

Use of Digital Signature to enhance Data Security

Vaibhav Singh
(151307)

Under the supervision of:

Dr. Amol Vasudeva



Department of Computer Science & Engineering and Information
Technology

**Jaypee University of Information Technology Waknaghat, Solan-
173234, Himachal Pradesh**

Candidate's Declaration

I hereby declare that the work presented in this report entitled "Use of digital signature to enhance data security" in partial fulfilment of the requirements for the award of the degree of Bachelor of Technology in Computer Science and Engineering/ Information Technology submitted in the department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology ,Waknaghat , is an authentic record of my own work carried out over a period from August 2018 to May 2019 under the supervision of Dr. Amol Vasudeva (Assistant Professor, Computer science and Engineering).The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Vaibhav Singh (151307)

This is to certify that the above statement made by the candidates is true to the best of my knowledge.

Dr. Amol Vasudeva

Assistant Professor

Computer Science & Engineering Date

ACKNOWLEDGEMENT

I have taken efforts in this project. However, it would not have been possible without the kind support and guidance of many individuals and organization. I would like to extend sincere thanks to all of them.

I would like to express my sincere gratitude to my guide Dr. Amol Vasudeva who always helped and encouraged me towards the successful completion of project. I would like to thank my parents and colleagues who believed and supported me in completion of my project.

At last I would like to express my gratitude to Jaypee University of Information Technology who gave me the opportunity to work on this project and thank my friends who always helped and supported me in completion of my final year project.

TABLE OF CONTENTS

TOPIC NAME	PAGE NUMBER
------------	-------------

1. INTRODUCTION

7

1.1 Introduction

7-8

1.2 Problem Statement

8-9

1.3 Objective

9-10

1.4 Methodology

10-11

2.1 LITERATURE SURVEY

12-17

3. SYSTEM DEVELOPMENT

19-23

3.1 SYSTEM REQUIREMENTS

20

3.2 MAIN CONFIGURATIONS

21

3.3 PROPOSED MODEL

22-23

4. ALGORITHMS

25-44

5. RESULT AND PERFORMANCE ANALYSIS

46-53

5.1 EXPERIMENTAL RESULTS

6. CONCLUSIONS

53

7. REFERENCES

54-55

FIGURE DETAILS

FIGURE	NAME
1.1	DIGITAL SIGNATURE DESIGN
1.2	E-R DIAGRAM OF DIGITAL SIGNATURE
1.3	SHA-WORKING
1.4	DSS APPROACH TO DIGITAL SIGNATURE
1.5	RSA APPROACH TO DIGITAL SIGNATURE
1.6	HASH FUNCTION DIAGRAM
1.7	INFLUENCE OF TOPOLOGY ON PERFORMANCE OF ECDSA AND RSA

ABSTRACT

The security of information in any organization was primary concern since the advent of paperwork. Thousands of years ago the sensitive information and documents were preserved in cabins and lockers. With the invention of computer and as the world progressed issue of information security also became a serious concern. In digital signature security of messages is assured so that the information can be transferred from one end to another without any threat to integrity of a message and documents.

In digital signature scheme the sender first signs a documents which send to receiver either directly or by a trusted third party. The recipient on receiving the messages validates the signature through an algorithm that is known as DSA or Digital Signature Algorithm. This scheme of digital signatures ensures that the information received is secured verified Integrated and authenticated. This makes the digitally signed document secure from forgery and any other foreign attacks that may prove to be a threat to security of data and information. This paper describes the devious factors of digital signature which helps in the working of electronic signature and also through various ways and procedures it involve the signing of the data which we use in digital signature.

CHAPTER I

INTRODUCTION

Digital signature is an electronic signature that is designed to provide high level of security and authenticity to its users. Digital signatures provide high level of assurance to its users by providing a unique identity to its signer. They make use of certificate based ID which is uniquely linked to each individual. So when a person signs a document the signature is attached to a document with an encryption which can be decrypted at the user end with help of various digital signature verification algorithms. Digital is a way that ensures contents of a document are not altered during any transaction. When we sign a document digitally we add a one way hash i.e. encryption by using public and private key pair. Then the receiver using the sender's public can decrypt the signature.

Nowadays digital signature is used in various fields like e-governance, e-shopping, e-learning etc. The rate of success of the digital signature techniques depends on various parameters like algorithm used for key generation, security at sender's end, technique used for decryption of hash message at receiver's end etc. To achieve the above parameters sensitive information i.e. signed by the sender should again be verified at receiver's end. Digital signature is basically a mathematical implementation of a cryptographic algorithm which is implemented on a digital document.

It's similar to a normal signature as both digital and pen paper signature aims to maintain the authenticity and integrity of the document. The digital signature technique is generally based on 3 phases:

- i. Key generation algorithm
- ii. Signing technique used
- iii. Signature verification algorithm

Also the digital signature technique can be broadly classified into two categories:

a.) Signature i.e. Directly Digitized:

The above scheme gives us a direct way to communicate among the two party which is the sender and receiver given:

- i. Recipient is aware of the private key of the sending party
- ii. Digital signature can be produced by encoding hash code of message with sending party's private key or encoding the whole message with sending party's private key.

The main drawback of this technique is that success of this method is totally dependent on security of the sender's private key.

b.) Digitized Signature of Arbitrary nature:

The above methodology allows the sender and receiver interact through a third trusted party i.e. the arbiter. The message signed by the sender first reaches the arbiter. The trusted third party performs various security checks and analysis. Therefore it verifies the authenticity of message before it reaches the receiver.

PROBLEM STATEMENT

A digital signature scheme works on a technique in a message i.e. encrypted by sender is passed via signature algorithm and is decrypted at a receiver end. The signature algorithm is generally based on a single hard problem. These hard problems are factoring, discrete logarithms and elliptical logarithms problems. Although these type of hard problems seems to secure the signature algorithms from any foreign attacks which may disrupt security and authenticity of algorithm. But it is possible that one day one may find a solution to these hard problems. This will result in cracking of algorithm.

Approach:

To overcome the above problem we must design our signature algorithm in such a way that it is based on combination of two or more hard problems like factoring, discrete logarithm etc. The problems were combined such that the signing equations depended on two secret keys whereas the verifying equations depended on two public keys.

OBJECTIVES:

Saves time:

Digital signature is a fast method of verification that can be implemented from your personal devices like laptops and phones.

Cost savings:

This method is also useful to save the cost that is otherwise spent on paper ink and other documents.

Security:

Digital signatures aim at providing security and authenticity to the documents. They are far more secure from forgery and tampering as compared to normal pen paper signature. Digital signatures are made secure through various algorithms and combinations of two or more hard problems.

Workflow Efficiency:

Digitally signed documents ensure fast workflow as they are easy to track and we can know the current status of the signed documents. For example the email notifications reminds the person to sign the document on time.

METHODOLOGY:

Like any other pen paper signatures, digital signatures are also unique to have their own unique key. The digital signature works on standard norms of key generation that is PKI(public key infrastructure). PKI involves using of mathematical algorithms to generate two long numbers. One can be designated as public key and other is designated as private key.

When the sender signs a document the signature is automatically generated using sender's private key .The mathematical algorithm is used to match the private key with the document and encrypt it therefore creating a hash message.

CHAPTER II

LITERATURE SURVEY

This chapter discusses the research work conducted by various researchers in the field of digital signature and security:

1. Paper title:

A digital signature scheme without using one way hash function and message/data repeating and its application on key agreement.

Authors:

Hua Zhang, Zheng Yuan, Qiao Yan Wen

Description:

This scheme of digital signature is based on cryptosystem using public key and it is highly prone to any forgery attack. The type of attack can be avoided by application/implementation of one way hash message and function for message repetition. The authors have improved the technique by using a new key agreement protocol which was not there in chang-chang model that avoided the use of one way hash function and redundancy padding.

2. Implementation of SHA-2 Hash Function for a digital signature system on chip in FPGA.

Authors:

M.Khalil, M.Nazrin, Y.W. Hau

Description: For the purpose of information security, due to advancement in e-mechanism the crypto-system had become a decisive factor. The requirement

can be met by embedding crypto-system design on chips i.e. system-on-chips (SoC).

The authors have given an insight about SHA-2 hash logic which can be configured on hardware.

3. A Fast ECC Digital Signature based on DSP

Authors:

Ying Qin, Chengxia li, Shouzhi Xu

Description:

The Elliptical Curve Digital Signature algorithm is nowadays a burning topic in information and security. The authors have created a technique to reduce computational complexity .This can be done by combining NAF and variable – length sliding window.

4. An Abuse-Free Contract – Signing Protocol Based on RSA Signature.

Author:

Guilin Wang.

Description:

A new digital Signature scheme is introduced by the author in this model. It involves the role of third party only when either of the party is cheating or the connection between the sender and receiver is getting interrupted.

Also this technique focuses on the new property which is known as abuse freeness. It implies that during the unsuccessful implementation of the protocol

neither the sender nor receiver can depict the correctness of intermediate result to one another.

5. Optimistic Fair-exchange techniques based on DSA algorithm.

Authors:

WANG Shaobin, HONG Fan, ZHU Xian.

Description:

One of the major issues in the transactions that are electronically secured is the problem of fair exchange. The authors in this publication have provided a technique consisting of multi signature to improve the efficiency of fair-exchange technique based on DSA signatures.

6. Preserving Transparency and Accountability in Optimistic Fair Exchange of Digital Signature

Authors: Xinyi Huang, Yi Mu, Robert H. Deng

Description:

The above scheme allows the sender and receiver to fairly exchange the information with the help of third party , i.e. involved only when required.

The third party involved must be very fair impartial and transparent as the fairness of the algorithm is entirely dependent of the third party. The accountability is defined by the Optimistic Fair Exchange by using the digital signature.

7. Integrated approach for fault tolerance and digital signature in RSA

Author: C.N. Zhang

Description: Fault tolerance and data security are two major problems in communication. The author creates a model that can reduce the total overheads by detecting and correcting up to three errors. This can be achieved by integrating the design that is used to implement fault tolerance using hash algorithms and RSA. In the end the author focuses on the implementation of this technique on other cryptographic techniques.

8. Public key encryption and digital signature based on permutation and combinations polynomials

Author:

J.Schwenk, K.Huber

Description:

The basic concept of RSA and public are based on polynomial functions. The use of permutation polynomial whose inverse is easy to compute is used in cryptography. In this article the public key restriction is avoided by generating signature key using gcd of 2 polynomials.

9. Publically verifiable authenticated encryption technique without using one way hash function

Authors:

SHI-YI XIE, BING XU

Description:

The scheme of using one way hash is prone to threats and forgery attacks from anywhere around the globe. To overcome this problem the author proposes to use a Discrete Logarithmic Problem i.e. DLP in order to improve the efficiency.

10. Optimistic Fair Exchange of Digital Signatures:

Author:

N.Asokan , Victor Shoup , Michael Waidner

Description:

The following article discusses about the scheme in which both the sender and receiver will get each other's signature or both of them will not receive the signatures of each other. The scheme relies on the third member but is "optimistic" in a way that the third party is only called upon when one of the party gets broken down or tries to cheat. An interesting feature of this scheme is that a sender/receiver can always force a fair and timely termination even without the support of other counterpart, even if the network is completely asynchronous.

The most important point of this scheme is that even if the third party tries to cheat, it can be held responsible as the forgery by the third party can be proved.

11. Design of Proxy signature in ECDSA

Author:

Ming-Hsin Chang, I-Te Chen, Ming-Te Chen

Description:

Even though ECDSA and DSA are considered the standard algorithm for digital signature yet they are devoid of proxy signature. Also most of the techniques that follow proxy signature hardly follow standard algorithms. In the following article the author has practically applied proxy protected signature technique that depends upon ECDSA to fulfill some of the properties of proxy signature.

12. A comparative Analysis of Signature scheme in a new approach to variant on ECDSA:

Authors:

M.Prabhu , Dr. Shanmugalakshmi

Description:

The authors give us an insight of variant technique level of ECDSA that gives high level of security. In order to show the effectiveness of this framework the authors have given the comparative study and result with other signature verification algorithms.

CHAPTER III

SYSTEM DEVELOPMENT OF DIGITAL SIGNATURE DESIGN

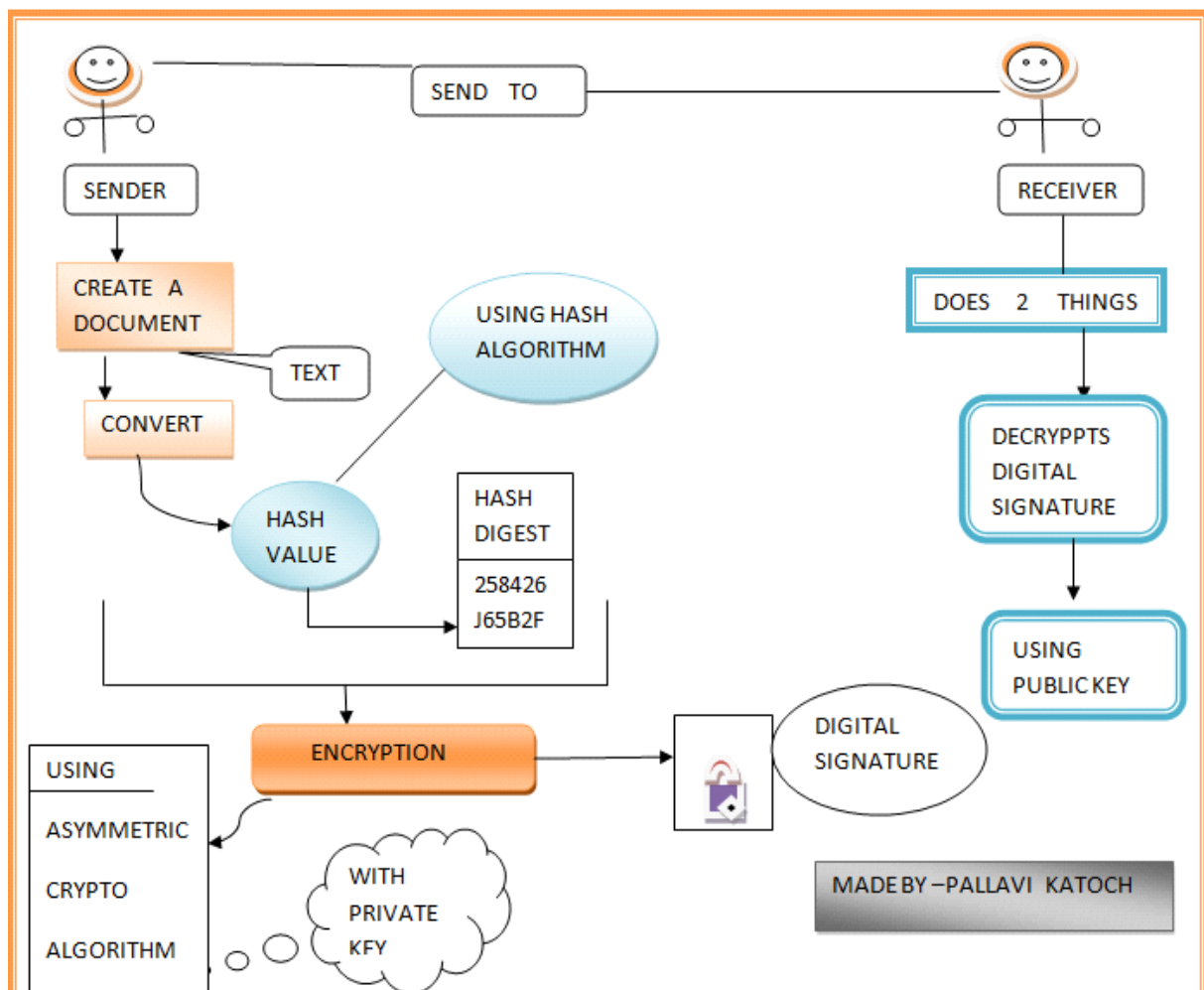


FIG 1.1 DIGITAL SIGNATURE DESIGN

In the design process each component has different roles to play improving the flexible nature, the integrity and portability of digital signature. Each part of

components are expected uses and to support the deployment part which are explained operationally.

Earlier identifying a signature was not easy task and needed full concentration with signature systems like PGP, PKCS-7... which was made through core data structure and cryptography. Protecting data was major concern. There are different goals to design such approaches.

GENERAL POINT

Digital signature block is default to fixed data process .We can use it anywhere messages should be signed (messages, email). Only that signature block is verified which is signed in document and no digital signature will go through the computation by default.

SELF CONTAINED

Unlike other secure approaches this method of digital signature is embedded within its data, and also from external sources. It will contain all the data which is needed to be verified this means that it needs to carry secured certificate as required.

SIMPLE ENCODING

Digital signature blocks are encoded as ASCII value which allows designers to use core data structure and can also reuse the binary data. Using the ASCII it will reduce the complexity value encoding problems.

CERTIFICATE NEUTRAL

This should be able to work on opaque certificates. We use certificate for trust factor and also management problem. It can add and delete the entries from the digital blocks as needed.

For example, a digital signature will have four different parts which is safe and useful when correctly done.

- User will create several associated resources(the sample files and its documentation)
- User will create clear points at respective resource.
- User will create a different part which points to several saying as “safe”.
- User will sign the part and set the signature result.

OPERATION STATEMENT

A digital signature is self contained, protected through cryptography, information resource and assertion.

- **Self contained**

Unlike other secure approaches this method of digital signature is embedded within its data, and also from external sources.

- **Protected through cryptography**

Digital signature will prove its integrity and authenticity as it will support different mixtures of cryptography processes.

- **Information resource**

A universal resource identifier will include different objects. When different data stored in database is stored as a information will help in further search for digital signature.

- **Assertion**

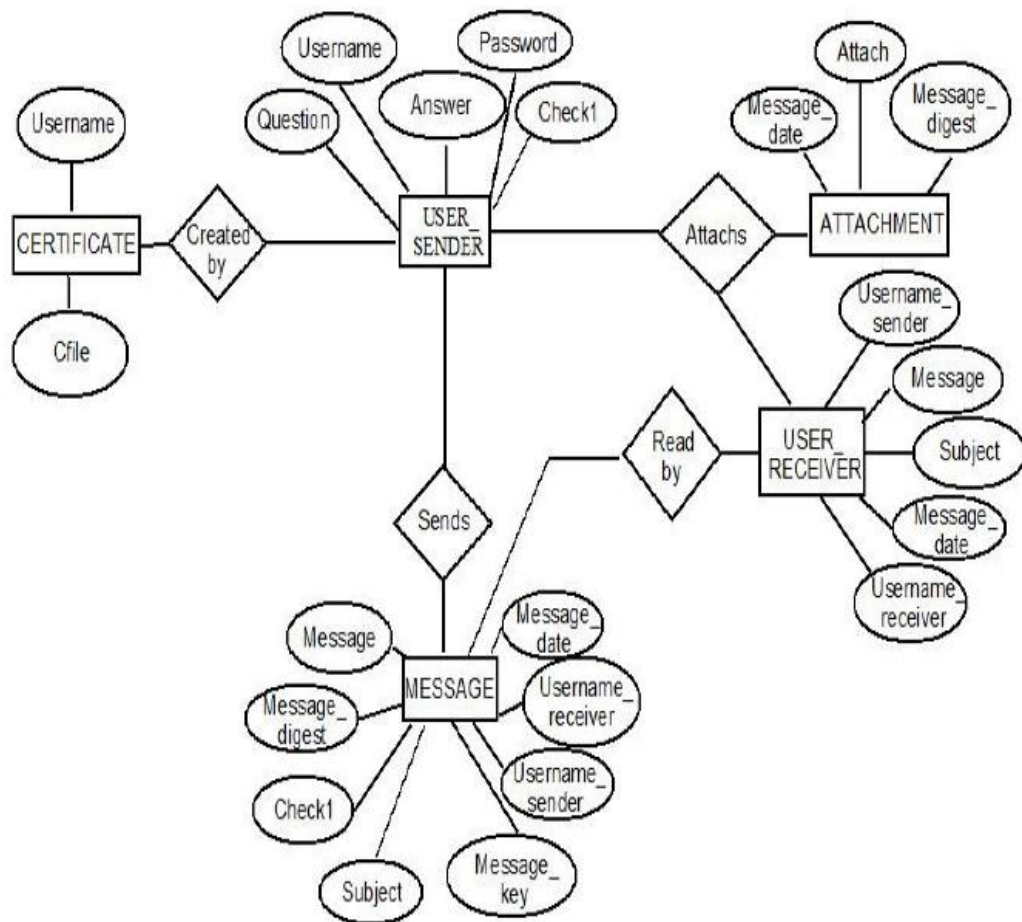
It means that a submission and forceful statement or an opinion which will explain the content of the information resource. Another way of reading it properly is text submission from a unchangeable grammar. Identifying certificate is also a part of design of digital signature to provide non repeating data and safe electronic data.

FUNCTIONAL ABSTRACTION

The particular security requirements which shows the importance of the operation for the correct data. Authentication is the process of knowing that whether this thing is correct and is declared to be. Authorization means that we are giving the other party the access to service a data resource.

	Authenticatio n	Authorizatio n	Integrit y	Privacy	Availabilit y
Importanc e	HIGH	HIGH	HIGH	MEDIU M	MEDIUM

FIG1.2



E-R DIAGRAM FOR DIGITAL SIGNATURE

PRIVATE KEY - It is used to create digital signature and one part of asymmetric cryptography that should be known to signer.

PUBLIC KEY - second part of cryptography asymmetric which is also used to verify the digital signature and should be available to all those needing to verify the signature.

CHAPTER IV

ALGORITHMS

There are main three different algorithms that we have used in our project and also which is most suitable for digital signature. The digital signature algorithms are as follows:

- ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)
- DSA ALGORITHM
- RSA ALGORITHM

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)

Let's suppose I want to send a message to my friend ram. In the first step they should agree on the curve parameters (n, G, CURVE). As a base point of prime order now we require G as a main point for devious orders on the curve and also here n will be the multiplicative of the order G as per requirement.

PARAMETER	
CURVE	The elliptic curve field and the resulted equation is used.
G	Elliptic curve base points where the points are (X0, Y0) on $z^5 = ^7+4$.
n	Integer order of G, means that $n * G = O$ is the main identity number.

Now here we will use the base point T as a **prime**.

Me and my friend ram creates a key pair, consists of private key integer DA, randomly selected [1, n-1] and then a public key curve point will be resulted as

$QL = DL * T$. We use $*$ to denote elliptic curve point for the multiplication by a scalar property.

For me sign a message L , I follow these steps:

- I. Evaluate $e = \text{HASH}(L)$, where HASH is a cryptographic hash function, such as SHA-2.
- II. Let z be the LN , where LN is the bit length of order n .
- III. Evaluate the cryptography secured arbitrary integer number as l from $[1, n-1]$.
- IV. Calculate the curve point $(x_1, y_1) = m * G$.
- V. Evaluate $s = X_1 \text{ mod } m$. If $s = 0$, step back to third.
- VI. Evaluate $r = o^{-1}(z + r * DA) \text{ mod } l$. If $r = 0$, step back to third.
- VII. The signature will be the two (s, p) .

When we compile the string K from $\text{HASH}(m)$ after that it should be changed to an integer so that the data cannot be changed. Here K can be larger than n but should not be extended.

Now, when ram will authenticate my digital signature, he should have a copy of his public curve point which is QA . Ram should check whether QA is right or not and will work accordingly.

- I. Examine that QA is in proficient to the element K , and its dimensions are otherwise it is proficient.
- II. Examine whether QA remain on the curve.
- III. Examine that $n * QA = P$.

Ram will follow these steps:

- I. Verify the s and m are the integers in range of $[1, n-1]$. If condition is false then the digital signature will be irrational.

- II. Examine $Y = \text{HASH}(K)$, when HASH is the similar function that is used for digital signatures.
- III. Let P be the MN bits of n .
- IV. Examine $w = s^{-1} \pmod n$.
- V. Examine $u_1 = rf \pmod n$ and $u_2 = cw \pmod n$.
- VI. Examine the curve point $(x_1, y_1) = u_1 * G + u_2 * QA$. If condition is $(x_1, y_1) = O$ then the digital signature will be irrational.
- VII. The digital signature will be irrational if $r = x_1 \pmod n$, will be irrational.

DSA ALGORITHM

It works on the frame of public key cryptosystems and is mainly based on the different algebraic properties of the mod, exponentiations and some discrete logarithm problem. The digital signature will provide authentication, integrity and non repudiation.

In the main DSS algorithm where H was consistent SHA-1 yet the main and also powerful function was SHA-2 hash function which was agreed for operating the DSS.

To decide the key length M and K . This is the starting part of the cryptography

Strength of the private and public key.

- Select a K bit prime m .
- Select a s -bit prime l such that $x-1$ is a multiple of q .
- Select g , a number where different multiplicative arrangement is s in the module which means that s is the smallest positive number like in $GP = 1 \pmod s$. This can be finished by setting $G = h^{(s-1)} \pmod p$ for some inconsistency $l(1 < l < p)$ and also most of the choices of h will be usable to g that is commonly $h=2$ is used.

PRE- USER KEYS

In the given set of parameters, the later phase will compute the public and the private keys for a solo user.

- We will first select the secret private key y by other arbitrary way , where $0 < y < m$.
- We will evaluate the public key $m = g^x \text{ mod } p$.

There exists some well organized algorithms for doing some enumerate the devious modular exponentiations $h^{(p-1)/q} \text{ mod } p$ and g^x such will be exponentiation by squaring them.

Let L and m be the hashing function and the data for result.

- We will generate a arbitrary pre-message value L where $1 < L < k$.
- We will calculate the $\text{mod } q(g^k \text{ mod } p)$.
- For other cases like $m = 0$, we will start it over again with a different arbitrary k .
- The digital sign will be (r, s) .

TO VERIFY

- We will dismiss the digital signature if $0 < m < r$ or $0 < l < s$ which is not well satisfied.
- We will evaluate the $w = s^{-1} \text{ mod } l$.
- We will evaluate $w_1 = h(m) \cdot w \text{ mod } q$.
- We will evaluate $w_2 = s \cdot m \text{ mod } q$.
- We will evaluate $a = (m^{x_1} k^{y_2} \text{ mod } h) \text{ mod } j$.
- The digital signature will only be valid if and only if $v = r$.

SHA ALGORITHM

- SHA -0 : A different form is applied that is retronym to the first version of hash function was nearly 160 bit and was recorded in 1993 as the name "SHA". It was neglected shortly after publications it due to a significant imperfection and exchanged by the slightly different sort of SHA-1.
- SHA- 1 : A hash function which typically look like the previous MD5 algorithm. So, that was mainly planned by the national security agency (NSA) that can be a segment of the digital signature cryptography algorithm.
- SHA- 2 : A similar two hash function which have different sizes of blocks which is well known as SHA-256 and SHA-512. They have different word size and used 64 bit. As we know that we have other versions which reflect the each standard and are also designed by NSA.
- SHA- 3: This was in public in 2012 after known family of SHA that is SHA-256 and 512. They are different in sizes it is generally called keccak and also support the same hash function and hash length as SHA-2 and internal structure is different from other SHA.

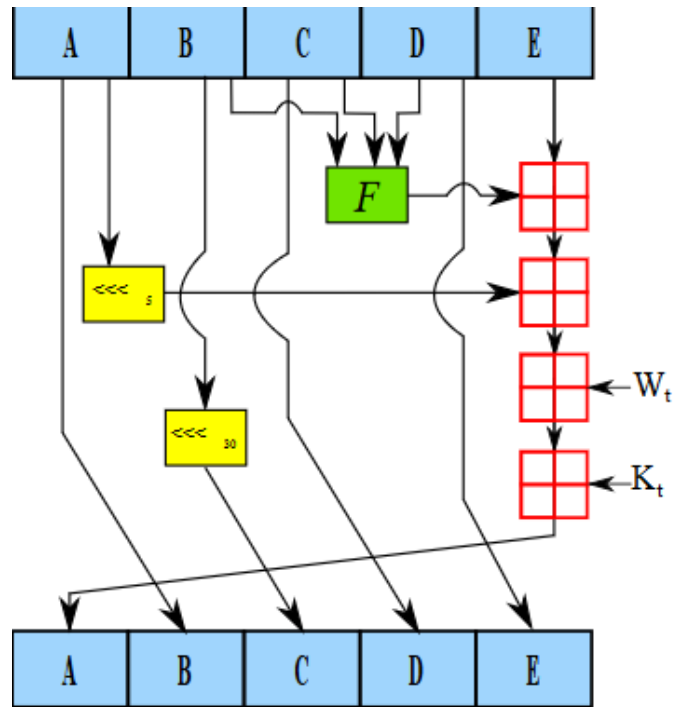


FIG 1.3 SHA-1 WORKING

DSA ALGORITHM ATTRIBUTES:

Global public elements

- P ; a prime n
- Q ; a prime divisor of $P-1$
- G ; $G = H^{(P-1)/Q} \pmod{P}$, $1 < H < P-1$

User's Private Key

X : a random integer where $0 < X < Q$

User's Public Key

$Y = G^X \pmod{P}$

User's Per message secret number

K =a random integer where $0 < K < Q$

Signing function

- $R = (G^K \bmod P) \bmod Q$
- $S = [K^{-1} (H(M) + XR)] \bmod Q$
- Signature = (R,S)

Verifying function

- $W = (S')^{-1} \bmod Q$
- $A = [H(M') * W] \bmod Q$
- $B = (R')W \bmod Q$
- $V = [(G^A * Y^B) \bmod P] \bmod Q$

Test

- $V = R'$

DSS Approach to Digital Signature

In DSS (Digital Signature Standard) the digital signature is generated with the help of global public key.

Also in DSS the digital signature is generated into two parts (s, r) and the verification is done using public key of sender, global public key and then the result is compared using the test function.

The message is first passed through a function (using SHA algorithm)

This hash code of message is now passed to signing function.

Now, sender's private key and global public key are used in signing function to generate digital signature

Now, the resultant is a digital signature and has two parts (s, r) .

This digital signature is now attached to message and is passed through hash function.

The public key of the sender and global public are used in verification function.

In the end the results of verification function and digital signature is compared in test function.

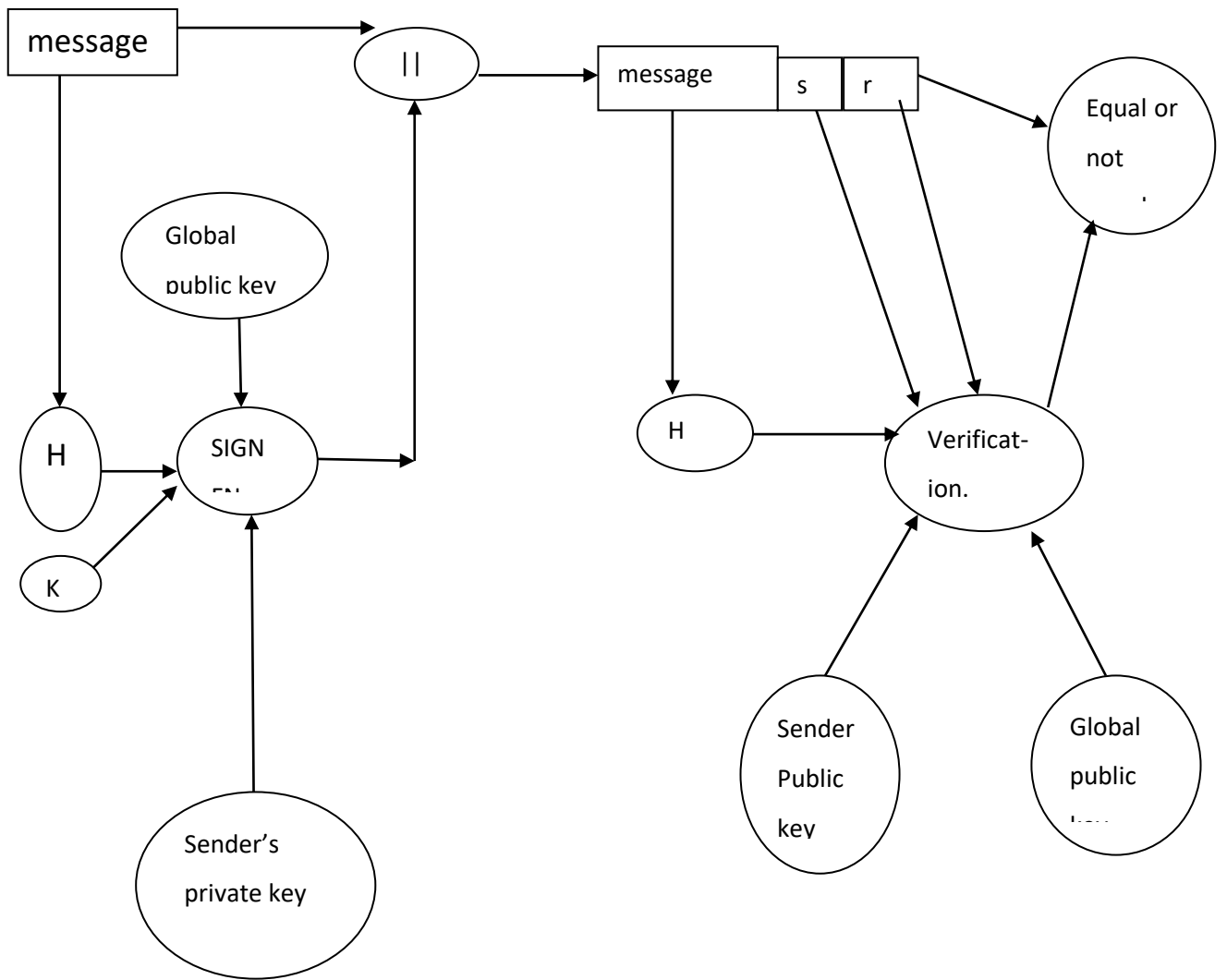


FIG 1.4 DSS approach to digital signature

RSA ALGORITHM

The start of RSA idea was dependent on the fact that it is time consuming to divide large integers and also RSA algorithm is asymmetric algorithm which means it will work on two keys that is public and private keys.

The RSA digital signature way will apply the communicator's private key to a message data to originate a digital signature. The digital signature after that can be confirmed by applying the next coming public key to the received data message and the digital signature through the digital verification process will provide either a CORRECT or INCORRECT result. There are two main operations of RSA algorithm which is sign and to verify which main thing for authentication and integration are to verify.

Let's suppose that we have one client1 and it sends its public key to the server and requests for data to reply back.

The server will reply and will encrypt the data using client1 public key and client1 will receive the data and then it will decrypts it.

MECHANISM BEHIND RSA ALGORITHM USING PUBLIC KEY

- Select two prime no's. let **P = 46 & Q = 91.**
- Now First part of the Public key will be: **n = P*Q = 4186 .**
- We also need a small exponent say **e :**

But e Must be in an

- An integer.
- Not be a factor of n.

1 < t < m

- Let us now consider it to be equal to 3.
- Our Public Key is made of n and e.

MECHANISM BEHIND RSA ALGORITHM USING PUBLIC KEY.

- We need to calculate $\Phi(n)$:

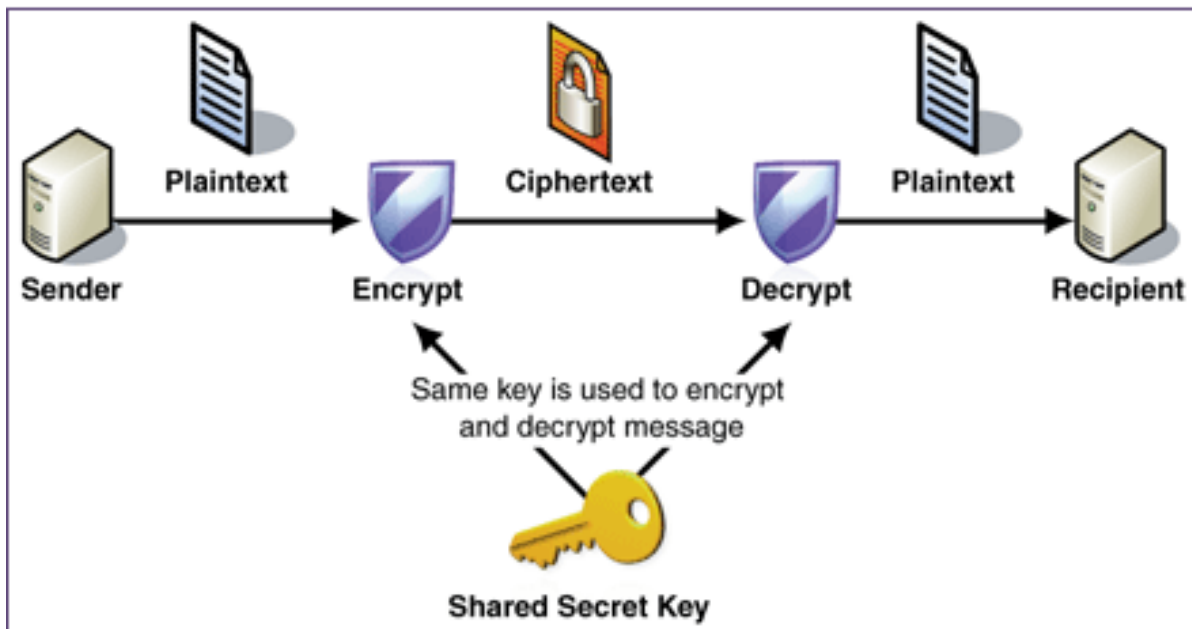
➤ This implies $\Phi(n) = (P-1)(Q-1)$
 $O(K) = 4186$

✓ Now we will find out the Private Key, K :

➤ $d = (k * \Phi(n) + 1) / e$ for some integer l

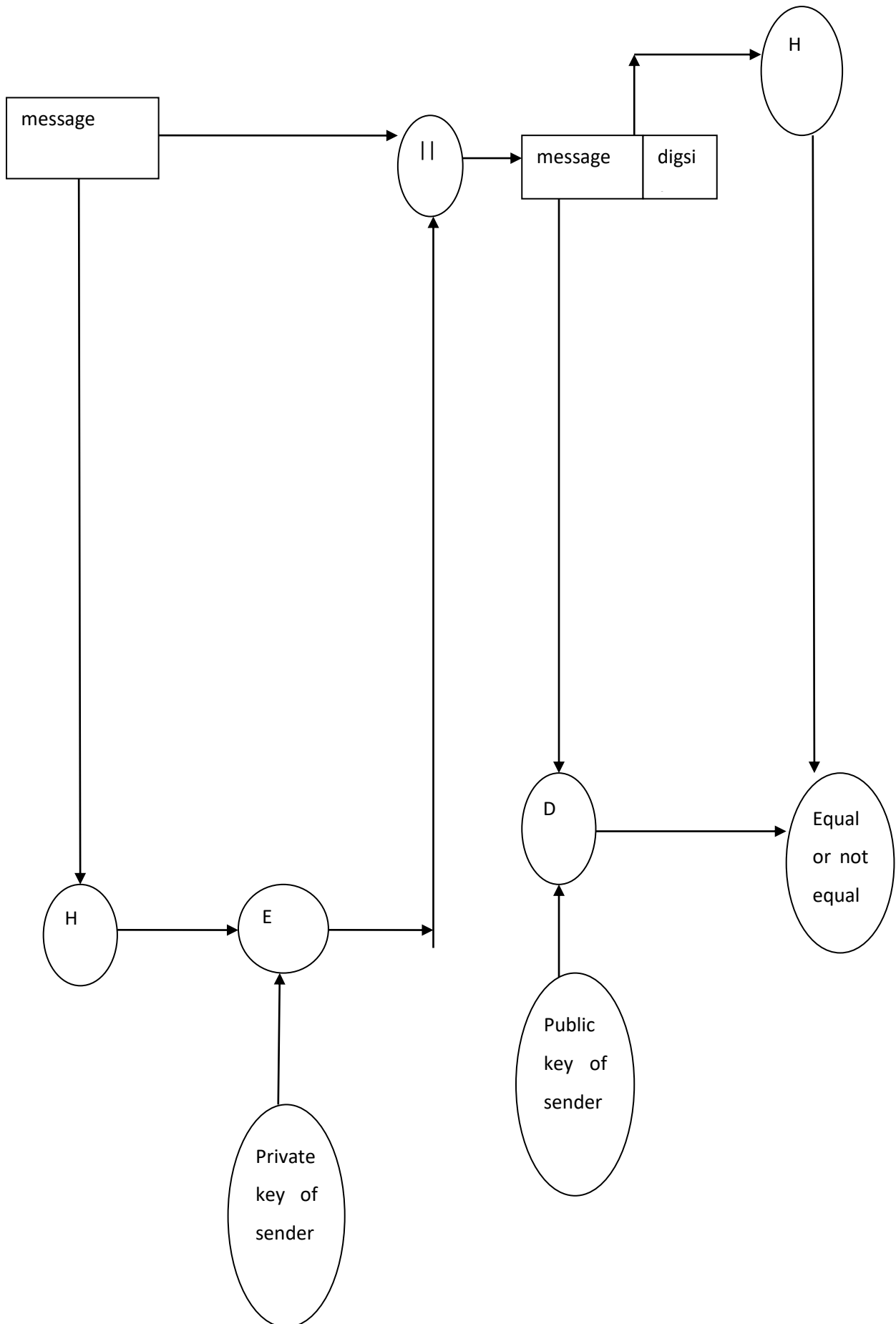
➤ For $k = 7$, value of d is 7866.

This algorithm is considered to be one of the most secured algorithms and because of that it uses wide range of integers as the key to perform the encryption and the decryption. The main steps are first key generation second encryption and the third one decryption. The signature after that can be confirmed by registering the next coming public key to the data message and through that signature there will be accurate confirmation.



- Client will decrypt the information and will write this one data. Then RSA message which is encrypted will be reply back to backend.
- Backend will decrypts RSA message from any person and log it into console. The Server will initiate AES key, and reply back to that particular person.
- Clients will decrypts RSA encrypted AES key and then will logs it on screen. Client sends AES encrypted message to main server.
- Server will decrypts the AES message which is from person and will sign in it on the console.
- Client will decrypt the AES messages and it is signup on the screen.

FIG 1.5 RSA APPROACH



RSA approach to digital signature

- In RSA approach unlike the DSA approach the message first passes through hash function .
- This hash digest is then encrypted using encryption algorithm using the private key of sender.
- The message after encryption is the digital signature which is then attached to message file.
- The message file is now decrypted using the public key of sender and also the message and digital signature is again passed through hash function.
- Unlike the DSA approach here the digital is not generated in two parts(s, r) rather the digital is generated as a single entity.
- Finally the two outputs are compared in the end. If the outputs are equal then digital is valid otherwise not.

PURPOSE OF DIGITAL SIGNATURE TEST PLAN

Electronic fields has taken several years to transform like electronic data interchange and it is used to confined to a nearer group where the different parties have enjoyed working relationship and trust other parties. Electronic field is touching heights of success and also have become the fastest growing communication channel in decades. With increase in communication or sharing data has begun our major concern increases with different institutions like banking, insurance and other financial things.

For the main security reason it is to protect the data, to protect the integrity of any message which shows end to end security. So, apart from the how secure our data is and the integrity part let's focus on extended issues which are:-

- The repudiation of data and discharge of a message.
- Risk of hacking the data or manipulating data.

- Corruption or loss of data.

CRYPTOGRAPHY

As today we can freely use the open network and can communicate very easily through systems. It also introduces the different challenges to the implementation of the vast network which is secured electronic. The regular use of the electronic fields it poses the problems of many to many different transactions.

The art of keeping a data secure here cryptography can be used as:-

- To hide the information we have in data.
- To authenticate data.
- To prevent the undetected modification.
- To prevent repeating data.
- To prevent the unauthorized use.

There are different ways to protect the data which is stored or not stored but to keep safe the confidentiality of financial secured data and other personal data records of data. The different techniques of encryption are serious for the development and information that is global and other technologies.

ENCRYPTION

Each clear text is muddled into incomprehensible text in encryption technique and also will hold the different and secret code key which is muddled. There is basically a mathematical formula by which the digital messages are muddled and unbundled.

Different algorithms are used like DES and RSA. Asymmetric algorithm generally have three code number because apart from the keys which are public

and private of a sender and a receiver, there is a common thing which is more secure and also hard calculate either private key.

PERFORMANCE TESTING

TEST RISKS

- Repeating data
- Modified/manipulated data
- Loss of data

Approve the test case here we can modify the name.

Workflow Transition Details

Name*:

Require electronic signature: Yes

Conditions

The following users / roles are allowed to execute this transition:

Condition Type

The creator of this test case can execute:: No

The owner of this test case can execute:: Yes

SIGNATURE IS HASHED AND VERIFIED

[← Back to List](#) [☰ View Item](#) [↶ Revert](#)

Change ID: 25

Change Date: 6/14/2016 1:34:38 PM

Changed By: System Administrator

Change Type: Modified

Artifact: [Test Case \[TC:18\]](#)

Field Set: Standard Fields

Artifact Name: Adding new author and book

Signed: Valid

Signature Hash: 6a0c58c5ebc95a8a466e2455742e58bc0a10a22c8d26cb5c409bf468cab1366c

Change Actions

Field Name ▲▼	Old Value ▲▼	New Value ▲▼
---------------	--------------	--------------

The hash will be stored with the history change record. Id will be given to the given data type of mode we entered is modified if sign is valid the data will be stored and will pop up that it is valid and it is invalid then it will pop up as invalid. When complete such process automatically a hash function generates the value. Every hash value is different from the other hence results that is it valid or not.

When the previous data records are being displayed on the screen, the record is dynamically re-hashed and after that it is compared with the stored hash values. This prevents someone alleviate with the data, so it will display a special data to indicate that the digital signature associated with the change is valid or invalid.

ITEM TO TEST	TEST DESCRIPTION	TEST DATE	SIGNED
#25	System administrator	15-11-2018	Valid
#24	System administrator	14-11-2018	Not signed
#25	System administrator	14-11-2018	Not signed

TEST PLAN APPROVAL

The digital signature test plan document and agree with the approach it shows to the database.

- Signature: RAM date: _____

Print name: _____

Title: _____

Role: _____

- Signature: PALLAVI date: _____

Print name: _____

Title: _____

Role: _____

- Signature: VAIBHAV date: _____

Print name: _____

Title: _____

Role: _____

These are list of the individual whose signature are required and also to fill up the details. Result will be printed in database.

TESTING HASH FUNCTION:

Before jumping into the testing of hash function. First we will know about the hash function.

The encrypted hash along with the other different data information such hashing algorithm is the digital signature. The main reason for encrypting the hash function instead of the entire data the hash function will automatically convert any random input to a constant length and that is way shorter this will save time as the hashing function is much faster than signing because it perform particular task. The hash function is different from others to be the hashed stored data also to modify any data even if it is a single character it will result in a devious values. If the case is that the decrypted result matches the other computed hash of the same data, then it will prove that the data hasn't modified at all and as it was digitally signed. In other way integrity or the digital signature was made with private key then that doesn't correspond to the public key as it presents by the signer which is authenticated.

REQUIREMENTS FOR HASH FUNCTIONS

1. It can be registered to any random size message L.
2. It can produce fixed length output.
3. It is easy to compute $h = H(L)$ for any random message L.

4. If Y is illogical then to find K.. $H(K) = H(Y)$.
5. It is illogical to find Y, K.. $H(K) = H(Y)$.
6. It is one way property.

SECURE HASH ALGORITHM

- SHA was designed on 1995.
- Produces 160-bit hash values.
- Based on design of MD5.
- SHA was revised in 2002 with the hash value of length 256, 384, and 512 bits.

We will follow steps

PASSWORDS AND OTHER PASS-PHRASES.

- We will prompt the user for a entering their name and password.
- After that we will verify that the identity of checking that password is valid or invalid.
- In other systems the password were recorded and were saved.
- Mostly we are using a hash function where later result can be used easily so that it can used to search the input values
- We will either take a constant sized input for example 8 characters.
- Now based on a hash function we have to acquire a variable sized input to make a new value.
- It is necessary that the passwords are choose with concentration so that no change or modification can be done.

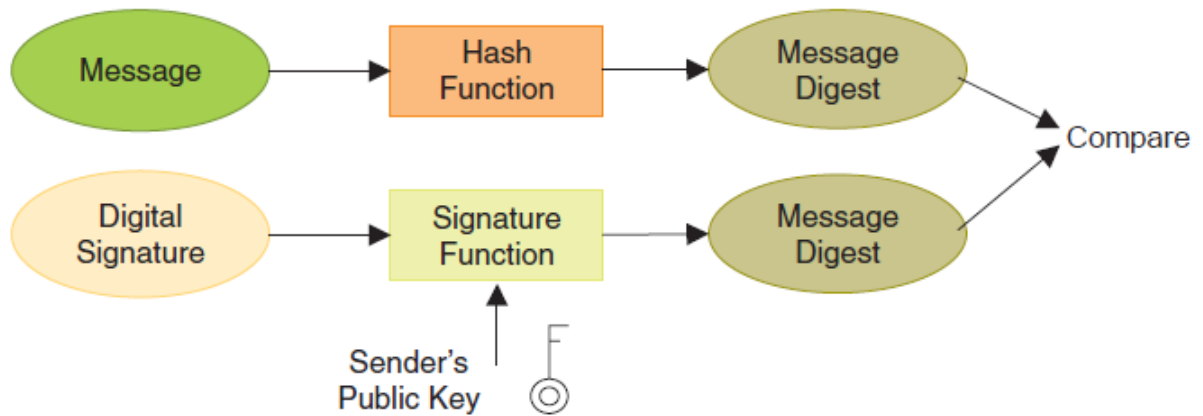


FIG 1.6 HASH FUNCTION

A hash function is registered to the message that can have a fixed-size message digest for better result. The signature function will use the message digest and then the sender's private key to acquire the digital signature. It is a very easy form of the digital signature which is obtained from the encrypting the message digest using the sender's private key. In above diagram we have one message which is to be delivered at the other end in between we have hash function where the generation of code will be made after making of hash function the message digest will perform different functions. On the other hand we have digital signature already there which comes across the signature function which also go through the message digest after performing both tasks we will compare them both and result will be shown.

CHAPTER V

RESULT AND PERFORMANCE ANALYSIS

PERFORMANCE ANALYSIS OF ECDSA AND RSA

Some the basic parameters that are used for comparison are rate of Generation and signature verification, security level per bit key size, and the length or span of actual digital signature in bits. Some basic measure has been adopted regarding the features of Secure Charging Protocol. It is clearly notable from the graph that the time of execution for signature verification is much shorter for RSA as compared to Elliptical Curved Digital Signature Algorithm. But the time of execution for RSA digital signature scheme is much longer as compared Elliptical Curved Digital Signature.

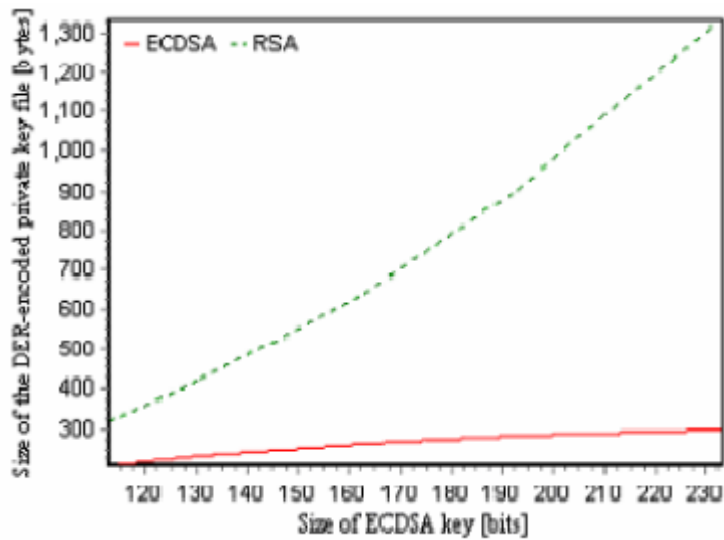
We will first compare the ECDSA and RSA on the basis on data overhead.

1. Choosing optimal scheme with respect to Data Overhead:

The open SSL programs are used to generate keys of different sizes for RSA digital signatures. The value of RSA approach has been found with key sizes providing an almost same level security as that of Elliptical Curved Digital Signature.

In the 3 parameters i.e. certificate files, key and signature there is a significant increase in size with increase in size of key for RSA digital signature technique. But this ascent is not so steep in ECDSA technique of digital signature. Because of relatively small growth of size of signatures, key and certificates the Elliptical Curved Digital Signature technique can applied easily in future for key sizes. Therefore ECDSA is a better option with respect to data overhead.

The figure below shows the variation private key with respect different digital signature techniques.



1. Preferable option in case of CPU time

The data packet on travelling along the route have node which consist of different type of roles over the route to execute different cryptographic features like verification or signing process or both.

TABLE I TIME FOR SIGNATURE OPERATIONS WITH DIFFERENT SIGNATURE SCHEMES ON A STRONGARM CPU @ 206 MHz

Year	Level of Security (key size[bits])		Time for Signature Generation [ms]		Time for Signature Verification [ms]	
	<i>ECDSA</i>	<i>RSA</i>	<i>ECDSA</i>	<i>RSA</i>	<i>ECDSA</i>	<i>RSA</i>
1999	113	512	2.8	13.7	7.5	1.3
2006	131	704	3.8	32.4	11.5	2.5
2015	163	1024	5.7	78.0	17.9	4.3
2026	193	1536	7.6	251.9	26.0	9.7
2039	233	2240	10.1	731.8	37.3	20.4

The second figure represents the change in performance of 163-bit Elliptical Curved Digital Signature and RSA of 1024 bits which is dependent on the average of route length. The networks having relatively small number of average hops between corresponding node and the mobile node, the Elliptical

Curved Digital Signature Algorithm having lesser average of CPU time per packet should be considered a better option. But the RSA gives better results for networks having more than five hops. AN analysis of multiple ad-hoc network showed, assuming UDP (User Datagram Protocol) traffic, the following scheme improves the efficiency for less than about five intermediate nodes. Thereby in most cases Elliptical Curved Digital Signature Algorithm is better option.

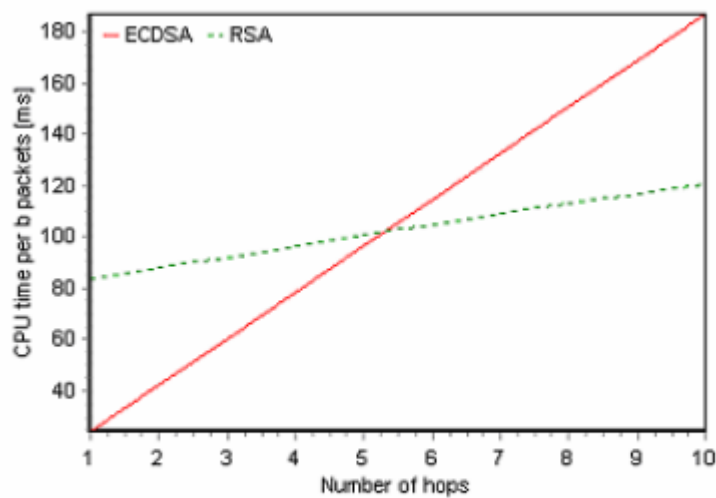
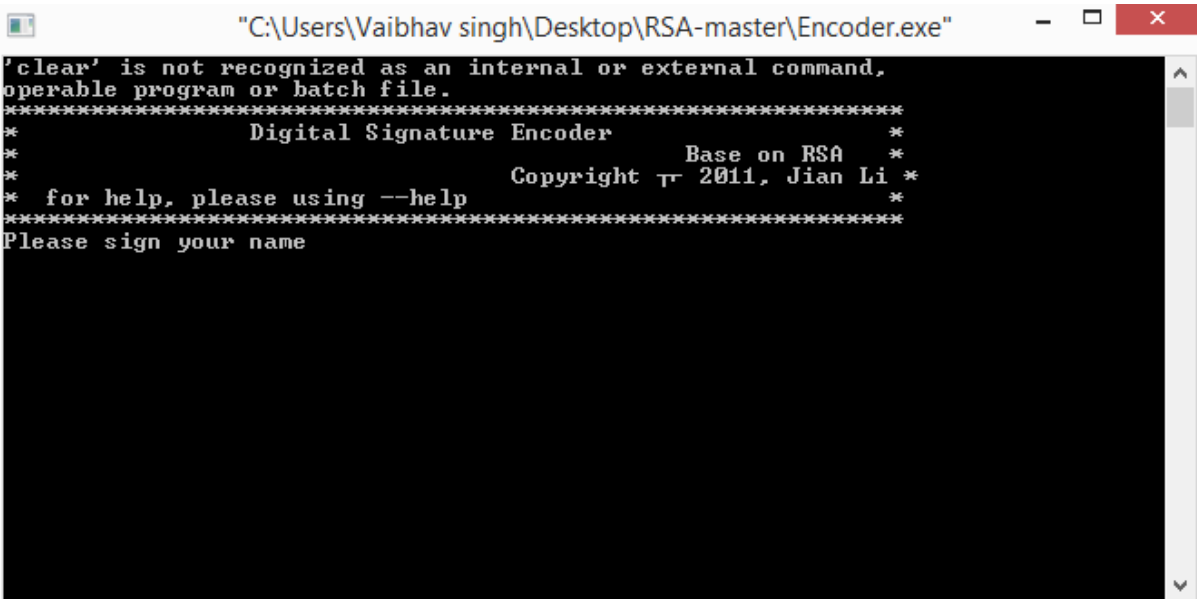


Figure 2. Influence of the topology on the performance of ECDSA and RSA

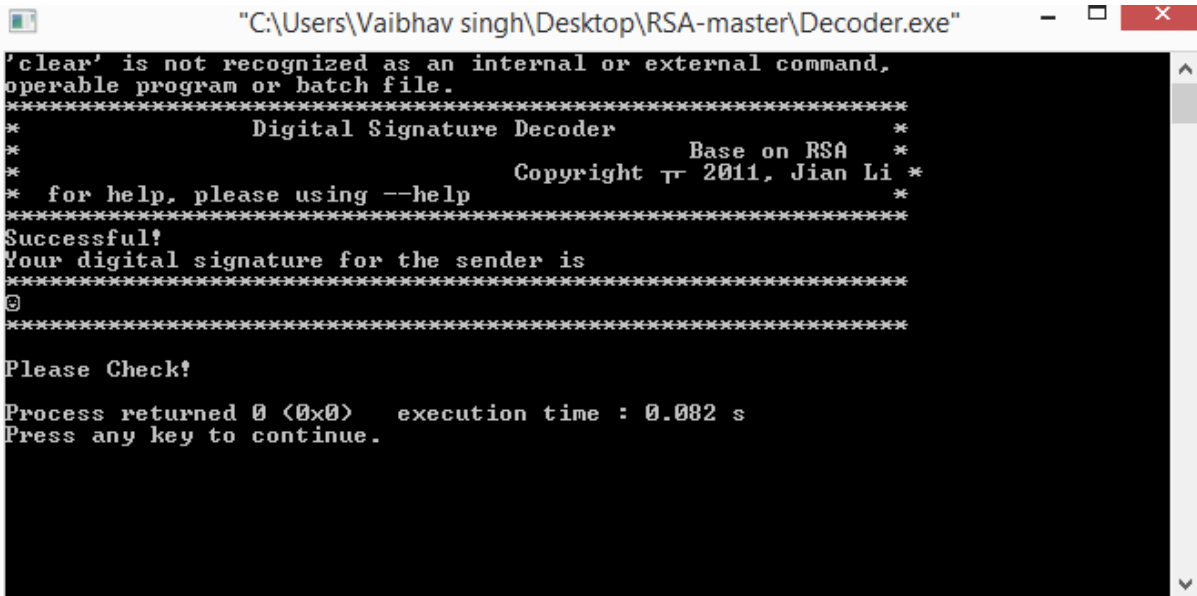
FIG 1.7

```
C:\WINDOWS\system32\cmd.exe
Expecting nothing
ok
Trying:
  dsa_key = {
    'Q': 11,
    'P': 23,
    'G': 4,
    'pub': 8,
    'priv': 7}
Expecting nothing
ok
Trying:
  sig = (2,3)
Expecting nothing
ok
Trying:
  print dsa.dsa_verify(sig[0], sig[1], dsa_key["G"], dsa_key["P"], dsa_key["Q"
1, dsa_key["pub"], message)
Expecting:
  True
ok
4 items had no tests:
  __main__
  __main__.__digits_of_n
  __main__.__random_s
  __main__.__modexp_lr_k_ary
2 items passed all tests:
  9 tests in __main__.dsa_sign
  8 tests in __main__.dsa_verify
17 tests in 6 items.
17 passed and 0 failed.
Test passed.
C:\Users\Vaibhav singh\Downloads\project\pydsa-master\pydsa>_
```

Generating output of DSA algorithm



```
"C:\Users\Vaibhav singh\Desktop\RSA-master\Encoder.exe"
'clear' is not recognized as an internal or external command,
operable program or batch file.
*****
*           Digital Signature Encoder           *
*                                           Base on RSA *
*           Copyright © 2011, Jian Li *
* for help, please using --help *
*****
Please sign your name
```



```
"C:\Users\Vaibhav singh\Desktop\RSA-master\Decoder.exe"
'clear' is not recognized as an internal or external command,
operable program or batch file.
*****
*           Digital Signature Decoder           *
*                                           Base on RSA *
*           Copyright © 2011, Jian Li *
* for help, please using --help *
*****
Successful!
Your digital signature for the sender is
*****
Ⓜ
*****
Please Check!
Process returned 0 (0x0)   execution time : 0.082 s
Press any key to continue.
```

Generating output of encoder and decoder of RSA master.

```
"C:\Users\Vaibhav singh\Desktop\RSA-master\RSA.exe"
'clear' is not recognized as an internal or external command,
operable program or batch file.
*****
*                RSA Public Key Generator                *
*                Copyright © 2011, Jian Li                *
* for help, please using --help                          *
*****
Please Wait...
Total Trial = 42
Total Trial = 190
Successful!

Process returned 0 (0x0)   execution time : 8.573 s
Press any key to continue.
```

RSA master results of trials

CHAPTER VI

CONCLUSION

The digital signature ensures a high degree of security and integrity in the document. With the use various digital signature algorithms the authenticity of these signatures is maintained. The algorithms implied in the signing process provides high level of security as they generate their secret keys by output of one or more hard problems like discrete logarithms, permutation of polynomials etc.

The digital signature is a great cryptographic scheme that can ensure:

- Security of the information from foreign attacks and forgery.
- Even if there is forgery in any phase i.e. even by the third party, it can be detected very easily using digital signature.
- Digital signature is a fast technique of verification and authentication as compared to pen paper. Thereby saving a lot of time.
- The traditional pen and paper signature are costly as compared to the digital signatures as the cost paper and ink is reduced. Once the digital signature software is established there is no need of thousands of paper and ink required for traditional signature scheme.
- The Digital Signature technique is environment friendly as it's an electronic way of verification thereby avoiding the use paperwork.

FUTURE SCOPE

Nowadays digital signature is future of electronic verification techniques. Now we need to frame the various laws, policies and legal procedure to make digital signature scheme available for government implementation

The traditional signature schemes were the basis of all the government and legal procedures for thousands of years. But with the change of time the techniques of signatures of also have been changed. From seals, stamps to pen and paper now is the era of digitization So the digital signature will be indispensable in the near future for various legal procedures.

REFERENCES

1. Authors: Hua Zhang, Zheng Yuan, Qiao Yan Wen /Title: A digital signature scheme without using one way hash function and message/data repeating and its application on key agreement.
2. Authors: M.Khalil, M.Nazrin, Y.W. Hau/ Implementation of SHA-2 Hash Function for a digital signature system on chip in FPGA
3. Authors: Ying Qin, Chengxia li, Shouzhi Xu/ A Fast ECC Digital Signature based on DSP
4. Author: Guilin Wang/ An Abuse-Free Contract – Signing Protocol Based on RSA Signature.
5. Authors: WANG Shaobin, HONG Fan, ZHU Xian./ Optimistic Fair-exchange techniques based on DSA algorithm.
6. Authors: Xinyi Huang, Yi Mu, Robert H. Deng/ Preserving Transparency and Accountability in Optimistic Fair Exchange of Digital Signature.
7. Author: C.N. Zhang/ Integrated approach for fault tolerance and digital signature in RSA.
8. Author: J.Schwenk, K.Huber/ Public key encryption and digital signature based on permutation and combinations polynomials

