Comparison of ECC and RSA algorithms in IOT devices

ABSTRACT

IoT is the evolution of the internet. Concerning tight communication between the individual and business, number of IoT nodes are rapidly increasing. Most of the services in IoT heavily rely on security mechanisms that pose security imperative for embedded devices in IoT. The failures in IoT can have severe results; consequently, the research toward security concerns are of extreme significance in IoT. Preserving the confidentiality and privacy, ensuring the availability of the services that are proposed by IoT ecosystem, assuring the safety of the assets in IoT like devices, data, infrastructures, and users, are the main objectives in IoT security. The significant issue that makes IoT devices vulnerable is the lack of an appropriate security mechanism to preserve data. Attackers can exploit these weaknesses to obtain access to valuable data. Hence, thoughtfully chosen and practically tested encryption algorithm must be performed to enhance the device efficiency and decrease the risk of sensitive data exposure. Understanding and comparing algorithms implemented in IoT devices, regarding performance discussed in this paper. RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptography) algorithms have been compared for identifying the most lightweight, secure, efficient implementation in IoT. Based on the findings, the ECC algorithm outperforms RSA in a constrained environment in terms of memory requirements, energy consumption, key sizes, signature generation time, key generation and execution time, and decryption time while RSA performs better in verifying the signature and encrypting.

Keyword: Elliptic Curve Cryptography; ECC; RSA; Internet of Things (IoT); Security Services