Achieving data integrity by forming the digital signature using RSA and SHA-1 algorithm

IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 5 (Mar. - Apr. 2013), PP 26-31
www.iosrjournals.org

Achieving data integrity by forming the digital signature using RSA and SHA-1 algorithm

Isha Shingari, Sourabh Singh Verma
M.Tech Computer Science Engineering, Dept. of Computer Science Engineering Mody Institute Of Technology and Science

Abstract: *Technology has been touching our lives in almost every domain. With the advent of modern technologies, the need of enhancing its security also arises. Data security has become one of the most important issues of concern. Data security is achieved with the help of adapting certain security measures. Here, in this paper we have analyzed the various cryptographic concepts. Encryption and decryption are two most important aspects of cryptography and data security. The special light has been thrown on data integrity and protection issues. The RSA algorithm has been explained. The implementation of the algorithm has also been given with the help of proving a graphical interface. The data integrity has been established at the client and receiver end by not limiting it to a standalone application.*

Keywords: *cryptography, data security, information security, data integrity, RSA, SHA-1, client/server*

I. Introduction

The concept of network security and cryptography is not new. It has been touching many areas which include the strong data encryption techniques, trusted third party access and a secure communication channel. While talking about data security, it can be considered as the main aspect of the secure data transmission over an unreliable network. Data security has become one of the major challenging issues which need a great deal of attention. The information could be accessed for malicious reasons. Therefore it has become very crucial to come up with the suitable security measures for making the data security stronger[1].

The meaning of information security suggests the protection of information systems from the unauthorized use, disclosure, modification, perusal, recording, destruction or access. This area is often related with the protection of integrity, availability and confidentiality of information.

The key concepts associated with information security are integrity, confidentiality, availability, authenticity and non-repudiation. The term integrity suggests that the data cannot be modified undetectably. It can be considered as the special case of ACID transaction processing. Confidentiality is the term which is used to denote the disclosure of information to unauthorized individuals or the systems. The credit card transactions on the internet preserve the confidentiality and thus maintain the privacy of the people.

Availability means that the information should always be available when it is needed. The computing systems which are used to store and process the information, the security controls use to protect it and communicate channels used to access it, must function in the correct manner. It thereby ensures the protection of information from the Denial Of Services attack.

The authenticity of information means that the data, transactions, communications and documents used should be genuine. There is a validation of both the parties and it is checked whether they are same which they claim to be. The non-repudiation means that the two information exchanging parties cannot deny their retrieval and transmission of information. It means that the one party cannot deny the fact of receiving the information nor the other party can deny having sent the information.

II. Data Integrity

The term data integrity suggests the security against the unauthorized modification of messages. The data integrity is very close to the classical subjects in communication which is the error detection code. The latter one is the procedure for the detection of errors which can be introduced in the messages due to the fault generated in the communications. It is often considered that by the usage of the information which has been modified maliciously, stands at the same risk as using the information which contains the defects due to the errors introduced in data processing or communications[2].

The asymmetric and symmetric ciphers play a remarkable role to establish the user authentication and confidentiality, but it cannot guarantee the data integrity. There must be alternate measures for ensuring the data integrity which can be possible through the added layer of security. Message digests generally posses the following characteristics:

- A variable length input is taken which is used then to generate the fixed length output which is known as the hash or a message digest.

- It is not computationally feasible for calculating the message which is based on the digest.
- It is also infeasible to find out the two messages which will generate the same digest, this feature is known as collision resistance.
- Thereby, the message digests or hashes achieve the data integrity by applying of the complex math to the data for ensuring that this data has not been tampered on its route towards the final destination.
- Data integrity is needed only in the situations where the value of data being transferred is high enough to warrant the added layer of security versus the risks involved in exposing the digital data.

III. Cryptography

The word “cryptography” has its Greek origin and it is literally translated as the “secret writing”. When the digital communications were not invented, the cryptographic methods were the only way used by military people for espionage. With the advent of modern technologies in communication, the individuals and businesses can transport information at a very marginal price with the help of public networks like Internet. This makes the data to be exposed over the medium. Therefore it is very important for the businesses to make sure that the sensitive date is transferred from one point to another in a secure manner.

Cryptography is the mechanism which helps in achieving the security by making the data incomprehensible to everyone except the projected receiver. The term encryption involves the conversion of the plaintext into the cipher text. The plaintext is the readable data and the cipher text is a data which is impossible to read without the key. The key acts as the medium to convert the plain text into cipher text and vice versa. The process of conversion of cipher text into the plain text is called decryption. The key for encryption and decryption is meant to be secret and the strength of key decides the privacy of cipher text.

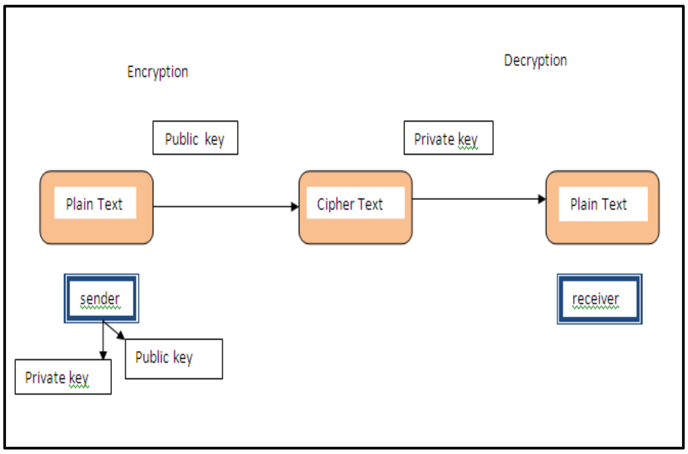


Figure 1: encryption and decryption

Types of Cryptography
There are two kinds of cryptographic algorithms: Public Key Cryptography and Secret Key Cryptography

a. Public Key Cryptography
This kind of cryptographic system uses two keys. One key is used for encryption and another key is used for the decryption. This is also known as the asymmetric cryptography.

- Every user owns two keys- one public key which is known to all the users and one is key is private key which is kept secret. The private and public key are mathematically linked.
- The encryption is performed using the public key and the process of decryption is undertaken with the help of private key.
- The examples are RSA and ECC(Elliptic Key Cryptography)
- It supports non-repudiation and considered very secure.

b. Secret Key Cryptography

- This kind of cryptographic system uses the same key for encryption as well as decryption. This is known as symmetric cryptography.
- The sender and receiver should have the same key for communicating successfully.
- The examples are DES, 3-DES, RC4, RC5

- It is widely used and very popular and the generated key is very strong.
- The non-repudiation cannot be achieved, and the generated key is subject to be intercepted by the hackers.

IV. The RSA algorithm

The RSA algorithm is for the public key cryptography which is based on the factoring of large integers. The algorithm is named after its invertors Ron Rivest, Adi Shamir and Len Adleman, who invented it in the year 1977. The RSA algorithm is known to be most widely used public key cryptography based algorithm around the world. The RSA algorithm can be used for both public key encryption as well as digital signatures. The security of this algorithm is based on its difficulty to factorize the large integers.

Through the RSA cryptosystem, the sender can send the encrypted message to the receiver without any kind of previous exchange of secret keys. Sender uses the receiver's public key for encrypting the text and the receiver uses its public key for decryption. RSA can also be used to sign a message, so A can sign a message using their private key and B can verify it using A's public key[3].

3.1 Operations in RSA algorithm

The RSA algorithm involves a three step procedure which includes the key generation, encryption and decryption.

3.1.1.Key generation

The RSA algorithm starts with the generation of key pair which includes the public key and a private key. The public key is known to all the users and it is used for encryption. The decryption is achieved by private key. The keys for the algorithm are generated by following the given procedure:

1. Select the two distinct prime numbers say p and q.

- Keeping in mind the security reasons, the integers p and q should be selected randomly and should be of the similar bit length. The prime numbers could be identified conducting the primality test.

2. Compute the value of the modulus say n. n= p*q.

- The value of n is used for both private and public keys and is called as the modulus.

3. The next step is to calculate the value of Euler's totient function. This function is denoted as :

$\emptyset(n) = (p-1)(q-1)$………………(1)

4. The next is to choose an integer(let us name it e)such that the value of e should lie between 1 and Ø(n). One more thing which is to be kept in mind is that the value of gcd(e, Ø(n)) should be 1. It means that the number e and Ø(n) are coprime.

- "e" is the public key exponent
- The most common value of e is 65,537. The smaller values of e like 5 are supposed to be less secure in certain settings. [4]

5. Then the value of d is calculated. $d \equiv e^{-}1 \ \left(mod\ \emptyset(n)\right)$…………………..(2)

- d is known as the multiplicative inverse of e modØ(n).
- The above equation (2) is more clearly stated as

(de) = 1 mod Ø(n)……………..(3)

- This is calculated as the Extended Euclidean algorithm .
- "d" is the private key component.

By the (3) equation, the public key consists of the modulus(n) and the public key exponent(e). The private key consists of two parameters one is the modulus(n) and other is exponent (d) which must be kept secret. The values of p, q, and Ø(n) should be kept secret. These three values are used for calculating the value of d.

3.1.2Encryption

The sender sends its public key(n,e) to the receiver. The private key is kept secret. Then the receiver sends the message M to the sender. The message is converted into an integer where its value lies between 0 and n. This is done by the padding scheme. Then the cipher text is calculated. $C=m^{e}$(mod n)……………………….(4)

3.1.3Decryption

The sender can recover the message (m) from the cipher text (c) by using the private key component (d) by using the equation:

m = c ^d (mod n)………………………(5)

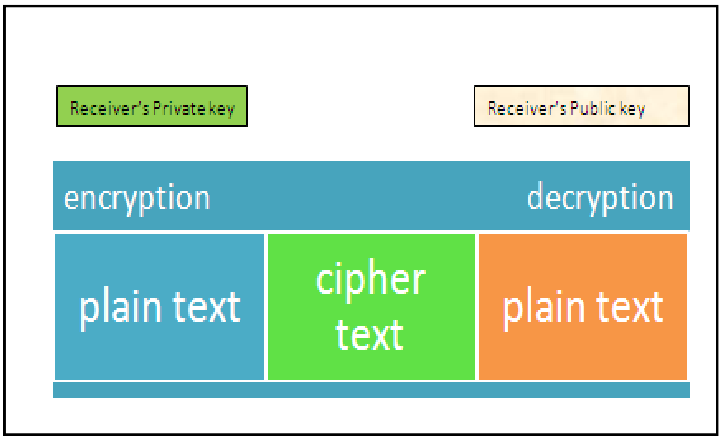


Figure 2: encryption and decryption in RSA

IV. Implementation

We perform to obtain data integrity through digital signature. In this project, the digital signature is obtained in two stages.

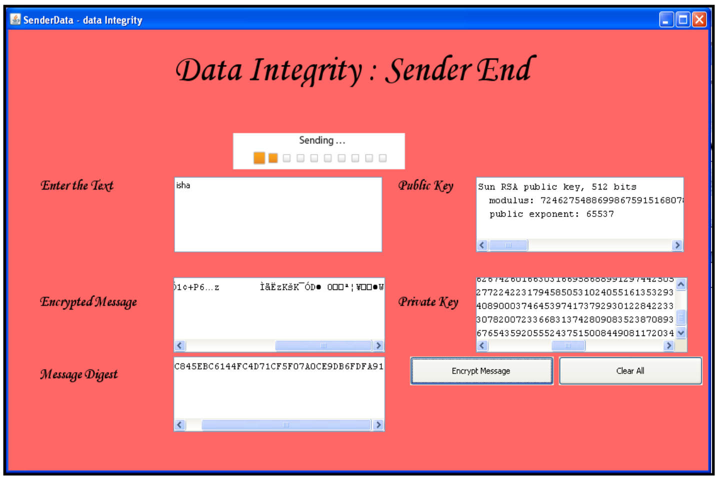
The two stages are:

1. Encryption by RSA algorithm
2. Creating message digest by SHA-1 algorithm

In our approach, we have implemented RSA using the Java platform. In this case we have not fixed up any kind of intervals for the selection of prime numbers. We are generating the prime numbers randomly. The prime numbers are generated and they are generating the public key and the private key components. These public key and private key have been used for encrypting the text message by the user. The encrypted message is saved in the database along with the original message. A graphical interface has been provided to enhance the understanding. We name the project as data integrity.

We wish to calculate the RSA encrypted message by generating the private and public key. We have also generated the message digest by using the SHA-1 algorithm. Here, we wish to achieve the data integrity by

1. Encrypting the user input text
2. Forming the message digest.
3. We have made a sender window.



Data Integrity : Sender End

Enter the Text: isha

Public Key:

```
Sun RSA public key, 512 bits
  modulus: 72462754886998675915168078
  public exponent: 65537
```

Encrypted Message: ◊1¢+P6…z ÌãËzKšK¯ÓD● O□□ª¦¥□□●W

Private Key:

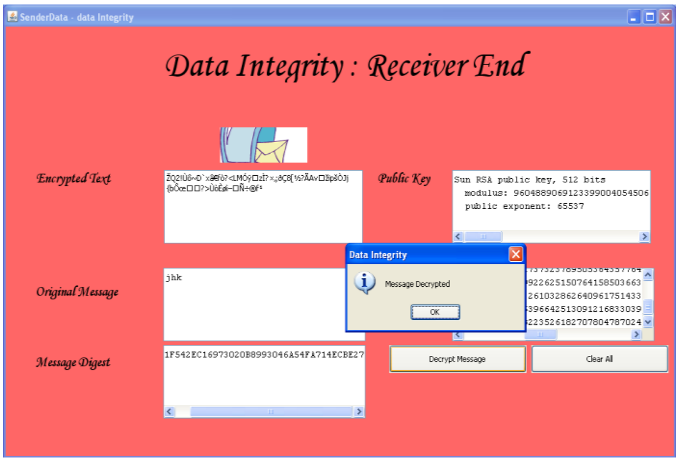
```
2772242231794585053102405516135329З
408900037464539741737929301228422З3
3078200723366831374280908352387089З
676543592055524375150084490811720З4
```

Message Digest: C845EBC6144FC4D71CF5F07A0CE9DB6FDFA91

Figure 3. A snapshot of implementation of RSA algorithm in Java.

We have made the receiver end also. In the receiver end:

1. The message is decrypted using the RSA algorithm.
2. The message digest of the decrypted text is calculated using the SHA-1 algorithm.
3. If the message digest match at the sender and receiver end then the data integrity is achieved else it is not achieved.



SenderData - data Integrity

Data Integrity : Receiver End

Encrypted Text: ŽQ2!Ù6~D`x☐fò?<LMÓÿ☐zÌ?×;ðÇ8[½?ÄAv☐ãpšÒJj {bÔœ☐☐?>ÙòÈøi–☐Ñ÷@f¹

Public Key:

```
Sun RSA public key, 512 bits
  modulus: 9604889069123399004054506
  public exponent: 65537
```

```
...9226251507641585036 63
...2610328626409617514 33
...3966425130912168330 39
...2235261827078047870 24
```

Original Message: jhk

Message Digest: 1F542EC16973020B8993046A54FA714ECBE27

Data Integrity

Message Decrypted

Figure:4 Snapshot of receiver end

The complete procedure can be completed in the format of sender and receiver side on one computer. This procedure is implemented in the client and server environment on different computers as well. To better understand it, the flowchart of the system is given.

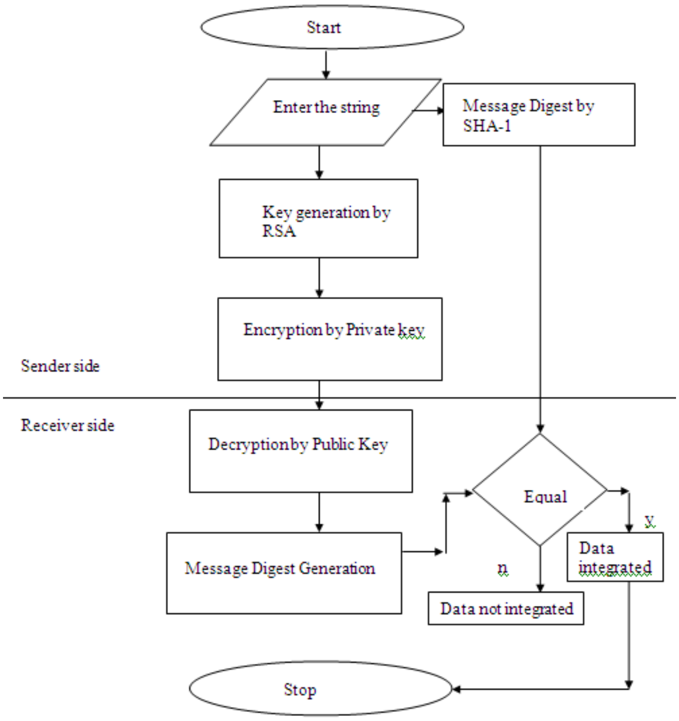


Figure 5: flowchart of the system

The application is run on the client end and the server end. The message from the client end is passed onto the server. This way the data integrity is achieved.

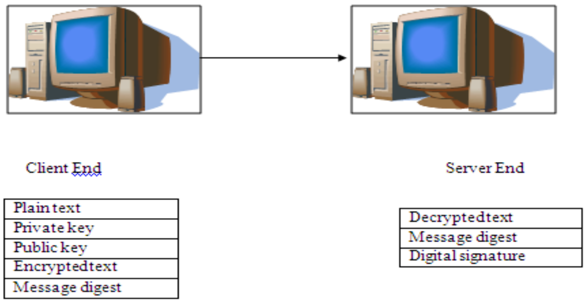


Figure 6: application layout of the system

V. Conclusion

The encrypted text has been successfully generated using the RSA algorithm. We have made one sender end. In this, the private key and the public key have been generated. The message digest is formed at the sender end and receiver end using the SHA-1 algorithm. The graphical interface enhances the understanding and achieves faster results.

VI. Future Scope

The above approach uses the RSA and SHA-1 algorithm. It can be further used in VANET kind of a scalable environment.

References

[1] http://en.wikipedia.org/wiki/Information_security

[2] modern cryptography theory and practice , chapter 10, 10.1 section

[3] Introduction to Cryptography By Mohan Atreya (matreya@rsasecurity.com)

[4] Boneh, Dan (1999). "Twenty Years of attacks on the RSA Cryptosystem". *Notices of the American Mathematical Society* **46** (2): 203–213.