International Journal of Engineering & Technology, 7 (3.4) (2018) 34-37

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Implementation of Digital Signature Using Hybrid Cryptosystem

Leela K[1*], Smitha Vinod[2]

[1]*Student, computer science department, Christ (deemed to be university), India.*
[2] *Faculty, computer science department, Christ (deemed to be university), India*
**Corresponding author E-mail: leesirvi@gmail.com*

Abstract

Security is a major concern when it comes to electronic data transfer. Digital signature uses hash function and asymmetric algorithms to uniquely identify the sender of the data and it also ensures integrity of the data transferred. Hybrid encryption uses both symmetric and asymmetric cryptography to enhance the security of the data. Digital Signature is used to identify the owner of the document but it does not hide the information while transferring the document. Anyone can read the message. To avoid this, data sent along with the signature should be secured. In this paper, Digital signature is combined with hybrid encryption to enhance the security level. Security of the data or the document sent is achieved by using hybrid encryption technique along with digital signature.

Keywords: *AES; Digital Signature; Hybrid encryption; RSA; Sha-256.*

1. Introduction

Digital signature uniquely identifies the owner of the document i.e., it identifies who sent it. It has similar properties of a handwritten signature. Digital signature is the one of the application of cryptography. Cryptography is an art of changing the text into an unreadable form. It can be broadly divided into two types, Symmetric cryptography, and Asymmetric Cryptography. The Same key is used to encrypt the data and to decrypt the encrypted data in symmetric cryptography whereas asymmetric cryptography has two keys: Encryption is done using Private Key and Decryption is done using the Public key. Digital signature uses hash function which creates hash value and Asymmetric cryptography which is also called as public key cryptography (PKC). A private key is used to encrypt the hash value which is then called Digital Signature. No two people will have the same signature as each will have unique PKC keys.

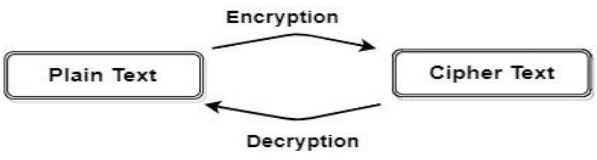

Fig. 1: Simple representation of Cryptography

The main goal of the digital signature is to provide validation and security to the data. There are three steps to complete the process of digital signature: Generating keys, encrypting (signing the document) and decrypting (verifying the signature along with the document).

Below are the steps followed to obtain a digital signature:

Sender:

1. Generate keys (private key and public key) using the asymmetric algorithm.
2. Produce hash value using the hash function.
3. Encrypt the hash value using Private Key. (The encrypted hash value is the signature)
4. Send the signature along with the document.

Receiver:

1. Hash value is obtained using the same hash function used by sender.
2. Signature is decrypted using public key.
3. Both hash values obtained from step 1 and 2 are compared. If they match, it means data is not tampered and the owner is authorized.

Hybrid cryptosystem is a method where both the types of cryptography is used i.e., Symmetric and Asymmetric cryptography. They are combined and used to enhance the security and also provide the signature. In this paper, RSA algorithm is used to obtain a signature and to secure the secret key, AES for encrypting the data and SHA-256 to produce the hash value. Hybrid Cryptosystem combines both the types of cryptography which is beneficial as the strength of both algorithms is incorporated. The strength such as speed of symmetric algorithm and security of asymmetric algorithm, both are obtained in hybrid cryptosystem. Until and unless both the keys are leaked, Hybrid encryption is considered as a highly secure type of encryption. The advantage of using hybrid encryption is that it creates a channel between two users where there can be a secure data transfer.

Hashing is a method of obtaining a small output from a huge data. Hash functions are designed to take the input as the data and produce and output knows as the hash value. Unlike cryptography, hashing is irreversible process. From the data, hash value can be produced but from the hash value, the original data cannot be retrieved. Hash functions are designed in such way that no two or more-different data can produce the same hash. Even a single

change, like change in the word or space will produce a whole new hash value.

2. Literature Review:

Security is an expansive subject and covers a huge amount of sins. [2] In the least complex frame, it is troubled about ensuring that any meddling person can't read, or more awful yet, subtly tamper messages sent for different beneficiaries. Most security issues are purposefully caused by vindictive individuals attempting to increase some profit, get consideration, or to hurt somebody. [3]Computerized marks speak to a standout amongst the most broadly utilized security advancements for guaranteeing unforgeability and non-denial of advanced information. [5] While a few information just requires the affirmation of uprightness for a moderately brief timeframe, say up to two years, there are many situations where it is essential for marked records to be viewed as lawfully legitimate for an any longer timeframe. [8] A portion of the cases of information that require long haul trustworthiness incorporate court records, long-haul rents and contracts.

An RSA calculation is a by and large utilized open key calculation. [10] It is the most usually utilized uneven cryptography calculation. It can be utilized for the encryption of little squares of information or in key trade advanced marks. RSA utilizes a variable key size and a variable encryption piece estimate. [12,13] The key match originates from an exceptionally vast number, which is the result of 2 prime numbers whose choice depends on unique standards. RSA is generally utilized for creating secure correspondence channels and for computerized marks.

[14] A main difference between handwritten signature and digital signature is that a digital signature cannot be constant. Every user has two different values, the public-key and the private-key that the Digital Signature Scheme uses for generating and verification of a digital signature. [16] The Digital signature cannot be forged, and a signer cannot later deny the validity of his signature. This has main applications such as in electronic mail, e-cash and electronic fund transfer system.

3. Existing Methods

Digital signature is implemented using the hybrid cryptosystems to ensure the data security along with the keys. In this paper, three algorithms are used to implement the digital signature using hybrid cryptosystems. The three algorithms used are: RSA, AES and SHA-2.

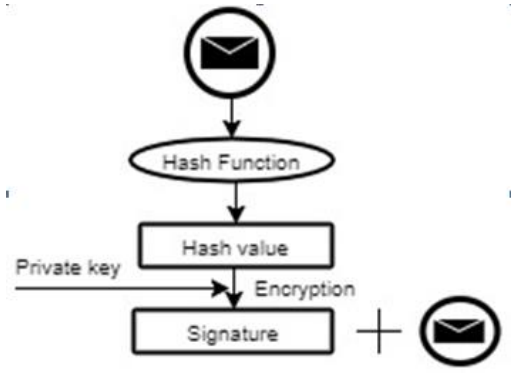

Fig. 2: Digital signature operations on sender side

In the figure 2, the Hash value of the message is obtained and it is encrypted using the private key of the sender. The encrypted hash value is the digital signature of the sender. The Digital signature along with the message is sent to the receiver.

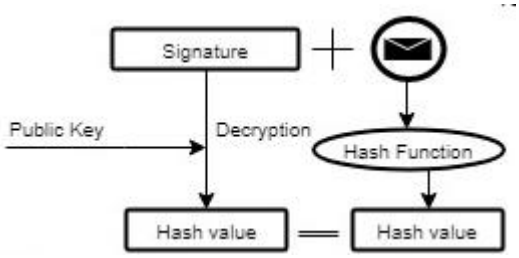

Fig. 3: Digital signature operations on receiver side

In figure 3, the receiver has the signature and the message sent by the sender. The signature is decrypted using the corresponding public key of the sender. The decrypted signature is the hash value. Now the document is sent through the hash function which results in hash value as the output. Both the hash values are compared, if they are same then the signature is verified and the message is not altered else either the key is not right or the message has tampered.

3.1. RSA

RSA is one of the most used public key cryptosystems and is generally utilized for secure information transmission. RSA is made of the underlying letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first openly depicted the calculation in 1977. Firstly, the user randomly selects two prime numbers, which produces two keys using modulus as the main function. The user should keep his/her private key very securely. Anyone who has the public key corresponding to that private key can decrypt the message. The RSA algorithm can be broadly divided into three steps: Key generation, Encryption and Decryption.

Key generation is a process of using a mathematical formula to obtain two keys in RSA: Private Key and Public Key. It is the first step in RSA algorithm. Encryption and decryption can be done only once the keys are generated. Following are the steps for RSA algorithm:

Key Generation:

i. Select two prime numbers, say IN1 and IN2.
ii. Calculate q = IN1 * IN2.
iii. Calculate 0(q) = (IN1-1)(IN2-1)
iv. Choose integer e = gcd(0(q),e)=1 where $1 < e < 0(q)$.
v. Calculate $x = e^{-1} \bmod 0(q)$.
vi. Public key = PuK {e, q}
vii. Private key = PR {x, q}

Encryption:

Consider M as the plain text,
Cipher text(C) = $M^e \bmod n$

Decryption:

To obtain plain text,
Plain text (P) = $C^x \bmod n$

RSA is widely and most used Asymmetric algorithm. Some of the advantages of RSA algorithm is that it is convenient as it solves the key distribution problem. It also helps to identify if data tampers. Also, less resource is required to maintain it. RSA uses modulus as a main function.

3.2. AES

The Advance Encryption Standard algorithm is a type of symmetric algorithm. Its development was started in 1997 by National Institute and Technology(NIST). AES is successor algorithm of Data Encryption Standard(DES). It was chosen by the U.S. government to secure data and is compatible in hardware and software all through the world to encode sensitive and important information. AES is faster and stronger than DES. Set of round keys

are derived from the encryption process. These keys are applied on the block of data along with other operations. The block of data is stored in an array. The steps for AES algorithms are:

i. The set of round keys are derived from the cipher key.

ii. State array is initialized using the block data (plain text).

iii. Initial round key is added to the starting of state array.

iv. Nine rounds of state manipulation are performed.

v. Perform final and tenth round of state manipulation.

vi. Copy the final state array out as the encrypted data.

3.3. SHA

Hash functions are part of cryptography family. The Hash function does mapping of data of any length to a fixed size. Hash functions are designed using mathematical operations. The output of a hash function is a hash value of a fixed length. Here hash function is used to verify that the data does not tamper or the correctness of the data.

SHA is abbreviated as Secure Hash Function. It is the cryptographic hash functions by NIST - Nation Institute of Standards and Technology as a FIPS- Federal Information Processing Standard. There are many standards of this family: SHA-0, SHA-1, SHA-2, SHA-3. The different standards are based on the hash value size and security strength. In this paper, SHA-2 standard is used. SHA-2 family consists of two alike hash functions SHA-256 and SHA-512 which are different only based on the block size and they have different additive constants and shift amounts. SHA-256 has 64 rounds of compression. The key size is 256 bits and the block size is 512 bits. Steps involved in SHA-256 are as follows:

i. Padding: To make the length as multiple of 512 bits.
ii. Initialize: Adding length as 64 bits.
iii. Processing: The message is processed in 512bits (16-word) blocks and uses 4 rounds of 20-bit operation on each block.
iv. Output: Hash value.

4. Proposed Model

The Digital signature authenticates the message and the sender. But it does not hide the content of the message. Anyone in the network can read the message. Tempering of the message can be identified but it cannot be identified if someone has seen it. Sometimes digitally signed documents can have sensitive information, which should not be disclosed to anyone. In such cases, encrypting the data is important. Encrypting the data using asymmetric key will take a long time, and encrypting it with a symmetric key can be less secure. To overcome their disadvantages, hybrid cryptosystem can be used where both symmetric and asymmetric algorithms are combined.

Let's consider two users as sender and receiver. Sender shares a secret key with the receiver, which is not known by anyone. The steps to send and receive a digitally signed and secure data are as follows:

4.1. Sender:

i. *Generate the private and public keys*: First, Private Key (PrK) and Public Key (PK) are generated using RSA key generator algorithm. Private Key is always used by the one who signs the document and it is not distributed to anyone. The Public key can be distributed to anyone who is the intended receiver of the document.

ii. *Encrypt the message:* The data or message (M) is encrypted using a secret key (SK) of AES. The message is converted into an unreadable form. Let's consider the encrypted message as EM.

$$EM = AES\ (M)\ using\ SK$$

iii. *Encrypt secret key (ESK) using private key (PrK):* The secret key is encrypted using the private key. This can be decrypted using the public key (PK).

$$ESK = RSA(SK)\ using\ PrK$$

iv. *Produce hash value (HV) of the encrypted message (EM):* The encrypted message is passed as an input for the hash function (HF, here SHA-256) which results in a hash value as the output.

$$HV = HF\ (EM)$$

v. *Encrypt the Hash Value (HV) using the private key (PrK):* The hash value obtained in step (iv) is encrypted using the private key. The encrypted hash value is the Digital Signature (DS).

$$DS = RSA(HV)\ using\ PrK$$

vi. *Sending:* The Encrypted Message, encrypted secret key and Digital Signature are sent to the receiver.

$$Send = DS + EM + ESK$$

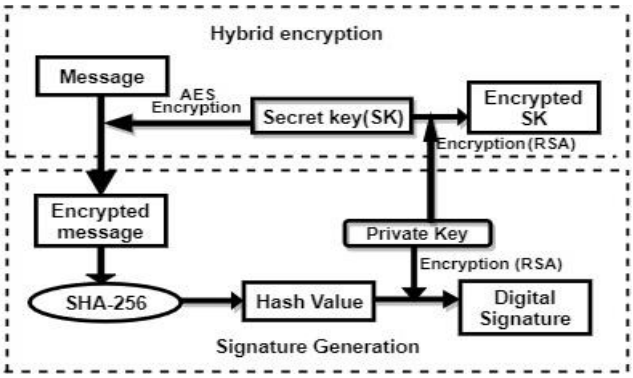

Fig. 4: Digital signature generation using hybrid encryption

4.2. Receiver:

The Receiver has the encrypted message, Digital Signature and Encrypted secret key. The Public key of the sender is also personally shared with the receiver. Steps followed by the receiver to decrypt the message and to verify the digital signature:

i. *Decrypt the digital signature using the public key:* The Signature is decrypted using the public key of the sender. The decrypted signature is nothing but the hash value of the encrypted message.

$$HV1 = RSA\ (DS)\ using\ PK$$

ii. *Produce hash value (HV) of the encrypted message (EM):* The encrypted message which is sent by the sender is passed as an input for the hash function (HF, used by the sender) which results in a hash value as the output.

$$HV2 = HF\ (EM)$$

iii. *Decrypt the encrypted secret key (ESK):* The encrypted secret key is decrypted using the public key. This key can now be used to decrypt the encrypted message.

$$SK = RSA\ (ESK)\ using\ PK$$

iv. *Decrypt the encrypted message:* To convert the message into readable form, the encrypted message should be decrypted. The message is decrypted using the secret key of AES. The message is now in a readable format.

$$M = AES\ (EM)\ using\ SK$$

v. *Compare and verify:* To verify the signature, the hash value from the step (i) and step (ii) are compared. If the values

match it means that the message is correct and the signature is verified. The sender is also verified. If the hash value from the step (i) and step (ii) are not matching, then either the message is altered or the sender is not authorized.

HV1 = HV2: Verified

HV1 != HV2: Something wrong

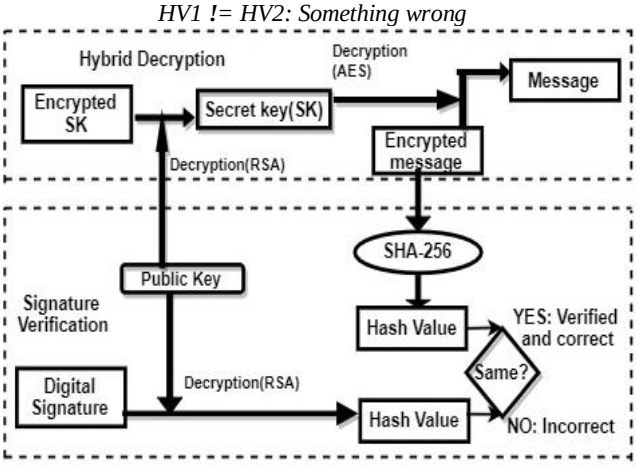

Fig. 5: Digital signature verification using hybrid decryption

5. Conclusion

Digital signature along with hybrid cryptosystem helps to securely transfer the message along with the verification of two things: message authentication and the sender's authentication. Data hiding was one of the drawbacks of the digital signature which is solved in this implementation. No one can read the data as it is in the encrypted form. This implementation results in the secure transfer of data. Data integrity and non-repudiation is obtained by this implementation. Even though there are many security issues and threats in the network, the proposed method will help to securely transfer the data.

Acknowledgement

This paper is made possible through the help and support of Dean of Science, Head of Computer science department, Guide and other faculty members of Christ (Deemed to be university), Bengaluru, Karnataka, India. I would also like to thank family and friends. The paper would not have been possible without them.

References

[1] R. Dhagat and P. Joshi, "New approach of user authentication using digital signature," in Symposium on Colossal Data Analysis and Networking (CDAN), Indore, 2016, pp. 1-3.

[2] N. R. Dodda and K. R. Kumari, "Enhanced Security For Hybrid Encryption Strategies With Key Reausability", IJSRST, vol. 3, no. 6, pp. 345–350, 2017.

[3] M. Enriquez, D. W. Garcia, and E. Arboleda, "Enhanced Hybrid Algorithm of Secure and Fast Chaos-based, AES, RSA and El-Gamal Cryptosystems", Indian journal of science and technology, vol. 10, no. 27, July 2017.

[4] G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, "Efficient Unconditionally Secure Digital Signatures," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., vol. E87–A, no. 1, pp. 120–130, January 2004.

[5] K. Kaur and E. Seema, "Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices", International Journal of Engineering Research and Applications, vol. 2, no. 5, pp. 914–917, September - October 2012.

[6] M. Kaur, "Enhanced Security using Hybrid Encryption", International Journal of Innovative Research in Computer and Communication Engineering, vol. 4, no. 7, pp. 13001–13007, July 2016.

[7] P. Khurana and P. Bindal, "Study and Comparative Analysis of Different Hash Algorithm", Journal of Engineering Computers & Applied Sciences, vol. 3, no. 9, pp. 1-3, September 2014

[8] V. V. Kumari, D. V. NagaRaju and K. Soumya "Secure Group Key Distribution Using Hybrid Cryptosystem", in Second International Conference on Machine Learning and Computing, Bangalore, 2010, pp. 188-192.

[9] P. Mahajan and A. Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, vol. 13, no. 15, 2013.

[10] A. Mashatan and K. Ouafi, "Forgery-resilience for digital signature schemes," Asiaccs, pp. 24–25, 2012.

[11] O. Y. Owolabi, P. B. Shola, and M. B. Jibrin, "Improved Data Security System Using Hybrid Cryptosystem", International Journal of Scientific Research in Science, Engineering and Technology, vol. 3, no. 3, pp. 90–93, 2017.

[12] V. R. Pallipamu, T. R. K, and S. V. P, "Design of RSA Digital Signature Scheme Using A Novel Cryptographic Hash Algorithm", International Journal of Emerging Technology and Advanced Engineering, vol. 4, no. 6, pp. 609–613, June 2014.

[13] P. K. Panda and S. Chattopadhyay, "A hybrid security algorithm for RSA cryptosystem," in 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, 2017, pp. 1-6.

[14] M. Sadeghpour, "Security Analysis of Digital Signature Scheme with Message Recovery using Self-Certified Public Keys", International journal of computer, vol. 4523, pp. 43–55.

[15] J. Raigoza and K. Jituri, "Evaluating Performance of Symmetric Encryption Algorithms," in International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, 2016, pp. 1378-1379.

[16] E. Salim and I. Harba, "Secure Data Encryption Through a Combination of AES, RSA and HMAC", Engineering, Technology & Applied Science Research vol. 7, no. 4, pp. 1781–1785, 2017.

[17] S. Saxena, "A Novel Digital Signature Algorithm based on Biometric Hash", I. J. Computer Network and Information Security, no. 1, pp. 12-19, 2017.

[18] J. Thakur and N. Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis," vol. 1, no. 2, pp. 6–12, 2011.