37/2020

UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

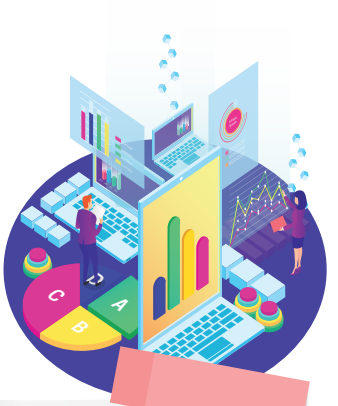
# INSPEM'S ONLINE
# WEEKLY SEMINAR

**DATE : 13 NOVEMBER 2020 | TIME : 3.15 PM**
**MEDIUM : VIDEO CONFERENCE (GOOGLE MEET)**
*https://meet.google.com/wvg-etio-equ*


## Dr. Normahirah Nek Abd Rahman

Senior Lecturer, Pusat GENIUS@Pintar Negara, UKM

INSPEM Class of 2017

CLICK HERE TO REGISTER

## Topic :Successful Factoring Directions upon the Modulus $N = p^2q$


## ABSTRACT

The RSA public key cryptosystem widely used in practical cryptographic systems due to its security and effective encryption and decryption implementation. To obtain higher implementation efficiency, RSA with specific parameters were adopted in practical applications including RSA with small encryption exponents aiming to achieve a very fast encryption operation and those with small decryption exponents to speed up decryption process. Meanwhile, many variants of RSA have also been proposed for instance to achieve a fast decryption implementation. This research focuses on the development of new approach to deal with the existing problems of the previous work for solving factorization problem. The effort to attain this is through the implementation of the modulus ulus $N=p^2q$. The first part the security and the difficulty level of factoring the modulus $N=p^2q$. As a result, four new cryptanalysis has been developed under certain conditions using continued fractions expansion to show that $N=p^2q$ can be factored in polynomial time consecutively together with an estimation number of weak exponents satisfying the generalized key equation. The second part concentrates on generating k moduli of the form $N_i=p_i^2 q_i$ for some of the generalized key equations with the goal to factor the modulus $N=p^2q$. Thus, the some attacks has been developed to compute the prime factors $p_i$ and $q_i$ of the module of the form $N_i=p_i^2 q_i$ in polynomial time with some restriction on some parameters. All the proposed attacks prove that after transforming the generalized key equations into simultaneous Diophantine approximation and then applying LLL algorithm to find suitably small parameters lead to factor moduli of the form $N_i=p_i^2 q_i$ simultaneously.


#UNSDG