JOHNNA SMITH, Dept of Mathematics, Shepherd University, Shepherdstown, WV, 25443, and DONALD MILLS, Dept of Computer Sciences, Mathematics, and Engineering, Shepherd University, Shepherdstown, WV, 25443. Analysis of basic cryptographic concepts and recent open problems in hash function security.

The objectives of this study are to show an understanding of cryptographic concepts as well as highlight recent open problems involving hash function security. The method of study used included reading the first five chapters of *Cryptography: Theory and Practice* by Stinson and Paterson as well as a recent paper that outlined open problems in hash function security. Then, written reports were delivered on the information learned which included selected proofs and solved examples. The essentials of the opening report introduce the basic elements of cryptography: cryptosystems, cryptographic tools, message integrity, protocols, and security approaches. Chapter 2 of "Cryptography" describes various types of ciphers including Shift, Substitution, Affine, Vigenère, Hill, Permutation, and Stream Ciphers, as well as how to cryptanalyze them. The third report focuses on the One-time Pad, entropy, perfect security, and cryptographic security, specifically unconditional security, as introduced by Claude Shannon in his work on information theory. Throughout the fourth report, block and stream ciphers, including substitution-permutation networks, attacks such as linear and differential cryptanalysis, and modes of operation are discussed. In the fifth report, basic concepts of cryptography, hash function and message authentication are discussed, including iterated hash function, sponge construction, and unconditionally secure MACS. Using the information learned from the previous reports, current problems in hash functions were then researched. In conclusion, open problems in hash function security include collision resistance, preimage resistance, and resistant to length extension attacks. The project was sponsored by the NSF S-STEM Grant (DUE-2130267).