Turkish Journal of Computer and Mathematics Education Vol.12 No.3 (2021), 2249-2255

Research Article

Improving the security of the Knapsack Cryptosystem by using Legendre Symbol

Hamza B. Habib[1], Wadhah Abdulelah Hussein[2], Diana Saleh Mahdi[3]

[1]Department of Mathematics, College of Science, University of Diyala, Iraq
[2]Department of Mathematics, College of Science, University of Diyala, Iraq
[3]Department of Mathematics, College of Science, University of Diyala, Iraq
[1]halsaadi18@yahoo.com ,[2]wadhah.hussein2@gmail.com,[3] dyaina198928@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: In this paper, we present a new cryptosystem based on combining the Knapsack cryptosystem with the Legendre symbol. This combination provides the Knapsack cryptosystem with the feature of using two different super-increasing sequences to generating the keys. The results show that the proposed cryptosystem is secure against the LLL algorithm and Shamir's attacks because it uses two different public keys instead of only one key as in the standard cryptosystem. Moreover, the comparison of the proposed cryptosystem with the standard cryptosystem confirms that using the Legendre symbol increases the decryption time in the proposed cryptosystem. The higher decryption time with the use of two different private keys increases the required time to break the cryptosystem if any possible attacks might exist that can be applied. Therefore, the proposed cryptosystem is more secure and highly effective.

Keywords: Knapsack cryptosystem, Legendre Symbol, public-key cryptosystem, super-increasing sequence, LLL Algorithm.

1. Introduction

Transmitting data through the internet or storing it in network computers has a high possibility of being visible to other people. This means the privacy and any other private online communications will be under a major threat of being used by unauthorized people. Therefore, to prevent the transmitted data from being used, cryptography is applied to convert the plaintext into ciphertext [1]. One type of cryptography is the public-key cryptosystems that use two different keys, public and private, to encrypt and decrypt data [1]. One of the earliest public-key cryptosystems is the Merkle-Hellman knapsack cryptosystem, which was invented by **"**Ralph erkle" and "Martin Hellman" in 1978, and it is based on using the "Subset Sum Problem" [2], [3]. Using subset problem in the Merkle-Hellman knapsack cryptosystem was to make it complicated and hard to be hacked; however, in 1982 Adi Shamir [4]–[6] broke it. Several studies have been done to improve the security of this cryptosystem, for example, using modular knapsack formula [7], elliptic curve and shift knapsack problem [8], by establishing a new easy knapsack cryptosystem [9], using the fact of "Permutation Combination Algorithm" [10], by combining Chinese remainder theorem with the linear transformation of the secret sequences [11] and by converting knapsack cryptosystem to 3CNF [12].

This paper we proposes a secure version of the knapsack cryptosystem based on combining Legendre Symbol with the standard knapsack cryptosystem. The proposed cryptosystem is secure against the LLL algorithm and Shamir's attacks because of the used randomness based on using Legendre Symbol. Moreover, the comparison of the proposed and standard cryptosystems shows that the encryption and decryption times take longer compared to the standard cryptosystem. Increasing the decryption time means more time to break the system if there is any other possible attacks may be applied. Therefore, the results show that the proposed cryptosystem is secured and more efficient compared to the standard cryptosystem.

The structure of this paper is as follows. In Section 2, the Knapsack cryptosystem is discussed. In Section 3, Legendre Symbol is introduced with some basic definitions and theorems. In Section 4, the proposed cryptosystem has been presented. in Section 5, security analysis has been discussed. Finally, in Section 6 conclusions are provided in Section 6.

2. The Knapsack Cryptosystem

Definition1: A sequence $S_n = \{s_n\}_{n=0}^{N-1}$, where $s_n \in \mathbb{Z}^+$, is a super-increasing sequence iff , $s_i > \sum_{j=0}^{i-1} s_j$, $\forall\ 0 \leq i \leq N-1$. [13] [14].

In order, for Alice and Bob to communicate using Knapsack Cryptosystem they need to follow the processes below [2].

A) Generating the Keys Process

The process of generating the keys is done by Alice by following the steps below.

1) A super-increasing sequence, $S = \{s_i\}_{i=0}^{k}$ is chosen.
2) A number n is chosen, such that, $n \geq \sum_i^k s_i$.
3) A number u is selected, such that, $\gcd(u, n) = 1$. Thus, (S, n, u) is the private key, and it is kept secret.
4) $q_i = u * s_i \ (mod\ n)$ is calculated, where $1 \leq i \leq k$, then the sequence $Q = \{q_i\}_{i=1}^{k}$ is the public key, and it is published to be available for everyone.

B) The Encryption Process

To encrypt the plaintext, Bob follows the steps below.

1) Bob converts each character of the plaintext to a binary form b_i of length k bits, where $1 \leq i \leq k$, then he writes them in a sequence $B = \{b_i\}_{i=0}^{k}$.
2) For each b_i, he calculates the corresponding expression en_i as

$$en_i = \sum_{j=1}^{k} q_j * b_{ij}$$

Then, $En = \{en_i\}_{i=1}^{k}$ is the ciphertext, and it is sent to Alice.

C) The Decryption Process

After receiving the ciphertext, the decryption process is performed by Alice. This process requires knowing the private key (S, n, u). Firstly, Alice needs to find the modular multiplicative inverse of a modulo n, u^{-1}, by using the extended Euclidean Algorithm [13]. Then, she multiplies each term of En by u^{-1} modulo n. That is,

$$l_i = en_i * u^{-1}(mod\ n) = \left(\sum_{j=1}^{k} q_i *\ b_{ij}\right) * u^{-1}(mod\ n)$$

where $1 \leq i \leq k$. Then, subtracting the largest number in S, which is less than l_i, from l_i and repeating the subtraction process until zero is obtained. Obtaining zero means b_i is formed, which represents the binary form for the i^{th} character in the plaintext.

3. Legendre Symbol

In this section, a brief introduction of Legendre Symbol is discussed, for more information see [13]–[16]

Definition 1: Let a be an integer and n be a positive integer, then a is a quadratic residue modulo n if $\gcd(a, n) = 1$ and the congruence $x^2 \equiv a\ (mod\ n)$ has a solution. If there is no solution, then a is a quadratic nonresidue modulo n.

Note 1: The only case when $x^2 \equiv a\ (mod\ p)$ and $\gcd(a, p) = 1$, where p is an odd prime number, is considered in this paper.

Definition 2: If p is an odd prime, a is an integer and $\gcd(a, p) = 1$, then the Legendre symbol $\left(\frac{a}{p}\right)$ is given as

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue;} \\ -1, & \text{if } a \text{ is a quadratic nonresidue.} \end{cases}$$

Theorem 1: (Euler's criterion) Let a be a positive integer and p be an odd prime, such that, $\gcd(a, p) = 1$. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}}\ \ (mod\ p).$$

Theorem 2: (Properties of Legendre Symbol) Let p be an odd prime and a and b be positive integers, such that, $\gcd(a, p) = \gcd(b, p) = 1$. Then, [14]

i. If $a \equiv b\ (mod\ p) \Longrightarrow \left(\frac{a}{p}\right)$,
ii. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$,
iii. $\left(\frac{a^2}{p}\right) = 1$.

Theorem 3: Let p an odd prime then,

i) $\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}} = \begin{cases} 1, & if\ \ p \equiv 1\ \ (mod\ 4); \\ -1, & if\ \ p \equiv 3\ \ (mod\ 4). \end{cases}$

ii) $\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} 1, & if\ \ p \equiv 1 \text{ or } 7\ \ (mod\ 8); \\ -1, & if\ \ p \equiv 3 \text{ or } 5\ \ (mod\ 8). \end{cases}$

Theorem 5: (The law of reciprocity) Let p and q be any two odd primes, then,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{2}\ \ 2}$$

4. Proposal Algorithm

In the proposed algorithm, the Knapsack cryptosystem is used based on the value of the Legendre Symbol. Both Alice and Bob agree on choosing a secret large prime number p. Then the quadratic residues and quadratic nonresidues a modulo p are calculated and sorted randomly in a set by both of them. Because Legendre Symbol is either 1 or -1, two separate processes to generate the keys are used instead of one as in the standard Knapsack cryptosystem. That is,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & Generating\ the\ Keys\ Process\ 1; \\ -1, & Generating\ the\ Keys\ Process\ 2. \end{cases} \quad (1)$$

The above formula is kept secret with Alice, and the public key 1 and public key 2 will be sent to Bod to use them based on Legendre symbol. Figure 1 below illustrates the proposed algorithm.

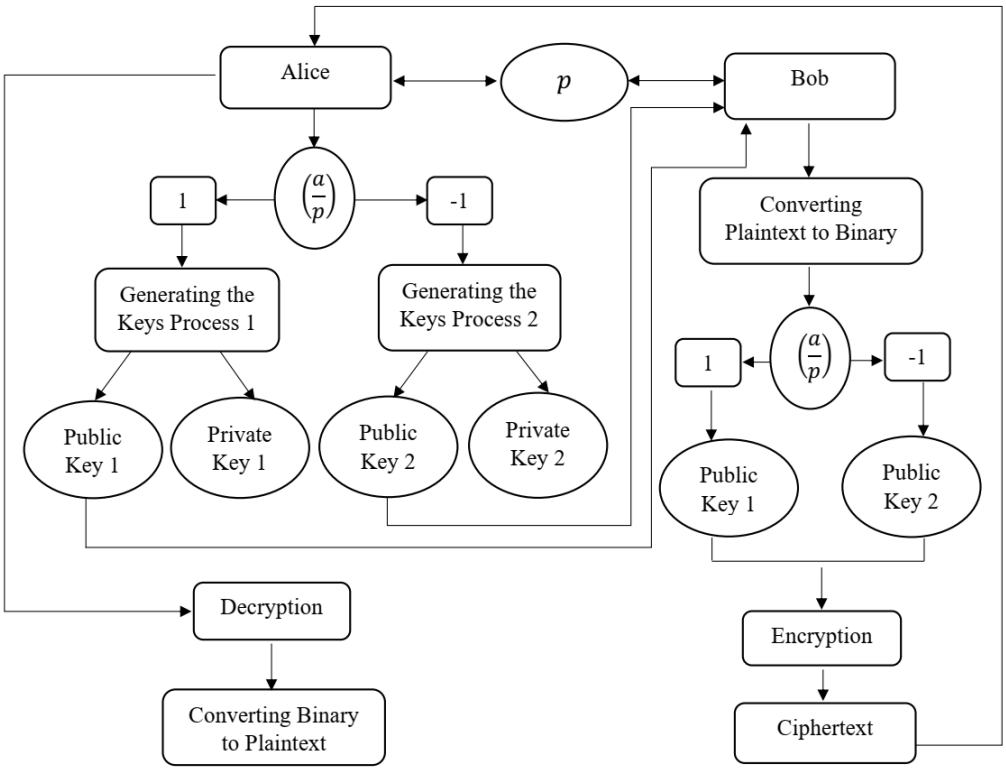

Figure 1: The figure illustrates the Proposed Algorithm

Now we will discuss a working example below using the proposed algorithm.

For simplicity, suppose Alice and Bob agreed on selecting $p = 19$, and the agreed randomly sorted set of quadratic residues and quadratic nonresidues is given as $\{4, 2, 7, 3, 8, 13, 5, \cdots\}$. That is, the agreed corresponding set of Legendre symbol is {1, -1, 1, -1, -1, -1, 1, ⋯}.

A) Generating the Keys Process

i) Process 1

Suppose that Alice generates $S_1 = \{3, 5, 11, 20, 41\}$ and selects $n_1 = 85$ and $u_1 = 44$. Therefore, the first private key is (S_1, n_1, u_1). By using the formula $q_i = u_1 * s_i\ (mod\ n_1)$, the first public key is $Q_1 = \{47, 50, 59, 30, 19\}$.

ii) Process 2

Suppose that $S_2 = \{2, 3, 7, 13, 27\}$ is generated by Alice. Also, she selects $n_2 = 60$ and $u_2 = 7$. Thus, the second private key is (S_2, n_2, u_2). Using $q_i = u_2 * s_i\ (mod\ n_2)$, the second public key is $Q_2 = \{14, 21, 49, 31, 9\}$.

B) The Encryption Process

Suppose that Bob has the plaintext "Help" and would like to send it to Alice. Firstly, the plaintext is converted to a binary form. Secondly, Bob calculates $en_i = \sum_{j=1}^{k} q_j * b_{ij}$ based on the resulting public key from using Formula (1), where the agreed set of Legendre symbol is {1, -1, 1, -1, -1, -1, 1, ⋯}. Table 1 below shows the encryption process.

Table 1: The table shows the encryption process

The Alphabet	b_i	$\left(\frac{a}{p}\right)$	The used Public Key	$en_i = \sum_{j=1}^{k} q_j * b_{ij}$
H	01000	1	$Q_1 = \{47, 50, 59, 30, 19\}$	50
E	00101	-1	$Q_2 = \{14, 21, 49, 31, 9\}$	58
L	01100	1	$Q_1 = \{47, 50, 59, 30, 19\}$	109
P	10000	-1	$Q_2 = \{14, 21, 49, 31, 9\}$	14

Therefore, $En = \{50, 58, 109, 14\}$ is the ciphertext, and it is sent to Alice.

C) The Decryption Process

When the ciphertext, $En = \{50, 58, 109, 14\}$ is received, then Formula (1) is applied by Alice. Alice firstly calculates the inverse of both u_1 modulo n_1 and u_2 modulo n_2

which are $u_1^{-1} = 29$ and $u_2^{-1} = 43$ respectively. Secondly, based on the agreed set of Legendre symbols, {1, -1, 1, -1, -1, -1, 1, ⋯}, Alice calculates $l_i = en_i * u_j^{-1}(mod\ n_j)$, where $1 \le j \le 2,\ 1 \le i \le k$. Then, b_i is calculated by subtracting the largest term in S_j from l_i and by continuing the subtraction process with the rest of the terms in S_j. See Table 2 below.

Table 2: The table shows the decryption process

en_i	$\left(\frac{a}{p}\right)$	The used Process to generate the Keys	n_j	u_i^{-1}	$l_i = en_i * u_j^{-1}(mod\ n_j)$	b_i
50	1	1	85	29	5	01000
58	-1	2	60	43	34	00101
109	1	1	85	29	16	01100
14	-1	2	60	43	2	10000

Then,

$$B = \{01000, 00101, 01100, 10000\}$$

Thus, the plaintext "Help" is obtained after converting B back to the numerical form.

5. Security Analysis

The standard Knapsack cryptosystem can be easily broken by the LLL algorithm only by knowing the public keys and the ciphertext [17]. To recover the plaintext, the LLL algorithm is applied to the matrix

$$\Upsilon = \begin{bmatrix} I_{k\times k} & 0_{1\times k} \\ Q_{k\times 1} & -en_i \end{bmatrix}_{k+1\times k+1}, 1 \le i \le k$$

Where, $I_{k\times k}$ is the identity matrix, $Q_{k\times 1}$ is the public key and en_i is the i^{th} element of the ciphertext [16]. However, the LLL algorithm cannot be applied to the matrix Υ to break the proposed cryptosystem because there are two different processes to generate the keys. These processes use two different super-increasing sequences of length k to generate two different public keys. Therefore, using any public key of length k or two of them of length $2k$ along with the ciphertext will not help the eavesdropper, to recover the plaintext.

Also, Shamir's attack, which breaks the standard cryptosystem [4]–[6], cannot be a serious risk on the proposed cryptosystem. Since it uses two different public keys based on the Legendre Symbol, then knowing the size of q_i, where $1 \le q_i \le n_1$ and $1 \le q_i \le n_2$, by the eavesdropper, does not help him to know the two different private keys. That is, the elements of the two super-increasing sequences will always be hidden from eavesdropper.

Moreover, the comparison between the standard and the proposed cryptosystems is done to calculate the running time of encryption and decryption processes for different text's length in characters, see Table 3 and

Table 4 respectively. The calculations are performed by Maple on a computer with i3-2350M CPU @ 2.30GHz 2.30 and 4GB RAM.

Table 3: The table shows CPU time for encryption processes of The Standard and Proposed Algorithms

Text length in characters	Standard Cryptosystem	Proposed Cryptosystem
21121	594 ms	2235 ms
15809	406 ms	1313 ms
10463	297 ms	875 ms
8681	234 ms	766 ms
6091	172 ms	516 ms
5059	140 ms	437 ms
4001	110 ms	328 ms
3109	94 ms	250 ms
2087	62 ms	156 ms
1093	47 ms	94 ms

Table 4: The table shows CPU time for decryption processes of The Standard and Proposed Algorithms

Text length in characters	Standard Cryptosystem	Proposed Cryptosystem
21121	890 ms	387112.4 ms
15809	422 ms	212412.4667 ms
10463	297 ms	86011.467 ms
8681	250 ms	57797 ms
6091	156 ms	31047 ms
5059	141 ms	18547 ms
4001	125 ms	11281 ms
3109	94 ms	6453 ms
2087	78 ms	2719 ms
1093	47 ms	750 ms

Table 3 and Table 4 above are represented in Figure 2 and Figure 3 respectively. Figure 2 shows the encryption time of the proposed cryptosystem is higher than the encryption time of the standards cryptosystem, and it increases gradually with the increase of text length characters. However, it is clear to notice that the time difference between them is not that high regarding a big text length in characters. Therefore, the proposed cryptosystem has the advantage of being faster to encrypt data.

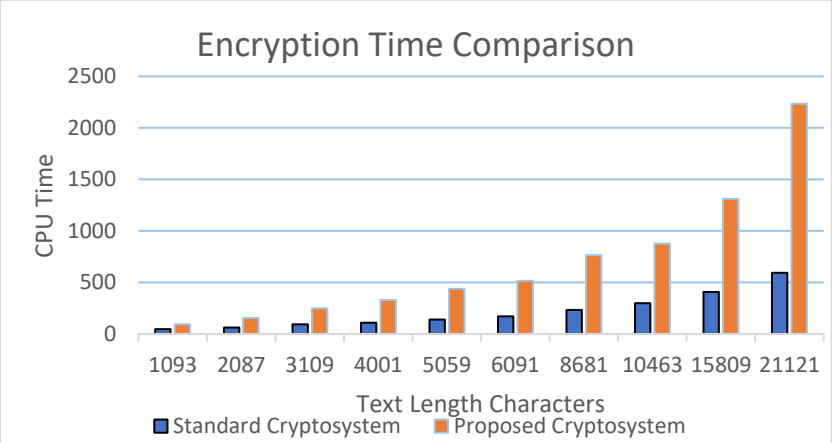

Figure 2: The figure shows the encryption time for both cryptosystems

Furthermore, Figure 3 shows the decryption time of the proposed cryptosystem is much higher than the decryption time of the standard cryptosystem.

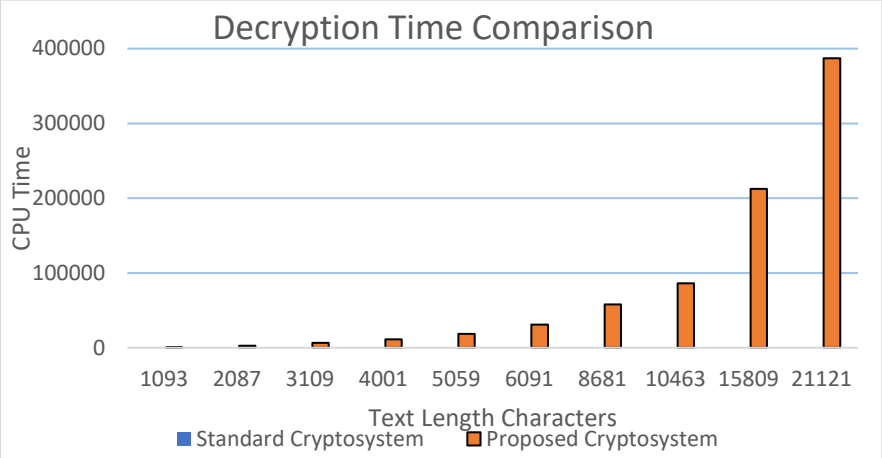

Figure 3: The figure shows the decryption time for both cryptosystems

From the figures above, it can easily be seen that the encryption and decryption times for the proposed algorithm is higher than the encryption and decryption times for the standard algorithm. Significantly, the increase in time increases strongly the security in the proposed cryptosystem.

Conclusion

In this paper, we have proposed an effective algorithm to improve the security of the knapsack cryptosystem. The improvement is based on using the combination of the standard knapsack cryptosystem with Legendre Symbol. Using Legendre Symbol, which is either 1 or -1, provides the advantage of using two different processes to generate the keys. The results show remarkably that the proposed cryptosystem is secure against the LLL algorithm and Shamir's attacks. Moreover, we have found that the decryption time in the proposed cryptosystem is higher than the time in the standard cryptosystem. The higher decryption time using the two different private keys increases the time needed to break the system, and that leads to an increase in the security of the system. Thus, the proposed cryptosystem is highly secured and more efficient comparing to the standard cryptosystem. Though we have shown that our proposed cryptosystem is secure against some famous attacks, some possible attacks might exist that can break it. For further study, the security of the proposed cryptosystem can be discussed against any other possible attacks.

References

1. T. Barakat, Mohamed and Eder, Christian and Hanke, "An Introduction to Cryptography," Timo Hanke RWTH Aachen Univ., pp. 1--145, 2018.
2. R. C. Merkle and M. E. Hellman, "Hiding Information and Signatures in Trapdoor Knapsacks," IEEE Trans. Inf. Theory, 1978, doi: 10.1109/TIT.1978.1055927.
3. K. Sachdeva, "Public Key Cryptography with Knapsack Systems," Int. J. Eng. Adv. Technol., vol. 3, no. 2, 2013.
4. A. Shamir, "A Polynomial Time Algorithm for Breaking The Basic Merkle-Hellman Cryptosystem.," in Annual Symposium on Foundations of Computer Science - Proceedings, 1982, doi: 10.1007/978-1-4757-0602-4_27.
5. A. Shamir, "A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem," 23rd Annu. Symp. Found. Comput. Sci. (sfcs 1982), pp. 145--152, 1982.
6. A. Shamir, "A Polynomial-Time Algorithm for Breaking the Basic Merkle—Hellman Cryptosystem," IEEE Trans. Inf. Theory, 1984, doi: 10.1109/TIT.1984.1056964.
7. R. M. F. Goodman and A. J. McAuley, "A new trapdoor knapsack public key cryptosystem," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1985, vol. 209 LNCS, pp. 150–158, doi: 10.1007/3-540-39757-4_15.
8. C.-H. T. Pin-Chang Su, "New cryptosystems design based on hybrid-mode problems," Comput. Electr. Eng., vol. 35, no. 3, pp. 478–484, 2009.
9. W. Zhang, B. Wang, and Y. Hu, "A New Knapsack Public-Key Cryptosystem," in Fifth International Conference on Information Assurance and Security, 2009, pp. 53–56.
10. M. S. Hwang, C. C. Lee, and S. F. Tzeng, "A new knapsack public-key cryptosystem based on Permutation combination algorithm," World Acad. Sci. Eng. Technol., 2009, doi: 10.5281/zenodo.1056018.
11. Y. Murakami, "A new construction method of knapsack PKC using linear transformation and Chinese

remainder theorem," in ISITA/ISSSTA 2010 - 2010 International Symposium on Information Theory and Its Applications, 2010, doi: 10.1109/ISITA.2010.5649316.

12. J. Thomas and N. Chaudhari, "Knapsack Cryptosystem and its reduction to 3CNF," in Twenty Fifth National Convention of Computer Engineers and National Seminar on Networked Home Systems and Services, 2011, pp. 23–26.
13. K. H. Rosen, Elementary number theory and its applications, 6th ed. Addison-Wesley, Pearson, 2011.
14. H. B. Habib and H. B. Habib, "Diyala Journal for Pure Science," no. 4, pp. 74–84, 2019.
15. B. Karaivanov and T. S. Vassilev, "On Certain Sums Involving the Legendre Symbol," Integers, vol. 16, no. 2, 2016.
16. A. A. ABDULLAH, R. Z. KHALAF and H. B. HABIB, "Modified BB84 Quantum Key Distribution Protocol Using Legendre Symbol", In: 2019 2nd Scientific Conference of Computer Sciences (SCCS). IEEE, 2019. p. 154-157.
17. A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," Math. Ann., vol. 261, no. 4, pp. 515–534, Dec. 1982, doi: 10.1007/BF01457454.