



NALBARI COMMERCE COLLEGE, NALBARI

Japarkuchi, P.O: Chowk Bazar, Nalbari, Assam - 781334

**Submitted on partial fulfillment for the three years
Degree Course**

Bachelor of Vocational (RMIT)

Of

GAUHATI UNIVERSITY

A PROJECT REPORT

ON

"DIGITAL SIGNATURE"

ACADEMIC GUIDE:

**Dr. DEVAJIT MAHANTA
Asstt. Professor & HoD
Dept. of B.VOC (IT)
N.C.C, Nalbari**

SUBMITTED BY:

**HIMANGSHU KALITA
Reg. No: 21069031
Roll No: UA-211-200-0022
B.Voc (RMIT)**



Nalbari Commerce College

Japarkuchi, P.O- Chowk Bazar, Nalbari, Assam-781334

CERTIFICATE OF GUIDANCE

This is to certify that **HIMANGSHU KALITA**, Roll Number UA-211-200-0022, Registration Number 21069031, a student of the sixth semester in the Department of B.Voc (RMIT) at Nalbari Commerce College, Nalbari, has successfully completed his project titled "**Digital Signature**" under my guidance.

Throughout the duration of the project, **HIMANGSHU KALITA** exhibited diligence, dedication, and a profound understanding of the subject matter. His commitments to excellence and willingness to learn have been commendable.

I wish him success in life.

Dr. DEVAJIT MAHANTA
Asstt. Professor & HoD
Dept. of B.VOC (IT)
Nalbari Commerce College

ACKNOWLEDGEMENT

I extend my sincere gratitude to all those who have contributed to my journey of understanding and working with digital signatures throughout the course of this project. It is with immense appreciation that I acknowledge the invaluable support and guidance I have received from various individuals and resources.

*I, **HIMANGSHU KALITA**, roll number **UA-211-200-0022**, registration number **21069031**, a student of the Department of B.Voc (RMIT), in the sixth semester, have only studied, understood, experimented, and utilized digital signatures in the execution of this project on digital signatures.*

*I am deeply grateful to my guide, **Dr. DEVAJIT MAHANTA**, Assistant Professor of the Department of B.Voc (IT), whose expertise, encouragement, and insightful feedback have been pivotal in shaping my understanding and implementation of digital signatures.*

Furthermore, I would like to express my appreciation to my fellow students and colleagues for engaging in meaningful discussions and providing assistance whenever needed.

Lastly, I am thankful to my family and friends for their unwavering support and understanding throughout this endeavor.

Once again, I express my heartfelt thanks to all those who have been a part of my journey in understanding and working with digital signatures.

Sincerely,

Himangshu Kalita

HIMANGSH KALITA

Roll No: **UA-211-200-0022**

Reg. No: **21069031**

Dept. of B.Voc (RMIT)

Table of Contents

1. Abstract.....	(1)
2. Introduction.....	(2)
3. Information Technology Act.....	(3)
4. Objectives.....	(4)
Ensuring the Security and Integrity of Digitally Signed Documents	
Providing a User-Friendly Interface for Signing and Verifying Documents	
5. Aims of the project.....	(5)
Environmental Sustainability	
Security Enhancement	
Ease of Maintenance	
Adherence to Standards	
6. Methodology.....	(7-9)
Test Plan Development	
Functional Testing	
Performance Testing	
Documentation Validation	
Validation Against Standards	
Data Integrity Testing	
7. Digital Signature Overview.....	(10-11)
What is a Digital Signature?	
How Does a Digital Signature Work?	
Key elements of a digital signature process	
Why Digital Signatures Matter	
Applications of Digital Signatures	
8. Technologies Used.....	(12-14)
Cryptographic Algorithms	
Hash Functions	
Cryptographic Libraries	
User Interface (UI) Technologies	
Database Technologies	
Programming Languages	

Digital Certificate Management
Security Protocols
Operating Systems
Cloud Services
Mobile Development Frameworks
Block chain Technology
Biometric Technologies

9. System Architecture.....(15-17)

High-Level Components
Communication Channels
Cryptographic Operations
Security Measures
Scalability and Redundancy
Integration and Interoperability
User Experience (UX)
Compliance and Legal Aspects
Performance Optimization

10. Implementation.....(18-20)

Coding and Development
Digital Signature Module
User Interface (UI)
Key Management
Database Integration
Security Features
Testing
Deployment
Integration
User Training
Documentation
Compliance and Legal Aspects
Monitoring and Maintenance
User Support
Post-Implementation Review

11. Digital signature generation.....	(31-36)
12. Digital Signature Verification and Validation.....	(37-40)
The Digital Signature Algorithm (DSA)	
Selection of Parameter Sizes and Hash Functions for DSA	
DSA Domain Parameters	
Domain Parameter Generation	
Domain Parameter Management	
Key Pairs	
DSA Key Pair Generation	
Key Pair Management	
DSA Per-Message Secret Number	
The RSA Digital Signature Algorithm	
RSA Key Pair Generation	
Key Pair Management	
Assurances	
The Elliptic Curve Digital Signature Algorithm (ECDSA)	
ECDSA Domain Parameters	
Domain Parameter Generation	
Domain Parameter Management	
Private/Public Keys	
Key Pair Generation	
Secret Number Generation	
ECDSA Digital Signature Generation and Verification	
APPENDIX A: Generation and Validation of FFC Domain Parameters	
Generation of the FFC Primes p and q	
Generation and Validation of Probable Primes	
13. Validation of the Probable Primes p and q.....	(41-42)
14. Generation of the Probable Primes p and q.....	(43-44)
15. Validation of the Probable Primes p and q.....	(45-48)
Generating DSA Primes	
Generating Primes for RSA Signatures	
16. Conclusion.....	(49)