



SRI RAMAKRISHNA
COLLEGE OF ARTS & SCIENCE (Autonomous)
(FORMERLY SNR SONS COLLEGE)
Avinashi Road, Nava India, Coimbatore - 641 006.



Proceedings of 4th International Conference on

INTELLIGENT COMPUTING AND TECHNOLOGY

ICICT '24

ORGANIZED BY
DEPARTMENT OF INFORMATION TECHNOLOGY

*March, 13
2024*

**Proceedings of the International Conference on
INTELLIGENT COMPUTING AND TECHNOLOGY**

ICICT - 2024

13th March 2024

Chief Editor

Dr. N. Sumathi

Editors

Mr. A. Sunil Samson

Mrs. S. Kiruthika

Organized By



**Department of Information Technology
Sri Ramakrishna College of Arts & Science
Coimbatore-641006
www.srcas.ac.in**



All Rights Reserved.

Original English Language edition © Copyright by **Coimbatore Institute of Information Technology.**

This book may not be duplicated in any way without the express written consent of the Publisher, except in the form of brief excerpts or quotations for the purpose of review. The information contained herein is for the personal use of the reader and may not be incorporated in any commercial programs, other books, database or any kind of software without written consent of the publisher. Making copies of this book or any portion thereof for any purpose other than your own is a violation of copyright laws.

This edition has been published by **Coimbatore Institute of Information Technology, Coimbatore.**

Limits of Liability/Disclaimer of Warranty: The author and publisher have used their effort in preparing this proceedings and author makes no representation or warranties with respect to accuracy or completeness of the contents of this book, and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. There are no warranties which extend beyond the description contained in this paragraph.

No warranty may be created or extended by sales representatives or written sales materials. Neither CiiT nor author shall be liable for any loss of profit or any other commercial damage, including but limited to special, incidental, consequential or other damages

Trademarks: All brand names and product names used in this book are trademarks, registered trademarks, or trade names of their respective holders.



ISBN - 978-93-6126-491-7

Coimbatore Institute of Information Technology,

#156, 3rd floor, Kaliadas Road, Ramnagar,

Coimbatore – 641009, Tamil Nadu, India.

www.ciitreasearch.org

Phone: 0422-4377821

24	REVOLUTIONIZING GLOBAL HEALTH WITH AI IN HEALTHCARE INNOVATIONS Dr. P. Dhanalakshmi, Dharshini. A	147
25	ENHANCING MENTAL WELL-BEING: A MULTI-FACETED APPROACH TO STRESS RELIEF IN THE 'STRESS RELIEF RECOVER' MOBILE APP Dr. A. Jeyalakshmi, N. Nishanth, N. Alagusundram	151
26	A SURVEY ON MOBILE APPLICATIONS AND THEIR GLOBAL IMPACT Dr. K. Vembandasamy, Dinesh. P, Nithishkumar. R	155
27	ALZHEIMER ASSISTANT: A MOBILE APPLICATION USING MACHINE LEARNING Dr. M. Sridhar, Mr. R. Sankaran	163
28	NAVIGATING THE WORLD OF WEB SERVICES, A SURVEY OF TRENDS AND TECHNOLOGIES G. Vishnudass, Dr. M. Sridhar	169
30	STRATEGIES FOR OPTIMIZING LOW POWER IN VLSI SYSTEM DESIGN: A COMPREHENSIVE ANALYSIS OF NETWORK SENSORS Dr. M. Thamarai selvan, M. Prasannakumar	183
31	SMART SHOPPING TROLLEY USING RFID BASED ON IOT Dr. K. Vembandasamy, Aishwarya. R	191
32	IMPLEMENTATION OF DENSELY CONNECTED CONVOLUTION NEURAL NETWORK FOR DIAGNOSIS OF GLAUCOMA USING FUNDUS IMAGES OF EYE N. Sanjay Kumar, Dr. A. Jeyalakshmi, S. Deepak Prakash	195
33	BORDER ALERT SYSTEM USING IOT Baby. S, S. Karthik	207
34	ANALYSIS OF TRADITIONAL WITH CONVENTIONAL RSA S. Nirmala Devi, Dr. M. Ganaga Durga	214
35	AN AI BASED ACCIDENT DETECTION SYSTEM WITH CCTV J. Sakthi Devi, R. Sanjay Kumar, A. Sunil Samson	220
36	EMOTION DETECTION AND FACE RECOGNITION FOR ATTENDANCE MONITORING USING MACHINE LEARNING S. Deepak Prakash, Dr. A. Jeyalakshmi, N. Sanjay Kumar	227
37	MEDICARE APP FOR ENHANCED HEALTHCARE SUPPORT FOR LITERATE PEOPLE Dr. K. Vembandasamy, Dinesh. P, Nithishkumar. R	234

ANALYSIS OF TRADITIONAL WITH CONVENTIONAL RSA

S. Nirmala Devi¹, Dr. M. Ganaga Durga²

¹Research Scholar, Assistant Professor, ²Research Supervisor,

¹Department of Computer Applications (UG), ²Department of Computer Applications,

¹Fatima College, ²Sri Meenakshi Government Arts College for Women(A), Madurai, India.

¹s.nirmaladeviap@gmail.com. ²mgdurga@yahoo.com

Abstract---During the implementation of any cryptography algorithm, it is important to consider about the computational aspect of the algorithm for the encryption and decryption process. This paper analyses the traditional and conventional RSA algorithms based on its encryption speed and decryption speed. The traditional RSA algorithm was compared with many of the other public key algorithms in various papers. But in this paper it is compared with an improved version of RSA. This improved version is proved with the help of following metrics like plain text size and key size with encryption time and decryption time. This proposed work is doing the encryption and decryption process as fast as the traditional RSA algorithm. This proposed work can be implemented for the encryption and decryption of data in strict source routing of Ad-hoc network.

Keywords---Asymmetric Encryption, Public Key Algorithm, Traditional RSA, Conventional RSA, Computational Aspects, Strict Source Routing

1. INTRODUCTION

A. Traditional RSA

This Asymmetric encryption (Public key encryption) is a form of cryptosystem in which encryption and decryption are performed using the different keys, a public key and a private key. It is also known as public-key encryption. Asymmetric encryption transforms plaintext into ciphertext using one of two keys and an encryption algorithm. Using the paired key and a decryption algorithm, the plaintext is recovered from the ciphertext. Asymmetric encryption can be used for confidentiality, authentication, or both. The most widely used public-key cryptosystem is RSA. The difficulty of

attacking RSA is based on the difficulty of finding the factors of a prime number [1].

A public-key encryption scheme has six ingredients. [1]

Plaintext: This is the readable message or data that is fed into the algorithm as input.

Encryption algorithm: The encryption algorithm performs various transformations on the plaintext.

Public and private keys: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.

Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.

Decryption algorithm: This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

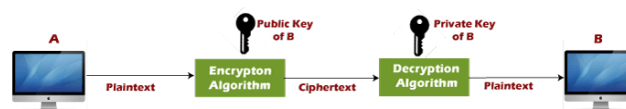


Figure 1. RSA Encryption with Public Key



Figure 2. RSA Encryption with Private Key

The essential steps are the following.