Survey on Mathematical Hard Problems Based Public-Key Cryptosystems

Mohammad Ahmad Alia

 ***Abstract*—**This paper summarizes the development in publickey encryption algorithms which are actually based on mathematical hard problems. In general, most of the currently used public-key encryption algorithms are computationally expensive with relatively lengthy key requirement due to the dependency on the number theory. Therefore, it’s important to show other public key encryption algorithms which are not based on number theory. In the surveyed algorithms, we present exemplified region of some public-key algorithms. Every public-key cryptosystem is based on a mathematical problem that is, in some sense, difficult to solve.  ***Keywords—***Cryptograph, Encryption, NP-Hard Problem, and Public-key*.* D. Johnson, A. Menezes, and S. Vanstone, “The Elliptic Curve Digital Signature Algorithm (ECDSA)”, Certicom Corporation, 2001.