Chapter 3
A Review of Cryptographic Algorithms for the Internet of Things

Issmat Shah Masoodi
University of Kashmir, India

Bisma Javid
University of Kashmir, India

ABSTRACT

There are various emerging areas in which profoundly constrained interconnected devices connect to accomplish specific tasks. Nowadays, internet of things (IoT) enables many low-resource and constrained devices to communicate, do computations, and make smarter decisions within a short period. However, there are many challenges and issues in such devices like power consumption, limited battery, memory space, performance, cost, and security. This chapter presents the security issues in such a constrained environment, where the traditional cryptographic algorithms cannot be used and, thus, discusses various lightweight cryptographic algorithms in detail and present a comparison between these algorithms. Further, the chapter also discusses the power awakening scheme and reference architecture in IoT for constrained device environment with a focus on research challenges, issues, and their solutions.

DOI: 10.4018/978-1-5225-5742-5.ch003