13/2020

UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

ONLINE
INSPEM'S WEEKLY SEMINAR

DATE : 22 MAY 2020 | TIME : 2.15 PM
APPLICATION : VIDEO CONFERENCE
The url will be given once the participant has confirmed attendance

DR. AMIR HAMZAH ABD GHAFAR

INSPEM CLASS OF 2020

CLICK HERE
TO REGISTER

Topic : Extending Pollard Class of Factorable RSA Modulus

ABSTRACT

RSA cryptosystem is a public-key cryptosystem that are widely utilized in securing our digital communication and transactions from being monitored by unwanted adversaries. One of the sources of security in RSA depends on the integer factorization problem or IFP. To be more precise, the hardness in factoring RSA modulus, N=pq where p and q are two large primes determines the security strength of RSA. However, an algorithm called Pollard's p-1 algorithm seems to undermine IFP by manipulating the structure of certain primes to factor N in feasible time. Hence, Pollard's algorithm is called a special-purpose factoring algorithm. In this talk, we discuss the outcome of Pollard's algorithm in the current cryptographic industrial standard, particularly the FIPS 180-4. We also discuss a new attack which extends the Pollard's p-1 method and show that the primes that are proven vulnerable to our attack may pass the current standard. Finally, we propose a countermeasure to avoid the weak primes being used in real-world implementation.

facebook.com/UniPutraMalaysia @uputramalaysia instagram.com/uniputramalaysia youtube.com/user/bppupm