Improved Pohlig - Hellman using Sieve of Eratosthenes for Three-Pass Protocol Security Enhancement

Robbi Rahim [1,3], Nik Adilah Hanin Zahri [2], Mohd Nazri Bin Mohd Warip [1]

[1]*School of Computer and Communication Engineering, Universiti Malaysia Perlis, Malaysia*
[2]*Advanced Communication Engineering Centre (ACE), School of Computer and Communication Engineering, Universiti Malaysia Perlis, Malaysia*
[3]*Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia*

***Abstract* – Password-based is widely used as an exchange model in many areas such as smartphones, computers and other devices in which the keys are directly distributed to the recipients. Therefore, the implementation of cryptographic protocols without key exchange remains an undesirable area. The three-pass protocol is an instrument that enables sender and receiver to send encrypted data without any of the keys being transmitted to recipients. Furthermore, this process eliminates key exchange between senders and recipients when there is three ways direct communication using their own key.**

Keywords– Protocol, Three-Pass Protocol, Security, No Key Cryptography.

1. Introduction

Nowadays, password-based is widely used as an exchange model in many areas such as smartphones, computers and other devices where keys are directly distributed to the recipients [6],[3],[2].

The key distributions are usually performed on algorithms that fall under symmetric type which make use of only one secret key to encrypt and decrypt data [24], [14], [10]. Cryptography [27], [16], [5] is the scientific method that uses encrypted data for encryption of keys, and it will be difficult for someone without decryption keys to understand. Furthermore, the process is carried out by an algorithm with several parameters such as random numbers and keys [7], [17]. Proper use of decryption key allows effective retrieve of the actual data. Therefore, the implementation of cryptographic protocols without key exchange remains an undesirable area, and the strength is based on padding and generated keys.

One of the model without key exchange protocols is Three Pass Protocol (TPP) [22], [24], [26], which is the main focus in this research work. The TPP is a framework that allows sending of encrypted messages without key distribution. TPP eliminates the process of exchanging keys between senders and recipients, where there is three-way direct communication using their own key. Therefore, this method is different from cryptographic symmetric techniques that requires mandatory distribution of key for decryption process. Meanwhile, the asymmetric method needs a long lock, it also requires a longer computation process than the symmetric, and it constrains session keys for delivery.

Data protection, encrypted communication, remote authentication and authentication of ownership are well recognized examples of digital security models. It is also known as information security, which plays an important role in almost every person's life [23]. These security schemes are barely used to check email, activate smart phones, turn on television etc. However, both of these processes conduct various mathematical calculations to verify the identity of the user and to preserve the validity of the information

DOI: 10.18421/TEM101-05
https://doi.org/10.18421/TEM101-05

Corresponding author: Robbi Rahim,
Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia.
Email: usurobbi85@zoho.com

Received: 04 November 2020.
Revised: 14 January 2021.
Accepted: 21 January 2021.
Published: 27 February 2021.

transmitted. These statistical measurements are referred to as a cryptographic operation [9], [12].

Traditionally, one or many keys are used to convert plain text to cipher text at the control panel level [1], and the plain text can be retrieved at the destination with the use of proper decryption keys. A transformation in terms of costs and time is not possible without access to suitable decryption keys [19]. Therefore, the cipher text becomes secure and the attacker could not have access to the important data. However, the main disadvantage in this process is the illegal sharing of key from one user to another, i.e. key distribution problem. The implementation of cryptographic protocols without key exchange remains an undesirable area. In addition, the effectiveness of these approaches without exchanges depends on both the padding and the keys generated.

The most widely used model is three pass protocol (TPP) which enables the transmitter to send cipher text to the receiver without key distribution. It avoids the procedure of key exchange between sender and receiver, in which the transmission occurs in 3 directions where the two parties own their individual keys. This is in contrast to symmetric cryptographic techniques which requires a large key distribution process for effective decryption, while the asymmetric type needs a long lock. It also takes a longer computation time compared to the limitation of symmetric model and session for keys delivering.

In this study, TPP was used for secure communication. In order to prevent and minimizes the attacks during the message communication, the Pohlig-Hellman (PH) Algorithm was individually combined with TPP to make the communication highly secure. This is because there is no exchange between sender and recipient, and the ciphertext result in an arbitrary. It makes use of 2^kPNs as algorithm for PN generator that was used for Encryption and Decryption in PH.

2. Methodology

2.1. Cryptography Technique

There are various forms of encryption techniques used in cryptography, as shown in Figure 1. The classification is ideally suited to the most important variants used by modern ciphers. There are variations between symmetric and asymmetric ciphers. In addition, symmetric techniques have been divided into two groups, namely stream and block ciphers.

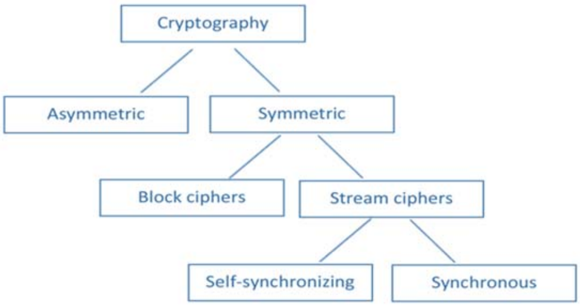


Figure 1. General categorization of cryptography

Cryptographic techniques are classified into two types, namely symmetric and asymmetric as it is shown in Figure 2 and Figure 3 [11], [20]. A cryptographic cipher is assumed to be symmetric when identical secret keys are used to encrypt and decrypt data. At the same time, two different keys are used in asymmetric cipher. Only one key is kept undisclosed which is known as a private key. The second key, on the other hand, is used to allow data encryption, which is especially aimed at the user of the respective private key. This second key is often revealed to average people because in certain cases, the receiver will like to send encrypted messages for all to be viewed. So, the key is known as the public key.

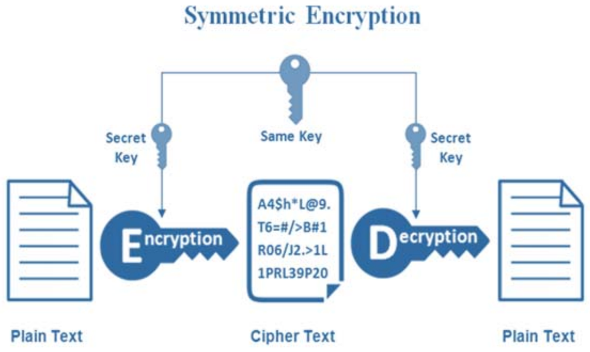


Figure 2. Process involved in Symmetric Encryption

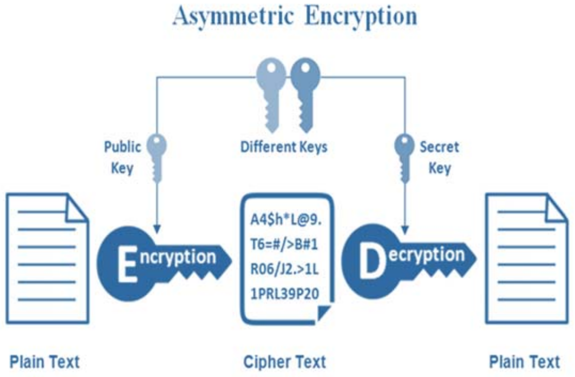


Figure 3. Process involved in Asymmetric Encryption

A message encrypted using a public key can only be decrypted using the corresponding private key, and vice versa. This is useful in situations where a recipient without previous communication wants to make a secure transmission with another party to transmit a shared secret key (similar to symmetric cryptography). If the user wants to transfer encrypted data, they can get the public key of the intended recipient from the public directory and use it to encrypt the message before sending it. The recipient of the message can be decrypted using the correct private key. At the same time, when the sender encrypts a private key, the message will be decrypted at the same time as the public key and the sender will be authenticated. These functions are carried out automatically. As a result users do not need to physically lock and unlock the post.

Asymmetric cryptography is based on mathematical problem that does not provide an efficient solution, such as integer factorization, discrete logarithm, or the ratio of elliptic curve. This is considered as an issue because it is time-consuming however, it is faster than brute Force in trying out every possible key, and it will required larger key sizes. The keys in the asymmetric encryption are at most twice the size as the symmetric key on the same security. This is because of the hardware constraints of embedded systems. The lighter need for symmetric cryptography is preferred above all to avoid the multiplication of large numbers when calculating and storing of large keys in an asymmetric cryptographic model.

2.2. Protocol and Authentication

Cryptography is also used for hidden purposes. The encryption and decryption features can be extended to a specific method such that the legitimacy of one person can be displayed to another. This method is defined in the Cryptosystem Authentication Protocol and additional details are given in Figure 4. A cryptosystem may embed multiple security levels to each entity across different access circumstances. Access circumstances will define the rights gained and the authorization of a specific person. In the meantime, an overview to the specifics of the principle of authorization is given in Figure 5.

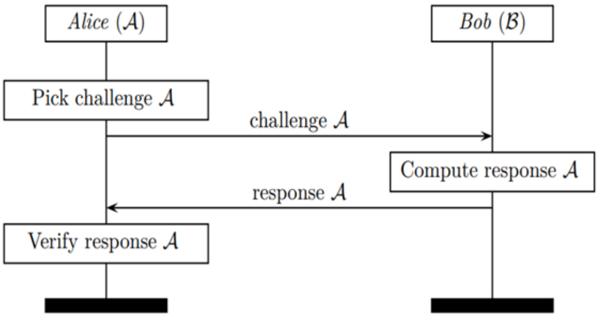

Alice ($\mathcal{A}$)
Bob ($\mathcal{B}$)
Pick challenge $\mathcal{A}$
challenge $\mathcal{A}$
Compute response $\mathcal{A}$
response $\mathcal{A}$
Verify response $\mathcal{A}$

Figure 4. Two-pass single authentication protocol [25]

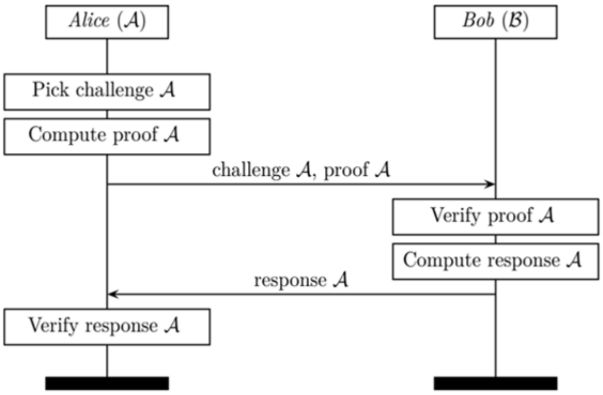

Alice ($\mathcal{A}$)
Bob ($\mathcal{B}$)
Pick challenge $\mathcal{A}$
Compute proof $\mathcal{A}$
challenge $\mathcal{A}$, proof $\mathcal{A}$
Verify proof $\mathcal{A}$
Compute response $\mathcal{A}$
response $\mathcal{A}$
Verify response $\mathcal{A}$

Figure 5. Two-pass mutual authentication protocol [25]

Figure 5 describes the fundamental security mechanism for a three-pass mutual. After a successful mutual [25], *Alice* and *Bob* could trust each location and initiate a transmission session. It is a common practice to cryptographically chain that every extra transmission for the original session should authenticate the credentials. A session has to be initialized with a specific (fresh) arbitrary challenge containing sufficient entropy to suppress predicted values or potential collisions. A structured ISO/IEC 9798-2 is an extra purified and difficult example of the three pass mutual authentication protocols. Furthermore, this special verification method is presented in the literature [4]. In the meantime, enhancing the authentication protocol is one way to reduce the use of confidential data that is spread globally in a symmetrical cryptosystem. One example is the development of diversification cryptographic keys. Diversified keys are provided by an individual that came from a confidential master and concerned with the identification of subscriber data. In this path, different keys are generated for each entity. When these keys have been enhanced, only advanced individuals operate together and are not private. Authorization is often confused with authentication. An authorized state shall classify an individual based on a particular group defined in the Access Catalog [18]. The authentication method can be used as a simple validation technique for reaching an authorized state, but its main objective is to identify and validate the individual. The access situation in the cryptosystem is defined quite strictly in the terms of the authorisation which required a comprehensive criterion for access circumstances that would be acceptable after verification of the ownership of a specific set of credentials. After a good confirmation, the status will be updated. The individual obtains the correct definition of authorisation in the access circumstances, as seen in Figure 6.

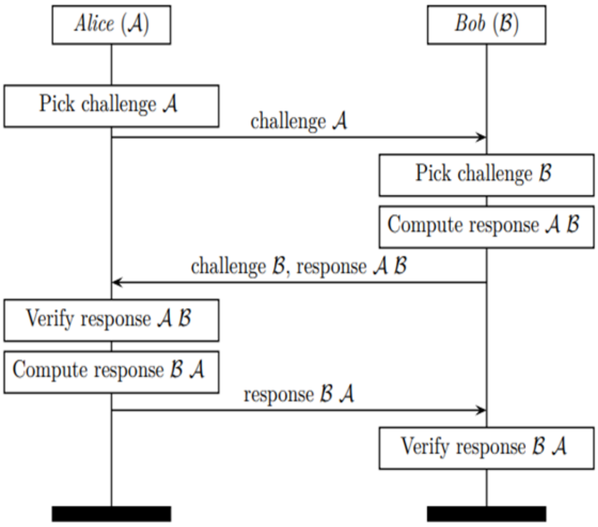


Figure 6. Three-pass mutual authentication protocol [25]

2.3. Proposed Method

Key distribution protocols are widely used as exchange model in which keys are distributed instantly to the receiving end, and this process takes place on the models which are symmetric in nature. On the other hand, TPP is a framework which enables the sender to transmit encrypted message to receiver without the used of secret key. This is known as TPP because the transmitting and receiving users do not required exchange of keys and the communication takes place in 3-directions where both parties use separate keys. It allows different type of cryptographic algorithms to be implemented. In this research work, PH algorithm is employed in TPP protocols with its extended versions.

In this paper, a proposed model was derived to improved Pohlig-Hellman (IPH) algorithm in TPP, furthermore, the derived used a prime number generator (PN) based on Sieve of Eratosthenes (SE) and is referred by IPH-TPP.

3. Result and Discussions

In cryptographic protocol, security is a mandatory factor because of multiple attacks which occur due to wrong selection of techniques. Only a few applications that are involved in PH and TPP is Modular Arithmetic, Greatest Common Divisor (GCD), Euclidean algorithm, PN and Inverse Modulo respectively. In the first objective, an IPH algorithm in TPP is derived by the use of SE based PN generator and is referred by IPH-TPP. The proposed IPH-TPP involves different processes which are explained below.

a. Modular Arithmetic

Modular arithmetic is an integers model in which the values reset to zero and starts to rise again, once a particular fixed value has been reached, known as modulus (modulo). It is commonly employed in computer science and cryptography. PH also used the technique for encryption and decryption. Encryption is applied to measure the values of intended message and the key which is acquired by performing modulo at fixed prime values. The modular arithmetic can be represented as follows:

$$\mathrm{y} = \mathrm{z} * \mathrm{q} + \mathrm{r}, 0 \leq \mathrm{r} < z$$

b. Computation of additional keys using Greatest Common Divisor

This is used in PH when we are calculating additional keys. Furthermore, the condition has to be in odd number, with the GCD ranging between an odd number and a total value of 1. This notation could be defined as $\mathrm{K_e} \in \mathrm{odd}, \mathrm{K_e GCD}(\mathrm{K_e}, \theta) = 1$ GCD is measured with number u and v and largest integer d so that it is derived as $d \mid u$ and $d \mid v$ which is stated as $GCD\ (u, v) = d$. For example, to determine $GCD\ (1.3) = 1$, it is noted that the values of u and v is 1 and 3.

c. Computation of Inverse modulo using Euclidean Algorithm

The Euclidean method was used to calculate the inverse of the number modulo n. In general, the multiplicative inverse of K is I/K, since K*(l\K) = 1. In modular arithmetic, it is hard to calculate the inverse number. The inverse modulo X of K can therefore be described as:

$$1 = (K * X) modulo\ (n)$$
$$(K * X) = 3\ 1\ modulo\ (n)$$
$$K = X - 1 modulo\ (n)$$

In general, it is difficult to find a solution to a modular inverse problem. For example, the inverse of the 4 module 11 is 3. At the same time, 4 does not have an inverse 12 modulo. There is a particular solution in many cases, if K and n are relatively primes. If K and n are not relatively prime, then there is no solution. When n is PN, each number from 1 to (n-1) is relatively prime to n and has exactly one inverse modulo n in that range. The basic principle of the Euclidean algorithm is to discover the two-digit Greatest Common Divisor (GCD). In this case, this technique is used in PH to evaluate the importance of additional keys [21]. It there is 2 negative integers y and z such that y ≥ z, the Euclidean technique could identify the maximum divisor of y and z.

Modulo Inverse Computation

In modular arithmetic, division operation is not available. Therefore, modular inverse is applied and the operation is listed as follows.

- A (mod C) is A^-1
- (A * A^-1) ≡ 1 (mod C) or equivalently (A * A^-1) mod C = 1
- Only numbers coprime to SC have a modular inverse (mod C)

It is helpful in finding the inverse function of numbers. If u and y is assumed to be PN and $y > 1$, then it is an inversion of modulo y. Therefore, $(mod\ y)$ is known as inversion multiplication and is an integer $u - 1$.

$$u * (u - 1) \equiv 1(mody)$$

The corresponding prime description is called GCD $(u, y) = 1$, and is based on above equation, the integers p and q, like: $p * u + q * y = 1$ implies: $p * u + q * m \equiv 1\,(mody)$ as $qy \equiv 0\,(mody)$ then if the value of $p * u \equiv 1\,(mody)$, defined p as the inverse of $(mody)$, therefore, these operation is applied to identify inverse value using PH encryption and decryption process.

The PH algorithm is a special-purpose technique used to compute the discrete logarithms in a finite abelian group whose order is a smooth integer. This encryption technique is similar to RSA algorithm. As it uses various keys for encryption and decryption, this PH model uses asymmetric algorithm [26], [13]. Meanwhile, there is no use of public key in PH technique in order to avoid security issues. This is also applicable to RSA algorithm, because it can be used to performing encryption and decryption using the following formula:

$$C = Pe \bmod z$$
$$P = Cd \bmod z$$

Given that the value of $e * d \equiv 1$. According to the implementation of PH and TPP models, the encryption and decryption of PH-TTP technique is depicted in Figure 7.

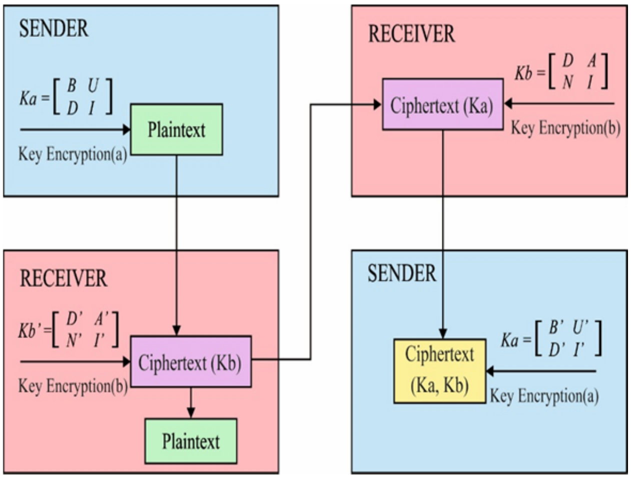
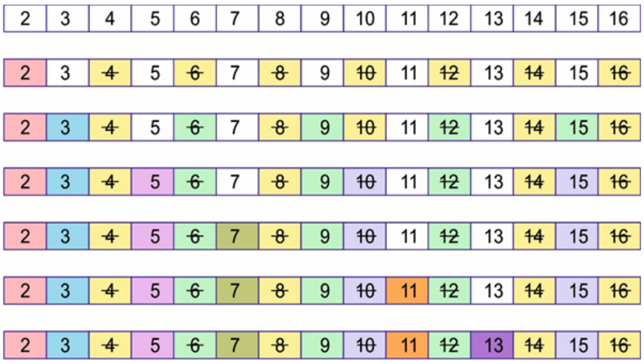


Figure 7. PH Process in TPP

Sieve of Eratosthenes (SE) is a pattern used for finding PN by organizing every natural numbers (1,2,3,4,…) in a sequential order [8]. Once it is arranged, across number 1 and continues the same process till n^{th}. All numbers are retained as PNs. It is assumed that this technique uses computation to identify each PN that are present in the segment $[1; z]$ with $O(zloglogz)$. Initially, it is easy to write numbers from 2 to n. Accurate multiplication of number x is greater than x, and it has to be divided by x. After that, the other number is no longer composite. In this case, 3 are marked where as 3 is the first prime, and multiples of 3 should be fixed as composite. Next, unmarked number is 5 and mark multiples of 5. This process is carried out for all numbers in a row. Figure 8 shows the process of computer engineering in which the PNs are often assembled in a sequential order.



2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15	~~16~~
2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15	~~16~~
2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15	~~16~~
2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15	~~16~~
2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15	~~16~~
2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15	~~16~~

Figure 8. PN generation mechanism

i. The above image reveals that a number is considered to be prime if no smaller PN divides it. The repetition occurs in sequence order, and it can be divided by one or more numbers. Thus, it attains a cell which is not marked, then it is considered as indivisible by small PN which is assigned as prime. The natural numbers are said to be PNs in which it comprised of 2 distinct divisors: 1 and itself. In order to identify PN less than or equal to a given integer z, Eratosthenes' algorithm is applied as follows:

ii. Form a list of consecutive integers from 2 to z such as $(2, 3, 4, \dots, z)$.

iii. Let p equal to 2, be the smallest PN.

iv. Enumerate multiples of p by counting p from $2p$-z, mark them in list i.e., it would be as $2p, 3p, 4p, \dots$; but p itself could not be marked.

v. Identify the first number higher than p which is not marked. If no number is found, then terminate the process, else proceed as let p equals to a new number which is a next PN.

vi. If the algorithm stops, the numbers that are not marked remains as PN below$z$.

The main process is that all the values provided to p are PN. If it is composite, then it is fixed as increment of another small PN. Some values are marked more than once, e.g., 15 can be marked for 3 and 5.

Consequently, it is enough to mark numbers from step 3 begins from p^2 since every smaller multiple of p is previously marked. Meanwhile, this technique makes it possible to stop at step 4 where p^2 is higher than z.

To initialize and increase the list of odd numbers $(3, 5, \ldots, z)$, from $2p$ to p^2in step 3, only odd numbers of p are highlighted. This is generalized using wheel factorization method by creating initial list from co-PNs using few primes rather than odd numbers i.e., co-prime with 2, and counts correspondingly have adjustable multiples. Therefore, the multiples of p originated are small primes.

This algorithm generates all PN which are not greater than n. It adds common optimization function to enumerate multiples of all prime i from i^2. The time complexity of this algorithm is $O(z\, loglog\, z)$ and the array is updated as O (1) process. Since the time complexity is$O(zlog\, logz)$, it performs $\frac{z}{p}$ operations to all primes, $p \leq z$ which is inner loop. Thus, it is evaluated by:

$$\sum_{\substack{p\leq z,\\ pPrime}} \frac{z}{p} = z.\sum_{\substack{p\leq z,\\ pPrime}} \frac{1}{p}.$$

The two important facts of SE are

- Number of PN is lower than or equal to z be approximately $\frac{z}{\ln z}$.
- The tth PN is equal to $tlnt$.
  Hence, the sum is expressed as:

$$\sum_{\substack{p\leq z,\\ pPrime}} \frac{1}{p} \approx \frac{1}{2}.\sum_{\substack{p\leq z,\\ pPrime}}^{\frac{z}{\ln z}} \frac{1}{tlnt}.$$

Here, a PN of 2 is extracted from the sum, since $k = 1$ is approximately equal to 0 and can be divided by zero. It is estimated that the sum is approximated using integral of similar function across t from 2 to $\frac{z}{\ln z}$ which used the rectangular model as the sum relevant to the integral:

$$\sum_{\substack{p\leq z,\\ pPrime}}^{\frac{z}{\ln z}} \frac{1}{tlnt} \approx \int_2^{\frac{z}{\ln z}} \frac{1}{tlnt} dt.$$

The result of anti-derivative for integral $\ln ln\, t$, by substituting and eliminating the lower order is

$$\text{here:} \int_2^{\frac{z}{\ln z}} \frac{1}{tlnt} dt = \ln\ln\frac{z}{\ln z} - \ln\ln 2 = \ln(\ln z - \ln\ln z) - \ln\ln 2 \approx \ln\ln z.$$

Approximate evaluation of actual sum as:

$$\sum_{\substack{p\leq z,\\ pPrime}} \frac{z}{p} \approx z\ln\ln z + o(z).$$

The major evidence could be found for precise estimation that is exactly inside the constant value.

3.1. Implementation of TPP using SE based PN

The conventional TPP protocol is presented by Shamir, but was not completely described in Massey's article [15]. This protocol is applied in several fields because it guarantees confidentiality without any advance distribution of secret keys. The transmitter and receiver use similar encryption technique E_K, where E is encryption algorithm and K indicates key. This corresponds commutatively to the correct use of keys. It is expressed mathematically by:

$$E_{K_{SEN}}\left(E_{K_{REC}}(P)\right) = E_{K_{REC}}\left(E_{K_{SEN}}(P)\right)$$

where K_{SEN} signifies the key of sender and K_{REC}denotes key of receiver which implies that the solution of dual encryption is identical while the receiver is first encrypted K_{SEN}or K_{REC}or transmitter. The classical TPP can be explained as follows:

- Sender and receiver selects its own private key randomly, the secret keys are,$K_{SEN}$and K_{REC}, respectively.
- Transmitter forwards a confidential plain-text P to receiver, and then sender encrypts P with senders key K_{SEN}, followed by sender forwards the simulation outcome cipher-text C_1 to reception.

$$C_1 = E_{ksen}(P).$$

- Next the receiver obtains C_1 and encrypts C_1using receivers key K_{REC}, then receiver transfers resulting cipher-text C_2 again to transmitter

$$C_2 = E_{K_{REC}}(C_1) = E_{K_{REC}}\left(E_{K_{SEN}}(P)\right)$$

- When the sender receives C_2, it is decrypted C_2 by the senders key K_{SEN}. Due to the commutative property in equation (3.1), to eliminate the before encryption with $K_{SEN}$and the outcomes are

$$C_3 = E^{-1}_{K_{SEN}}\left(E_{k_{REC}}\left(E_{k_{SEN}}(P)\right)\right) = E^{-1}_{K_{SEN}}\left(E_{k_{SEN}}\left(E_{k_{REC}}(P)\right)\right) = E_{k_{REC}}(P).$$

  It is followed by the sender forwards C_3 again to receiver.
- While receiver getsC_3, it is decrypted using receiver key in order to acquire K_{REC} which us plain-text P that is successfully sent by sender.

From summary it is acquired that plain-text is produced in two-box with security to receiver. In addition, the receiver used 2 keys for opening two-box with no distribution keys for all patterns in conventional TPP.

4. Conclusion

IPH uses SE to increase security process in Three-Pass Protocol by implementing several algorithms. Furthermore, IPH uses keys that do not use private or public schemes. Therefore, the application of the TPP is very good as the Sender and Receiver can use their respective keys and IPH security level is increase by applying prime numbers and inverse modulo TPP. Further research is likely to evolve into the quantum process as the application will be extended and the results can be compared with the IPH-TPP results of this study.

References

[1]. Ahmad, M., Mittal, N., Garg, P., & Khan, M. M. (2016). Efficient cryptographic substitution box design using travelling salesman problem and chaos. *Perspectives in Science*, *8*, 465-468.

[2]. Lat, J. A. S., Bondoc, R. X. R., & Atienza, K. C. V. (2013). SOUL System: secure online USB login system. *Information Management & Computer Security*, *21*(2), 102-109.

[3]. Bager, K. (2012). Remote access: don't be a victim. *Network Security*, *2012*(6), 11-14.

[4]. Basin, D., Cremers, C., & Meier, S. (2013). Provably repairing the ISO/IEC 9798 standard for entity authentication 1. *Journal of Computer Security*, *21*(6), 817-846.

[5]. Bruce, S. (1996). Applied cryptography. *2nd John Wiley and Sons, Inc*.

[6]. Enos, G., & Zheng, Y. (2015). An ID-based signcryption scheme with compartmented secret sharing for unsigncryption. *Information Processing Letters*, *115*(2), 128-133.

[7]. Silverman, J. H., Hoffstein, J., & Pipher, J. (2008). *An introduction to mathematical cryptography*. Springer.

[8]. Hwang, S., Chung, K., & Kim, D. (2007, October). Load balanced parallel prime number generator with sieve of eratosthenes on cluster computers. In *7th IEEE International Conference on Computer and Information Technology (CIT 2007)* (pp. 295-299). IEEE.

[9]. Reddy, M. I., Kumar, A. S., & Reddy, K. S. (2020). A secured cryptographic system based on DNA and a hybrid key generation approach. *Biosystems*, *197*, 104207.

[10]. Islam, M., Shah, M., Khan, Z., Mahmood, T., & Khan, M. J. (2015, December). A new symmetric key encryption algorithm using images as secret keys. In *2015 13th International Conference on Frontiers of Information Technology (FIT)* (pp. 1-5). IEEE.

[11]. Jallouli, O. (2017). *Chaos-based security under real-time and energy constraints for the Internet of Things* (Doctoral dissertation, Universite De Nantes).

[12]. Le, V. H., den Hartog, J., & Zannone, N. (2018). Security and privacy for innovative automotive applications: a survey. *Computer Communications*, *132*, 17-41.

[13]. Maheswari, A. U., & Durairaj, P. (2018). Modified Shanks'baby-Step Giant-Step Algorithm And Pohlig-Hellman Algorithm. *International Journal of Pure and Applied Mathematics*, *118*(10), 47-56.

[14]. Manna, S., & Dutta, S. (2014). A Stream Cipher based Bit-Level Symmetric Key Cryptographic Technique using Chen Prime Number. *Int. J. Comput. Appl.*, *107*(12), 975-8887.

[15]. Massey, J. L. (1988). An introduction to contemporary cryptology. *Proceedings of the IEEE*, *76*(5), 533-549.

[16]. Buchmann, J. (2013). *Introduction to cryptography*. Springer Science & Business Media.

[17]. Mollin, R. A. (2000). *An introduction to cryptography*. CRC Press.

[18]. Samarati, P., & de Vimercati, S. C. (2000, September). Access control: Policies, models, and mechanisms. In *International School on Foundations of Security Analysis and Design* (pp. 137-196). Springer, Berlin, Heidelberg.

[19]. Shundong, L., Daoshun, W., Yiqi, D., & Ping, L. (2008). Symmetric cryptographic solution to Yao's millionaires' problem and an evaluation of secure multiparty computations. *Information Sciences*, *178*(1), 244-255.

[20]. Simmons, G. J. (1979). Symmetric and asymmetric encryption. *ACM Computing Surveys (CSUR)*, *11*(4), 305-330.

[21]. Sklavos, N., Papadomanolakis, K., Kitsos, P., & Koufopavlou, O. (2002, September). Euclidean algorithm VLSI implementations. In *9th International Conference on Electronics, Circuits and Systems* (Vol. 2, pp. 557-560). IEEE.

[22]. Sui, L., Duan, K., & Liang, J. (2016). A secure double-image sharing scheme based on Shamir′ s three-pass protocol and 2D Sine Logistic modulation map in discrete multiple-parameter fractional angular transform domain. *Optics and Lasers in Engineering*, *80*, 52-62.

[23]. Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, *160*, 102642.

[24]. Uchoa, A. G. D., Pellenz, M. E., Santin, A. O., & Maziero, C. A. (2007, January). A Three-Pass Protocol for Cryptography Based on Padding for Wireless Networks. In *Proceedings of the 2007 4th IEEE Consumer Communications and Networking Conference* (pp. 287-291).

[25]. Verdult, R. (2015). *The (in) security of proprietary cryptography* (Doctoral dissertation, [Sl: sn]).

[26]. Yang, L., Wu, L. A., & Liu, S. (2002, September). Quantum three-pass cryptography protocol. In *Quantum Optics in Computing and Communications* (Vol. 4917, pp. 106-111). International Society for Optics and Photonics.

[27]. Yin, Y., Gan, Y., Wen, H., & Li, T. (2014). A symmetric key exchange protocol bsaed on virtual S-box. *China Communications*, *11*(14), 46-52.