Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Secure Message Recovery and Batch Verification using Digital Signature

Sarika[1] and Silvi[2]

[1] Manav institute of technology and Management ,jevra(Hissar) Haryana

Received: 12 December 2013 Accepted: 3 January 2014 Published: 15 January 2014

Abstract

This paper about the study of Secure message Recovery and batch verification using Digital Signature. Security is increased in batch verification through triple DES algorithm. Encryption is used for the Security in which the plaintext is transforming into the cipher text. A digital signature scheme involves two phases, the signature generation phase which is performed at the sender side and the signature verification phase that is performed by the receiver of that message. In computer to computer communication, the computer at sender?s end usually transforms a plaintext into cipher text using encryption. When the message is recovered at the Receiver Side than the original text is converted in to the encrypted text. That encrypted text is secure for the authenticated person. After recover the message if authentic person wants to get the original text then he/she enter the key and take the plaintext.

Index terms— digital signature, forgeries, encryption, triple des algorithm.

1 Introduction

igital signature is an authentication process that is used to prove the identity of source and integrity of message. A digital signature scheme involves two phases, the signature generation phase which is performed at the sender side and the signature verification phase that is performed by the receiver of that message. in this pair of key is used private key and public key. Private key is Secret and public key known all the users.

Digital signature provides the following security services: a) Message integrity It guards against the In appropriate information modification or damage. Message integrity ensures the information nonrepudiation and authenticity By using this, users are able to ensure that the message has not been altered during transmission. A loss of message integrity means that there is insertion, deletion or modification in message or replay of the message.

2 b) Authentication

This property defines being real and being able to be trusted and verifiable. The functionality of the authentication service is to guarantee the recipient that message is from the source that it state to be. two aspects are involved: first at the connection initiation time, the entities are authentic that is each entity is the entity which it state to be. Second the process of authentication must assure that the connection is not interfere by the third party in such a way that a third party can impersonate one of the two legal parties for unauthorized transmission or reception of messages.

c) It prevents from denying transmission of a message by either sender or receiver. Thus if the message is sent then the receiver can validate that the claimed sender has sent the message. This is called origin nonrepudiation. Similarly, when a message is received the source can validate that the claimed receiver has in fact receive the message.

Thus digital signature must have to posses the following properties:

1. The digital signature must validate the sender and date and time of the digital signature. 2. Digital signature must authenticate the content of message at the time of digital signature. 3. In case of any dispute, digital signature must be verifiable by third party to resolve it.

II.

3 Digital Signature Requirements

The points described below states the requirement of the digital signature:

1. Digital signature (a bit pattern) must depend upon the message that is to be signed by the sender.

2. It must make use of some information related to sender that is unique to it to prevent against denial and forgeries. 3. Digital signature must be comparatively easy to compute on message.

It must be comparatively easy to recognize and validate digital signatureIII.

4 Encryption And Decryption

Encryption is used for the Security in which the plaintext is transforming into the cipher text. In computer to computer communication, the computer at sender's end usually transforms a plaintext into cipher text using encryption the encrypted cipher text message is sent to the receiver over a network then the receiver takes encrypted message and performs the reverse of encryption. I.e. performs the decryption process obtain the plaintext. Abstracte-mails: sarikamakkar0@gmail.com , silvithakral1@gmail.com.

5 Nonrepudiation a) Plaintext and cipher text

Any communication in the language that we speak that is the human language, takes the form of plain text or clear text. That is, a message in plaintext can be understood by anybody knowing the language as long as the message is not codified in any manner. Plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to the message. when a plaintext message is codified using is codified using any suitable IV.

6 Digital Signature Modes a) Appendix mode

In appendix mode the creator of the message attach a code with the message that act as a signature. Typically the signature is produced by taking the hash of the message and encrypts it with the private key of sender. This signature guarantees the integrity of message and claimed identity of source.

In the figure 3 first a hash code generation algorithm has been applied on the message and then it is encrypted with the private key of the sender. The generated code then appends to the message and transmitted to receiver via network. Receiver verifies the signature using three items, the public key of sender, the packet and the signature. The receiver first cut off the message from digital signature. It first computes the hash of the message and decrypts the received signature with the public key of sender. If both values are equal then the message will be considered as authentic otherwise it has been modified during transmission.

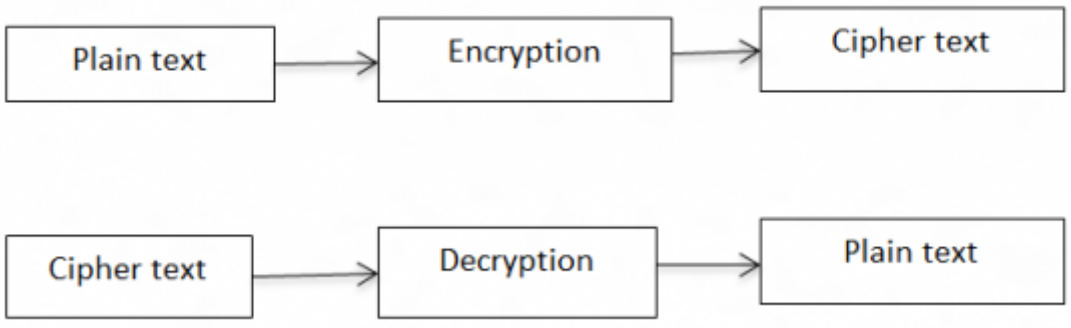
7 b) Recovery mode

In message recovery mode the signed message is implanted in the digital signature and it can be recovered from it. The well-known digital signature scheme with message recovery is the RSA digital signature scheme which security is based upon solving the factor of large prime numbers. Later Nyberg and Rueppel also proposed the digital signature scheme with message recovery based upon the discrete logarithm. Some of these schemes have the capability of privacy of signed message and thus only the legal receiver can recover the message and verify its authenticity. However the scheme only allows a signer to sign each message independently.

As shown in the figure 4, the receiver requires only two parameters to verify the digital signature of the message, the public key of sender and the digital signature. The receiver first recovers the message from the received signature and then performs computation for digital signature verification. Triple DES Algorithm is same as the DES with two 56 bit key is applied. Given a plaintext message first key is used to DES encrypt the message. The second key is used to decrypt the encrypted message. The twice scrambled message is encrypted again with the first key to yield the final cipher text.it uses three 56 bits DES keys giving a total key length of 168 bits. The block size is is 64 bits and the key sizes are 168, 112, or 56 bits with respect to keying option 1, 2, or 3. The input key sizes are 3 64 bit keys, which are shortened to 56 bits because of the internal key scheduler.

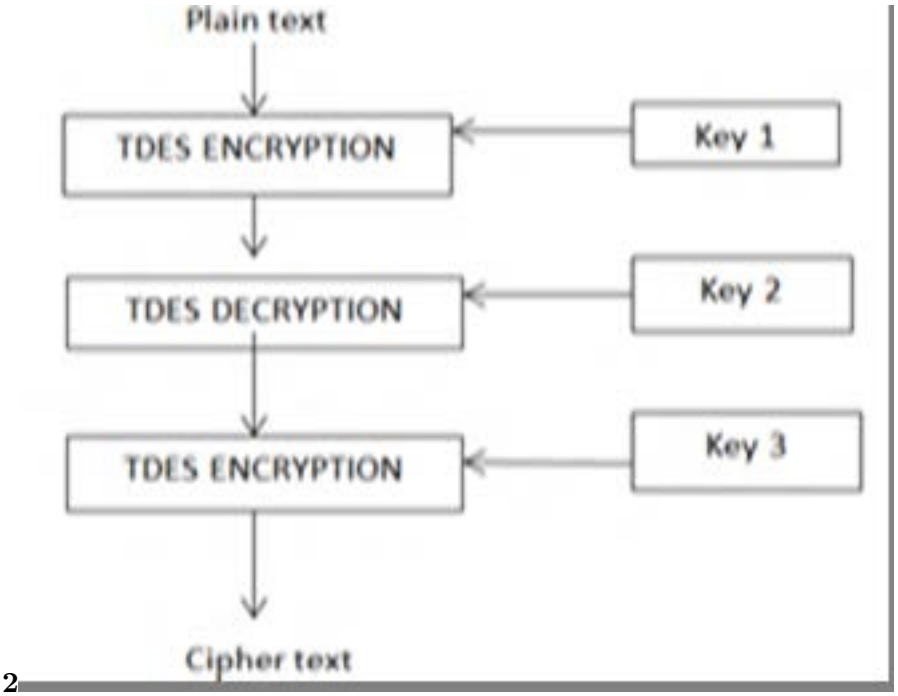
The block of data is encrypted 3 times with each of the keys according to the keying options: [1]

Figure 1: D



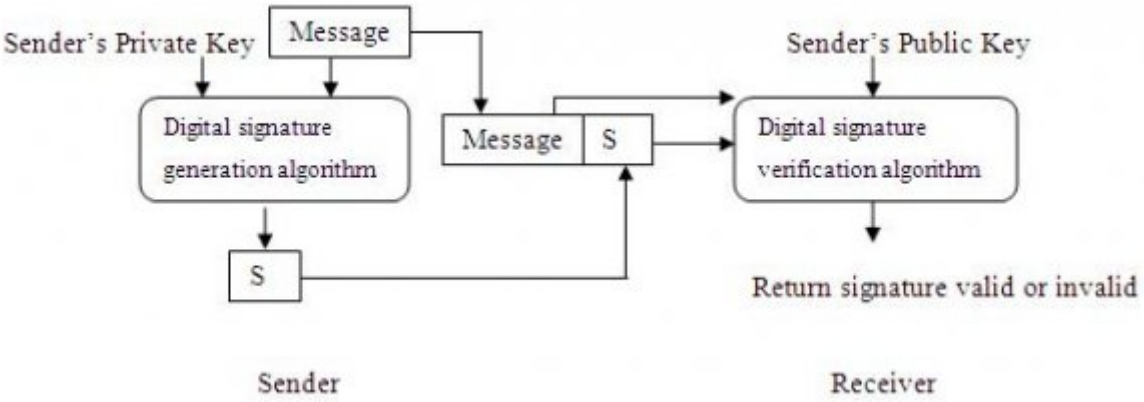
1

Figure 2: Figure1 1 .



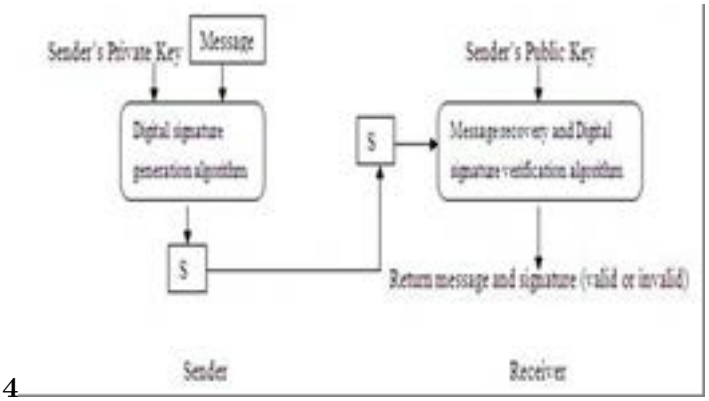
2

Figure 3: Figure 2 :



3

Figure 4: Figure 3 :



4

Figure 5: Figure 4 :

.1 Global Journals Inc. (US) Guidelines Handbook 2014

www.GlobalJournals.org

[Changchien and Hwang ()] 'A batch verifying and detecting multiple RSA digital signatures'. S W Changchien , M S Hwang . *International Journal of Computational and Numerical Analysis and Applications* 2002.

[Hwang et al. ()] 'An ElGamal-like cryptosystem for enciphering large messages'. M S Hwang , C C Chang , K F Hwang . *IEEE Transactions on Knowledge and Data Engineering* 2002.

[Boyd and Pavlovski ()] 'Attacking and Repairing Batch Verification Schemes'. C Boyd , C Pavlovski . *Proc. Sixth Int'l Conf. Theory and application of Cryptology and Information Security Advances in Cryptology (ASIANCRYPT '00)*, (Sixth Int'l Conf. Theory and application of Cryptology and Information Security Advances in Cryptology (ASIANCRYPT '00)) 2000.

[Zhang ()] *Cryptanalysis of Chang et al.'s Signature Scheme with Message Recovery*, F G Zhang . 2005. IEEE Communication Letters.

[Hwang and Li ()] 'Cryptanalysis of Shieh-Lin-Yang-Sun signature scheme'. S J Hwang , E.-T Li . *IEEE Commun. Lett* 2003.

[Shieh et al. ()] *Digital multisignature schemes for authenticating delegates in mobile code systems*, S P Shieh , C T Lin , W B Yang , H M Sun . 2000.

[Kang and Tang ()] 'Digital signature scheme without hash functions and message redundancy'. L Kang , X H Tang . *Journal on Communications* 2006.

[Park et al. ()] 'Efficient Multicast Packet Authentication Using Signature Amortization'. J M Park , E K P Chong , H J Siegel . *Proc. IEEE Symp. Security and Privacy*, (IEEE Symp. Security and Privacy) 2002.

[Hung and Chien ()] *Forgery Attacks on Digital Signature Schemes without sing One-way Hash and Message Redundancy*, Yu Hung , Chien . 2006. (IEEE communications letters)

[Liu and Li ()] *Improvement on a Digital Signature Scheme without using One-way Hash and Message Redundancy*, Jie Liu , Jianhua Li . 2006. Department of Electronic Engineering, Shanghai Jiao Tong University

[Chang and Chang ()] *Signing a digital signature without using one-way hash functions and message redundancy schemes*, Chin-Chen Chang , Ya-Fen Chang . 2004. IEEE Communication Letters.