Mathematics for Cryptography: A Guide to Mathematical Fundamentals of Different Classes of Cryptography Algorithms

Zahra Dorostkar
Skolkovo Institute of Science and Technology

Mathematics for Cryptography

A Guide to Mathematical Fundamentals of Different Classes of Cryptography Algorithms

Zahra Dorostkar
Skolkovo Institute of Science and Technology, Moscow, Russia
zdorostkar@stud.etu.ru

Abstract

This article provides an overview of various cryptography algorithms, discussing their mathematical underpinnings and the areas of mathematics needed to understand them. While not delving deeply into specific algorithmic details, the article aims to familiarize readers with the mathematical concepts and principles that are essential for understanding each of these algorithms.

By providing an overview of the necessary mathematical backgrounds for various cryptography algorithms, this article aims to equip readers with the foundational knowledge needed to explore these algorithms in greater depth and to engage in the ongoing research and development in this rapidly evolving field.

Keywords: Cryptography, mathematical foundations, number theory, algebra, probability theory, public-key, symmetric-key, quantum, post-quantum, algorithms, information theory.

1 Introduction

Cryptography is the practice of securing communication and protecting sensitive data, and understanding the mathematical concepts behind these algorithms is crucial for working with them effectively. Each class of cryptography algorithms is associated with specific mathematical areas that are essential to be familiar with. For example, number theory plays a vital role in public-key cryptography, as it involves the difficulty of factoring large prime numbers. Algebraic structures such as groups, rings, and fields are fundamental in constructing cryptographic systems. Probability theory is used to analyze the security aspects of these systems. Additionally, knowledge of computer science topics like data structures, algorithms, and programming is important for implementing and utilizing cryptography algorithms. By exploring the related mathematical areas for each class of cryptography, individuals can gain the necessary prerequisites to engage effectively with these algorithms and contribute to the ongoing research and development in this important field. This article aims to provide insight into the mathematical foundations underlying different classes of cryptography algorithms.

2 Algorithms

2.1 Basic Encryption Algorithms

These ciphers were commonly used in the past for encryption and decryption purposes. They generally involve substitution or transposition techniques to encode and decode information. Classic ciphers have played a significant role in the historical development of cryptography and have paved the way for modern encryption techniques. By exploring these algorithms, you will gain insights into the foundations and principles of cryptography.

While some algorithms do involve mathematical concepts like modular arithmetic or matrix operations, they can be implemented without an in-depth understanding of those concepts. However, having knowledge of the underlying mathematical principles can certainly be beneficial when working with cryptography algorithms.

Atbash: Atbash is a substitution cipher where letters of the alphabet are reversed. For example, 'A' becomes 'Z', 'B' becomes 'Y', and so on. It is a simple way of encrypting text by substituting each letter with its reverse counterpart.
ROT13: ROT13 is a substitution cipher where each letter is replaced with the 13th letter after it in the alphabet. It is often used to hide spoilers or as a simple form of encryption.
Caesar: The Caesar cipher is a shift cipher where each letter is replaced by a letter with a fixed shift number. For example, with a shift of 3, 'A' becomes 'D'.The shift can be any number.
Affine: The Affine cipher is a substitution cipher where each letter is encrypted using the formula (ax + b) mod 26, where 'a' and 'b' are arbitrary values. It involves both multiplication and addition operations. The values of 'a' and 'b' determine the encryption key. It requires knowledge of modular arithmetic and linear algebra.
Rail-fence: Rail-fence is a transposition cipher where the plaintext is written diagonally in a zigzag pattern and then read off row by row.
Baconian: The Baconian cipher is a 'biliteral' cipher that uses a binary encoding scheme. Each letter of the alphabet is represented by a five-letter code consisting of 'A' and 'B'. The message is concealed within the presentation of text by substituting each letter with its corresponding binary code.
Polybius Square: The Polybius Square is a substitution cipher where characters are substituted with pairs of digits. It uses a 5x5 grid where the letters of the alphabet are arranged, usually omitting 'J'. Each letter is represented by its row and column number in the grid.
Simple Substitution: Simple Substitution is a basic substitution cipher where each unit or letter of the plaintext is replaced with another letter. The substitution is determined by a pre-defined mapping of letters.
Codes and Nomenclators: Codes and Nomenclators is a substitution cipher that uses a substitution table or codebook to replace letters or words with substitutes. It involves substituting common phrases or names with predefined codewords. The mathematical background required depends on the specific codes and nomenclators being used.

2.2 Transposition Algorithms

These ciphers involve replacing letters or units of the plaintext with other letters or units to create the ciphertext. They generally operate on the basis of fixed substitution rules or patterns. The algorithms in the list exhibit various characteristics such as rearranging columns, utilizing modular arithmetic, or using a subset of alphabets. Overall, they are part of the broader category of classical substitution ciphers, each with its own unique approach to encryption and decryption.
Columnar Transposition: This algorithm is a transposition cipher that involves rearranging the columns of the plain text based on a given key. It focuses on the reorganization

of characters rather than substitution.
Autokey: The Autokey cipher is a variation of the Vigenere cipher. It enhances security by combining the plain text with a key using modular arithmetic. The resulting cipher is used as part of the key for encrypting subsequent characters.
Beaufort: The Beaufort cipher is another variation of the Vigenere cipher. It differs in the encryption formula, where the plain text is subtracted from the key modulo 26 to obtain the ciphertext.
Porta: The Porta cipher is a polyalphabetic cipher like the Vigenere cipher, but it only uses a subset of 13 alphabets. It narrows down the key space compared to the Vigenere cipher.
Running Key: The Running Key cipher is similar to the Vigenere cipher, but it uses a long text as the key that is not repeated. This uniqueness of the key adds an extra layer of security compared to the Vigenere cipher.

While these algorithms do not require specific mathematical fields, having a basic understanding of *modular arithmetic* and *number theory* can be helpful when working with them.

Modular arithmetic is a branch of mathematics that deals with the remainder when dividing one integer by another. It focuses on the properties and operations involving remainders. In modular arithmetic, numbers "wrap around" after a certain value called the modulus. This means that if we divide a number by the modulus, the remainder represents the value in the modular system.

Number theory is a branch of mathematics that studies properties and relationships of numbers, particularly integers. It involves the study of prime numbers, divisibility, factorization, prime factorization, congruences, and other number-related concepts. Number theory is the foundation of many cryptographic algorithms and plays a significant role in cryptography and encryption techniques.

In addition the following areas within mathematics are closely related to modular arithmetic and number theory:
For modular arithmetic:
Group Theory: Group theory deals with the study of algebraic structures called groups, which are sets with operations that satisfy specific properties. Modular arithmetic can be viewed as a group under addition modulo a fixed modulus.
Ring Theory: Ring theory is the study of algebraic structures called rings, which generalize the concept of arithmetic operations. Modular arithmetic can be understood in the context of rings, specifically the ring of integers modulo a fixed modulus.
For number theory:
Prime Number Theory: Prime number theory focuses on the properties and distribution of prime numbers. It involves topics such as prime factorization, prime number theorems, and the Riemann zeta function.
Diophantine Equations: Diophantine equations are polynomial equations in two or more variables with integer coefficients. Number theory often deals with solving Diophantine equations and studying their properties.
Analytic Number Theory: Analytic number theory applies tools from analysis, such as complex analysis and calculus, to study number-theoretic problems. It includes topics like the Riemann Hypothesis, prime number theorem, and Dirichlet's theorem on arithmetic progressions.
Set Theory: Set theory is a foundational area of mathematics that deals with the study of

sets, which are collections of objects. While set theory is not directly related to modular arithmetic and number theory in terms of their techniques and applications, it provides a fundamental framework for mathematical reasoning and serves as the basis for many mathematical structures and concepts.

2.3 Polygraphic Substitution Algorithms

These algorithms all fall under the category of polygraphic substitution ciphers because they replace multiple symbols in the plaintext with corresponding symbols in the ciphertext. They may also involve additional techniques like matrix operations, fractionation, or transposition. They provide stronger encryption compared to simple substitution ciphers.

Vigenère and Gronsfeld: This algorithm encrypt plaintext by shifting each letter based on a keyword or key number. The Vigenère cipher uses a repeating keyword, while Gronsfeld uses a key number for each letter. It uses the 'tabula recta' to encrypt the plaintext.

Homophonic Substitution: This cipher replaces each letter of the plaintext with multiple symbols or numbers to increase encryption strength. Each letter has multiple possible substitutions, making it more difficult to analyze the ciphertext.

Four-Square: It uses four 5x5 matrices containing letters of the alphabet. It encrypts plaintext by mapping each letter to a corresponding letter in the matrices based on a keyword.

Hill: It encrypts plaintext by performing matrix multiplication using a key matrix. The key matrix determines the encryption permutation.

Playfair: It encrypts pairs of letters. The key is a 5×5 matrix of alphabets which starts by a key and continues by the rest of the alphabet. The row and column of each two letters shows the substitution cipher letter.

ADFGVX and ADFGX: These are transposition and substitution ciphers used by the German army in World War I. They involve combining a modified Polybius square with a transposition step. The ADFGVX cipher uses a 6x6 grid, while the ADFGX cipher uses a 5×5 grid.

Bifid: It combines substitution and transposition techniques. It encrypts plaintext by first converting each letter to its corresponding row and column numbers in a Polybius square. Then, it combines the row and column numbers to create a new ciphertext.

Straddle Checkerboard: It uses a modified Polybius square with additional digits to encrypt plaintext. It assigns unique symbols or numbers to frequently occurring letters, making the encryption more efficient.

Trifid: It encrypts plaintext by first converting each letter to its corresponding row and column numbers in a $3 \times 3 \times 3$ cube. It then combines the row, column, and depth numbers to create the ciphertext.

Fractionated Morse: It encrypts plaintext by first converting each letter to its corresponding Morse code. It then combines the Morse code letters to create the ciphertext.

In the previous section, modular arithmetic and number theory were discussed. In this section, while they do not require advanced mathematical concepts, a basic understanding of the following topics in addition to the previous ones, will be useful:

Probability Theory: Probability theory is a branch of mathematics that deals with the study of uncertainty and randomness. It provides a framework for quantifying and analyzing the likelihood of events occurring in various situations. It involves concepts such as probability, random variables, probability distributions, and statistical inference.

Linear Algebra: Linear algebra is a branch of mathematics that focuses on the study of vector spaces and linear transformations. It deals with the properties and operations involving vectors, matrices, and linear equations. It includes concepts like vector addition, scalar multiplication, matrix multiplication, determinants, eigenvalues, and eigenvectors.

Basic Algebra: Basic algebra is the foundation of algebraic reasoning and manipulation. It involves the study of mathematical symbols and the rules governing their operations, such as addition, subtraction, multiplication, and division. Basic algebra encompasses concepts like variables, equations, inequalities, and solving for unknowns.

Also, There are some areas that are related to them and beneficial to be familiar with:
For Probability Theory:
Statistics: Understanding statistical concepts and techniques can complement and enhance the understanding and application of probability theory.
For Linear Algebra:
Multivariable Calculus: Familiarity with multivariable calculus, which deals with functions of multiple variables and their derivatives, can enhance the understanding of vector calculus and its applications in linear algebra.
Numerical Linear Algebra: Knowledge of numerical methods and algorithms for solving linear systems and eigenvalue problems can complement the theoretical aspects of linear algebra.
Optimization: Understanding optimization techniques and algorithms can be useful in the context of linear algebra, as optimization often involves solving linear systems or optimizing linear models.
For Basic Algebra:
Number Theory: Familiarity with number theory, which studies the properties and relationships of numbers, can provide a deeper understanding of algebraic structures and operations.
Abstract Algebra: Knowledge of abstract algebra, which explores more general algebraic structures like groups, rings, and fields, can broaden the understanding of basic algebraic concepts and provide a more abstract perspective.
Mathematical Logic: Understanding mathematical logic can enhance the rigor and logical reasoning skills applied in algebraic contexts.

2.4 Modern Symmetric-Key Algorithms

Symmetric keys encryption uses one key to encrypt and decrypt data. The key should be distributed before transmission between entities [1].

On the basis of the input data, encryption algorithms are classified as block ciphers, in which the size of the block is of fixed size for encryption and stream ciphers in which a continuous stream is passed for encryption and decryption. RC2, AES, DES, RC6 and BLOWFISH are some of the examples of block cipher. In a symmetric algorithm high security can't be achieved as it makes use of the same key for both encryption and decryption, hence asymmetric algorithms are used. It is also known as Public key encryption. [2–5]

DES: DES is a block cipher encryption algorithm that operates on 64-bit blocks of data and uses a 56-bit key. It uses a series of substitution and permutation operations, S-boxes and P-boxes, along with a Feistel network structure to encrypt and decrypt data.

Advanced Encryption Standard (AES, Rijndael): It is a block cipher encryption algorithm that operates on 128-bit blocks of data and supports key sizes of 128, 192, or 256 bits. It uses substitution-permutation network (SPN) structure and consists of multiple rounds with four main operations: SubBytes, ShiftRows, MixColumns, and Ad-

dRoundKey.
MARS: MARS is a block cipher encryption algorithm that operates on 128-bit blocks of data and supports key sizes of 128, 192, or 256 bits. It uses a combination of modular addition, bitwise XOR, and S-box operations in a Feistel network structure with multiple rounds.
Triple DES (3DES): 3DES is an extension of the DES algorithm. It applies the DES algorithm three times, using either two or three different keys, to enhance security.
TEA (Tiny Encryption Algorithm): TEA is a block cipher that encrypts data in 64-bit blocks using a key length of 128 bits. It uses a simple algorithm that involves multiple rounds of additions, XOR operations, and bit shifts. TEA is a simple and fast algorithm, but is not as secure as more modern ciphers.
Educational Data Encryption Standard (E-DES): E-DES is a simplified version of the DES algorithm designed for educational purposes. It operates on 64-bit blocks of data and uses a 56-bit key, similar to DES.
Blowfish Encryption: It is a block cipher encryption algorithm that operates on 64-bit blocks of data and supports variable-length of up to 448 bits keys. It uses a Feistel network structure with a variable number of rounds and performs substitution and modular addition operations. Blowfish is widely used and considered to be secure.
SEAL(SEcure Algorithm): SEAL is a block cipher encryption algorithm that operates on variable-sized blocks of data and supports key sizes of 128, 192, or 256 bits. It uses a combination of substitution-permutation networks (S-boxes) and diffusion operations.
RC2(Rivest Cipher 2): RC2 is a block cipher encryption algorithm that operates on 64-bit blocks of data and supports variable-length of up to 1024 bits keys. It uses a combination of bitwise operations, modular additions, and S-box lookups.
RC4(Rivest Cipher 4): RC4 is a stream cipher encryption algorithm that operates on streams of data. It generates a pseudo-random stream of bytes by swapping elements of a permutation based on a key, which is XORed with the plaintext to produce the ciphertext.
RC6(Rivest Cipher 6): RC6 is a block cipher encryption algorithm that operates on 128-bit blocks of data and supports key sizes of 128, 192, or 256 bits up to 2048 bits. It uses a combination of substitution-permutation networks (S-boxes) and modular arithmetic operations.
Twofish: Twofish is a block cipher encryption algorithm that operates on 128-bit blocks of data and supports key sizes of 128, 192, or 256 bits. It uses a combination of substitution-permutation networks (S-boxes) and key-dependent permutations.
Serpent: Serpent is a block cipher encryption algorithm that operates on 128-bit blocks of data and supports key sizes of 128, 192, or 256 bits. It uses a combination of substitution-permutation networks (S-boxes) and Galois field arithmetic.
IDEA(International Data Encryption Algorithm): IDEA is a block cipher encryption algorithm that operates on 64-bit blocks of data and uses a 128-bit key. It involves modular additions, bitwise XOR operations, multiplications in a finite field, and S-box substitutions.
CAST(Carlisle Adams and Stafford Tavares cipher): CAST is a block cipher encryption algorithm that operates on 64-bit blocks of data and supports key sizes of up to 128 bits. It uses a combination of substitution-permutation networks (S-boxes) and modular additions.
HiSea(High-Speed Encryption Algorithm): HiSea is a block cipher encryption algorithm that operates on 128-bit blocks of data and supports key sizes of 128, 192, or 256

bits. It uses a combination of substitution-permutation networks (S-boxes) and modular additions.
Skipjack: Skipjack is a block cipher encryption algorithm that operates on 64-bit blocks of data and uses an 80-bit key. It involves a series of substitution and permutation operations, as well as a key-dependent transformation process.
GOST: GOST is a block cipher encryption algorithm that operates on 64-bit blocks of data and uses a 256-bit key. It includes a complex set of substitution and permutation operations, as well as a key mixing process.
Salsa20: Salsa20 is a stream cipher encryption algorithm that operates on streams of data. It uses a pseudo-random number generator based on a 512-bit key and a 64-bit initialization vector (IV). The algorithm involves a series of additions, rotations, and XOR operations.
ChaCha20: ChaCha20 is a stream cipher encryption algorithm that operates on streams of data. It is an improved version of Salsa20 and uses a 256-bit key and a 96-bit nonce. The algorithm involves a series of additions, rotations, and XOR operations.
Simon and Speck: Simon and Speck are a pair of lightweight block cipher encryption algorithms developed by the National Security Agency (NSA). Simon supports block sizes of 32, 48, 64, 96, or 128 bits, while Speck supports block sizes of 64, 96, or 128 bits. Both algorithms use a Feistel network structure and involve bitwise XOR and substitution operations [6].

As it is illustrated in Table.1, In addition to the previous mathematical concepts, there are some new concepts as following:

Boolean Logic: Boolean logic is a branch of mathematics that deals with variables that can only have one of two possible values: true or false. It involves logical operations such as AND, OR, and NOT, which can be used to manipulate and analyze these variables.

Galois Field Arithmetic: Galois Field Arithmetic, also known as finite field arithmetic, is a mathematical structure that operates on a finite set of elements. It involves operations such as addition, subtraction, multiplication, and division, but with a limited set of possible values. It is commonly used in cryptography algorithms for its mathematical properties. It is a subfield of abstract algebra and is indeed a specific area of mathematics.

Bitwise Operations: Bitwise operations are operations performed on individual bits of binary numbers. They include operations such as AND, OR, XOR, and shifting, which manipulate the binary representation of numbers at the bit level. Bitwise operations are often used for low-level data manipulation and optimization in programming.

Substitution-Permutation Networks: Substitution-Permutation Networks (SPN) are a class of cryptographic algorithms that combine substitution and permutation operations. Substitution involves replacing elements with others based on predefined rules, while permutation involves rearranging elements. SPN structures are commonly used in block ciphers to provide confusion and diffusion properties, making them resistant to cryptographic attacks.

Substitution-Permutation Networks and Bitwise Operations are not standalone areas of mathematics, but rather concepts or techniques used in the field of cryptography and computer science.

There are also some areas that are related to these concepts and benefitial to be familiar with when dealing with them:
For Boolean Logic:

This is closely related to propositional logic and Boolean algebra. Having a good understanding of logic gates and truth tables is beneficial for working with Boolean logic.
For Galois Field Arithmetic:
Galois field arithmetic is related to abstract algebra, specifically finite fields. Knowledge of algebraic structures like groups, rings, and fields can be helpful when working with Galois fields.
For Bitwise Operations:
Bitwise operations are related to binary number systems and number theory. Understanding binary representation, binary arithmetic, and concepts like bitwise AND, OR, XOR, and bit shifting can be useful.
For Substitution-Permutation Networks:
Substitution-permutation networks are related to symmetric key cryptography and cryptanalysis. Having knowledge of cryptology, probability theory, and algebraic structures like permutations can be beneficial for understanding SPNs.

Modern Symmetric-Key Ciphers					
Algorithm Name	Modular arithmetic	Boolean logic	Galois field arithmetic	Bitwise operations	Substitution-permutation networks
DES	*	*		*	*
AES	*	*	*	*	*
MARS	*	*		*	*
3DES	*	*		*	*
E-DES	*	*		*	*
Blowfish	*			*	*
SEAL	*	*		*	*
RC2	*			*	*
RC4	*			*	*
RC6	*	*		*	*
Twofish	*	*	*	*	*
Serpent	*		*	*	*
IDEA	*			*	*
CAST	*			*	*
HiSea	*	*	*	*	*
Skipjack	*			*	*
GOST	*		*		*
Salsa20	*			*	
ChaCha20	*			*	
Simon and Speck	*			*	*

Table 1: Modern symmetric-key ciphers

2.5 Modern Public-Key Ciphers:

These algorithms are considered modern public-key ciphers because they are based on the principles of public-key cryptography, where encryption and decryption keys are different. They may use different mathematical concepts, such as modular arithmetic, elliptic curves, lattice-based cryptography, or other techniques to achieve their cryptographic goals.

RSA: RSA (Rivest-Shamir-Adleman) is an asymmetric encryption algorithm. It involves generating a public and private key pair based on the product of two large prime numbers. The public key is used for encryption, while the private key is used for decryption and signing. RSA relies on the mathematical difficulty of factoring large numbers to ensure the security of encrypted data.

ECC(Elliptic Curve Cryptography): ECC is a cryptographic system based on the mathematics of elliptic curves. It uses points on the curve to generate a public-private key pair. ECC provides strong security with shorter key lengths compared to some other encryption algorithms, making it suitable for resource-constrained environments [7].

ElGamal Encryption System: The algorithm begins with Diffie-Hellman key exchange to establish a shared secret, used as a one-time pad for encryption. ElGamal encryption has three phases: key generation, encryption, and decryption. Key generation focuses on key exchange, while the latter phases combine key exchange computations with message computations. ElGamal encryption can be implemented on any cyclic group, like the multiplicative group of integers modulo n. Note that the Digital Signature Algorithm (DSA) is a variation of the ElGamal signature scheme, distinct from ElGamal encryption [8].

XTR: XTR is a cryptographic algorithm used for public-key encryption. Its name, "ECSTR," stands for Efficient and Compact Subgroup Trace Representation. This method enables the representation of elements within a subgroup of the multiplicative group of a finite field. It achieves this by utilizing the trace over $GF(p^2)$ to represent elements belonging to a subgroup of $GF(p^6)^*$.

From a security perspective, XTR relies on the complexity of solving Discrete Logarithm problems within the entire multiplicative group of a finite field. [9]

Quantum Cryptography: Quantum cryptography uses principles from quantum mechanics to establish secure communication. By leveraging quantum particles like photons, these systems ensure the confidentiality and integrity of transmitted information. Messages are sent using photons, and if the intended recipient can decode the message, it is understood. Otherwise, the sender modifies the photons and resends the message. However, it's important to note that quantum cryptography is an expensive technology with limited practical applications. Traditional computers use bits (0 or 1), while quantum computers use qubits from a finite-dimensional complex vector space (Hilbert space) H [10, 11].

NTRU: NTRU is a lattice-based public-key encryption algorithm that relies on finding short vectors in high-dimensional spaces. It offers fast encryption and decryption operations, making it suitable for resource-constrained devices.

Lattice-based Cryptography (NTRU, Ring LWE, BLISS): These algorithms are based on finding the shortest vector in a high-dimensional lattice, and their security depends on the hardness of this problem. NTRU is based on the closest vector problem (CVP), while Ring-LWE and BLISS (a digital signature) are based on the learning with errors (LWE) problem.

Ring LWE: Ring Learning With Errors (LWE) is a lattice-based encryption scheme that

involves solving a learning with errors problem in a polynomial ring. It provides security against attacks by quantum computers and offers efficient encryption and decryption operations.
McEliece: McEliece is an encryption algorithm that uses error-correcting codes. It generates a public key by encoding a random error vector with a random matrix. To encrypt a message, a random error vector is added to the message and multiplied with the public key. The recipient can decrypt the ciphertext by multiplying it with a private key and applying error correction techniques. McEliece's security relies on the difficulty of decoding the received vector without the private key.

Code-based Cryptography (McEliece, Niederreiter): These algorithms use error-correcting codes to create a one-way function. Their security depends on the difficulty of decoding specific codes like Goppa codes.
Niederreiter: Niederreiter is a public-key encryption scheme based on algebraic geometry codes. It provides security against attacks by quantum computers and offers efficient encryption and decryption operations. It is a variant of the McEliece cryptosystem, extending the concept of the parity check matrix. Niederreiter achieves similar security to McEliece but with a faster encryption process. It also has potential for constructing a digital signature scheme [12].
Rainbow: It combines elements of both symmetric and asymmetric encryption. It is designed to provide efficient and secure encryption and signature operations. It is based on the use of multivariate quadratic polynomials to create a one-way function. The security of it depends on the hardness of solving a system of multivariate equations over a finite field. This problem involves concepts from multivariate polynomial algebra, such as Gröbner bases and elimination theory,linear algebra and number theory [13].
Fully Homomorphic Encryption (FHE): Fully Homomorphic Encryption (FHE) is an advanced encryption scheme that allows computation on encrypted data without decrypting it. It enables performing operations on encrypted data while preserving its confidentiality. FHE is a complex and resource-intensive cryptographic technique.

Prime factorization, Modular arithmetic, Discrete logarithm problem, Galois Fields: These are sub-fields of Number theory and play a crucial role in various cryptographic algorithms. Prime factorization involves breaking down a number into its prime factors. The discrete logarithm problem entails finding the exponent needed to raise a base number to obtain a specific result. Galois Fields and modular arithmetic are important concepts in number theory.

Digital signatures: Mathematical schemes used to verify the authenticity and integrity of digital documents or messages. They ensure that a message hasn't been tampered with and originated from a specific sender. Digital signatures draw upon concepts from cryptography, which combines elements of mathematics, computer science, and information security.

Key exchange: The secure process of exchanging cryptographic keys between two parties to establish a shared secret key. Key exchange is a sub-area of cryptography that relies on number theory and computational mathematics.

Quantum mechanics: The branch of physics that describes the behavior of matter and energy at the smallest scales. It provides a mathematical framework for understanding phenomena such as superposition, entanglement, and quantum computing. Quantum mechanics has connections to mathematical fields like linear algebra and functional analysis.

Information theory: The study of quantification, storage, and communication of information. It deals with concepts such as entropy, data compression, error correction, and channel capacity. Information theory is a branch of applied mathematics that focuses on quantifying and communicating information.

Coding theory: The study of error-detection and error-correction codes. It involves designing codes that can detect and correct errors introduced during the transmission or storage of data. Coding theory is a sub-area of information theory.

Multivariate cryptography: A type of cryptography that utilizes multivariate polynomial equations as the foundation for cryptographic algorithms. It explores the difficulty of solving systems of multivariate polynomial equations. Multivariate cryptography combines concepts from algebraic geometry, multivariate polynomial equations, and computational mathematics.

Elliptic curves: Mathematical curves defined by certain equations that possess properties suitable for use in cryptography, particularly in elliptic curve cryptography. The security of cryptographic algorithms based on elliptic curves relies on the challenge of solving elliptic curve equations. Elliptic curves are a topic in algebraic geometry, a branch of mathematics studying geometric objects defined by polynomial equations.

Polynomial rings: Algebraic structures composed of polynomials with coefficients taken from a given ring. They are significant in algebraic geometry, number theory, and algebraic coding theory. Polynomial rings are topics within abstract algebra and commutative algebra.

Algebraic geometry: A branch of mathematics focusing on the study of geometric objects defined by polynomial equations. It combines methods from algebra and geometry to comprehend the properties and structure of these objects. Algebraic geometry finds applications in cryptography, coding theory, and computer science.

Lattice-based cryptography: A type of cryptography that relies on the hardness of certain problems involving lattices. It offers security based on the difficulty of solving lattice problems, such as finding short vectors within a lattice. Lattice-based cryptography is a sub-area of cryptography that incorporates concepts from number theory, linear algebra, and computational mathematics.

Boolean circuits: Mathematical models utilized to represent and analyze the behavior of logical gates and circuits. They are fundamental to the design and analysis of digital systems, including computer hardware and software. Boolean circuits are topics within discrete mathematics and computer science, specifically in the study of logic and digital circuits.

Public-key cryptography: Also known as asymmetric cryptography, it is a cryptographic system employing pairs of keys: a public key for encryption and a private key for decryption. Public-key cryptography enables secure communication and digital signatures without relying on a shared secret key. It is a sub-area of cryptography that incorporates concepts from number theory, algebra etc.

Modern Public-Key Ciphers																	
Algorithm Name	Prime factorization	Modular arithmetic	Digital signatures	Key exchange	Discrete logarithm problem	Quantum mechanics	Information theory	Coding theory	Multivariate cryptography	Elliptic curves	Galois Fields	Polynomial rings	Lattice-based cryptography	Number theory	Boolean circuits	Public-key cryptography	Algebraic geometry
RSA	*	*												*		*	
ECC		*	*	*						*						*	
XTR					*					*	*					*	
Quantum algorithm						*	*									*	
NTRU												*	*	*		*	
Ring LWE												*	*	*		*	
McEliece								*								*	*
Niederreiter								*								*	
Rainbow									*						*	*	*
FHE														*	*	*	

Table 2: Modern Asymmetric-key ciphers

2.6 Cryptographic Hash Functions:

A cryptographic hash function is a special type of algorithm that takes an input and produces a fixed-size output called a hash value. It has properties that make it useful for cryptographic applications:
1.The probability of getting a specific hash value for a random input is very low, making it useful as a representation of the input.
2.It's extremely difficult to find an input that matches a given hash value, providing pre-image resistance.
3.It's also difficult to find a second input that produces the same hash value as a known input, providing second pre-image resistance.
4.Finding two different inputs that produce the same hash value (collision) is also very difficult.
Cryptographic hash functions are widely used in digital signatures, message authentication codes, and other authentication mechanisms to ensure information security [14].

MD2, MD4, MD5: These are cryptographic hash functions that generate a 16-byte message digest for an input message. MD4 and MD5 have a digest length of 128 bits. MD5 is a strengthened version of MD4 with an additional round and more operations per round. The time complexity for finding a message with a given digest is $O(2^{128})$, and for finding two messages with the same digest, it is $O(2^{64})$.

SHA-1, SHA-2, SHA-3: SHA-0 and SHA-1 have a digest length of 160 bits, a block size of 512 bits, and 80 rounds. SHA-2 has varying output sizes from 224 to 512 bits. For output sizes of 224 and 256 bits, the block size is 512 bits with 64 rounds. For output sizes of 384, 512, and others, SHA-2 uses a 1024-bit block size and 80 rounds. SHA-3 has a fixed number of 24 rounds for all types, a similar hash length as SHA-2, and a different internal state that is resistant to length expansion attacks.

RIPEMD-160: It is a hash function that combines two parallel versions of MD4 with some improvements to shifts and the order of message words.

Whirlpool: Whirlpool is an iterated hash function that uses a compression function based on a dedicated 512-bit block cipher with a 512-bit key.

BLAKE2 and BLAKE3: BLAKE2 is based on the HAsh Iterative FrAmework (HAIFA) and uses a simplified version of HAIFA that retains its desirable properties. BLAKE2 includes four hash functions with different word lengths, block sizes, and digest sizes. BLAKE3 is the latest version and has a word length of 64 bits, a block size of 1024 bits, and digest sizes of 224, 256, 384, and 512 bits.

HAVAL: HAVAL is a hash function similar to MD5 but with additional advantages. It uses five nonlinear boolean functions with the Strict Avalanche Criterion property. HAVAL has 15 versions with different numbers of passes and digest lengths, ranging from 128 to 256 bits. It is faster than MD5 when fewer passes are required.

Cryptographic hash functions rely on various areas of mathematics for their design and analysis. Some of the key mathematical areas used in cryptographic hash functions include:

Number theory and Probability theory that were discussed before are being used here. Cryptographic hash functions often involve probabilistic analysis, such as the probability of collisions or pre-image resistance.

Boolean algebra: Cryptographic hash functions often operate on binary data, and Boolean algebra helps in manipulating and analyzing the binary inputs and outputs.

Complexity theory: Concepts such as computational hardness, polynomial time reductions, and complexity classes are relevant for analyzing the security properties of cryptographic hash functions.

2.7 Key Exchange:

Key exchange is a cryptographic process where two or more parties securely share a secret key over an insecure communication channel. This shared key can then be used for encrypting and decrypting messages, ensuring confidentiality and integrity in the communication.

Diffie-Hellman: It involves selecting random values and performing mathematical operations based on modular arithmetic. The shared secret key can then be used for symmetric encryption or other cryptographic purposes. Diffie-Hellman is based on symmetric key exchange for both encryption and decryption [15]. The simplest implementation uses the multiplicative group of integers modulo p, where p is prime, and g is a primitive root modulo p. These two values are chosen in this way to ensure that the resulting shared secret can take on any value from 1 to p–1.

Supersingular Isogeny Key Exchange (SIKE): It is a post-quantum key encapsulation mechanism based on isogeny-based cryptography. It provides security against attacks by quantum computers and offers efficient key exchange operations.

New Hope: It is a post-quantum key exchange protocol based on lattice-based cryptography. It uses mathematical problems related to lattices to ensure security. The parties perform computations involving random polynomials and error terms, making it difficult for eavesdroppers to extract the shared key. New Hope is designed to be resistant against attacks by quantum computers and offers efficient key exchange operations.

Having a solid understanding of the following mathematical concepts can help in understanding the underlying principles and analyzing the security properties of these protocols:

Number Theory that has been discussed before, can be fruitful, particularly modular arithmetic, prime numbers, and mathematical structures like groups and fields.

Algebraic Geometry that has been mentioned in the previous sections, is useful area here. This field deals with geometric objects defined by algebraic equations. It is used in isogeny-based cryptography, which is the foundation of protocols like SIKE.

Lattice Theory: Lattice-based cryptography, as used in New Hope, relies on the mathematical theory of lattices, which are structures formed by grids of points in multidimensional space.

Computational Complexity Theory: Understanding concepts like hardness assumptions, computational hardness, and complexity classes is beneficial in analyzing the security of key exchange protocols.

2.8 Digital Signature Schemes:

Digital signatures are constructed using mathematical algorithms and operations, such as modular arithmetic and elliptic curve cryptography, to provide a mechanism for verifying the authenticity and integrity of digital messages. The security properties of digital signatures are also analyzed using mathematical techniques, such as the discrete logarithm problem and the birthday paradox.

Digital Signature Algorithm(DSA): DSA is a digital signature algorithm used for verifying the authenticity of digital messages. It involves generating a key pair and creating a digital signature using the private key. The signature can be verified using the corresponding public key. DSA is commonly used in digital certificates and secure communication protocols.

DSA (Digital Signature Algorithm): A cryptographic algorithm used for generating and verifying digital signatures. It involves key pair generation, signature creation using the private key, and signature verification using the corresponding public key.

Lamport Signature: A one-time signature scheme that uses cryptographic hash functions to generate signing and verification keys. Signatures are created by selecting specific bits from the signing key based on the message hash, and verified by comparing corresponding bits from the verification key with the message hash.

Merkle Signature: A Merkle tree is used to efficiently verify large dataset integrity. Data is organized in a binary tree, with leaf nodes representing hashes of data portions. Tampering can be detected by comparing the root hash with a trusted value.

ECDSA (Elliptic Curve Digital Signature Algorithm): A widely used algorithm that generates and verifies digital signatures using elliptic curve mathematics over finite fields. It involves key pair generation, signature creation by combining the private key with the message, and signature verification using the public key and the original message.

DSS (Digital Signature Standard): A standard for digital signatures defined by NIST. It utilizes the SHA-1 hash function and the DSA algorithm for signature generation and verification. The process involves key pair generation, signature creation using the private key, and signature verification using the public key and the original message.

EdDSA (Edwards-curve Digital Signature Algorithm): A modern digital signature algorithm based on elliptic curve cryptography. It employs a twisted Edwards curve for generating and verifying signatures, offering strong security, shorter signatures, and enhanced efficiency compared to other schemes.

Schnorr Signature: A digital signature algorithm that provides strong security, shorter signatures, and improved efficiency. It involves key pair generation, signature creation by combining the private key with the message, and signature verification using the public key and the original message.

BLISS (Bimodal Lattice Signature Scheme): A post-quantum digital signature scheme based on lattice cryptography, offering robust security against attacks from both classical and quantum computers.

Digital Signature Schemes						
Algorithm Name	Elliptic curves	Lattice Theory	Discrete logarithm	Modular arithmetic	hash functions	Prime numbers
DSA			*	*		*
Lamport					*	
Merkle					*	
ECDSA	*		*			
DSS			*	*		*
EdDSA	*					
Schnorr			*	*		*
BLISS		*				

Table 3: Digital Signature Schemes

3 Summery and Conclusion

As we delve into different classes of cryptography algorithms, the required mathematical knowledge becomes more specific and advanced. Transposition ciphers rely on a foundation of mathematical concepts such as modular arithmetic and number theory, including prime numbers and finite fields. Moving to polygraphic substitution ciphers, we expand into probability theory, linear algebra, basic algebra, statistics, and multivariate calculus, enabling us to analyze frequency distributions and perform mathematical transformations. Modern symmetric-key algorithms build upon these foundations and incorporate boolean logic, propositional logic, boolean algebra, Galois Field arithmetic, bitwise operations, and substitution-permutation networks, allowing for secure and efficient cryptographic operations. In the realm of modern public-key algorithms, we further extend our mathematical knowledge to include digital signatures, key exchange, quantum mechanics, information theory, coding theory, elliptic curves, polynomial rings, algebraic geometry, lattice theory, boolean circuits, and public-key cryptography, all of which contribute to secure key exchange and encryption in a public-key setting. Hash functions draw from number theory, probability theory, boolean algebra, and complexity theory, while key exchange algorithms involve number theory, algebraic geometry, lattice theory, and computational complexity. Finally, digital signature algorithms rely on elliptic curves, discrete logarithm, modular arithmetic, hash functions, and prime numbers for generating secure signatures and verifying message authenticity and integrity. This progression showcases the deepening and diversification of mathematical areas as we explore more advanced classes of cryptography algorithms.

References

[1] T. Nie and T. Zhang, A study of DES and blowfish encryption algorithms, IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON, pp. 1–4, 2009, doi: 10.1109/TENCON.2009.5396115.

[2] O.Abood, S.Guirguis, A Survey on Cryptography Algorithms. International Journal of Scientific and Research Publications. 8. 495-516. 10.29322/IJSRP.8.7.2018.p7978.

[3] M.Mushtaq et al. A Survey on the Cryptographic Encryption Algorithms. International Journal of Advanced Computer Science and Applications. 8. 333-343,2017

[4] S.V. Swathi, P.M. Lahari, B.A. Thomas. Encryption Algorithms: A Survey, International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016), Vol. 4, Issue 2.

[5] C. Burwick and D. Coppersmith, The Mars Encryption Algorithm, NIST AES Propos., pp. 1–12, 1999, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.35.5887&rep=rep1&type=pdf.

[6] Delfs, Hans; Knebl, Helmut (2007). ”Symmetric-key encryption”. Introduction to cryptography: principles and applications. Springer. ISBN 9783540492436.

[7] I. Setiadi, A. I. Kistijantoro, and A. Miyaji, Elliptic curve cryptography: Algorithms and implementation analysis over coordinate systems, ICAICTA 2015 - 2015 Int. Conf. Adv. Informatics Concepts, Theory Appl., no. November, 2015, doi: 10.1109/ICAICTA.2015.7335349.

[8] T. Elgamal, ”A public key cryptosystem and a signature scheme based on discrete logarithms,” in IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, July 1985, doi: 10.1109/TIT.1985.1057074.

[9] Lenstra, Arjen K. and Verheul, Eric R.. ”An overview of the XTR public key system”. Public-Key Cryptography and Computational Number Theory: Proceedings of the International Conference organized by the Stefan Banach International Mathematical Center Warsaw, Poland, September 11-15, 2000, edited by Kazimierz Alster, Jerzy Urbanowicz and Hugh C. Williams, Berlin, New York: De Gruyter, 2001, pp. 151-180. https://doi.org/10.1515/9783110881035.151

[10] R. Kumar. A Survey on Post-Quantum Cryptography for Constrained Devices. International Journal of Applied Engineering Research. 14. 2608-2615. 2019.

[11] D. Bruss, G. Erdelyi, T. Meyer, T. Riege, and J. Rothe, 2007, ACM Computing Surveys, Vol. 39, No. 2, Article

[12] H. Niederreiter (1986). ”Knapsack-type cryptosystems and algebraic coding theory”. Problems of Control and Information Theory. Problemy Upravlenija I Teorii Informacii. 15: 159–166.

[13] Buchmann, J.A., Butin, D., Göpfert, F., Petzoldt, A. (2016). Post-Quantum Cryptography: State of the Art. In: Ryan, P., Naccache, D., Quisquater, JJ. (eds) The New Codebreakers. Lecture Notes in Computer Science(), vol 9100. Springer, Berlin, Heidelberg. $https : //doi.org/10.1007/978 - 3 - 662 - 49301 - 4_6$

[14] Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A. (7 December 2018). ”Hash functions”. Handbook of Applied Cryptography. CRC Press. pp. 33–. ISBN 978-0-429-88132-9.

[15] N. A. Lal, A Review Of Encryption Algorithms-RSA And Diffie-Hellman, Int. J. Sci. Technol. Res., vol. 06, no. 07, pp. 84–87, 2017.