UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

INSPEM WEEKLY SEMINAR

8/2018

Date & Time

2nd March 2018, Friday @ 3.15 pm

Venue

Al-Farabi Seminar Room, Second Floor, INSPEM

Presenter

Dr. Muhammad Asyraf Asbullalh
Associate Researcher
Laboratory of Cryptography, Analysis and Structure

Topic

On the Notion of Weak Keys for the RSA Type Cryptosystems.

Abstract

A class of weak keys is a notion that was also introduced by Alexander May in his doctoral thesis in 2003. Consider the RSA public keys (e, N), hence a weak key is one that hinted to the factorization of the modulus N via an efficient method using both e and N. Since then, several new classes of weak keys were introduced in the literature. This session surveys some of the existing results to date