Global Journal of Computer Science and Technology: H
Information & Technology
Volume 15 Issue 2 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

High Security by using Triple Wrapping Feature and their Comparison

By Pooja Lal Mundaniya & Naveen Choudhary

College of Technology and Engineering, India

Abstract- In the age of information, cryptography is a predominant obligation for the security of our documents. Cryptography inclusive of authentication, integrity, confidentiality and non-repudiation has lot to offer. To protect users' information and their data from being attacked, encryption and digital signature algorithms could be utilized with distinct approaches to administer secure network and security solutions. In the current scenario, encryption alone cannot withstand the novel attacks; for notable security, we require encryption with digital signature. In this paper symmetric, asymmetric algorithm and digital signature techniques are proposed to elevate security. ElGamal encryption algorithm, ElGamal digital signature algorithm and IDEA algorithms are employed in the proposed methodology.

Keywords : *digital signature, elgamal algorithm, encrypt-sign, encrypt-sign-encrypt, idea algorithm, sign-encrypt, sign-encrypt-sign.*

GJCST-H Classification: *D.4.6*

High Security by using Triple Wrapping Feature and their Comparison

Pooja Lal Mundaniya [α] & Naveen Choudhary [σ]

Abstract- In the age of information, cryptography is a predominant obligation for the security of our documents. Cryptography inclusive of authentication, integrity, confidentiality and non-repudiation has lot to offer. To protect users' information and their data from being attacked, encryption and digital signature algorithms could be utilized with distinct approaches to administer secure network and security solutions. In the current scenario, encryption alone cannot withstand the novel attacks; for notable security, we require encryption with digital signature. In this paper symmetric, asymmetric algorithm and digital signature techniques are proposed to elevate security. ElGamal encryption algorithm, ElGamal digital signature algorithm and IDEA algorithms are employed in the proposed methodology. Comparisons between encrypt-then-sign, sign-then-encrypt, encrypt-sign-encrypt and sign-encrypt-sign techniques are performed and the outcome reveals that sign-encrypt-sign technique is more robust.

Keywords: digital signature, elgamal algorithm, encrypt-sign, encrypt-sign-encrypt, idea algorithm, sign-encrypt, sign-encrypt-sign.

I. Introduction

Security for confidential data is required by innumerable organizations across the Globe, and cryptography fulfils this fundamental in different ways. It contributes confidentiality, integrity, authentication and non-repudiation of data. Cryptography is divided into two parts, namely symmetric and asymmetric cryptography. In symmetric (or secret key) cryptography, a single key is required for both encryption as well as for decryption. A problem of key sharing emanates from this single key, as the same key is required for decryption. Nonetheless, it has an advantage of speed. A serious concern is that there may be a chance that an enemy (attacker) can discover the secret key during transmission. While in asymmetric (public key) cryptography, two different keys are used, one for encryption i.e. public key and another key (private key) for decryption. It solves the problem of key sharing, but engenders the problem of low speed.

For encryption, the optimal solution is to fuse public-key and secret-key systems in order to get both, the security and speed. This solution is called hybrid security. In our proposed paper, Encrypt-Sign-Encrypt (ESE) and Sign-Encrypt-Sign (SES) triple wrapping techniques are employed, and it is established that they are better and more secure than encrypt-then-sign and sign-then-encrypt techniques. In the sign-then-encrypt (SE) technique, a recipient can decrypt the message, followed by re-encrypting it with the signature intact and send it to a third party. As a consequence, that third party will believe the original author sent the message directly to him, while it was actually forwarded by the original recipient. In Encrypt-then-sign (ES) technique, an attacker can remove the signature, replace it with his own, and claim authorship of the message without knowing its contents. To overcome both the above problems, a novel technique is proposed, namely Encrypt-Sign-Encrypt (ESE) technique. In this ESE technique, double encryption is performed and the results demonstrate it to be more secure when compared to ES and SE. However, it has disadvantage of high computational time and computational cost. This computational time and cost is reduced by another proposed technique called Sign-Encrypt-Sign (SES). SES is also secure with an advantage that it requires less time and computational cost. The remainder of this paper is organized as follows: In section 2, brief description of hybrid cryptography is given. In the next section related work is presented. Section 4 presents the proposed scheme and is analyzed in detail. Section 5, comparison of proposed methodology with ES and SE is given, section 6 gives results and discussion and finally conclusions and future work are presented in the last section based on the implementation.

II. Hybrid Cryptgrpahy

Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security. Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. Digital signature is used to validate that the message was created by authorized sender, such that the sender cannot deny having sent the message and that the message was not altered in transit. The notion of a digital signature is useful and is a legal replacement for handwritten signature. Encryption and digital signature techniques are fundamental in any cryptographic tool for privacy of the data and authenticity respectively. Hybrid-key cryptosystem and digital signature, which is more secure and the security

Author α σ: Dept. of CSE, CTAE, MPUAT, India.
e-mail: pooja_lalm@yahoo.com

relies on the problem of solving discrete logarithms and on factorization [1]. The hybrid scheme may use encrypt-then-sign or sign-then-encrypt technique. In this proposed work, triple wrapping feature is put to use by implementing Encrypt-Sign-Encrypt and Sign-Encrypt-Sign techniques. These proposed techniques are expected to be more secure in comparison to the existing techniques but at the cost of extra overhead.

III. Related Work

In [1] encrypt-then-sign scheme is proposed. In this IDEA-RSA algorithm is used for hybrid encryption and RSA digital signature algorithm is used to obtain digital signature. The end result shows that hybrid cryptographic scheme can be used for fast encryption and digital signature jointly and achieved speed of 2.8 Mbps which is faster than the existing implementations. This scheme is applicable in secure internet computing, e-payment in distance education system as well as in a mobile environment, because the overall computational cost is low. This scheme is also advantageous for mobile devices like smart card based applications and many other applications.

In [5] a new deniable authentication protocol based on the generalized ElGamal signature scheme is proposed, and has two characteristics:

1. It enables an intended receiver to identify the source of a given message.
2. The intended receiver cannot prove the source of a given message to any third party. This new protocol needs less computation and communication time. Moreover the new protocol is on-interactive. Therefore, the new protocol is more efficient.

In [3], author solves the problem of key management and database encryption in the implementation process of the database encryption system. Some difficult technology of encrypt / decrypt engine in the implementation process is discussed, the hybrid cryptography encryption program is presented based on IDEA combined with RSA, and the encryption system is designed and realized. The key management module is responsible for encryption key generation, distribution, updating and storage, and is the core of the database encryption system. This shows that, new program can solve problems and make the whole encrypted database system work effectively.

In [10] an improved version of ElGamal signature algorithm for better security is proposed and this makes the ElGamal digital signature algorithm more adaptable and extensive use of digital signatures to provide security guarantees. It reduces the overall operation, and also saves storage space. Moreover the proposed method can be applied with the specific role of a particular digital signature system, to upgrade its attack against the resilience of random numbers.

In [8] hybrid cryptography algorithm is designed for better security by combining two symmetric cryptography techniques Data Encryption Standard (DES) and International Data Encryption Standard (IDEA). This hybrid algorithm has high security of data transmission over the network. This work results into more secure transmission of data comparatively DES, IDEA and AES data encryption algorithms. As both symmetric algorithms are used for hybrid cryptography security, the computational process used for encryption and decryption of the plaintext and ciphertext is essentially same.

The existing techniques videlicet Sign-then-Encrypt and Encrypt-then-Sign fails some security parameters as shown in Table 1. In SE, the recipient can decrypt the message, then re-encrypt it with the signature intact and send it to a third party. In ES, any attacker can remove the signature, replace it with his own, and claim authorship of the message without knowing its contents. To overcome both problems new (triple wrapping) ESE and SES methods are proposed which uses hybrid security, mixture of symmetric and asymmetric cryptography which solves the problem of key transmission and speed respectively. These proposed methods prove to be more secure as compared to existing techniques.

IV. Proposed Methodology

In this proposed methodology, various issues in hybrid cryptography are analyzed and are improve for better security. Hybrid cryptography combines two or more encryption systems to achieve effective security, but as new techniques appear; the attacker generates new attack. In this paper, two techniques are proposed ESE and SES, and they take advantage of the triple wrapping feature. In ESE – double encryption is implemented. In the first stage of encryption, plaintext is encrypted followed by the second stage where the sender's signature is also attached. In SES – sender's private key is used firstly to sign the message (plaintext) and then the encrypted message (ciphertext). These proposed techniques turn out to be secure and are improved alternative to sign-then-encrypt and encrypt-then-sign techniques. These novel techniques use IDEA algorithm for message encryption, ElGamal encryption algorithm for encrypting IDEA key and ElGamal digital signature algorithm for generating digital signature. Figure 1 and 2 shows the block diagram of ESE technique for encryption and decryption respectively.

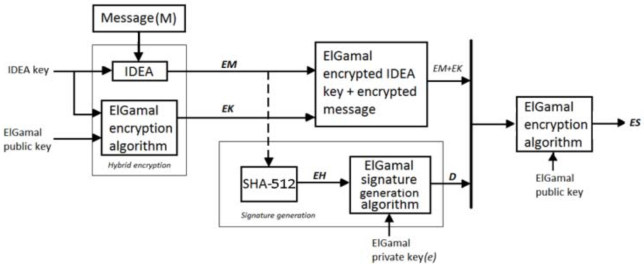
Message(M)
IDEA key
IDEA
EM
ElGamal encrypted IDEA key + encrypted message
EM+EK
ElGamal public key
ElGamal encryption algorithm
EK
Hybrid encryption
ElGamal encryption algorithm
ES
ElGamal public key
SHA-512
EH
ElGamal signature generation algorithm
D
Signature generation
ElGamal private key(e)

Figure 1 : ESE Encryption

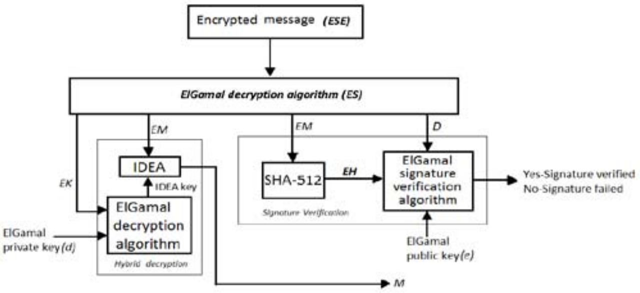

Figure 2 : ESE Decryption

Figure 3 and 4 shows the block diagram of SES technique for encryption and decryption respectively.

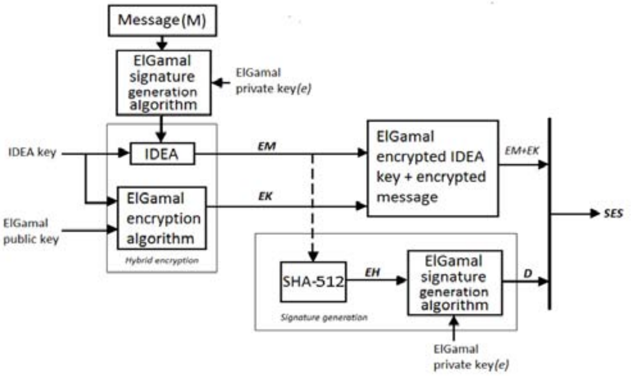
Message(M)
ElGamal signature generation algorithm
ElGamal private key(e)
IDEA key
IDEA
EM
ElGamal encrypted IDEA key + encrypted message
EM+EK
ElGamal public key
ElGamal encryption algorithm
EK
Hybrid encryption
SES
SHA-512
EH
ElGamal signature generation algorithm
D
Signature generation
ElGamal private key(e)

Figure 3 : SES Encryption

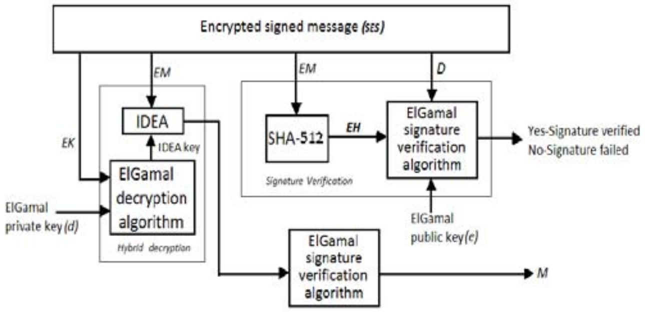

Figure 4 : SES Decryption

V. Comparison of Proposed Methodology with ES and SE Methods

Comparison is done on the basis of security parameters, computational time and cost. Two types of attacks are considered in proposed work videlicet third person attack and receiver attack. Both attacks are applied on existing methods as well as proposed methods and on this basis, security parameters are evaluated as shown in table 1, and the results establish that the proposed methodologies are more secure.

1. *Third Person Attack*

In this attack, any third person (or man-in-middle) can undertake the attacker work, and vandalize our information. In Encrypt-then-Sign and Sign-Encrypt-Sign techniques, the attacker can discard outer signature and attach his own digital signature. Now, the receiver will believe that message was sent by the third person and not the original sender. In this scenario, authentication fails. Nevertheless, this outer signature has an advantage of public verifiability, which means that any person can verify the signature owing to the fact that signature's public key is open to all, and this digital signature is signed by sender's private key only.

In Sign-Encrypt-Sign technique if outer signature is changed by third person then original receiver will find out that the message has been attacked and it is not the original message, this is because the outer signature will not match the inner signature. So, SES technique is safe from this attack.

2. *Receiver attack*

In some cases if receiver becomes attacker; he can forward our signature to others. In Sign-then-Encrypt and Encrypt-Sign-Encrypt techniques, after the receiver receives the message, he decrypts it with his private key and again encrypts it (re-encrypt) and send it to the third person with our digital signature intact. That third person (new receiver) will observe that the message is sent by the original sender, but actually it has been sent by the original receiver.

SES and ESE technique are safe from both attacks, and proves secure as compare to ES and SE techniques.

Table 1 : Security parameters table Techniques

Techniques / Parameters	ES	SE	ESE	SES
Authentication	NO	NO	YES	YES
Confidentiality	YES	NO	YES	YES
Integrity	YES	YES	YES	YES
Non-Repudiation	YES	NO	YES	YES
Public Verification	YES	NO	NO	YES

a) *Sign-then-Encrypt (SE)*

In this technique, the document is first digitally signed with private key of sender, and then that signed document is encrypted with hybrid encryption. Document is encrypted by employing IDEA key algorithm, and then IDEA key is encrypted with ElGamal Encryption Algorithm. This document is transmitted to the receiver. At the receiver end, SE document is decrypted with receiver's private key and with IDEA key, the encrypted message is deciphered. In this case receiver can verify that the document is transmitted by the original sender with sender's digital signature.

Problem: In above technique, if the receiver becomes intruder, the recipient can decrypt the message, then re-encrypt it with the signature intact and send it to a third party. That third party will believe that the original author sent the message directly to him, while it was actually forwarded by the original recipient. In this case, authentication fails, no public-verification and repudiation problem occurs.

b) *Encrypt-then-Sign (ES)*

In this technique, the document is first encrypted with Hybrid encryption technique, and then the encrypted document is digitally signed by the sender.

i. *Problem*

Any attacker can remove the signature, replace it with his own, and claim authorship of the message without knowing its contents. In this case, authentication fails, as original sender's signature is removed by third person.

c) *Encrypt-Sign-Encrypt (ESE)*

In this proposed technique, the document is first encrypted with hybrid technique and then digitally signed with sender's private key. Then again encryption is done on that document. This last encryption is done for better security; as a consequence outer signature cannot be replaced by third person.

i. *Problem*

In ESE the inner encryption ensures only the intended recipient can read the message. In this case, the recipient won't know the message is signed until after it's decrypted. Encrypting a message twice is more time consuming. Furthermore, encrypt-then-sign is known to be vulnerable to attack. Double encryption requires more time and no public-verification.

d) *Sign-Encrypt-Sign (SES)*

In this proposed technique, double signature is performed on document- one on plaintext and another on ciphertext. Here, the inner signature means the author is aware of the content. The encryption ensures only the recipient can decrypt it. And the outer signature means that the author intended the message for the recipient. If an attacker tries to claim ownership by removing the outer signature and replacing it with his own, then the (replaced) outer signature won't match the inner signature.

i. *Problem*

Computational time and cost is more as compared to ES, SE techniques but less than ESE technique.

The architecture of sign-then-encrypt approach deteriorates from forwarding attack. On the other hand, the architecture of encrypt-then-sign approach deteriorates from cipher text stealing attacks. The two-block approach has many security flaws and to alleviate those, we present the three-block approach (triple wrapping feature) i.e., Encrypt-Sign-Encrypt and Sign-Encrypt-Sign. One major drawback of three-block approach is that the cost involved in securing a message using Encrypt-Sign-Encrypt or Sign-Encrypt-Sign is the total costs of three blocks of digital signature and encryption. In addition to this, computation time for signature verification and decryption process is involved at the receiving end. All of these constitute the cost of performing cryptographic operation on a message.

SE and ES techniques have their disadvantages; these disadvantages are overcome by proposed ESE technique. ESE technique is safe from both receiver attack and third person attack. Because of double encryption ESE requires high computational time and cost. So, second technique is proposed; SES, which is as secure as ESE technique and requires very low time and cost as compared to ESE technique, but slightly more than ES and SE techniques.

The first graph in Figure 5 illustrates line graph for computational time between number of operations and computational time in seconds when encrypting a message. SE and ES techniques manage to decrypt the message in almost the same time. On the other hand, ESE technique requires four times the computational time required by other techniques. Our second proposed technique SES utilizes approximately the same computational time when compared to ES and SE techniques.

The second graph in Figure 5 portrays line graph for computational time between number of operations and computational time in seconds when decrypting a message. Time required by both the existing techniques videlicet SE and ES is similar. The ESE technique takes four times the computational time required by other methodologies. Corresponding to the encryption technique, the computational times utilized by SES is similar to ES and SE techniques.

The first bar graph in Figure 6 interprets comparison between the four methodologies in terms of computational costs when encrypting message. ES and SE techniques utilize equal number of operations in every case without exception. It is clear that ESE utilizes almost twice the number of *Texp* operations as compared to other techniques. The other proposed technique SES virtually exploits the same computational cost except in case of *Th* operation where it utilized thrice the number of operations when compared to ES and SE techniques.

The second bar graph in Figure 6 delineates collation between the four methodologies in terms of computational costs when decrypting message. The number of operations used by ES and SE techniques is equal in every case with the exception in *Th* where SE requires an operation less than ES methodology. Even when decrypting a message, ESE requires almost twice the number of *Texp* operations as compared to the other methodologies. Analogous to the encryption technique, SES uses about the same number of operations when compared to ES and SE techniques with the exception of *Th* operation where it utilized thrice the number of operations.

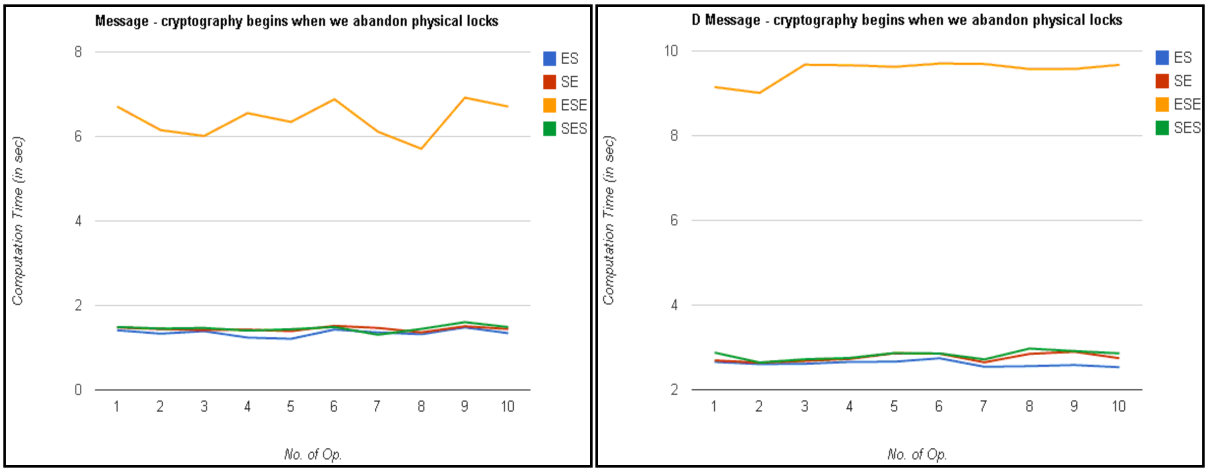

Figure 5 : Graph for computational time

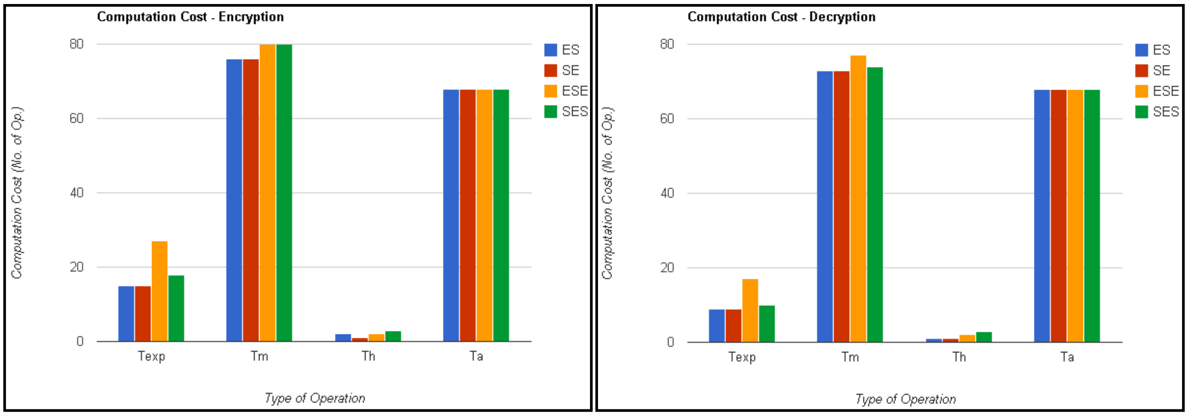

Figure 6 : Graphs for computational cost

VI. Results and Discussion

The computational cost is evaluated by summing the number of operations (i.e. modulo, hash, multiplication, addition, exponentiation, and division (inversion)) for all schemes ES, SE, SES and ESE. The results for the same are depicted in the graph as shown in figure5 and 6. All schemes are implemented using MATLAB and executed *on a machine with a 1.73GHz Intel Dual Core processor, with 1GB installed memory.*

Security parameters of our proposed methodology such as confidentiality, authentication, integrity and non-repudiation are proves to be secure as compare to existing methods as shown in table 1. Figure 5 shows the comparison between existing techniques and our proposed ESE and SES techniques. The results show that the proposed methodology ESE requires four times more computational time for encryption and decryption as compared to existing methods. And second proposed method SES utilizes approximately the same computational time when compared to ES and SE techniques. Figure 6 shows the graph between computational cost and number of operations.

a) Where

Texp: the time for a modular exponential computation, *Tm*: the time for a modular multiplication computation, *Th*: the time for a one way hash function f(_) computation and *Ta*: the time for a modular addition / subtraction computation.

ES and SE require almost same number of operations except in case of Hash operation during encryption where ES takes 1 operation more than SE technique. Furthermore, SES methodology is not far behind and utilizes only few more operations than the existing technology i.e., for SES encryption 1 *Th*, 3 *Texp* and 4 *Tm* operations more and for SES decryption 2 *Th*, 1 *Texp* and 1 *Tm* additional operations. However, ESE encryption put to use 27 *Texp* operations which is nearly twice the number of operations when compared to 15 *Texp* operations of the existing technology and 1.5 times greater than 18 *Texp* operations of the second proposed methodology SES. Although the computational time and cost of the proposed methodology increases, it still proves to be better in terms of security parameters such as confidentiality, authentication, integrity and non-repudiation.

VII. Conclusion and Future Work

Encryption together with digital signature technique is employed to safeguard users' vital information from being compromised as encryption independently can be vulnerable to pristine attacks. Here, security is boosted by the amalgamation of symmetric-key, asymmetric-key and digital signature algorithms. To be precise, the proposed methodology exerts the merits of IDEA, ElGamal encryption algorithm and ElGamal digital signature algorithm.

In this paper, we have proposed triple wrapping feature namely Encrypt-Sign-Encrypt and Sign-Encrypt-Sign techniques and presented a comparison between the Sign-then-Encrypt, Encrypt-then-Sign, Encrypt-Sign-Encrypt and Sign-Encrypt-Sign. The proposed scheme is more secure for hybrid encryption and digital signature as compared to existing techniques ES and SE. ESE and SES demonstrates confidentiality, integrity, authentication and non-repudiation, and also SES is publically verifiable. Computational time and cost required for proposed SES technique is almost same as existing techniques ES and SE, where as proposed ESE technique requires four times more computational time when compared to ES, SE and SES. Future work can be done on SES technique to reduce computational time and cost.

References Références Referencias

1. M. Y. Khan and Y. P. Singh, On the security of Joint Signature and Hybrid Encryption, *IEEE,* 2005, 109-112.
2. W. Diffie and M. E. Hellman, New Directions in Cryptography, *IEEE TRANSACTIONS ON INFORMATION THEORY, 22(6),* 1976, 644-654.
3. W. Xing-hui and M. Xiu-jun, Research of the Database Encryption Technique Based on Hybrid Cryptography, *International Symposium on Computational Intelligence and Design IEEE,* 2010, 68-71.
4. R. L. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public- Key Cryptosystems, *Communications of the ACM, 21(2),* 1978, 120-126.
5. Z. Shao, Efficient deniable authentication protocol based on generalized ElGamal signature scheme, *Computer Standards & Interfaces 26*, 2004, 449–454.
6. K. R. Reddy and G. S. Raju, A New Design of Algorithm for Enhancing Security in Bluetooth Communication with Triple DES, *International Journal of Science and Research (IJ SR), 2(2),* 2013, 252-256.
7. M. Malhotra, A. Singh, Study of Various Cryptographic Algorithms, *International Journal of Scientific Engineering and Research (IJSER), 1(3),* 2013, 77-88.
8. M. Jain and A. Agrawal, Implementation Of Hybrid Cryptography Algorithm, *International Journal Of Core Engineering & Management(IJCEM), 1(3),* 2014, 126-142.
9. S. A. Jain, A. B. Abhale, A. S. Jadhav, Improved Security with Signcryption, *International Journal of Engineering Research and Applications (IJERA), 2(2)*, 2012, 424-427.

10. Z. Jun, Z. H. Ying and J. W. Don, ElGamal Digital Signature Scheme With a Private Key Pairs, *IEEE,* 2010.
11. Y. Zheng, Digital Signcryption or How to Achieve Cost (Signature &: Encryption) << Cost (Signature) + Cost (Encryption), *Springer*, 1996, 165-179.
12. D. T. Gonzalez and W. Kinsner, Comparison Of Cryptosystems Using A Single-Scale Statistical Measure, *26th IEEE Canadian Conference Of Electrical And Computer Engineering (CCECE),* 2013.
13. P. Mohit and G. P. Biswas, Design of ElGamal PKC for Encryption of Large Messages, *IEEE,* 3.38-3.42
14. S. Subasree and N. K. Sakthivel, Design Of A New Security Protocol Using Hybrid Cryptography Algorithms, *IJRRAS, 2(2)*, 2010, 95-103.
15. WILLIAM STALLINGS, *Cryptography And Network Security, Fifth Edition* (Pearson, Prentice-Hall, 2011).

This page is intentionally left blank