Proposed Digital Signature Using One Time Pad

Dr. Shaimaa H. Shaker
University of Technology,Computer Engineering Department/Baghdad
Email:sh_n_s2004@yahoo.com

Received on: 21/5/2012& Accepted on:4/10/2012

ABSTRACT

Authentication protects two parties from the third party, but not protect against each other. Digital signature verification of the message source, protects the authority from anyone.

This paper proposes a solution for digital signature generation to digitally signing an submitted request to library website using the one time pad(OTP). In this paper, we focus our attention on decreasing the electronic requests security vulnerability by securing requests using an approximate one-time pad. A one-time pad, considered to be the only perfectly secure cryptosystem, secures an electronic request message for transport over any medium. The keys generated from request information using proposed hash algorithm deal with multiple parameters each one has multi state (0,1,2,3) as input and output hashed key of (0..9) state.

Keywords: Security threats , Digital signature, One time pad, Hash function.

اقتراح توقيع رقمي باستخدام نظام المرة الواحدة

الخلاصة

المصادقة حماية الطرفين من الطرف الثالث، ولكن ليس حماية ضد بعضها البعض. التوقيع الرقمي يتحقق من مصدر الرسالة، ويحمي السلطة من أي شخص.

تم اقتراح حلا لتوليد التوقيع الرقمي للتوقيع رقميا على طلب تقدم به موقع مكتبة باستخدام نظام المرة واحدة (OTP). في هذا البحث، نحن نركز اهتمامنا على خفض ضعف أمن الطلبات الالكترونية من خلال تأمين طلبات باستخدام تقريبي نظام المرة الواحدة .حيث ان نظام المرة الواحدة يعتبر نظام تشفير آمن تماما، ويؤمن نقل رسالة الطلب إلالكتروني من خلال اي وسط. المفاتيح ولدت من معلومات الطلب باستخدام خوارزمية التجزئة المقترحة التي تتعامل مع معاملات متعددة كل واحد له حالات متعددة (٠،١،٢،٣)، كمدخلات والمخرجات هي مفتاح من دالة التجزئة بحالة (٠ .. ٩) .

https://doi.org/10.30684/etj.31.2B.13
2412-0758/University of Technology-Iraq, Baghdad, Iraq

INTRODUCTION

Modern computer network makes it possible to transmit and distribute information quickly, securely and economically. This is because of decreasing cost of the equipment needed to copy, print and fast process of information. These features enable people to try investigating methods to protect information. Mobile devices have become indispensable tools for today's highly mobile workforce. Small and relatively inexpensive, these devices can be used for sending and receiving electronic mail, storing documents, delivering presentations, and remotely accessing data. While these devices provide productivity benefits, they also pose new risks to organizations.

Mobile device users are demanding fast and efficient connections that support data applications. Wireless connection has to be provided by the networks and protocols, mobile networks must function efficiently by using their protocol, performing routing and management for mobile device users [1]**.** Mobile communication systems are characterized by a variety of features. The attributes of all mobile communication systems are the mobility of at least one of the connection users and the lack of wire line connection of this user's terminal with remaining part of the system. One of the classification criteria of the mobile systems is their degree of complexity, the range of the offered services and operation cost [2].One way to counter security attacks would be to cryptographically protect and authenticate the control and data traffic. The strong cipher system can be used with authentication based on hash function. A one-time pad is a very simple yet completely unbreakable symmetric cipher where the same key is used for encryption and decryption of a message. To use a one-time pad, you need two copies of a "pad" or key which is a block of truly random data. To encrypt a message each bit of each letter in the plaintext is combined with the corresponding letter's bit in the pad in sequence using a transformation called the bitwise exclusive or (XOR). This means that two bits are taken as input and produce a single bit as output. If the key is truly random, an XOR-based one-time pad is perfectly secure against ciphertext cryptanalysis. A pad is only used once and discarded, hence the name one-time pad[3].

A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified [4]. Another work was done on designing an off-line signature verification system based on a displacement extraction method [5] in which a questionable signature is compared with a corresponding authentic one . The goal of this paper is to build application for mobile devices that ensure users can securely send their librarian information via the GSM network. mobile library solution developed provide platforms for users to library using SMS .

Sections 2,3,4,5 introduces some definitions and preliminaries will use in the paper. Section 6 describes the proposed digital signature scheme. Sections 7 ,8 give discussions and conclusions.

MOBILE COMMUNICATION SYSTEM

Mobile communication systems manage resources, dispersed in space, such as a fleet of truck or service vehicles. Cellular Telephony is the next and perhaps the most representative example of mobile communication systems. The cellular phone system is characterized as a system ensuring bidirectional wireless communication with mobile stations moving even at high speed in a large area covered by a system

of base stations. The cellular system can cover whole country. Moreover, a family of systems of the same kind can cover the area of many countries. Initially, the main task of a cellular system was to ensure the connections with vehicles moving within a city and along highways. The power used by cellular mobile stations is higher than that used by the wireless telephony and reaches the values of single watts. Personal Satellite Communication Systems already do exist. The characteristic feature of currently existing satellite systems is uni-or bidirectional voice and/or data communication at a limited quality in very large areas. Their main advantage is their wide range. A new category of mobile systems has appeared in recent years. The wireless technology has been used to realize a wireless access to computer networks[6]. Smart phones and tablets can use a dedicated mobile device application for secure access to online services. The mobile device application uses the Web browser or Web service capabilities of the device for authentication and subsequent access to the service. This approach allows a cryptographic key to be used to authenticate the user, which protects against a man-in-the-middle attack.

THE SECURITY THREATS

One of the most serious security threats to any computing device is unauthorized use. User authentication is the first line of defense against this threat. Unfortunately, management oversight of user authentication is a persistent problem, particularly with handheld devices, which tend to be at the fringes of an organization's influence. Other security issues related to authentication that loom over their use include the following items[4]:Because of their small size, handheld devices are easily lost or stolen. User authentication may be disabled, a common default mode, divulging the contents of the device to anyone who possesses it.

• Even if user authentication is enabled, the authentication mechanism may be weak or easily circumvented.

• Once authentication is enabled, changing the authentication information regularly is seldom done.

• Limit processing power of the device, may preclude the use of computationally intensive authentication techniques or cryptographic algorithms[6].

DIGITAL SIGNATURE

A digital signature is a checksum which depends on the time period during which

it was produced [7] . It depends on all bits of a transmitted message and also on a secret key but which can be checked without knowledge of the secret key. A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified [8]. There are several benefits to implementing a mobile digital signing process:

- Faster Customer Acquisition: The results in a more efficient customer time and reduces the risk of cancellation.
- Cost Reduction: Process has reduced the cost of paper products, courier charges, and storage.
- Straight-Through-Processing: digital process removes the time consuming task of re-keying information and eliminates data entry errors.
- Easy Retrieval and Archiving: Automatically archived and easily retrieved when needed.
- Customer-Friendly Process: Offers an easy, and customers enjoy.

The idea of digital signature has derived from handmade one, so digital signature should have its all features. The main features of handmade signature are simple production, simple identification and difficult generation . General Key coding can be used both for confident ability and digital signature . For make confident ability, encryption key is private so that, everyone can code a message. Generation of digital signature is based on keeping encryption key private and decryption key is public. Digital signature depends some parameter , like person who signature and data that should be visited [9].

CRYPTOSYSTEM :HASH FUNCTION AND ONE-TIME PAD

A cryptosystem is a mechanism that allows two or more users to communicate in a secure manner, that is nobody but these users must be able to learn the content of the communication message. A hash function H is a transformation that takes a variable size input and returns a fixed-size output, often referred to as the hash value or h = H(x). The basic properties of a hash function are:

• The input can be any length
•The output has a fixed length
• H(x) is relatively easy to compute for any given x
• H(x) is one-way meaning it's difficult to invert

A perfect, or unconditionally secure cryptosystem, is an encryption technique that cannot be broken even if unlimited time and computational power were present. A common example of a perfect cryptosystem is the Vernam cipher, often referred to as one-time pad. At a character-level, all the bits in the first letter of the message m are XORed with all the bits in the first letter of the key k. This produces a binary pattern of the encrypted letter. So for example the first letter of the message m is the letter “b” and the first letter of the key k is “#” the resultant encrypted letter is the character “A”

The one-time pad has the following requirements, namely:

• Each key k is used only once
• The key k used to encrypt a message m is at least as long as m, that is length(k) ≥ length(m)
• Each key k is random and unpredictable

If these requirements are satisfied, the one-time pad is an unconditionally secure cryptosystem. However, the one-time pad has some associated difficulties in its practical implementation. These include the fact that a new truly random secret key must be issued prior to every communication and must be significantly long for large messages. Again, once a key is generated it must be distributed between the communicating parties. This aspect is commonly referred to as the key distribution problem, as the key k used in the encrypting and decrypting of messages m must only be shared between the communicating parties[10] .

THE PROPOSED METHOD

To generate a Digital signature one need to design an algorithm that can be used on customer's mobile. The proposed algorithm is capable of generating a unique digital signature code for each submitted request details using user's private key to sign the submitted request details and then input this submitted request onto mobile. Figure(1) explains the abstract of digital signature. The proposed algorithm is translated to a program has an easy to use graphical user interface (GUI) . The main steps of the proposed method are explained in algorithm(1).

The username, personal identification number, and digital signature code generator is never stored on the mobile in case of the mobile is stolen a third party cannot run the request as proper authentication is required to run the program.

The Proposed Function Using Multi-States of Multiple Keys to Generate the Digital Signature

The input used in the proposed hash operation function(f) may come in binary form and convert to a decimal-states input. Multiple inputs will be used with (f)operation , the first one is Code no with 16 characters length convert to 64 bits (each one represent with 4 bits) and consider to be the first operand of the (f)operation .The 64bits divided into 32 digits each one is 2-bits length of (0,1,2,3). The first operand detect the table number should be used of (f)operation (figure(3)) there are four tables of decimal-states , the second one will be the Acc No with 16 characters length convert to 64 bits (each one represent with 4 bits) . The 64 bits divided into 32 digits each one is 2-bits length of (0,1,2,3). The second operand detect the row number of specific table (figure(2)) each table have 4 rows(1,2,3,4) , and the third input to the (f)operation will be the value of Book No with 16 characters length convert to 64 bits (each one represent with 4 bits) . The 64 bits divided into 32 digits each one is 2-bits length of (0,1,2,3). The third operand detect the column number of the specific table each table have 4 columns(1,2,3,4), then the result of (f)operation's value is the cross point of row and column of specific table(Table(1)) explain the example aid applied of (f)operation. Figure (3) shows the three 32-bits input to the (f) operation , and the 64-bits output, these three inputs to the (f)operation should be firstly converted from 64-bits to 32 digits each may be one of four states (0, 1, 2, 3), i.e., each two bits converted to its equivalent decimal digits, using convertor function see algorithm(2). Then the (f)operation will be applied to generate a new 32 digits of (0-9) according to the random value in the tables then this 32 digits should be reconverted to 64 bits .

The value of these tables applied using algorithm(3) . Table (2) explains When changed test data and observed that their output and will be changed too.

Digital Signature Generation

The Digital Signature code is generated on the mobile by input the following operands from the library website onto the mobile interface.

Code No: A unique code provided by the library for each submitted request, unique for each user and each submitted request.

Acc No: It indicates the account to which submitted request has to be made. It's entered by the user.

Book No: It indicates the book number that the user wishes to deal with .

After entering these operands onto the mobile interface the user selects the sign option. The application concatenates these operands and the result is applied using proposed method that use multi-state(0,1,2,3) instead of (0,1) for each of these operands and return the result value as s of 64bit(0..9).

The message is then breaking into blocks of 64 bit length (i.e.: 8 digits) and padding extra bits if necessary. The result is then encrypted using user's Private Key to obtain the digital signature code (DS). RSA encryption scheme is used to encrypt the value of the submitted request details. See figure(4) .

f=Hash(Acc No, Code No, Book No)

SG= Encryption(private key of user, f)

Where, Encryption is RSA encryption function , Hash = proposed method Acc No = receivers account no Code No =code no for the particular submitted request

Book No = book number selected for submitted request. Algorithm(3) explain the steps of key generation. Figure(5)explains the digital signature generation using (f) operation.

First the library server generates unique (Private, Public) key pairs. The private key is making each submitted request unique for each user. The corresponding public key is stored in the database against the user's data. In order to make an application , the user enters the library site with authenticate way . When the library server receives an submitted request with submitted request details and digital signature code, the public key corresponding to the particular user is applied onto the digital signature code provided by the user to obtain back the hash result of the submitted request signed by the user. This ensures authenticity of the submitted request as only the user can sign the application using the corresponding private key pair.

The result is obtained back as follows, see Figure(6)

Verification = decryption using RSA (Public key of user ,SG)

The libraries server re-computes the hash of the submitted request details the library has received from the user and compares it with the decrypted hash. If both the hash results match, integrity of the application can be ensured and be sure that the submitted request was not modified. If the hashes do not match, it means that some modifications have been made in the submitted request and the submitted request cannot be proceeded and a corresponding message is send to the user.

DISCUSSION

The security requirements, such as authentication, confidentiality and integrity, always make computationally intensive processes and can easily become the bottleneck of the related applications. Digital signatures are used in message transmission to verify the identity of the sender of the message and to ensure that the message has not been modified after signing.

The risk of intrusion and eavesdropping goes up as electronic communication equipment becomes increasingly wireless and ubiquitous. With the specter of hackers/crackers looming, security is becoming a major consideration in a growing number of embedded systems. Digital signature schemes can be used to provide the following basic cryptographic services: data integrity (the assurance that data has not been altered by unauthorized or unknown means), data origin authentication (the assurance that the source of data is as claimed), and non-repudiation (the assurance that an entity cannot deny previous actions or commitments).

The increasing key sizes needed by proposed method for security against brute force attacks by powerful computers or distributed computing .

Proposed method introduce of Using the 4-tables of multi state (0,1,2,3) for substitution the new value for each digit ,these new values is based on using random function to generate the decimal values(0-9) for each table.

The security of proposed method will be increased by using the operation based on random function to generate the tables values each time so each request submitted has a unique signature while the block size and key length were still the same. The proposed algorithm works good with files with low size see Figure(7) .

Using asymmetric method provide good confidentiality , has integrity because using digital signature ,easy key generation ,easy key distributed when ensure authenticity of public key, acceptable power for short key length, time is acceptable for short key length. Using OTP

Using random function to generate the value of digital signature the permuted these values according the 4-tables each time make more complexity of digital signature even using small block size(at least 64bit). So the proposed method offer the authentic manner. The proposed method using GUI to easy and friendly dealing with user.

CONCLUSIONS

The proposed system is secure and consists of two parts, the first part is the software on the client's mobile to generate the digital signature code and the second part is the server side verification software to verify the authenticity of the user and integrity of the application based upon the digital signature code.
The results from the proposed solution have proven to provide secure and economic communications between the mobile application and the library servers. The proposed solutions allow the users to library using secure SMS **.**

REFERENCES

[1]. Richard N. and Ramjee P. "OFDM for Wireless Multimedia Communications. " , Norwood, MA: Artech House, 2000.
[2]. Korhonen, J. " Introduction to 3G Mobile Communications.", Second Edition. USA: Artech House, 2003.
[3]. Schneier,B. Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley Computer Publishing, John Wiley and Sons, Inc,1996.
[4]. Pankanti, S. R. M. Bolle, A. Jain, " Biometrics: the Future of Identification," IEEE Computer, vol. 33, pp. 46–81, 2000.
[5]. Mizukami,Y. M. Yoshimura, H. Miike, and I. Yoshimura, "An Off-line Signature Verification System Using an Extracted Displacement Function," . Pattern Recogn . Letter 32. 1573-1579. 2004.
[6]. Wayne J." Smart Cards and Mobile Device Authentication: An Overview and Implementation ", NISTIR 7206, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20988-8930 July 2005 .
[7]. Rivest, R. LA. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Communications of the ACM, vol. 21, pp. 120- 126, 2003.
[8]. Erfaneh,N. R.E. HAGHIGHI , F. Peyravi, A. K. zadeh ,"A New Digital Signature Algorithm", 2009 International Conference on Machine Learning and Computing IPCSIT vol.3 (2011) © (2011) IACSIT Press, Singapore.
[9]. Hwan and C.-C. Chen, S. J. "New multi-proxy multi signature schemes," Applied Mathematics and Computation,vol. 147, pp. 57-67, 2004.
[10]. Croft and M.S Olivier,N.J Using an approximated One-Time Pad to Secure Short Messaging Service ,University of Pretoria,2006.

Table(1) An example of applying the (f)operation based of figure (4)

1st input(Code no.)	2nd input(Acc o.)	3rd input(Book number)	Output(The random key)
1	**2**	**3**	**1**
1	**3**	**2**	**2**
0	**0**	**2**	**1**
3	**1**	**2**	**9**
2	**3**	**2**	**3**
2	**1**	**1**	**6**
1	**1**	**1**	**0**
1	**1**	**0**	**7**
0	**0**	**0**	**3**
3	**0**	**1**	**6**
1	**2**	**1**	**2**
2	**3**	**1**	**6**

Table (2):Different output of the same input.

1st input	2nd input	3rd input	Output
110322110312	**230131110023**	**322221100111**	**121936073626**
110322110312	**230131110023**	**322221100111**	**113420016739**
110322110312	**230131110023**	**322221100111**	**982346103018**

Algorithm(1)
Main-Steps algorithm;
Input :user name, personal identification number (PIN);
Output :digital signature;
Begin

1- **user input the library website (input user name, personal identification number (PIN))**
2- **the user selects from the library website the option called Make Submitted Request.**
3- **The user enters the information to be requested (account number and the book number) onto the library website.**
4- **The library provides a unique code number for this particular submitted request.**
5- **The user calls the proposed digital signature generation, then runs it on his mobile with authenticate way using his account number and password.**
6- **The user inputs the code number, account number and book number on the library website onto his mobile**
7- **The user selects from the library website the option called Digital signature generation .**
8- **input the digital signature generation and details of submitted request onto the library website to deal with the submitted request.**

End.

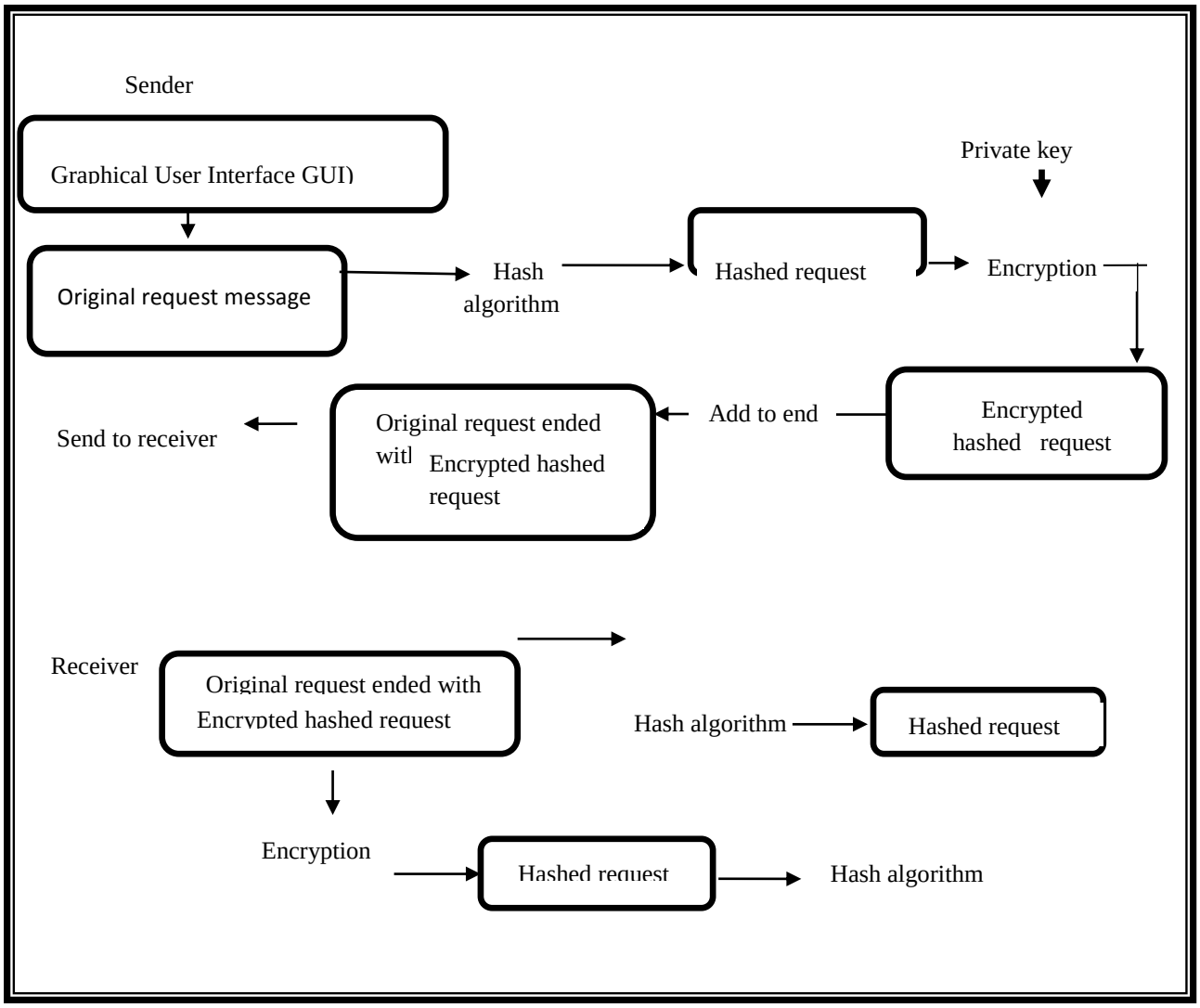
Algorithm(2)
Converted1 algorithm;
Input : 64 bit of(0,1)
Output: 32 digit of (0,1,2,3)
Begin

1- **Divided the 64bit into Blocks of 2bits.**
2- **Convert each Block to binary numbers**
   - **if 0 0 then 0**
   - **if 0 1 then 1**
   - **if 1 0 then 2**
   - **if 1 1 then 3**
3- **Output the result as 32 digit of (0,1,2,3);**

end

Algorithm(3)
The tables of (f)operation;
Input : 3 input each of one is digit of (0,1,2,3) states.
Output :digit of (0..9) states.
Begin
1- The 1st input is I.
2- The 2nd input is J.
3- The 3rd input is K.
4- For I=0 to 3 do
For J=0 to 3 do
For K=0 to 3 do
C[J,K]= Random integer number from 0 to 9.
Next K
Next J
Save the table C[J,K] in T[I]
Next I
End

Algorithm(4)
Key generated algorithm;
Input : 3 input of (32 digit of (0,1,2,3))
Output : key of 32 digit of (0..9)
Begin
1- Enter the 1st input(Code no.) that detect the number of table.
2- Enter the 2nd input(Acc no.) that detect the number of row in the table.
3- Enter the 3rd input(Book number) that detect the number of column in the table.
4- For all digits of three inputs , the cross point of row and column in the table is the output
5- The 32 digit of output is converted to 64 bit represent the key.
6- Send the key to the recipient.
End



Figure(1) :Abstract of digital signature

Table no.1	(f)	0	1	2	3
	0	3	9	1	0
	1	2	4	5	7
	2	6	8	0	9
	3	8	7	2	1

Table no.2	(f)	0	1	2	3
	0	9	1	4	3
	1	7	0	3	6
	2	8	2	5	1
	3	3	6	2	0

Table no.3	(f)	0	1	2	3
	0	1	4	2	7
	1	5	6	3	0
	2	0	3	9	8
	3	2	6	3	1

Table no.4	(f)	0	1	2	3
	0	1	6	3	5
	1	0	7	9	4
	2	6	2	8	0
	3	2	1	8	2

Figure(2):Tables of (f) operation :each time these values are change randomly

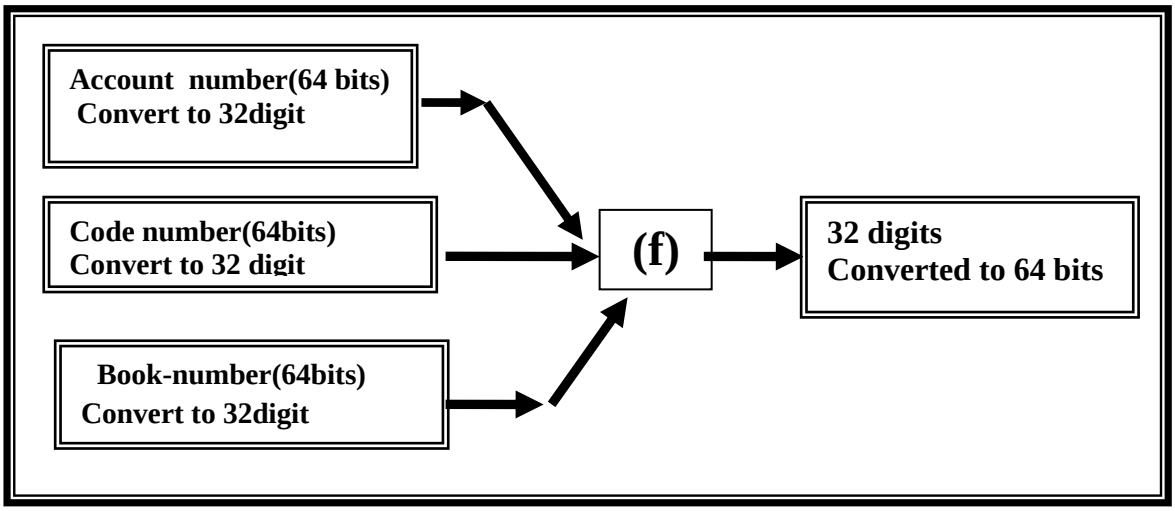
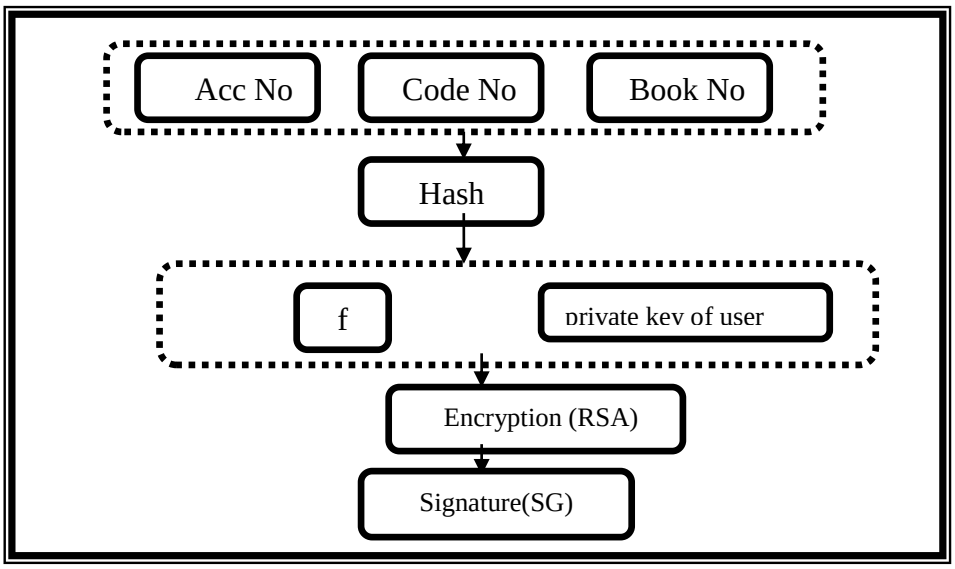
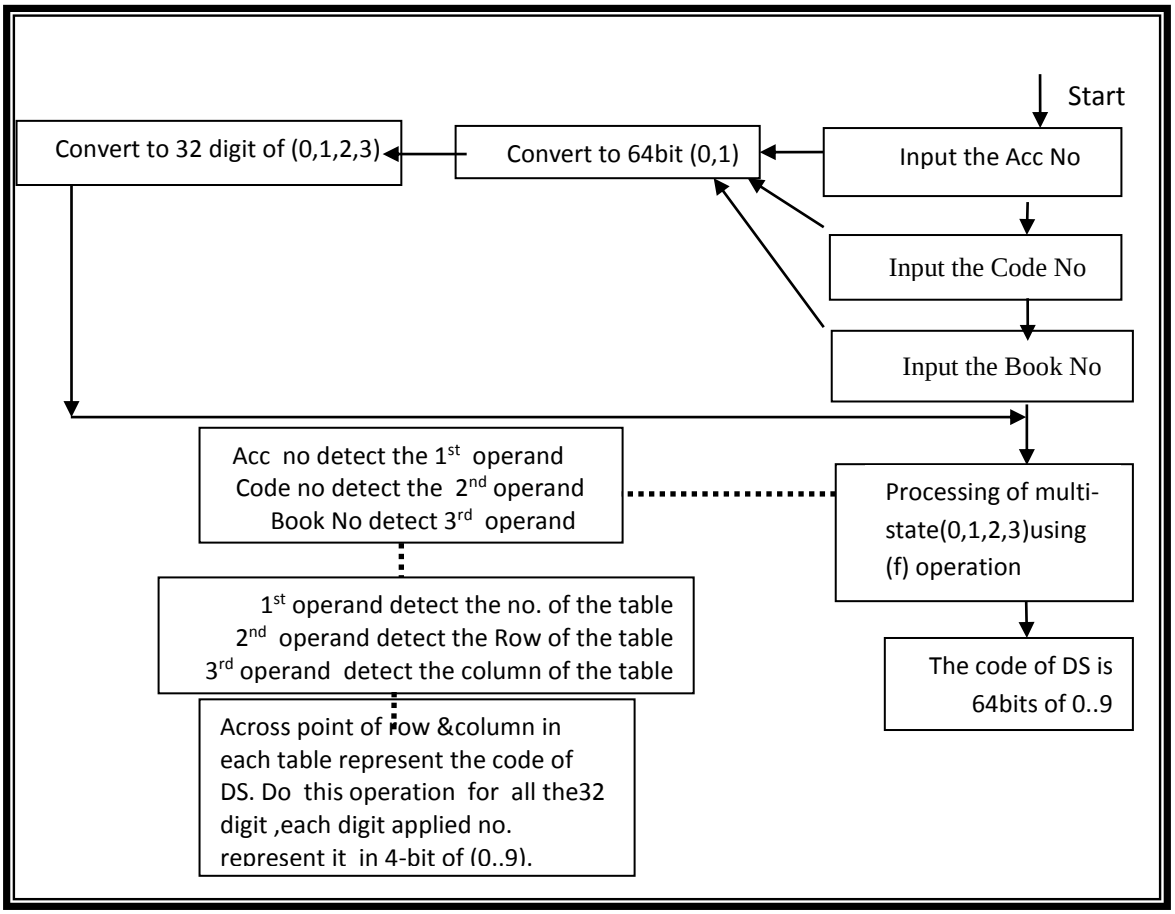


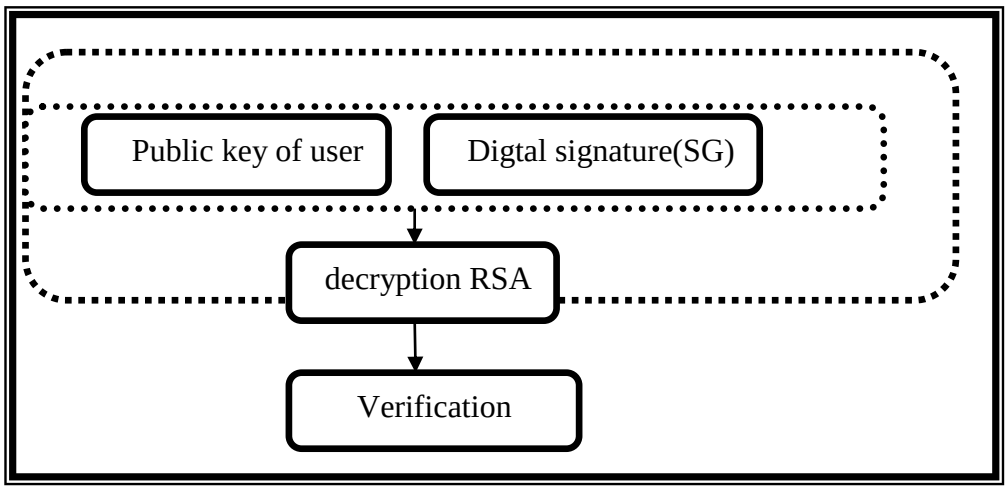
Figure (3) Inputs and Output of the proposed hash function ((f) (Operation) of proposed algorithm



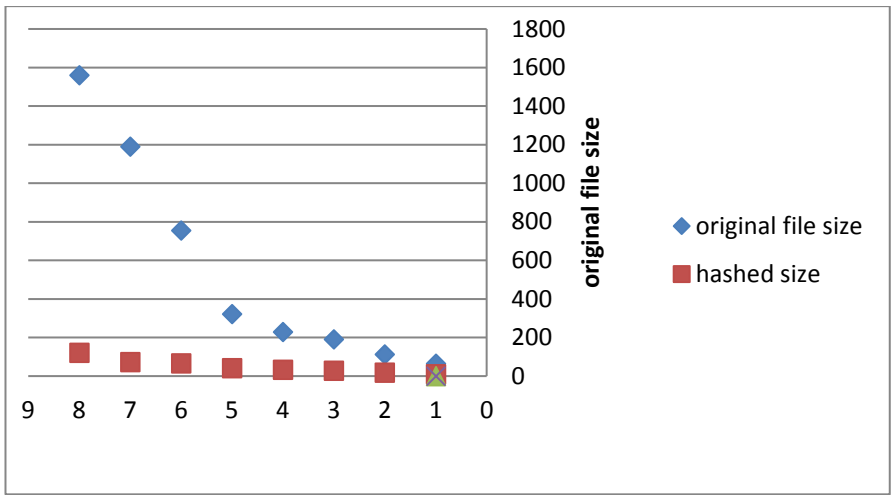
Figure(4):Explain the steps to produce the digital signature



Figure(5) digital signature generation using (f)operation.



Figure(6):explain the verification process using RSA.



Figure(7) Size of 8 hashed files