SYNOPSIS

Report on

# DIGITAL SIGNATURE CRYPTOGRAPHY

By

Akarsh Mishra-Roll No.2200290140016

Session:2023-2024 (III Semester)

Under the supervision of

Ms. Divya Singhal (Assistant Professor)

KIET GROUP OF INSTITUTIONS, Delhi-NCR, Ghaziabad



DEPARTMENT OF COMPUTER APPLICATIONS

KIET GROUP OF INSTITUTIONS, DELHI-NCR,

GHAZIABAD-201206

(2023-2024)

# 

# ABSTRACT

Elliptic Curve Digital Signature Algorithms (ECDSA) have recently come into strong consideration, particularly by the standards developers, as alternatives to established standard cryptosystems such as the integer factorization cryptosystems and the cryptosystems based on the discrete logarithm problem. Crypto algorithms are always the most important core tool in security applications. The elliptic curve-based digital signature algorithms were implemented in this study using the open-source software from GNU's Not Unix (GNU) Compiler collection version 3.4.4-1 (2005). The introduction of Cygwin version 1.5.18-1 (2005) release into this study, also enable users of Microsoft windows to make use of the software. ECDSA was examined and the main reason for the attractiveness of elliptic curve cryptography was brought out in the fact that there is no sub-exponential algorithm so far known to solve the elliptic curve discrete logarithm problem on a properly chosen elliptic curve. Hence, it takes full exponential time to solve while the best algorithms known for solving the underlying integer factorization and discrete logarithm problem both take sub-exponential time. The ECDSA have a smaller key size, which leads to faster computation time and reduction in processing power, storage space and bandwidth. This makes ECDSA ideal for constrained environments such as pagers, cellular phones and smart cards.

# CONTENTS

1. Introduction Of Project
2. Literature Review
3. Objective Of the Project
4. Research Methodology
5. Project Outcome
6. Proposed Time Duration 7. References

# 1.INTRODUCTION

Cryptography is a multifaceted field that revolves around securing communication in the presence of potential adversaries. Its primary goal is to develop and analyse protocols that safeguard information shared between entities, ensuring that malicious third parties cannot access it. This practice is essential for various aspects of information security.

One of the central principles of modern cryptography is data confidentiality, which involves restricting access to information through confidentiality agreements or rules. Data integrity is another critical aspect, ensuring that data remains accurate and consistent throughout its lifecycle. Authentication is the process of verifying that the claimed user corresponds to the data, while non-repudiation ensures that parties cannot deny the authenticity of their signature or message sending in contracts or communications.

Digital signatures serve as the cornerstone of message authentication in the realm of public-key cryptography. They bind individuals or entities to digital data, allowing independent verification by receivers and third parties. In practical scenarios, recipients require assurance that a message originates from the claimed sender and cannot be repudiated, making digital signatures vital for businesses where disputes over exchanged data are common. Digital signatures offer higher security than other electronic signature forms, enhancing transparency in online interactions and fostering trust among stakeholders. These signatures rely on mathematical techniques to validate the authenticity and integrity of digital content, acting as a more secure alternative to handwritten signatures or seals. They address the challenges of tampering and impersonation in digital communications.

Digital signatures also provide evidence of origin, identity, and the status of electronic documents, transactions, or messages. In numerous countries, including the United States, digital signatures hold the same legal weight as traditional handwritten signatures on documents. Blockchain technology, known for underpinning cryptocurrencies like Bitcoin, Ethereum, and Litecoin, relies on public-key cryptography to protect user accounts from unauthorized access. Public and private keys enable encryption and verification of messages, ensuring message authority and detecting alterations caused by adversaries.

In summary, cryptography is instrumental in securing communication and data in the digital age, with digital signatures playing a crucial role in verifying authenticity and integrity. Moreover, blockchain technology relies on cryptographic principles to safeguard user accounts and maintain the integrity of transactions in the realm of cryptocurrencies and beyond.

# 2.LITERATURE REVIEW

## 2.1. Introduction

The Digital Signature Project is a comprehensive endeavour aimed at harnessing the power of cryptographic technology to enhance the security and trustworthiness of digital communications and transactions. This project delves into the multifaceted world of cryptography, emphasizing the pivotal role of digital signatures as a means to validate the authenticity and integrity of digital data. By exploring the principles of data confidentiality, integrity, authentication, and non-repudiation, this initiative seeks to establish a robust framework for secure communication in the presence of potential adversaries. Furthermore, the project extends its focus to the application of digital signatures in real-world scenarios, particularly in business applications, where the prevention of disputes over exchanged data is paramount. Additionally, it explores the integration of digital signatures into emerging technologies like blockchain, showcasing their indispensable role in safeguarding accounts and transactions in the digital realm.

## 2.2. Historical Overview

The history of digital signatures spans several decades, marked by technological milestones and the evolution of cryptographic techniques. In the 1970s, public-key cryptography, introduced by Diffie and Hellman, laid the foundation. The RSA algorithm, developed by Rivest, Shamir, and Adleman in 1977, became pivotal for digital signatures.

The 1980s saw the emergence of the Digital Signature Standard (DSS) by NIST, with the adoption of the Digital Signature Algorithm (DSA) in 1991. By the 1990s, digital signatures gained recognition in governments and businesses, leading to legislation and legal recognition in various countries.

The early 2000s witnessed widespread adoption, particularly in e-commerce, online banking, and secure email communication. Standardization efforts resulted in XML Digital Signatures (XMLD Sig) in 2000, providing a universal format. Advancements in cryptographic techniques, such as Elliptic Curve Cryptography (ECC), improved efficiency and security. In the 2010s, blockchain technology integrated digital signatures, enhancing trust and integrity in transactions.

Today, digital signatures are legally binding in many countries and industries, serving as a standard for secure authentication, document signing, and data integrity. This historical journey reflects the continuous pursuit of secure methods to authenticate digital content and transactions, shaping the modern digital landscape.

## 3.OBJECTIVE OF PROJECT

This project has been developed keeping in view the security features that need to be implemented in the networks following the fulfilment of these objectives:

* To develop an application that deals with the security threats that arise in the network.
* To enable the end-users as well as the organizations come out with a safe messaging communication without any threats from intruders or unauthorized people.

To deal with the four inter-related areas of network security namely Secrecy, Authentication, Nonrepudiation, and Integrity

Digital signatures work by proving that a digital message or document was not modified—intentionally or unintentionally—from the time it was signed. Digital signatures do this by generating a unique hash of the message or document and encrypting it using the sender’s private key. The hash generated is unique to the message or document, and changing any part of it will completely change the hash.

Once completed, the message or digital document is digitally signed and sent to the recipient. The recipient then generates their own hash of the message or digital document and decrypts the sender’s hash (included in the original message) using the sender’s public key. The recipient compares the hash they generate against the sender’s decrypted hash; if they match, the message or digital document has not been modified and the sender is authenticated.

Source authentication ‘can be achieved by Digital signatures in cryptography. Researchers have proposed many digital signatures to achieve authentication. A method that allows a group member to make sign on a message on behalf of the group anonymously, is known as Group signature scheme (GSS). This concept was firstly introduced by David Chaum in 1991.

## 4.Project Methodology

Developing a digital signature project involves a structured methodology to ensure the successful implementation of digital signature technologies. Below is a high-level methodology for a digital signature project:

1. Project Initiation: Identify key stakeholders, including users, legal teams, IT staff, and management, and determine their needs and expectations.
2. Requirements Analysis: Ensure that the project adheres to relevant industry regulations and legal standards governing digital signatures.
3. Technology Selection: Choose the appropriate digital signature technology or solution based on the project's requirements. Evaluate different options, such as public-key infrastructure (PKI) systems or thirdparty digital signature services.
4. System Design: Ensure that the digital signature system integrates seamlessly with existing software, applications, and workflows.

5.Security Considerations: Implement robust security measures to protect digital signatures and associated data. This includes encryption, access controls, and secure storage practices.

Establish Key Management: Define procedures for the generation, distribution, and revocation of digital signature keys.

## 5.Outcome of Project

The project is confined to the intranet in an organization. This application makes sure that security services such as secrecy, authentication, integrity, and non-repudiation are provided to the communicating parties. Digital signatures create a virtual fingerprint that is unique to a person or entity and are used to identify users and protect information in digital messages or documents.

In the Future, Digital Signatures Will Play an Integral Role in Helping to Secure Electronic Commerce. Ecommerce is the act of selling, buying, and exchanging goods and services over an electronic network, for instance, the internet. There has been a constant need for data security during the transmission of sensitive information. Due to the e-commerce and online banking boom, companies needed to secure their networks to gain confidence in customers. This has led to greater and faster rate of adoption rates of digital signatures, which act as the sender's personal seal of authenticity over any electronic document.

With the evolution of technology, the way of executing documents has also evolved. With the increasing demand for modern, convenient methods for entering binding transactions, electronic agreements and digital signatures have gained a lot of momentum in recent years. Such developments have significantly changed how these transactions are entered and the execution processes.

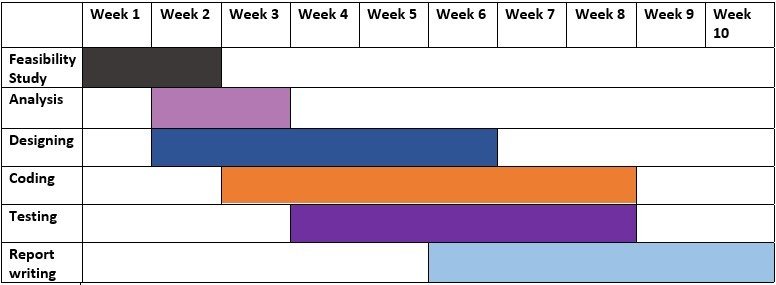
Younger consumers have also been a driving force behind the rise in digital signatures in the financial services industry. Various Gen Z and Millennials across the world have signed financial documents, such as

opening a bank account, loan agreement, investment, wealth management, mortgage agreements during the pandemic, which has resulted in a burgeoning of digital signature demand. Also, government agencies, like the DMV and immigration, have also provided more e-signature support for the critical documents.

With the outbreak of COVID-19, the digital signature market is anticipated to exhibit a positive growth rate due to the rise in remote working that has shifted the focus from relying on paper-based documentation and increasing digitalization of the transaction process. Enterprises are seeking business methods that are seamless and efficient and can be done from anywhere. Enterprises are also considering taking document processes online.

## 6. Proposed Time Duration

Gantt chart



* Feasibility Study: We have decided 2 weeks for feasibility study and requirement gathering for that we can analysis our capabilities and resources.

* Analysis: From 2 to 3 week, we proposed our self for esteem analysis of software requirements and risk and resource management.

* Designing: In this phase (from 2 week to 6 week) we will focus on designing the blueprint of software and tries to focus on coding part also.

* Coding: Form week 3" to week 8, we focus on coding part and tries to follow predeveloped prototype of software.

* Testing: Testing is not a part of only testing phase hence testing will be applied through each phase of software development life cycle.

* Report Writing: During the process of developing project (software) we will constantly writes report on current project.

Hence the total time required to develop this project is around 10 weeks.

## 7.References

Web Resources

* www.java.sun.com

Official Java Website

* www.java.sun.com/developer/onlineTraining/J2EE/Intro2/j2ee.html Training for J2EE
* www.java.sun.com/j2se/1.4.2/docs/api/index.html

J2SE Online Documentation from Sun

* www.w3schools.com

JavaScript Tutorials

|  |  |
| --- | --- |
| BOOKS | |
| * API DOCS –JAVA, J2EE, Java Mail, Java Servlets, JSPs By: Sun Microsystems      * Java2 - The Complete Reference(7TH Edition) By: Herbert Schildt      * JSP - The Complete Reference By: Philhanna      * Oracle 10g   By: Ivan Baross     * Software Engineering   By: Roger Pressman     * Head First Servlets & JSP   By: Bryan Bashan, Kathy Sierra & Bert Bates | net m |
| Literature |  |

https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.72.3151&rep=rep1&type=pdf



Hussein\_2020\_IOP\_Conf.\_Ser.\_\_Mater. \_Sci.\_Eng.\_928\_0320221

Page