Diyala Journal for Pure Science

The Application of Chebyshev Polynomial on the Three-Pass Protocol

Hamza B. Habib

Department of Mathematics, College of Science, University of Diyala

halsaadi18@yahoo.com

Received: 17 April 2022 **Accepted: 31 May 2022**

DOI: https://dx.doi.org/10.24237/djps.1803.587A

Abstract

Chebyshev polynomial has wide applications in applied Mathematics. The Three Pass Protocol is a cryptographic protocol that is used for the encryption and decryption of data without the need to exchange the keys. We propose in this paper a new cryptosystem based on applying the Chebyshev polynomial to the Three Pass Protocol. The proposed cryptosystem is structured as asymmetric encryption that provides a high level of security to transmit the data. This cryptosystem depends on the fact that the Chebyshev polynomial forms a semigroup based on the composition property. The features of the proposed cryptosystem that are provided by the Chebyshev polynomial are similar to the features that are provided by the Discrete Logarithm. That is, it is secure from attacks, and it is faster to do mathematical calculations. Therefore, the proposed cryptosystem is reliable, secure and faster compared to the other cryptosystems.

Keywords: Chebyshev polynomial, Three-Pass Protocol, Cryptography, composition, Discrete Logarithm.

Diyala Journal for Pure Science

The Application of Chebyshev Polynomial on the Three-Pass Protocol

Hamza B. Habib

تطبيق متعددة الحدود لتشيبيشيف على بروتوكول ثلاثي التمريرات

حمزة بركات حبيب

قسم علوم الرياضيات - كلية العلوم - جامعة ديالى

الخلاصة

متعددة الحدود الحدود لتشيبيشيف لها تطبيقات واسعة في الرياضيات التطبيقية. بروتوكول ثلاثي التمريرات هو بروتوكول تشفير يستخدم لتشفير البيانات وفك تشفيرها دون الحاجة إلى تبادل المفاتيح. في هذا البحث نقدم نظام تشفير جديد يعتمد على تطبيق متعددة الحدود لتشيبيشيف على بروتوكول ثلاثي التمريرات. تم تصميم نظام التشفير المقترح كتشفيرغير متماثل حيث انه يوفر مستوى عالٍ من الأمان لنقل البيانات. يعتمد نظام التشفير هذا على حقيقة أن متعددة حدود لتشيبيشيف تشكل شبه مجموعة بناءً على خاصية التركيب. تتشابه ميزات نظام التشفير المقترح التي يوفرها متعددة الحدود لتشيبيشيف مع الميزات التي يوفرها اللوغاريتم المنفصل. أي أن هذا النظام آمن من الهجمات، وهو أسرع لإجراء العمليات الحسابية. لذلك، فإن نظام التشفير المقترح موثوق وآمن وأسرع مقارنة بأنظمة التشفير الأخرى.

الكلمات المفتاحية: متعددة الحدود لتشيبيشيف، بروتوكول ثلاثي التمريرات، التشفير، التركيب، الوغاريتم المنفصل.

Introduction

In the past few years, transmitting data via digital communication channels has become an essential matter in people's daily lives. Transmitting data between two parties via such channels needs to be secure and confidential; therefore, cryptography is applied to prevent unauthorized parties from knowing the private transmitted data [1-2]. As the attacks on the transmitted data by the standard cryptosystems have increased, several cryptography systems have been developed and introduced, see [3-5].

In 1980, the Three Pass Protocol, which is a cryptographic technique, was introduced by Adi Shamir, [6]. It has an essential role in cryptography because it does not need to exchange the keys to encrypt and decrypt the message. That is, the sender and receiver use their private keys to encrypt and decrypt the messages [7-10].

Volume: 18, Issue: 3, July 2022
Manuscript Code: 587A
P-ISSN: 2222-8373
E-ISSN: 2518-9255

Diyala Journal for Pure Science

The Application of Chebyshev Polynomial on the Three-Pass Protocol

Hamza B. Habib

Chebyshev polynomials have wide applications in applied Mathematics, such as Numerical Analysis, Differential Equations, Cryptography and so on, see [11,12]. Chebyshev polynomials satisfy the composition property, which says for any two positive integers m and n, we have $\mathcal{T}_m(\mathcal{T}_n) = \mathcal{T}_n(\mathcal{T}_m)$, [11-15].

In this paper, we apply the Chebyshev polynomial of the first order on the Three-Pass Protocol to construct a secure hybrid cryptosystem. In the Three-Pass Protocol, the two parties do not exchange the encryption and decryption keys because they use their private keys. The main idea of this cryptosystem is that the two parties choose their independent Chebyshev polynomials to be their private encrypted keys. While the decryption keys are the inverse of these polynomials.

The rest of the paper is structured as: the Three-Pass Protocol is described in section 2. In section 3, the Chebyshev Polynomials are briefly discussed. In section 4, The proposed Algorithm is introduced. In section 5, the conclusion is provided.

The Three Pass Protocol

The Three Pass Protocol, which is a cryptographic technique, provides the feature of communicating between two parties privately without the need in advance to distribute the keys [6]. The name of the Three Pass Protocol comes from the three directions that are carried out by the two parties to communicate [7]. In the Three Pass Protocol, privately each party has an independent encryption key and an independent decryption key. That is, Alice uses her encryption key to encode the plaintext and sends the result to Bob. Then, Bob uses his encryption key to encrypt the result from Alice and sends back the outcome to Alice. Alice then decrypts the outcome from Bob by using her decryption key and sends the result again to Bob. Lastly, Bob decrypts the result by using his decryption key to recover the plaintext [4, 6-10]. Figure 1, shows the steps that are performed by Alice and Bob, where

M = The message,

Volume: 18, Issue: 3, July 2022
Manuscript Code: 587A
P-ISSN: 2222-8373
E-ISSN: 2518-9255

K_{Alice} = Alice's encryption key,

En_{Alice} = Alice's encryption process,

En_{Bob} = Bob's encryption process,

K_{Bob} = Bob's encryption key,

De_{Alice} = Alice's decryption process,

K_{Alice}^{-1} = Alice's encryption inverse key,

De_{Bob} = Bob's decryption process, and

K_{Bob}^{-1} = Bob's decryption inverse key.

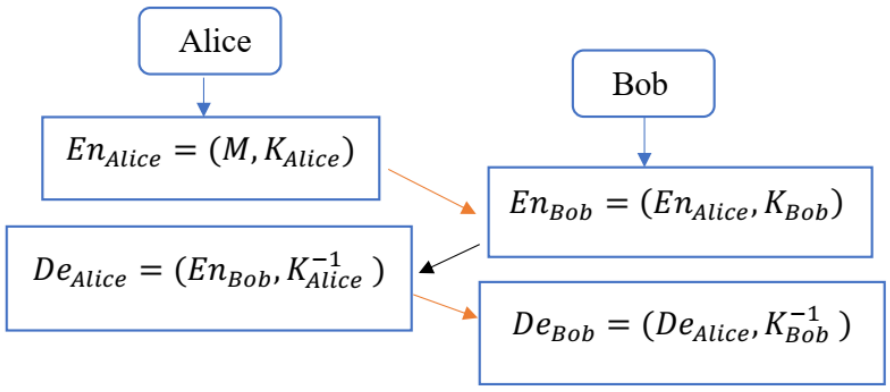

Figure 1: The Figure illustrates the encryption and decryption in the Three Pass Protocol.

Chebyshev Polynomials

Chebyshev Polynomials are used in the applications of Mathematics. In this section, we describe Chebyshev polynomials briefly.

Definition 1: (Chebyshev Polynomials): The Chebyshev Polynomial of degree an integer $m \geq 0$ is given as

Diyala Journal for Pure Science

The Application of Chebyshev Polynomial on the Three-Pass Protocol

Hamza B. Habib

$$\mathcal{T}_m(x) = \cos(m \arccos(x)), \qquad (1)$$

where $-1 \leq x \leq 1$, see [13-15].

Note 1: Formula (1) can be written in another form as

$$\mathcal{T}_m(x) = cos(n\theta), \qquad (2)$$

where $x = \cos(\theta)$ and $\theta \in [0, \pi]$.

Definition 2: (The Recurrence Relation for the Chebyshev Polynomials): The relationship is given as, see [13]

$$\mathcal{T}_{m+1}(x) = 2x\mathcal{T}_m(x) - \mathcal{T}_{m-1}(x),$$

where $m \geq 1$, $\mathcal{T}_0(x) = 1$ and $\mathcal{T}_1(x) = x$.

Example 1: As $\mathcal{T}_0(x) = 1$ and $\mathcal{T}_1(x) = x$, then $\mathcal{T}_2(x)$ is given as

$$\mathcal{T}_2(x) = 2x\mathcal{T}_1(x) - \mathcal{T}_0(x)$$

$$= 2x^2 - 1.$$

Also, $\mathcal{T}_3(x)$ is given as

$$\mathcal{T}_3(x) = 2x\,\mathcal{T}_2(x) - \mathcal{T}_1(x)$$

$$= 2x(2x^2 - 1) - x$$

$$\Rightarrow \mathcal{T}_3(x) .= 4x^3 - 3x$$

Definition 3: (Composition): Let $\mathcal{T}_m(x)$ and $\mathcal{T}_n(x)$ be two Chebyshev polynomials, then, see [13], the composition of them is given by

$$\mathcal{T}_m\big(\mathcal{T}_n(x)\big) = \mathcal{T}_{mn}(x).$$

Volume: 18, Issue: 3, July 2022
Manuscript Code: 587A
P-ISSN: 2222-8373
E-ISSN: 2518-9255

Diyala Journal for Pure Science

Proposition 1: Let $\mathcal{T}_m(x)$ and $\mathcal{T}_n(x)$ be two Chebyshev polynomials, see [11, 16], then

$T_m(T_n(x)) = T_n(T_m(x))$.

Proof: From Formula (1) we have

$$\mathcal{T}_m(\mathcal{T}_n(x)) = \cos(m \arccos(\cos(n \arccos(x))$$

$$, \text{ by Formula (2)} = \cos(mn \arccos(x))$$

$$= \cos(nm \arccos(x))$$

$$= \cos(n \arccos(\cos(m \arccos(x)))$$

$$\Rightarrow \mathcal{T}_m(\mathcal{T}_n(x)) = \mathcal{T}_n(\mathcal{T}_m(x)).$$

Example 2: Let $m = 2$, $n = 3$, then $\mathcal{T}_2(x) = 2x^2 - 1$ and $\mathcal{T}_3(x) = 4x^3 - 3x$. Also, let $x = 5$, then

$$\mathcal{T}_2(\mathcal{T}_3(5)) = 2 * (4 * (5^3) - 3 * 5)^2 - 1$$

$$\Rightarrow \mathcal{T}_2(\mathcal{T}_3(5)) = 470449$$

Also,

$$\mathcal{T}_3(\mathcal{T}_2(5)) = 4 * (2 * (5^2) - 1)^3 - 3 * (2 * (5^2) - 1)$$

$$\Rightarrow \mathcal{T}_3(\mathcal{T}_2(5)) .= 470449$$

Thus, $\mathcal{T}_3(\mathcal{T}_2(5)) = \mathcal{T}_2(\mathcal{T}_3(5))$ as expected.

The Proposed Cryptosystem

The Theoretical Part

Volume: 18, Issue: 3, July 2022
Manuscript Code: 587A
P-ISSN: 2222-8373
E-ISSN: 2518-9255

Diyala Journal for Pure Science

The two parties, Alice and Bob follow the steps below.

1. Alice chooses private positive integers m and x, such that, $T_m(x)$ is the Chebyshev polynomial.
2. Alice calculates

$$X = M * T_m(x) \quad (3)$$

Alice sends X to Bob.

3. Bob chooses private positive integers n and y, such that, $T_n(y)$ is the Chebyshev polynomial.
4. Bob calculates

$$Y = X * T_n(y) \quad (4)$$

and sends Y back to Alice.

5. Alice finds the inverse of $T_m(x)$ as

$$(\mathcal{T}_m(x))^{-1} = \frac{1}{\mathcal{T}_m(x)}.$$

Also, Alice multiplies Formula (4) by $(\mathcal{T}_m(x))^{-1}$, that is,

$$(\mathcal{T}_m(x))^{-1} * Y = (\mathcal{T}_m(x))^{-1} * X * \mathcal{T}_n(y)$$

$$= (\mathcal{T}_m(x))^{-1} * M * \mathcal{T}_m(x) * \mathcal{T}_n(y)$$

$$\Rightarrow (\mathcal{T}_m(x))^{-1} * Y = M * \mathcal{T}_n(y). \quad (5)$$

Then, Alice sends $M * \mathcal{T}_n(y)$ to Bob.

6. Bob finds the inverse of $\mathcal{T}_n(y)$ by working out the formula below

$$(\mathcal{T}_n(y))^{-1} = \frac{1}{\mathcal{T}_n(y)}.$$

Volume: 18, Issue: 3, July 2022
Manuscript Code: 587A
P-ISSN: 2222-8373
E-ISSN: 2518-9255

Also, Bob multiplies Formula (4) by $(\mathcal{T}_n(y))^{-1}$. Then,

$$M * \mathcal{T}_n(y) * (\mathcal{T}_n(y))^{-1} = M.$$

Therefore, the original message, M, is recovered, see Figure 2.

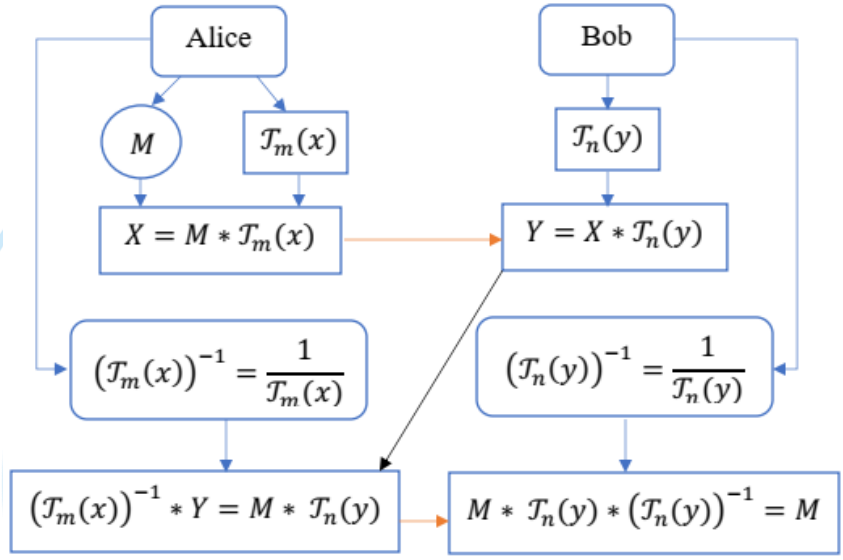

Figure 2: The figure shows the steps followed in the proposed cryptosystem..

The Practical Part

Suppose that Alices chooses $\mathcal{T}_2(x) = 2x^2 - 1$ and $x = 3$, implies $\mathcal{T}_2(3) = 17$. Also, suppose that Alice's message is $M = 8$. Then, Alice calculates

$$X = M * \mathcal{T}_m(x)$$

$$= 8 * \mathcal{T}_2(3)$$

$$\Rightarrow X = 8 * 17 = 136$$

Then, $X = 136$ will be sent to Bob.

After receiving the first pass $X = 136$ by Bob, then suppose that Bob chooses $\mathcal{T}_3(x) = 4x^3 - 3x$ and $x = 5$, implies $\mathcal{T}_3(5) = 485$. Then,

$$Y = X * \mathcal{T}_n(y)$$
$$= 136 * 485$$
$$\Rightarrow Y = 65960$$

That is, $Y = 65960$ will be sent back to Alice.

Alice finds the inverse of $\mathcal{T}_2(3) = 17$, which is $(\mathcal{T}_m(x))^{-1} = \frac{1}{17}$. Then,

$$(\mathcal{T}_m(x))^{-1} * X * \mathcal{T}_n(y) = \frac{1}{17} * 136 * 485 = 3880$$

Then, Alice sends 3880 to Bob.

Bob finds the inverse of $\mathcal{T}_3(5) = 485$, which is $(\mathcal{T}_n(y))^{-1} = \frac{1}{485}$. Then, Bob computes

$$3880 * \frac{1}{485} = 8$$

Then, 8 is the original Alice's message.

Security Analysis

The security of the proposed cryptosystem is directly based on the Chebyshev polynomial and the Three-Pass protocol. To verify the security of this cryptosystem, we notice that when the ciphertext $X = M * T_m(x)$ is given, then the attacker cannot drive M without the information of $T_m(x)$. Moreover, given a ciphertext

$Y = X * T_n(y) = M * T_m(x) * T_n(y)$,

and without the information of $T_m(x)$ and $T_n(y)$, the attacker cannot know M. Finally, given

$$(T_m(x))^{-1} * Y = (T_m(x))^{-1} * M * T_m(x) * T_n(y),$$

cannot recover M without knowing $T_m(x)$, $T_n(y)$, and $(T_m(x))^{-1}$.

Conclusion

In this paper, a new cryptosystem algorithm is proposed. It is based on the application of the Chebyshev polynomial of the first kind on the Three-Pass Protocol. Chebyshev polynomial allows forming of asymmetric encryption, which provides secure communication to send and receive data. The reason behind that is the Chebyshev polynomial form a semigroup based on the composition property. Using Chebyshev polynomial in the proposed cryptosystem makes it secure and fast similar to the discrete logarithm. Moreover, in the Three Pass Protocol, no keys are needed to be exchanged to perform the encryption and decryption processes. Thus, the proposed cryptosystem is secure, fast and reliable compared to the other cryptosystems.

References

1. A. Gupta, N. K. Walia, International Journal of Engineering Development and Research, 2, 2, 1667-1672(2014).
2. A. P. U. Siahaan, International Journal of Computer Science and Engineering, 3, 7, 1-6 (2016)
3. H. B. Habib, W. A. Hussein, D. S. Mahdi, Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12, 11, 2249-2255 (2021)
4. R. Z. Khalaf, H. B. Habib, S. K. Aljaff, Attacking the Application of Three-Pass Protocol in Hill-Cipher, in Next Generation of Internet of Things: Lecture Notes in Networks and Systems, 2021, Springer, Singapore, 121-127
5. R. Z. Khalaf, H. B. Habib, T. A. Jawad, Webology, 19, 1, 5302- 5309 (2022)

6. B. Oktaviana, A. P. U. Siahaan, IOSR Journal of Computer Engineering, 18, 04, 26-29 (2016)

7. Abdullah, Alharith A., Rifaat Khalaf, Mustafa Riza, Mathematical Problems in Engineering 2015(2015)

8. Abdullah, Alharith Abdulkareem, Modified quantum three pass protocol based on hybrid cryptosystem, (2015)

9. A. P. U. Siahaan, International Journal of Science and Research (IJSR), 5, 7, 1149 – 1152 (2016)

10. R. Rahim, M. A. Rosid, A. S. Fitrani, A. Daengs GS, and N. L. W. S. R. Ginantra, Enhancement three-pass protocol security with combination caesar cipher and vigenere cipher, In Journal of Physics: Conference Series, 1402, 6, 2019, IOP Publishing, 066045

11. A. Gil, J. Segura, N. M. Temme, in Numerical methods for special functions, (Society for Industrial and Applied Mathematics, 2007), 51-86

12. H. B. A. Wahab, T. A. Jaber, Engineering and Technology Journal, 34, 5, Part (B) Scientific, 666-674(2016)

13. A. T. Benjamin, and D. Walton, Journal of Statistical Planning and Inference, 140, 8, 2161-2167(2010)

14. P. Brandi, P. E. Ricci, Symmetry, 12, 5, 746 (2020)

15. C. Niu, H. Liao, H. Ma, H. Wu, Mathematics, 9, 24, 3271(2021)

16. M. Lawnik, A. Kapczyński, Computer Science, 20, 3, 367-381(2019)