UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

INSPEM WEEKLY SEMINAR

29/2018

Date & Time

7 September 2018 (Friday) @ 3.15 pm

Venue

**Al-Farabi Seminar Room,
Second Floor, INSPEM**

Presenter

Mr. Zahari Mahad

**Research Officer
Laboratory of Cryptography,
Analysis and Structure, INSPEM**

Topic

Enhanced AA_β Cryptosystem – A Comparative Analysis

Abstract

A major enhancement strategy of the AA_β cryptosystem is currently proposed which incorporates the Rabin-p decryption method upon its original design while maintaining the key generation and encryption procedures. Consequently, such strategy improved the decrytion procedure of the AA_β cryptosystem compare to any previously proposed design. In this paper, the aim is to provide a comparative analysis of the new design of the AA_β cryptosystem with the original and the other enhancement methods in existence. The scope of this work is a comparative analysis upon the decryption procedure only. The results show that the new design for the AA_β cryptosystem is efficient and faster in term of computational complexity and running time.

Keywords: AA_β Cryptosystem, Rabin-p Cryptosystem, Comparative Analysis, Internet of Things, Embedded System