Jurnal Teknologi

Full Paper

ELGAMAL DIGITAL SIGNATURE SCHEME WITH INTEGRATED CFEA-TECHNIQUE

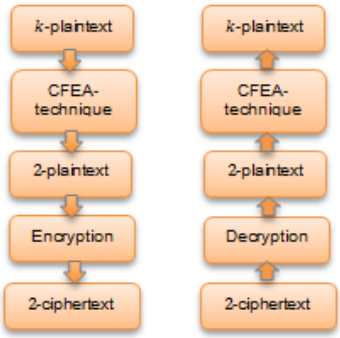
Arif Mandangan*, Che Haziqah Che Hussin, Chang Ee Hung

Faculty of Science and Natural Resources, University Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu, Sabah, Malaysia

Article history
Received
26 July 2015
Received in revised form
24 December 2015
Accepted
20 January 2016

*Corresponding author
arifman@ums.edu.my

Graphical abstract



Abstract

One of the four security goals is authentication. Authentication is a mechanism to ensure that we are communicating with the intended party. If Alice and Bob want to communicate securely, then the authentication mechanism will be able to ensure that Alice is truly communicating with Bob, and Bob is truly communicating with Alice. This mechanism can be provided by the cryptography. One of the most established cryptography schemes is ElGamal cryptosystem. The original version of this cryptosystem is to provide confidentiality through encryption and decryption procedures. By manipulating these procedures, the authentication mechanism can be carried out. Thus, ElGamal Digital Signature Scheme emerges as one of the most popular authentication mechanisms. In order to provide good level of security, proper parameters must be used in this scheme. This includes the size of the parameters. Larger parameters will provide a better level of security. As a consequence, the performance of the scheme becomes an issue in real life application. In this paper, we proposed the enhancement of the ElGamal Digital Signature Scheme by integrating the Continued-Fraction-Euclidean-Algorithm (CFEA) technique. This technique is able to reduce the number of data to be processed in the signing and verification procedures. By integrating the CFEA-technique into the ElGamal Digital Signature Scheme, any number of documents can be compressed becomes a pair of documents. Therefore, the signing and verification procedures can be done in smaller number of steps.

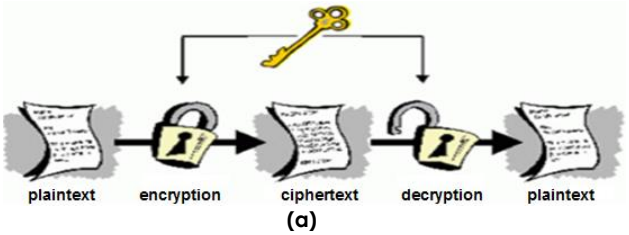
Keywords: Authentication, El-Gamal digital signature scheme, CFEA-technique

1.0 INTRODUCTION

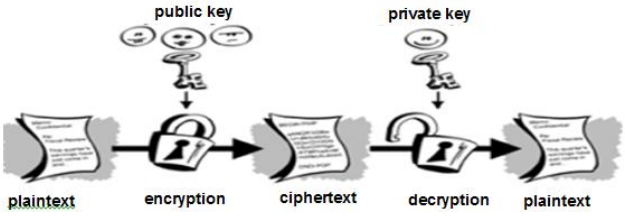
Nowadays, the Internet has been the main platform for communication across the globe. The Internet has indirectly changed our lifestyle. The Internet makes our lives become easier, faster and smarter. The world is now smaller than before since we can easily communicate with our colleagues around the world by simply being connected to the Internet. As an open communication channel, the Internet is faced with various security problems such as confidentiality, integrity, repudiation and authentication [1]. As a consequence, the network security has become crucial and essential. Network security is a set of protocols that is able to minimize cyber security attacks in order to allow us to use the Internet comfortably and safely. One of the most important parts in network security is cryptography. Cryptography is a branch of study discussing method, technique and algorithm to achieve security goals in network security. By using cryptography, we may achieve confidentiality, integrity, authentication and non-repudiation. Confidentiality is provided by the encryption and decryption procedures. Then, the hash function can be used to provide data integrity. Finally, digital signature is used to provide both authentication and non-repudiation [1]. Basically, we may categorize cryptography into two major classes based on the types of keys. If the cipher uses a common secret key, then the cipher is categorized under symmetric key cryptography. But if the cipher uses two different keys known as public and private keys, then the cipher is categorized as an asymmetric key cryptography.

For further discussion, we explain some important terminologies in cryptography. The readable original data is known as plaintext. By using encryption procedure, this plaintext can be transformed into unreadable data and known as ciphertext. In order to recover the plaintext, decryption procedure must be performed. Both encryption and decryption procedures need a parameter known as key. Only the authorized party must possess the key especially the decryption key because in modern cryptography, the key is the only parameter that would hide the secret information from any unauthorized party. Other information is considered as open knowledge including the type of cryptosystem, encryption-decryption procedures and key generation procedure. The unauthorized party is assumed to be a powerful and smart person with sophisticated attacking tools. Therefore, proper parameters especially the key must be used in real life application to avoid successful attack by the unauthorized party. In cryptography, there are some important characters with their important role respectively. Alice as a sender, Bob as a recipient and Eve as the eavesdropper or attacker.

In asymmetric cryptosystem, two different keys are required to perform both encryption and decryption procedures. The encryption process is done by using a public key and the corresponding private key will be used to decrypt the ciphertext. Suppose Bob has a pair of public key and private key. Bob may publish his public key but he must keep his private key a secret. Everybody may use the Bob's public key to encrypt plaintext and send the produced ciphertext to Bob. Since Bob is the only person who has the corresponding private key, then Bob is the only person who is able to decrypt the ciphertext sent to him [2]. The asymmetric cryptosystem is designed to solve key distribution problem which arises in symmetric cryptosystem. Hence, asymmetric key cryptography is more preferred in this modern era. Some of the most establish asymmetric cryptosystems are the Rivest-Shamir-Adleman (RSA) cryptosystem [3], ElGamal cryptosystem [4] and Elliptic Curve Cryptography. All these cryptosystems have their own digital signature schemes. The implementation of both symmetric and asymmetric cryptosystems are shown in Figure 1(a) and Figure 1(b) respectively. Figure 2 shows the general idea behind digital signature scheme.



(a)



(b)

Figure 1 The difference between symmetric (a) and asymmetric cryptosystems (b)

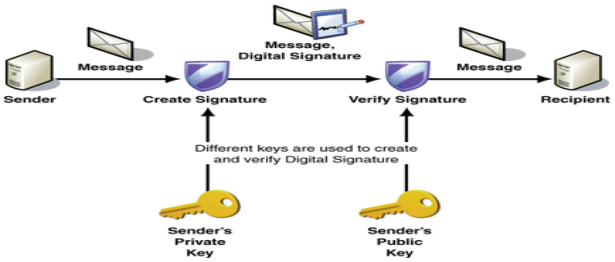


Figure 2 The general idea behind digital signature scheme

2.0 EL-GAMAL DIGITAL SIGNATURE SCHEME

ElGamal cryptosystem was proposed by Egyptian cryptologist, TaherElGamal in 1985 [4]. This system adopted the Diffie-Hellman key exchange algorithm. The security of this cryptosystem is based on Discrete Logarithm Problem which is defined as follow [5]:

Definition 1: Given integers g, h and p where g is the generator of finite field $\mathbb{F}_p^*$ and p is a prime. Discrete Logarithm Problem is defined as a problem to find a positive integer x such that

$$g^x \equiv h(mod\ p)$$

The algorithm of the ElGamal cryptosystem is given as follows [4]:

Algorithm 1: Suppose that Alice wants to send a secret message to Bob and they agree to use ElGamal cryptosystem to communicate securely. They agree to use large prime p and an integer g where g is a generator of finite field $\mathbb{F}_p^*$.

Key generation: (done by Bob)

i. Chooses an integer $b \in [0, p-2]$ as his private key
ii. Computes $e_B = g^b\ mod\ p$ as his public key
iii. Sends his public key e_B to Alice and keeps his private key b secretly

Encryption: (done by Alice)

i. Converts the message to integer form, $m \in [0, p-2]$
ii. Chooses a random integer $t \in \mathbb{F}_p^*$ as her ephemeral key
iii. Computes the ciphertext pair

$$C_1 = g^t\ mod\ p$$

and

$$C_2 = m(e_B)^t \ mod \ p$$

iv. Sends the ciphertext pair (C_1, C_2) to Bob.

Decryption: (done by Bob)

i. Upon receiving ciphertext pair (C_1, C_2) from Alice, Bob computes

$$x = (C_1)^b \ mod \ p$$

ii. Computes the multiplicative inverse of x modulo p, denoted as x^{-1} such that

$$x(x^{-1}) \equiv 1 \ (mod \ p)$$

iii. Recovers the original message m as follows

$$m = x^{-1}(C_2) \ mod \ p$$

The ElGamal cryptosystem is used to provide confidentiality. For authentication purpose, ElGamal Digital Signature Scheme has been proposed. The algorithm of the El-Gamal Digital Signature Scheme is given as follows [4]:

Algorithm 2: Suppose that Alice wants to send a document D to Bob. To authenticate herself, she makes an agreement with Bob to sign the document digitally via the ElGamal Digital Signature Scheme using large prime p and an integer g where g is a generator of finite field $\mathbb{F}_p^*$.

Key generation: (done by Alice)

i. Chooses a secret signing key $s \in [0, p-1]$

ii. Computes the verification key v as $v = g^s \ mod \ p$

Signing: (done by Alice)

i. Chooses a random integer $t \in \mathbb{F}_p^*$ as her ephemeral key

ii. Signs the document D where $D \in (1, p)$ as follows

$$S_1 = g^t \ mod \ p$$

$$S_2 = (D - sS_1)t^{-1} \ mod \ (p-1)$$

iii. Sends s (v, C_1, C_2) to Bob and keeps(s, t) secretly.

Verification: (done by Bob)

i. Upon receiving (v, C_1, C_2) from Alice, Bob computes

$$D^* = v^{S_1} S_1^{S_2} \ mod \ p$$

If $D^* = g^D \ mod \ p$, then Alice's signature is valid. Otherwise, the signature is void.

3.0 CFEA-TECHNIQUE

Efficiency is another big issue in cryptography. For real life application, we need a cryptosystem that not only can provide security, but also can be implemented efficiently especially when we need to deal with large amount of data. Some remarkable works to enhance the efficiency of data enciphering processes have been done. In 2002, Hwang *et.al*. [6] proposed a cryptosystem based on ElGamal cryptosystem and Diffie-Hellman distribution scheme which is able to encipher a large amount of message. Since this scheme is a combination of two schemes, then the user has to generate several numbers of keys.

For ElGamal digital signature scheme, some remarkable works also have been proposed. Chang *et.al* proposed an ElGamal-like Digital Signature Scheme and multisignature schemes using self-certified public keys [7]. The advantage of the schemes is that the authentication of the public key can be accomplished with the verification of the signature or multi-signature. Unfortunately, the proposed scheme can be attacked by the attack which inspired by insider-attack [8]. Then, Hwang *et al.* come out with the improved version of the Chang's scheme in 2004 [9]. Furthermore, Yoon *et al.* in 2004 proposed an efficient remote user authentication scheme based on generalized Elgamal signature scheme [10]. By using this scheme, a user is able to update his or her password freely without the help of a remote system. The scheme also able to provide mutual authentication.

As we can see, most of the works are focused on the improvement of the security and efficiency of cryptography schemes. In addition, the proposed schemes also must be easy to be implemented. Since that, we inspired to proposed a scheme which is almost identical to the original version but only embedded by a simple technique to provide efficiency. In [11], Mandangan*et.al* introduced a technique which is able to reduce the number of plaintext from any numbers to only two plaintexts. This techniques known as Compression-RSA since the first try on this technique was by embedding it into RSA cryptosystem [12]. After further research on this technique, it was found that this technique can be easily embedded into any asymmetric cryptosystem without major alteration on its key generation, encryption and decryption algorithms. Therefore, the technique has been renamed as the CFEA-technique (Continued Fraction-Euclidean Algorithm). Instead of encrypting large amount of plaintext, an asymmetric cryptosystem only needs to encrypt two plaintexts to produce two ciphertexts by applying this technique. By decrypting these ciphertexts and then applying the inverse of CFEA-technique, we will get the actual and original plaintext without any alteration. In [13], it was shown that the number of original plaintext has a linear relationship with the sizes of each compressed plaintext. As the number of original plaintext increases, the size of the compressed plaintext M_1 and M_2 will also linearly increase. But it does not affect the performance of the RSA cryptosystem with embedded CFEA-technique especially when involving a large amount of data.

Let the set of original plaintext as $\{m_1, m_2, m_3, \cdots, m_{k-1}, m_k\}$ where $k \in \mathbb{Z}^+$ and $k > 2$. By using the CFEA-technique, these k plaintexts can be compressed to only 2 plaintexts, denoted as $\{M_1, M_2\}$. Nomatter how big the value k is, the plaintext will be reduced to only 2 plaintexts M_1 and M_2. The CFEA-technique was basically designed by combining two methods namely Continued Fraction and Euclidean Algorithm.CFEA is the acronym of these methods (Continued Fraction and Euclidean Algorithm).

Algorithm 3: The algorithm of CFEA-technique [12]:

i. Compression procedure

Step 1:Let the set of original k plaintext as

$\{m_1, m_2, m_3, \cdots, m_{k-1}, m_k\}$

Step 2: By using Continued Fraction method, compute the new plaintext M_1 and M_2as follows

$$m_1 + \cfrac{1}{m_2 + \cfrac{1}{m_3 + \cfrac{1}{\vdots \; m_{k-1} + \cfrac{1}{m_k}}}} = \frac{M_1}{M_2}$$

ii. Decompression procedure

By using Euclidean algorithm, compute the following

$$M_1 = M_2(q_1) + r_1$$
$$M_2 = r_1(q_2) + r_2$$
$$r_1 = r_2(q_3) + r_3$$
$$\vdots$$
$$r_{k-3} = r_{k-2}(q_{k-1}) + r_{k-1}$$
$$r_{k-2} = r_{k-1}(q_k) + r_k$$

whereM_1, M_2 are the compressed plaintexts, q_i is quotient and r_i is remainder for $i = 1,2, \dots, k$.From this step, we have

$\{q_1, q_2, q_3, \cdots, q_{k-1}, q_k\} = \{m_1, m_2, m_3, \cdots, m_{k-1}, m_k\}$

which is the set of original plaintext.

The implementation of CFEA-technique in asymmetric cryptosystem is shown in Figure 3.

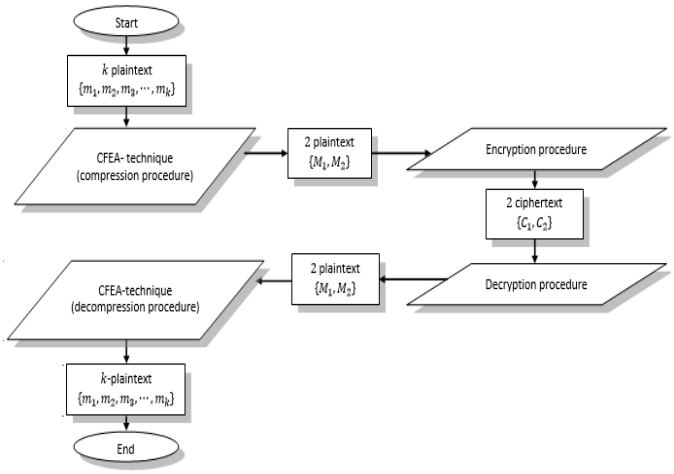


Figure 3 Implementation of CFEA-Technique in Asymmetric Cryptosystem

4.0 CFEA-TECHNIQUE IN EL-GAMAL DIGITAL SIGNATURE SCHEME

In [14], we successfully integrated the CFEA-technique into the ElGamal cryptosystem. It was proven that the ElGamal cryptosystem with embedded CFEA-technique is more efficient especially when we deal with large amount of data. In this paper, we integrated the CFEA-technique into the ElGamal Digital Signature Scheme to reduce the number of documents prior the signing and verification processes. Let say Alice has k documents $D_1, D_2, D_3, \dots, D_k$. Instead of repeating the signing-verification procedures k times, the number of tasks can be reduced by integrating the CFEA-technique into the ElGamal Digital Signature Scheme. The user also does not need to generate k different ephemeral keys each time doing the signing procedure for $k$number of documents.The algorithm of the proposed scheme is shown below:

Algorithm 4: Suppose that Alice wants to send a set of documents $\{D_1, D_2, D_3, \dots, D_k\}$ to Bob. To authenticate herself, she makes an agreement with Bob to sign the document digitally via the El-Gamal Digital Signature Scheme with integrated CFEA-technique.

Compression: (done by Alice)

i. Let $\{D_1, D_2, D_3, \dots, D_k\}$with$D_i \in \mathbb{Z}^+$ for all $i = 1,2, \dots, k$ as the documents.

ii. Compress the k-documents as follows

$$D_1 + \cfrac{1}{D_2 + \cfrac{1}{D_3 + \cfrac{1}{\vdots \; D_{k-1} + \cfrac{1}{D_k}}}} = \frac{d_1}{d_2}$$

iii. Chooses a large prime p such that $d_1, d_2 < p$.

iv. Chooses an integer g where g is a generator of finite field $\mathbb{F}_p^*$.

v. Sends the chosen p and g to Bob.

Key generation: (done by Alice)

i. Chooses a secret signing key $s \in [0, p-1]$

ii. Computes the verification key v as $v = g^s \; mod \; p$

Signing: (done by Alice)

i. Chooses random integers $t_1, t_2 \in \mathbb{F}_p^*$ as her ephemeral keys

ii. Signs the document d_1 and d_2 as follows

$$S_{1,1} = g^{t_1} \; mod \; p$$
$$S_{1,2} = \left(d_1 - sS_{1,1}\right){t_1}^{-1} \; mod \; (p-1)$$
$$S_{1,3} = g^{d_1} \; mod \; p$$

and

$$S_{2,1} = g^{t_2} \; mod \; p$$
$$S_{2,2} = \left(d_2 - sS_{2,1}\right){t_2}^{-1} \; mod \; (p-1)$$
$$S_{2,3} = g^{d_2} \; mod \; p$$

iii. Sends $\left(v, S_{1,1}, S_{1,2}, S_{1,3}, S_{2,1}, S_{2,2}, S_{2,3}\right)$ to Bob and keeps(s, t_1, t_2) secretly.

Verification: (done by Bob)

i. Upon receiving $\left(v, S_{1,1}, S_{1,2}, S_{1,3}, S_{2,1}, S_{2,2}, S_{2,3}\right)$ from Alice, Bob computes

$${d_1}^* = v^{S_{1,1}} S_{1,1}^{S_{1,2}} \; mod \; p$$

and

$${d_2}^* = v^{S_{2,1}} S_{2,1}^{S_{2,2}} \; mod \; p$$

ii. If ${d_1}^* = S_{1,3}$and ${d_2}^* = S_{2,3}$, then Alice's signature is valid. Otherwise, the signature is void.

Decompression: (done by Bob)

i. If the signature is valid, then Bob will proceed to recover the original documents $\{D_1, D_2, D_3, \dots, D_k\}$

ii. Decompresses the document pair d_1 and d_2 to recover the whole document D as follows

$$d_1 = d_2(q_1) + r_1$$
$$d_2 = r_1(q_2) + r_2$$

$$r_1 = r_2(q_3) + r_3$$
$$\vdots$$
$$r_{k-3} = r_{k-2}(q_{k-1}) + r_{k-1}$$
$$r_{k-2} = r_{k-1}(q_k) + r_k$$

Where q_i is quotient and r_i is remainder for $i = 1,2,\dots,k$. From this step, we have

$$\{q_1, q_2, q_3, \cdots, q_{k-1}, q_k\} = \{D_1, D_2, D_3, \cdots, D_{k-1}, D_k\}$$

which is the set of original set of document.

To show that the verification process works, we provided the proof below:

Proof:

$$\begin{aligned} {d_1}^* &= v^{S_{1,1}} S_{1,1}^{S_{1,2}} \bmod p \\ &= [g^s]^{S_{1,1}} S_{1,1}^{S_{1,2}} \bmod p \\ &= [g^s]^{S_{1,1}} [g^{t_1}]^{S_{1,2}} \bmod p \\ &= [g^{sS_{1,1}}][g^{t_1}]^{(d_1 - sS_{1,1}){t_1}^{-1}} \bmod p \\ &= [g^{sS_{1,1}}] g^{(t_1 {t_1}^{-1} d_1 - t_1 {t_1}^{-1} sS_{1,1})} \bmod p \\ &= [g^{sS_{1,1}}] g^{(d_1 - sS_{1,1})} \bmod p \\ &= \left[g^{sS_{1,1} + (-sS_{1,1})}\right] g^{d_1} \bmod p \\ &= g^{d_1} \bmod p \\ &= S_{1,3} \end{aligned}$$

and

$$\begin{aligned} {d_2}^* &= v^{S_{2,1}} S_{2,1}^{S_{2,2}} \bmod p \\ &= [g^s]^{S_{2,1}} S_{2,1}^{S_{2,2}} \bmod p \\ &= [g^s]^{S_{2,1}} [g^{t_2}]^{S_{2,2}} \bmod p \\ &= [g^{sS_{2,1}}][g^{t_2}]^{(d_2 - sS_{2,1}){t_2}^{-1}} \bmod p \\ &= [g^{sS_{2,1}}] g^{(t_2 {t_2}^{-1} d_2 - t_2 {t_2}^{-1} sS_{2,1})} \bmod p \\ &= [g^{sS_{2,1}}] g^{(d_2 - sS_{2,1})} \bmod p \\ &= \left[g^{sS_{2,1} + (-sS_{2,1})}\right] g^{d_2} \bmod p \\ &= g^{d_2} \bmod p \\ &= S_{2,3} \end{aligned}$$

■

5.0 CONCLUSION

In this paper, we successfully embedded the CFEA-technique into the ElGamal Digital Signature Scheme. From the provided proof, the signing and verification procedures worked mathematically. No matter what number the document to be transmitted is, the authentication procedures can be done in smaller number of steps. In addition, the user just needs to generate two ephemeral keys, $t_1, t_2 \in \mathbb{F}_p^*$ to authenticat k documents $\{D_1, D_2, D_3, \cdots, D_{k-1}, D_k\}$ instead of generating k unique ephemeral keys. We expect that the performance of the ElGamal Digital Signature Scheme could be improved especially when we deal with large amount of documents. To verify our claim, further research would be carried out. Some experiments would be conducted to compare the performance of the original ElGamal Digital Signature Scheme with the modified version with integrated CFEA-technique.

Acknowledgement

The authors would like thank University Malaysia Sabah for supporting our participation in the 2015 International Symposium on Sciences and Mathematics (ISySM15). This research is supported by *Research Acculturation Grant Scheme* (*RAGS*) RAG0001-SG-2012 (Malaysia).

References

[1] Farouzan, B. A. 2008. Security Goal in *Introduction to Cryptography & Network Security*. NY: McGraw-Hill Companies Inc. 2-3.

[2] Hoffstein, J., Pipher, J. and Silverman, J. H. 2008. Introduction to Cryptography. In Axier, S. and Ribet, K. A. (ed.). *An Introduction to Mathematical Cryptography*. New York: Springer Sciences Bussiness Media. 1-47.

[3] Rivest, R. L., Shamir, A. and Adleman, L. 1978. A Method of Obtaining Digital Signature and Public Key Cryptosystem. *Commun. ACM21*. 120-126.

[4] El-Gamal, T. 1985. A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithm Algorithm. *IEEE Transactions on Information Theory*. 31(4): 469-472.

[5] Hoffstein, J., Pipher, J. and Silverman, J. H. 2008. Discrete Logarithm and Diffie Hellman. In Axier, S. and Ribet, K. A. (ed.). *An Introduction to Mathematical Cryptography*. New York: Springer Sciences Bussiness Media. 59-92.

[6] Hwang, M. S., Chang, C. C., & Hwang, K. F. 2002. An-ElGamal-Like Cryptosystem for Enciphering Large Messages. *IEEE Transactions of Knowledge and Data Engineering*. 14(2): 445-446.

[7] Chang, Y. S., Wu, T. C., & Huang, S. C. 2000. ElGamal-like Digital Signature and Multisignature Schemes using Self-Certified Public Keys. *The Journal of System and Software*. 99-105.

[8] Sun, M. H., Chen, B. J., & Hwang, T. 1999. Cryptanalysis of Group Signature Scheme using Self-Certified Public Keys. *Electronics Letters*. 35(22).

[9] Hwang, S. J., and Lee, H. Y. 2004. Repairing ElGamal-like Multi-signature Schemes using Self-Certified Public Keys. *Applied Mathematics and Computation*. 73-83.

[10] Yoon, E. J., Ryu, E. K., & Yoo, K. Y. 2004. Efficient Remote User Authentication Scheme based on Generalized ElGamal Signature Scheme. *IEEE Transactions of Knowledge and Data Engineering*. 50(2): 568-570.

[11] Mandangan, A., Loh, C. M., Chang, E. H. and Hussin, C. H. C. 2015. CFEA-Technique: Smaller Size of the Compressed Plaintext. *International Journal of Cryptology Research*. 5(1): 1-10.

[12] Chang, E. H. and Mandangan, A. 2013. Compression-RSA: New Approach of Encryption and Decryption. *AIP Conference Proceedings*. 1522. 50-54.

[13] Mandangan, A., Loh, C. M., Chang, E. H. and Hussin, C. H. C. 2014. Compression-RSA Technique: A More Efficient Encryption-Decryption Procedure. *AIP Conference Proceedings*. 1602: 50-55.

[14] Mandangan, A., Lee, S. Y., Chang, E. H. and Hussin, C. H. C. 2014. El-Gamal Cryptosystem with Embedded Compression-Crypto Technique. *AIP Conference Proceedings*. 1635: 455-460.

[15] Mandangan, A., Chang, E. H., Lee, S. Y. and Hussin, C. H. C. 2014. Integration of CFEA-Technique in Asymmetric Key Cryptosystems. *Proceeding of 3rd International Conference on Interactive Digital Media*. 362-366.