Paper ID: 52650
oral
student

26th IAA SYMPOSIUM ON SMALL SATELLITE MISSIONS (B4)
Generic Technologies for Nano/Pico Platforms (6B)

Author: Mr. Niranjan Dindodi Ramesh
R V College of Engineering, Bengaluru, India, niranjana.dr@gmail.com

Mr. Abeer Vaishnav
R V College of Engineering, Bengaluru, India, abeer.vaishnav13@gmail.com
Mr. SHASHANK SHRIVASTAVA
R V College of Engineering, Bengaluru, India, shashank0700@gmail.com
Ms. Samana H Managoli
R V College of Engineering, Bengaluru, India, samanahmanagoli@gmail.com
Ms. Ankitha Selvam
R V College of Engineering, Bengaluru, India, mys.ankitha@gmail.com
Mr. Deekshith Nayak
R V College of Engineering, Bengaluru, India, deekshithnayak1999@gmail.com

IMPLEMENTATION AND COMPARISON OF AES-RSA AND AES-ECC HYBRID ENCRYPTION SCHEMES FOR NANOSATELLITES

Abstract

The paper expounds the implementation of two hybrid encryption systems, an Advanced Encryption Standard (AES-128) with Rivest, Shamir, Adleman algorithm (RSA-2048) and AES-128 with Elliptic Curve Cryptography (ECC) in nanosatellites. Lightweight and impregnable encryption is the need of the hour for small satellites on account of increasing application of the same for fulfilling demands of communication and experimentation. The hybrid encryption techniques discussed in the paper will be implemented on RVSAT-1, a 2U nanosatellite hosting a biological payload for experimentation in space. The payload data thus obtained has to be sent to the ground station via the downlink when a line of sight is achieved. The security of this data from potential interceptors is of paramount importance as the payload data is immensely valuable. Hybrid encryption combines the swiftness of the symmetric encryption algorithm (AES-128) and the security of the asymmetric encryption algorithm (RSA or ECC). It altogether eliminates the vulnerability of the symmetric algorithm and slower execution time of the asymmetric encryption algorithm.

In the paper, the efficiency of the aforementioned hybrid cryptosystems is compared and analyzed, based on conventional encryption tests such as Chi-square test, entropy test, execution time and brute force attacks and it was found that the hybrid encryption of AES-128 along with ECC is the most optimal and lightweight algorithm for establishing secure downlink from nanosatellites.