Brno University of Technology

University of L'Aquila

# Double-Degree Master's Programme - InterMaths
# Applied and Interdisciplinary Mathematics

| Master of Science<br>Mathematical Engineering<br>Brno University of Technology (BUT) | Master of Science<br>Mathematical Engineering<br>University of L'Aquila (UAQ) |
|---|---|

## Master's Thesis

*PUBLIC-KEY CRYPTOGRAPHY AND CHEBYSHEV POLYNOMIALS*

**Supervisor**
Dr Roberto Civino

Roberto Civino

**Candidate**
Francis Appiah

Student ID (UAQ): 279730
Student ID (BUT): 253523

**Academic Year** 2022/2023

# BRNO UNIVERSITY OF TECHNOLOGY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

## FACULTY OF MECHANICAL ENGINEERING

FAKULTA STROJNÍHO INŽENÝRSTVÍ

## INSTITUTE OF MATHEMATICS

ÚSTAV MATEMATIKY

# PUBLIC-KEY CRYPTOGRAPHY AND CHEBYSHEV POLYNOMIALS

PUBLIC-KEY CRYPTOGRAPHY AND CHEBYSHEV POLYNOMIALS

MASTER'S THESIS

DIPLOMOVÁ PRÁCE

| | |
|---|---|
| AUTHOR<br>AUTOR PRÁCE | Francis Appiah |
| SUPERVISOR<br>VEDOUCÍ PRÁCE | Dr. Roberto Civino |

BRNO 2023

BRNO UNIVERSITY OF TECHNOLOGY

Faculty of Mechanical Engineering

MASTER'S THESIS

Brno, 2023

Francis Appiah

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF MECHANICAL ENGINEERING

# Assignment Master's Thesis

| | |
|---|---|
| Institut: | Institute of Mathematics |
| Student: | **Francis Appiah** |
| Degree programm: | Applied and Interdisciplinary Mathematics |
| Branch: | no specialisation |
| Supervisor: | **Dr. Roberto Civino** |
| Academic year: | 2022/23 |

As provided for by the Act No. 111/98 Coll. on higher education institutions and the BUT Study and Examination Regulations, the director of the Institute hereby assigns the following topic of Master's Thesis:

## Public–key cryptography and Chebyshev polynomials

### Brief Description:

After introducing Chebyshev polynomials and discussing their relevant properties, we discuss how to provide public–key encryption from the commutativity under composition. In particular, we show two cryptosystem constructions, one being ElGamal–like and the other being RSA–like, due to Kocarev et al.

### Master's Thesis goals:

– Learn the use of chaotic maps in cryptography, and how they can be used to implement RSA–like and El–Gamal–like cryptosystems by means of Chebyshev polynomials.
– Discuss security matters concerning a new protocol.

### Recommended bibliography:

SMART, N.P. Cryptography made simple. Springer, 2016.

KOCAREV, L., MAKRADULI, J., AMATO, P. Public-key encryption based on Chebyshev polynomials. Circuits Syst. Signal Process. 24(5) (2005), 497-517.

Deadline for submission Master's Thesis is given by the Schedule of the Academic year 2022/23

In Brno,

L. S.

| | |
|---|---|
| doc. Mgr. Petr Vašík, Ph.D.<br>Director of the Institute | doc. Ing. Jiří Hlinka, Ph.D.<br>FME dean |

## Abstract

Public-key encryption enables secure communication over an insecure network. In this thesis, we discuss two public key encryption schemes based on Chebyshev polynomials, which are a class of polynomials that exhibit chaotic properties suitable for cryptographic applications. We discuss that the RSA and ElGamal algorithms are secure, practical, and can be used for encryption. We extend the Chebyshev polynomials over a finite field and demonstrate that the new ElGamal-like and RSA-like algorithms are as secure as the original ElGamal and RSA algorithms.

## Keywords

Public key encryption, RSA, ElGamal algorithm, Chaotic maps, Chebyshev polynomials

Appiah, F.: *Public-key Cryptography and Chebyshev Polynomials*, Brno University of Technology, Faculty of Mechanical Engineering, 2023. xx pp. Supervisor: Dr. Roberto Civino, Ph.D.

I declare that I wrote the diploma thesis *Public-key Cryptography and Chebyshev Polynomials* independently under the guidance of *Dr. Roberto Civino, Ph.D.* using the literature included in the list of references.

Appiah Francis

Blessed be the Lord, for protecting and giving me guidance throughout this study. I would like to extend my sincerest gratitude to Dr. Roberto Civino, Ph.D., who has been a great supervisor and a good mentor, for his patience, support, and guidance during the time of research and writing of this thesis. To my lovely parents and friends, I couldn't have done this without you. Thank you for your support and encouragement along the way.

Appiah Francis

# Contents

# List of Figures

# List of Tables

# 1 Introduction

This section introduces the scope of the thesis: Public-key encryption based on Chebyshev polynomials. A brief history of cryptography and works related to public-key encryption based on chaotic maps, specifically Chebyshev polynomials are discussed. In section 1.1 the goal of the thesis is stated, section 1.2 discusses the outline of the thesis, and in section 1.3 algebraic concepts and theorems related to the study are defined, and stated respectively.

The subject of Cryptography has a long and captivating history, with its complete non-technical account provided in Kahn's "The Codebreakers". The book covers cryptography from its earliest limited use by the Egyptians over 4000 years ago to the 20th century, where it played a crucial role in both world wars. The predominant practitioners of cryptography were associated with the military, diplomatic service, and government, and the subject was used as a tool to protect national secrets and strategies.

Public-key cryptography has contributed significantly to the development of digital signatures, with the first international standard (ISO/IEC 9796) based on the RSA public-key scheme adopted in 1991. In 1994, the U.S. Government adopted the Digital Signature Standard, which uses the ElGamal public-key scheme. The search for new public-key schemes, improvements to existing mechanisms, and security proofs continues at a rapid pace, with various standards and infrastructures involving cryptography being put in place to address the security needs of an information-intensive society.

Cryptography plays a crucial role in computer security as it ensures that data transmitted through unsecured channels is only readable by the authenticated receiver with the correct key. This process is used to encrypt various forms of data, including documents, images, and phone conversations. In addition to privacy, cryptography aims to achieve other goals in communication security, such as guaranteeing the integrity and authenticity of communications. The field has evolved to encompass many sophisticated and fascinating goals beyond just privacy. Diffie and Hellman introduced the concept of public key cryptography in 1976 with their paper "New Directions in Cryptography" [1]. Later, Rivest, Shamir and Adlemann proposed the well-known RSA cryptosystem which implemented this idea. Since then, many new cryptosystems have been proposed and public key cryptography has become a well-established and reliable field of knowledge [2].

Chaotic maps are mathematical functions that display chaotic behavior and can be parameterized by discrete-time or continuous-time parameters. Discrete maps are usually iterated functions and exhibit properties similar to those of confusion and diffusion cryptography. Therefore, they have been used to construct robust and secure cryptosystems that are resistant to statistical attacks [3].

In recent years, there has been interest in exploring the use of chaotic systems in cryptography due to their sensitive dependence on initial conditions and similarity to random behavior [4]. A symmetric key cryptosystem based on chaos theory was presented at a cryptographic conference, but it was found to be vulnerable to attacks at the same conference [5, 6]. Another cryptosystem based on chaotic maps was also broken [7]. Despite these setbacks, chaos theory has found applications in other communication areas, and researchers continue to explore the potential of chaotic systems in designing effective cryptographic primitives [8]. Chebyshev polynomials are a well-known example of one-dimensional chaotic maps used in various applications [4].

Pichler and Scharinger [9] suggested a cryptographic approach that utilizes chaotic permutations which are created by discretizing the two-dimensional bakers map. This method was expanded by Fridrich [10] to include chaotic permutations on two-dimensional lattices of any size. Truong et al. [11] introduced an authentication scheme using chaotic Chebyshev polynomials while Lawnik and Kapczynski [12] investigated the use of modified Chebyshev polynomials in asymmetric cryptography, and Li et al. [13] proposed an outsourcing scheme for verifiable chaotic encryptions based on Chebyshev maps.

Kocarev et al. [14] have proposed a public-key encryption algorithm that utilizes Chebyshev polynomials. Chebyshev polynomials have a commutative property that enables the creation of a public-key cryptosystem. Despite the chaotic properties of these polynomials being well-suited for cryptographic purposes, they do not provide sufficient security against attacks [8]. Therefore, a prime finite field version for Chebyshev polynomials was suggested to prevent attacks and improve the security of the algorithm [15, 14]. As a result, the algorithm was modified to utilize this version of the polynomials.

## 1.1 Goal of the thesis

The purpose of this thesis is to replace the monomial $x^n$ with the Chebyshev polynomials $T_n(x)$ in the Diffie-Hellman and RSA cryptography algorithms and investigate the possibilities of Chebyshev polynomials in the creation of efficient and secure public key encryption algorithms, as well as evaluate their performance in terms of security, computational complexity, and practicality. The thesis will thoroughly review the existing literature on public key encryption, Chebyshev polynomials, and their cryptographic applications. We will also investigate that the inverse problem of computing the degree $n$, the discrete log problem for $T_n(x) \bmod p$, is as difficult as that for $x^n \bmod p$.

## 1.2 Outline of the thesis

Section 2 covers the two most commonly used public-key schemes, the ElGamal and RSA algorithms. Section 3 briefly discusses chaotic maps and the properties that make them suitable for cryptosystems, along with an example of a chaotic map in section 3.2. Chebyshev polynomials are discussed in section 4, including their properties in section 4.1 and theorems supporting the use of Chebyshev polynomials for cryptosystems in section 4.2. Section 4.3 discusses the importance of implementing public-key algorithms with integers over real numbers. The core of the thesis is section 4.4, where we introduce the extended Chebyshev polynomials and two properties critical for designing public-key algorithms. In sections 5.1 and 5.2, we discuss the ElGamal and RSA algorithms on the extended Chebyshev polynomials, respectively, while section 5.3 covers the security of cryptosystems built on the extended Chebyshev polynomials. Finally, we conclude the thesis in section 6.

## 1.3 Algebraic concepts

Although mathematics concepts used in this work are very diverse, attempts to give a universal definition of mathematical terms and concepts are of interest. In this subsection algebraic terms and concepts related to the study are defined and important theorems are stated.

### Groups

**Definition 1.1** (Groups)**.** Let $G$ be a non-empty set with an operation $*$ on its element. $(G, *)$ is called a group if

1. it is closed: i.e $\forall a, b \in G, \quad a * b \in G$.
2. $\exists$ a neutral element $e$, such that $a * e = e * a = a, \quad \forall\, a \in G$.
3. it is associative: $\forall a, b, c \in G \quad (a * b) * c = a * (b * c)$.
4. every element has an inverse: $\forall\, a \in G, \exists\, b \in G$, such that $a * b = b * a = e$.

A group that satisfies the commutative property, i.e. $a * b = b * a \,\forall\, a, b \in G$, is abelian. Almost all groups that are studied under cryptography are abelian and the commutative property is what most cryptosystems are built on.

**Definition 1.2** (Cyclic group)**.** An abelian group is cyclic if there is an element $g$, from which every other element can be obtained by repeated application of the group operation on $g$ or on $g^{-1}$.

**Example 1.3.** $(\mathbb{Z}, +)$ is a cyclic group; it has $g = 1$ and its inverse $-g = -1$, from which every positive integer can be obtained by repeated addition on 1 and negative integers are the inverses of the positive integers.

The order of a group denoted by $\mathrm{ord}(G)$ or $|G|$ is a fundamental concept that can be defined when a group has a finite number of elements.

**Definition 1.4** (Order of group)**.** The order of a finite group is the number of its elements. If a group is not finite, one says that its order is infinite.

For instance, one could mention the group of integers modulo n, which has order n, and the group of real numbers under addition, which has infinite order.

**Definition 1.5** (Order of an element)**.** The order of an element $a$ of a group (also called period) is the order of the subgroup generated by the element.

For instance, if the group operation is denoted as multiplication, the order of an element $a$ of a group is thus the smallest positive integer $m$ such that $a^m = e$, where $e$ denotes the identity element of the group. The order of an element $a$ is denoted by $\mathrm{ord}(a)$ or $|a|$.

**Theorem 1.6** (Lagrange's theorem)**.** *For any subgroup $H$ of a finite group $G$, the order of the subgroup divides the order of the group. In particular for every $a \in G$, it holds that*

1. *$\mathrm{ord}(a)$ divides $|G|$.*
2. *$a^{|G|} = 1$.*

*Point 1 follows from the definition of order of an element and point 2 follows from the fact that, if $m = \mathrm{ord}(a)$, then $|G| = mn$ for some $n \in Z$ from point 1. This implies that $a^{|G|} = a^{mn} = (a^m)^n = 1^n = 1$.*

## Modular arithmetic

**Definition 1.7.** Let $a, b, n$ be integers with $n \neq 0$. We say $a$ is congruent to $b$ mod $n$ denoted as $a \equiv b \pmod{n}$ if $a$ and $b$ differ by a multiple of $n$, thus $a = b + nk$ for some integer $k$ or $a - b$ is a multiple of $n$. The following properties of modular arithmetic are trivially verified.

Let $a, b, c, n$ be integers with $n \neq 0$.

1. $a \equiv 0 \pmod{n}$ if and only if $n \mid a$.
2. $a \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n}$ if and only if $b \equiv a \pmod{n}$.
4. If $a \equiv b$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

**Theorem 1.8** (Fermat's little theorem [16])**.** *If $p$ is a prime number, then for any integer $a$, the number $a^p - a$ is an integer multiple of $p$. In the notation of modular arithmetic, this is expressed as*

$$a^p \equiv a \pmod{p}.$$

*If $p$ is a prime and $p$ does not divide $a$, then Fermat's little theorem is equivalent to*

$$a^{p-1} \equiv 1 \pmod{p}.$$

## Chinese Remainder theorem

For the purpose of this study, the Chinese remainder theorem will be focused on two systems of congruences. The theorem shows that a system of congruences can be replaced by a single congruence under certain conditions.

**Theorem 1.9** (Chinese remainder theorem [16])**.** *Suppose* $\gcd(m, n) = 1$. *Given integers $a$ and $b$, there exists exactly one solution $x \pmod{mn}$ to the simultaneous congruences*

$$\begin{cases} x \equiv a & \pmod{m}, \\ x \equiv b & \pmod{n}. \end{cases}$$

### Fields

A field is a set with two binary operations $(\mathbb{F}, \cdot, +)$ such that

1. $(\mathbb{F}, +)$ is an abelian group with identity 0.
2. $(\mathbb{F}/\{0\}, \cdot)$ is an abelian group.
3. $(\mathbb{F}, \cdot, +)$ satisfies the distribution law i.e $(a + b) \cdot c = (ac + bc)$.

If $F$ is a finite set and is a field then $F$ is a finite field, also known as a Galois field. Throughout this study, the finite field plays a crucial role since the domain of the Chebyshev polynomials is changed from real numbers to finite fields. The most used examples of finite fields in this study are integers modulo $N$, where $N$ is prime, and quadratic extension fields.

### Integer modulo $N$

The integers modulo $N$ are denoted by $\mathrm{GF}(N)$, where $N$ is a prime. $\mathrm{GF}(N)$ is made by integer elements from 0 to $N - 1$ and is a finite field of order $N$. In $\mathrm{GF}(N)$, addition and multiplication are performed modulo N. Addition is defined as the operation of taking the remainder of the sum of two integers when divided by $N$, while multiplication is defined as the operation of taking the remainder of the product of two integers when divided by $N$.

### Quadratic extension fields

Extension fields are finite fields obtained by extending $\mathrm{GF}(N)$ of order $N$ by means of an irreducible polynomial($\mathcal{P}$) of degree $p$, obtaining $\mathrm{GF}(N^p)$, where a polynomial is called irreducible if it has no proper factors other than itself and the constant polynomials [17]. These fields have $N^d$ elements, where $d$ is the degree of $\mathcal{P}$, a positive integer. For $d = 2$ we have a quadratic extension of $\mathrm{GF}(N)$ denoted by $\mathrm{GF}(N^2)$. $\mathrm{GF}(N^2)$ is the field of polynomials of degree at most one with coefficients in the field $\mathrm{GF}(N)$ which represent the remainder of all possible polynomials when divided by a chosen irreducible polynomial of degree 2 in $\mathrm{GF}(N)$.

**Example 1.10.** For the finite field $\mathrm{GF}(2^2)$, $x^2 + x + 1$ is the only irreducible polynomial of degree 2, and the elements of $GF(2^2)$ are $\{0, 1, x, 1 + x\}$ with coefficients $\{0, 1\} \in \mathrm{GF}(2)$.

Hence the elements of $\mathrm{GF}(N^2)$ are of the form $a+bx$, where $a, b \in \mathrm{GF}(N)$ and $x$ is an indeterminate variable satisfying the equation $x^2 - c = 0$, where $c$ is a non-square element of $\mathrm{GF}(N)$. This implies that $x = \sqrt{c}$ and the elements in $\mathrm{GF}(N^2)$ can be rewritten as $a + b\sqrt{c}$, hence in quadratic extension, we consider the set of surds. Moreover, addition, subtraction, and multiplication of surds lead to results of the same form.

### Automorphism of GF$(N^2)$

In the quadratic extension field automorphism is a one-to-one correspondence that takes elements of the form $a + b\sqrt{c}$ to other elements of the same form while preserving the field operations. There are two types of automorphisms of the quadratic extension of $\mathrm{GF}(N)$:

1. Identity automorphism: This automorphism leaves every element of the quadratic extension of GF$(N)$ unchanged.
2. Conjugation automorphism: This automorphism takes any element of the quadratic extension of GF$(N)$ to its conjugate. The conjugate of an element $a + b\sqrt{c}$ is $a - b\sqrt{c}$. This automorphism swaps the two roots of the quadratic polynomial. When $N = 2$ the conjugation automorphism, which maps the element $a + b\sqrt{2}$ to its conjugate $a + b\sqrt{2}$ corresponds to the identity map on GF(2).

## Discrete logarithm problems

A discrete logarithm problem is a mathematical problem that involves finding an integer $x$, given a cyclic group $G$ generated by an element $g$, and $h$ another element in $G$ such that $x$ satisfies the equation $g^x = h$. Let $(G, \cdot)$ be a finite abelian group with prime order $|G| = q$, such as a subgroup of the multiplicative group of a finite field. The discrete logarithm problem in $G$ is: given $g, h \in G$ find an integer $x \in \{1, 2, \ldots, q - 1\}$ such that

$$g^x = h.$$

For some groups this problem is easy to solve: if we consider $(\mathbb{Z}_N, +)$, then given $g, h \in \mathbb{Z}_N$ we find $x$ such that

$$x \cdot g = h.$$

The discrete logarithm problem is considered difficult to solve in $(\mathbb{Z}_p^*, \cdot)$ for large prime values of $p$, and also due to the multiplicative structure of the group. It makes it difficult to apply linear algebraic techniques based on addition and subtraction to the discrete logarithm problem. Although a solution exists since the group is cyclic, there are no known efficient algorithms to find a generator of the group $(\mathbb{Z}_p^*, \cdot)$ making it computationally infeasible for large values of $p$. Many algorithms are known that address the discrete logarithm problem. Some of them have subexponential complexity. However, describing them goes beyond the scope of this work. Discrete logarithm problems are important in cryptography, particularly in public-key cryptography, where they are used to create secure cryptographic algorithms. Some well-known cryptographic algorithms that rely on the difficulty of the discrete logarithm problem include the following.

1. Diffie-Hellman key exchange: In this algorithm, two parties agree on a large prime number $p$ and a primitive root $g$ modulo $p$. The parties then choose secret exponents $a$ and $b$, respectively, and exchange values of $g^a \bmod p$ and $g^b \bmod p$. By computing $(g^a)^b \bmod p = (g^b)^a \bmod p$, the two parties can establish a shared secret key that can be used for symmetric-key encryption. One commonly used algorithm for computing exponentials in a finite group, which is computationally feasible, is the "square and multiply" algorithm. The exponentiation by squaring algorithm is an efficient method for computing the power of an element in a group, especially when the exponent is large.
2. ElGamal encryption: This algorithm is a public-key encryption algorithm that relies on the

difficulty of the discrete logarithm problem in a cyclic group and uses Diffie-hellman key exchange for its secret key generation. The algorithm involves generating a public-private key pair, and using the public key to encrypt messages and the private key to decrypt them.

### Jordan normal form

Finding the Jordan normal form of a matrix is an important tool in linear algebra and it simplifies the matrix in a way that makes its properties more easily understood. It can tell us the matrix's eigenvalues, and the algebraic and geometric multiplicities of each eigenvalue. The Jordan normal form can simplify matrix computations, such as matrix exponentiation and matrix diagonalization. This concept is useful in proving the periodic property of the Chebyshev polynomials over a finite field in this study.
Let $A$ be a $2 \times 2$ matrix with integer entries. Then exists an matrix $S$ which has a inverse such that $A = SBS^{-1}$, where $B$ has one of the following forms:
1. $B = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$. (diagonal matrix)
2. $B = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. (upper triangular matrix)
The matrix $B$ is called the Jordan normal form of $A$, and matrix $S$ is formed by the eigenvectors of the corresponding eigenvalues $(\lambda_1, \lambda_2)$.

# 2 Public-key encryption

The study of secure transmission in the presence of adversaries is known as cryptography. A key component of cryptography is encryption, which enables us to safeguard confidential data from unwanted access. The same key is used for encryption and decryption in conventional symmetric key cryptography. However, this makes it difficult to safely share keys between two parties without the key being intercepted by a third party. On the other hand, public key cryptography employs two distinct keys: a public key for encryption and a private key for decryption. Without a shared secret key, this enables secure contact.

The concept of public key cryptography was first introduced by Whitfield Diffie and Martin Hellman in 1976, but the actual implementation of the system was later developed by Ron Rivest, Adi Shamir, and Leonard Adleman [18, 1, 19]. Public key encryption revolutionized the field of cryptography by allowing secure communication without the need for a shared secret key beforehand and has become a critical component of modern internet security, being widely used in various applications such as SSL/TLS, PGP, and digital signatures.

The RSA scheme is based on another hard mathematical problem, the intractability of factoring large integers [20]. The 1980s saw major advances in this area but none of which rendered the RSA system insecure. Another class of powerful and practical public-key schemes was founded by ElGamal in 1985. These are also based on the discrete logarithm problem [14].

In public-key encryption, let $K$ be the key space and $M$ be the message space, let $\{E_e : e \in \mathcal{K}\}$ be a set of encryption transformations and $\{D_d : d \in \mathcal{K}\}$ be the set of corresponding decryption transformations [20]. Bob uses the encryption transformation to obtain the cipher text $c = E_e(m)$ where $m \in \mathcal{M}$ and sends it to Alice. Alice then applies the decryption transformation to obtain the original message $m = D_d(c)$.

**Definition 2.1.** An encryption scheme is a set of encryption and decryption transformations $\{E_e : e \in \mathcal{K}\}$ and $\{D_d : d \in \mathcal{K}\}$, respectively. The encryption scheme is said to be a public-key encryption scheme if for each associated encryption/decryption pair $(e, d)$, one key $e$ (the public key) is made publicly available, while the other $d$ (the private key) is kept secret. In a secure system, knowledge of the public key $e$ does not allow computation of the private key $d$.

In this section, we will discuss the two mostly used public key schemes, that are the RSA and ElGamal algorithms. We will also discuss their key generation, encryption, and decryption processes.

## 2.1 RSA encryption scheme

RSA is a popular public key cryptography system that operates by utilizing the mathematical properties of prime numbers to ensure secure data transmission. When using RSA, a user generates two keys: a public key for encrypting messages and verifying digital signatures and a private key for decrypting messages and creating digital signatures. RSA is frequently used for secure communication and is particularly prevalent in applications such as encrypted email, digital signatures, and secure web browsing.

## RSA key generation

The RSA algorithm involves a set of messages that can be encrypted and decrypted. This set of messages is called the message space, which is usually depicted as a group of non-negative whole numbers that are lower than a specific value. The message space is denoted as $\mathcal{M} = \{0, 1, 2, ..., k-1\}$, where $k$ is a positive integer indicating the size of the message space. The key space refers to the collection of all possible public and private key pairs for encrypting and decrypting messages.

In RSA, the keys are originated by two large prime integers, $p$, and $q$. The private key is made up of the decryption exponent $d$, which is calculated with the help of $p, q$, and the encryption exponent $e$. The public key is denoted by the values $(n, e)$, where $n = pq$ is the modulus used in encryption and decryption processes. Key generation is a crucial step in RSA and care must be taken to ensure that the primes chosen are sufficiently large and that the keys are kept secure. Key generation in RSA involves creating the public key and the private key. The following are the steps involved in generating the keys:

- Generate two large distinct prime numbers $p$ and $q$.
- compute $n = pq$ and $\varphi(n) = (p-1)(q-1)$ where $\varphi$ is Euler's function.
- select a public exponent $e$, such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$, thus $e$ is coprime to $\varphi(n)$.
- compute the private exponent $d$, $1 < d < \varphi(n)$ such that $ed \equiv 1 \bmod(\varphi(n))$ by extended Euclidean algorithm.
- the public key is the pair $(n, e)$ and the private key is $d$.

## RSA public - key encryption

RSA encryption and decryption are performed using the public and private keys generated during the key generation process. To encrypt a message, using the recipient's public key $(n, e)$, the message is represented as an integer $m$ in the interval $[0, n-1]$. We then compute $c = m^e \pmod{n}$, which is the encrypted message. The cipher text $c$ is sent to the recipient.

To decrypt the cipher text to recover the plaintext $m$, the recipient uses the private key $d$ and computes $m = c^d \pmod{n}$. The decryption is based on Fermat's theorem. Since $ed \equiv 1 \pmod{\varphi(n)}$, there exists an integer $k$ such that $ed = 1 + k\varphi(n)$. Now, if $\gcd(m, p) = 1$ then by Fermat's theorem, $m^{p-1} \equiv 1 \pmod{p}$. Raising both sides of this congruence to the power $k(q-1)$ and then multiplying both sides by $m$ yields

$$m^{1+k(p-1)(q-1)} \equiv m \pmod{p}.$$

On the other hand, if $\gcd(m, p) = p$, then this last congruence is again valid since each side is congruent to 0 modulo $p$. Hence, in all cases $m^{ed} \equiv m \pmod{p}$. By the same argument, $m^{ed} \equiv m \pmod{p}$. Finally, since $p$ and $q$ are distinct primes, it follows that

$$m^{ed} \equiv m \pmod{n}.$$

## 2.2 ElGamal encryption scheme

The ElGamal algorithm is a public-key cryptosystem that was proposed by Taher ElGamal in 1985 [14]. It is based on the mathematical problems of finding discrete logarithms and computing modular exponentiation. This scheme can be viewed as a Diffie-Hellman key agreement in key transfer mode.

### ElGamal key generation

Consider a class of functions defined as $\phi_p(x) = x^p \pmod{n}$, where $n$ is a prime number, $x \subseteq \mathbb{Z}_n^*$ is a generator and $1 \leq p \leq n-2$. The function commute under composition

$$\phi_p(\phi_q(x)) = \phi_{pq}(x). \tag{2.1}$$

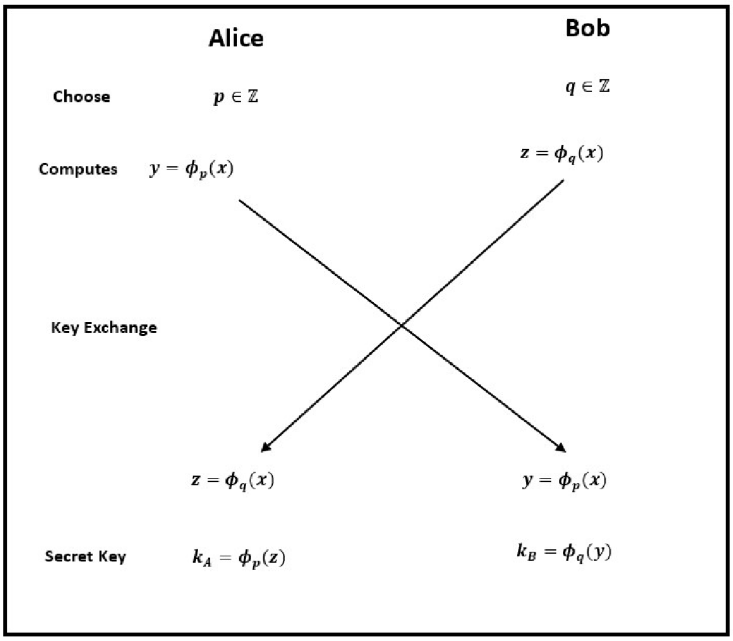

**Figure 2.1:** ElGamal Key Exchange

### ElGamal public - key encryption

In the ElGamal public-key scheme, Alice generates a large random prime $n$ and a generator $x$ of the multiplicative group $\mathbb{Z}_n^*$ of integers modulo $n$. She also generates a random integer $s \leq n-2$

and computes $A = x^s \pmod{n}$. Alice's public and private keys are $(x, n, A)$ and $s$ respectively. To encrypt a message $m$, Bob selects a random integer $r \leq n - 2$, computes $B = x^r \pmod{n}$ and $X = mA^r \pmod{n}$, and sends the cipher-text $c = (B, X)$ to Alice. To recover the message $m$ from $c$, Alice uses the private key $s$ to recover $m$ by computing $m = B^{-s}X \pmod{n}$. The decryption recovers the original message because

$$B^{-s}mA^r \equiv x^{-rs}mx^{rs} \equiv m \pmod{n}.$$

# 3 Chaotic maps

Chaotic maps are mathematical functions that exhibit chaotic behavior, which means that their behavior is highly sensitive to initial conditions and small perturbations. Chaotic maps are used in a variety of fields, including cryptography, engineering, and biology, to model complex systems and phenomena. They describe how a system evolves over time, based on its current state and a set of parameters. One important property of chaotic maps is that they can generate randomness, which is useful in applications such as cryptography and random number generation. In this section, we will discuss the properties of chaotic maps and how they can be used for cryptographic purposes such as encryption and key generation. Finally, we will also examine some of the popular chaotic maps used in cryptography, such as the two-dimensional torus automorphism.

## 3.1 Chaotic maps in Cryptography

Chaotic maps are used in cryptography because they exhibit several properties that make them suitable for cryptographic applications. Here are some important properties of chaotic maps in cryptography.

- Sensitivity to initial conditions: Chaotic maps are highly sensitive to initial conditions, which means that a small change in the initial conditions can lead to a completely different sequence of outputs. This property is important in cryptography because it allows for the generation of unpredictable and random-like sequences of numbers, which can be used as cryptographic keys or for data encryption.
- Mixing property: Chaotic maps have a mixing property, which means that nearby points in the input space are mapped to widely separated points in the output space. This property is important in cryptography because it makes it difficult for an attacker to predict the output sequence based on the input sequence.
- Non-linear behavior: Chaotic maps exhibit non-linear behavior, which means that the output sequence is not a simple function of the input sequence. This property is important in cryptography because it makes it difficult for an attacker to derive the input sequence from the output sequence.
- Non-Periodicity: Chaotic maps typically produce output sequences that are non-repeating and non-periodic, meaning that the same value will not be repeated after a fixed number of iterations. This property is important for ensuring that the output sequence is sufficiently long and unpredictable.

Overall, chaotic maps offer a powerful tool for creating secure cryptographic keys and protecting sensitive data. They are also used as the basis of stream ciphers and the creation of cryptographic hash functions. While they are not foolproof and can be vulnerable to certain types of attacks, they remain an important component of modern cryptography.

### Applying chaotic maps in cryptography

Public key encryption relies on the use of mathematical functions that are computationally difficult to invert. However, there are some variants of public key encryption that use chaotic maps as part of their encryption process, such as the following:

- Chaotic Maps as Pseudo-Random Number Generators: Chaotic maps can be used as a source of randomness in the generation of keys for public key encryption schemes. The initial conditions and parameters of the chaotic map can be used to seed a random number generator, producing a sequence of pseudo-random numbers that can be used as keys for encryption and decryption.
- Chaos-Based Public Key Cryptography: Some public key encryption schemes use chaotic maps as part of their encryption and decryption algorithms. These schemes typically involve the use of a secret chaotic map, known only to the owner of the private key, to generate a public key that can be used for encryption. The corresponding private key can then be used to decrypt the ciphertext.
- Key Exchange Using Chaotic Maps: Chaotic maps can be used in key exchange protocols that allow two parties to agree on a shared secret key for use in symmetric key encryption. In these protocols, the parties agree on a set of initial conditions for a chaotic map and then use the output of the map as the shared secret key.

## 3.2 Torus automorphism

Geometrically, a torus is a closed surface defined as the product of two circles. A torus is a doughnut-shaped object with a hole in the middle. To represent the transformations of the 2-dimensional torus, we need to use matrices that preserve its topology, which means that we can't stretch or shrink the torus or its holes. Automorphisms are mathematical functions that maintain an object's structure. They are useful in many fields of mathematics, including algebra, geometry, and topology. Automorphisms are used in cryptography to create attack-resistant encryption and decryption methods. Torus automorphisms have properties such as periodicity, and mixing that make them suitable for cryptographic purposes.

In this study, we briefly discuss the automorphism of the two-dimensional torus which will be used in understanding the periodicity of the Chebyshev polynomials when extended from real number field to finite fields. Torus automorphism provides a link between number theory and strongly chaotic systems and the $2 \times 2$ torus matrix will be used to prove the period property of the Chebyshev polynomials over a finite field.

**Definition 3.1.** An automorphism of a torus is a bijective function that preserves the algebraic and topological structure of the torus.

A torus automorphism can be described by a linear transformation implemented by a $2 \times 2$ transformation matrix

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

$a, b, c, d$ are integers to ensures that $M$ maps torus into itself and $|M| = 1$ to guarantee invertibility. Let $M$ be a 2 - torus automorphism, then it can be written as a map from $M : (x, y) \longrightarrow (x', y')$ of the form:

$$\begin{aligned} (x', y') &= (ax + by, cx + dy) \mod (1) \\ \begin{pmatrix} x' \\ y' \end{pmatrix} &= M \begin{pmatrix} x \\ y \end{pmatrix} \mod (1). \end{aligned}$$

Characteristic polynomial of a $2 \times 2$ matrix $M$ is $f(z) = \det (M - zI)$. This implies that

$$\begin{aligned} f(z) &= (a - z)(d - z) - cb \\ &= z^2 - (a + d)z + ad - cb \\ &= z^2 - kz + 1. \end{aligned}$$

Let $k$ be the trace of the automorphism $M$ and $\lambda$ one of its root, then

$$\lambda = \frac{k + \sqrt{k^2 - 1}}{2}.$$

It is known that for $k > 2$, the automorphism $M$ has strong chaotic properties, in particular, it has a dense set of unstable periodic orbits [14]. A detailed structure of periodic orbits of the 2-torus automorphism is well structured by [21].

**Example 3.2.** Consider the matrix $M = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$. The trace of $M$ is $k = 3$ which is greater than 2, hence the eigenvalues or the roots of its characteristic polynomial is

$$\lambda = \frac{3 \pm \sqrt{9 - 1}}{2} > 0.$$

In a system, eigenvalues are used to study the behavior of period orbits whether they are stable or not. If any eigenvalue has a positive real part, then the periodic orbit is unstable, meaning that small perturbations in the initial state variables grow over time and the system moves away from the equilibrium. This implies that the matrix $M$ has strong chaotic properties.

# 4 Chebyshev polynomials

Polynomials are fundamental mathematical objects that play a significant part in many areas of cryptography. They are used in a range of cryptographic applications, including error-correcting codes, hash functions, and symmetric encryption. Chebyshev polynomials are a subclass of polynomials with unique properties that are used in a variety of cryptographic uses. In this section, we will look more closely at Chebyshev polynomials since they are the cornerstone on which the public key cryptosystem in this thesis is built. We will talk about their characteristics, such as recurrence relations, chaotic property, and semi-group property. We'll also look at how they're used in encryption, their limitations over the real number field, the need to extend the domain to a finite field, and some mathematically hard problems associated with the polynomial. Finally, we will discuss the properties of the extended Chebyshev polynomials that play crucial roles to build the RSA and ElGamal cryptosystem on the Chebyshev polynomials and explore their advantages.

**Definition 4.1** (Chebyshev polynomials of the first kind)**.** Let $n$ be a non-negative integer. The Chebyshev polynomial of order $n$ is defined as

$$T_n(\cos\theta) = \cos(n\theta). \tag{4.1}$$

The Chebyshev polynomials of the first kind can be alternatively defined as the unique polynomials satisfying the following: Let us define

$$T_n(x) = \begin{cases} \cos(n \arccos x) & \text{if } |x| \le 1, \\ \cosh(n \operatorname{arcosh} x) & \text{if } x \ge 1, \\ (-1)^n \cosh(n \operatorname{arcosh}(-x)) & \text{if } x \le -1. \end{cases}$$

**Definition 4.2** (Chebyshev polynomials of the first kind)**.** Let $n \in \mathrm{Z}^+$ and $x \in [-1, 1]$, the Chebyshev polynomial of order $n$, $T_n(x) : [-1, 1] \to [-1, 1]$ is defined as

$$T_n(x) = \cos(n \cdot \arccos(x)) \quad \text{for } x = \cos(\theta). \tag{4.2}$$

From equation (4.1) and equation (4.2) ;

$T_0(\cos\theta) = \cos(0) = 1;$ $\quad T_0(x) = 1$

$T_1(\cos\theta) = \cos(\theta);$ $\quad T_1(x) = x$

$T_2(\cos\theta) = \cos(2\theta) = 2\cos^2\theta - 1;$ $\quad T_2(x) = 2x^2 - 1 = 2x \cdot T_1(x) - T_0$

$T_3(\cos\theta) = \cos(3\theta) = 4\cos^3\theta - 3\cos\theta;$ $\quad T_3(x) = 4x^3 - 3x = 2x(2x^2 - 1) - x = 2x \cdot T_2(x) - T_1(x).$

From the above relations, the Chebyshev polynomials of order $n$, $T_n(x) : [-1, 1] \to [-1, 1]$ satisfy the recurrence relation

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \tag{4.3}$$

with $T_0(x) = 1$ and $T_1(x) = x$. It is easy to see that all the above definitions of Chebyshev polynomials are equivalent.

Some examples of Chebyshev polynomials are

$$\begin{aligned}
T_0(x) &= 1\\
T_1(x) &= x\\
T_2(x) &= 2x^2 - 1\\
T_3(x) &= 4x^3 - 3x\\
T_4(x) &= 8x^4 - 8x^2 + 1\\
T_5(x) &= 16x^5 - 20x^3 + 5x\\
T_6(x) &= 32x^6 - 48x^4 + 18x^2 - 1\\
T_7(x) &= 64x^7 - 112x^5 + 56x^3 - 7x\\
T_8(x) &= 128x^8 - 256x^6 + 160x^4 - 32x^2 + 1\\
T_9(x) &= 256x^9 - 576x^7 + 432x^5 - 120x^3 + 9x.
\end{aligned}$$

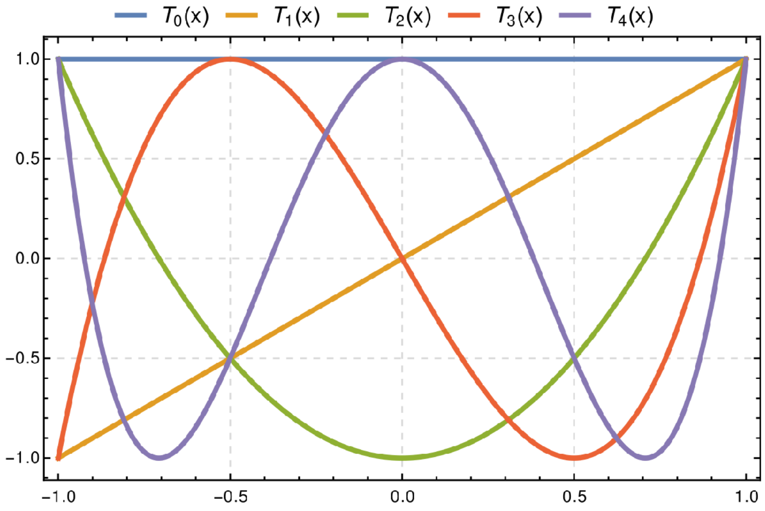

**Figure 4.1:** First 5 Chebyshev polynomials

## 4.1 Properties of Chebyshev polynomials

The Chebyshev polynomials exhibit the following important properties which are very crucial in public key encryption.

**Property 4.3** (Chaotic property)**.** When the degree $n > 1$, the Chebyshev polynomials map $T_n : T_n([-1,1]) = [-1,1]$ is a chaotic map with the function $\mu(x) = \frac{d}{\pi\sqrt{1-x^2}}$ as its invariant measure, and positive Lyapunov exponent $\lambda = \ln|n| > 0$.

When $n = 1$, $T_1(x) = x$ and is not chaotic, but when $n > 1$, the map $T_n(x)$ exhibits chaotic behavior. The invariant measure $\mu(x)$ gives the density of points in the limit as the number of iterations of the map goes to infinity, where $d$ is a normalization constant that ensures that the integral of $\mu(x)$ over the interval $[-1, 1]$ is equal to 1. The Lyapunov exponent $\lambda$ measures the rate at which nearby trajectories diverge or converge. In chaotic systems, the Lyapunov exponent is positive, which means that nearby trajectories diverge exponentially fast. Since $n > 1$, the Lyapunov exponent $\lambda$ is positive. This means that the Chebyshev polynomials map of degree $n$ is a chaotic map, and nearby trajectories diverge exponentially fast.

**Property 4.4** (Even and odd functions)**.** Based on their degrees, the Chebyshev polynomials $T_n(x)$ admit two possibilities as either even or odd functions. Precisely:

- For $n$ even, $T_n(x)$ are even functions.
- For $n$ odd, $T_n(x)$ are odd functions.

*Proof.* From the recurrence relation of Chebyshev polynomials, we can prove that $T_n(x)$ is even when $n$ is even and odd when $n$ is odd using mathematical induction.
Base Case:
When $n = 0$, $T_0(x) = 1$, which is an even function.
When $n = 1$, $T_1(x) = x$, which is an odd function.
Inductive Step:
Assume that $T_k(x)$ is even when $k$ is even and odd when $k$ is odd for some $k \geq 1$. We want to show that $T_{k+1}(x)$ is odd when $k$ is even and even when $k$ is odd.
Case 1: $k$ is even.
By the recursive definition of $T_n(x)$, we have: $T_{k+1}(x) = 2xT_k(x) - T_{k-1}(x)$. Since $T_k(x)$ is even and $T_{k-1}(x)$ is odd (by the inductive hypothesis), then $2xT_k(x)$ is odd. Therefore, the difference between two odd functions is an odd function. Hence, $T_{k+1}(x)$ is odd when $k$ is even.
Case 2: $k$ is odd.
By the recursive definition of $T_n(x)$, we have: $T_{k+1}(x) = 2xT_k(x) - T_{k-1}(x)$. Since $T_k(x)$ is odd and $T_{k-1}(x)$ is even (by the inductive hypothesis), then $2xT_k(x)$ is even. Therefore, the difference between two even functions is an even function. Hence, $T_{k+1}(x)$ is even when $k$ is odd.
Therefore, by mathematical induction, we have shown that $T_n(x)$ is even when $n$ is even and odd when $n$ is odd. □

We will now introduce a crucial property of Chebyshev polynomials. The Chebyshev map has a semi-group property.

**Property 4.5** (Semi - group property)**.** For any positive integers $r, s$ and a real number $x \in [-1, 1]$, this equation is always true.

$$T_r(T_s(x)) = T_{rs}(x). \tag{4.4}$$

An immediate consequence of its semigroup property is Chebyshev polynomials commute under composition [22]

$$T_r(T_s(x)) = T_s(T_r(x)). \tag{4.5}$$

*Proof.* Let us start by proving the relation in equation (4.4)

$$\begin{aligned}
T_r(x) &= \cos(r\arccos(x)); \quad \text{for } -1 \le x \le 1 \\
T_r(T_s(x)) &= T_r(\cos(s\arccos(x))) \\
&= \cos\left[r\arccos(\cos(s\arccos(x)))\right]; \quad \text{but } \arccos(\cos x) = x \\
&= \cos\left[r \cdot s\arccos(x)\right] \\
&= T_{rs}(x).
\end{aligned}$$

□

*Proof.* Let us start by proving the relation in equation (4.5)

$$\begin{aligned}
T_r(x) &= \cos(r\arccos(x)); \quad \text{for } -1 \le x \le 1 \\
T_r(T_s(x)) &= \cos\left[r\arccos(\cos(s\arccos(x)))\right] \\
&= \cos\left[r \cdot s\arccos(x)\right] \\
&= \cos\left[s \cdot r\arccos(x)\right] \\
&= \cos\left[s\arccos(\cos(r\arccos(x)))\right] \\
&= T_s(T_r(x)).
\end{aligned}$$

□

## 4.2 Cryptosystem based on Chebyshev polynomials

Can polynomials in any class other than the pure monomial $x^n$ satisfy property (4.5)? In this section, we answer the above question to explain why this study is focused on Chebyshev polynomials and to justify why public-key cryptosystems like RSA and ElGamal algorithm can be built on Chebyshev polynomials. In the generalized Diffie - Hellman key agreement, instead of generalizing the basic rule of exponents $(g^m)^n = (g^n)^m = g^{mn}$ to an arbitrary group, we consider it as a polynomial identity satisfying the commutative composition $(x^m)^n = (x^n)^m = x^{mn}$. We will show that the pure monomial $x^n$ and Chebyshev polynomials are the only class of polynomials that satisfy the commutative composition.

The characterization of permutable polynomials is complicated and is due to the fact that algebraic structures have different properties that can affect whether polynomials are permutable. The degree of the polynomials can also play a role in determining whether they are permutable.

**Definition 4.6** (Permutable polynomials)**.** Two polynomials, $p$ and $q$, are called permutable if $p(q(x)) = q(p(x))$ for all $x$. If we adopt the notation $p \cdot q$ to indicate the composition $p(q(x))$, then $p$ and $q$ are permutable if $p \cdot q = q \cdot p$.

If $p$ and $q$ are permutable, we shall also say that $p$ commutes with $q$ and, of course, $q$ commutes with $p$. Composition satisfies the associative law

$$p \cdot (q \cdot r) = (p \cdot q) \cdot r$$

From the semi-group property (4.5), we see that any two Chebyshev polynomials are permutable.

**Definition 4.7** (Chain polynomials)**.** A chain polynomial is a sequence of polynomials that are obtained by iterating a given polynomial $p(x)$ such that $P^{(n+1)}(x) = P\left(P^{(n)}(x)\right)$ for $n \geq 0$. We shall write $p^{\{n\}}$ for the $n$-fold composition $p \cdot p \cdots p$.

**Definition 4.8** (Similar polynomials)**.** The polynomials $p(x)$ and $q(x)$ are said to be similar if there exists a non-singular linear transformation $\lambda(x)$ such that $g(x) = \lambda(f(x))$ for all $x$.

**Definition 4.9** (Set of polynomials)**.** Let $\mathscr{P}_n$ be the set of polynomials whose degree does not exceed $n$, i.e., if $p(x) = a_0 + a_1 x + \cdots + a_k x^k$ and $k \leqslant n$, then $p \in \mathscr{P}_n$.

The answer to the above question is that the Chebyshev polynomials $\{T_j\}$ and the pure monomials $\{\pi_j\}$ are the only possible chain polynomials up to similarities [22, 23]. If two polynomials commute, they are either both chain polynomials or both similar to either a Chebyshev polynomial or a pure monomial function, with respect to the same rational function $\lambda(x)$.

To prove the above statement, our first result is that no polynomials other than Chebyshev polynomials can commute with a given $\{T_n\}$ if $n \geqslant 2$.

**Theorem 4.10** (Bertram)**.** *If $n \geqslant 2$ and the polynomial $p$ of degree $k \geqslant 1$ commutes with $T_n$, then $p = T_k$ if $n$ is even and $p = \pm T_k$ if $n$ is odd.*

*Proof.* It is possible to prove that $\pm T_m(x)$ are the only polynomial solutions of

$$\left(1 - x^2\right)\left(y'\right)^2 = m^2\left(1 - y^2\right) \tag{4.6}$$

for $m > 0$. The theorem is proved by showing that, if $p$ commutes with $T_n$, $y = p$ satisfies (4.6) with $m = k$. The polynomial

$$q(x) = \left(1 - x^2\right)\left(p'(x)\right)^2 - k^2\left(1 - p^2(x)\right)$$

is in $\mathscr{P}_{2k-1}$, since the coefficient of $x^{2k}$ is zero, but

$$\begin{aligned} n^2 q \cdot T_n &= n^2\left(1 - T_n^2\right)\left(p' \cdot T_n\right)^2 - n^2 k^2\left(1 - \left(p \cdot T_n\right)^2\right) \\ &= \left(1 - x^2\right)\left(T_n'\right)^2\left(p' \cdot T_n\right)^2 - k^2\left(1 - p^2\right)\left(T_n' p\right)^2, \end{aligned}$$

where we have used the permutability of $p$ and $T_n$ and the fact that $T_n$ satisifies (4.6) with $m = n$. Now,

$$\left(p' \cdot T_n\right) T_n' = \left(p \cdot T_n\right)' = \left(T_n \cdot p\right)' = \left(T_n' \cdot p\right) p'$$

hence

$$\begin{aligned} n^2 q \cdot T_n &= \left(1-x^2\right)\left(p'\right)^2 \left(T_n' p\right)^2 - k^2\left(1-p^2\right)\left(T_n' \cdot p\right)^2 \\ &= \left(T_n' \cdot p\right)^2 \left(\left(1-x^2\right)\left(p'\right)^2 - k^2\left(1-p^2\right)\right) \\ &= \left(T_n' p\right)^2 q. \end{aligned} \tag{4.7}$$

Suppose that $q \neq 0$ has degree $s (\leqslant 2k-1)$, then (4.7) implies that $sn = 2(n-1)k + s$ so that $s = 2k > 2k-1$, a contradiction. Thus $q$ is identically zero and $p = \pm T_k$. If $n$ is even, $T_n \cdot (-T_k) = T_n \cdot T_k = T_k \cdot T_n \neq -T_k \cdot T_n$, hence $p = T_k$. If $n$ is odd, $T_n \cdot (-T_k) = -T_n \cdot T_k = -T_k \cdot T_n$, hence $p = \pm T_k$. □

A sequence of polynomials, each of positive degrees, containing at least one of each positive degree and such that every two polynomials are permutable is called a chain. The Chebyshev polynomials $T_1(x), \ldots, T_n(x), \ldots$, form a chain. So do the powers $\pi_j(x) \equiv x^j$, $j = 1, 2, \ldots$, as is easily verified. We shall see that these are essentially the only chains. Suppose that

$$\lambda(x) = ax + b, \quad a \neq 0, \tag{4.8}$$

so that

$$\lambda^{-1}(x) = \frac{x-b}{a}.$$

If $p$ and $q$ commute, it is clear that $\lambda^{-1} \cdot p \cdot \lambda$ and $\lambda^{-1} \cdot q \cdot \lambda$ also commute. Thus for any $\lambda$ of the form (4.8) the sequences $\lambda^{-1} \cdot T_j \cdot \lambda$, $j = 1, 2, \ldots$, and $\lambda^{-1} \cdot \pi_j \cdot \lambda$, $j = 1, 2, \ldots$, are also chains, and this is the reason the word "essentially" was needed above. We shall say that $p$ and $\lambda^{-1} \cdot p \cdot \lambda$ are similar, hence our goal is to show that the sequences $\left\{T_j\right\}$ and $\left\{\pi_j\right\}$ are the only chains, up to similarities. A first step in this direction is a companion piece to Theorem 4.10.

In the next theorem, we show that no polynomials other than pure monomials can commute with a given $\{\pi_n\}$ if $n \geqslant 2$.

**Theorem 4.11.** *If $n \geqslant 2$ and the polynomial $p$ of degree $k \geqslant 1$ commutes with $\pi_n(x)$ $(= x^n)$ then $p = \pi_k$ if $n$ is even and $p = \pm\pi_k$ if $n$ is odd.*

*Proof.* The polynomial $y = \pi_n(x)$ satisfies

$$xy' = ny. \tag{4.9}$$

The polynomial $q(x) = xp'(x) - kp(x)$ is in $\mathscr{P}_{k-1}$, since the coefficient of $x^k$ is zero. An argument analogous to that given in the proof of Theorem 4.10 yields

$$\begin{aligned} nq \cdot \pi_n &= n\pi_n p'(\pi_n) - knp(\pi_n) \\ &= n\pi_n p' \cdot \pi_n - kn\pi_n(p) \\ &= x\pi_n' \cdot p'\pi_n - kp\pi_n'(p) \end{aligned}$$

$$
\begin{aligned}
&= x\pi_n'(p) \cdot p' - kp\pi_n'(p) \\
&= \pi_n'(p)[xp'(x) - kp(x)] \\
&= \left(\pi_n' \cdot p\right) q.
\end{aligned}
$$

$nq \cdot \pi_n = \left(\pi_n' \cdot p\right) q$, and if $q$ is of degree $s$ such that $0 \leqslant s \leqslant k-1$ then $sn = k(n-1)+s$ implies that $s = k > k-1$, a contradiction; $q$ must therefore be the zero polynomial. Hence $y = p$ satisifies (4.9) with $n$ replaced by $k$, which means that $p(x) = cx^k (c \neq 0)$. The requirement that $p$ commute with $\pi_n$ implies that $cx^{kn} = c^n x^{kn}$, i.e., $c^{n-1} = 1$. Since $c$ must be real, $c = 1$ if $n$ is even and $c = \pm 1$ if $n$ is odd. □

In this theorem, we aim to show that, a chain contains exactly one polynomial of each positive degree and that there cannot be two distinct polynomials of degree $k$ commuting with a quadratic function.

**Theorem 4.12.** *There is at most one polynomial of degree $k \geqslant 1$ permutable with a given quadratic, $s(x) = a_0 + a_1 x + a_2 x^2, a_2 \neq 0$.*

*Proof.* If we put

$$
\begin{aligned}
\lambda(x) &= \frac{x}{a_2} - \frac{a_1}{2a_2}, \qquad (4.10)\\
\lambda^{-1}(x) &= a_2 x + \frac{a_1}{2},
\end{aligned}
$$

$$
\begin{aligned}
(s \cdot \lambda)\,(\mathrm{x}) &= a_0 + a_1\left(\frac{x}{a_2} - \frac{a_1}{2a_2}\right) + a_2\left(\frac{x}{a_2} - \frac{a_1}{2a_2}\right)^2 \\
&= a_0 + \frac{a_1 x}{a_2} - \frac{a_1^2}{2a_2} + \left(\frac{x^2}{a_2} - \frac{2a_1 x}{2a_2} + \frac{a_1^2}{4a_2}\right).
\end{aligned}
$$

We obtain

$$
\begin{aligned}
\left(\lambda^{-1} \cdot s \cdot \lambda\right)(\mathrm{x}) &= a_2\left(a_0 + \frac{a_1 x}{a_2} - \frac{a_1^2}{2a_2} + \frac{x^2}{a_2} - \frac{2a_1 x}{2a_2} + \frac{a_1^2}{4a_2}\right) + \frac{a_1}{2} \\
&= a_0 a_2 + a_1 x - \frac{a_1^2}{2} + x^2 - a_1 x + \frac{a_1^2}{4} + \frac{a_1}{2} \\
&= x^2 + c
\end{aligned}
$$

where $c = a_0 a_2 + (a_1/2) - \left(a_1^2/4\right)$. Thus to prove the theorem it suffices to show that there cannot be two distinct polynomials of degree $k$ commuting with $x^2 + c$, for, if $f$ and $g$ are distinct polynomials of degree $k$ commuting with $s$, there are distinct polynomials of degree $k$ similar to $f$ and $g$ via (4.10) that commute with $x^2 + c$. Suppose that $p$ and $q$ are distinct polynomials that satisfy

$$\begin{aligned} p\left(x^2+c\right) &= p^2(x)+c, \\ q\left(x^2+c\right) &= q^2(x)+c, \end{aligned} \tag{4.11}$$

then comparing leading coefficients on both sides of each equality reveals that $p$ and $q$ both have leading coefficient 1. Thus $r = p - q \in \mathscr{P}_{k-1}$. Also

$$r\left(x^2+c\right) = p^2(x) - q^2(x) = r(x)(p(x)+q(x)). \tag{4.12}$$

If the degree of $r$ is $t \geq 0$, then according to (4.12) $2t = t + k$ or $t = k$, a contradiction. Therefore $r$ is the zero polynomial and $p = q$. This contradiction establishes the theorem. □

An immediate consequence of Theorem 4.12 is that a chain contains exactly one polynomial of each positive degree; i.e., a chain is a sequence $\left\{p_j\right\}, j = 1, 2, \ldots$ where $p_j$ is of degree $j$ and each pair of polynomials commutes. Two chains are called similar if there exists a $\lambda(x)$ satisfying (4.8) such that each polynomial in one is similar via $\lambda$ to the polynomial of the other of the same degree. We can now prove our main result that, the sequence $\{T_j\}$ and $\{\pi_j\}$ are the only chains, up to similarities.

**Theorem 4.13.** *Every chain is either similar to* $\left\{x^j\right\}, j = 1, 2, \ldots$, *or* $\left\{T_j\right\}, j = 1, 2, \ldots$

*Proof.* Let $\left\{p_j\right\}, j = 1, 2, \ldots$, be a chain, with $p_2(x) = a_0 + a_1x + a_2x^2$. Let $\left\{a_j\right\}, j = 1, 2, \ldots$, be the chain similar to $\left\{p_j\right\}$ with $\lambda$ as defined in (4.10). Then $q_2(x) = x^2 + c$; $q_3$ commutes with $q_2$, hence

$$q_3\left(x^2+c\right) = q_3^2(x) + c. \tag{4.13}$$

Thus ${q_3}^2(-x) = {q_3}^2(x)$, and since $q_3$ is of degree 3 we see that $q_3(-x) = -q_3(x)$; i.e., $q_3$ is an odd polynomial, say,

$$q_3(x) = b_1x + b_3x^3. \tag{4.14}$$

If we substitute (4.14) into (4.13), we obtain

$$\begin{aligned} q_3\left(x^2+c\right) &= \left(b_1x + b_3x^3\right)^2 + c \\ &= b_1^2x^2 + 2b_1b_3x^4 + b_3^2x^6 + c \\ q_3\left(x^2+c\right) &= b_1\left(x^2+c\right) + b_3\left(x^2+c\right)^3 \\ &= b_1x^2 + b_1c + b_3x^6 + 3b_3cx^4 + 3b_3c^2x^2 + b_3c^3. \end{aligned}$$

By equating coefficients of like powers, we obtain $b_3 = 1, b_1 = \left(\frac{3}{2}\right)c$

$$b_1^2 = 3b_3c^2 + b_1 \Rightarrow c(c+2) = 0$$

and

$$c = b_1c + b_3c^3, \quad 2c^3 + 3c^2 - 2c = 0 \Rightarrow c(2+c)(2c-1) = 0.$$

Therefore the only possible values of $c$ are -2 and 0. If $c = 0$, then $q_2(x) = x^2$ and, according to Theorem 4.11, $q_j(x) = x^j$ for $j = 1, 2, \ldots$, and $\{p_j\}$ is similar to $\{x^j\}$. If $c = -2$ consider the chain $\{\mu^{-1} \cdot q_j \cdot \mu\}$, where $\mu(x) = 2x$,

$$\begin{aligned} \mu^{-1}(x) &= x/2 \\ q_2 \cdot \mu &= (2x)^2 - 2 \\ &= 4x^2 - 2 \\ \mu^{-1} \cdot q_2 \cdot \mu &= 2x^2 - 1. \end{aligned}$$

Since

$$\left(\mu^{-1} \cdot q_2 \cdot \mu\right) = T_2,$$

Theorem 4.10 informs us that

$$\mu^{-1} \cdot q_j \cdot \mu = T_j, \quad j = 1, 2, \ldots$$

Thus $\{p_j\}$ is similar to $\{T_j\}$ via the linear transformation $\lambda \cdot \mu$. □

The proof of the above theorems is in the literature Chebyshev polynomials From Approximation Theory to Algebra and Number Theory by THEODORE J. RIVLIN [24].

The pure monomial $x^n$ and the Chebyshev polynomials are the only classes of polynomials that satisfy the commutative composition (4.5). This commutative property enables us to construct public-key cryptosystems based on Chebyshev polynomials.

**Lemma 4.14.** *Suppose that $\lambda(x) = ax + b$, $a \neq 0$, so that $\lambda^{-1}(x) = (x - b)/a$. If P and Q commute, then $\lambda^{-1} \circ P \circ \lambda$ and $\lambda^{-1} \circ Q \circ \lambda$ also commute.*

*Proof.* $PQ = QP$ and $\lambda = ax + b$ a non - constant polynomial.
Let $f = \lambda^{-1} \circ P \circ \lambda$ and $g = \lambda^{-1} \circ Q \circ \lambda \quad \Longrightarrow f(x) = \lambda^{-1}(P(\lambda(x))) \quad g(x) = \lambda^{-1}(Q(\lambda(x)))$
$fg(x) = f(g(x)) = \lambda^{-1}(P(\lambda(\lambda^{-1}(Q(\lambda(x))))))$
$gf(x) = g(f(x)) = \lambda^{-1}(Q(\lambda(\lambda^{-1}(P(\lambda(x))))))$
Since $P$ and $Q$ commute, then $P(\lambda(x))$ and $Q(\lambda(x))$ commute
Therefore, $\lambda^{-1}(P(\lambda(x)))$ and $\lambda^{-1}(Q(\lambda(x)))$ also commute. Hence $f$ and $g$ commute. □

## 4.3 Chebyshev polynomials over the Finite field

A public key cryptosystem based on Chebyshev polynomials has been proposed by [25] and we will be presenting it in this study shortly. The cryptosystem was broken shortly after its implementation. The attack was based on the fact that rounding numbers could lead to multiple representations of the same number [8]. To avoid such an attack, Chebyshev polynomials were extended from the real number fields to finite fields [14]. In this section, we explain why there is a need to implement the cryptosystem on a finite field over floating-point numbers.

First, chaos-based cryptosystems are defined over real numbers, however, due to the finite representation of real numbers in a computer and the finite precision of operations, it makes it insecure to implement a secure cryptosystem. Floating-point numbers are approximate and have limited precision due to the finite number of bits used to store them. Taking any interval of real numbers, for example, $[-1, 1]$, and mapping it to a range of floating-point numbers, not all the possible values of the floating-point numbers in that range will be equally likely to be generated or represented.

Second, due to the finite precision of floating-point arithmetic, there may be multiple representations of the same number. This means that there are multiple combinations of significands and exponents that can represent the same number, leading to redundant number representations. For example, the numbers 0.1 and 0.10000000000000001 are equivalent, but they have different representations in floating-point arithmetic. This redundancy in number representations can lead to potential issues in numerical computations, particularly when comparing or rounding numbers which in turn affects the commutative property of the Chebyshev polynomials. When comparing two floating-point numbers, it is important to take into account the potential for redundant representations and use appropriate tolerance levels to account for the potential differences between equivalent representations.

Third, it is important to note that Chebyshev polynomials are not invertible in the traditional sense, meaning that it is not possible to recover the original message from the encrypted message without additional information. This non-invertibility of Chebyshev polynomials, combined with their implementation in floating-point arithmetic, can impose a restriction on the length of the message that can be encrypted using this technique. Specifically, as the length of the message increases, the errors introduced by the floating-point arithmetic can accumulate and become significant, potentially leading to decryption errors or security vulnerabilities. In this case, messages are broken into small blocks that can be encrypted and decrypted separately to ensure that the length of the message does not exceed the maximum length that can be securely encrypted using the Chebyshev polynomials-based encryption scheme.

Lastly, chaotic maps are mathematical systems that are difficult to understand and analyze when implemented using floating-point numbers in computers. The lack of analytical tools for understanding the periodic structure of the periodic orbits in these implementations is the most important reason for this difficulty [14]. Using integers instead of floating-point numbers may provide a possible solution to this problem. This is because a link between number theory and chaos theory has been exploited to understand the structure of the orbits. An example is toral automorphisms, which are a type of chaotic map that can be studied using number theory techniques, as evidence for this possibility.

### Limitation of algorithm based on over real number field

Kocarev and Tasev [25], described public key encryption on Chebyshev polynomials using its recursive relations over real numbers. The algorithm is presented as follows [26]:

**Setup:** Alice picks a large integer $s$ and a random number $x \in [-1,1]$. Her public key is $(x, T_s(x))$ and the secret key is $s$.
**Encryption:** Bob represents the message $M \in [-1,1]$ and pick a large integer $r$ to compute the ciphertext $(c_1, c_2) = (T_r(x), M \cdot T_r(T_s(x)))$.
**Decryption:** Alice recover the plaintext by computing $M = c_2/T_s(c_1)$. This really decryptes ciphertext because $T_s(c_1) = T_r(T_s(x)) = T_s(T_r(x))$.

The algorithm described above is innovative and claimed to be efficient and secure by the author, but in [8] an attack that enables one to recover the corresponding plaintext from a given ciphertext is studied. The result is based on the fact that several Chebyshev polynomials pass through the same point.

**Description of attack:** Given Alice's public key $(x, T_s(x))$ and the ciphertext $(T_r(x), X)$, an adversary can recover $M$ by computing an $r'$ such that $T_{r'}(x) = T_r(x)$. He then evaluates $T_{r's}(x) = T_{r'}\left(T_s(x)\right)$ and recovers $M$ by computing $M = \frac{X}{T_{r',}(x)}$. The attack is always successful because, if $r'$ is such that $T_{r'}(x) = T_r(x)$, then:

$$\begin{aligned} T_{r\cdot s}(x) &= T_{s\cdot r}(x) \\ &= T_s\left(T_r(x)\right) = T_s\left(T_{r'}(x)\right) \\ &= T_{s\cdot r'}(x) = T_{r'\cdot s}(x) \\ &= T_{r'}\left(T_s(x)\right). \end{aligned}$$

To show that such an $r'$ can be computed, let $\mathcal{N}$ be the set of natural numbers and let $\mathcal{Z}$ be the set of integers. Let

$$\mathcal{P} = \left\{ \frac{\pm \arccos\left(T_r(x)\right) + 2k\pi}{\arccos(x)} \quad | \quad k \in \mathcal{Z} \right\},$$

such that $r' \in \mathcal{P} \cap \mathcal{N}$. They showed that $\mathcal{P}$ contains all possible integers $r'$ such that the polynomials $T_{r'}(x)$ passing through $T_r(x)$ by proving that for each pair $(x, T_r(x))$, the integer $r'$ satisfies $T_{r'}(x) = T_r(x)$ if and only if $r' \in \mathcal{P} \cap \mathcal{N}$.

Moreover, the above algorithm has a significant flaw that makes it impractical to use. The algorithm relies on the semi-group property, which is always true for Chebyshev maps in theory. However, there are two important factors to consider. Firstly, Chebyshev maps are defined over real numbers and are sensitive to initial conditions. Secondly, computers can only perform approximate computations rather than precise ones. Hence equality does not strictly hold.

**Example 4.15** (Chaotic computation [27]). Consider the Chebyshev map with parameters $r = 68$, $s = 96$ and $x = 0.39$. Then $T_r(x) = -0.513634$, $T_s(x) = 0.723788$, $T_r(T_s(x)) = 0.0528869$, $T_s(T_r(x)) = 0.0524104$, $T_{rs}(x) = 0.0523997$. Hence , $T_r(T_s(x)) \neq T_{rs}(x) \neq T_s(T_r(x))$. This contradicts the expected outcome based on the theory on which this algorithm is built. Although it is possible to remove this error, it requires a significant amount of time and memory resources.

## 4.4 Extended Chebyshev polynomials

The semi-group property is very useful to construct a public key cryptosystem based on Chebyshev polynomials. We have shown that when $x \in [-1,1]$, not all members can compute the same keys, and the explicit expression $T_n(x)$ has a security loophole. To resist this attack on the cryptosystem, Kocarev et al extended the definition of $T_n(x)$ to the finite field and improved the public key cryptosystem [28].

The extended Chebyshev polynomials $T_n(x)$ is defined as a map $T_n : \{0, 1, \cdots, N-1\} \to \{0, 1, \cdots, N-1\}$ with

$$\begin{aligned} T_0(x) &= 1 \mod N \\ T_1(x) &= x \mod N \\ T_{n+1}(x) &= 2xT_n(x) - T_{n-1}(x) \mod N \end{aligned}$$

where $x \in \{0, 1, 2, \cdots, N-1\}$ and $N$ is a large prime.

### Mathematical Hard problems on Chebyshev polynomials

The extended algorithm has its security grounds on the hard discrete algorithm problem. We introduce some basic mathematical hard problems which form key points to prove the security of this cryptosystem [28].

1. Chebyshev discrete logarithm problem: Given the element $(x, y)$, find the integer $s$ , such that $T_s(x) = y$.
2. Chebyshev Diffie-Hellman problem: Given the element $(x, T_r(x), T_s(x))$, find $T_{rs}(x)$.

Both of the above problems are assumed to be computationally unfeasible and can serve as assumptions for demonstrating the security of the public key cryptosystem based on Chebyshev polynomials.

### Software Implementation

In this section, we seek to generalize the Chebyshev form of the square and multiply algorithm which makes the computation of exponentials in a finite group computationally feasible. This procedure will help us to quickly compute values of the Chebyshev polynomials modulo $N$, for large numbers $n$ and $N$. The Chebyshev polynomials in the recurrence relation is $T_{n+1} = 2xT_n(x) - T_{n-1}$, which can be rewritten as a matrix equation as :

$$\begin{bmatrix} T_n \\ T_{n+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2x \end{bmatrix} \begin{bmatrix} T_{n-1} \\ T_n \end{bmatrix} = A \begin{bmatrix} T_{n-1} \\ T_n \end{bmatrix} \tag{4.15}$$

where

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 2x \end{bmatrix}.$$

From $T_n = 2xT_{n-1}(x) - T_{n-2}$ we get the matrix equation:

$$\begin{bmatrix} T_{n-1} \\ T_n \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2x \end{bmatrix} \begin{bmatrix} T_{n-2} \\ T_{n-1} \end{bmatrix} = A \begin{bmatrix} T_{n-2} \\ T_{n-1} \end{bmatrix}. \tag{4.16}$$

Combining the matrix equations (4.16) and (4.15) yields

$$\begin{bmatrix} T_n \\ T_{n+1} \end{bmatrix} = A^2 \begin{bmatrix} T_{n-2} \\ T_{n-1} \end{bmatrix}.$$

We continue to rewrite the vector on the right side until they are in terms of $T_0$ and $T_1$. Following from the above, it can be deduced that

$$\begin{bmatrix} T_n \\ T_{n+1} \end{bmatrix} = A^n \begin{bmatrix} T_0 \\ T_1 \end{bmatrix} \tag{4.17}$$

where

$$T_0(x) = 1 \text{ and } T_1(x) = x.$$

To calculate for $T_n(x) \mod N$ we need to find $A^n$ (matrix exponentiation) which can be done effectively by the square and multiply algorithm.

### Properties of extended Chebyshev polynomials

We established the fact that up to a linear transformation, the pure monomial $x^n$ and the Chebyshev polynomials are the only classes of polynomials that satisfy the commutative composition (4.5). The extended Chebyshev polynomials can replace the monomial $x^n$ in RSA and ElGaml algorithm if it satisfies the commutative property and we can find the period of their orbits.

**Property 4.16** (Semi-group property)**.** The extended Chebyshev map satisfies the semi-group property:

$$T_r\,(T_s(x) \bmod N) \bmod N = T_{rs}(x) \bmod N. \tag{4.18}$$

*Proof.* By congruence relation $T_q(x) \equiv \cosh(p\cosh^{-1}(x)) \mod N \quad \text{for } x > 1$
$T_p(x) = 2xT_{p-1}(x) - T_{p-2}(x) \quad \text{with} \quad T_0(x) = 1 \quad \text{and} \quad T_1(x) = x.$

$$T_p(T_q(x)(\mathrm{mod} N))(\mathrm{mod} N) = \quad 2(T_q(x) \bmod N)T_{p-1}(T_q(x) \bmod N) - T_{p-2}(T_q(x) \bmod N). \tag{4.19}$$

Substitute $T_q(x) \equiv \cosh(q\cosh^{-1}(x)) \mod N$ into equation (4.19) and the using the identity $\cosh^{-1}(\cosh x) = x$, then the right-hand side of the equation becomes:

$$\begin{aligned} &= 2(\cosh(q\cosh^{-1}(x)))T_{p-1}(\cosh(q\cosh^{-1}(x))) - T_{p-2}(\cosh(q\cosh^{-1}(x))) \\ &= 2(\cosh(q\cosh^{-1}(x))) \cdot \cosh((p-1)\cosh^{-1}(\cosh(q\cosh^{-1}(x)))) \bmod N \end{aligned}$$

$$
\begin{aligned}
&- \cosh((p-2)\cosh^{-1}(\cosh(q\cosh^{-1}(x)))) \bmod N \\
&= 2(\cosh(q\cosh^{-1}(x))) \cdot \cosh(q(p-1)\cosh^{-1}(x)) \bmod N - \cosh(q(p-2)\cosh^{-1}(x)) \bmod N
\end{aligned}
$$

but $2\cosh(\alpha)\cosh(\beta) = \cosh(\alpha+\beta) + \cosh(\alpha-\beta)$ and $\cosh(\alpha) = \cosh(-\alpha)$, where

$$\alpha = q\cosh^{-1}(x) \text{ and } \beta = q(p-1)\cosh^{-1}(x)$$

$$
\begin{aligned}
&= \cosh(q\cosh^{-1}(x)[1+p-1]) \bmod N + \cosh(q\cosh^{-1}(x)[1-p+1]) \bmod N \\
&- \cosh(q(p-2)\cosh^{-1}(x)) \bmod N \\
&= \cosh(pq\cosh^{-1}(x)) \bmod N + \cosh(q(2-p)\cosh^{-1}(x)) \bmod N - \cosh(q(p-2)\cosh^{-1}(x)) \bmod N \\
&= \cosh(pq\cosh^{-1}(x)) \bmod N \\
&= T_{pq}(x) \bmod N.
\end{aligned}
$$

□

**Example 4.17** ([27]). Let $x = 13, N = 41, r = 4, s = 5$, by computation $T_4(13) = 38, T_5(13) = 29, T_{20}(13) = 40$ and $T_5(38) = 40, T_4(29) = 40$. It can be observed that, $T_4(T_5(13)) = T_5(T_4(13)) = T_{20}(13)$.

**Property 4.18** (Periodicity of extended Chebyshev map). The extended Chebyshev map does not have chaotic properties, instead, it is periodic. This is due to the fact that we changed the domain from real numbers to a finite field. The periodicity of the extended Chebyshev map refers to the property that the values of the function repeat themselves after a certain period of time $\tau_x$. The polynomial $T_n(x)$ is periodic with period $\tau = \tau_x$ if for $x$ we have

$$T_{n+k\tau}(x) = T_n(x) \tag{4.20}$$

where $k = \{1, 2, 3, \ldots\}$. Thus, the smallest positive value of $\tau$ for which equation (4.20) holds is called the period of the map $T_n(x) \mod N$.

**Example 4.19.** Let $N = 7$. When $x = 2$, the sequence $T_n(2) \mod 7$ for $n = 0, 1, 2, \ldots$ is :

$$1, 2, 0, 5, 6, 5, 0, 2, 1, 2, 0, 5, 6, 5, 0, 2, \ldots \quad .$$

Indeed for $x = 2$, we have:

$$
\begin{aligned}
&T_0(x) = 1 \quad T_1(x) = 2 \quad T_2(x) = 0 \quad T_3(x) = 5 \quad T_4(x) = 6 \\
&T_5(x) = 5 \quad T_6(x) = 0 \quad T_7(x) = 2 \quad T_8(x) = 1 \quad \cdots .
\end{aligned}
$$

The periodicity of the sequence $T_n(2)$ is 8. Below is the sequence $T_n(x)$ for each $x = 0, 1, 2, \ldots, 6$:

**Table 4.1:** Periods of the sequence $\{T_n(x) \pmod 7\}$

| $x$ | Sequence | Period |
|---|---|---|
| 0 | $1, 0, 6, 0, 1, 0, 6, 0, \ldots$ | 4 |
| 1 | $1, 1, 1, 1, \ldots$ | 1 |
| 2 | $1, 2, 0, 5, 6, 5, 0, 2, 1, 2, 0, 5, 6, 5, 0, 2, \ldots$ | 8 |
| 3 | $1, 3, 3, 1, 3, 3, \ldots,$ | 3 |
| 4 | $1, 4, 3, 6, 3, 4, 1, 4, 3, 6, 3, 4, \ldots$ | 6 |
| 5 | $1, 5, 0, 2, 6, 2, 0, 5, 1, 5, 0, 2, 6, 2, 0, 5, \ldots$ | 8 |
| 6 | $1, 6, 1, 6, 1, 6, \ldots$ | 2 |

**Example 4.20.** For $N = 11, \quad x = 0, 1, 2, \ldots, 10, \quad n = 0, 1, 2, \ldots.$

**Table 4.2:** Periods of the sequence $\{T_n(x) \pmod{11}\}$

| $x$ | Sequence | Period |
|---|---|---|
| 0 | $1, 0, 10, 0, 1, 0, 10, 0, 1, 0, 10, 0, \ldots$ | 4 |
| 1 | $1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, \ldots$ | 1 |
| 2 | $1, 2, 7, 4, 9, 10, 9, 4, 7, 2, 1, 2, \ldots$ | 10 |
| 3 | $1, 3, 6, 0, 5, 8, 10, 8, 5, 0, 6, 3, \ldots$ | 12 |
| 4 | $1, 4, 9, 2, 7, 10, 7, 2, 9, 4, 1, 4, \ldots$ | 10 |
| 5 | $1, 5, 5, 1, 5, 5, 1, 5, 5, 1, 5, 5, \ldots$ | 3 |
| 6 | $1, 6, 5, 10, 5, 6, 1, 6, 5, 10, 5, 6, \ldots$ | 6 |
| 7 | $1, 7, 9, 9, 7, 1, 7, 9, 9, 7, 1, 7, \ldots$ | 5 |
| 8 | $1, 8, 6, 0, 5, 3, 10, 3, 5, 0, 6, 8, \ldots$ | 12 |
| 9 | $1, 9, 7, 7, 9, 1, 9, 7, 7, 9, 1, 9, \ldots$ | 5 |
| 10 | $1, 10, 1, 10, 1, 10, 1, 10, 1, 10, 1, 10, \ldots$ | 2 |

The period of the sequence $\{T_n(x) \pmod N\}$ is at most $N + 1$ for any given input argument $x = 0, 1, 2, \ldots, N - 1$. Generally, the periodicity satisfies the theorem below.

**Theorem 4.21.** *Let $N$ be an odd prime and $x \in \mathbb{Z}$ such that $0 \le x \le N$. Let $\tau$ be the period of the sequence $T_n(x) \mod N$ for $n = 0, 1, 2, \ldots$ then $\tau$ is a divisor of $N^2 - 1$.*

*Proof.* We will prove the theorem by showing that if we let $M = \begin{bmatrix} 0 & 1 \\ -1 & 2x \end{bmatrix}$, with $\lambda = q_1, q_2$ as the roots of the characteristic polynomial $\lambda^2 - 2x\lambda + 1$, then :

(i) $\tau | N - 1$ if the roots are in $\mathrm{GF}(N)$, otherwise
(ii) $\tau | N + 1$ if the roots are in $\mathrm{GF}(N^2)$.

From the generalized Chebyshev form of the square and multiply algorithm for software implementation, it is shown that we can compute $T_n(x) \pmod N$ by computing the nth power of the recurrence relation matrix $M$, which is a 2 - automorphism, with characteristics polynomial $f(\lambda) = \lambda^2 - 2x\lambda + 1$. The matrix is non-singular with a determinant of 1. The identity matrix is the 0th power of the matrix $M$, hence if $\tau$ is the period of the matrix $M$ then $\tau$ is the smallest positive integer such that the $\tau$th power of the matrix is the identity matrix. One way of computing matrix exponentiation is by finding its Jordan normal form which is either a diagonal matrix with distinct eigenvalues on the diagonals or an upper triangular matrix with repeated eigenvalues on the diagonal. These eigenvalues form the roots of the characteristics polynomials [29].

If the characteristic polynomial has repeated roots, then the discriminant is zero. Hence

$$\begin{aligned} 4x^2 - 4 &= 0 \pmod N \\ x^2 - 1 &= 0 \pmod N \\ x &= \pm 1 \pmod N. \end{aligned}$$

If $x = 1$ , then $T_{n+1}(x) = 2T_n(x) - T_{n-1}(x)$, $T_0 = 1$, $T_1 = 1$, $T_2(x) = 1$ and $T_3(x) = 1$. Hence the sequence is $1, 1, 1, 1, \ldots$ with a period 1.
If $x = -1$ , then $T_{n+1}(x) = -2T_n(x) - T_{n-1}(x)$, $T_0 = 1$, hence

$$\begin{aligned} T_1(x) &= -1 \pmod N = N - 1 \\ T_2(x) &= -2(N-1) - 1 \pmod N = 1 - 2N \pmod N = 1 \\ T_3(x) &= -2(1) - (N-1) \pmod N = -1 - N \pmod N = N - 1. \end{aligned}$$

Hence the sequence is $1, N-1, 1, N-1, \ldots$ with a period 2 which divides $N - 1$ because from the theorem $N$ is odd so $N - 1$ is even.

If the characteristic polynomial has distinct roots in GF(N), we will apply Fermat's little theorem $a^{(N-1)} = 1 \pmod N$ for any non-zero $a$, in the matrix equation $M^{(N-1)} = 1 \pmod N$ where 1 is the identity matrix. From the matrix equation, the $(N-1)$th power of the matrix in the Jordan normal form gives the identity matrix, hence the sequence has period $N - 1$. From the Lagrange theorem for order of a subgroup, if we can find a smaller exponent $\tau < N - 1$ such that the $\tau$th power of matrix $M$ in Jordan normal form gives the identity matrix then $\tau$ divides $N - 1$.

It is also possible that the roots exist only in a quadratic extension of GF(N). It may not be possible to find a complete set of eigenvalues in GF(N), however, if we extend the field to a larger field such as complex numbers, then we can guarantee the existence of a complete set of eigenvectors. This implies that in the quadratic extension field, we extend GF(N) by adding a square root of a non-square element. We can now find a complete set of eigenvectors for our matrix and use them to diagonalize the matrix. However, all arithmetic needs to be done in the quadratic extension field. We then raise the matrix in the Jordan normal form to the power $N$, which is known as the $N$th power map, and it is an automorphism in the quadratic extension field. This is a consequence of Fermat's Little Theorem, which states that for any prime $N$ and any element $a$ in the field, $a^N = a \bmod N$. In other words, raising an element in the field to the power $N$ yields the same result as raising it to the first power. Now, suppose we have a matrix $M$ in Jordan normal form with diagonal entries $\sigma$ and $\mu$. Since $\sigma$ and $\mu$ are elements in GF($N^2$), we can raise them to the power $N$ using the $N$th power map. It follows that:

$$\begin{aligned} \sigma^p &= \sigma \pmod{p}, \\ \mu^p &= \mu \pmod{p}. \end{aligned}$$

Therefore, the matrix $M^N$, which is the diagonal matrix with entries $\sigma^N$ and $\mu^N$, is obtained by applying the $N$th power map to the diagonal entries of $M$. Since the $N$th power map is an automorphism of the quadratic extension field, the resulting matrix $M^N$ is still in the Jordan canonical form. The quadratic extension field has only one conjugate automorphism, which maps the square root of the non-square element to its negative. Therefore, applying this automorphism to the diagonal entries of $M$ will swap the two roots of the characteristic polynomial, but leave the matrix otherwise unchanged. Hence, there is a positional swap of the roots of the quadratic polynomial on the diagonal, as we have conjugate automorphism in a quadratic extension field. We then find $(N+1)$st power by multiplying the original Jordan normal form to the matrix $M$ to power $N$. The $(N+1)$st power multiplies two pairs of conjugate roots, and from our characteristics polynomial the product of the conjugate roots is the coefficient of $\lambda^0$, which is 1. Hence the $(N+1)$st power is the identity matrix and the period is at most $N+1$. From the Lagrange theorem for order of a subgroup, if we can find a smaller exponent $\tau < N+1$ such that the $\tau$th power of matrix $M$ in Jordan normal form gives the identity matrix then $\tau$ divides $N+1$. □

For maximum security, $N$ should be a prime number such that $2N+1$ is also prime and $x$ should be chosen such that the period is large.

# 5 Cryptosystem on Extended Chebyshev polynomials

From section 4 we have shown that the extended Chebyshev polynomials can replace the monomial $x^n$ because it satisfies the semi-group property and the periodicity property. In this section, we will construct an ElGamal-like and RSA-like algorithm based on the extended Chebyshev polynomials. We will present the Diffie-Hellman key agreement algorithm using the extended Chebyshev polynomials, the ElGamal-like and RSA-like public key encryption, we will also show why the Decryption algorithm works in RSA-like and ElGamal-like, and then prove that the security of the ElGamal-like algorithm is still based on the discrete logarithm problem.

## 5.1 The Chebyshev polynomials ElGamal-like Algorithm

ElGamal public key cryptosystem consists of an algorithm for key generation and an algorithm for encryption. Its security is based on the intractability of the discrete logarithm and Diffie - Hellman problem [16, 20, 17]. The basic ElGamal and generalized ElGamal encryption schemes are described in section 2 and in [16, 20, 17]. In this section, the ElGamal encryption scheme is generalized for Chebyshev polynomials.

### ElGamal-like (based on Chebyshev polynomials) key generation

In the key generation mode, the scheme can be viewed as a Diffie-Hellman key agreement. In the key generation Alice and Bob should do the following:

1. Alice generates a positive integers $x$ and a large random prime $N$ such that $x < N$.
2. Alice generates a secret integer $s$ such that $0 < s < N$.
3. Alice computes $A = T_s(x) \bmod N$.
4. Alice's public key is $(x, N, A)$, and private key is $s$.
5. Bob generates a secret integer degree $r$ such that $0 < r < N$.
6. Bob computes $B = T_r(x) \bmod N$.
7. Bob sends $B$ to Alice.
8. Alice computes the secret key $k = T_s(B) \bmod N$.
9. Bob computes the secret key $k = T_r(A) \bmod N$.

The common secret key is $k$ as both Alice and Bod have computed $T_{rs}(x) \bmod N$.

**Example 5.1** ([29]). Below is a simple example of the Diffie-Hellman key exchange algorithm based on the extended Chebyshev polynomials in which $m = 2$ and $n = 3$ are chosen hence we need to evaluate the polynomials $T_2(x) = 2x^2-1$, $T_3(x) = 4x^3-3x$, and $T_6(x) = 32x^6-48x^4+18x^2-1$.

1. Alice generates $N = 89$ and $x = 7$.
2. Alice generates $s = 2$.
3. Alice computes $A = T_2(7) = 2\left(7^2\right) - 1 \bmod 89 = 97 \bmod 89 = 8$.
4. Alice sends $N = 89, x = 7$, and $A = 8$ to Bob.
5. Bob generates $r = 3$.

6. Bob computes $B = T_3(7) = 4\left(7^3\right) - 3(7) \bmod 89 = 1351 \bmod 89 = 16$.
7. Bob sends $B = 16$ to Alice.
8. Alice computes $k = T_2(16) = 2\left(16^2\right) - 1 \bmod 89 = 511 \bmod 89 = 66$.
9. Bob computes $k = T_3(8) = 4\left(8^3\right) - 3(8) \bmod 89 = 2024 \bmod 89 = 66$.

Both Alice and Bob have generated the same secret key $k = 66$, which is also $T_6(7) \bmod 89 = 3650401 \bmod 89 = 66$.

### ElGamal-like (based on Chebyshev polynomials) public-key encryption

Public key encryption consists of encryption and decryption algorithms. Bob obtains Alice's public key components, represents the message as an integer, and encrypts the message. He sends the ciphertext to Alice. Alice then uses her private key to decrypt the ciphertext to obtain the original message. To encrypt the message $m$, Bob should do the following:

1. Obtains Alice's authentic public key $(x, N, A)$.
2. Represent the message as an integer $m \bmod N$.
3. Generates a random integer $r < N$ , computes $B = T_r(x) \bmod N$ and $X = mT_r(A) \bmod N$
4. Sends the cipher-text $c = (B, X)$ to Alice.

For Alice to decrypt the cipher-text $c$ to recover the message $m$, she should do the following:

1. Use her private key $s$ to compute $C = T_s(B) \bmod N$.
2. Recover $m$ by computing $m = XC^{-1} \bmod N$.

The decryption process in the ElGamal public key algorithm works because of the properties of modular arithmetic and from the semi-group property (4.4). It follows from the fact that

$$T_s(B) = T_s(T_r(x)) = T_r(T_s(x)) = T_r(A).$$

Computing $C$, is possible because of the properties of modular arithmetic. Specifically, The correctness of the decryption process relies on the fact that $C$ is equal to $T_s(T_r(x)) \bmod N$, which can be computed efficiently. This is essentially the same as computing the shared secret in the Diffie-Hellman key exchange protocol. Computing $m$, works because of the properties of the modular inverse. Since $T_n(x)$ is a self-mapping, it has a modular inverse $C^{-1}$ in the same group. This means that we can compute $m$ by multiplying $X$ with the inverse of $C$, and then taking the result modulo $N$. In the next section, we will discuss the correctness of the ElGamal algorithm which relies on the difficulty of computing discrete logarithms in the field. Without knowledge of the private key $s$, an attacker cannot compute $C$ or recover the plaintext $m$ from the ciphertext $(B, X)$.

## 5.2 The Chebyshev polynomials RSA-like Algorithm

The RSA-like cryptosystem security is built on the difficulty of factoring big integers . The RSA-like algorithm involves the use of two large prime numbers, $p$ and $q$, to generate public and private keys for encrypting and decrypting data. In general, the encryption is more secure the bigger the key size. The most well-known algorithms for factoring huge numbers require exponential time, so the longer it takes to decrypt data, the bigger the key size. However, if the prime variables $p$ and $q$ are discovered, RSA's security may be jeopardized. In this section, we will discuss the critical components of the RSA-like algorithm. The RSA-like public key cryptosystem consists of an algorithm for key generation and an algorithm for encryption. We replace Euler's $\varphi(N) = (p-1)(q-1)$ by $\Psi(N) = (p^2-1)(q^2-1)$, according to theorem 4.21.

### RSA-like (based on Chebyshev polynomials) key generation

For the RSA-like key generation process, Alice should do the following:

1. Generate two distinct prime numbers $p$ and $q$, each roughly the same size.
2. Compute $N = pq$ and $\Psi(N) = (p^2-1)(q^2-1)$.
3. Select a random integer $e, 1 < e < \Psi(N)$ such that $\gcd(e, \Psi(N)) = 1$.
4. Compute the unique integer $d, 1 < d < \Psi(N)$ such that $ed \equiv 1 \bmod \Psi(N)$.
5. Alice's public key is $(N, e)$ and private key is $d$.

### RSA-like (based on Chebyshev polynomials) public-key encryption

The RSA public key encryption consists of encryption and decryption algorithms. Bob obtains Alice's public key components, represents the message as an integer, and encrypts the message. He sends the ciphertext to Alice. Alice then uses her private key to decrypt the ciphertext to obtain the original message. To encrypt the message $m$, Bob should do the following:

1. Obtains Alice's authentic public key $(N, e)$.
2. Represent the message as an integer $m \bmod N$.
3. Computes $c = T_e(m) \bmod N$ .
4. Sends the ciphertext $c$ to Alice.

For Alice to decrypt the ciphertext $c$ to recover the message $m$, she should use her private key $d$ to compute $m = T_d(c) \bmod N$. The decryption recovers the original message $m$ because if $p$ is an odd prime number and $0 \leq x < p$, then the period of the sequence $T_n(x) \bmod p, n = 0, 1, 2, \ldots$ is a divisor of $p^2 - 1$. We now show that if a ciphertext can be decrypted modulo each of the primes $p$ and $q$ then the message can be recovered modulo $N$ by the Chinese remainder theorem. Since $ed \equiv 1 \bmod \Psi(N)$, there exist an integer $k$ such that $ed = 1 + k\Psi(N)$. Hence for modulo $p$,

$$T_d(c) = T_d(T_e(m)) = T_{ed}(m) = T_{1+k\Psi(N)}(m) = T_{1+k(p^2-1)(q^2-1)}(m).$$

Since the period is a divisor of $p^2 - 1$ and $k(q^2-1) \in \mathbb{Z}$ then from the definition of period of a sequence

$$T_{1+k(p^2-1)(q^2-1)}(m) = T_1(m) \equiv m \bmod p.$$

From the same argument for modulo $q$,

$$T_d(c) = T_d(T_e(m)) = T_{ed}(m) = T_{1+k\Psi(N)}(m) = T_{1+k(p^2-1)(q^2-1)}(m) = T_1(m) \equiv m \bmod q.$$

From the two equations, we have two systems of congruence equations

$$\begin{cases} T_1(m) \equiv m & \bmod p \\ T_1(m) \equiv m & \bmod q \end{cases} = \begin{cases} m \equiv T_1(m) & \bmod p, \\ m \equiv T_1(m) & \bmod q. \end{cases}$$

Finally, since $p$ and $q$ are distinct primes, it follows from the Chinese remainder theorem that there exists one solution

$$T_d(c) \equiv T_d(T_e(m)) \equiv T_{ed}(m) \equiv T_{1+k\Psi(N)}(m) \equiv T_1(m) \equiv m \bmod N.$$

## 5.3 Security of cryptosystem based on Chebyshev polynomials

In this section, we will show that an attacker will not compromise the security of the cryptosystems RSA-like and ElGamal-like algorithms based on the extended Chebyshev. We will show that for ElGamal-like public key algorithm if an attacker knows $N, x, A, B$ but not the secret degrees $s$and $r$, the ElGamal-like algorithm can be broken by solving $A = T_s(X) \pmod N$ which is a hard Chebyshev discrete logarithm problem.

**Theorem 5.2.** *Let $x$ and $y$ be integers such that $x > 1$ and $N$ a prime. If $y = T_n(x) \bmod N$, then $n = \log_{x+\sqrt{x^2-1}} y + \sqrt{y^2-1}$.*

*Proof.* If $x > 1$ the Chebyshev polynomials can be defined as the unique polynomial satisfying

$$T_n(x) = \cosh(n \cosh^{-1}(x))$$

then, $y = \cosh(n \cosh^{-1}(x))$ and $\cosh(t) = \frac{e^t+e^{-t}}{2}$. This implies that,

$$2y = e^{n\cosh^{-1}(x)} + e^{-n\cosh^{-1}(x)} \tag{5.1}$$

but $\cosh^{-1}(x) = \ln(x + \sqrt{x^2-1})$ for $x > 1$.
Let

$$z = e^{\cosh^{-1}(x)} = e^{\ln(x+\sqrt{x^2-1})} = (x + \sqrt{x^2-1}).$$

Now we substitute $z$ into equation (5.1) and solve for $z^n$

$$\begin{aligned} z^n + z^{-n} &= 2y \\ z^{2n} + 1 &= 2yz^n \\ z^{2n} - 2yz^n + 1 &= 0. \end{aligned}$$

Finding the roots of the quadratic equation in terms of $z^n$ yields

$$\begin{aligned} z^n &= \frac{2y + \sqrt{4y^2 - 4}}{2} \\ z^n &= y + \sqrt{y^2 - 1}. \end{aligned}$$

From the logarithm definition

$$\begin{aligned} n &= \log_z(y + \sqrt{y^2 - 1}) \\ n &= \log_{x+\sqrt{x^2-1}}(y + \sqrt{y^2 - 1}). \end{aligned}$$

□

If the two square roots $\sqrt{x^2 - 1}$ and $\sqrt{y^2 - 1}$ can be found in the field $GF(N)$, then the discrete logarithm problem is a standard one. Otherwise, if at least one square root cannot be found, then a quadratic extension field $GF(N^2)$ is used, leading to a more generalized version of the discrete logarithm problem. Hence the modified ElGamal algorithm is secure.

In the RSA-like algorithm, if an attacker knows only the public key $(N, e)$ such that $N = pq$ and $\gcd(e, (p^2 - 1)(q^2 - 1)) = 1$, the plaintext $m$ can be recovered from the corresponding $c$ by finding an integer $m$ such that $T_e(m) \equiv c(\text{mod} N)$. This problem is a hard Chebyshev RSA-like problem and can be reduced to a factor problem. Let's assume we have an algorithm $\mathcal{A}$ which can factorize $N = pq$ then we can compute $\Psi(N) = (p^2 - 1)(q^2 - 1)$. From $e$ and $\Psi(N)$ we can compute $d \equiv e^{-1} \bmod \Psi(N)$ since $\gcd(e, \Psi(N)) = 1$. Once $d$ is obtained, the attacker can decrypt any ciphertext $c$ intended for Alice. Hence solving the factoring problem implies solving the hard Chebyshev RSA-like problem. The security of the RSA-like algorithm is therefore based on the intractability of the integer factorization problem, similar to what happens with classical RSA.

# 6 Conclusion

In this study, we discuss two public key encryption schemes based on Chebyshev polynomials, which are a type of polynomials that behave like the pure monomial $x^n$ which satisfies the semi-group property. We showed that the RSA and ElGamal algorithms are secure and practical for encryption. We also extended the Chebyshev polynomials over a finite field and demonstrated that the new ElGamal-like and RSA-like algorithms are as secure as the original ElGamal and RSA algorithms. Therefore, in this study, we conclude that Chebyshev polynomials can be used for secure communication over an insecure network.

# References

[1] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory,vol. 22, pp. 454–654*, 1976.

[2] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[3] Eng Heba A Abughali and Mohammed A Mikki. Cryptography using quasi group and chaotic maps. 2018.

[4] Daisaburo Yoshioka. Properties of chebyshev polynomials modulo $p^k$. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 65(3):386–390, 2017.

[5] Eli Biham. Cryptanalysis of the chaotic-map cryptosystem suggested at eurocrypt'91. In *Advances in Cryptology—EUROCRYPT'91: Workshop on the Theory and Application of Cryptographic Techniques Brighton, UK, April 8–11, 1991 Proceedings 10*, pages 532–534. Springer, 1991.

[6] Toshiki Habutsu, Yoshifumi Nishio, Iwao Sasase, and Shinsaku Mori. A secret key cryptosystem by iterating a chaotic map. In *Advances in Cryptology—EUROCRYPT'91: Workshop on the Theory and Application of Cryptographic Techniques Brighton, UK, April 8–11, 1991 Proceedings 10*, pages 127–140. Springer, 1991.

[7] Th Beth, Dejan E Lazic, and A Mathias. Cryptanalysis of cryptosystems based on remote chaos replication. In *Advances in Cryptology—CRYPTO'94: 14th Annual International Cryptology Conference Santa Barbara, California, USA August 21–25, 1994 Proceedings 14*, pages 318–331. Springer, 1994.

[8] Pina Bergamo, Paolo D'Arco, Alfredo De Santis, and Ljupco Kocarev. Security of public-key cryptosystems based on chebyshev polynomials. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 52(7):1382–1393, 2005.

[9] Franz Pichler and Josef Scharinger. Finite dimensional generalized baker dynamical systems for cryptographic applications. In *Computer Aided Systems Theory—EUROCAST'95: A Selection of Papers from the Fifth International Workshop on Computer Aided Systems Theory Innsbruck, Austria, May 22–25, 1995 Proceedings 5*, pages 465–476. Springer, 1996.

[10] Jiri Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos*, 8(06):1259–1284, 1998.

[11] Toan-Thinh Truong, Minh-Triet Tran, Anh-Duc Duong, and Isao Echizen. Chaotic chebyshev polynomials based remote user authentication scheme in client-server environment. In *ICT Systems Security and Privacy Protection: 30th IFIP TC 11 International Conference, SEC 2015, Hamburg, Germany, May 26-28, 2015, Proceedings 30*, pages 479–494. Springer, 2015.

[12] Marcin Lawnik and Adrian Kapczyński. Application of modified chebyshev polynomials in asymmetric cryptography. *Computer Science*, 20:289–303, 2019.

[13] Jing Li, Licheng Wang, Lihua Wang, Xianmin Wang, Zhengan Huang, and Jin Li. Verifiable chebyshev maps-based chaotic encryption schemes with outsourcing computations in the cloud/fog scenarios. *Concurrency and Computation: Practice and Experience*, 31(22):e4523, 2019.

[14] L. Kocarev, J. Makraduli, and P. Amato. Public-key encryption based on Chebyshev polynomials. *Circuits, Systems and Signal Processing*, 24:497–517, 2005.

[15] Hongzhou Ning, Yun Liu, and Dequan He. Public key encryption algorithm based on chebyshev polynomials over finite fields. In *2006 8th international Conference on Signal Processing*, volume 4. IEEE, 2006.

[16] Wade Trappe, Lawrence Washington, Michael Anshel, and Kent D Boklan. Introduction to cryptography with coding theory. *The Mathematical Intelligencer*, 29(3):66–69, 2007.

[17] P Nigel Smart. *Cryptography made simple*. Springer, 2016.

[18] C. E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech. J vol. 28, pp. 656–715*, 1949.

[19] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. In *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, pages 365–390. 2022.

[20] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC press, 2018.

[21] Ian Percival and Franco Vivaldi. Arithmetical properties of strongly chaotic motions. *Physica D: Nonlinear Phenomena*, 25(1-3):105–130, 1987.

[22] T. J. Rivlin and Chebyshev Polynomials. From approximation theory to algebra and number theory. *Pure and Applied Mathematics (New York), John Wiley & Sons, Inc., New York*, 1990.

[23] Peter Borwein and Tamás Erdélyi. *Polynomials and polynomial inequalities*, volume 161. Springer Science & Business Media, 1995.

[24] TJ Rivlin and Chebyshev Polynomials. From approximation theory to algebra and number theory. *Pure and Applied Mathematics (New York), John Wiley & Sons, Inc., New York*, 1990.

[25] Ljupco Kocarev and Zarko Tasev. Public-key encryption based on Chebyshev maps. In *Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS'03.*, volume 3, pages III–III. IEEE, 2003.

[26] Zhengjun Cao, Lihua Liu, and Leming Hong. Evaluation methods for chebyshev polynomials. *Cryptology ePrint Archive*, 2020.

[27] Ke Qin, Mingtian Zhou, and Yong Feng. A novel multicast key exchange algorithm based on extended chebyshev map. In *2010 International Conference on Complex, Intelligent and Software Intensive Systems*, pages 643–648. IEEE, 2010.

[28] Shijie Yan, Ping Zhen, and Lequan Min. Provably secure public key cryptosystem based on chebyshev polynomials. *J. Commun.*, 10(6):380–384, 2015.

[29] GJ Fee and MB Monagan. Cryptography using chebyshev polynomials. In *Maple Summer Workshop, Burnaby, Canada*, 2004.