

## **AA $\beta$ public-key cryptosystem - a practical implementation of the new asymmetric**

### **ABSTRACT**

This paper aims to provide a practical implementation one of a probabilistic cipher proposed by M.R.K. Ariffin, M.A. Asbullah and N.A. Abu called as AA $\beta$ . We provide details on designing and implementing the AA $\beta$  algorithm. Furthermore, to support our understanding by providing a statistical analysis of times taken to implement the key generation, encryption and decryption algorithm for the key sizes 3072, 6144, 9216 and 12288 bits for message spaces of  $4n$  where  $n = 512, 1024, 1536$  and  $2048$  bits. We show the working of the AA $\beta$  algorithm purely from a practical standpoint to justify if it is practically implementable even for large data sets operating on large key sizes.

**Keyword:** Probabilistic cipher; Public key cryptosystem; AA $\beta$  public key cryptosystem.