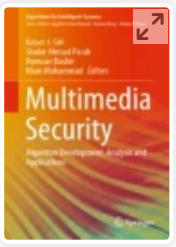

Multimedia Security pp 45–88

Impact of Computational Power on Cryptography

M. Iqbal Bhat & Kaiser J. Giri

Chapter | First Online: 12 January 2021

Part of the Algorithms for Intelligent Systems book series (AIS)

Abstract

From ancient times to modern digital era, one thing that never lost its importance is data. Extensive efforts have been made by people to protect and secure data. Advancements in computational technologies have provided many new ways to generate, process and utilize data, thus connecting technology with every sphere of human life. Adaptation of these new technologies has always been guaranteed and assured by the security procedures provided by cryptographic schemes. Same is true about multimedia which has

emerged as one of the most demanding and exciting inventions of technological era. Currently, almost entire population of world is living within the reach of mobile network with about 4.57 billion active Internet users regularly generating, processing and sharing multimedia content. The only tool securing them digitally is the cryptographic techniques. The security of almost all of the cryptographic schemes is based on some computational and mathematical assumptions. Each new advancement in computational technology results in profound impact on cryptographic world by challenging these computational and mathematical assumptions. Recent computational advancements have compromised security of many famous and widely used cryptosystems like DES by favoring the cryptanalyst tools. Increasing computational power favors brute-force solutions, and attacks which were once considered computationally infeasible have become feasible. Emerging technologies like cloud computing, mobile cloud computing (MCC), quantum computing, parallel computing together with the advancements of GPUs, CUDA, clustering of standard CPUs and FPGA-based computing have provided new ways to solve many problems like integer factorization problem (IFP), discrete logarithm problem (DLP), elliptic curve discrete logarithm problem (ECDLP) etc., which were previously considered intractable. This has also resulted in great impact on many cryptosystems. Utilization of growing computational power has also resulted in development of robust and secure cryptosystems. The time taken for encryption and decryption especially in case of