Mesopotamian journal of Cybersecurity
Vol.2023, **pp**. 7–15
DOI: https://doi.org/10.58496/MJCS/2023/002; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/CyberSecurity

Review Article

Theoretical Background of Cryptography

Rusul Mansoor Al-Amri[1,2,*], Dalal N. Hamood[2], Alaa Kadhim Farhan[3]

[1] *Computer Department/College of Science University AL-Nahrain, Baghdad, 10001, Iraq*

[2] *College of Nursing, University of Al-Ameed Karbala, PO No: 198 Iraq*

[3] *Department of Computer Sciences, University of Technology, Baghdad 10011, Iraq*

ARTICLE INFO

Article History

Received 17 Oct. 2022
Accepted 20 Jan 2023
Published 26 Jan 2023

Keywords

Cryptography

Cryptography concepts

Cryptography techniques

Cryptosystem Attacks

ABSTRACT

Cryptography is the practice of secure communication and the study of secure communication techniques. The theoretical foundations of cryptography include concepts such as cryptography, secure key exchange, digital signatures, and authentication. These technologies are used to protect the confidentiality, integrity, and reliability of information while it is being transmitted over a network or stored in digital form. The core of encryption is the concept of an encryption algorithm, which is a set of mathematical rules used to encrypt and decrypt data. The security of a cryptographic system depends on the strength of the underlying algorithm and the confidentiality of the key used to encrypt and decrypt the data. In this paper, Cryptography concepts and modern techniques are reviewed for types of encryption algorithms and the best ones, and many types of attacks and their impact on the encryption process.

1. INTRODUCTION

To ensure that only the intended audience can read and process the information, cryptography encrypts data and communications using codes. In computer science, the term "cryptography" refers to safe information and communication methods that use mathematical principles and a system of calculations based on rules, or "algorithms," to change messages in ways that are challenging to read. In another sense, digital data is protected via encryption. It's a branch of computer science that focuses on converting data into representations that only authorized users can understand. A message that is encrypted and has letters substituted with other characters is an illustration of fundamental cryptography[1].

The following security principles are addressed by cryptography:

1- **Confidentiality**: - Only the sender and the intended recipient(s) should be able to access the communication, according to the confidentiality clause. If a message may be accessed by someone who is authorized, confidentiality will be lost.

2- **Authentication** establishes the identity of a user or computer system so that it may be trusted.

3- **Integrity** The assurance that data is accurate from the time it leaves the source until it arrives at the destination.

4- **Non-repudiation**:- In the event of a disagreement, it states that the sender of a message cannot be denied for having sent it.

The main components used in cryptographic systems are:

Sender: - A person, group, or organization that starts the communication is known as the sender.

Receivers: - The individual to whom the source communicates the message via various media is referred to as the destination or receiver.

Encryption: - The process of converting information into a secret code that conceals its true meaning is known as encryption. Cryptography is the study of information encryption and decryption.

[*] *Corresponding author. Email: sosoalhaji28@gmail.com*

Decryption: - A procedure known as the decryption cipher converts the ciphertext into plaintext.

Secret key: - is a variable that works with an algorithm to encrypt and decrypt data.

Plaintext: - Plaintext in the context of cryptography is typically just plain text that can be read before it is converted into ciphertext or is still readable after being converted.

Ciphertext: - The process of converting plaintext into encrypted text is known as cipher. Ciphertext must first be decrypted (turned into plaintext) with a key before it can be read.

2. CRYPTOGRAPHY CONCEPTS

There are three types of cryptography explained below:

2.1 Cryptography Using a Secret Key

Data is encrypted using symmetric cryptography, often known as secret key cryptography, using only one key. Symmetric cryptography is the simplest kind of encryption because it uses the same key for both encryption and decryption, as shown in figure (1). When data has to be accessible again, a person with access to the secret key can decrypt the data using the cryptographic algorithm, which uses the key in a cipher to encrypt the data. Although secret key cryptography can be used for both in-transit and at-rest data, it is typically exclusively utilized on the latter due to the risk of compromise posed by disclosing the secret to the message's recipient, for example, CAESAR CIPHER, AES, and DES [2].

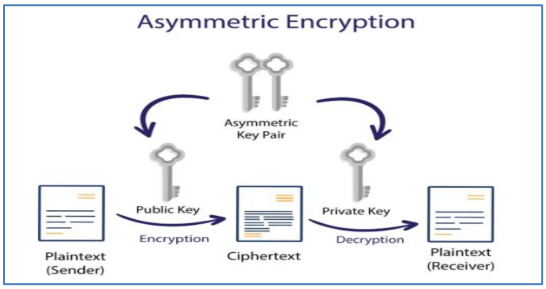

Fig.1. Cryptography with a Secret Key

2.2 Cryptography Using Public Key

Data is encrypted using two keys in public key cryptography, also known as asymmetric cryptography. The message can be decrypted using the other key, while the first is utilized for encryption. In contrast to symmetric cryptography, when one key is used to encrypt a message, a different key must be used to decode it, [3] as shown in figure (2).

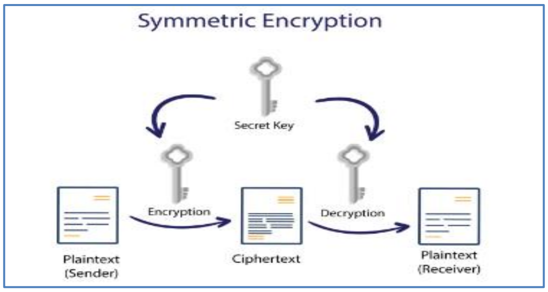

Fig.1. Cryptography with a public key

The "private key" is the one that is kept secret; the "public key" is the one that is made available for use by everyone and is disclosed openly. The public key cannot be deduced from the private key, while the private key can be derived from the public key due to the mathematical relationship between the keys. The owner should be the only one to possess the private key; it should not be shared, for example, DSS(Decision Support System), ECC (Elliptic Curve Cryptography), and Diffie-Hellman [4].

3. CRYPTOGRAPHY TECHNIQUES

Cryptography is the most effective way of data security. Today's increased cybersecurity needs are considerably aided by modern encryption approaches. In cryptography, several algorithms are used to encrypt text, some of which are famous because of their strength in terms of protection and preservation of information from hacking. The most famous of these algorithms at present are AES, DES, TDES, DSA, RSA, ECC, and CR4 (… etc.). These algorithms are described below briefly [5].

3.1 Data Encryption Standard (DES) Algorithm

A team from IBM developed the DES (Data Encryption Standard) algorithm, a symmetric-key block cipher that was later accepted by the National Institute of Standards and Technology (NIST). The algorithm transforms the plain text into ciphertext using 48-bit keys, taking the plain text in 64-bit blocks [6].

3.2 Triple Data Encryption Standard (DES) Algorithm

The Triple Data Encryption Algorithm, also known as Triple DES (Data Encryption Standard), Triple DEA, or TDEA, is a symmetric key-block cipher that applies the DES cipher in triplicate by encrypting with the initial key (k1). The 56-bit keys required by the original DES symmetric encryption technique were insufficient by 1999 to fend against actual brute force attacks. For a total key length of 168 bits, Triple DES calls for the usage of three different DES keys [7].

3.3 Digital Signature Algorithm (DSA)

Based on the mathematical ideas of modular exponentiation and the discrete logarithm problem, the Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. Asymmetric encryption techniques use two separate keys, one for encryption and the other for decryption. For encryption, you use the public key, and for decryption, you use the private key. The receiver's end must, however, generate both keys [8].

3.4 Rivest–Shamir–Adleman (RSA) Algorithm

Popular exponentiation over integers, including prime numbers, in a finite field, is done using the RSA algorithm. The RSA algorithm employs a public key and a private key, which are mathematically related keys. As an asymmetric cryptography algorithm, it uses public and private keys. A private key is kept secret and should never be shared, a public key is shared publicly. A message is decrypted using the opposite key to that which was used to encrypt it. Because it offers a way to ensure the privacy, integrity, validity, and non-repudiation of electronic communications and data storage, RSA has grown to be the most popular asymmetric algorithm [9].

3.5 Elliptic-Curve Cryptography (ECC) Algorithm

In this algorithm, there are two sets of keys: a private key and a public key. The key used to decrypt a message is the opposite of the key used to encrypt it. Behind contemporary ECC purposes, an elliptic curve is a plane curve over a finite field composed of points satisfying the formula y2=x3 + ax + b. This property is one of the reasons for this definition. Any point on the curve in this elliptic curve cryptography illustration can be mirrored over the x-axis without changing the curve's shape in figure (3)[10].

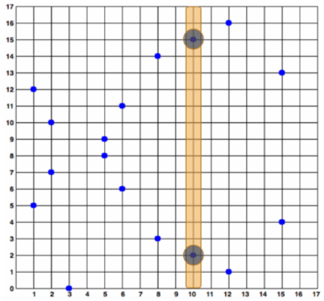

Fig.2. illustration of property graphic elliptic curve cryptograph

3.6 Rivest Cipher 4 (RC4) algorithm

Because of its ease of use and speed of operation, the RC4 stream cipher is one of the most popular stream ciphers. It is a stream cipher with byte-oriented operations and changeable key sizes. It employs key sizes of 64 bits or 128 bits. Features of the RC4 algorithm include consecutive pseudo-random byte generation and the generation of a pseudo-random stream that is XORed with the plaintext to produce the ciphertext. The state table's elements are all switched at least once. Provides the ability to use keys with a bit size between 1 and 2048 Due to its speed and ease of usage, the RC4 cipher has become the most popular stream cipher. It is used in widely used protocols, including Wired Equivalent Privacy, Secure Sockets Layer, and Transport Layer Security (TLS) [11].

3.7 Advance Encryption Standard (AES) algorithm

A symmetric block cipher algorithm with a block/chunk size of 128 bits is the AES Encryption algorithm, also referred to as the Rijndael algorithm. These distinct blocks are converted using keys that are 128, 192, and 256 bits long. It then puts these blocks together to create the ciphertext after encrypting them[1].

Reviewing AES's general structure, let's pay close attention to the four phases that are carried out in each round: (1) Byte substitution, (2) Row shifting, (3) Column mixing, and (4) Round key addition. AES is used to encrypt sensitive data, and AES is used in hardware and software across the globe. For government computer security, cybersecurity, and the protection of electronic data [12].

```
Algorithm  (1) : AES 192-bit Algorithm (Encryption and Decryption )
// Key expansion to generate a key schedule
KeyExpansion (key);
// Encryption
For each 128-bit block of plaintext
    AddRoundKey (state, expandedKey [0]);
        For round = 1 to 6
        SubBytes (state);
        ShiftRows (state);
        MixColumns (state);
        AddRoundKey (state, expandedKey [round]);
End For
       SubBytes (state);
      ShiftRows (state);
     AddRoundKey (state, expandedKey [7]);
End For
// Decryption
for each 128-bit block of ciphertext
   AddRoundKey (state, expandedKey [7]);
     For round = 6 to 1
     InvShiftRows (state);
     InvSubBytes (state);
    AddRoundKey (state, expandedKey [round]);
    InvMixColumns (state);
End For
      InvShiftRows (state);
     InvSubBytes (state);
     AddRoundKey (state, expandedKey [0]);
End For
```

AES is significantly more secure than other algorithm keys since it offers 128-bit, 192-bit, or 256-bit key options.

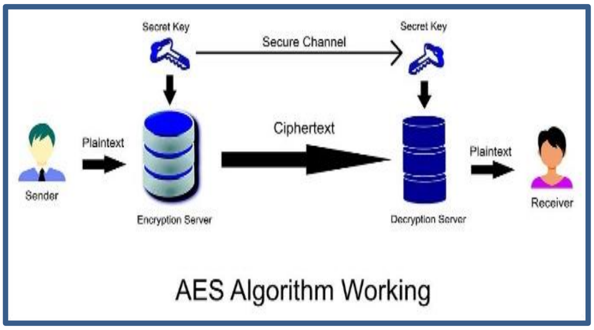

Fig.3 . General Idea for AES Algorithm Work

The length of the key affects a variety of AES factors. For instance, if the key size is 128 bits, then there are 10 rounds, whereas there are 12 and 14 rounds for keys that are 192 bits and 256 bits, respectively. The 128-bit key is now the most popular key size that will likely be employed.

Figure (5) illustrated the architecture of the AES algorithm [13]. The following features of Rijndael:

- Resistance to all known attacks
- Speed and code compactness on a variety of platforms.
- Simple Designs

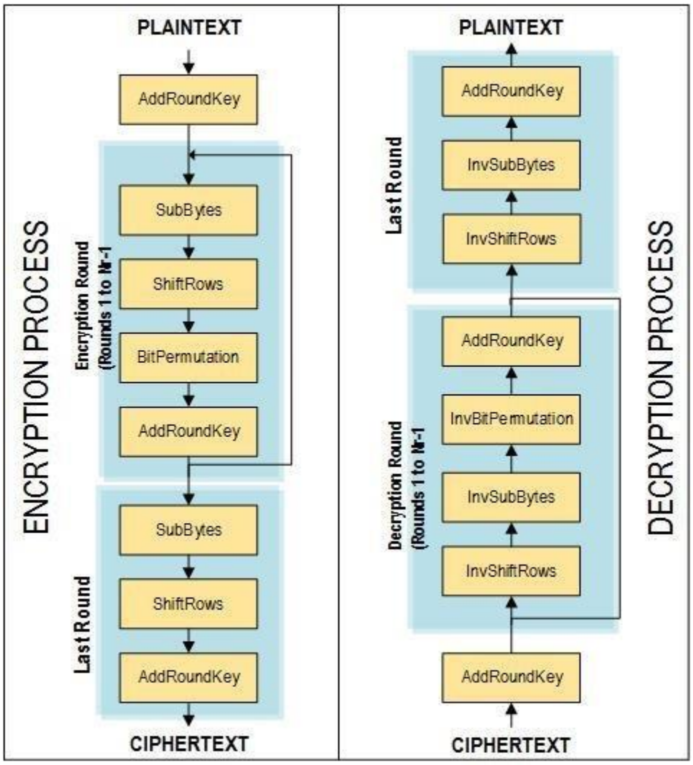

Fig. 4. AES Architecture

This algorithm has several advantages in terms of:

- Security: AES can resist attacks better than other encryption algorithm
- Cost: This algorithm includes an unlimited global domain and is royalty-free.
- Implementation: The AES algorithm is flexible and well-suited when implemented in hardware and software.

It is known that the AES algorithm has evolved and started to take more than one key, and where (the AES 192-bit key) was chosen in our work it turned out the AES-192 (bit) algorithm is used for encrypting a text. The text consists of different lengths of characters. The AES-192 (bit) is used because it is more complex than the AES-128 (bit) and less expensive than the AES-256 (bit). We will demonstrate the work of the AES-192-bit algorithm theoretically through an example below[14].

4. Cryptosystem Attacks

Attacks are often grouped according to what the attacker did. Thus, an attack can be either passive or active.

4.1 A passive attack's

A passive attack's primary objective is to gain unauthorized access to the data. The resources of the system are unaffected, and the data can continue to be used as before. Passive attacks are challenging for the victim to identify because they are typically carried out in secrecy [15]. A passive attack attempts to access data or scans for network weaknesses and open ports. Passive attacks examples :(**Eavesdropping attack and the release of messages) .**

4.2 Active Attacks

A network exploits that allows the attackers to change the content or affect the system resource qualifies as an active attack. Damage will be done to the victims. Before pretending to launch an aggressive attack, the attackers can launch passive attacks to acquire information. Attackers try to break the system's lock and cause disruption. The victims can learn more about the ongoing attack. Their a possibility and integrity may be at risk from such an attack[16]. A forceful attack is more difficult to execute than a quiet attack. Active attacks examples:

4.2.1 Denial-of-Service attacks (DoS)

There is one active attack in each of the samples. As soon as the attackers take steps to shut down a tool or network, a denial-of-Service assault occurs. The initial user can as a result be unable to access the device or network. The target device or network may be bombarded with traffic by the attackers until it stops responding or flames. Emails, websites, and online banking accounts are among the services that are impacted. DoS attacks can only be carried out from one area [17].

4.2.2 Trojan Horse Attack

Another type of network attack is a Trojan horse attack, the most common of which is a backdoor Trojan. A backdoor Trojan gives unauthorized attackers access to the computer system, network, or software application. As an illustration, the attackers might bury some malware under an apparent link. A backdoor will be downloaded into the device after the users click the link. The attackers could then have straightforward access to the system. Flame is a piece of malware designed to attack Windows OS that was created in 2012. It will carry out a few tasks like taking screenshots, collecting audio, and monitoring network traffic[18].

4.2.3 Replay attack

Furthermore, one sample of an active attack is a replay attack. Before starting a replay attack, the attackers can spy on a particular user. The same communication, which has been correctly encrypted, will then be sent to the victim by a user who has been permitted to do so. Attackers can access the data and knowledge stored on the compromised device through replay assaults. They can also make money since they can imitate the victim's group action. This is because the attackers can listen in on the frames of this session, using constant information to assault without having to stop after a certain number of times. Similar to a repeat assault, there is another attack known as a cut-and-paste attack. The attacker can combine various ciphertext components and send them to the victim in a cut-and-paste attack. Once they have the information they need, the attacker can utilize it to breach the system [19].

4.2.4 Known Plaintext Attack (KPA)

with this technique, the attacker is aware of some of the ciphertext's plaintext. With this knowledge, the remaining ciphertext must be decrypted. This can be accomplished in several ways, including by figuring out the key. The best illustration of this assault is the use of block ciphers in linear cryptanalysis [19].

4.2.5 Chosen Plaintext Attack (CPA)

The attacker uses this technique to encrypt the text of his choice. can now choose the ciphertext-plaintext pair he wants. This makes finding the encryption key easier. Differential cryptanalysis used against block ciphers and hash functions is an illustration of this technique. RSA is a well-known public key cryptosystem and is open to chosen-plaintext attacks [19].

4.2.6 Dictionary Attack

There are numerous variations of this approach, all of which entails creating a "dictionary." The most basic form of this attack involves the attacker creating a dictionary of plaintexts and ciphertexts that learned over time. In the future, an attacker will consult the dictionary after receiving the ciphertext to determine the corresponding plaintext[19].

4.2.7 Brute Force Attack (BFA)

Using all potential keys, the attacker uses this technique to try to identify the key. There are 2^8= 256 potential keys if the key is 8 bits long. Knowing the algorithm and the ciphertext, the attacker is now trying each of the 256 keys one at a time to decrypt the data. If the key is long, it would take a very long time to finish the attack [19].

4.2.8 Birthday Attack

A variation of the brute-force attack is this one. It is employed in opposition to the cryptographic hashing algorithm. When asked about their birthdays in class, students must respond with one of the 365 days potential dates [24].

4.2.9 Man in Middle Attack (MIM)

The majority of public key cryptosystems, which require key exchange before communication can occur, are the targets of this attack [25].

- To interact with host B, host A requests access to host B's public key.
  - This request is intercepted by an attacker, who transmits his public key in its place.
  - The attacker can so read anything host A sends to host B.
  - After accessing the data, the attacker uses his public key to re-encrypt it before sending it to B to continue communication.
  - For B to accept it as though it were taking it from A, the attacker submits his public key as A's public key.

4.2.10 Side Channel Attack (SCA)

No specific algorithm or kind of cryptosystem is targeted by this attack. Instead, it is launched to take advantage of the cryptosystem's physical implementation's flaw [26].

4.2.11 Timing Attacks

type of attack that involves introducing flaws or defects into the computing process in order to extract secret information from a cryptographic system. Different techniques, including physically modifying the device or taking advantage of software flaws, can be used to introduce these problems. AFA seeks to deduce hidden information, such as a cryptographic key, by observing how the system reacts to these flaws. AFA is a potent and useful attack technique that can be used to break both symmetric and asymmetric cryptography systems. Attackers utilize this advanced method to give crucial information to uninvited parties [27].

4.2.12 Power Analysis Attacks (PAA)

These attacks resemble timing attacks, with the exception that they exploit the amount of power consumed to learn more about the makeup of the underlying calculations**.**

4.2.13 Fault analysis Attacks (FAA)

fault analysis is a type of attack that aims to extract secret information from a cryptographic system by introducing faults or errors into the computation process. These faults can be introduced in various ways, such as by physically altering the device or by exploiting software vulnerabilities. The goal of AFA is to observe the system's response to these faults and use this information to infer secret information, such as a cryptographic key. AFA is a powerful and practical attack method that can be applied to a wide range of cryptographic systems, including symmetric and asymmetric ciphers. It's a sophisticated technique used by attackers to reveal sensitive information to unauthorized parties.

4.2.14 Ciphertext-Only Attacks (COA)

The attacker in a ciphertext-only attack (COA) has access to a set of ciphertext (s). He does not possess the associated plaintext. When the relevant plaintext can be extracted from a given collection of ciphertext, COA is said to have been successful. On rare occasions, this assault can yield the encryption key. Ciphertext-only attacks are protected against by contemporary cryptosystems.

Conflicts Of Interest

Author declare no conflict of interest

Acknowledgment

The authors would like to thank Al-Nahrain University, the University of Technology, University of Al-Ameed Karbala, and the Iraqi Ministry of Education for their support in the conduct of the work published in this paper.

Funding

The authors receive no funding for this work

References

[1] A. M. J. C. Abdullah and N. Security, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," vol. 16, no. 1, p. 11, 2017.

[2] P. Gaži and S. Tessaro, "Secret-key cryptography from ideal primitives: A systematic overview," in *2015 IEEE Information Theory Workshop (ITW)*, 2015, pp. 1-5: IEEE.

[3] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight cryptography for internet of insecure things: A survey," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019, pp. 0475-0481: IEEE.

[4] S. Tayal, N. Gupta, P. Gupta, D. Goyal, M. J. A. i. C. S. Goyal, and Technology, "A review paper on network security and cryptography," vol. 10, no. 5, pp. 763-770, 2017.

[5] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. J. I. T. o. S. C. Bian, "Blockchain security: A survey of techniques and research directions," vol. 15, no. 4, pp. 2490-2510, 2020.

[6] V. S. Shetty, R. Anusha, D. K. MJ, and P. Hegde, "A survey on performance analysis of block cipher algorithms," in *2020 International Conference on Inventive Computation Technologies (ICICT)*, 2020, pp. 167-174: IEEE.

[7] M. S. Mehmood, M. R. Shahid, A. Jamil, R. Ashraf, T. Mahmood, and A. Mehmood, "A comprehensive literature review of data encryption techniques in cloud computing and IoT environment," in *2019 8th International Conference on Information and Communication Technologies (ICICT)*, 2019, pp. 54-59: IEEE.

[8] M. A. Al-Absi, A. Abdullaev, A. A. Al-Absi, M. Sain, and H. J. Lee, "Cryptography Survey of DSS and DSA," in *Advances in Materials and Manufacturing Engineering: Proceedings of ICAMME 2019*, 2020, pp. 661-669: Springer.

[9] F. Mallouli, A. Hellal, N. S. Saeed, and F. A. Alzahrani, "A survey on cryptography: comparative study between RSA vs ECC algorithms, and RSA vs El-Gamal algorithms," in *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2019, pp. 173-176: IEEE.

[10] M. Habek, Y. Gene, N. Aytas, A. Akkoc, E. Afacan, and E. Yazgan, "Digital image encryption using elliptic curve cryptography: A review," in *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2022, pp. 1-8: IEEE.

[11] S. A. Jassim and A. K. Farhan, "A survey on stream ciphers for constrained environments," in *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*, 2021, pp. 228-233: IEEE.

[12] A. A. Yazdeen, S. R. Zeebaree, M. M. Sadeeq, S. F. Kak, O. M. Ahmed, and R. R. J. Q. A. J. Zebari, "FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review," vol. 1, no. 2, pp. 8-16, 2021.

[13] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight cryptography for internet of insecure things: A survey," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019, pp. 0475-0481: IEEE.

[14] A. M. J. C. Abdullah and N. Security, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," vol. 16, no. 1, p. 11, 2017.

[15] M. Bozdal, M. Samie, and I. Jennions, "A survey on can bus protocol: Attacks, challenges, and potential solutions," in *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, 2018, pp. 201-205: IEEE.

[16] O. J. I. J. o. I. T. Hosam and C. Science, "Attacking image watermarking and steganography-a survey," vol. 11, no. 3, pp. 23-37, 2019.

[17] A. Huseinović, S. Mrdović, K. Bicakci, and S. J. I. A. Uludag, "A survey of denial-of-service attacks and solutions in the smart grid," vol. 8, pp. 177447-177470, 2020.

[18] F. Salahdine and N. J. F. i. Kaabouch, "Social engineering attacks: A survey," vol. 11, no. 4, p. 89, 2019.

[19] H. A. Patil and M. R. Kamble, "A survey on replay attack detection for automatic speaker verification (ASV) system," in *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, 2018, pp. 1047-1053: IEEE.

[20] T. J. A. J. o. M. R. Mehrotra, "A review on attack in wireless and computer networking," vol. 10, no. 10, pp. 1457-1463, 2021.

[21] A. J. C. J. P. T. I. Mallik, "Man-in-the-middle-attack: Understanding in simple words," vol. 2, no. 2, pp. 109-134, 2019.

[22] A. Akram, M. Mushtaq, M. K. Bhatti, V. Lapotre, and G. J. I. A. Gogniat, "Meet the Sherlock Holmes' of side channel leakage: A survey of cache SCA detection techniques," vol. 8, pp. 70836-70860, 2020.

[23] R. Mansoor, D. N. Hamood, A. K. J. I. J. F. C. S. Farhan, and Mathematics, "Image Steganography Based on Chaos Function and Randomize Function," vol. 4, no. 1, pp. 71-86, 2023.

[24] S. R. Shanmugham and S. J. I. W. S. S. Paramasivam, "Survey on power analysis attacks and its impact on intelligent sensor networks," vol. 8, no. 6, pp. 295-304, 2018.

[25] R. J. W. J. o. C. Mansoor and M. Sciences, "The Steganography Based On Chaotic System for Random LSB Positions: SBOCSFRLSBP," vol. 1, no. 4, pp. 171-193, 2022.

[26] M. Liao, W. He, D. Lu, and X. J. S. R. Peng, "Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination: from the view of imaging through scattering medium," vol. 7, no. 1, p. 41789, 2017.

[27] R. M. Al-Amri, D. N. Hamood, A. K. J. A.-S. J. f. E. Farhan, and Technology, "Generation Initial Key of the AES Algorithm based on Randomized and Chaotic System," vol. 2, no. 1, pp. 53-68, 2023.