Annotated Bibliography

Menezes, Alfred. *Handbook of applied cryptography*. Florida: CRC Press LLC, 1997.

Thicker than the CS200 Algorithms book, this text provides an extremely detailed introduction into all modern areas of cryptography. Like most cryptography books a mathematical background to probability, information theory, complexity theory, number theory, abstract algebra, and finite fields is given. This background is then used in specific number-theoretic problems. A particularly useful problem it covers is the factoring of polynomials over finite fields, a key component to the paper topic. The text proceeds to move into the application of these mathematical methods in cryptography. This application begins with pseudorandom numbers and sequences and how they are critical to modern cryptography. Ciphers are introduced as a foundation of applied cryptography and stream ciphers and block ciphers (relating to private and public cryptography, respectively) are covered, and explained in specific used cryptographic algorithms.

Savas, Erkay. *Finite Field Arithmetic for Cryptography*. IEE Circuits and Systems, 2010.

Wagstaff, Samuel. *Cryptanalysis of Number Theoretic Ciphers*. Florida: Chapman & Hall/CRC.

This small yet dense book covers a wide range of material regarding the area of cryptanalysis and its relation to cryptography. However, what sets this book apart is that it introduces cryptanalysis solely through its mathematical foundations. This is of extreme use to my topic since its focus is on on the mathematical foundations of cryptography. There is a chapter of the book dedicated to the use of groups, rings, and fields in the use of cryptographic algorithms. The mathematical use of Galois (or finite) fields is covered and how it can be used in cryptography. Later chapters integrate fields with other mathematical techniques such as factoring algorithms and elliptic curves. The book proceeds to discuss private key ciphers, and goes specifically in-depth into the AES and its implementation. Lastly, methods of attacks are covered, which include the cracking of cryptographic methods through the solving mathematical problems.

Wenbo, Mao. *Modern Cryptography: Theory and Practice*. New Jersey: Prentice Hall PTR, 2004.

The usefulness of this book comes from specific combination of mathematical theory and cryptographic practice. Algebraic foundations are introduced, focusing on the structure of finite fields, irreducible polynomials, primitive roots, and groups constructed using elliptical curves. Number theory is then given to bring further understanding to how these mathematical objects can are related and their special properties. These chapters serve as the “how” and “why” specific areas of mathematics are used in cryptography. These special properties then serve as the foundation for basic cryptographic techniques, which the book cover heavily. Though these techniques are no longer high-security, since analytic or computation solutions have been found, they are still incredibly useful in understanding where the current cryptographic algorithms came from. Another relevant portion of the book is the formal treatment of public cryptographic techniques and protocols. Unlike the chapter on basic techniques the techniques given here are nontrivial and are used in real world applications.

Wong, Kennith. *Applications of Finite Field Computation to Cryptology: Extension Field Arithemetic in Public Key Systems and Algebraic Attacks on Stream Ciphers.* Queensland University of Technology, 2003.