Vol 4, Issue 8, 2021 **Impact Factor: 5.355** DOI: https://doi.org/10.31426/ijamsr.2021.4.8.4616

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Applications of Composite Numbers in Cryptography and Security

Dr. Deepali Parashar

Principal, Bharathi College of Education,
Kandri, Mandar, Ranchi, Jharkhand

ABSTRACT

Composite numbers, which are integers greater than one that can be factored into smaller integers, are fundamental to cryptographic systems and information security. Their applications span a wide range of cryptographic protocols and algorithms, demonstrating their critical role in securing digital communications and protecting sensitive data. One of the most prominent uses of composite numbers is in the RSA algorithm, a public-key cryptographic system that relies on the difficulty of factoring large composite numbers to ensure security. In RSA, two large prime numbers are multiplied to create a composite modulus used in both public and private keys. The challenge of factorization provides robust protection against unauthorized access. Composite numbers are also significant in Elliptic Curve Cryptography (ECC), where they influence the design of finite fields and elliptic curves, optimizing performance and security. The Discrete Logarithm Problem (DLP), central to cryptographic protocols like Diffie-Hellman and ElGamal, also relies on the difficulty of computing discrete logarithms in groups of composite order, adding an additional layer of security. Furthermore, composite numbers are utilized in Public Key Infrastructure (PKI) for key generation and certificate management, ensuring secure communication and identity verification. They also enhance the complexity and effectiveness of zero-knowledge proofs, hash functions, and random number generators (RNGs), contributing to data integrity and security. Overall, composite numbers are integral to modern cryptographic systems, underpinning various methods and protocols that safeguard digital information.

Keywords: RSA Algorithm, Elliptic Curve Cryptography, Discrete Logarithm Problem

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Introduction

Composite numbers, which are integers with more than two positive divisors, play a pivotal role in modern cryptography and security. Their unique mathematical properties are harnessed in various cryptographic algorithms to safeguard digital communication and data integrity. One of the most notable applications is in RSA encryption, where large composite numbers, formed by multiplying two prime numbers, are central to public key cryptosystems. The difficulty of factoring these large composites underpins the security of RSA, making it a cornerstone of secure digital transactions. Additionally, composite numbers are instrumental in public key infrastructure (PKI) systems and digital signature algorithms, where they contribute to key generation, authentication, and data verification. Key exchange protocols, such as Diffie-Hellman, also rely on the properties of composite numbers to establish secure communication channels. While elliptic curve cryptography (ECC) uses different mathematical frameworks, composite numbers still influence its parameter settings. Hash functions and other cryptographic mechanisms often utilize modular arithmetic involving composite numbers to ensure data integrity and security. Thus, composite numbers are fundamental to a wide range of cryptographic techniques, enabling robust protection of information in our increasingly digital world [1].

Review Of Literature

Gunathilake, (2020) Lightweight cryptography is a novel approach to minimize the high resource requirements of traditional cryptography, making it ideal for the Internet of Things (IoT) environment. IoT devices are limited in physical size, internal capacity, RAM/ROM storage, and data rates, and are often battery-powered, requiring efficient energy use. Existing cryptographic methods are too resource-intensive for IoT, leading to the development of lightweight cryptographic algorithms. Despite these efforts, achieving robustness against evolving IoT threats remains challenging. This study provides a comprehensive survey of lightweight cryptography, including its development, advancements, parametric limitations, research progress, and future enhancements.

Sahari, & Boukemara, I. (2018). A unique three-dimensional chaotic map is proposed by us in this study. This map is created by connecting the piecewise map with the logistic map. We have been able to develop and explore a novel chaotic pseudo-random number generator (CPRNG) thanks to this map, which has good qualities such as a high unpredictability, a high complexity, and a very long period. In addition to displaying a uniform distribution, the pseudo-random numbers that were generated are able to successfully pass the NIST SP 800-22 randomness tests suite examination. Furthermore, a colour picture encryption application is given, in which the encryption key is highly connected with the plain image, and it is then used to carry out the confusion and diffusion phases. This application is presented in the area of colour image encryption. In addition, the capability of increasing the size of our map has an effect on the complexity of the system. It also increases the size of the key space, which results in our cryptosystems being more effective and secure. In addition to this, we provide a number of statistical tests and computer simulations that demonstrate that the suggested method has a high degree of security.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Damaj, I., & Kasbah, S. (2018). The strengthening of the synergy between hardware and software has garnered a lot of attention in recent years due to the richness of today's hardware designs. The growing interest in unified methods has cleared the path for the development of new frameworks that focus on the co-design of hardware and software. In this study, it is shown that a unified statistical framework is capable of correctly classifying algorithms on the basis of a combination of the heterogeneous properties of their software and hardware implementations. The framework that has been presented generates indications that may be customised for any hybridisation of processing systems and can be contextualised for any field of application. The framework is used in the development of the Lightness Indicator System (LIS), which is a case study that aims to target a collection of cryptographic algorithms that are known to be small and lightweight in the existing body of research. Field Programmable Gate Arrays (FPGAs) of the highest quality and multi-core CPUs of the most recent generation are the goals of the LIS. In addition to a comprehensive performance analysis and assessment, the work that is being given also contains a generic benchmark model that helps with the presentation of the framework in a comprehensible manner.

Zargar et al (2017). Elliptical Curve Cryptography, sometimes known as ECC, is now one of the most popular buzzwords in the field of network security. One of the most effective methods of cryptography, it makes it possible to safeguard both our personal and professional information as it is sent over the network. In the course of our day-to-day lives, the need for the exchange of data has drastically expanded. Our desire to be a "know-it-all" is fuelled by our need to be current on all of the happenings in the surrounding area. As a result of the proliferation of social networking, individuals are able to maintain constant connections. They create their own accounts on social media platforms and then utilise those profiles to connect with one another by sharing information throughout the network. It is become an irreplaceable component of our everyday lives. In order to avoid attacks that might result in unauthorised access to our data, abuse of our data, or alteration of our data, as well as to ensure privacy over the network, the necessity to secure that data has also risen. Furthermore, this is necessary in order to prevent assaults. For this reason, the data must be sent in a manner that ensures only the sender and the recipient are able to comprehend it, and that no other users on the network are able to interpret it. The process is accomplished by the use of encryption and decryption techniques, in which our data is altered in such a manner that it is rendered incomprehensible to all individuals, until it is reverted to its initial form in order to get comprehension from it. We are equipped with a wide variety of methods for doing the same thing. In this article, we will be covering two such strategies that span not just server and desktop computers, but also a significant number of tiny devices ranging from personal digital assistants and mobile phones to appliances and networked sensors. At the conclusion of this discussion, we will make a comparison between the approaches that is essential in order to demonstrate why ECC is superior to any other cryptographic techniques that have been developed in recent times.

Acosta et al (2017). The purpose of this article is to offer an overview of various crypto-hardware devices, with a particular emphasis on the lightweight electronic implementation of encryption and decryption techniques, hash functions, and genuine random number generators. We discuss the hardware implementation of the primary algorithms that are used in private-key cryptography,

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

public-key cryptography, and hash functions. Additionally, we discuss some significant security concerns that are associated with electronic crypto-devices. These concerns are related to side-channel attacks (SCAs), fault injection attacks, and the design countermeasures that can be taken to address these concerns. In conclusion, we will provide an overview of the hardware implementation of real random number generators. In this section, we will examine the primary electrical sources of randomness as well as the many post-processing methods that are used to enhance the statistical properties of the random sequences that are created.

Su et al (2017). Within the realm of algorithmic number theory, one of the most fundamental computations is known as modular inversion. When it comes to cryptosystems, this calculation takes a significant amount of time since the modulus is often a very high number. It would be unreasonable to expect some devices, such as mobile devices and IC cards, which have limited computational capabilities, to be able to carry out a calculation that takes so much time. In the present study, we examine the means by which the inversion modulo a large composite number may be outsourced in a safe manner. The Chinese Remainder Theorem (CRT) serves as the foundation for our safe outsourcing method, which we build for the purpose of inversion modulo a big composite number with two prime components that are understood by the client. Our approach preserves not only the confidentiality of the number but also the confidentiality of the modulus, in addition to the modular inversion of the number. A probability of one indicates that we are able to confirm that the result is accurate. In the past, the difficulty of modular inversion for a modulus of l bits was traditionally written as O(l3). With the help of the cloud, our technique brings the complexity of the client side down to O(l2), which is much reduced. In addition, we demonstrate the safety of our approach by using the one-malicious version of two untrusted software models (the one-malicious model). A number of tests are carried out in order to establish the validity and the applicability of the algorithm that we have devised. A demonstration is provided in the appendix that demonstrates how our suggested technique may be expanded and used in the production of secret keys using the RSA algorithm on devices with limited resources.

Kumar, M. G. V., & Ragupathy, U. S. (2016, March). Applications that run on the internet are expanding and increasing at a very rapid rate. Considering the rapid advancement of technology, the work of ensuring the safety of data transmission via the internet is becoming more difficult to do. Cybercriminals break into the system and utilise the information for their own personal gain. Cryptography is used to guarantee the safety of the covert and secure communication in order to minimise the occurrence of these undesired activities. The data that has been encrypted is not only difficult to understand, but it is also rather simple to identify. The implementation of robust encryption algorithms and appropriate key management strategies for the systems will be of great assistance in accomplishing the goals of data integrity, authentication, and secrecy. Several different encryption techniques, both symmetric and asymmetric, have been put under the microscope in this study endeavour. For the purpose of cryptography, a literature review has been conducted, which included the incorporation of significant publications concerning data encryption based on performance criteria (security and time limitations). Observation and potential work for the future have been highlighted as a result of this.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Gu, L., & Zheng, S. (2014). Several nonabelian algebraic structures have been built on the stage of current cryptography in order to defend against assaults that are known to be carried out by quantum algorithms. A significant comparison between the integer factorisation issue and the factorisation problem over nonabelian groups was recently provided by Baba and colleagues on the basis of their work. In this study, we first offer three constructions of cryptographic primitives based on these newly proposed conjugacy systems: encryption, signature, and signcryption. These constructions are based on numerous conjugated issues that are linked to the factorisation problem over nonabelian groups. As part of this presentation, we also provide examples of how our idea may be implemented, as well as an analysis of its performance.

Pardeshi et al (2013). Steganography and cryptography are the two methods of secret writing that are now accessible, as stated by the new age. By embedding data in other digital media, such as an image or audio file, steganography has the ability to conceal the presence of a message. Cryptography, on the other hand, is able to turn data into cypher text, which may be in a format that is unreadable to a regular user. This study focusses on data concealing strategies that may be used for the purpose of ensuring the safety of data. The purpose of this research was to propose an RSA method for encryption and to embed encrypted data in a picture by using a steganographic approach that is based on DCT. In comparison to other approaches, such as LSB and modulus arithmetic steganography, the DCT-based methodology has a superior position.

Wang et al (2013). Over the course of the last several years, chaotic cryptography has been the subject of much research. Chaotic cyphers, on the other hand, have a lower level of security due to the unfavourable dynamical aspects of the chaotic systems that they are based on, which discourages their use in practical applications. The purpose of this work is to solve this problem by first presenting discriminating criteria for secure chaotic systems (SCSs), which are systems whose dynamical qualities make them helpful for the creation of secure cyphers. Following this, the research addresses a class of chaotic systems known as digital dynamical filters (DDFs), which are systems that match the requirements for SCSs. Following that, a DDF-based pseudorandom bit generator, also known as a DDF-PRBG, is developed for the purpose of building stream cyphers. The DDF and the DDF-PRBG, both of which meet the SCS requirements, are shown to have desirable cryptographic features, as shown by the results of theoretical study and simulations. As a consequence of this, the SCS criterion and the DDF reference model may be used to solve the issues that are brought about by the dynamical features of the chaotic systems that are underpinning chaotic cyphers and to enhance the safety of chaotic cyphers.

Dinur et al (2012, August). In this research, we demonstrate that a wide class of different issues have a bicomposite structure, which makes it feasible to solve them using a new kind of algorithm called dissection. This approach has much better time/memory tradeoffs than other techniques that have been known in the past. The difficulty of locating the key to various encryption systems that each have r separate n-bit keys is a classic illustration of this kind of problem. All of the preceding error-free assaults needed a time T and memory M that satisfied the equation $TM=2rn$. Even if "false negatives" are permitted, no attack could reach $TM<23rn/4$. We have developed a novel method that

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

results in the first algorithm that is error-free and discovers all of the potential keys using a smaller product of TM. For example, we have used a time of 24 seconds and a memory of 2 seconds to break the sequential execution of a block cypher with a size of 7 bits. The improvement ratio that we acquire improves in an infinite manner as r increases, and if we allow algorithms that may occasionally miss solutions, we can achieve even better tradeoffs by combining our dissection approach with concurrent collision search. This is because we know that algorithms can sometimes miss solutions. We demonstrate how to use the new dissection technique in a generic manner in order to attack hash functions with a rebound attack, to solve hard knapsack problems, and to find the shortest solution to a generalised version of Rubik's cube with better time complexities (for small memory complexities) than the best algorithms that were previously known. This is done in order to demonstrate the generality of the technique [2].

RSA Algorithm

The RSA algorithm, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is a widely used public key cryptosystem that secures digital communications through encryption and digital signatures. It relies on the mathematical difficulty of factoring large composite numbers into their prime factors. The RSA algorithm involves three primary steps: key generation, encryption, and decryption.

- Key Generation: RSA starts by selecting two large prime numbers, (p) and (q). These are multiplied to produce a composite number (n), which forms part of the public key. The totient function, (phi(n)), is computed using (p) and (q). A public exponent (e) is chosen, which is relatively prime to (phi(n)), and a private exponent (d) is calculated such that (e cdot d equiv 1 pmod{phi(n)}). The public key consists of ((e, n)), while the private key is ((d, n)).

- Encryption and Decryption: In encryption, the sender uses the recipient’s public key to convert plaintext into ciphertext. The recipient then uses their private key to decrypt the ciphertext back into plaintext. RSA's security is based on the computational difficulty of factoring the large composite number (n), making unauthorized decryption practically infeasible [3-5].

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a modern public key cryptographic system that leverages the mathematics of elliptic curves over finite fields to provide secure communication and data protection. Unlike traditional methods such as RSA, which rely on the difficulty of factoring large composite numbers, ECC’s security is based on the complexity of the Elliptic Curve Discrete Logarithm Problem (ECDLP). ECC offers comparable security with much smaller key sizes, resulting in faster computations and reduced storage and bandwidth requirements. This efficiency makes ECC particularly well-suited for resource-constrained environments such as mobile devices and embedded systems. By using elliptic curves, ECC achieves high levels of security while maintaining performance, making it a preferred choice in modern cryptographic applications, including secure email, digital signatures, and key exchange protocols [6].

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Discrete Logarithm Problem (DLP)

The Discrete Logarithm Problem (DLP) is a fundamental computational challenge in number theory and cryptography. Given a prime number (p), a primitive root (g) modulo (p), and an integer (y), the DLP involves finding an integer (x) such that (g^x equiv y pmod{p}). This problem is considered hard because, while computing (g^x) for a given (x) is efficient, deducing (x) from (g^x) requires significant computational effort. The difficulty of solving the DLP forms the basis for the security of various cryptographic protocols and systems. In cryptography, the DLP underpins the security of algorithms such as the Diffie-Hellman key exchange and the Digital Signature Algorithm (DSA). The robustness of these systems relies on the assumption that solving the DLP is computationally infeasible within a reasonable timeframe, even with advanced computational resources. This difficulty ensures that an adversary cannot easily derive secret keys or compromise encrypted communications, thus providing a strong foundation for secure cryptographic practices [7].

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is a comprehensive framework that supports the use of public key cryptography to secure communications, authenticate identities, and manage digital certificates. PKI encompasses hardware, software, policies, and procedures designed to ensure the integrity and confidentiality of digital interactions. At its core, PKI uses a combination of public and private keys to encrypt and decrypt data, where the public key is widely distributed while the private key is kept secure. The infrastructure involves several key components: a Certification Authority (CA) that issues and verifies digital certificates, a Registration Authority (RA) that handles the initial verification of identities, and a Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) for managing the status of certificates. Digital certificates, which contain a public key and the identity of the certificate holder, are issued by the CA and are used to establish trust between parties. PKI is fundamental to many security applications, including secure email, digital signatures, and secure web browsing. By providing a scalable and manageable way to issue, validate, and revoke digital certificates, PKI helps ensure that online transactions and communications are conducted securely, protecting against fraud, impersonation, and data breaches [8].

Zero-Knowledge Proofs

Zero-Knowledge Proofs (ZKPs) are cryptographic protocols that allow one party, the prover, to convince another party, the verifier, of a statement's validity without revealing any additional information beyond the truth of the statement itself. In other words, ZKPs enable the prover to demonstrate knowledge of a secret or the validity of a claim without disclosing the secret or specific details. This concept is crucial for enhancing privacy and security in various applications, such as secure authentication and blockchain technologies. ZKPs ensure that sensitive information remains confidential while proving its authenticity or correctness.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Hash Functions and Random Number Generation

- Hash Functions: Hash functions are algorithms that convert input data of any size into a fixed-size hash value or digest. They are designed to be fast, deterministic, and collision-resistant, meaning that the same input will always produce the same output, and it is computationally infeasible to find two different inputs that produce the same output. Hash functions are widely used in data integrity verification, digital signatures, and password storage, where the goal is to ensure that data has not been altered and to securely manage sensitive information.

- Random Number Generation: Random number generation involves producing a sequence of numbers that lack any predictable pattern, which is crucial for cryptographic applications. Secure random number generators (RNGs) are used to create cryptographic keys, initialization vectors, and nonces, ensuring that the outcomes are truly unpredictable and resistant to attacks. In contrast, pseudo-random number generators (PRNGs) use algorithms to produce sequences that appear random but are generated from a deterministic process. While PRNGs are useful for simulations and non-security-critical applications, secure RNGs are essential for maintaining cryptographic security [9-10].

Conclusion

Composite numbers are not merely mathematical curiosities but are essential to the functionality and security of modern cryptographic systems. Their applications in key cryptographic protocols such as RSA, ECC, and DLP demonstrate their importance in ensuring secure digital communication and protecting sensitive information. With forming the basis for encryption algorithms, influencing finite fields in ECC, and complicating discrete logarithm computations, composite numbers enhance the robustness of these systems. Additionally, their role in PKI, zero-knowledge proofs, and cryptographic primitives like hash functions and RNGs further illustrates their critical contribution to data security and integrity. The complex properties of composite numbers make them indispensable in creating secure and reliable cryptographic solutions. As digital security challenges evolve, the foundational role of composite numbers in maintaining encryption strength and computational complexity underscores their ongoing relevance and importance in safeguarding information in the digital age.

References

1. Su, Q., Yu, J., Tian, C., Zhang, H., & Hao, R. (2017). How to securely outsource the inversion modulo a large composite number. Journal of Systems and Software, 129, 26-34.
2. Kumar, M. G. V., & Ragupathy, U. S. (2016, March). A survey on current key issues and status in cryptography. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 205-210). IEEE.
3. Pardeshi, S. M., Sonawane, I. R., Punjabi, V. D., & Saraf, P. A. (2013). A Survey on compound use of Cryptography and Steganoghaphy for Secure Data Hiding. International Journal of Emerging Technology and Advanced Engineering Website, 3(10).
4. Sahari, M. L., & Boukemara, I. (2018). A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption. Nonlinear Dynamics, 94, 723-744.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

5. Dinur, I., Dunkelman, O., Keller, N., & Shamir, A. (2012, August). Efficient dissection of composite problems, with applications to cryptanalysis, knapsacks, and combinatorial search problems. In Annual Cryptology Conference (pp. 719-740). Berlin, Heidelberg: Springer Berlin Heidelberg.
6. Zargar, A. J., Manzoor, M., & Mukhtar, T. (2017). ENCRYPTION/DECRYPTION USING ELLIPTICAL CURVE CRYPTOGRAPHY. International journal of Advanced Research in computer science, 8(7).
7. Gu, L., & Zheng, S. (2014). Conjugacy systems based on nonabelian factorization problems and their applications in cryptography. Journal of Applied Mathematics, 2014(1), 630607.
8. Damaj, I., & Kasbah, S. (2018). An analysis framework for hardware and software implementations with applications from cryptography. Computers & Electrical Engineering, 69, 572-584.
9. Acosta, A. J., Addabbo, T., & Tena‐Sánchez, E. (2017). Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview. International Journal of Circuit Theory and Applications, 45(2), 145-169.
10. Wang, X., Zhang, W., Guo, W., & Zhang, J. (2013). Secure chaotic system with application to chaotic ciphers. Information Sciences, 221, 555-570.
11. Gunathilake, N. A., Al-Dubai, A., & Buchana, W. J. (2020, November). Recent advances and trends in lightweight cryptography for IoT security. In 2020 16th International Conference on Network and Service Management (CNSM) (pp. 1-5). IEEE.