UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

INSPEM WEEKLY SEMINAR

19/2019

Date & Time

Friday , 31 May 2019 @ 3.15 pm

Venue

Al-Farabi Seminar Room, Second Floor, INSPEM

Presenter

Dr. Muhammad Asyraf Asbullah
Associate Researcher
Laboratory of Cryptography, Analysis & Structure

Topic

Analysis of Rabin-p Key Encapsulation Mechanism - An Overview

Abstract

MySEAL is a project to develop a portfolio of national trusted cryptographic algorithms while AKBA MySEAL is new submitted algorithms or published algorithms not included in existing standards or other cryptographic algorithm listing projects. One of the cryptographic algorithms that have been considered as a candidate for national trusted cryptographic algorithms are the Rabin-p KEM, design and developed by INSPEM cryptography team members. In this session, a number of mathematical (crypt)analysis conducted upon the Rabin-KEM will be discussed.