A survey of partial key exposure attacks on RSA cryptosystem

ABSTRACT

In today's digital world, RSA cryptosystem is regarded as the most widely deployed public-key cryptosystem on digital machines that compute cryptographic processes. It secures the sensitive data that are either transmitted via internet or at rest in the computing machines. It utilizes integer factoring problem which is essentially one of the unsolved number theoretic problem. Due to its vital functionality, RSA is confronted by cryptanalysis or 'attacks' to which define a higher benchmark of its security level. In this paper, we survey the established partial key exposure attacks on RSA. The attacks assume that an adversary employs an incomplete arrangements of bits of the RSA private keys. The methods used in the attacks manipulate mathematical structures of the keys.