Analysis on the Rabin-p cryptosystem

ABSTRACT

This paper presents an analysis toward estimating the algorithm running time on the Rabin-p cryptosystem. Next, we evaluate the memory cost for system parameters and accumulators for the Rabin-p encryption and decryption procedure, respectively. We then conduct a comparative analysis between three Rabin-like cryptosystems, namely the Rabin-p, the Rabin-Takagi and the HIME(R) cryptosystem. In summation, we conclude that Rabin-p cryptosystem performs faster and used less storage in comparison to the other two Rabin-like cryptosystems in consideration.

Keyword: Rabin-p cryptosystem; Running time; Storage