IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Signcryption and Its Perspectives for Network Security

Richa kunal Sharma #1, Dr. Nalini Kant Joshi#2

Research Scholar, Career Point University, Kota, Computer Science

Asso.Prof. Deptt. of Computer science and Engineering

Rajasthan Technical University Kota

Abstract— Signcryption is a new paradigm in public key cryptography that simultaneously fulfils both the functions of digital signature and public key encryption in a logically single step, and with a cost significantly lower than that required by the traditional “signature followed by encryption” approach. . The framework of signcryption involves key generation, signcryption and unsigncryption. Current signcryption schemes development is still limited by the certain constraints given by real-time applications. For example, broadcasting signcrypted message increases bandwidth consumption and computational resource usage remains largely an unsolved problem. In order to address these problems, ElGamal’s signature scheme, Schnarr’s signature scheme or Digital signature schemes, Diffie Hellman method, Elliptic Curve method and RSA algorithm are widely used for signcryption. This paper provides a tutorial and overview of strategies in implementing these algorithms and provides a focus on asymmetric techniques in research.

Index Terms—DES, AES, Elliptic curve, Signcryption, Unsigncryption, Key generation, Asymmetric algorithms.

1 INTRODUCTION

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. Applications of cryptography is surveyed in (4). Private key cryptography uses private key which is shared between sender and receiver where keys may be compromised due to disclosed communication. This method is also called as symmetric key cryptography. Several symmetric key algorithms include Data Encryption Standard (DES), 3DES, Advanced Encryption Standard (AES), Rivets Cipher or Ron’s Code etc. Comparative analysis of symmetric key cryptography algorithms is described in [7][8]. Pair of keys shared between parties in public key cryptography. Message is encrypted using public key and private key is used for decryption. Signcryption is cryptographic primitive which simultaneously provide both the function of digital signature and public key encryption in a single logical step. Identity based cryptography is an alternative to the traditional certificate-based cryptosystem [1]. Signcryption is a public-key encryption scheme that performs the purposes of numerical name as well as of encryption simultaneously. The two fundamental cryptographic tools are Encryption and Digital signature which can guarantee confidentiality, integrity, and nonrepudiation.

Signcryption has wide variety of applications such as ecommerce, groupware (such as video conferencing, multicasting a message to specific members, electronic filing cabinets) and ATM networks etc. There exists a web portal that provides all information about signcryption standards[5].Data communication includes the following:1) Sender, which is a source to transmit data, source usually a computer.; 2)Medium through which data is transferred, it may be wired or wireless.:3)Receiver, which is a device to receive the Data[6]. In this paper, we focus on signcryption based data communication and a survey on signcryption methods.

2. LITERATURE SURVEY

In this paper [3] Generalized signcryption can adaptively work as an encryption scheme, a signature scheme, or a signcryption scheme with only one algorithm. The paper proposes an efficient certificateless generic signcryption scheme without utilizing bilinear pairing operations. It is proved to satisfy confidentiality and unforgeability against chosen ciphertext and message attacks in an adaptive manner, respectively, in the random oracle model. Due to the lower computational cost and communication overhead, the proposed scheme is suitable for low power and processor devices.

In this paper [9] Signcryption is a cryptographic primitive that fulfils both the functions of digital signature and public key encryption simultaneously, at a cost significantly lower than that required by the traditional signature-then-encryption approach. Signcryption has found many applications, such as electronic transaction protocol, mobile agent protocol, key management, and routing protocol. In this article, the state-of-the-art of identity-based signcryption (IBSC) is surveyed. We examine the security model of IBSC. We survey the existing IBSC schemes and compare their security properties and efficiency. IBSC with special properties and identity-based hybrid signcryption are investigated. Some possible future work is also pointed out.

In this paper [2] proposed methodology implemented here for the efficient data sharing by providing mutual authentication between users of the public clouds. The methodology implemented here provides efficient computational cost and time for encryption and decryption as well as provides secure data communication over public clouds.

In this paper [10] Signcryption is a new public key cryptography approach to address the problem of bandwidth consumption and computational resource which also ensures four facets of data transfer. ElGamal's signature scheme, Schnarr's signature scheme or Digital signature schemes, Diffie Hellman method, Elliptic Curve method and RSA algorithm are widely used for signcryption. The importance of signcryption and key generation with the overview of strategies in implementing these algorithms are discussed.

In this paper[11] Signcryption is a new paradigm in public key cryptography that simultaneously fulfils both the functions of digital signature and public key encryption in a logically single step, and with a cost significantly lower than that required by the traditional “signature followed by encryption” approach. This paper summarizes currently known construction methods for signcryption, carries out a comprehensive comparison between signcryption and “signature followed by encryption”, and suggests a number of applications of signcryption in the search of efficient security solutions based on public key cryptography.

Traditional signature-then- encryption method signs the message using digital signature and it is encrypted using sender's private key followed by receiver's public key. Signature –then- Encryption Scheme gives the framework of signature then encryption method. This method consumes more machine cycles and increases cost for digital signature and encryption. Signcryption fulfills the requirement of digital signature then encryption. It combines both the functionalities which reduces the cost and average computation time.

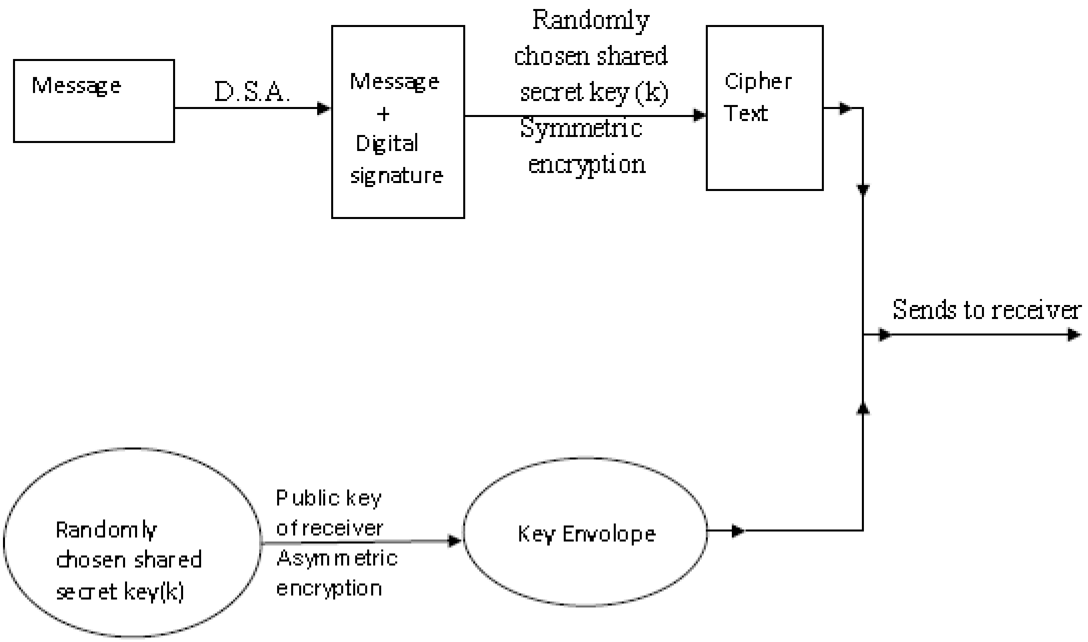

Fig 1. Signature –then- Encryption Scheme

Signcryption is a public key primitive which full fill both the functionality of a digital signature and public key encryption in a single logical step. In the Signcryption scheme, the sender generates a one times secret key by using the recipient's public key for symmetric key encryption. Then the sender sends the ciphertext to recipient. After the recipient receives the ciphertext, he derives same secret key by using his/her private key [12].

In this paper, the methods used for Signcryption and future developments in signcryption are reviewed. The main contribution of this paper is 1) Signcryption components and its relationships are described clearly. 2) Various approaches for signcrypting meassge are discussed with its merits and demerits. The above said points clearly distinguish this survey from other surveys. It gives the detail as broad as earlier works. The paper is organized as follows: Section 3 reviews the work related to key generation. Section 4 discusses signcryption techniques. Section 5 summarizes the current work.

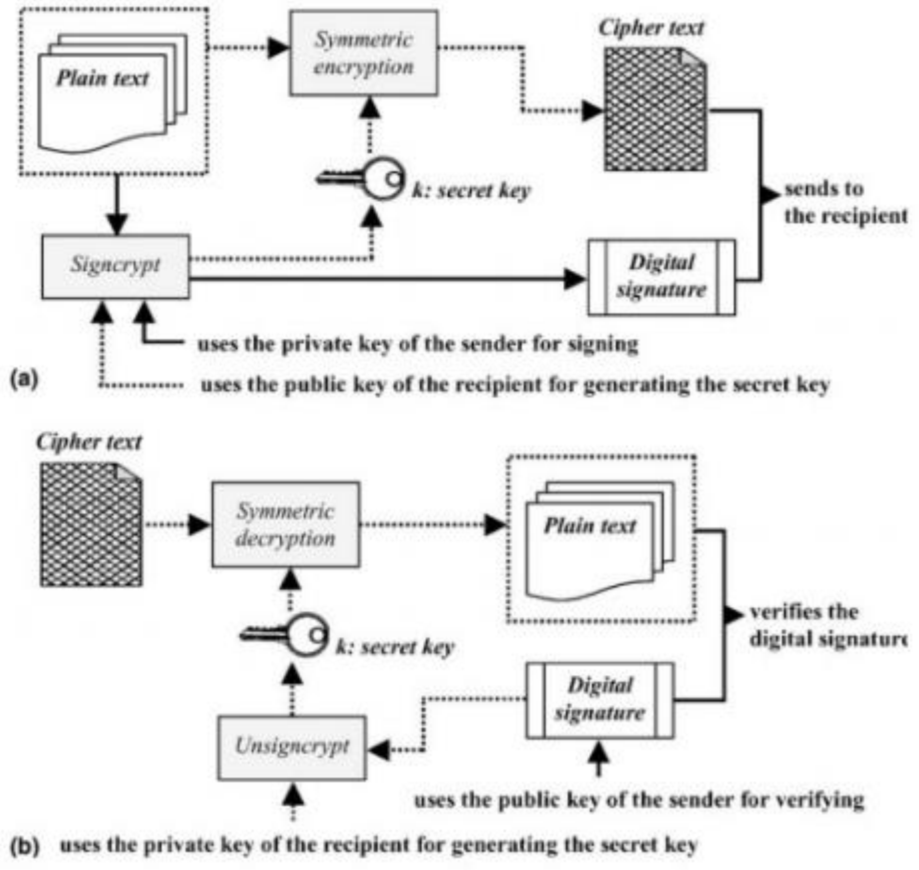
Plain text
Symmetric encryption
Cipher text
k: secret key
sends to the recipient
Signcrypt
Digital signature
uses the private key of the sender for signing
(a)
uses the public key of the recipient for generating the secret key
Cipher text
Symmetric decryption
Plain text
verifies the digital signature
k: secret key
Digital signature
Unsigncrypt
uses the public key of the sender for verifying
(b) uses the private key of the recipient for generating the secret key

Fig 2 Signcryption Scheme

3. KEY GENERATION

a **key** is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical **key**, it locks (encrypts) data so that only someone with the right **key** can unlock (decrypt) it. Key plays an important role in transformation of plaintext to ciphertext and vice versa. Protection of key is easy, and it can be changed easily, if it is compromised. In private key cryptography same key is used for both encryption and decryption but in public key cryptography pair of keys used.

i. Keys Classification

Different types of keys used for cryptography. Key types can also be used in combinations to increase security level Key types can be either private or public. All these key types can be used both for symmetric and asymmetric algorithms.

a. Private Key-The private key is used to both encrypt and decrypt the data. This key is shared between the sender and receiver of the encrypted sensitive information. The private key is also called symmetric being common for both parties. Private key cryptography is faster than public-key cryptography mechanism. Private key encryption is simple and faster than public key encryption. It uses less computation resources.

b.Public Key-The public key is used to encrypt and a private key is used decrypt the data. The private key is shared between the sender and receiver of the encrypted sensitive information. The public key is also called asymmetric cryptography. Public key encryption is convenient because private keys are kept secret and also provides authenticity of message.

ii. Key Management

Key management used to protect secrecy of data. Because, if key is obtained by the attacker, then data can be easily decrypted. It deals with generating, exchanging, storing, using and replacing keys as needed at the user level.
A key management system will also include key servers, user procedures and protocols, including

cryptographic protocol design. The security of the cryptosystem is dependent upon successful key management [13].

iii. Key Size

Key size is an important factor that must be considered for secrecy. It is simplest to use brute force attack which tries all possible numbers up to the length of the key. Key size must as long as the message size otherwise the attacker can predict all possible combinations. Key size (in bits) is a number in power of two which is preferred. If key length is n bits, it can produce exponential number of keys.128-bit key size is used widespread. To achieve the high -level security, different algorithms use different key sizes. The security of algorithm is distinct and cannot exceed than key length. Symmetric key algorithm 3DES has key length 168 bits but provides security of almost 112 bits. Symmetric key algorithms are designed to have key size equivalent to security. But asymmetric algorithms like elliptic curve cryptography algorithm uses security equivalent to half its key length.

4. TECHNIQUES of SIGNCRYPTION

1.ASYMMETRIC ALGORITHMS

A. Elliptic curve Algorithm

Elliptical curve cryptography (ECC) is a public key encryption technique based on *elliptic curve theory* that can be used to create faster, smaller and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve [15]. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications.

B.RSA Algorithm

The algorithm implements public key cryptosystem where public key is used for encryption and private key is used for decryption. In [18] Hong Biao Zeng introduced new method to carry out the calculations of RSA algorithms using spreadsheet. The algorithm uses large numbers; therefore it is secure due to the cost of factoring large numbers. But chosen ciphertext attack is possible. Factoring problem is an open challenge in RSA encryption. In [17], author demonstrated an efficient method for the factoring problem in this algorithm.

C.DSA Algorithm

DSA stand for **Digital Signature Algorithm**. It is used for **digital signature** and its verification. It is based on mathematical concept of modular exponentiation and discrete logarithm. It was developed by National Institute of Standards and Technology (NIST) in 1991.

D. Diffie Hellman Algorithm

The algorithm uses exponential key agreement protocol and allows the users to exchange secret key which is based on discrete logs. Diffie Hellman algorithm plays a vital role in creation of secure protocols such as Secure Socket Layer (SSL), Secure Shell (SSH), Internet Protocol Security (IpSec), Public Key Infrastructure (PKI) etc [20].

E. Elgamal Encryption

The algorithm is based on Diffie Hellman method and used in hybrid cryptosystem where message is encrypted using symmetric method and elgamal encrypts the key used for symmetric method. The security of algorithm depends on difficulty of computing discrete logarithms in a large prime module. The method is quite slow and used for key authentication protocols [18].

2.ENCRYPTION

a **cipher** (or **cypher**) is an algorithm for performing encryption or decryption. Cipher is an algorithm which converts the plaintext into ciphertext by using key which is called an encryption. Traditionally substitution techniques and transposition techniques were used [14].

A. Rotor Machines

Rotor Machine is set of rotors to have an array of electrical contacts to implement fixed letter substitution which is complex than polyalphabetic substitution cipher [1].

B. Transposition Methods

The simplest method is rail fence cipher which writes the plaintext in diagonal and reads the sequence horizontally. The simplest method is rail fence cipher which writes the plaintext in diagonal and reads the sequence horizontally.

c. Substitution Methods

Substitution technique is a classical encryption **technique** where the characters present in the original message are replaced by the other characters or numbers or by symbols.

Substitution technique is a classical encryption technique where the characters present in the **original message** are **replaced** by the **other characters or numbers or by symbols.** If the plain text (original message) is considered as the string of bits, then the substitution technique would replace bit pattern of plain text with the bit pattern of cipher text. There are explain **Substitution technique** are 1.Caesar Cipher,2.Monoalphabetic Cipher ,3.Playfair Cipher,4.Hill Cipher,5.Polyalphabetic Cipher,6.One-Time Pad[16].

D. Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent. In many countries, including the United States, digital signatures are considered legally binding in the same way as traditional handwritten document signatures.

E. Steganography

The method hides the existence of plaintext which makes concealed writing. Traditionally character marking, invisible ink, pin punctures, typewrite correction ribbon etc. were used. Stefan katzenbeisser et al. [19] introduced the field of information hiding followed by detailed description of stenographic techniques and its applications.

5. CONCLUSION

signcryption is a public-key primitive that simultaneously performs the functions of both digital signature and encryption. Signcryption is a new public key cryptography approach to address the problem of bandwidth consumption and computational resource which also ensures four facets of data transfer ElGamal's signature scheme, Schnarr's signature scheme or Digital signature schemes , Diffie Hellman method, Elliptic Curve method and RSA algorithm are widely used for signcryption. The importance of signcryption and key generation with the overview of strategies in implementing these algorithms are discussed.

6.REFERENCES

1.En.wikipedia.org/wiki

2. Richa Singh Dangi1, Mr. Amit Saxena 2, Mr. Manish Memoria," An Effective Signcryption Based Authentication for Security in Cloud Computing", international Journal of Computer Science and Information Technologies, Vol. 6 (6), 2015, 5284-5288.

3. Zhongtian Jia,[1,3] and Chuan Zhao," An Efficient Certificateless Generalized Signcryption Scheme",

https://doi.org/10.1155/2018/3578942, May 2018.

4.Shivangi Goyal, "A Survey on the Applications of Cryptography", International Journal of Engineering and Technology, Volume 2 No.3, March 2012.

5.www.signcryption.org/standards

6. Behrouz Forouzan, "Data communications and Networking", Tata McGrew Hill, Fifth Edition, 2012.

7.Anjali Patil and Rajeshwari Goudar, "A Comparative Survey of Symmetric Encryption Techniques for Wireless Devices, International Journal of Scientific and Technology Research, Volume 2, Issue 8, August 2013.

8. Monika Agarwal and Pradeep Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering, Vol 4, 2012.

9. Fagen Li & Muhammad Khurram Khan," A Survey of Identity-based Signcryption", Volume 28, 2011

10. S.K.B.Sangeetha, S.L.Jayalakshmi," Signcryption Approaches for Network Security", International Journal of Scientific & Engineering Research, Volume 6, Issue 5, May-2015 ISSN 2229-5518.

11.Yuliang Zheng," Signcryption and Its Applications in Efficient Public Key Solutions", URL: http://www-pscit.fcit.monash.edu.au/~yuliang/.

12. Hwang, Ren-Junn, Chih-Hua Lai, and Feng-Fu Su. "An efficient signcryption scheme with forward secrecy based on elliptic curve." Applied Mathematics and computation 167.2 (2005): 870-881.

13. Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid, "Recommendation for Key Management", National Institute of Standards and Technology, Special Publication, 2007

14. William Stallings," Cryptography and Network Security Principles and Practice", 5th edition,Pearson education,2011.

15. https://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography

16. https://binaryterms.com/substitution-technique-in-cryptography.html

17. Ambedkar, Gupta, Gautam, Bedi, "An Efficient Method to Factorize the RSA Public Key Encryption", IEEE International Conference on Communication Systems and Network Technologies, june,2011.

18. Flonta.S, Miclea.L, "An Extension of the ElGamal Encryption Algorithm",IEEE International Conference on Automation, Quality and Testing, Robotics, 2008.

19. Stefan katzenbeisser and Fabien A.P.Petitcolas, " Information Hiding Techniques for Stegnography and Digital Watermarking", Artech House, INC , London,2000, ISBN 1-58053-035-4.

20. Ik Rae Jeong, ETRI,Daejeon, Jeong Ok Kwon and Dong Hoon Lee, " Strong Diffie-Hellman-DSA Key Exchange", Communications Letters, IEEE, Volume 11, Issue 5, May 2007.