

Dooley, John. *A Brief History of Cryptology and Cryptographic Algorithms.* New York: Springer Publishing. 2013.

- This text reviews the history of and struggle between the code writer (cryptologist) and code breakers (crypto-analyst) throughout history. The history of almost 2000 years of this relationship is examined and perspective of where it is headed is also included.

Francillon, Aurelien and Pankaj Rohatgi. *Smart Card Research and Advanced Applications*. Paper presented at 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013.

- This book is comprised of 17 papers related to security technologies and software. Cyber-attacks and information technologies countermeasures to prevent attacks.

Huang, Xinyl and Jianying Zhou. *Information Security Practice and Experience.* Presented at 10th International Conference ISPEC 2014, Fuzhou, China, May 5-8, 2014. (Lecture Notes in Computer Science/ Security and Cryptology).

- Composed of 36 submitted papers, this book reviews network, cloud and systems security. It also discusses digital and encrypted signatures as means to government and personal protect computer systems.

Mel, H. X. and Doris Baker. *Cryptography Decrypted.* New York: Addison-Wesley Professional Publishing. 2000.

- This book delivers its content in a manner that all levels of experienced computer professional can understand. Rich with content it allows the reader to being with basic concepts of cryptology and encryption and work through the topic to the more complex ideas. The appendix contains many mathematical concepts for those who wish for a more enlightened discussion.

Nguyen, Phong and Elizabeth Oswald. Advances in Cryptology- EUROCRYPT 2014. Presented at the 33rd International Conference on the Theory and Applications of Cryptographic Technics, Copenhagen, Denmark. (Lecture Notes in Computer Science/ Security and Cryptology).

- This book is comprised of 38 full papers related to cyber-analysis and encryption on multi-use computers.

Paar, Christof and Jan Pelzl, and others. *Understanding Cryptography: A Textbook for Students and Practitioners.* New York: Springer Publishing. 2011.

- Borrowing from math, computer science and engineering, this book provides a basis for the topic of cryptology. There are multiple examples and figures to help the reader understand the concepts.

Qin, Zhiguang, Hu Xiong and Guobin Zhu. *Ad Hoc Anonymous Signatures: States of the Art, Challenges and New Directions (Cryptology, Steganography and Data Security).* Hauppauge, New York: Nova Science Publishing, Inc. 2013.

- This text reviews the challenges and solutions to security of users in Ad Hoc systems. These systems rely upon others to wirelessly forward or "flood" information to the next without the use of routers, or other existing infrastructure.

Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms and Source Code in C.* New York: Wiley Publishing Co. 1996.

- This text provides the basic groundwork for an understanding of cryptology. As the reader moves through this text however, they will increase their understanding as the text also includes information on C code for the use in encryption for public domains.

UNDERGRADUATE/GRADUATE LEVEL

Barr, Thomas. *Invitation to Cryptology*. New York: Pearson Publishing. 2001.

- Written with a focus on mathematical formulas, this text provides readers topics including the theories necessary to write encrypted text.

Boone, J.J. *A Brief History of Cryptology*. Annapolis, MD: Naval Institute Press. 2005.

- This text provides a review how codes play a role in everyday lives in addition to its historic perspective of the topic. He specifically focuses on what he believes to be the future of cryptology based on military advances.

Callimahos, Lambros. *The Legendary William F. Friedman*. Washington, DC: National Security Agency. 2013.

- A bibliography of the former head of the Army's Signals Intelligence Service in the 1930s. Friedman is considered by many to be the "dean of American Cryptology".

Ferguson, Niels and Schneier. *Cryptography Engineering: Design Principles and Practical Applications.* New York: Wiley Publishing. 2010.

- This text spends a great deal of time stressing the importance of the "coder" trying to break their own codes. There are topics related to codes, mathematics, and key exchanges (transposition) as they are relevant to cryptology.

Cyber Missions
Annotated Bibliography

Hoffstein, Jeffrey and Pipher, Jill and others. *An Introduction to Mathematical Cryptology (Undergraduate Texts in Mathematics).* New York: Springer Publishing. 2008.

- This text is well-written and easy to read and understand. There is little higher order math comprehension necessary to absorb the content. This text could easily be used by entry level students to being concepts of public-key cryptology.

Johnson, Thomas. *American Cryptology during the Cold War*. Washington, DC: National Security Agency. 2013.

- A semi-annual publication that focuses on the history of United States cryptology from 1945 until 1960.

Klima, Richard and Neil Sigmon. *Cryptology: Classical and Modern Maplets (Discrete Mathematics and its Applications).* Boca Raton, FL: CRC Press. 2012.

- This text guides students with little mathematics experience through the process of creating codes through the use of a computer algebra system used to create Maplets.

Rothe, Jorg. *Complexity Theory and Cryptology*. New York: Springer Publishing. 2005.

- By stressing the inter-relationship, this text seeks to stress the importance of cryptology and complexity in systems theory. It is a suitable text for both graduate and undergraduate students who may have an interest in the topic. The multiple disciplines within the textbook makes it applicable for those students of engineering, computer sciences and math.

SECONDARY LEVEL

Blackwood, Gary. *Mysterious Messages: A History of Codes and Ciphers.* New York: Dutton Juvenile Publishing. 2009.

- This book provides an in-depth history of code –making and breaking. The history begins in Ancient Greece and moves to the present. There are plenty of examples of codes and multiple examples of codes that will allow the reader to create her own.

Cobb, Chey. *Cryptology for Dummies.* New York: Wiley Publishing. 2004.

- A very basic, beginner's guide to protection of information security. This text reviews a variety of topics including: encryption, public-key infrastructure and digital signatures, to name a few.

Forrest, Christopher. *Street Cryptography: A Quick and Dirty Way to Maintain Your Secret Conspiracy.* Christopher Forrest.

- Provides a guideline to creating one's own code and to assists in deciphering those that existing. The book also provides an historic overview of the topic.

Kahn, David. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York: Scribner Publishing Co. 1996.

- This book is purely for those who wish to learn and understand the history of cryptology. There is no mathematical explanation of the concepts or creation of codes. Although inclusive of other regions and histories of the world this text is mostly involved with the U.S and its codes making a breaking from WWII forward.

Lewand, Robert E., *Crpytological Mathematics*. Washington, DC: The Mathematical Association of America. 2000.

- This book begins with the simple mathematics of encryption and moves to the more complex. A basic understanding of algebra is necessary to grasp the text. Sample problems are provided at the end of each chapter to assure that the reader has an understanding of the concepts.

Lunde, Paul. *The Book of Codes: Understanding the World of Hidden Messages: An Illustrated Guide to Signs, Symbols, Ciphers and Secret Languages.* Richmond, CA: University of California Press. 2009.

- Rich with graphics this book provides a through overview of the history of cryptology. Unlike multiple other texts, this author begins his writing with a definition of what a code is comprised and what it is not. There are many examples of codes in society and the military.

Piper, Fred and Sean Murphy. *Cryptography: A Very Short Introduction*. Oxford: Oxford University Press. 2002.

- This text takes into account the historical political and social importance of cryptology. It provides a brief, but through overview of the topic without going into the depths of the mathematics concepts.

Singh, Simon. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptology*. New York: Anchor. 2000.

- This book provides a historically and enjoyable read about the history of codes and code breaking. Although the book focuses primarily on a social history of the machines and person involved in the evolution of cryptology, there is also a deeper perspective provided. In the several appendices the book provides an examination of the algorithms involved in processes of cryptology.

Cyber Missions
Annotated Bibliography

Wobst, Reinhard and Angelika Shafir. *Cryptology Unlocked*. New York: Wiley Publishing. 2007.

- This book provides an historic and current perspective on the importance of secure codes and code writing. It allows those with a background in encryption the opportunity to read additional materials related to the topic without delving into vast amount of mathematics.