



# Nalbari Commerce College

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



## DIGITAL SIGNATURE

**MAINUL ALI**

Reg. No: 21069036

Roll No: UA-211-200-0027

Semester: 6<sup>th</sup>

Dept. of B.Voc (RMIT)

Nalbari Commerce College, Nalbari



# **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:**

**MAINUL ALI**  
**Reg. No: 21069036**  
**Roll No: UA-211-200-0027**  
**B.Voc (RMIT)**



# **Nalbari Commerce College**

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

## **CERTIFICATE OF GUIDANCE**

This is to certify that **MAINUL ALI**, Roll Number UA-211-200-0027, Registration Number **21069036**, 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, **MAINUL ALI** 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, **MAINUL ALI**, roll number **UA-211-200-0027**, registration number **21069036**, 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,*

**Signature valid**

Digitally Signed  
Signed by: MAINUL ALI  
Reason: Project Report Signed  
Location: N.C.C, Nalbari  
Date: 08-Apr-2024 11:24:08

**MAINUL ALI**

Roll No: **UA-211-200-0027**

Reg. No: **21069036**

Dept. of B.Voc (RMIT)



# Table of Contents

<b>1. Abstract.....</b>	<b>(1)</b>
<b>2. Introduction.....</b>	<b>(2)</b>
<b>3. Information Technology Act.....</b>	<b>(3)</b>
<b>4. Objectives.....</b>	<b>(4)</b>
Ensuring the Security and Integrity of Digitally Signed Documents	
Providing a User-Friendly Interface for Signing and Verifying Documents	
<b>5. Aims of the project.....</b>	<b>(5)</b>
Environmental Sustainability	
Security Enhancement	
Ease of Maintenance	
Adherence to Standards	
<b>6. Methodology.....</b>	<b>(7-9)</b>
Test Plan Development	
Functional Testing	
Performance Testing	
Documentation Validation	
Validation Against Standards	
Data Integrity Testing	
<b>7. Digital Signature Overview.....</b>	<b>(10-11)</b>
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	
<b>8. Technologies Used.....</b>	<b>(12-14)</b>
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

<b>11. Digital signature generation.....</b>	<b>(21-26)</b>
<b>12. Digital Signature Verification and Validation.....</b>	<b>(27-40)</b>
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	
<b>13. Validation of the Probable Primes <math>p</math> and <math>q</math>.....</b>	<b>(41-42)</b>
<b>14. Generation of the Probable Primes <math>p</math> and <math>q</math>.....</b>	<b>(43-44)</b>
<b>15. Validation of the Probable Primes <math>p</math> and <math>q</math>.....</b>	<b>(45-48)</b>
Generating DSA Primes	
Generating Primes for RSA Signatures	
<b>16. Conclusion.....</b>	<b>(49)</b>