UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

# INSPEM WEEKLY SEMINAR

06/2020

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

#UNSDG

**Date & Time**

**Monday, 3rd February 2020 @ 3.15 pm**

**Venue**

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

**Presenter**

**Prof. Dr. Abderrahmane Nitaj**
**University of Caen, France**

**Topic**

## Cryptanalysis of variants of the RSA cryptosystem

## Abstract

RSA is a prominent system in modern cryptography and has several variants such as CRT RSA, prime power RSA, elliptic curve RSA, and Edwards curve RSA. In this talk, we will consider specific variants of RSA and present an analysis of their security, in particular their resistance to cryptanalysis by algebraic and lattice methods.

**Key words**: RSA cryptosystem, Lattice reduction, Coppersmith method, elliptic curve, Edwards curve.