MATHEMATICS IN CRYPTOGRAPHY

Internship report submitted

In partial fulfillment of the requirement for the degree of

Bachelor of Science
In
Mathematics

COURSE
B . Sc (H) Mathematics
By

MADHURI RAJPOOT (2103110002)

Under the guidance of

DR. ARVIND KUMAR

(HANSRAJ COLLEGE)

Department of Mathematics

School of Basic and Applied Science

K. R. Mangalam University, Gurugram - 122003

July-2023

DECLARATION

We declare that this written submission represents our ideas in our own words and where other's ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all the principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will because for disciplinary action by the Institute and canal so evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed. We further declare that if any violation of the intellectual property right or copyright, my supervisor and university should not be held responsible for the same.

MADHURI RAJPOOT	**2103110002**	(Signature)
Student Name	(Roll No.)	

Place: **K.R. Mangalam University**

Date: **05th August 2023**

Hansraj College
University of Delhi
Mahatma Hansraj Marg, Malka Ganj
Delhi – 110007

हंसराज महाविद्यालय
दिल्ली विश्वविद्यालय
महात्मा हंसराज मार्ग, मलकागंज
दिल्ली 110007

Date 29/09/2023

Certificate

This is to certify that **Madhuri Rajpoot** a student of **K R Mangalam University Gurugram** has carried out internship on the topic "**Cryptography and its applications**" at **Hansraj College, University of Delhi, Delhi 110007** as part of **B.Sc (H) Mathematics** Degree requirement. The student carried out his work sincerely during the period from **4 July to 5 Aug 2023** and completed the training successfully.

Arvind

(Dr Arvind)
Professor
Department of Mathematics
Hansraj College

E-mail: principal_hrc@yahoo.com Tel: +91-11-27667458, +91-11-27667747

ACKNOWLEDGEMENT

"Enthusiasm is the feet of all progress, with it there is accomplishment and Without it there are only slits alibis."

Acknowledgment is not a ritual but is certainly an important thing for the successful completion of the project. At the time when we were made to know about the project, it was really tough to proceed further as we were to develop the same on a platform, which was new to us. More so, the coding part seemed tricky that it seemed to be impossible for us to complete the work within the given duration.

We really feel indebted in acknowledging the organizational support and encouragement received from the university.

The task of developing this system would not have been possible without the constant help of our faculty members and friends. We take this opportunity to express our profound sense of gratitude and respect to those who helped us throughout the duration of this project.

We express our gratitude to our supervisors Dr. Mina Kumari for giving their valuable time and guidance to us.

Place: - **K.R. Mangalam University** **MADHURI RAJPOOT**

Date: - 05th August 2023 **Name of Student**

ABSTRACT

Cryptography is the science of encoding and decoding information to protect it from unauthorized access and is central to secure communication systems in today's digital age. This summary provides an overview of the fundamental role that mathematics plays in the field of cryptography. Mathematics serves as the foundation upon which cryptography is built, providing the tools and concepts needed to ensure the confidentiality, integrity, and integrity of sensitive information.

Mathematical principles underlie many aspects of cryptography, including the development of cryptographic algorithms, the generation of encryption keys, and the analysis of security protocols. This summary describes some important mathematical concepts in cryptography, including number theory, remainder calculus, prime numbers, and finite fields. These mathematical tools enable the creation of computationally secure cryptographic algorithms, which make it difficult to break the encryption even with advanced computing resources.

In addition, mathematics plays an important role in the design and analysis of cryptographic protocols. Concepts such as probability theory and information theory are essential for evaluating the security of cryptographic systems and quantifying their resistance against various attacks such as brute force attacks, statistical analysis, and cryptanalysis.

Mathematics is the basis of cryptography, which enables the construction of secure communication systems that protect the privacy and security of individuals, organizations, and nations. Understanding the mathematical foundations of cryptography is critical for researchers, practitioners, and policymakers who strive to ensure the confidentiality and integrity of digital information in an ever-evolving technology landscape.

TABLE OF CONTENTS

INTRODUCTION

Mathematics plays an important role in cryptography by providing the foundation for secure communication and data protection. Concepts such as prime numbers, remainder calculus, and number theory are used to create cryptographic algorithms that guarantee confidentiality and integrity. Public key cryptography relies on mathematical problems that are difficult to solve, such as factoring large numbers or solving discrete logarithms. It is the foundation for secure communications and protection of sensitive information.

Cryptography involves the application of mathematical principles to the development of secure communication and data protection methods. This includes creating cryptographic keys through mathematical algorithms, applying complex mathematical operations for encryption and decryption, and applying problem-solving mathematical intrusions to ensure security. Concepts such as prime numbers, remainder calculus, and number theory support cryptography. The relationship between mathematics and cryptography is important for establishing secure digital communications, protecting sensitive information, and building trust in online transactions and data exchange.

The importance of mathematics in cryptography cannot be overemphasized. Mathematics serves as the foundation upon which secure communications and data protection are built. The main reasons for emphasizing its importance are:

1. **Foundation of Security:** Mathematics provides the theoretical foundations of cryptographic algorithms. Concepts such as number theory, prime factorization and discrete logarithms underlie the security of encryption and decryption processes.
2. **Complexity and intractability:** Cryptography relies on mathematical problems like computational solution is difficult. These problems serve as the basis for cryptographic methods. Prevent unauthorized people from easily decrypting encrypted data.
3. **Key generation and management:** Cryptographic keys, which are the basis of data protection, are generated using mathematical algorithms. As seen in public key cryptography, the difficulty of deriving a private key from a public key depends on mathematical concepts.

4. **Resilience to attacks:** Cryptanalysts use mathematical techniques to break cryptographic systems. The strength of cryptographic algorithms is measured by their resistance to these mathematical attacks.
5. **Confidentiality and Privacy:** Mathematical principles ensure the confidentiality and privacy of confidential information. Encryption algorithms use mathematical transformations to convert plaintext into ciphertext that cannot be decrypted without the appropriate key.
6. **Digital signatures and authentication:** Mathematics allows the creation of digital signatures, which are unique mathematical representations of messages. These signatures are used to authenticate, ensure the integrity and provenance of digital communications.
7. **Secure Transactions and Data Protection:** In modern digital transactions, mathematics enables secure communication over insecure networks. Online banking, e-commerce and communication platforms rely on encryption technology to protect user data.
8. **Provable Security:** Mathematics enables the development of provably secure cryptographic protocols. Theorems and proofs prove that a particular algorithm satisfies certain security properties and ensure its validity.
9. **Innovation and progress:** The continuous evolution of cryptography is driven by innovative mathematical research. New mathematical discoveries can lead to stronger cryptographic algorithms and techniques.
10. **Protection of critical infrastructure:** Mathematics plays a key role in protecting critical infrastructure such as power grids, communication networks and government systems against cyber threats.

- ## MODULAR ARITHMETIC

Modular calculus is a fundamental concept in mathematics and plays an important role in various fields including cryptography. It involves operations on numbers or moduli within a fixed range. When a certain value is reached, the operation "winds" and starts again.

For example, consider module 12 arithmetic operations. In this case, the numbers are "rounded" when they reach 12. So 7 + 5 is 0, not 12, because 12 is the modulus.

Key operations in Modular Arithmetic

1. **Addition (module m):** Given two numbers a and b, the sum (a + b) of the module m is calculated. When the sum is divided by m, the result is the remainder.

   Example: (7 + 5) mod 12 = 0

2. **Subtraction (modulo m):** Similarly, for subtraction, the remainder is the difference divided by m.

   Example: (7 - 5) mod 12 = 2

3. **Multiplication (modulo m):** The product of two numbers a and b of modulus m is calculated. This means that the result after multiplication is the remainder when the product is divided by m.

   Example: (7 * 5) mod 12 = 11

4. **Division (modulo m):** This is a bit more complicated and not always clearly defined. It is important to note that division is only possible if the numbers involved are relatively prime (there are no common divisors other than 1).

For example: (7/5) mod 12 is not always defined by the coefficients and numbers involved.

Cryptography makes extensive use of modular operations. One notable application is the RSA encryption algorithm, where large prime numbers and modular power operations are central to the encryption and decryption process. Modular operations provide an efficient way to perform calculations while keeping the results within manageable limits.

In addition, modular operations are also used in a variety of other cryptographic protocols and algorithms for tasks such as key exchange, digital signatures, and hash functions. Its features make it a powerful tool for protecting information in the digital world.

- ## PRIME NUMBER THEORY

  - A prime number is a positive integer greater than 1 that has no positive integer divisors other than 1 and itself. For example, 2, 3, 5, 7, 11 and 13 are prime numbers.
  - **Fundamental Theorem of Arithmetic:** This theorem states that every positive integer greater than 1 can be represented uniquely as a product of prime numbers (prime factorization).

How to check the number is prime or not:

Trial Division: This is the easiest way. To check if n is prime, divide it by any integer between 2 and the square root of n. If there is no integer that divides n evenly, then it is a prime number. This method is relatively slow for very large numbers, but works well for small numbers.

Sieve of Eratosthenes: This is an efficient way to find all prime numbers up to a certain limit, rather than checking if a number is prime. Not practical for large numbers, but great for generating lists of prime numbers.

Fermat's Little Theorem: If n is prime, it states that for every integer a that is not divisible by n, a^(n-1) ≡ 1 (mod n). However, the opposite is not always true (Carmichael numbers). Therefore, this test is probabilistic and may require multiple tests.

Miller-Robin Primary Test: This is a widely used primary probability test. Check for primality by repeatedly applying Fermat's Little Theorem. Multiple iterations can provide a high level of confidence about prime numbers

AKS Initial Testing: A deterministic polynomial time algorithm for initial testing, but rarely used in practice due to its complexity.

Elliptic curve primitive proof (ECPP): Another deterministic algorithm that is more efficient than AKS, but still not commonly used due to its complexity.

In cryptography, probabilistic a priori tests, such as the Miller-Rabin test, are often used because they are fast and provide high confidence. Large prime numbers are used in various

cryptographic algorithms such as RSA. Cryptographic security depends on the difficulty of factoring large complex numbers into prime factors.

- ## GROUPS AND FINITE FIELD

A group is a set of elements and an operation that combines any two of those elements to produce a third element. To consider a group, the following four characteristics must be met:

a. **Closure:** The operation must combine any two elements in the set to produce another element in the set.
b. **Associativity:** How elements are combined does not depend on how they are grouped (i.e. (a * b) * c = a * (b * c)).
c. **Element identity:** The element identified by 'e' exists in the collection. So, for any element 'a', the operation using 'e' does not change 'a' (i.e. a * e = e * a = a).
d. **Inverse Element:** For every element 'a', there is an element 'a-1' (the reverse of 'a'), and the operation of 'a' and 'a-1' creates an identity element (i.e. *). a-1 = a-1 * a = e).

A finite field (also known as a Galva field) is a special type of mathematical structure that forms a set of elements together with two operations: addition and multiplication. A finite field has the properties of a field, meaning that it satisfies the following conditions:

a. **Closure under addition and multiplication:** the sum and product of two elements in a field creates another element in the field.
b. **Commutativity, Associativity and Distributivity:** these properties apply to addition and multiplication.
c. **Existence of addition and multiplication:** There are elements "0" and "1" and for the element "a" a + 0 = a and a * 1 = a.
d. **Existence of additive and multiplicative inverses:** for every non-zero element "a", there exist elements "-a" and "a-1" (inverse of "a") such that a + (-a) = 0. and a * a^{-1} = 1.

USE IN CRYPTOGRAPHY

1. **RSA Algorithm:** As mentioned earlier, the RSA algorithm relies heavily on prime numbers. This involves choosing two large prime numbers to use in the key generation process. How primality is checked is important to ensure the security of RSA encryption.
2. **Elliptic Curve Encryption (ECC):** ECC is a widely used public key encryption method. It consists of points on the elliptic curve that form groups under certain operations. ECC security is based on the difficulty of the elliptic curve discrete logarithm problem.
3. **Diffie-Hellman Key Exchange:** Diffie-Hellman allows two parties to agree on a shared secret over an insecure channel. It is based on properties of finite fields and modular power.
4. **AES (Advanced Encryption Standard):** Although not directly based on groups or fields, AES uses finite field operations (specifically the Galois field GF(2^8)) for operations such as permutations, permutations, and mixed columns.
5. **Digital signature:** Various digital signature algorithms, such as DSA (Digital Signature Algorithm) and ECDSA (Elliptic Curve Digital Signature Algorithm), rely on bounded fields and groups for mathematical operations.

Understanding the mathematical properties of groups, finite fields and their applications is important for the design and analysis of cryptographic systems. These structures provide the mathematical basis for many encryption, key exchange, and authentication protocols used to secure digital communications and information.

- ## LITERATURE REVIEW

A literature review on the role of mathematics in cryptography reveals a rich and complex relationship between these two disciplines. Mathematics serves as the fundamental framework upon which cryptographic techniques are built, providing the necessary tools to create secure communication systems. This literature review will highlight key aspects and contributions of mathematics in the field of cryptography.

1.**Number theory:** Number theory is the basic branch of mathematics in cryptography. Concepts such as prime numbers, modulo calculus, and the Euclidean algorithm are necessary to develop

cryptographic algorithms such as RSA (Rivest-Shamir-Adleman) and Diffie-Hellman. The work of mathematicians such as Euler and Fermat has contributed to the formation of modern cryptographic systems.

2.**Bounded fields:** Bounded fields, also called Galva fields, are essential for many cryptographic algorithms. The algebraic properties of bounded fields enable efficient and secure cryptographic techniques, such as those used in Advanced Encryption Standard (AES) and Elliptic Curve Encryption (ECC).

3.**Probability theory:** Probability theory plays an important role in evaluating the security of cryptographic systems. Cryptographers use probabilistic models to analyse the probability of successful attacks against encryption schemes and guide the development of stronger algorithms and key lengths.

4.**Information theory**: Information theory, pioneered by Claude Shannon, had a major impact on cryptography. Shannon's research laid the foundation for understanding information security, leading to concepts such as entropy and complete confidentiality that are fundamental to the design of secure communication protocols.

5.**Cryptanalysis:** Cryptanalysis, the study of deciphering cryptographic systems, relies heavily on mathematical techniques. Cryptographers use mathematical reasoning and computational techniques to search for vulnerabilities in cryptographic algorithms and gain insight into their security.

6.**Public-key cryptography:** The basis of modern secure communications, public-key cryptography relies on mathematical problems that are computationally difficult to solve. For example, the RSA algorithm relies on the difficulty of factoring large primes and the security of elliptic curve cryptography on the discrete logarithm problem.

7.**Network-based encryption:** Recent advances in network-based encryption further highlight the importance of mathematical structure in encryption. The network provides a rich source of hard computational problems, making it suitable for building secure post-quantum cryptographic schemes.

8.**Homomorphic encryption:** Homomorphic encryption allows computations to be performed on encrypted data without decryption and relies on complex mathematical structures. This field is a testament to the continued integration of mathematics and cryptography in addressing real-world privacy challenges.

9.**Quantum cryptography:** Quantum cryptography, a rapidly evolving field, relies on the principles of quantum mechanics and advanced mathematical frameworks. Quantum algorithms such as Scholl's algorithm threaten the security of classical cryptographic systems, so there is a need to develop quantum-resistant cryptographic algorithms.

❖ TABLE OF CONTENTS

❖ COLLEGE INFORMATION

Hansraj College, is become co-educational constituent college of the University of Delhi in 1978. The college was founded on July 26, 1948, in memory of Maharshi Dayanand Saraswati and Mahatma Hansraj, by D.A.V. College Managing Committee, Dr. Rama (Principal of Hansraj College) a Master of Philosophy (M.Phil) , took over as chairman of the college governing body in 1978. The college had been ranked as the 12th best college in India as per the National Institutional Ranking Framework India Rankings 2023. In 2022, Hansraj College ranked 12th among colleges across India.

❖ INTERNSHIP DESCRIPTION

- Collaborate with the cryptography team to develop and analyze cryptographic algorithms.
- Apply mathematical principles to design and evaluate security protocols.
- Research and implement advanced number theory, algebraic structures, and other mathematical concepts for encryption.
- Assist in the identification and resolution of security vulnerabilities.
- Contribute to the development of mathematical models to improve encryption efficiency

and robustness.

- Participate in team discussions and share insights on emerging cryptographic trends.

Overview of internship experience

During this internship, I had the opportunity to dive into the fascinating world of cryptography, a field that focuses on creating secure communications and data protection mechanisms. My internship was at a leading company in the field of cyber security and encryption solutions.

• Internship Objective

1. **Understanding Cryptographic Fundamentals:** Gain a deep understanding of the core principles and concepts of cryptography, including encryption, decryption, cryptographic keys, hashing, and digital signatures.
2. **Cryptography in Action:** Learn to apply cryptographic techniques to practical security scenarios, including secure communication, data protection, and authentication. Study and analyze various cryptographic algorithms, both symmetric and asymmetric, including AES, RSA, and ECC.
3. **Vulnerability Analysis and Mitigation:** Learn how to identify potential vulnerabilities and weaknesses in cryptographic implementations. Explore techniques for securing cryptographic systems against attacks and threats.
4. **Research and Innovation:** Engage in research activities related to cryptography, staying updated on the latest developments and emerging trends in the field. Contribute to ongoing research projects aimed at advancing the state of the art in cryptography.
5. **Documentation and Communication:** Develop strong documentation skills to record your research findings, experiments, and project work. Practice clear and effective communication of cryptographic concepts and solutions to both technical and non-technical stakeholders.

• Internship Task & Responsibilities

As an intern in the field of cryptography, you will have the opportunity to engage in a range of tasks and responsibilities aimed at deepening your understanding of cryptographic concepts and their practical applications. These tasks are designed to give you hands-on experience and contribute to real-world projects related to information security.

1. **Cryptographic Research:** Conduct research on various cryptographic algorithms, protocols, and techniques. Stay updated with the latest developments and emerging trends in the field of cryptography.
2. **Algorithm Implementation:** Implement cryptographic algorithms using programming languages like Python, C/C++, or Java. Develop scripts or software tools for encryption, decryption, and cryptographic operations.
3. **Security Assessments:** Perform security assessments and vulnerability analysis of cryptographic systems. Identify potential weaknesses or vulnerabilities in encryption implementations.
4. **Cryptographic Tool Testing:** Test and evaluate cryptographic tools and libraries for their performance and security. Generate test data and conduct experiments to assess the reliability of cryptographic solutions.
5. **Documentation:** Document your research findings, experiments, and observations in a clear and organized manner. Create technical reports, documentation, and presentations to communicate your insights to the team.

- ## Requirement

1. **Education:** A Ph.D. in computer science, mathematics, or a related field with a focus on cryptography is often preferred. A master's degree may be acceptable for some positions.

2. **Experience:** Significant research experience in cryptography, with a track record of publications in reputable conferences or journals.

3. **Skills:** Proficiency in mathematics, particularly number theory, algebra, and discrete mathematics. Strong programming skills in languages like C/C++, Python, or Java. Knowledge of cryptographic algorithms, protocols, and cryptographic libraries.

- ## Benefits

1. **Data Confidentiality:** Cryptography ensures that sensitive information remains confidential by transforming it into an unreadable format (ciphertext). Only authorized

parties with the appropriate decryption keys can access and decipher the data. This benefit is crucial for protecting personal and sensitive data from unauthorized access.

2. **Data Integrity:** Cryptographic techniques help maintain the integrity of data by detecting any unauthorized changes or tampering. Hash functions, in particular, are used to generate fixed-size values (hashes) for data, and even a small alteration in the data results in a significantly different hash value, alerting users to potential tampering.

3. **Authentication:** Cryptography enables authentication, allowing individuals and systems to verify the identity of parties involved in communication or transactions. Digital signatures, for example, confirm that a message or document originated from a specific sender and has not been altered during transmission.

➢ Conclusion

In the ever-evolving world of digital communication and data storage, the importance of mathematics in cryptography cannot be overemphasized. Mathematics not only provides a tool for creating secure cryptographic algorithms, but also serves as a compass for navigating the complex realm of data security.

This research shows the fundamental role of mathematics in strengthening the security of our digital sphere. Collaboration between mathematicians and cryptographers continues to innovate, creating cryptographic systems that stand up to the relentless tide of cyber threats.

As we complete this journey through the realm of mathematics in cryptography, we believe that mathematics is not just a tool, but a guardian that ensures the sanctity of our digital conversation and strengthens our faith in the digital age. The enduring partnership between mathematics and cryptography underscores our commitment to securing the data that defines our interconnected world.

Consequently, finite groups and fields are fundamental mathematical constructs that play a central role in modern cryptography.

Groups provide a framework for defining operations and understanding the properties of elements in a collection. These guarantee closure, associability, existence of identity elements and availability of inverses. This concept is especially important when understanding symmetric

key cryptography, where operations such as encryption and decryption depend on group properties.

Finite fields, a special type of mathematical structure, extend the concept of groups to include the operations of addition and multiplication. These are essential for various cryptographic algorithms and ensure that computations are confined to a limited set of elements. Bounded fields are at the heart of protocols such as RSA, Diffie-Hellman, and elliptic curve cryptography.

These mathematical concepts form the basis of cryptographic protocols. The security of encryption, key exchange, and digital signatures all depend on the mathematical properties of these structures.

INTRODUCTION IN CRYPOTRAGHY

Internship report submitted

In partial fulfillment of the requirement for the degree of

Bachelor of Science
In
Mathematics

COURSE
B . Sc. (H) Mathematics
By

RITIK (2103110005)

Under the guidance of

Dr. Arvind Kumar

(Hansraj College)

\

Department of Mathematics

School of Basic and Applied Science

K. R. Mangalam University, Gurugram - 122003

July-2023

DECLARATION

We declare that this written submission represents our ideas in our own words and where other's ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all the principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will because for disciplinary action by the Institute and canal so evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed. We further declare that if any violation of the intellectual property right or copyright, my supervisor and university should not be held responsible for the same.

RITIK	**2103110005**	Ritik
(Student Name)	(Roll No.)	(Signature)

Place: **K.R. Mangalam University**

Date: **05th August 2023**

Hansraj College
University of Delhi
Mahatma Hansraj Marg, Malka Ganj
Delhi – 110007

हंसराज महाविद्यालय
दिल्ली विश्वविद्यालय
महात्मा हंसराज मार्ग, मलकागंज
दिल्ली 110007

Date 29/09/2023

Certificate

This is to certify that **Ritik** a student of **K R Mangalam University Gurugram** has carried out internship on the topic "**Cryptography and its applications**" at **Hansraj College, University of Delhi, Delhi 110007** as part of **B.Sc (H) Mathematics** Degree requirement. The student carried out his work sincerely during the period from **4 July to 5 Aug 2023** and completed the training successfully.

(Dr Arvind)
Professor
Department of Mathematics
Hansraj College

E-mail: principal_hrc@yahoo.com Tel: +91-11-27667458, +91-11-27667747

ACKNOWLEDGEMENT

"Enthusiasm is the feet of all progress, with it there is accomplishment and Without it there are only slits alibis."

Acknowledgment is not a ritual but is certainly an important thing for the successful completion of the project. At the time when we were made to know about the project, it was really tough to proceed further as we were to develop the same on a platform, which was new to us. More so, the coding part seemed tricky that it seemed to be impossible for us to complete the work within the given duration.

We really feel indebted in acknowledging the organizational support and encouragement received from the university.

The task of developing this system would not have been possible without the constant help of our faculty members and friends. We take this opportunity to express our profound sense of gratitude and respect to those who helped us throughout the duration of this project.

We express our gratitude to our supervisors **Dr. Mina Kumari** for giving their valuable time and guidance to us.

Place: - **K.R. Mangalam University** **RITIK**

Date: - **05th August 2023** **(Name of Student)**

ABSTRACT

Cryptography plays a role, in ensuring information security in the digital era. It is a field that involves a range of techniques and principles aimed at safeguarding data from unauthorized access, tampering or interception. In this abstract we will explore the scope of cryptography delving into its origins core principles, diverse encryption methods, practical applications, in real world scenarios and the ongoing challenges it encounters amidst rapid technological advancements.

Cryptography has a rich history dating back to ancient civilizations. Initially, it was mainly used for secret communications between military and political leaders.

This is one of the earliest ciphers invented by Julius Caesar. Julius Caesar was the emperor of Rome who devised this to use in wars. The way this worked was all the alphabets of the English letter were shifted by 3 places and thus resulted in the cipher text. To break it, all one needed to do was shift the alphabet back 3 places. Though this was very easy to break, it was very useful in wars in ancient times.

Now also a shift algorithm is often regarded as Caesar Cipher. There is a shift of three in this method but the number could range between 1 to 25.

The roots of cryptography are found in Roman and Egyptian civilizations.

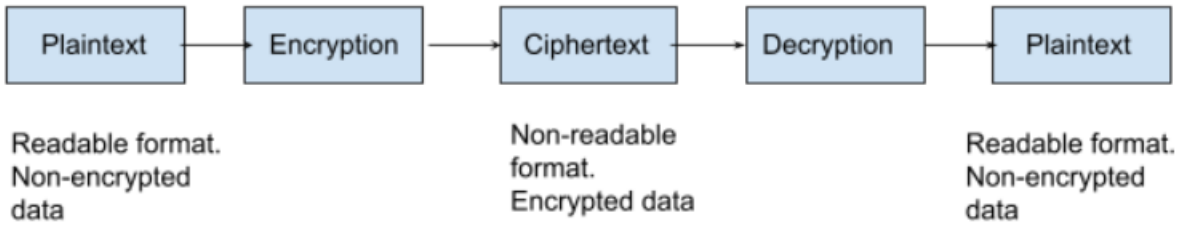
TABLE OF CONTENTS

INTRODUCTION

Cryptography is the science of secure communication. It involves encoding and decoding information to protect it from unauthorized access. Cryptography has been used for centuries to ensure the confidentiality, integrity, and authenticity of messages. It plays a crucial role in modern cybersecurity, from securing online transactions to safeguarding sensitive data. Cryptographic techniques include encryption, which transforms plaintext into ciphertext, and decryption, which reverses the process to retrieve the original message. Public-key cryptography, symmetric-key cryptography, and cryptographic algorithms are fundamental components of this field, providing the tools and methods to secure digital communication in an increasingly interconnected world.

- ## What is Cryptography?

Cryptography is the science and practice of securing communication and information by converting it into a code or cipher to protect it from unauthorized access or tampering.



Cryptography

- **Strong Cryptography**

Strong cryptography refers to the use of highly secure encryption algorithms and practices to protect information and communications from unauthorized access or decryption. The term "strong" in this context implies that breaking or circumventing the encryption would require a significant amount of computational resources, time, or expertise, making it practically infeasible for attackers.

Here are some characteristics of strong cryptography:

1) **Complexity**: Strong cryptographic algorithms are designed to be mathematically complex, making it extremely difficult for attackers to reverse engineer or guess the encryption keys.
2) **Key Length:** Longer encryption keys generally result in stronger encryption. For example, AES-256 (256-bit key) is considered stronger than AES-128 (128-bit key) due to the increased key length.
3) **Resistance to Attacks:** Strong encryption should be resistant to various cryptographic attacks, including brute-force attacks (trying all possible keys) and known-plaintext attacks (exploiting knowledge of the plaintext and corresponding ciphertext).
4) **Security Protocols**: Strong cryptography is often used within secure communication protocols, such as TLS/SSL for secure web browsing and SSH for secure remote access. These protocols incorporate strong encryption to protect data in transit.
5) **Regular Updates**: Strong cryptography evolves over time as new cryptographic research and computational advancements occur. It's essential to use up-to-date cryptographic algorithms and practices to maintain security.

Common examples of strong cryptographic algorithms include:

1) **AES (Advanced Encryption Standard):** Widely used for symmetric encryption, available in key lengths of 128, 192, and 256 bits.
2) **RSA (Rivest-Shamir-Adleman):** A popular asymmetric encryption algorithm used for secure key exchange and digital signatures.
3) **ECC (Elliptic Curve Cryptography):** Another asymmetric encryption technique known for its strong security with shorter key lengths compared to RSA.
4) **SHA-256 (Secure Hash Algorithm 256-bit):** Used for creating cryptographic hash values, which ensure data integrity.

Strong cryptography is essential for protecting sensitive data, securing online transactions, and maintaining the confidentiality and integrity of digital communication in an increasingly interconnected and data-driven world. Security practices should continually evolve to keep pace with emerging threats and vulnerabilities.

Asymmetric encryption: Unlike symmetric encryption, which uses the same key for encryption and decryption, asymmetric encryption uses two separate but related keys: a public key and a pri

vate key. These keys are mathematically related but have different functions.

Public key: The public key is exactly what it looks like: it is public and can be freely distributed to anyone. It is used to encrypt data or verify digital signatures, but not to decrypt data or create digital signatures.

This is the key you share with others. It's like a padlock that you leave behind in everyone. It is u sed for encryption. Anyone who wants to send you a secure message can log in with your public number. However, only your private key can decrypt and open the message once encrypted with your public key. It is safe to share your key publicly.

Private Key: The private key is confidential and should not be shared with others. It is used to d ecrypt data encrypted with the corresponding public key and create a digital signature that can be verified using the corresponding public key.

This is the secret key that only you have. It's like a key that unlocks a lock generated by your pub lic key. When you receive the encrypted message, you can decrypt the message with your private key. Keeping your private key safe is very important because anyone with access to it can decrypt messages sent to you and possibly even yourself. digital signature.

Encryption: When someone wants to send an encrypted message to another party, they use the r ecipient's public key to encrypt the message. When encrypted with the public key, only the corre sponding private key can decrypt the message. This ensures that only the intended recipient can r ead the message.

- ## What is Hash Functions?

A hash function is a fundamental concept in cryptography and computer science. It is a mathematical function that takes an input (or "message") and produces a fixed-size string of characters, which is typically a hexadecimal number or a bit string of a fixed length. The output, known as the hash value or hash code, is unique to each unique input. Hash functions are widely used for a variety of purposes, including data integrity verification, password storage, and digital signatures. Here are some key characteristics and uses of hash functions:

1. **Deterministic:** A hash function always produces the same hash value for the same input. This determinism ensures that you can verify data consistency and integrity over time.

2. **Fixed Output Length**: Hash functions produce hash values of a fixed length, regardless of the length of the input. Common hash lengths include 128 bits, 256 bits, and 512 bits.

3. **Efficiency**: Hash functions are designed to be computationally efficient, allowing for quick computation of hash values even for large inputs.

4. **Pre-image Resistance**: It should be computationally infeasible to reverse a hash value to find the original input (pre-image). In other words, given the hash value, it should be extremely difficult to find an input that produces that hash.

5. **Collision Resistance:** A good hash function minimizes the likelihood of two different inputs producing the same hash value (collision). Collision resistance is crucial for the security of many applications, such as digital signatures and password storage.
6. **Avalanche Effect**: A small change in the input should result in a significantly different hash value. This property ensures that similar inputs produce entirely distinct hash values.
7. **Deterministic and Repeatable**: Hash functions should produce the same hash value for the same input every time it is calculated.

Common uses of hash functions include:

1. **Data Integrity**: Hash functions are used to verify the integrity of data during transmission or storage. By comparing the hash value of the received data with the original hash value, you can detect any changes or corruption in the data.
2. **Password Storage**: Hash functions are employed to securely store passwords. Instead of storing plain text passwords, systems store their hash values. When a user logs in, the system hashes the entered password and compares it to the stored hash.
3. **Digital Signatures:** Hash functions are a critical component of digital signatures. A digital signature is created by hashing the data to be signed and then encrypting the hash value with a private key.
4. **Cryptographic Applications:** Hash functions are used in various cryptographic protocols and applications, including blockchain technology (e.g., Bitcoin), certificate authorities, and secure communications.
5. **Data Deduplication**: Hash values can be used to identify duplicate data and eliminate redundant copies, saving storage space.

How Cryptography Works?

1. It works by using mathematical algorithms to convert information into a form that is unreadable without the correct key. Here's a simplified overview:
2. **Encryption:** This process transforms plaintext (original data) into ciphertext (unreadable data) using an encryption algorithm and a secret key.
3. **Decryption:** To revert ciphertext back to plaintext, the recipient uses a decryption algorithm and the same secret key.

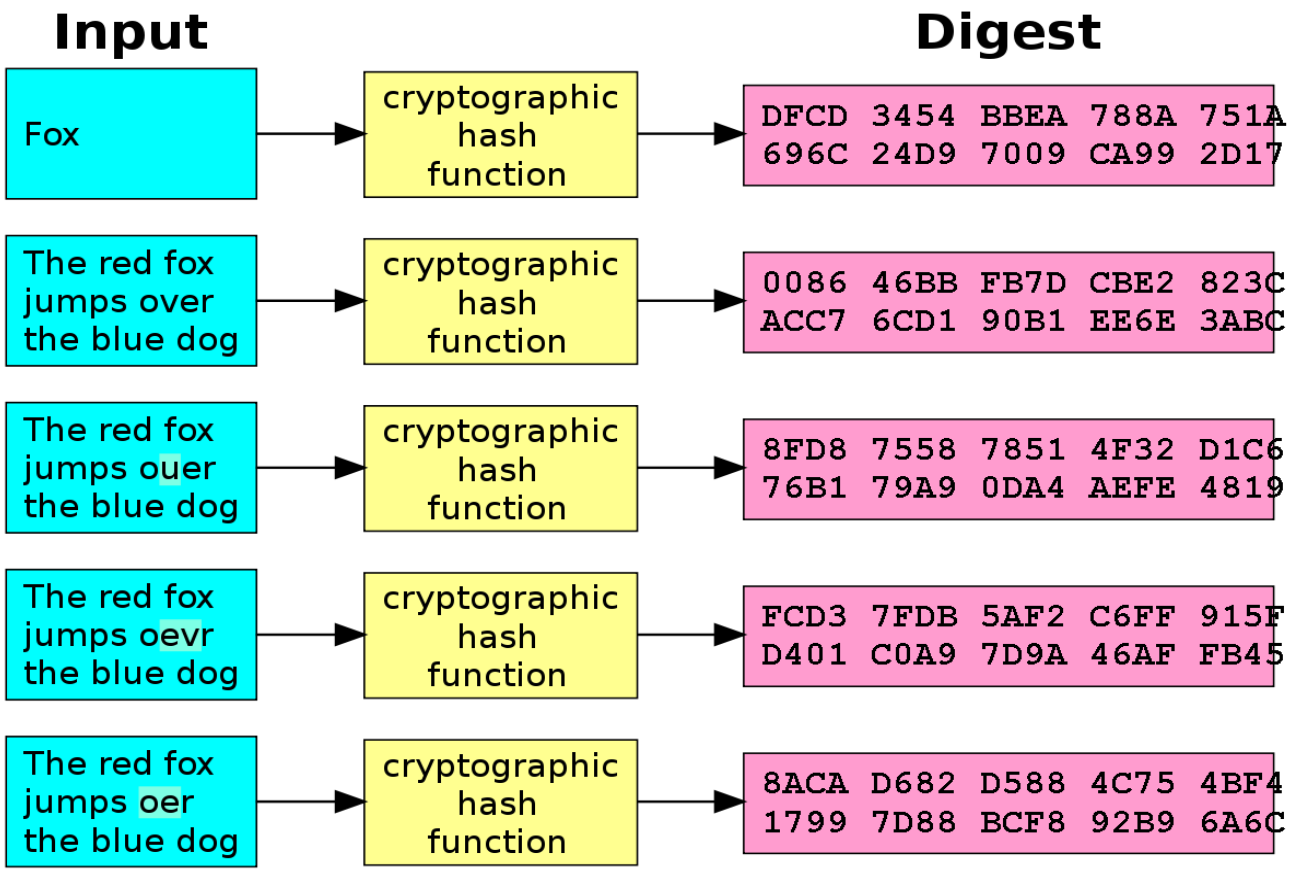
4. **Key Management:** The security of cryptographic systems relies on keeping the encryption keys secret. There are symmetric cryptography (same key for both encryption and decryption) and asymmetric cryptography (public and private key pairs).

5. **Security:** Cryptographic algorithms are designed to be computationally difficult to reverse without the key, ensuring data confidentiality.

6. **Authentication**: Cryptography can also be used for verifying the authenticity of a message sender or ensuring data integrity (that it hasn't been tampered with).

7. **Use Cases**: Cryptography is used in various applications, including securing online transactions (SSL/TLS for web), securing data at rest (e.g., hard drive encryption), and digital signatures for document authenticity.

8. **Cryptanalysis**: This is the science of breaking encrypted messages without knowing the key. Strong encryption algorithms make this extremely difficult and time-consuming.



- **Digital Signature**

Digital signatures are mathematical techniques used to verify the authenticity and integrity of me ssages or data. It provides a way for the senders or creators of the information to prove that they are the creators of the correct content and that the content has not been tampered with during tran smission or storage.

Digital signature works like this:

Keys: The process starts by generating a key pair for the organization to log on. form: private ke y and public key correspond. The private key is kept secret and known only to the owner, while t he public key can be freely distributed.

Signature: When the sender wants to sign a message or document, it uses a private key to create a unique digital signature of that content. This process usually involves hashing the message to cr eate a long-term representation, and then encrypting the hash with a private key.

Delivery: The sender then sends the original message with its signature and key to the receiver. The receiver can use the sender's public key to verify the signature.

Authentication: To verify a digital signature, the receiver uses the sender's public key to decrypt the signature, which creates the original hash value. Then their own hash messages are retrieved to get another hash. If the two hashes match, it indicates that the message has not been modified and is signed by the owner of the private key.

Digital signatures provide many important security features:

Authentication: The recipient can verify the identity of the sender by confirming that the signatu re was created by the sender's private key.

Integrity: The recipient must ensure that the message or document has not been altered after it h as been signed because changes in content can make a difference.

Rejection: The sender cannot subsequently refuse to send the message because the digital signat ure provides proof of his or her participation.

Digital signatures are widely used for many purposes, including:

Email Security: To ensure that an email is sent by a verified sender and has not been altered

in transit.

Document Signing: Digitally sign contracts, legal documents and digital certificates.

Software and Firmware Verification: Verify the accuracy and integrity of software updates and firmware.

Online Business: Online security and financial transactions.

Authentication: Proving the identity of the user in the digital system.

- ## DIGITAL CERTIFICATE

1. Digital certificates in cryptography are often called digital certificates or public key ce rtificates and are an essential part of modern digital security. It plays an important rol e in ensuring the accuracy, integrity and confidentiality of information transmitted on computer networks such as the Internet. A detailed explanation of what a digital certif icate is and how it works can be found here:
2. **Digital Identity**: A digital certificate is actually a digital identity. It associates a publi c key with an entity (such as a person, organization, or website) and provides a way fo r others to verify the authenticity of that entity.
3. **Public Key**: The certificate contains the source of the public key used for encryption and digital signature. This key is public, meaning anyone can use it to encrypt data th at only the certificate owner can decrypt with the private key.
4. **Certificate Authority (CA):** Digital certificates issued by trusted third parties, usuall y called Certificate Authorities (CA), are used to establish trust in the system. These o rganizations verify the identity of the certificate holder before issuing the certificate.
5. **Certificate content:** Digital certificates usually contain the following information: Subject: The entity (such as a website or person) associated with the document certifi cate.
6. **Validity Period :** It is the working period during which the certificate is considered valid.

7. **Chain of trust:** In most cases, certificates form a chain of trust, also known as a certif icate chain or certificate hierarchy. This means that a certificate issued by one CA can be used to verify the authenticity of another certificate. The basis for this chain is usu ally a self-signed certificate from a highly trusted CA, such as the root CA.
8. **TLS/SSL:** Digital certificates are commonly used in Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols to secure communication on the web. Whe n you connect to a secure website (https://), your browser checks

One issue with public key cryptosystems is that users must be constantly vigilant to make sure they are encrypting to the correct person's key. In an environment where it is safe to freely exchange keys via public servers, man-in-the-middle attacks are a potential threat. In this type of attack, someone posts a phony key with the name and user ID of the user's intended recipient.

Data encrypted to and intercepted by the true owner of this bogus key is now in the wrong hands.

A digital certificate contains key information, including:

1. The public key of the certificate holder.
2. Information about the certificate holder (e.g., name, organization).
3. The digital signature of the CA, which attests to the validity of the certificate.

- ## LITERATURE REVIEW

1. This review delves into the core principles of cryptography, emphasizing the importance of encryption, decryption, and key management. It discusses symmetric-key cryptography, where a single secret key is used for both encryption and decryption, and public-key cryptography, which relies on a pair of keys, public and private, for secure communication. Key exchange mechanisms and cryptographic protocols, such as Diffie-Hellman and SSL/TLS, are also examined in detail.
2. Contemporary Applications: Cryptography has become an integral part of our digital lives, ensuring the security of online transactions, communications, and data storage. This

literature review explores its applications in securing e-commerce, online banking, and secure messaging platforms. It also discusses the role of cryptography in blockchain technology and cryptocurrencies, enabling trustless peer-to-peer transactions.

3. Emerging Trends:The review highlights emerging trends in cryptography, including post-quantum cryptography, which addresses the potential threat posed by quantum computers to current encryption methods. Additionally, it explores homomorphic encryption, which allows computations on encrypted data without revealing the data itself, opening new possibilities for privacy-preserving data analytics.

❖ TABLE OF CONTENTS

❖ COLLEGE INFORMATION

Hansraj College, is become co-educational constituent college of the University of Delhi in 1978. The college was founded on July 26, 1948, in memory of Maharshi Dayanand Saraswati and Mahatma Hansraj, by D.A.V. College Managing Committee, Dr. Rama (Principal of Hansraj College) a Master of Philosophy (M.Phil) , took over as chairman of the college governing body in 1978. The college had been ranked as the 12th best college in India as per the National Institutional Ranking Framework India Rankings 2023. In 2022, Hansraj College ranked 12th among colleges across India.

- **INTERNSHIP DESCRIPTION**
- Collaborate with the cryptography team to develop and analyze cryptographic algorithms.
- Apply mathematical principles to design and evaluate security protocols.
- Research and implement advanced number theory, algebraic structures, and other mathematical concepts for encryption.
- Assist in the identification and resolution of security vulnerabilities.

- Contribute to the development of mathematical models to improve encryption efficiency and robustness.
- Participate in team discussions and share insights on emerging cryptographic trends.

❖ INTERNSHIP OBJECTIVE

1. I am seeking an internship opportunity in the field of cryptography to further my understanding of this critical area of information security and to contribute to real-world cryptographic projects. My objective is to gain hands-on experience, develop practical skills, and apply the knowledge I have acquired during my academic studies in a professional setting.

2. **Skill Development:** My primary goal is to enhance my proficiency in cryptographic algorithms, protocols, and tools. I aim to gain practical experience in implementing encryption and decryption processes, as well as understanding key management and cryptographic best practices.

3. **Real-World Application:** I aspire to work on practical cryptographic projects that address real-world security challenges. Whether it's developing secure communication protocols, analyzing encryption vulnerabilities, or contributing to the design of cryptographic solutions, I am eager to apply my knowledge to solve complex problems.

4. **Collaboration:** During my internship, I aim to collaborate with experienced professionals in the field. I want to learn from their expertise, engage in knowledge sharing, and actively contribute to a team's success in developing secure systems and applications.

5. **Quantum Cryptography:** Given the growing concern about the potential impact of quantum computing on current encryption methods, I am particularly interested in exploring and gaining insight into post-quantum cryptography. I hope to work on projects that address the challenges posed by quantum computing threats.

6. **Research and Innovation:** Cryptography is an ever-evolving field, and I aspire to contribute to its advancement through research and innovation. I look forward to working on research projects that explore novel cryptographic techniques or address emerging security issues.

7. **Practical Problem-Solving:** I aim to gain experience in identifying security vulnerabilities and devising practical solutions. Whether it involves analyzing cryptographic protocols for weaknesses or participating in penetration testing exercises, I am eager to contribute to enhancing the security posture of organizations.

1. ## REQUIREMENT

2. The introduction in a document or presentation on cryptography serves as a critical foundation for the understanding of the subject matter. It should effectively capture the reader's or audience's attention while providing essential context and setting the stage for what follows. Here are the key requirements for a strong introduction to cryptography:

3. **Engagement and Hook:** Begin with a captivating statement, question, anecdote, or fact that draws the reader or audience into the topic. This could be a historical tidbit, a recent cybersecurity incident, or a thought-provoking question related to information security.

4. **Definition and Explanation:** Clearly define what cryptography is in simple terms, emphasizing that it is the science and art of securing information through encryption and decryption techniques. Provide a concise explanation of its significance in today's digital world, emphasizing the need for confidentiality, integrity, and authenticity.

5. **Historical Context:** Briefly touch upon the historical evolution of cryptography, highlighting key milestones or breakthroughs. Mention early methods such as the Caesar cipher or the Enigma machine to showcase its ancient roots and its role in pivotal moments in history.

1. **Relevance in the Digital Age:** Explain why cryptography is especially relevant in the modern digital age. Discuss the proliferation of digital data, the rise of online communication and transactions, and the need to protect sensitive information in an interconnected world.
2. **Security Challenges:** Acknowledge the ever-present security challenges, including cyber threats, data breaches, and the potential impact of emerging technologies like quantum computing on current encryption methods. This highlights the ongoing importance of cryptography.

❖ CONCLUSION

Cryptography is the science of securing digital communication and data. It involves techniques such as encryption and decryption to protect information from unauthorized access. Public key cryptography allows for secure communication without sharing secret keys, and digital certificates verify the authenticity of public keys and entities.

ASYMMETRIC IN CRYPTOGRAPHY

Internship report submitted

In partial fulfillment of the requirement for the degree of

Bachelor of Science
In
Mathematics

COURSE

B . Sc (H) Mathematics
By

AMRIT AGARWAL (2103110004)

Under the guidance of

DR. ARVIND KUMAR

(HANSRAJ COLLEGE)

Department of Mathematics

School of Basic and Applied Science

K. R. Mangalam University, Gurugram - 122003

July-2023

DECLARATION

We declare that this written submission represents our ideas in our own words and where other's ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all the principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will because for disciplinary action by the Institute and canal so evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed. We further declare that if any violation of the intellectual property right or copyright, my supervisor and university should not be held responsible for the same.

Amrit Agarwal

AMRIT AGARWAL Student Name	**2103110004** (Roll No.)	**AMRIT AGARWAL** (Signature)

Place: **K.R. Mangalam University**

Date: **05th August 2023**

Hansraj College
University of Delhi
Mahatma Hansraj Marg, Malka Ganj
Delhi – 110007

हंसराज महाविद्यालय
दिल्ली विश्वविद्यालय
महात्मा हंसराज मार्ग, मलकागंज
दिल्ली 110007

Date 29/09/2023

Certificate

This is to certify that **Amrit Agarwal** a student of **K R Mangalam University Gurugram** has carried out internship on the topic "**Cryptography and its applications**" at **Hansraj College, University of Delhi, Delhi 110007** as part of **B.Sc (H) Mathematics** Degree requirement. The student carried out his work sincerely during the period from **4 July to 5 Aug 2023** and completed the training successfully.

(Dr Arvind)
Professor
Department of Mathematics
Hansraj College

E-mail: principal_hrc@yahoo.com Tel: +91-11-27667458, +91-11-27667747

ACKNOWLEDGEMENT

"Enthusiasm is the feet of all progress, with it there is accomplishment and Without it there are only slits alibis."

Acknowledgment is not a ritual but is certainly an important thing for the successful completion of the project. At the time when we were made to know about the project, it was really tough to proceed further as we were to develop the same on a platform, which was new to us. More so, the coding part seemed tricky that it seemed to be impossible for us to complete the work within the given duration.

We really feel indebted in acknowledging the organizational support and encouragement received from the university.

The task of developing this system would not have been possible without the constant help of our faculty members and friends. We take this opportunity to express our profound sense of gratitude and respect to those who helped us throughout the duration of this project.

We express our gratitude to our supervisors Dr. Mina Kumari for giving their valuable time and guidance to us.

Place: - **K.R. Mangalam University** **AMRIT AGARWAL**

Date: - 05th August 2023 **Name of Student**

ABSTRACT

Cryptography plays a role, in ensuring information security in the digital era. It is a field that involves a range of techniques and principles aimed at safeguarding data from unauthorized access, tampering or interception. In this abstract we will explore the scope of cryptography delving into its origins core principles, diverse encryption methods, practical applications, in real world scenarios and the ongoing challenges it encounters amidst rapid technological advancements.

Cryptography has a rich history dating back to ancient civilizations. Initially, it was mainly used for secret communications between military and political leaders. The oldest known form of encryption is the Caesar cipher, which was used by Julius Caesar to encrypt messages. Over the centuries, cryptography has evolved from simple substitution ciphers to more complex methods such as the Visionary cipher.

In modern times, encryption was revolutionized during World War II, when the Allied forces developed the Enigma machine to decipher Nazi communications. This was the beginning of a more systematic and mathematical approach to cryptography.

TABLE OF CONTENTS

INTRODUCTION

In cryptography, symmetric encryption is a fundamental technique used to secure data by using a shared secret key for both encryption and decryption. This method involves using the same key for both the sender and the receiver, making it crucial to keep the key secret and secure. Let's delve into an introduction to symmetric encryption and its significance in cryptography.

Symmetric encryption, also known as secret-key encryption or private-key encryption, is a cryptographic method where the same key is used for both encrypting plaintext (original data) and decrypting ciphertext (encrypted data). This key is shared securely between the sender and the receiver. The process involves applying mathematical algorithms to the plaintext using the key to produce the ciphertext, and then applying the same algorithms in reverse using the key to retrieve the original plaintext.

The importance of asymmetric in cryptography cannot be overstated. Mathematics serves as the bedrock upon which secure communication and data protection are built. Here are key reasons highlighting its role:

1. **Key Management:** Since the same key is used for both encryption and decryption, the security of the key is of utmost importance. If an unauthorized party gains access to the key, they can decrypt the data. Therefore, secure key management practices are crucial.
2. **Efficiency:** Symmetric encryption is typically faster and requires less computational resources compared to asymmetric encryption methods (such as RSA or ECC), which involve separate keys for encryption and decryption. This efficiency makes symmetric encryption suitable for securing large amounts of data.
3. **Data Confidentiality:** The primary purpose of symmetric encryption is to ensure the confidentiality of data. By encrypting data before transmission and decrypting it at the receiver's end, sensitive information remains secure even if intercepted by unauthorized parties.
4. **Algorithm Types:** There are various symmetric encryption algorithms, ranging from older ones like DES (Data Encryption Standard) to more modern and secure ones like AES (Advanced Encryption Standard). AES is widely adopted and considered highly secure for a variety of applications.

1. **Challenges:** One of the main challenges with symmetric encryption is securely exchanging the key between sender and receiver. If a third party intercepts the key during transmission, the security of the encrypted data can be compromised. Techniques such as key exchange protocols and using secure channels (e.g., TLS/SSL) address this issue.
2. **Perfect Forward Secrecy (PFS):** Symmetric encryption alone does not provide Perfect Forward Secrecy, which ensures that even if one key is compromised, past communications cannot be decrypted. This is one of the reasons asymmetric encryption is often used alongside symmetric encryption in some cryptographic protocols.

- **ROLE OF ASYMETRIC IN CRYPOTOGRAPHY**

The role of asymmetric in cryptography is pivotal, as it provides the foundation for creating secure communication and data protection mechanisms. Mathematical concepts and principles form the basis for various cryptographic techniques:

1. **Key Distribution and Management:** Asymmetric cryptography solves this problem by allowing the public key to be widely distributed while keeping the private key secret. This means that anyone can encrypt data using the recipient's public key, but only the recipient possessing the corresponding private key can decrypt the data.
2. **Digital Signatures:** Asymmetric cryptography enables the creation of digital signatures, which provide authentication, integrity, and non-repudiation. A digital signature is created by encrypting a hash of the message using the sender's private key. This process ensures that the message has not been tampered with and that it originated from the claimed sender.
3. **Secure Communication:** Asymmetric cryptography facilitates secure communication in scenarios where parties have not previously exchanged a secret key. For example, in secure email communication, users can encrypt messages using the recipient's public key, ensuring that only the recipient can decrypt and read the message using their private key.
4. **Key Exchange:** Asymmetric cryptography allows for secure key exchange protocols, such as Diffie-Hellman key exchange, which enable two parties to establish a shared secret key over an insecure channel without directly transmitting the key. This property

is crucial for establishing secure connections in protocols like TLS/SSL used for secure web.

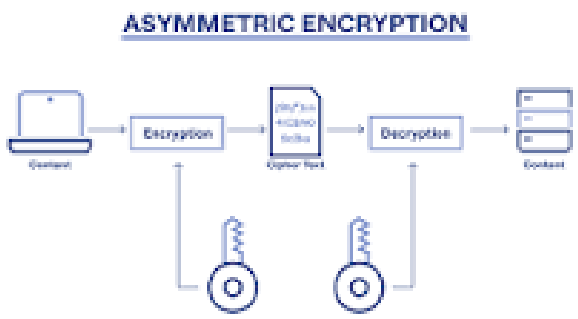
5. **Encryption and Decryption:** Asymmetric cryptography also supports encryption and decryption. While asymmetric encryption is generally slower than symmetric encryption, it is often used for key exchange and establishing secure channels.
6. **Key Revocation:** Asymmetric cryptography allows for easier key revocation and management. If a private key is compromised or no longer trusted, it can be revoked without affecting the security of other communication channels.
7. **Perfect Forward Secrecy (PFS):** Asymmetric cryptography, when used in conjunction with symmetric cryptography, can provide Perfect Forward Secrecy. This means that even if an attacker compromises a private key, they cannot decrypt past communications that were secured using separate symmetric keys.

- **INTRODUCTION OF ASYMETRIC CRYPTOGRAPHY:-**

Definition: Asymmetric cryptography is used to exchange the secret key to prepare for using symmetric cryptography to encrypt information. In the case of a key exchange, one party produce the secret key and encrypts it with the public key of the recipient. The recipient can decrypt it with their private key.

How Does Asymmetric Cryptography Work?

I. **Registration:** The user and the sender have connected with an official entity that generated both public and private keys.
II. **Lookup:** The sender scours a public-key directory for the recipient's public key information.
III. **Encrypt:** The sender creates a message, encrypts it with the recipient's public key, and sends it.
IV. **Decode:** The recipient uses the private key to unscramble the message.
V. **Reply:** If the recipient wants to respond, the process moves in reverse.



- **LITERATURE REVIEW**

A literature review in the field of cryptography would typically involve an in-depth examination and analysis of existing research, studies, publications, and scholarly articles related to cryptographic concepts, techniques, algorithms, and their applications. Below is an overview of some key topics and themes that could be covered in a literature review on cryptography:

1. **Historical Evolution of Cryptography:** Explore the historical development of cryptography, from ancient encryption methods to modern cryptographic techniques. Analyse the pivotal moments and innovations that have shaped the field over time.

2. **Cryptographic Fundamentals:** Review the foundational principles of cryptography, including encryption, decryption, cryptographic keys, and mathematical concepts such as number theory and modular arithmetic.

3. **Symmetric Cryptography:** Investigate symmetric encryption algorithms, their working principles, and practical applications. Analyse the strengths and weaknesses of symmetric cryptography, as well as real-world use cases.

4. **Asymmetric Cryptography**: Explore asymmetric encryption techniques, including the use of public and private keys. Assess the advantages and limitations of asymmetric cryptography in secure communication and digital signatures.

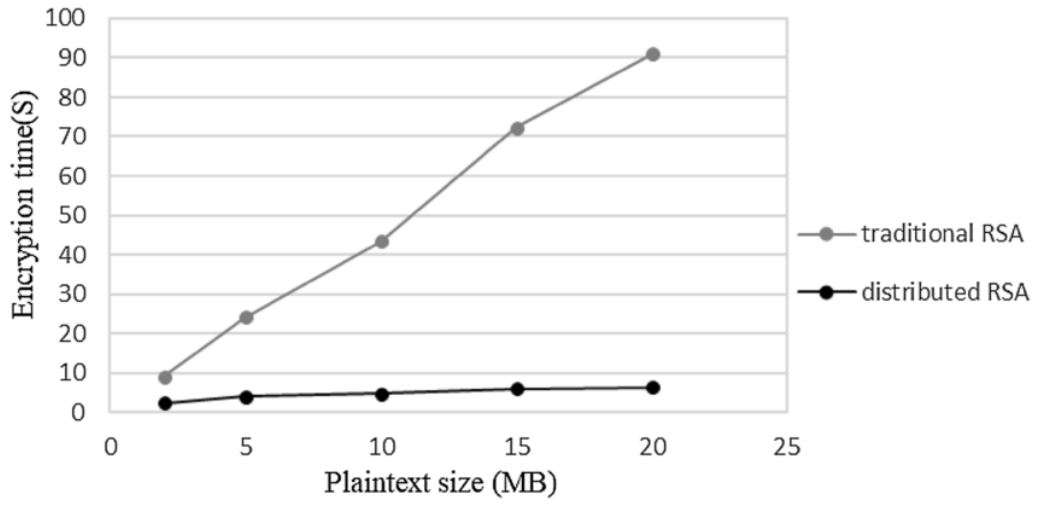
- **INTRODUCTION ON RIVEST, SHAMIR, ADLEMAN (RSA)**

RSA (Rivest-Shamir-Adleman) is one of the most widely used and influential encryption algorithms in modern cryptography. It falls under the category of asymmetric or public-key cryptography, which means it uses a pair of distinct keys: a public key for encryption and a private key for decryption. RSA is named after its inventors: Ron Rivest, Adi Shamir, and Leonard Adleman, who introduced the algorithm in 1977. The significance of RSA lies in its ability to provide secure communication, digital signatures, and key exchange in a public key infrastructure. Here's an introduction to RSA:

- **APPLICATIONS:**

1. **Secure Communication:** RSA is commonly used to secure communication between parties over insecure networks. Users can encrypt messages using the recipient's public key, ensuring that only the recipient with the corresponding private key can decrypt and read the message.
2. **Digital Signatures:** RSA enables the creation of digital signatures, providing authentication, integrity, and non-repudiation. The sender uses their private key to sign a message, and the recipient can verify the signature using the sender's public key.
3. **Key Exchange:** RSA can be used to establish a shared symmetric key between two parties using the Diffie-Hellman key exchange protocol. This shared key can then be used for faster symmetric encryption.

GRAPH RELATED TO Rivest, Shamir, Adleman (RSA)



- **ELLIPTIC CURVES CRYPTOGRAPHY (ECC)**

Elliptic curve cryptography (ECC) is a branch of public-key cryptography that utilizes the properties of elliptic curves to provide secure communication, digital signatures, and other cryptographic functionalities. Elliptic curves are mathematical objects defined by a set of points that satisfy certain algebraic properties. ECC offers a high level of security with relatively small key sizes compared to traditional RSA and other asymmetric encryption methods. Here's an introduction to elliptic curves and their significance in cryptography:

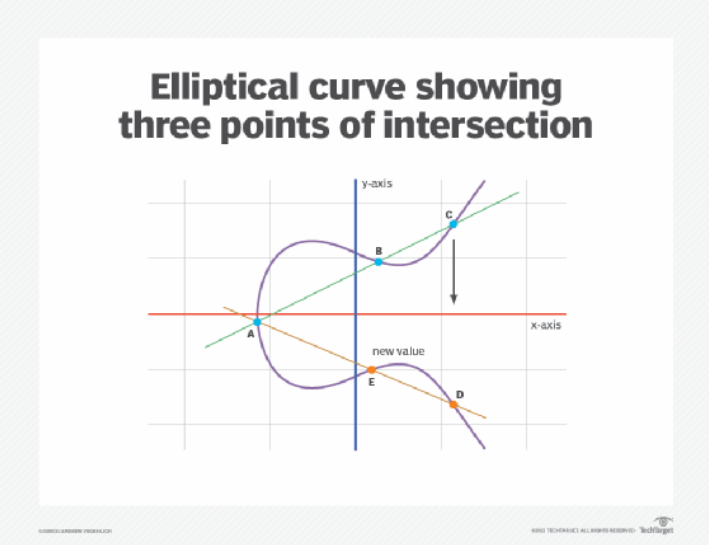
Elliptic Curves: An elliptic curve is defined by an equation of the form:

$$y\text{^}2 = x\text{^}3 + ax + b$$

Where:

- x and y are coordinates on the curve.
- a and b are constants that define the curve's shape.

GRAPH RELATED TO ELLIPTIC CURVES CRYPTOGRAPHY (ECC)



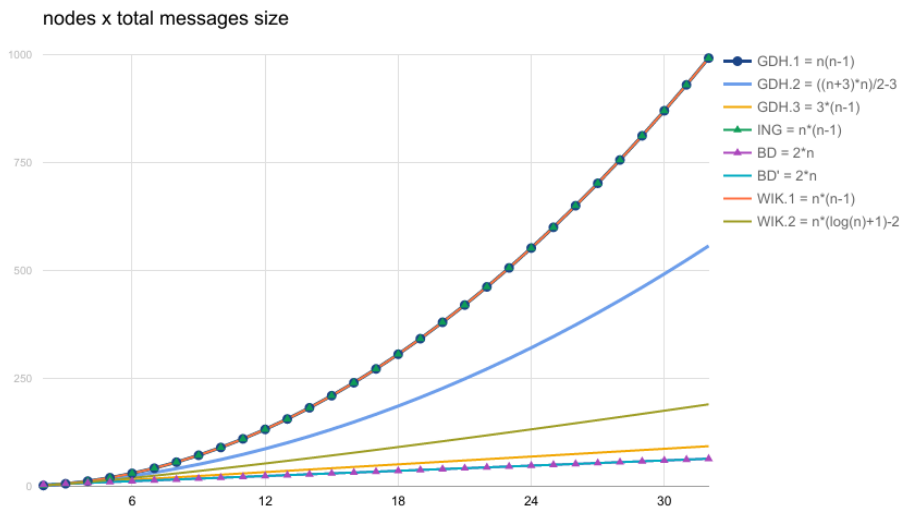
- **DIFFIE-HELLMAN KEY**

The Diffie-Hellman key exchange is a foundational cryptographic protocol that allows two parties to securely establish a shared secret key over an insecure communication channel. This shared key can then be used for symmetric encryption to protect subsequent communication. The protocol was introduced by Whitfield Diffie and Martin Hellman in 1976.

- **ADVANTAGES:**

1. **Key Exchange Without Prior Communication:-** Diffie-Hellman enables secure key exchange even when the parties have never communicated before. This is crucial for establishing secure communication in scenarios where pre-shared keys are not feasible.
2. **Perfect Forward Secrecy (PFS):** Diffie-Hellman provides Perfect Forward Secrecy, meaning that even if a long-term private key is compromised in the future, past communications protected by session keys are still secure.
3. **Independence of Communication Channel:** The security of Diffie-Hellman does not depend on the secrecy of the communication channel itself.

GRAPH RELATED TO DIFFIE-HELLMAN KEY



❖ TABLE OF CONTENTS

❖ COLLEGE INFORMATION

Hansraj College , is become co-educational constituent college of the University of Delhi in 1978. The college was founded on July 26, 1948, in memory of Maharshi Dayanand Saraswati and Mahatma Hansraj, by D.A.V. College Managing Committee, Dr. Rama (Principal of Hansraj College) a Master of Philosophy(M.Phil) , took over as chairman of the college governing body in 1978. The college had been ranked as the 12th best college in India as per the National Institutional Ranking Framework India Rankings 2023. In 2022, Hansraj College ranked 12th among colleges across India.

❖ INTERNSHIP DESCRIPTION

- Collaborate with the cryptography team to develop and analyze cryptographic algorithms.
- Apply mathematical principles to design and evaluate security protocols.
- Research and implement advanced number theory, algebraic structures, and other mathematical concepts for encryption.
- Assist in the identification and resolution of security vulnerabilities.
- Contribute to the development of mathematical models to improve encryption efficiency and robustness.
- Participate in team discussions and share insights on emerging cryptographic trends.

❖ Overview of internship experience

During this internship, I had the opportunity to dive into the fascinating world of cryptography, a field that focuses on creating secure communication and data protection mechanisms. My internship took place at a leading company in the field of cybersecurity and cryptography solutions.

• INTERNSHIP OBJECTIVE

1. **Understanding Cryptographic Fundamentals:** Gain a deep understanding of the core principles and concepts of cryptography, including encryption, decryption, cryptographic keys, hashing, and digital signatures.
2. **Cryptography in Action:** Learn to apply cryptographic techniques to practical security scenarios, including secure communication, data protection, and authentication. Study and analyze various cryptographic algorithms, both symmetric and asymmetric, including AES, RSA, and ECC.
3. **Vulnerability Analysis and Mitigation:** Learn how to identify potential vulnerabilities and weaknesses in cryptographic implementations. Explore techniques for securing cryptographic systems against attacks and threats.
4. **Research and Innovation:** Engage in research activities related to cryptography, staying updated on the latest developments and emerging trends in the field. Contribute to ongoing research projects aimed at advancing the state of the art in cryptography.
5. **Documentation and Communication:** Develop strong documentation skills to record your research findings, experiments, and project work. Practice clear and effective communication of cryptographic concepts and solutions to both technical and non-technical stakeholders.

• REQUIREMENT

1. **Education:** A Ph.D. in computer science, mathematics, or a related field with a focus on cryptography is often preferred. A master's degree may be acceptable for some positions.

2. **Experience:** Significant research experience in cryptography, with a track record of

publications in reputable conferences or journals.

3. **Skills:** Proficiency in mathematics, particularly number theory, algebra, and discrete mathematics. Strong programming skills in languages like C/C++, Python, or Java. Knowledge of cryptographic algorithms, protocols, and cryptographic libraries.

- **BENEFITS:**

1. **Data Confidentiality:** Cryptography ensures that sensitive information remains confidential by transforming it into an unreadable format (ciphertext). Only authorized parties with the appropriate decryption keys can access and decipher the data. This benefit is crucial for protecting personal and sensitive data from unauthorized access.

2. **Data Integrity:** Cryptographic techniques help maintain the integrity of data by detecting any unauthorized changes or tampering. Hash functions, in particular, are used to generate fixed-size values (hashes) for data, and even a small alteration in the data results in a significantly different hash value, alerting users to potential tampering.

3. **Authentication:** Cryptography enables authentication, allowing individuals and systems to verify the identity of parties involved in communication or transactions. Digital signatures, for example, confirm that a message or document originated from a specific sender and has not been altered during transmission.

➢ CONCLUSION

In the ever-evolving landscape of the digital age, where information flows freely over networks and data is the lifeblood of modern society, the importance of cryptography cannot be overstated. Cryptography is a steadfast guardian, protecting sensitive information, ensuring data integrity, and protecting the foundations of trust and security in our interconnected world. As we conclude our exploration of this important area, some key takeaways emerge.