Article Citation Format
Wemegah, J. (2022): A Review of Various Data Security Techniques in
Wireless Communication Systems. Journal of Digital Innovations &
Contemporary Research in Science, Engineering & Technology.
Vol. 10, No. 2. Pp 15-24
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V10N4P3

A Review of Various Data Security Techniques in Wireless Communication Systems

Wemegah Joshua
School of Technology
Ghana Institute of Management & Public Administration
GreenHills, Accra, Ghana
E-mail: joshua.wemegah01@gmail.com
Phone: +233243963930

ABSTRACT

Sensitive data is constantly being transmitted particularly over wireless communication systems due to how convenient this wireless communication systems are. However, these communication systems are generally weak in terms of privacy protection and security as a whole. This is because anyone within the perimeter of a wireless network can attempt hacking into the network without physically connecting to it. This paper will focus on the two most common data security techniques in wireless communication systems – steganography and cryptography. Steganography is the practice of hiding information in another message or physical item such that its presence cannot be detected by human examination. Cryptography on the other hand is the science of encrypting information in a way that unintended recipients cannot interpret and then decrypting the said message back into plaintext.

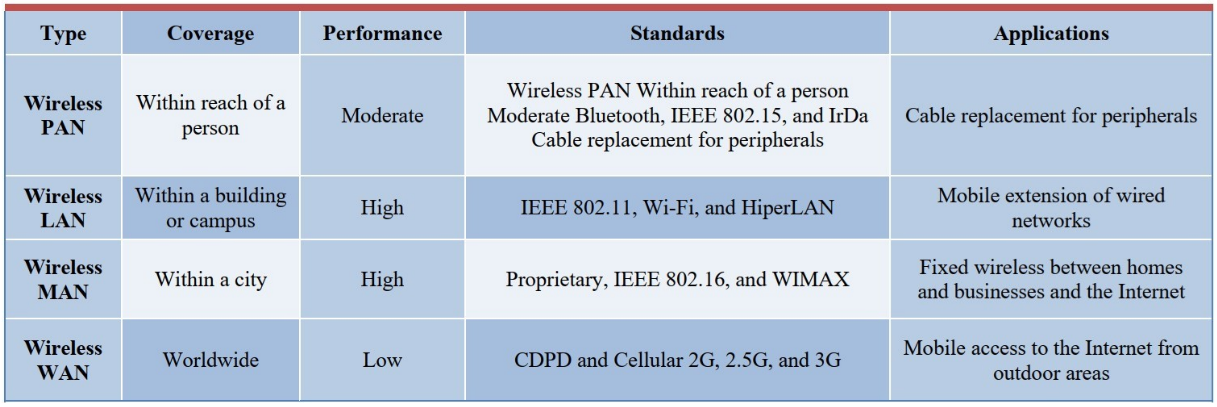
Keywords: Cryptography, Data Encryption, Data Decryption, Steganography, Wireless Communication

1. INTRODUCTION

The wireless communication revolution is bringing fundamental changes to data networking and telecommunications, as well as making integrated networks a reality. Businesses and consumers alike frequently use wireless networks. Many laptop computers come with pre-installed wireless cards. Being able to join a network while on the go has a number of benefits (Kadhim & Sadkhan, 2021). Wireless communication is the exchange of data between two or more points that are not directly connected by an electrical transmitter. The most widely known wireless communication systems use electromagnetic (EM) signals such as radio waves and satellites for data communication as opposed to wired communication systems that use copper wire, fiber optic cables etc. (Kumar & Gambhir, 2014).

Wireless communication systems are sometimes referred to as unguided communication systems. Communication is achieved with the help of a transmitter as the source and a receiver as the destination. Wireless networking is less costly and much easier to set up than conventional wired networking. Wireless networking is utilized at airports, hotel lobbies, and small business or home networks, among other places. The transmission distance can range from a few meters as that between a television and its remote control to thousands of kilometers for radio communication (Sharma & Dhir, 2014). Table 1 illustrates the comparison among the various types of wireless communication network systems.

Table 1: Comparison of wireless network types.



Type	Coverage	Performance	Standards	Applications
Wireless PAN	Within reach of a person	Moderate	Wireless PAN Within reach of a person Moderate Bluetooth, IEEE 802.15, and IrDa Cable replacement for peripherals	Cable replacement for peripherals
Wireless LAN	Within a building or campus	High	IEEE 802.11, Wi-Fi, and HiperLAN	Mobile extension of wired networks
Wireless MAN	Within a city	High	Proprietary, IEEE 802.16, and WIMAX	Fixed wireless between homes and businesses and the Internet
Wireless WAN	Worldwide	Low	CDPD and Cellular 2G, 2.5G, and 3G	Mobile access to the Internet from outdoor areas

Data Security Techniques

The data that is transmitted through the wireless communication medium need to be secured against various adversaries. Various secured data transmission techniques are used to provide security to data transmitted from the transmitter to the receiver. These strategies prevent data from falling into the wrong hands. Steganography and cryptography are the primary strategies deployed to safeguard data in wireless communication systems (Sood et al., 2013).

Steganography

Steganography essentially dwells on secrecy. In other words the security of steganography system relies on secrecy of the system. The art of steganography involves concealing a message within (or even on top of) an otherwise public communication. Almost anything you desire may be that item. Nowadays, many steganography instances include concealing a text message within an image. Or inserting a covert message or script into an Excel or Word document. Steganography has two main goals: concealment and deception.

It involves the use of any media to encrypt communications and is a type of covert communication. The goal of steganography is to conceal messages within other "harmless" digital media in such a way that no one can detect the presence of the hidden message. Steganography does not change the structure of the secret message, but rather conceals it within a medium so that the difference is not visible (Sood et al., 2013). So the objective of steganography is to conceal a message and this message is then transmitted over the wireless communication medium.

Cryptography

The oldest recorded instance of cryptography in writing goes back to around 1900 BC, when an Egyptian scribe utilized unconventional hieroglyphs in an inscription. Cryptography is the study of writing in secret code and is an age-old art. Some scholars argue that cryptography spontaneously developed some time after the invention of writing, with uses ranging from diplomatic missives to military battle preparations. Therefore, it is not surprising that new types of cryptography appeared not long after computer communications became widely used. Cryptography is required in data and telecommunications when interacting across any untrusted medium, including most networks, especially the Internet (Kessler, 2019). Cryptography involves encrypting plaintext into a cyphertext and then decrypting the cyphertext back into plaintext.

An example of the use of cryptography is illustrated in the narrative that follows. Assume a sender, who will be referred to as Alice, wants to send a message *m* to a recipient, who will be called Bob. Alice communicates through an unsecured channel (such as wireless communication system). If the message includes sensitive data, there may be an issue. An eavesdropper might be able to intercept the message and read it. Let’s name the eavesdropper Eve. Eve may read the message, violating the confidentiality in the communication supposed to be between Alice and Bob. Eve again, might be able to alter the message, violating the integrity in the communication supposed to be between Alice and Bob. One objective of cryptography is to provide methods for preventing such attacks. Other objectives are discussed in the subsequent sections.

Types of Cryptographic Algorithms

There are three basic kinds of NIST-approved cryptographic algorithms, which are determined by the number or type of cryptographic keys used with each (NIST, 2017).

a. Hash Functions
b. Symmetric-key algorithms
c. Asymmetric-key algorithms

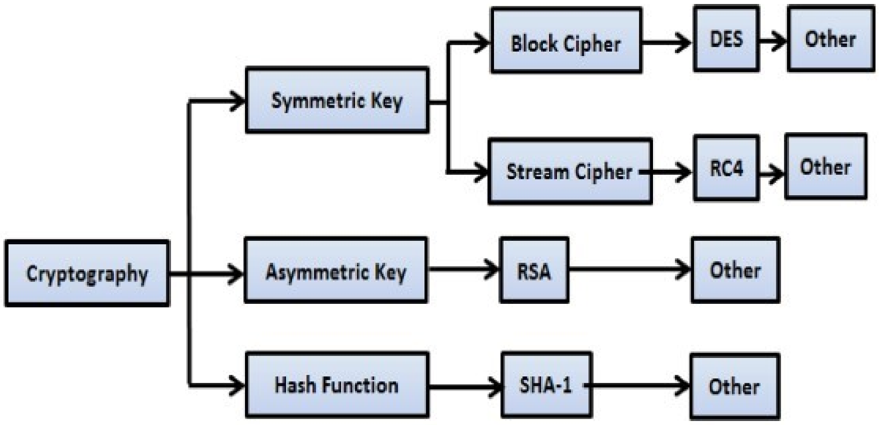


Fig. 1 Different types of cryptographic techniques (Ubaidullah & Makki, 2016)

Hash Functions

In a sense, techniques that employ hash functions—also known as message digests and one-way encryption—require no key. Instead, a fixed-length hash value is calculated using the plaintext, which makes it impossible to reconstruct the plaintext's length or contents. To create a digital fingerprint that is frequently utilized by various operating systems to encrypt passwords, hash techniques are generally used. Therefore, hash functions give an indication of a file's integrity (Kessler, 2019).

Hash algorithms that are in common use today include;

i. Message Digest (MD) algorithm
    - MD2 (RFC 1319: Designed for systems with limited memory.
    - MD4 (RFC 1320)
    - MD5 (RFC 1321)

ii. Secure Hash Algorithm
    - SHA-1 produces a 160-bit hash value
    - SHA-2
    - SHA-3

Symmetric-key algorithms

Also referred to as a secret-key algorithm, a symmetric-key algorithm transforms data to make it extremely difficult to view without possessing a secret key. The key is considered symmetric because it is used for both encrypting and decrypting. So in symmetric-key algorithm, the same key is used to encrypt and decrypt the message (Sood et al., 2013).

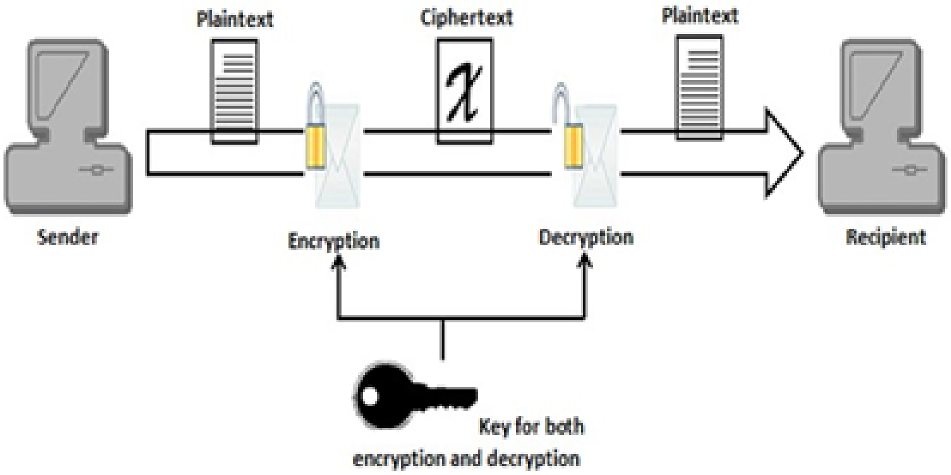


Fig. 2 Symmetric-key algorithm (Ubaidullah & Makki, 2016)

The components of a symmetric-key algorithm are illustrated in fig. 2 (Ubaidullah & Makki, 2016)

i. Plaintext: It is the original message that the sender wishes to convey to a particular receiver. These pieces of information will be fed into the encryption algorithm.

ii. Encryption algorithm: It consists of a number of procedures that, with the aid of a secret key, will run on the plaintext to produce ciphertext.
iii. Secret key: It is the value that is utilized to combine plaintext in order to convert it to ciphertext; this value is independent of plaintext.
iv. Ciphertext: It is the result of the original plaintext after it has been encrypted. It will be very dissimilar from plaintext.
v. Decryption algorithm: is a collection of operations that will be carried out on ciphertext with the use of a secret key to produce the original plaintext.

Symmetric-key algorithm can be broadly classified into; block cipher and stream cipher. These two broad classifications produce;

- Data Encryption Standard (DES)
- Triple Data Encryption Standard (T-DES)
- Advanced Encryption Standard (AES)
- Blowfish Algorithm

Data Encryption Standard (DES) is one such symmetric block cipher algorithm, consisting of 64-bit plain-text encrypted as 64-bit cipher text using a 64-bit key. As technology advanced, different cryptanalytic methods such as brute force were developed to decrypt the cipher text by breaking the key, limiting the use of DES. To combat such attacks, the DES cipher was reinforced as the Triple Data Encryption Standard (Triple-DES), which applies the DES cipher three times (Vuppala et al., 2020).

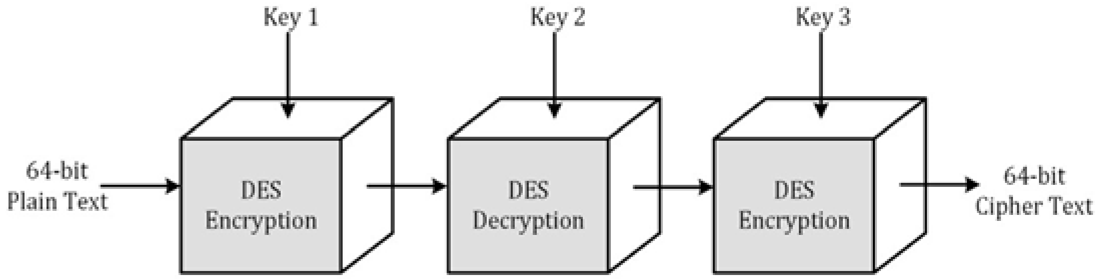


Fig. 3: Block diagram of Triple-DES (Vuppala et al., 2020)

Advanced Encryption Standard (AES)

The current standard for secret key encryption is Advanced Encryption Standard (AES). Vincent Rijmen and Joan Daemen, two Belgian cryptographers, developed AES to replace the outdated Data Encryption Standard (DES) (Mukta & Azad, 2014). AES is simple, secured and can be suited to both hardware and software.

There were several different algorithms developed based on the block size. 128 bits, 192 bits, and 256 bits were utilized as block sizes. 10, 12, and 14 cycles were used to operate AES 128-bit, 192-bit, and 256-bit encryption (Sood et al., 2013).

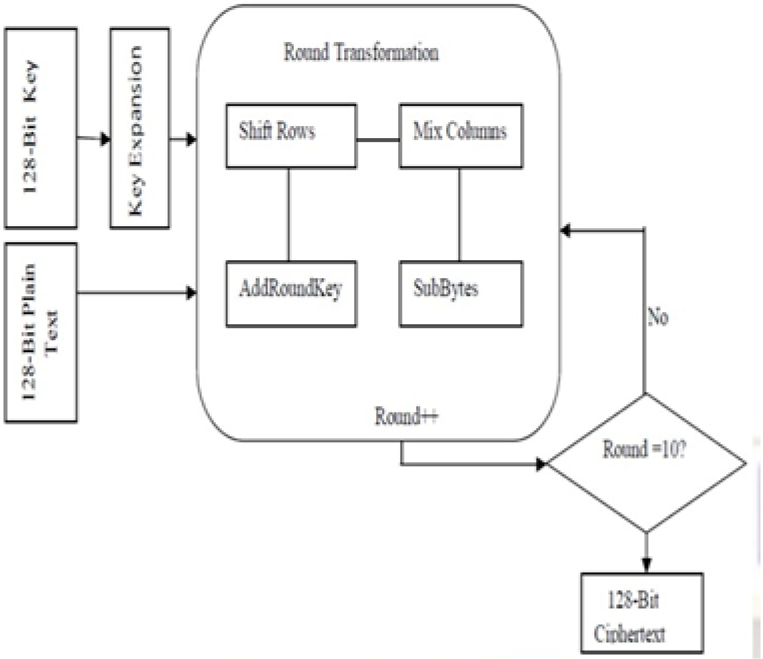


Fig. 4 AES 128 algorithmic structure (Sood et al., 2013)

Asymmetric Encryption Algorithm

The asymmetric encryption algorithm is also referred to as the public key algorithm. Two separate keys are deployed in achieving the implementation of this algorithm. The encryption key also known as the public key and encryption algorithm are known. However, the decryption key also known as the private key is only known to its owner (Fanfara et al., 2012). Fig. 6 illustrates the asymmetric encryption algorithm.

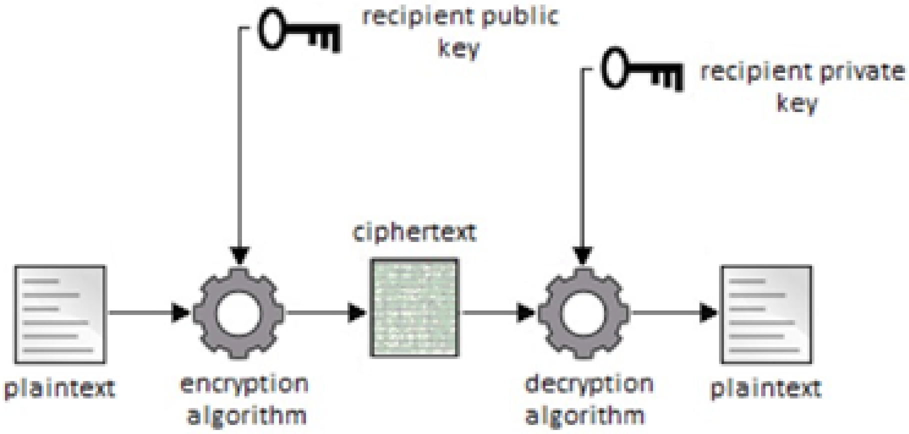


Fig. 5: Asymmetric encryption algorithm (Fanfara et al., 2012)

The encryption and authentication services provided by public key cryptography are based on the fact that each communication participant has their own private and public key (Fanfara et al., 2012). The following are some examples of algorithms that fall under the asymmetric encryption algorithm.

- Rivest-Shamir-Adleman (RSA)
- Digital Signature Algorithm (DSA)
- Elliptical Curve Cryptography (ECC)
- Diffie-Hellman exchange method
- TLS/SSL protocol

Rivest-Shamir-Adleman (RSA)

The RSA algorithm employs a public key and a private key. RSA was created in 1977. It is a block cipher used in digital signature or key exchange algorithms. The cloud service provider (sender) encrypts a message, which the cloud service consumer decrypts (receiver) (Yassein et al., 2018). In effect, the message is encrypted by the public key and decrypted by the appropriate private key owned by the receiver. There are three steps under the RSA algorithm i.e; key generation, encryption and decryption.

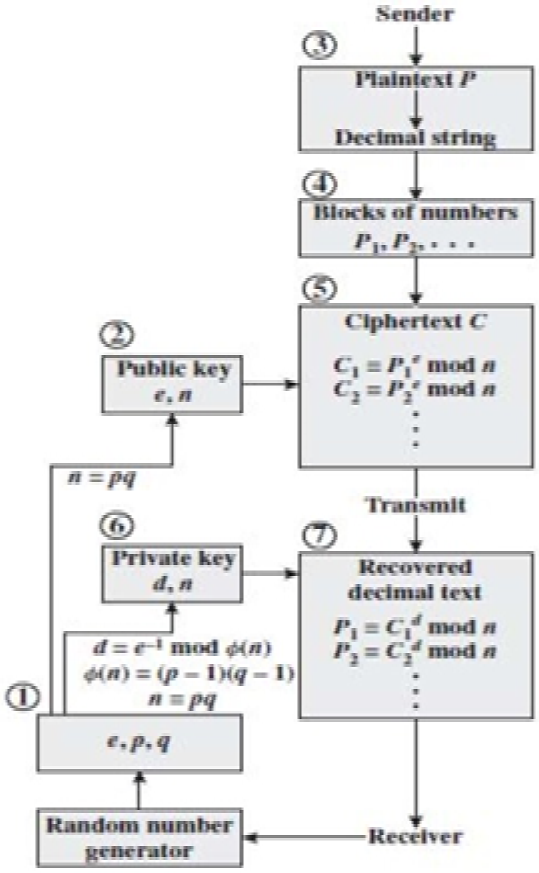


Fig. 6 RSA algorithm process (Yassein et al., 2018)

2. LITERATURE REVIEW

(Fanfara et al., 2012) stated that one of the many aspects of informatics that has made significant development is communication security. Sensitive data are utilized in communications on a growing basis, making security requirements more pertinent and crucial. As the power of today's computers is enhanced, the likelihood that data will be acquired through an attack grows as well. The focus of the paper is on sender authentication utilizing asymmetric encryption with a one-way hash function to compute the public and private keys.

(Kadhim & Sadkhan, 2021) presented that due to the broadcast nature of radio transmission, the wireless air interface is open and available to both authorized and illegal users. In a wired network, communication devices are interconnected together, thereby making it difficult for a station without a direct link to access the network for nefarious purposes. Compared to cable transmissions, wireless transmissions are more susceptible to malicious attacks because of the open communications environment, which allows both passive and active attackers to interfere with legitimate signals.

(Kumar & Gambhir, 2014) opined that the progress of wireless technology has been tremendous in recent years. We are more exposed to wireless technologies. Given the broadcast nature of wireless networks, there are a variety of security concerns with wireless communication. It is not possible to generalize the security principles designed for wired systems to wireless systems. The vulnerabilities of wireless communication can be exploited by attackers and intruders. In this essay, we'll discuss the many remote security risks that wireless systems and protocols like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access 2 now have to offer (WPA2). Because it uses the Advanced Encryption Standard (AES) encryption, WPA2 is a more robust security standard than WPA.

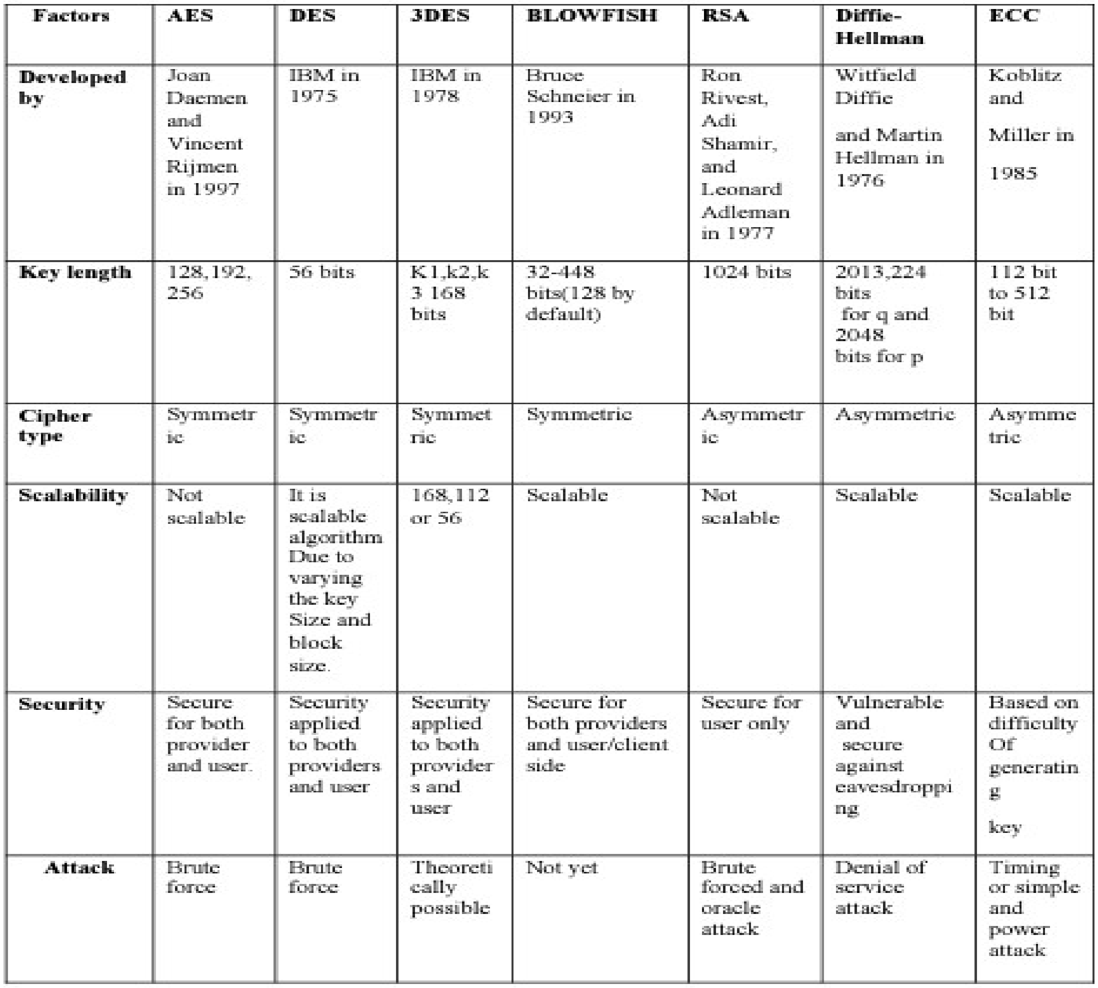
(Nadeem & Javed, 2005) stated that any encryption algorithm's main objective while designing it must be security from unauthorized access. Performance and implementation costs are significant considerations for any practical applications. It is standard practice to incorporate encryption algorithms in other applications such as e-commerce, banking, and online transaction processing ones, therefore a data encryption technique that is safe enough but poor in speed would not of much use. The four widely used secret key encryption algorithms—DES, 3DES, AES, and Blowfish—have all been implemented in this study, and the effectiveness of each is evaluated by encrypting input files with variable contents and sizes on various hardware platforms.

(Sood et al., 2013) stated that both cable and wireless methods of data transfer require privacy and security. The two primary techniques used in wireless means of communication when the data is in the route to prevent the data from falling into the wrong hands are steganography and cryptography. Cryptography is the science of composing the secret message and the science of encryption and decryption, whereas steganography conceals the messages inside other innocuous digital media without changing it so that no one can identify their presence.

3. COMPARISON BETWEEN SYMMETRIC-KEY ENCRYPTION AND ASYMMETRIC ENCRYPTION ALGORITHMS

(Nadeem & Javed, 2005) conducted performance evaluations for symmetric algorithms DES, 3DES, AES, and Blowfish written in Java and implemented on two distinct hardware platforms Algorithms were compared using a block cipher with varied block sizes and key sizes. They find that when the block size is greater, the speed time is faster; this is because large block sizes require less execution time to encrypt data, but small block sizes require more execution time for the same block cipher. It is also established that Blowfish is the fastest symmetric-key algorithm and Triple-DES is the slowest algorithm. Table 2 below compares the various algorithms under the symmetric-key encryption algorithm and the asymmetric encryption algorithm.

Table 2: Comparison between symmetric-key and asymmetric encryption algorithms (Source: Yassein et al., 2018).



Factors	AES	DES	3DES	BLOWFISH	RSA	Diffie-Hellman	ECC
Developed by	Joan Daemen and Vincent Rijmen in 1997	IBM in 1975	IBM in 1978	Bruce Schneier in 1993	Ron Rivest, Adi Shamir, and Leonard Adleman in 1977	Witfield Diffie and Martin Hellman in 1976	Koblitz and Miller in 1985
Key length	128,192, 256	56 bits	K1,k2,k3 168 bits	32-448 bits(128 by default)	1024 bits	2013,224 bits for q and 2048 bits for p	112 bit to 512 bit
Cipher type	Symmetric	Symmetric	Symmetric	Symmetric	Asymmetric	Asymmetric	Asymmetric
Scalability	Not scalable	It is scalable algorithm Due to varying the key Size and block size.	168,112 or 56	Scalable	Not scalable	Scalable	Scalable
Security	Secure for both provider and user.	Security applied to both providers and user	Security applied to both providers and user	Secure for both providers and user/client side	Secure for user only	Vulnerable and secure against eavesdropping	Based on difficulty Of generating key
Attack	Brute force	Brute force	Theoretically possible	Not yet	Brute forced and oracle attack	Denial of service attack	Timing or simple and power attack

4. CONCLUDING REMARKS

In this paper, we reviewed the various data security techniques in wireless data communication. We focused on the two most common data security techniques– steganography and cryptography. We posited that steganography is the practice of hiding information in a media such that its presence cannot be detected while cryptography on the other hand is the science of encrypting information in a way that unintended recipients cannot interpret and then decrypting the said message back into plaintext. These techniques were highlighted showing their strengths and applicable scenarios.

REFERENCES

Fanfara, P., Danková, E., & Dufala, M. (2012). Usage of asymmetric encryption algorithms to enhance the security of sensitive data in secure communication. *IEEE 10th Jubilee International Symposium on Applied Machine Intelligence and Informatics, SAMI 2012 - Proceedings*, 213–217. https://doi.org/10.1109/SAMI.2012.6208959

Kadhim, A. N., & Sadkhan, S. B. (2021). Security Threats in Wireless Network Communication-Status, Challenges, and Future Trends. *2021 International Conference on Advanced Computer Applications, ACA 2021*, 176–181. https://doi.org/10.1109/ACA52198.2021.9626810

Kessler, G. C. (2019). *An Overview of Cryptography (Updated Version*. *January*, 1–65. https://www.garykessler.net/library/crypto.html

Kumar, U., & Gambhir, S. (2014). A Literature Review of Security Threats to Wireless Networks. *International Journal of Future Generation Communication and Networking*, *7*(4), 25–34. https://doi.org/10.14257/ijfgcn.2014.7.4.03

Mukta, S. H., & Azad, S. (2014). Secure hash algorithm ADVANCED ENCRYPTION STANDARD. *Practical Cryptography: Algorithms and Implementations Using C++*, *6*(2), 207–223.

Nadeem, A., & Javed, M. Y. (2005). A performance comparison of data encryption algorithms. *Proceedings of 1st International Conference on Information and Communication Technology, ICICT 2005*, *2005*(September 2005), 84–89. https://doi.org/10.1109/ICICT.2005.1598556

NIST. (2017). Report on Lightweight Cryptography March 2017 • Final Publication : https://doi.org/10.6028/NIST.IR.8114 (which links to • Information on other NIST cybersecurity publications a. *Nist*, *8114*(March).

Sharma, K., & Dhir, N. (2014). A Study of Wireless Networks : WLANs , WPANs , WMANs , and WWANs with Comparison. *IJCSIT International Journal of Computer Science & Information Technology*, *5*(6), 7810–7813.

Sood, M., Wagh, M., & Cheema, M. (2013). *A Review on Various Data Security Techniques in Wireless Communication System*. *3*(2), 883–890.

Ubaidullah, M., & Makki, Q. (2016). A Review on Symmetric Key Encryption Techniques in Cryptography. *International Journal of Computer Applications*, *147*(10), 43–48. https://doi.org/10.5120/ijca2016911203

Vuppala, A., Roshan, R. S., Nawaz, S., & Ravindra, J. V. R. (2020). An Efficient Optimization and Secured Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm. *Procedia Computer Science*, *171*(2019), 1054–1063. https://doi.org/10.1016/j.procs.2020.04.113

Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2018). Comprehensive study of symmetric key and asymmetric key encryption algorithms. *Proceedings of 2017 International Conference on Engineering and Technology, ICET 2017*, *2018-January*, 1–7. https://doi.org/10.1109/ICEngTechnol.2017.8308215