AAβ public key cryptosystem - a comparative analysis against RSA and ECC

ABSTRACT

This paper aims to provide a comparative analysis between probabilistic and deterministic security models. We provide a benchmark by practically implementing and comparing three ciphers - AAɓ, RSA and ECC. This paper provides the algorithms to implement these ciphers as well as highlights the operating time and performance for varying key sizes of 128/1024/3072, 160/2048/6144 and 192/4096/12288 bits. We target our implementation to justify if the probabilistic model - AAɓ, can perform equivalently against deterministic models so as to be considered to be used in practical scenarios today.

Keyword: AAɓ cryptosystem; Cipher implementation; Comparative analysis; Probabilistic cipher; Public-key cryptosystem