DELSU Journal of
NIGER DELTA STUDIES **Volume 1, Number 2 (December), 2025**

PISSN 3115-6037
EISSN 3115-6045

CRITICAL REVIEW OF CRYPTOGRAPHY TECHNIQUES FOR SECURING DIGITAL INFORMATION

M. O. Odighi

And

M. I. Omogbhemhe
Department of Computer Science,
Ambrose Alli University,
Ekpoma, Nigeria
onojiasun.odighi@aauekpoma.edu.ng
mikeizah@aauekpoma.edu.ng

Abstract: Cryptography is a crucial component of information security in today's digital world, providing confidential, integrity, and authenticity of information. This explores various cryptography techniques including symmetric-key encryption (AES, DES), Asymmetric –key encryption (RSAA) and hash functions. The paper discussed the strengths and weakness of each techniques as well as their application in secure communication protocol, digital signature and data protection. Similarly, comprehensive comparison between the different cryptography techniques was presented and this will allow users in choosing the best techniques that is suitable for their information processing. The different cryptography techniques algorithms presented will help developed in implementing cryptography in data security, and safeguarding sensitive information in the digital age.

Keywords: Cryptography, Encryption, Asymmetric, Hash Functions, Symmetric, Information

DELSU Journal of
NIGER DELTA STUDIES **Volume 1, Number 2 (December), 2025**
PISSN 3115-6037
EISSN 3115-6045

Introduction

In today's interconnected digital world, the need for secure communication and data protection is paramount. Whether its safeguarding sensitive information, securing financial transactions, or ensuring the privacy of personal data, cryptography plays a vital role in giving the necessary security measures. The place of information security cannot be over emphasized in this digital age since people entrusted with the system still trying to compromise the system (Omogbehemhe & Momodu, 2015). Singh, (2023) define Cryptography as the science of encrypting and decrypting the data so as to keep the data more secured. This technique is carried out by cryptographic key and serves as a string of characters which is used to encrypt and decrypt the data (Lange, 2017). It has the ability of keeping the data in secret while passing it through the unprotected networks, like internet (Stein, 2017). This is happens in order to protect the data from the hackers and make it meaningful only to the intended receiver. Lange, (2017) defined Cryptography as a technique for coding data and making sure the only person who is meant for see information–and has the key to break the code–and read it. The word is a combination of two Greek words: "kryptós", which means hidden, and "graphein", which means to write. Qadir and Varol (2019) define cryptography as the transformation of readable and understandable data into data into a form which cannot be understood in order to secure data. Cryptography refers exactly to the methodology of concealing the content of messages. About 2000 years ago, according to Qaim and Rahul (2023), the Greek knew cylinder device called Scytale, which was sender's part very similar to the recipient part, where a narrow strip of parchment or leather, was wounded around the Scytale and the message was written across it, so if anyone tries to read the text must be the one who has the Scytale. Naser (2021) discovered that some cryptographic approach depend on the privacy of the algorithms, which are only of historical relevance and are sufficient or enough for real world requirements.

The main objective of cryptography is to secure important data on the hard disk or as it passes through a medium that may not be secure itself. Usually, that medium is a computer network.

PISSN 3115-6037
EISSN 3115-6045

The four major benefits of using cryptography are:

(a) Confidentiality. The information cannot be understood by anyone for whom it was not unintended.

(b) Integrity. The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

(c) Non-repudiation. The creator/sender of the information cannot deny at a later stage their intentions in the creation or transmission of the information.

(d) Authentication. The sender and receiver can confirm each other's identity and the origin/destination of the information.

In cryptography process, a message is plaintext (sometimes called cleartext) which helps to disguise the message in such a way that hides its substance. An encrypted message is ciphertext. The process of turning ciphertext back into plaintext is decryption. A cipher is an algorithm for performing encryption or decryption

The flow or conversion of cryptography involving both encryption and decryption (Banerjee, 2020) is illustrated in the figure below.

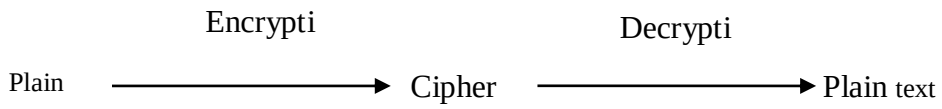

Figure 1.1 describes the flow diagram of Cryptography.
Source: Banerjee, *et al,* (2020).

Plain text: The original data of obtaining the cipher text from plain text.

Encryption: The process of realizing the cipher text from plain text is known as encryption.

Cipher text: The confused or the distorted data obtained as a result of encryption process is known as cipher text.

Decryption: Decryption is the opposite process of encryption. The initial message obtained as a result of this process.

In this paper we examined various cryptographic techniques such as symmetric and asymmetric encryption, digital signatures, and key exchange protocols. We also

PISSN 3115-6037
EISSN 3115-6045

discussed the utilization of cryptography in other areas like secured communication, digital signatures and authentication. The essence is to amplify the use and benefits of cryptography in securing digital data for the benefit of information security expert and chatting a way forward for their deployment and implementation.

Types of Cryptography

(a) . Symmetric Key Cryptography: It is an encryption system where the sender and receiver of message apply a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the limitations is that the sender and receiverhavetoin any case exchange key in a secured manner. According to Banerjee, *et al,* (2020), symmetric key is the most popular cryptography system in Data Encryption System (DES).

Examples of Symmetric Key Cryptography are: Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), The International Data Encryption Algorithm (IDEA).

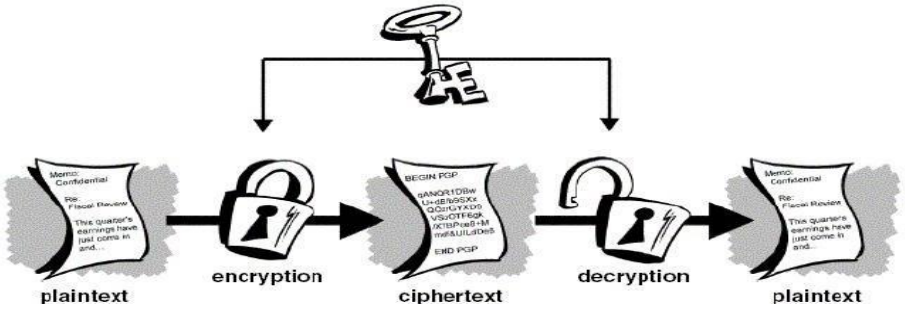

Figure 1.2 Symmetric Key Cryptography
Source: Banerjee, *et al,* (2020).

PISSN 3115-6037
EISSN 3115-6045

Symmetric-key systems are simpler and faster; the major problem is that the two parties must exchange the key in a secure manner and ensure it security thereafter.

Key Management resulted into a nightmare for the parties using the symmetric key cryptography. They were seriously concerned about how to get the keys protected and securely across to all users such that the decryption of the message would be a possibility. More so, if the key is compromised, all the coding system will be compromised and the "Secret" would no longer remain what it was meant to be, hence, the "Public Key Cryptography" was established.

(b) **Asymmetric Key Cryptography:** In this case a pair of keys is used to encrypt and decrypt information. A public key is used for encryption while a private key is used for decryption. Public key and Private Key differ because even if the public key is known by lots of people, the intended receiver can only decode it because he alone knows the private key.

Examples of Asymmetric Key Cryptography are: Digital Signature Standard (DSS), Rivest, Shamir and Adleman Algorithm (RSA), RSA Cryptanalysis, ElGamal

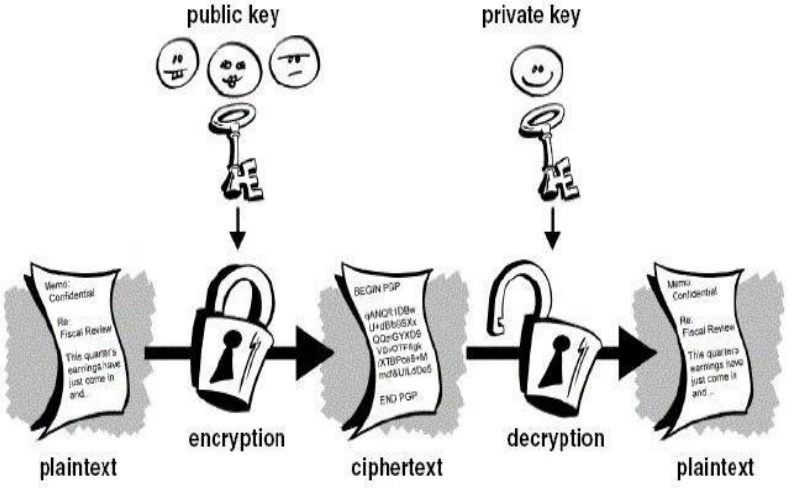

Figure 1.3 Asymmetric Key Cryptography: (Banerjee, *et al,* 2020).

PISSN 3115-6037
EISSN 3115-6045

(c) Hash Functions: This algorithm does not allow the use of keys. A hash value with fixed length is calculated as per the plaintext and this makes recovery impossible for the contents of plaintext. Many operating systems apply hash functions in encrypting passwords.

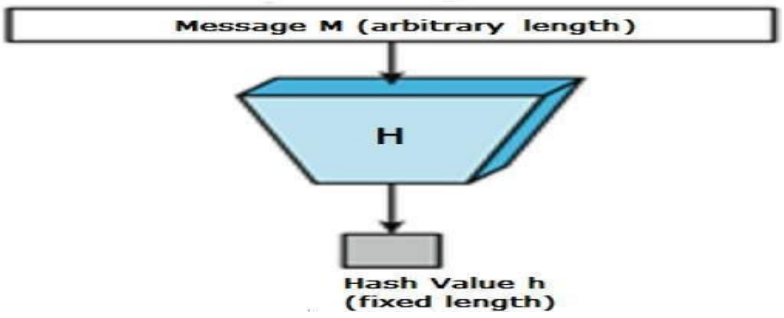

Figure 1.4 Hash Functions: Source: (Aparajita & Rana, 2003).

Properties of hash function

- Computation of hash value is easy for any available message
- It is impossible to generate a message that has a given hash
- It is difficult to change a message without using a different hash
- The difficulty in to finding two different messages with the similar hash

Technical Term Used In Cryptography

(a) Encryption

The conversion of digital information into secret code in order to hide its main facts is described as encryption. In Computing an encrypted message is called ciphertext and a message is refer to as plaintext. Encryption algorithms are called cyphers, which represent the mathematical formula used to encode and decode communications (Stinson, 2005). An encrypted message is known as ciphertext.

According to Bernstein, *el at,* (2017), a cipher's algorithm must involves a variable to work and this variable is called akey. This is what differentiates the output of

PISSN 3115-6037
EISSN 3115-6045

a cypher. Unauthorized parties who intercept encrypted messages must determine the cypher the sender engaged to encrypt the message and the keys that were used as variables. Because it is time consuming and difficult to guess, encryption is a very effective security measure. Sensitive information has conventionally been safeguarded through encryption. Historically, military and governments have engaged it. Data saved on computers and other storage devices, as well as data being transmitted across networks, are all protected by encryption (Dodis, *el at*, 2012).

(b) Decryption

One of the reasons for using encryption-decryption system is privacy. As information move across the Internet, it's essential to check for unwanted users from companies or people. Consequently, the data is encrypted to prevent theft and loss of data. Text files, photos, emails, user data, and directories are a few typical objects that are encrypted. The person who receives decryption gets a pop up window where they may input a password to access the encrypted data. In order to decrypt the data, the system extracts and turns it into words and visuals that may be readily understood by both a reader and a system. It is possible to decrypt data manually or automatically and this might be carried out using a keys or password (Bellare, *el at*, 1998).

A type of encryption called as symmetric encryption apples a single secret key to both encrypt and decode electronic data. To be useful in the decryption procedure, the key must be exchanged between the parties communicating via symmetric encryption. This encryption technique is different from asymmetric encryption, which encrypts and decrypts data using a pair of keys—one public and one private.

Asymmetric cryptography, often known as public-key cryptography, is a method for encrypting decrypting messages and securing them from unwanted users. It makes use of a pair of linked keys, a public key and a private key. A public key is a cryptographic key that anybody may use to encrypt messages such that only the right recipient can decrypt them using their private key. A private key, usually called to as a secret key, is only known to the key's creator. A hash function is a flexible one-way cryptographic technique that changes any size input into a clear

PISSN 3115-6037
EISSN 3115-6045

output with a possible number of bits.

Characteristics of Cryptography

Cryptographic Systems are characterized along three independent dimensions:

(a) The type of operations used for transforming plaintext to ciphertext. All encryption algorithms are based on two general principles. These principles are substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information should be lost (that is, that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions (Kumari, 2024).

(b).The number of keys used. If both sender and receiver use the same key, the system is said to be symmetric, single-key, secret key, or conventional encryption. When the sender and receiver use different keys, the system is called to as asymmetric, two-key or public-key encryption.

(c).The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing one element at a time, as it goes along.

Cryptography Algorithms

(a) Data Encryption Standard Algorithm (DES)

The purpose of DES (Data Encryption Standard) algorithm is to provide a standard method for protecting sensitive commercial and unclassified data. In this algorithm, the same key is used for both encryption and decryption process. DES algorithm consists of the following steps.

Encryption

1. DES accepts an input of 64-bit long plaintext and 56-bit key (8 bits of parity) and produce output of 64 bit block.

PISSN 3115-6037
EISSN 3115-6045

---

2. The plaintext block has to shift the bit around.

3. The 8 parity bits are removed from the key by subjecting the key to its Key permutation.

4. The plaintext and key will be processed by following

i. The key is split into two 28 halves

ii. Each half of the key is moved by one or two bits, depending on the round.

iii. The halves are merged and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed key used to encrypt this round's plaintext block.

iv. The rotated key halves from step 2 are used in next round.

v. The data block is split into two 32-bit halves.

vi. One half is subjected to an expansion permutation to increase its size to 48 bits.

vii. Output of step 6 is exclusive-OR'ed with the 48- it compressed key from step 3

viii. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48 bit block back down to 32-bits.

ix. Output of step 8 is subject to a P-box to permute the bits.

x. The output from the P-box is exclusive-OR'ed with other half of the data block. K. the

xi. Data halves are swapped and become the next round's input.

Also, the DES algorithm is depicted with flowchart in figure 1.5 below:

DELSU Journal of
NIGER DELTA STUDIES **Volume 1, Number 2 (December), 2025**
PISSN 3115-6037
EISSN 3115-6045

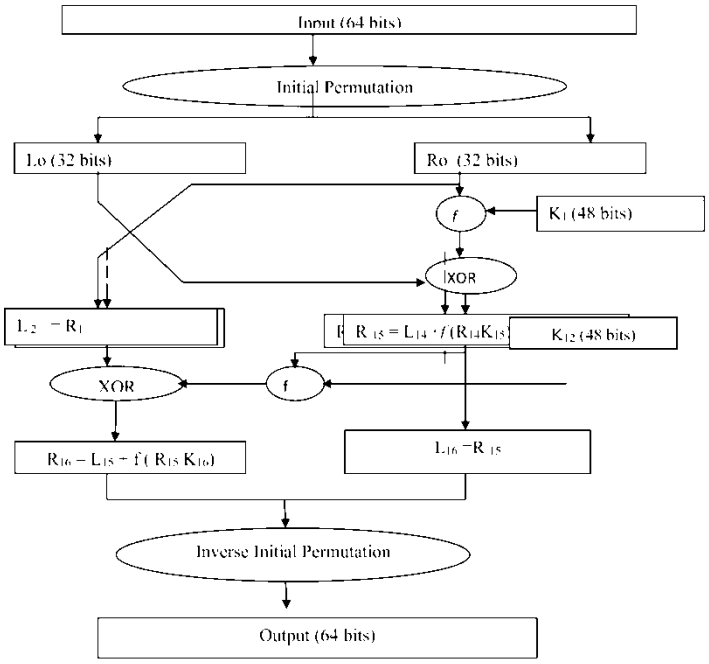

Figure 1.5: Diagram of DES Algorithm:
Source: (Kumari, 2024).

(b) Triple DES (3DES)

3DES or Triple Data Encryption Algorithm (TDEA) was developed to tackle the fault in DES without designing a whole new cryptosystem. Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. Triple DES (3DES) simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits TDEA involves using three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt-Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3. The standards define three keying options (Gupta, 2023).

Option 1: This option, employs three mutually independent keys (K1′= K2′ = K3′ = K1). It gives key space of 3 x 56 = 168 bits.

PISSN 3115-6037
EISSN 3115-6045

Option 2: This employs two mutually independent keys and a third key that is the same as the first key (K1 = K2 = and K3 = K1). This gives key space of 2 x 56 = 112 bits.

Option 3 is a key bundle of the three identical keys (K1 = K2 = K3). This option is equivalent to the DES algorithm. In 3-DES, the 3-times iteration is applied to increase the encryption level and average time. It is a known fact that 3DES is lower than other block cipher methods.

The flowchart of the 3DES is as shown in figure 1.6 below:

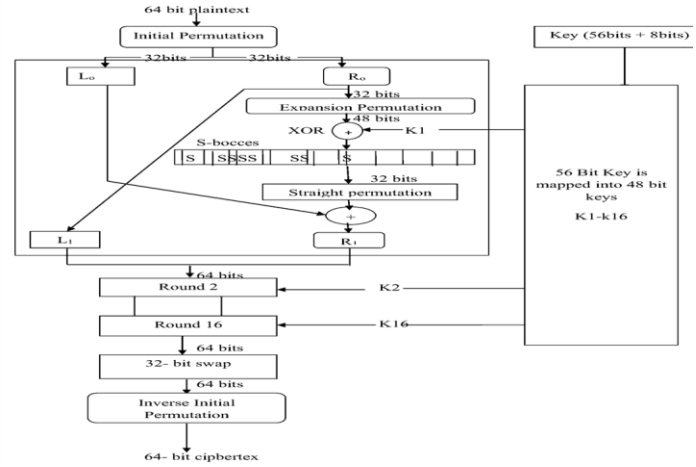

Figure 1.6: Depiction of 3DES:
Source: (Sadaqat, & Muhammad, 2024)

(c) Advanced Encryption Standard (AES)

Advanced Encryption standard (AES) algorithm is for both security and better speed. It is a new encryption standard recommended by NIST to replace DES. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size. It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications. This algorithm is divided into algorithm steps, usual round, final round, and encryption and decryption process. These are as shown below:

PISSN 3115-6037
EISSN 3115-6045

---

1. Algorithm Steps: These steps are used to encrypt the 128-bit block

i. The set of round keys from the cipher key

ii. Initialize state array and add the initial round key to the starting state array.

iii. Perform round = 1 to 9: Execute usual round.

iv. Execute Final Round

v. Corresponding cipher text chunk output of final round step

2. Usual Round: Execute the following operations which are described above.

i. SubBytes

ii. ShiftRows

iii. MixColumns

iv. Add Round Key, using K (round).

3. Final Round:

Execute the following operations which are described above.

i. SubBytes

ii. ShiftRows

iii. AddRound Key, using K(10)

4. Encryption:

Each round consists of the following four steps:

i. Sub Bytes: The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

ii. Shift Rows: In the encryption, the transformation is called Shift Rows.

iii. Mix Columns: The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.

iv. Add Round Key: Add Round Key precedes one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition.

PISSN 3115-6037
EISSN 3115-6045

5. Decryption: Decryption involves reversing all the steps taken in encryption using inverse functions like (a) Inverse shift rows, (b) Inverse substitute bytes, (c) Add round key, and (d) Inverse mix columns.

The AES algorithm is depicted in figure 1.7 below:

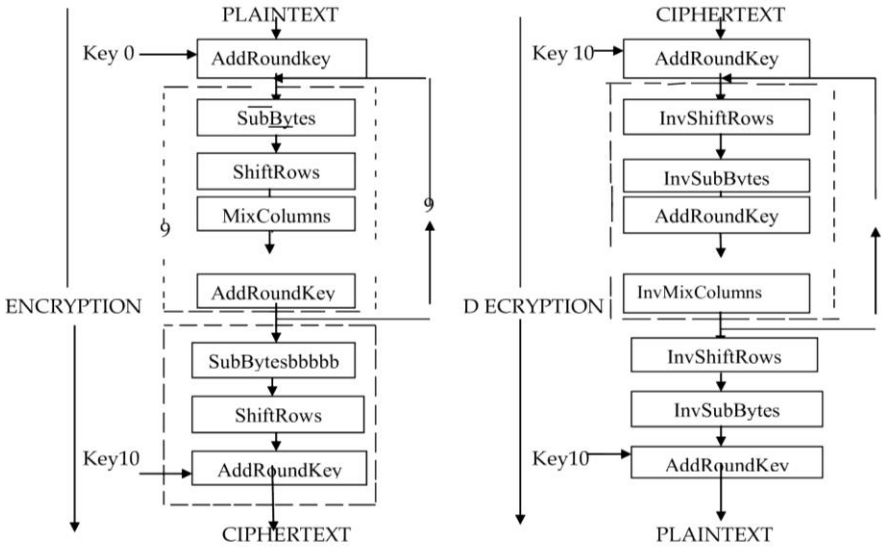

Figure 1.7: AES Encryption and Decryption
Source: (Rabah, 2004).

(d) Rivest-Shamir-Adleman Algorithm (RSAA)

RSA is named after its creators, Ron Rivest, Adi Shamir, and Leonard Adleman, and is one of the first asymmetric public-key encryption/decryption systems. It uses the properties of modular arithmetic of prime numbers to generate a public key that can be used for encryption and a private key that can be used for decryption The RSA algorithm is used to encrypt data in order to provide the data with adequate security so that only the concerned user can access it. RSA is commonly used as a catalyst to send shared encryption keys (Rabah, 2004).
RSA algorithm involves these steps:

1. Key Generation

PISSN 3115-6037
EISSN 3115-6045

---

2. Encryption

3. Decryption

1. Key Generation

Before the data is encrypted, key generation is done in these Steps:

i. Generate two large distinct primes p and q

ii. Compute n = pq and φ = (p – 1)(q – 1)

iii. Select an e, 1 < e > φ, relatively prime to φ.

iv. Compute the unique integer d, 1 < d < ω where ed ≡ φ1.

v. Return public Key (n, e) and private key d

2. Encryption

Encryption is the process of converting original plain text (data) into cipher text (data). The steps in encryption are:

i. Represent the message as an integer m € {0, …. , n – 1}

ii. Compute $c = m^e \bmod n$

3. Decryption

Decryption is the process of converting the cipher text (data) to the original plain text (data).Decryption with key d: compute $m = c^d \bmod n$

The RSAA flowchart is as shown in figure 1.8 below:

DELSU Journal of
NIGER DELTA STUDIES **Volume 1, Number 2 (December), 2025**
PISSN 3115-6037
EISSN 3115-6045

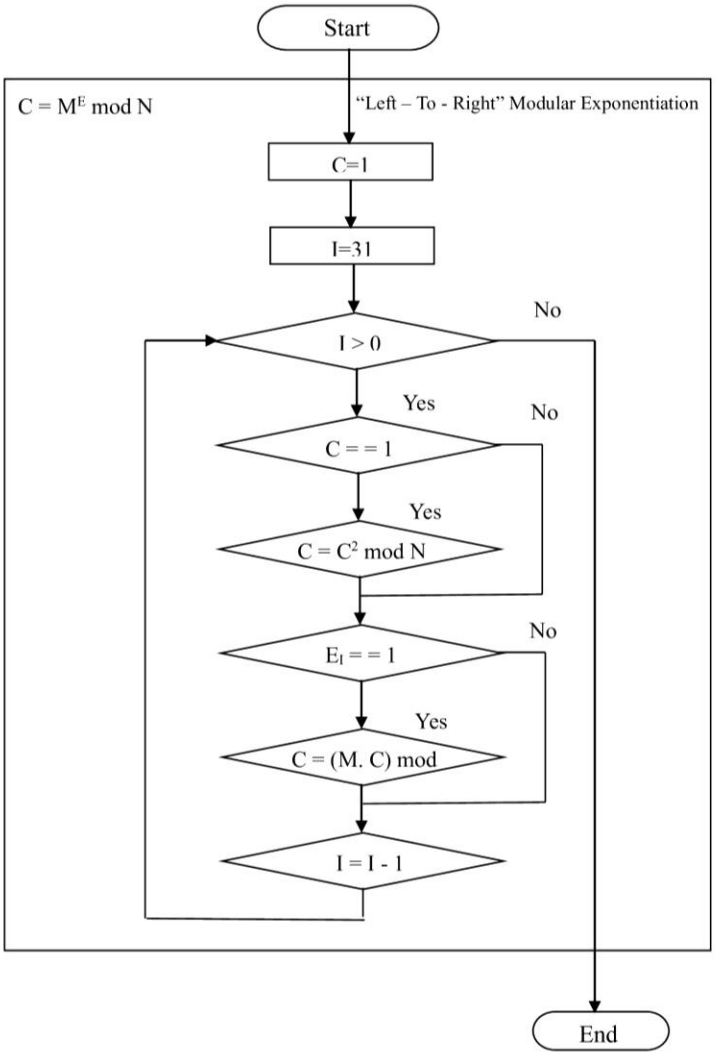

Figure 1.8: RSA Encryption and Decryption Flowchart:
Source: (Peter, 2022).

Comparison between AES, DES, 3DES and RSA

In the table below a comparative study between AES, DES, 3DES and RSA is presented using eighteen factors, which are key size, Block Size, Ciphering & Deciphering Key, Scalability, Algorithm, Encryption, Decryption, Power Consumption, Security, Deposit of Keys, Inherent Vulnerabilities, Key used,

PISSN 3115-6037
EISSN 3115-6045

Rounds, Stimulation Speed, Trojan horse, Hardware and Software Implementation and Ciphering & Deciphering Algorithm (Stephens & Ryan, 2024).

Table 1.1: Comparison between AES, DES, 3DES and RSA
Source: Stephens and Ryan (2024).

Factors	**AES**	**DES**	**3 DES**	**RSA**
Developed	2000	1977	1978	1978
Key Size	128,192,256 bits	56 bits	(K1,K2 and K3) 168bit (K1 and K2 same)112bit	>1024
Block Size	128 bits	64 bits	64 bits	Minimum 512 bits
Ciphering & deciphering key	Same	Same	Same	Different
Scalability	Not scalable	It is scalable algorithm due to varying the key size and block size.	It is scalable algorithm due to varying the key size and Block size.	Not Scalable
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Encryption	Faster	Moderate	Slower	Slower
Decryption	Faster	Moderate	Slower	Slower
Power Consumption	Low	Low	Low	High
Security	Excellent Secure	Not Secure Enough	Secure Enough	Least Secure

PISSN 3115-6037
EISSN 3115-6045

Deposit of keys	Needed	Needed	Needed	Needed
Inherent Vulnerabilities	Brute Forced Attack	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack
Key Used	Same Key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
Rounds	10/12/14	16	14	1
Stimulation Speed	Faster	Faster	Slower	Faster
Trojan Horse	Not proved	No	No	No
Hardware & Software Implementation	Faster	Better in hardware than in software	Better in software than in hardware	Not Efficient
Ciphering & Deciphering Algorithm	Different	Different	Different	Same

Application of Cryptography:

Cryptography, the art of secure communication and data protection, finds widespread application across various domains in today's digital landscape. Its techniques and algorithms are employed to ensure the confidentiality, integrity, and authenticity of data. Let's explore some of the key applications of cryptography:

Secure Communication: Cryptography plays a crucial role in securing communication channels, particularly over the internet. Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), utilize cryptographic protocols to establish secure connections between web browsers and servers. This ensures that sensitive information, such as login credentials, financial data, and personal information, transmitted during online transactions or web browsing remains encrypted and protected from unauthorized access.

Data Encryption: Cryptography is widely used to encrypt sensitive data stored on devices or transmitted over networks. This includes encrypting files and folders on

PISSN 3115-6037
EISSN 3115-6045

computers, securing data in databases, and protecting information in cloud storage. Encryption algorithms, such as Advanced Encryption Standard (AES) are employed to convert plaintext into ciphertext, rendering the data unreadable to unauthorized individuals or attackers.

Authentication and Digital Signatures: Cryptography enables the verification of the authenticity and integrity of digital documents and messages. Digital signatures, which employ asymmetric encryption, provide a way to authenticate the source of a message or document and verify its integrity. They are commonly used in electronic transactions, software updates, and document signing, ensuring non-repudiation and tamper-proof validation.

Password Protection: Cryptographic techniques are utilized to safeguard passwords and ensure secure authentication. Instead of storing actual passwords, systems often store their hash values. When a user enters a password, its hash value is computed and compared to the stored hash value. This prevents the exposure of actual passwords even if the system's data is compromised.

Virtual Private Networks (VPNs): VPNs utilize cryptographic protocols to establish secure and private connections over public networks. By encrypting network traffic, VPNs provide a secure tunnel for remote access to corporate resources; protect sensitive data transmitted between remote locations, and enable individuals to browse the internet securely and anonymously.

Secure Messaging and Email Encryption: Cryptographic tools, such as Pretty Good Privacy (PGP) and its open-source implementation, GNU Privacy Guard (GPG), are used for secure messaging and email encryption. These tools enable end-to-end encryption, ensuring that only the intended recipients can read the messages while preventing eavesdroppers or unauthorized parties from accessing the content.

Financial Transactions: Cryptography is crucial for securing financial transactions conducted over digital platforms. It is used in technologies like chip-based payment cards (EMV), online payment gateways, and crypto currencies like Bitcoin. Cryptographic protocols ensure the privacy, integrity, and security of financial transactions, protecting against fraud and unauthorized access.

PISSN 3115-6037
EISSN 3115-6045

Block chain Technology: Cryptography forms the foundation of block chain technology, which underpins crypto currencies and decentralized systems. Block chain relies on cryptographic hashing, digital signatures, and consensus mechanisms to ensure the immutability, integrity, and security of data stored in the distributed ledger. Cryptography plays a pivotal role in maintaining the integrity of transactions, verifying identities, and securing the decentralized network (Rabah, 2004). Digital cryptography has come a long way in providing secure communication and data protection. However, as technology evolves and new threats emerge, cryptography faces ongoing challenges and requires continuous advancements.

Challenges and future directions in digital cryptography:

Quantum Computing Threat: One of the most significant challenges facing modern cryptography is the potential threat posed by quantum computers. Quantum computers have the potential to break traditional cryptographic algorithms, such as RSA and ECC, by exploiting their computational power. As a result, there is a growing need to develop and standardize post-quantum cryptographic algorithms that can resist attacks from quantum computers (Stallings, 2020).

Key Management: Cryptographic systems rely on the secure generation, storage, and distribution of encryption keys. Effective key management is crucial for maintaining the security of encrypted data. However, key management becomes increasingly complex as the number of encrypted connections and devices grows. Future directions in cryptography involve exploring efficient and scalable key management solutions, including advancements in key exchange protocols, secure key storage mechanisms, and key life cycle management practices.

Privacy in the Digital Age: With the increasing digitization of personal information, preserving privacy has become a significant concern. Future cryptographic techniques will need to address privacy challenges, particularly in areas such as data analytics, machine learning, and biometric authentication. Differential privacy, homomorphic encryption, and secure multi-party computation are emerging cryptographic methods that aim to strike a balance between data utility and individual privacy.

PISSN 3115-6037
EISSN 3115-6045

Secure Internet of Things (IoT): The rapid proliferation of IoT devices presents unique security challenges. Many IoT devices have limited computational power and storage capabilities, making traditional cryptographic methods impractical. Future directions in digital cryptography involve developing lightweight cryptographic algorithms and protocols tailored for resource-constrained IoT environments. Additionally, securing IoT device-to-device communication, data integrity, and authentication are crucial areas for cryptographic advancements.

Verifiable and Transparent Cryptography: Ensuring the transparency and verifiability of cryptographic algorithms and protocols is gaining importance. Openness and peer review contribute to the trustworthiness of cryptographic systems. Future directions in cryptography involve promoting open standards, conducting security audits, and encouraging public scrutiny of cryptographic designs to enhance trust and detect potential vulnerabilities.

Human Factors and Usability: Cryptographic systems often rely on end-users to correctly implement and use cryptographic mechanisms. However, human errors in key management, secure password practices, or understanding the intricacies of encryption can weaken overall security. Future directions include enhancing user-friendly interfaces, improving user education and awareness, and integrating cryptographic mechanisms seamlessly into everyday digital interactions.

Conclusion

Cryptography techniques play a pivotal role in ensuring the security and integrity of sensitive information in this digital age. By employing symmetric- key encryption, asymmetric -key encryption and hash function. Individual and organization can protect their data from unauthorized access, tempering and cyber threats. As technology continue to evolve, It is important to stay up-to- date with the latest cryptography techniques and protocol to ensures the confidentiality and authenticity of the data. Furthermore, the integration of cryptography with emerging technologies, such as block chain and quantum computing will be crucial in shaping the future of information security. By leveraging the power of cryptography, we can safeguard sensitive information and maintain trust in digital world.

PISSN 3115-6037
EISSN 3115-6045

Reference

Aparajita & Rana, A. (2003). Steneography- The Art of Hiding Information: A comparison from Cryptography. *International Journal of Innovative Research in Science, Engineering and Technology,* 2(5), 1308-1312.

Banerjee, A., Gupta, A., & Saini, S. (2020). Blockchain-based secure IoT framework A review, taxonomy, and open research issues. *Journal of Network and Computer Applications,* 164, 102688.

Bellare, M., Rogaway, P., & Wagner, D. (1998). The EAX Mode of Operation. Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, 247-259,

Bernstein, D. J., Lange, T., & Schwabe, P.(2017). Post-quantum cryptography. *Nature*, 549(7671), 188-195,

Gupta, R. K. (2023). A Review Paper on Concepts of Cryptography and Cryptographic Hash Function. *European Journal of Molecular & Clinical Medicine,* 7(7), 3397-3408.

Dodis, Y., Kiltz, E., Pietrzak, K., & Rosen, A.(2012). Advances in cryptology-CRYPTO 2012: 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings. Springer.

Lange, T.(2017). *Elliptic Curve Cryptography: Theory and Implementation.* CRC Press.

Naser M.(2021). From The Ancient History To Now, It's Applications And A New Complete Numerical Model**.** *International Journal of Mathematics and Statistics Studies,* 9(3), 11-30.

Kumari, S. (2024). Cryptography Encryption and Compression Techniques. *International Journal of Engineering and Computer Science,* 6(4), 20915-20919. DOI: 10.18535/ijecs/v6i4.20

Omogbhemhe M.I. & Momodu I.B.A (2015). Various Biometric Techniques suitable for securing.Banking system. *International Journy of Advances in Science and Technnlogy*, 3(3), 11-13.

Stein, W. (2017). *Elementary Number Theory: Primes, Congruences and Secrets.* Springer.

PISSN 3115-6037
EISSN 3115-6045

Stinson, D. R. (2005). Cryptography: Theory and Practice Third Edition (Discrete Mathematics and its Applications), Chapman and Hall/CRC, London.

Stephens, M. & Ryan, I. (2024). Comparative Analysis of Encryption Algorithm for Data Communication. *International Journal of Computer Science and Technology*, 2(2), 292-294.

Sadaqat, U. &Muhammad, B. (2024). Comparison Based Analysis of Different Cryptographic and Encryption Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN). *IJCSI International Journal of Computer Science Issues*, 9(1), 2.

Stallings, W. (2020) Cryptography and Network Security Principles and Practice, Pearson Education, Inc., New York.

Singh, P. & Shende, P. (2023). Symmetric Key Cryptography: Current Trends. *International Journal of Computer Science and Information Technology*, 3(12), 410-415.

Peter, S. (2022). Comparison and Performance Evaluation of Modern Cryptography and DNA Cryptography. Unpublished Masters of Science Thesis Submitted to Royal Institute Of Technology India

Rabah, K. (2004). Data Security and Cryptographic Techniques. A Review. *Asian Network for Scientific Information Technology Journal* 3(1), 106 132

Ramaraj, E,. Karthikeyan, S. & Hemalatha, M. (2009). A design of security protocol using hybrid encryption technique. *International Journal of the Computer, the Internet and Management,* 17(1), 78-89.

Qaim, M. & Rahul, S. K. (2023). *International Research Journal of Modernization in Engineering Technology and Science*, 5(5).

Qadir A. M. & Varol N. (2019). A Review Paper on Cryptography, In Proceedings of 2019th International Symposium on Digital Forensics Security (ISDFS), IEEE, Barcelos,
Portugal.