UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

INSPEM WEEKLY SEMINAR

02/2020

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

#UNSDG

Date & Time

Friday, 10th January 2020 @ 3.15 pm

Venue

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

Presenter

Dr. Muhammad Asyraf Bin Asbullah
Senior Lecturer,
Centre of Foundation Studies for
Agricultural Science

Topic

Random number generation, what can go wrong.

Abstract

The security of any cryptosystem or cryptographic algorithm is based on the assumption that its keys are generated randomly and secretly maintained by the user, according to Kerckhof's principle. However, the most troublesome (though important) part of cryptographic security is the generation of random numbers (let alone prime numbers). Randomness is the cryptographic security's hardest part. We will see why people deviate from ' a purely theoretical approach ' in this presentation and use modifications to produce random/prime numbers. Besides, we're going to see real-world examples of what can happen if Kerckhof's principle is not followed.