International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 05 | May 2023 www.irjet.net p-ISSN: 2395-0072

CRYPTOGRAPHY ALGORITHMS FOR WEB SECURITY

Dhruv Dhiman[1], Tushar Mehta[2], Amiteshvar Singhr[3], Rahul[4], Ankit Thakur[5]

[1,2,3,4,5]*Under Graduate, University institute of engineering, Chandigarh University, Gharuan*

Abstract – *In this paper we are going to look at various cryptographic algorithms and their performance. We will discuss about the types of cryptographic algorithms, also the need of cryptography in blockchain and cloud security as they fall under cryptography for web security. We are also going to see the reasons why we need cryptography algorithms and what kind of algorithms are going to be used at what specific task and their resistance from various attacks. We will also take a look at the differences between asymmetric and symmetric cryptography.*

Key Words: Cryptography, Encryption, Decryption, Symmetric cryptography, asymmetric cryptography

1. INTRODUCTION

Cryptography has become an integral part of our daily lives in the digital age. With the increasing use of the internet, protecting sensitive data and information has become a top priority for individuals and organizations alike. Cryptographic techniques such as encryption, hashing, and digital signatures have been developed to safeguard our privacy and security online.

Encryption, for example, is used to ensure the confidentiality of data by converting plaintext into ciphertext, making it unreadable to unauthorized parties. Hashing, on the other hand, is used to ensure the integrity of data by creating a unique fingerprint or hash of the original data that cannot be reversed. Digital signatures provide a means of verifying the authenticity of data by using a private key to sign a message, which can be verified by anyone with the corresponding public key.

The importance of cryptography in web security cannot be overstated. Without it, sensitive information would be vulnerable to attacks from cybercriminals, leading to identity theft, financial fraud, and other forms of malicious activity. Cryptography provides a layer of protection that is critical for maintaining privacy and security in the digital age. In addition, cryptography has become a cornerstone of modern communication systems, such as email, messaging apps, and social media platforms. These systems rely on encryption and digital signatures to ensure that messages are secure and authentic. In government and military contexts, cryptography plays a crucial role in safeguarding classified information and national security.

The role of cryptography in privacy and security in the digital age cannot be overstated. It is essential for protecting sensitive data and information in various contexts, including online transactions, personal information storage, and government communications. As technology continues to advance, the importance of cryptography in web security will only increase, making it essential to understand and implement cryptographic techniques effectively.

2. LITERATURE REVIEW

As discussed in [3] the fundamental concepts and techniques of modern cryptography. The paper covers a wide range of topics including symmetric-key cryptography, public-key cryptography, hash functions, digital signatures, and key exchange protocols. It also discusses the security properties of these cryptographic primitives and how they can be used to build secure systems for various applications and it also provides a comprehensive introduction to modern cryptography.

The paper [5] proposes a new cryptographic system that allows for secure communication over an insecure channel without requiring the prior exchange of a secret key. The authors introduce the concept of public and private keys, where each user has a public key that can be freely shared, and a private key that is kept secret. They demonstrate how this approach can be used to solve key distribution problems and enable secure communication between parties without needing to share a secret key beforehand. The paper also discusses the potential applications of this new approach to cryptography and its implications for the security of modern communication systems. Overall, the paper is a seminal work that has had a significant impact on the field of cryptography and computer security.

In the paper [2] the writers discussed the importance of cryptographic hash functions and their properties for various applications in computer security. The paper defines the concepts of preimage resistance, second-preimage resistance, and collision resistance and explores the implications of each property for different security requirements. It also provides an overview of existing attacks on cryptographic hash functions and discusses the importance of selecting appropriate hash functions for different applications. The paper highlights the need for secure hash functions in various cryptographic protocols and systems, including digital signatures, message authentication codes, and password storage. Overall, the paper emphasises the importance of cryptographic hash functions as a fundamental building block of secure systems and provides a

comprehensive overview of the properties and implications of hash function security.

In [7] the authors discussed the importance of cryptographic hash functions as a fundamental tool for ensuring the integrity, authenticity, and confidentiality of data in various applications. The paper provides a comprehensive review of the history, properties, and applications of cryptographic hash functions, including their use in digital signatures, message authentication codes, password storage, and other cryptographic protocols. The authors also discuss the security requirements and evaluation criteria for hash functions, as well as the existing attacks and vulnerabilities that have been identified in various hash function designs. The paper highlights the importance of selecting appropriate hash functions for different applications and provides recommendations for best practices in hash function usage. Overall, the paper emphasises the crucial role of cryptographic hash functions in modern computer security and provides a useful resource for researchers, practitioners, and students in the field.

In [1] the authors discussed the revolutionary idea of using public-key cryptography for secure communication without the need of a secret key. The paper provides the concept of a trapdoor one-way function, which is a function that is easy to compute in one direction but difficult to invert without a secret key. The authors tell how this concept can be used to create a public-key encryption system and a digital signature scheme; this also enables a secure communication over an insecure channel without the exchange of key before the message. The paper also discusses the potential applications and implications of public-key cryptography for modern computer security, which includes secure communication, authentication, and key management. Overall, the paper has a significant impact on the field of cryptography and computer security and has given a way for the development of modern cryptographic protocols and systems.

In [6] the writers talk about the evaluation of the security of the Data Encryption Standard, which was at that time the most widely used cryptographic algorithm for securing sensitive data. The paper analyses the security of DES against various types of attacks, including brute-force attacks, differential cryptanalysis, and linear cryptanalysis. The author also proposes numerous modifications to the algorithm to increase its security against these attacks. The paper provides a detailed description of the DES algorithm and its cryptographic properties which include key length, substitution-permutation structure, and the Feistel network. The author analyses the security of DES against brute-force attacks and shows that its 56-bit key length is insufficient to provide enough protection against exhaustive search attacks. The author also evaluates the security of DES against differential cryptanalysis and linear cryptanalysis, two new attack techniques that were not considered during the original design of the algorithm, so paper shows that DES is vulnerable to these attacks and proposes modifications to the algorithm to increase its resistance against them. Overall, the paper highlights the importance of evaluating the security of cryptographic algorithms against new attack techniques and shows that even widely used algorithms such as DES may require modifications to remain secure over time. The paper has had a significant impact on the field of cryptography and computer security, leading to the development of new cryptographic algorithms and the adoption of stronger key lengths in modern cryptographic systems.

The main point of [4] is to provide a comprehensive review of cryptographic hash functions, which are a fundamental tool for ensuring the integrity, authenticity, and confidentiality of data in various applications. The paper discusses the history and the properties of cryptographic hash functions, and also their various applications such as digital signatures, message authentication codes, password storage, and other cryptographic protocols. The authors also evaluate the security requirements and evaluation criteria for hash functions, and also about the existing attacks and vulnerabilities that have been identified in various hash function designs and their implementation. They have also provided necessary recommendations for best practices in hash function usage and the importance of selecting appropriate hash functions for different applications. Overall, the paper discussed the crucial role of cryptographic hash functions in modern computer security, and highlights the importance of selecting appropriate hash functions for different applications.

In [8] authors discussed the development of a new public-key cryptography system which enables secure communication without the need of a shared secret key. The paper proposes the RSA encryption algorithm, which utilises the difficulty of factoring large numbers as a means of providing secure encryption and digital signature functionality. The RSA algorithm allows for secure communication over an unsecured channel by enabling public-key encryption and digital signatures, thus eliminating the need for a prior key exchange. The paper provides a detailed description of the RSA algorithm, including its mathematical research, key generation, encryption, and decryption. The authors also analyse the security of the RSA algorithm against various types of attacks, including brute-force attacks and attacks based on the mathematical properties of the algorithm. The paper also discusses the potential applications and implications of public-key cryptography for modern computer security, including secure communication, authentication, and key management.

3. BACKGROUND STUDY

Cryptography is the science of ensuring secure communication in the presence of adversaries or third parties. Its purpose is to protect information by transforming it into an unreadable form, making it accessible only to

authorized individuals who possess the corresponding decryption key. The fundamental objectives of cryptography include maintaining the confidentiality of data, ensuring its integrity, and verifying its authenticity. By employing various encryption algorithms and cryptographic protocols, cryptography plays a crucial role in safeguarding sensitive information and enabling secure digital interactions. Cryptography is indispensable in today's digital landscape due to the multitude of risks involved in information sharing, particularly online. Cybercriminals have the ability to intercept and access sensitive data like credit card details, personal identification information, and passwords. Additionally, unauthorized parties such as governments and organizations may attempt to gain access to confidential information. The purpose of cryptography is to mitigate these risks by encrypting data, rendering it incomprehensible to anyone without the corresponding decryption key. By employing cryptographic techniques, data can be safeguarded from unauthorized access and potential breaches.

There are two main types of cryptography: symmetric key cryptography and public key cryptography.

In the field of cryptographic techniques, symmetric key cryptography, also known as secret key cryptography, employs a single key for both encryption and decryption procedures. This implies that for successful communication, both participating parties must possess access to the same key. Symmetric key cryptography, renowned for its efficiency and speed, outperforms public key cryptography in these aspects. However, it necessitates careful management of the shared key to ensure its security. Public key cryptography, also referred to as asymmetric cryptography, employs a pair of distinct keys for encryption and decryption purposes. The first key, known as the public key, is openly accessible to anyone wishing to transmit a message. On the other hand, the second key, called the private key, remains confidential and exclusive to the intended recipient. When a message is encrypted with the public key, it can only be decrypted using the corresponding private key. This characteristic renders public key cryptography more secure compared to symmetric key cryptography. However, it is important to note that the computational overhead and slower processing speed are inherent trade-offs of public key cryptography.

Within these two main types of cryptography, there are many different algorithms and methods for encryption and decryption. Examples include AES, RSA, and SHA. These algorithms differ in terms of their strengths, weaknesses, and performance characteristics, and are chosen based on the specific needs of a given application or use case.

4. SECURITY CONCERNS FOR DATA

Data that we send or receive over the internet travels through a network of computers. Unfortunately, this means that there are opportunities for hackers to intercept and steal the data. To protect against this risk, it's important to implement measures to secure the data as it travels over the network. Cryptography provides a powerful set of tools for achieving this goal. By using encryption, digital signatures, and proper key management, organizations can help ensure that their sensitive data is protected from theft and tampering. Cryptography allows data to be transmitted securely, without fear of interception by hackers. This ensures the confidentiality and integrity of the data, and helps to maintain user trust in online systems and services. Even if our data is stolen, we can be sure that it is still protected due to the encryption we have performed over it.

5. METHODOLOGY

To evaluate the outcomes of different cryptography algorithms we will be understanding the differences between both the cryptography types. These will be differentiated by theoretical understanding of between the two, and that can help us understand the difference between the use case of both the types; i.e., symmetric and asymmetric cryptography.

Parameters to test evaluate:

1. Key length: This is an important factor when selecting a cryptography algorithm. Key length will determine the possible ways the data can be encrypted. The longer the key size will be the stronger will be the encryption.

2. Rounds: Rounds are a series of operations performed on data to make a more complex and secure form of output. The number of rounds performed will also determine the efficiency of algorithm and the time which it will take to encrypt the data.

3. Efficiency: Defines, how fast much resources are being consumed by the algorithm and how fast is the algorithm is performing within that environment.

4. Vulnerabilities: The function of any cryptography algorithm is to protect the data. This will tell above the ways our data can be compromised.

Using the above parameters, we can understand the use case of different algorithms and how and where to use them. Table 1 and 2 show the analysis on both symmetric and asymmetric cryptography.

Table-1: Performance and analysis on symmetric cryptography

Algorithms	AES	TripleDES	Rabbit	Blowfish
Key length (in bits)	128, 192, 256	112,168	128, 192, 256	32 - 488
Security	Very high	Moderate	Very high	Moderate
Rounds	10, 12, 14	48	Variable	16
Block size (in bits)	128	64	128	64
Vulnerabilities	None currently known	Vulnerable to certain attacks	None currently known	Known-key distinguishing attack
Applications	SSL/TLS, VPNs, disk encryption, mobile devices	Legacy systems, financial transactions	SSL/TLS, disk encryption, streaming media	VPNs, file encryption, legacy systems
Efficiency	Very efficient	Less efficient	Very efficient	Efficient

Table-2: Performance and analysis on asymmetric cryptography

Algorithms	RSA	Diffie-Hellman key exchange	Elliptic Curve Cryptography	DSA
Key length (in bits)	1024-4096	2048-3072	160-521	1024-3072
Security	Moderate	Moderate	Very high	Moderate
Algorithm	Modular exponentiation	Modular exponentiation	Elliptic curve point multiplication	Modular exponentiation with discrete logarithm
Vulnerabilities	Side-channel attacks (timing, cache, power analysis)	Man-in-the-middle (if not used with authentication)	Side-channel attacks (timing, fault injection)	Side-channel attacks (timing, power analysis)
Applications	SSL/TLS, email encryption, digital signatures	SSL/TLS, VPNs, secure communications	SSL/TLS, mobile devices, smart cards, blockchain	Digital signatures, SSH
Efficiency	Medium	Medium	High	Medium

6. OUTCOME

We have discussed several cryptographic algorithms, including symmetric algorithms such as AES, TripleDES, RC4, Rabbit, Rabbit-Legacy, and Blowfish. For each of these algorithms, we discussed their key length, security, vulnerabilities, block size, mathematical algorithm, applications, and efficiency.

We also covered several asymmetric algorithms, including RSA, Diffie-Hellman key exchange, Elliptic Curve Cryptography (ECC), and DSA. For these algorithms, we discussed their key length, security, vulnerabilities, mathematical algorithm, applications, and efficiency.

Both types of cryptographic algorithms used to secure data and communications. Each type has its strengths and weaknesses, and they are used in different scenarios based on their characteristics.

Symmetric cryptography algorithms, such as AES, TripleDES, RC4, Rabbit, Rabbit-Legacy, and Blowfish, use a single key for both encryption and decryption. They are efficient and fast, making them suitable for applications that require high-speed data processing, such as network communication and bulk data encryption. However, one of the main weaknesses of symmetric cryptography is the challenge of securely distributing and managing the shared secret key among communicating parties. If an attacker gains access to the key, they can decrypt the encrypted data. To mitigate this weakness, key management techniques like key exchange protocols and secure storage mechanisms are employed. On the other hand, asymmetric cryptography algorithms, including RSA, Diffie-Hellman, ECC, and DSA, use a pair of keys: a public key for encryption and a private key for decryption or digital signatures. Asymmetric algorithms provide secure key exchange mechanisms and are particularly useful in scenarios where two parties need to establish a secure communication channel without sharing a pre-existing secret key. They are also utilized for digital signatures, ensuring data integrity and non-repudiation. However, asymmetric algorithms are computationally more intensive and slower compared to symmetric algorithms. The key length and security of asymmetric algorithms are crucial, as shorter key lengths can be susceptible to attacks. To enhance security, longer key lengths are recommended. Additionally, protecting the private key is vital to prevent unauthorized access.

To overcome weaknesses in both symmetric and asymmetric cryptography, various measures can be implemented. Some approaches include:

1. Key Management: Implementing secure key generation, storage, distribution, and rotation mechanisms is essential to protect keys from unauthorized access or compromise.

2. Hybrid Cryptography: Combining symmetric and asymmetric algorithms in a hybrid approach can leverage the benefits of both. For example, using asymmetric cryptography for key exchange and symmetric cryptography for data encryption, achieving a balance between security and efficiency.

3. Strong Random Number Generation: Using high-quality random number generators to generate cryptographic keys helps avoid predictability and enhances the security of encryption.

4. Regular Algorithm Updates: Keeping up with the latest advancements in cryptographic algorithms and adopting updated versions can address known vulnerabilities and ensure stronger security.

Even in the field of cloud technology, where data is stored and processed remotely on servers, the significance of cryptography becomes apparent as it safeguards sensitive information from unauthorized access. By leveraging cryptographic algorithms, data can be encrypted before transmission and decrypted upon retrieval, thus ensuring confidentiality. This is especially critical in cloud environments characterized by shared infrastructure among multiple users, where data privacy is of utmost importance. Cryptography also serves to verify data integrity, guaranteeing that information remains unaltered during transit or while at rest within the cloud.

Similarly, in blockchain technology, which embraces decentralization and immutability as core principles, cryptography assumes a foundational role within its security architecture. Cryptographic algorithms are employed to fortify transactions and uphold the integrity of the blockchain network. Public-key cryptography, for instance, enables the creation of digital signatures that authenticate transactions and verify the identities of network participants. Additionally, cryptography aids in hashing transaction data, establishing connections between blocks, and forging an immutable chain of data. Through these cryptographic mechanisms, the trustworthiness and tamper-proof nature of the blockchain are ensured, enabling secure and intermediary-free transactions and data storage.

In both cloud and blockchain technologies, cryptography emerges as a vital element that protects sensitive data, guarantees privacy, verifies authenticity, and upholds the integrity of the systems. Its application within these technological domains fosters secure and trustworthy operations, addressing the inherent security challenges and enabling the seamless execution of tasks.

It is important to note that while cryptographic algorithms play a vital role in securing data and communications, their effectiveness relies not only on the algorithms themselves but also on proper implementation, key management practices, and adherence to security protocols.

REFERENCES

[1] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21, no. 2 (1978): 120-126.

[2] Rogaway, Phillip, and Thomas Shrimpton. "Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance." In *FSE*, vol. 3017, pp. 371-388. 2004.

[3] Mahabadi, Ladan. ""“Introduction to Modern Cryptography” by Jonathan Katz and Yehuda Lindell Chapman & Hall CRC, 2008." (2011).

[4] Sobti, Rajeev, and G. Geetha. "Performance comparison of Keccak, Skein, Grstl, Blake and JH: SHA-3 final round candidate algorithms on ARM Cortex A8 Processor." *Int. J. Security Appl* 9, no. 12 (2015): 367-384.

[5] Hellman, Martin. "New directions in cryptography." *IEEE transactions on Information Theory* 22, no. 6 (1976): 644-654.

[6] Coppersmith, Don. "The Data Encryption Standard (DES) and its strength against attacks." *IBM journal of research and development* 38, no. 3 (1994): 243-250.

[7] Sobti, Rajeev, and Ganesan Geetha. "Cryptographic hash functions: a review." *International Journal of Computer Science Issues (IJCSI)* 9, no. 2 (2012): 461.

[8] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21, no. 2 (1978): 120-126.