**DIGITAL SIGNATURE CRYPTOGRAPHY**

**A Synopsis**

**Submitted in partial fulfilment of the requirements for the final year**

**Project of**

**Bachelor of Computer Application**

**By**

* **Akarsh Mishra-Roll No.2200290140016**
* **Akansha Mangal-Roll NO.2200290140015**

**Under the guidance of**

**Ms. Divya Singhal**

****

**Department of Computer Application**

**AKTU University, Lucknow**

**2022-24**

**ACKNOWLEDGEMENT**

*I express my deep sense of gratitude to my* ***Head of Department (Computer Application)*** *for the valuable guidance and for permitting us to carry out this project.*

With gratitude,

1. Arun Tripathi \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**CONTENTS**

* **Introduction Of Project**
* **Objective Of the Project**
* **Scope Of the Project**
* **Project Plan (initial phase)**
* **The Existing System**
* **Current Problems (RSA ECDSA Comparison)**
* **Areas Of Improvement**
* **Proposed System (Group Signature )**
* **Input /Output Requirement**
* **Hardware and Software Requirement**
* **Conclusion**
* **References**

**Introduction**

***Cryptography****is the study and practice of techniques for secure communication in the presence of third parties called* ***adversaries****. It deals with developing and analysing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.*

*Secure Communication refers to the scenario where the message or data shared between two parties can’t be accessed by an* ***adversary****.*

*Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.*

1. ***Confidentiality****refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.*
2. ***Data integrity****refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.*
3. ***Authentication****is the process of making sure that the piece of data being claimed by the user belongs to it.*
4. ***Non-repudiation****refers to ability to make sure that a person or a party associated with a contract or a communication cannot deny the authenticity of their signature over their document or the sending of a message.*

*Digital signatures are the public-key primitives of message authentication. A digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.*

*In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications , since likelihood of a dispute over exchanged data is very high.*

Digital signatures are significantly more secure than other forms of electronic signatures. Digital signatures increase the transparency of online interactions and develop trust between customers, business partners, and vendors.

**A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.**

**Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge**

**informed consent.** In many countries, including the United States, digital signatures are considered legally binding in the same way as traditional handwritten document signature.

*The blockchain is the technology behind cryptocurrencies like Bitcoin, Ethereum and Litcoin and others. ( Like many other internet technologies, blockchain relies on public key cryptography to protect accounts of users from unauthorized parties. The public and private keys enable users to encrypt information and send it to each other, where the receiver will be able to verify the message authority, and whether it had been altered by an adversary or not.*

**Objective**

This project has been developed keeping in view the security features that need to be implemented in the networks following the fulfillment 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, Non-repudiation 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.

.

**Scope of digital signature**

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**. **E-commerce** 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.

**Project Plan**

* ***Project Overview***

This application makes use of **Elliptic Curve** **Digital Signature Algorithm (ECDSA)** along with a hash function. The hash code is provided as input to a signature function along with a random number generated for this particular signature. The signature function also depends on the sender’s private key and a set of parameters known to a group of At the receiving end, verification is performed. The receiver generates a quantity that is a function of the public-key components, the sender’s public key, and the hash code of the incoming message. If this quantity matches with one of the components of the signature, then the signature is validated.

This application makes sure that the security services Authentication, Secrecy, Integrity, and Non-repudiation are provided to the user.

* This application allows to keep the information out of the hands of unauthorized persons. This is called **Secrecy.**
* It also deals with determining whom a person is communicating with before revealing sensitive information or entering a business deal. This is called **Authentication.**
* **Non-repudiation** deals with proving that a particular message was sent by a particular person in case he denies it later.
* **Integrity** makes sure whether a particular message has been modified or something has been added to it.

Digital signatures are the most advanced and secure type of electronic signatures. One can use them to comply with the most demanding legal and regulatory requirements because they provide the highest levels of assurance about each signer's identity and the authenticity of the documents they sign. It has applications in government, judicial, telecom, e-commerce, and BFSI.

A **group signature scheme** is a method for allowing a member of a group to anonymously [sign](https://en.wikipedia.org/wiki/Digital_signature) a message on behalf of the group. The concept was first introduced by [David Chaum](https://en.wikipedia.org/wiki/David_Chaum) and Eugene van Heyst in 1991. For example, a group signature scheme could be used by an employee of a large company where it is sufficient for a verifier to know a message was signed by an employee, but not which particular employee signed it. Another application is for [keycard](https://en.wikipedia.org/wiki/Keycard) access to restricted areas where it is inappropriate to track individual employee's movements, but necessary to secure areas to only employees in the group.

Essential to a group signature scheme is a *group manager*, who is in charge of adding group members and has the ability to reveal the original signer in the event of disputes. In some systems the responsibilities of adding members and revoking signature anonymity are separated and given to a membership manager and revocation manager respectively. Many schemes have been proposed, however all should follow these basic requirements:

* **Soundness and completeness**
  + Valid signatures by group members always verify correctly, and invalid signatures always fail verification.
* **Unforgeable**
  + Only members of the group can create valid group signatures.
* **Anonymity**
  + Given a message and its signature, the identity of the individual signer cannot be determined without the group manager's [secret key](https://en.wikipedia.org/wiki/Secret_key).
* **Traceability**
  + Given any valid signature, the group manager should be able to trace which user issued the signature. (This and the previous requirement imply that only the group manager can break users' anonymity.)
* **Unlinkability**
  + Given two messages and their signatures, we cannot tell if the signatures were from the same signer or not.
* **No framing**
  + Even if all other group members (and the managers) [collude](https://en.wikipedia.org/wiki/Collusion), they cannot forge a signature for a non-participating group member.
* **Unforgeable tracing verification**
  + The revocation manager cannot falsely accuse a signer of creating a signature he did not create.
* **Coalition resistance**
  + A colluding subset of group members cannot generate a valid signature that the group manager cannot link to one of the colluding group members.[[1]](https://en.wikipedia.org/wiki/Group_signature#cite_note-ACJT2000-1)

**The existing system**

These days almost all organizations around the globe use a messaging system to transfer data among their employees through their exclusive intranet. But the security provided is not of high standards. More and more unauthorized people are gaining access to confidential data.

**Disadvantages:**

* The validity of sender is not known.
* The sender may deny sending a message that he/she has actually sent and similarly the receiver may deny the receipt that he/she has actually received.
* Unauthorized people can gain access to classified data.
* Intruders can modify the messages or the receiver himself may modify the message and claim that the sender has sent it.

The algorithm used in digital signature system are:-

1. Rivest, Shamir, Adleman Algorithm (RSA)

2. Digital Signature Algorithm (DSA)

3. Elliptic curve digital Signature algorithms (ECDSA)

4. Edwards-curve Digital Signature Algorithm (EdDSA)

**Rivest, Shamir, Adleman Algorithm (RSA)**

RSA algorithm is a symmetric cryptography algorithm .Asymmetric actually means that it works on two different keys i.e , pubic key and private key .As the name describes that the public key is given to everyone and private key is kept private.

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

**Digital Signature Algorithm (DSA)**

We sign a document to show that is approved by us or created by us. The signature is proof to the recipient that this document is coming from the correct source. The signature on the document simply means the document is authentic.

When A sends a message to B, B needs to check the authenticity of the message and confirm it comes from A and not C. So B can ask A to sign the message electronically. The electronic signature proves the identity of A is also called a digital signature.

A digital signature scheme typically consists of three algorithms:

* A [*key generation*](https://en.wikipedia.org/wiki/Key_generation) algorithm that selects a *private key* [uniformly at random](https://en.wikipedia.org/wiki/Uniform_distribution_(discrete)) from a set of possible private keys. The algorithm outputs the private key and a corresponding *public key*.
* A *signing* algorithm that, given a message and a private key, produces a signature.
* A *signature verifying* algorithm that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature.

**Elliptic Curve Digital Signature Algorithms (ECDSA)**

Elliptic Curve Digital Signature Algorithm (ECDSA) is a Digital Signature Algorithm (DSA) which uses keys derived from elliptic curve cryptography (ECC). While functionally providing the same outcome as other digital signing algorithms, because ECDSA is based on the more efficient elliptic curve cryptography, ECDSA requires smaller keys to provide equivalent security and is therefore more efficient.

Elliptic-curve cryptography (ECC) is type of public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys than to non-EC cryptography (i.e. RSA) to provide equivalent security, and is therefore preferred when higher efficiency or stronger security (via larger keys) is required.

ECC is used for key agreement, digital signatures, pseudo-random generators and other tasks.

**Current Problems**

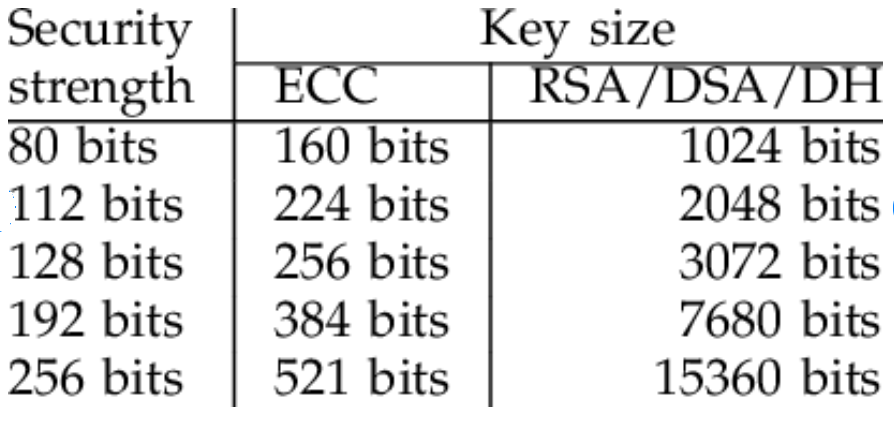
## Problem Definition

Message authentication protects two parties who exchange messages from any third party. However, it does not protect the two parties against each other. Several forms of disputes between the two parties are possible.

For example, suppose that A sends an authenticated message to B. Consider the following disputes that could arise:

1. B may forge a different message and claim that it came from A. B would simply have to create a message and append an authentication code using the key that A and B share.
2. A may deny sending the message. Because it is possible for B to forge a message, there is no way to prove that A did in fact send the message.

The most attractive solution to this problem is the Digital Signature.



Difference between RSA and ECC

* For the same length of key faster than RSA.
* For same degree of security, shorter key required than RSA.
* 160 ECC key is equivalent to 1024 RSA key.



**Areas For Improvement**

Introduction

In our time, the beneﬁts of cryptographic information security are continuing to gain

momentum. However, this use could be much wider. At the moment, a cryptographic

tool such as electronic digital signature is most commonly used in banking records, but

even this makes it very popular. Thus, to be able to provide the service of concealment,

and given the fact that usually important electronic documents are signed, it can be said

that it is necessary to take care of preserving the secrecy of conﬁdential data, which is

an invariable attribute of each document. Therefore, an important problem with all

digital signing of information is the improvement of algorithms and methods for

signing conﬁdential data recovery from the signature itself.

Introduction

In our time, the beneﬁts of cryptographic information security are continuing to gain

momentum. However, this use could be much wider. At the moment, a cryptographic

tool such as electronic digital signature is most commonly used in banking records, but

even this makes it very popular. Thus, to be able to provide the service of concealment,

and given the fact that usually important electronic documents are signed, it can be said

that it is necessary to take care of preserving the secrecy of conﬁdential data, which is

an invariable attribute of each document. Therefore, an important problem with all

digital signing of information is the improvement of algorithms and methods for

signing conﬁdential data recovery from the signature itself.

Our time, the beneﬁts of cryptographic information security are continuing to gainmomentum. However, this use could be much wider. At the moment, a cryptographictool such as electronic digital signature is most commonly used in banking records, buteven this makes it very popular. Thus, to be able to provide the service of concealment, and given the fact that usually important electronic documents are signed, it can be saidthat it is necessary to take care of preserving the secrecy of conﬁdential data, which isan invariable attribute of each document. Therefore, an important problem with alldigital signing of information is the improvement of algorithms and methods forsigning conﬁdential data recovery from the signature itself.

Introduction

In our time, the beneﬁts of cryptographic information security are continuing to gain

momentum. However, this use could be much wider. At the moment, a cryptographic

tool such as electronic digital signature is most commonly used in banking records, but

even this makes it very popular. Thus, to be able to provide the service of concealment,

and given the fact that usually important electronic documents are signed, it can be said

that it is necessary to take care of preserving the secrecy of conﬁdential data, which is

an invariable attribute of each document. Therefore, an important problem with all

digital signing of information is the improvement of algorithms and methods for

signing conﬁdential data recovery from the signature itself.

our time, the beneﬁts of cryptographic information security are continuing to gain

momentum. However, this use could be much wider. At the moment, a cryptographic

tool such as electronic digital signature is most commonly used in banking records, but

even this makes it very popular. Thus, to be able to provide the service of concealment,

and given the fact that usually important electronic documents are signed, it can be said

that it is necessary to take care of preserving the secrecy of conﬁdential data, which is

an invariable attribute of each document. Therefore, an important problem with all

digital signing of information is the improvement of algorithms and methods for

signing conﬁdential data recovery from the signature itself.

our time, the beneﬁts of cryptographic information security are continuing to gain

momentum. However, this use could be much wider. At the moment, a cryptographic

tool such as electronic digital signature is most commonly used in banking records, but

even this makes it very popular. Thus, to be able to provide the service of concealment,

and given the fact that usually important electronic documents are signed, it can be said

that it is necessary to take care of preserving the secrecy of conﬁdential data, which is

an invariable attribute of each document. Therefore, an important problem with all

digital signing of information is the improvement of algorithms and methods for

signing conﬁdential data recovery from the signature itself.

our time, the beneﬁts of cryptographic information security are continuing to gain

momentum. However, this use could be much wider. At the moment, a cryptographic

tool such as electronic digital signature is most commonly used in banking records, but

even this makes it very popular. Thus, to be able to provide the service of concealment,

and given the fact that usually important electronic documents are signed, it can be said

that it is necessary to take care of preserving the secrecy of conﬁdential data, which is

an invariable attribute of each document. Therefore, an important problem with all

digital signing of information is the improvement of algorithms and methods for

signing conﬁdential data recovery from the signature itself.

**Proposed System**

The system will provide the following security services:

**Confidentiality:**

Confidentiality is the protection of transmitted data from passive attacks. With respect to the release of message contents, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. For example, if a virtual circuit is set up between two systems, this broad protection would prevent the release of any user data transmitted over the virtual circuit. Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message. These refinements are less useful than the broad approach and may even be more complex and expensive to implement. The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

**Authentication:**

The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic (i.e. that each is the entity that it claims to be). Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

**Integrity:**

Integrity basically means ensuring that the data messages are not modified. An integrity service that deals with a stream of messages assures that messages are received as sent, with no duplication, insertion, modification, reordering or replays. The destruction of data is also covered under this service. Thus the integrity service addresses both message modification and denial of service.

**Non-repudiation:**

Non-repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. Similarly, when a message is received, the sender can prove that the message was in fact received by the alleged receiver.

**Group signature**

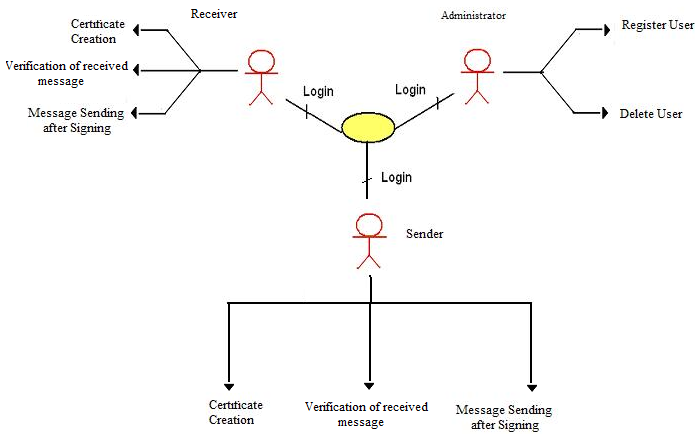
A group signature scheme is a method for allowing a member of group to anonymously sign a message on behalf of the group. The identity of individual signer cannot be determined without the group manager’s secret key.

Here, we are creating a group signature by our algorithm based on ECC. That takes less bit and give maximum security level. We basically reduces the bit size and time taken with the help of Elliptic curve cryptography.

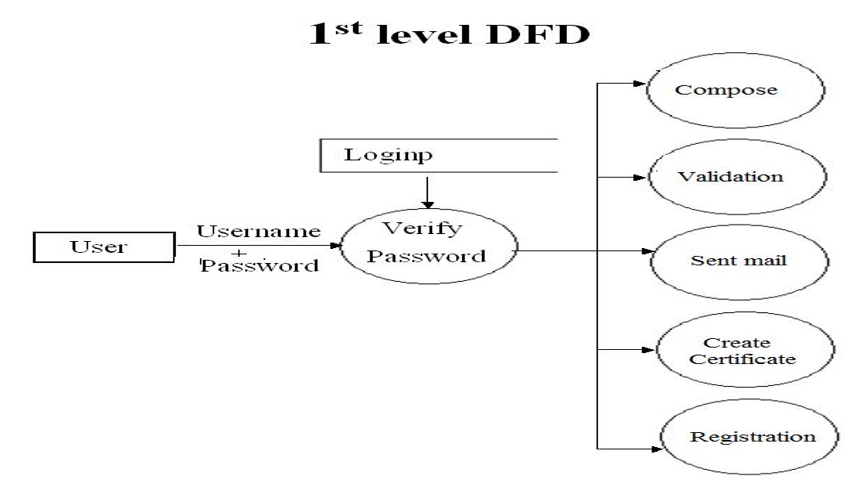
In today’s digital world, group signature plays an important role for different security aspects in Institutions, government organisations etc. Group signature is basically applicable if there is a need of signing a digital document by an authorized group member on behalf of whole group. we propose an ID based group signature scheme based on Elliptic curve discrete logarithm problem(ECDLP). Proposed scheme satisfies all the security requirements: Correctness, Unforgeability, Anonymity, Unlinkability, Exculpability and Traceability. Our proposed scheme is the first Group Signature scheme whose security is based.

On only ECDLP. Due to security settings over elliptic curves, our proposed scheme is much more efficient in terms of computational complexity. It is applicable in all those environments where less bandwidth is required.

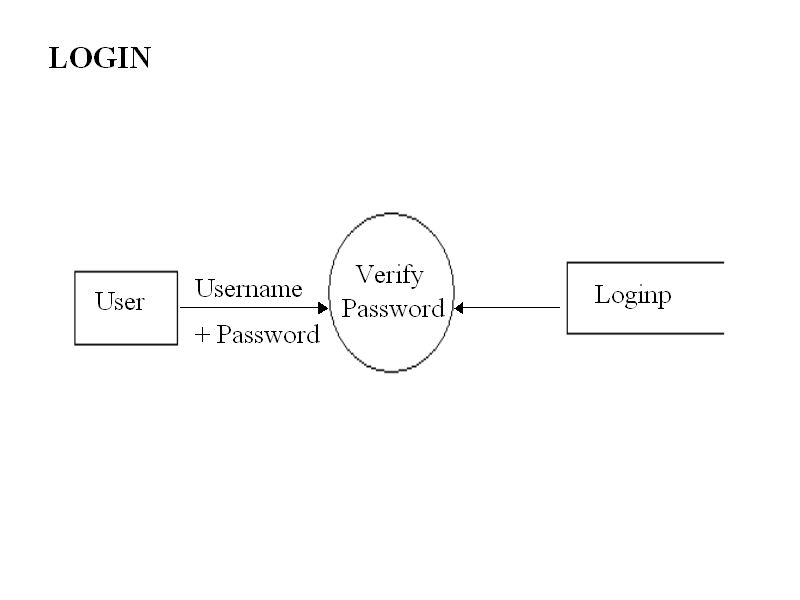
## UML Diagram

****

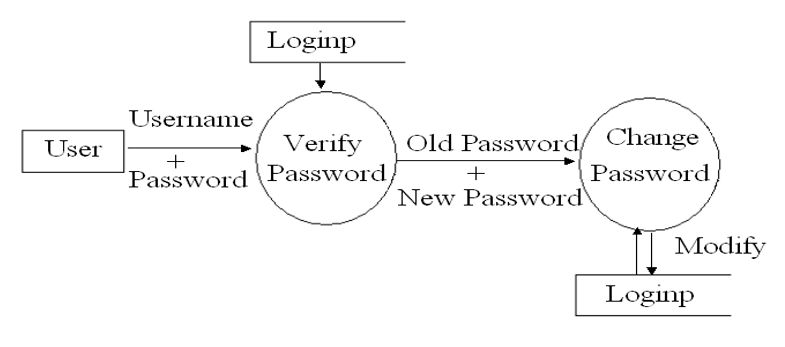
## Data flow diagrams



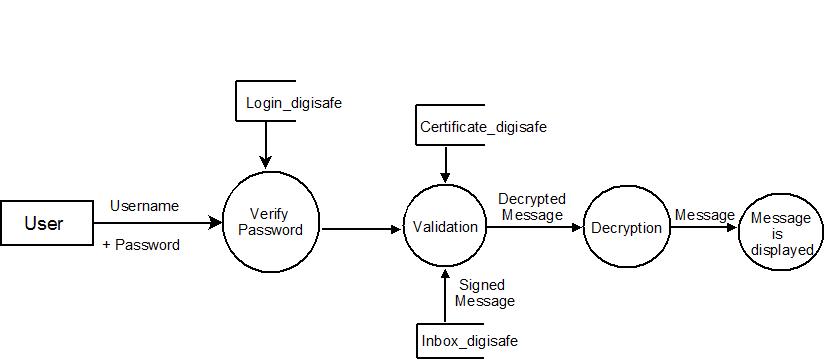
**2nd Level DFD’S**



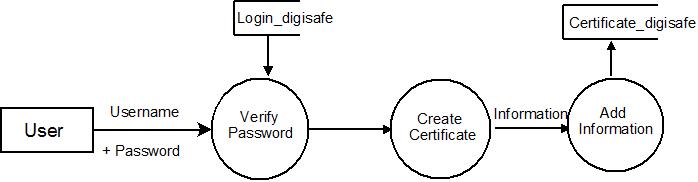
**CHANGE PASSWORD**



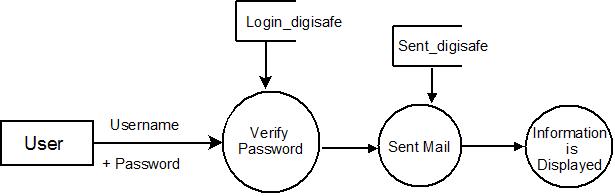
**Validate Mail**



**Create Certificate**



**Sent Mail**



**INPUT/ Output Requirement**

**Input**

* Java library
* Key generator
* Public and Private k
* Hash function
* Random Number Generator
* Elliptic curve group parameters

**Output**

* Group Signatures by using ECC

**Hardware and Software Requirement**

**Hardware**

* 64-bit operating system
* x64-based processor
* Intel(R) Core(TM) i3-4030U CPU @ 1.90GHz 1.90 GHz

**Software**

* Operating system- windows 10
* Programing language – Java
* Java version “1.7.0\_25”
* SQL
* ECC library
* Hash Function- SHA256withECDSA
* ECCprovidertest
* Java library- java.security.\*;

Java.security.spec.\*;

* Documentation tool - Ms Word

**Conclusion**

Systems based upon elliptic curves are an effective alternative to the RSA. Cryptosystems since they involved different mathematical approaches. Elliptic curve cryptosystems are reputed for robustness equivalent to RSA cryptosystems with shorter key length. Accordingly, elliptic curve cryptosystems are perfectly suitable for embedded systems, e.g., smart cards, documents in which memory and power of the processors are not sufficient to achieve computation as required by RSA cryptosystems.

However, ECC and RSA cryptosystems involved the use of keys for security. We will

Due to the major drawback of the symmetric algorithms, we therefore concluded the

Algorithm implementing the elliptic curves are less costly in terms of key length. This

is the main reason why the ECC algorithm is increasingly becoming the preferred choice

for embedded systems with very limited memory and computing power.

Considering Bandwidth saving, ECC offers considerable bandwidth savings over RSA

and considering computational overheads, ECC offers Roughly 10 times than that of RSA

can be saved [18]. Considering key sizes, System parameters and key pairs are shorter for

the ECC than RSA and After the different results obtained at the level of the encryption

and decryption and those obtained for the digital signature, we have deduced that the

elliptic curve algorithms are more efficient than the one based on the RSA. Also, we

found that the digital signature ECDSA is more efficient than the ECNR. This is why

among the algorithms based on the elliptic curves, the ECDSA algorithm was adopted

and published as an international standard in ANSI X9.623.

We proposed the first ECDLP based GSS which is more efficient and secure due

to use of Elliptic Curve cryptography and can be used practically in the situations if there is a need to hide identity of Group of signers while any member can

sign on behalf of Group. Our proposed scheme can also be used in Block-chain

applications.

**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