

# Document details

1 of 1


 Export
  Download
  Print
  E-mail
  Save to PDF
  Add to List
  More... >

Journal of Theoretical and Applied Information Technology

Volume 61, Issue 1, March 2014, Pages 37-43

Open Access

## Cryptanalytic attacks on Rivest, Shamir, and Adleman (RSA) cryptosystem: Issues and challenges (Article)

Abubakar, A.<sup>a</sup> , Jabaka, S.<sup>b</sup> , Tijjani, B.I.<sup>c</sup> , Zeki, A.<sup>a</sup> , Chiroma, H.<sup>d</sup> , Usman, M.J.<sup>e</sup> , Raji, S.<sup>a</sup> , Mahmud, M.<sup>a</sup> 

<sup>a</sup>Department of Information Systems, Kulliyah of Information and Communication Technology, International Islamic University, Malaysia

<sup>b</sup>Department of Computer Science, Federal College of Education(Technical) Gusau, Zamfara, Nigeria

<sup>c</sup>Department of Physics, Bayero University Kano, Nigeria

View additional affiliations >

### Abstract

[View references \(25\)](#)

RSA cryptosystem is an information security algorithm used for encrypting and decrypting of digital data in order to protect the content of the data and to ensure its privacy. Prior research studies have shown that RSA algorithm is very successful in protecting enterprises commercial services and systems as well as web servers and browsers to secure web traffic. In an email application, it's utilized to ensure the privacy and authenticity of email message. Some studies have also shown the efficiency of RSA algorithm in securing remote login sessions, and electronic credit-card payment systems. Generally RSA algorithm gain a security support because of it's frequently use in most applications where security of digital data is mostly a concern. Its strength lies with its ability of withstanding many forms of attacks. While many studies focus on proving that RSA algorithm is breakable under certain cryptanalytic attacks, yet there are some confrontations on the circumstances of applying those attacks. This paper presents the issues and challenges on some key aspects of cryptanalytic attacks on RSA algorithm. The paper also explores the perceived vulnerabilities of implementing RSA algorithm which can render a cryptanalyst easier means of attack. © 2005 - 2014 JATIT & LLS. All rights reserved.

### Author keywords

[Cryptanalysis](#)
[Cryptanalytic attacks](#)
[RSA cryptosystem](#)

ISSN: 19928645

Source Type: Journal

Original language: English


Document Type: Article


Publisher: Asian Research Publishing Network (ARPN)

### Metrics

[View all metrics >](#)

2  Citations in Scopus  
50th Percentile

0.68  Field-Weighted Citation Impact

 PlumX Metrics  
Usage, Captures, Mentions, Social Media and Citations beyond Scopus.

### Cited by 2 documents

A comprehensive literature review of asymmetric key cryptography algorithms for establishment of the existing gap

Gaithuru, J.N. , Bakhtiari, M. , Salleh, M. (2016) 2015 9th Malaysian Software Engineering Conference, MySEC 2015

Randomized text encryption: A new dimension in cryptography

Memon, J. , Abd Rozan, M.Z. , Uddin, M. (2014) International Review on Computers and Software

[View all 2 citing documents](#)

Inform me when this document is cited in Scopus:

