

Table of Contents

A Fast and Efficient Design for AA_β Cryptosystem	1
Muhammad Asyraf Asbullah, Muhammad Rezal Kamel Ariffin & Zahari Mahad	
New Cryptanalysis of Multiple Moduli $N_i = p_i^2 q_i$ Using Good Approximation of $\phi(N_i)$	17
Normahirah Nek Abd Rahman, Muhammad Rezal Kamel Ariffin, Muhammad Asyraf Asbullah & Faridah Yunos	
Extending Pollard's $p - 1$ Class of Weak Primes and Its Application on RSA	33
Amir Hamzah Abd Ghafar, Muhammad Rezal Kamel Ariffin & Muhammad Asyraf Asbullah	
Evaluation Criteria on Ambience-Based True Random Number Generators	54
Nur Azman Abu, Shekh Faisal Abdul Latip & Shahrin Sahib	