A New Method Encryption and Decryption

Ali Abdulwahhab Mohammed*
Lecturer, College of Remote Sensing and Geophysics, Department of Remote Sensing, AL-Karkh University of Sciences, Baghdad, Iraq. E-mail: ali_abdulwahhab@kus.edu.iq

Haitham A. Anwer
Engineering, Ministry of Transportation, Iraqi Airways Company, Baghdad, Iraq.
E-mail: haitham.ameer90@gmail.com

Received November 07, 2020; Accepted December 12, 2020
ISSN: 1735-188X
DOI: 10.14704/WEB/V18I1/WEB18002

Abstract

In all times manual investigation and decryption of enciphered archives is a repetitive and mistake inclined work. Regularly considerably in the wake of investing a lot of energy in a specific figure, no decipherment can be found. Computerizing the unscrambling of different kinds of figures makes it conceivable to filter through the huge number of encoded messages found in libraries and files. We propose in this paper new algorithm has been made to encrypt the information; this algorithm works to shield information from robbery and can't be decrypted in the text. It is taken care of precisely to very accurately to avoid any penetration to arrive at the first text. It tends to be used in companies or some other system; however, it takes a long time to encrypt it. To the first text when encryption to ensure the assurance of information in full and security. Encrypted text contains a unique key, even when stolen. The private key can't be decrypted by the specialist and licensed by the maker of the code in order to protect the data in an excellent manner. While demonstrating in addition much stronger security guarantees with regards to Differential/ direct assaults. Specifically, we are can to provide new Method Encryption and Decryption with strong bounds for all versions.

Keywords

Encryption, Cipher, Decryption, Algorithm, Security, Information.

Introduction

During the most recent decades, data security has become a critical issue. Encrypting and decrypting data have starting late been broadly explored and made considering the way that there is an interest for a more grounded encryption and decoding which is very hard

to split. The Cryptography assumes significance jobs (delete) to the satisfaction of these requests. In These days, a large number of analysts have the proposed a considerable lot of the encryption and unscrambling algorithms, for the example, AES (Advanced Encryption Standard), DES (Data Encryption standard), RSA (Rivest–Shamir–Adleman), what's more, However, the vast majority of the proposed algorithms experienced a few issues, the security destinations were upgraded by another methodology for Complex scrambling and unraveling Information which keeps up the security on the correspondence channels by making it difficult for attacker to predicate a model similarly as speed of the encryption - unscrambling Scheme [1][2].

The plan of code and cipher systems has experienced significant changes in present day times. Ground-breaking (PCs) have brought about a blast of e-mail, e-banking, and e-commerce, and as an outcome the encryption of interchanges to ensure security has gotten a matter of open premium and noteworthiness. Furthermore, and investigations many cipher systems extending from the soonest and rudimentary to the latest and modern, for example RSA and DES, similarly as wartime machines, such as, the Hagelin and Enigma and ciphers utilized by spies [3][4][5]. In the research paper [6][7] the "Goldwasser – Micali" (GM) encryption scheme is an public key encryption differentiation of being the primary probabilistic public key encryption contrive which is provably secure under standard cryptographic presumptions. The work in [8] distributed cipher type classifier for conventional ciphers 2. This classifier is prepared on 16; 800 cipher texts and is executed in Java Script to run in the web program. The client can give the cipher text message as contribution to a site page that profits the classifier's gauges. The source code of the classifier is accessible on the web. Our work incorporates a reimplementation of the highlights utilized in that classifier. As models for work that manages the computerized decipherment of cipher texts, we point to [9][10]. These distributions create particular a algorithms for solving basic and homophonic replacement ciphers, which are just two out of the 56 cipher types characterized by the ACA (American Cryptogram Association). In [11] which present a cipher type classifier for the finalist the algorithms of the AES challenge.

The refined chips and sensors are implanted in the physical things that envelop us, and transmitting important information. The route toward sharing such huge measure of data starts with the gadgets themselves which ought to safely speak with the (Internet of Things) IoT stage. This stage coordinates the information from numerous gadgets and applies examination to impart the most important information to the applications. The (Internet of Things) IoT is taking the standard web, sensor system and compact system to another level as everything will be related with the web. A matter of worry that must be

held getting looked at is to guarantee the issues related to classification, information respectability and realness that will create by virtue of protection and security assurance [12][13]. And other wise Homomorphic encryption is a type of encryption which permits explicit kinds of calculations to be done on cipher texts and make an encoded outcome which, when decoded, matches the aftereffect of tasks performed on the plaintexts. This is a needed component in current correspondence system structures [14] [15].

This paper presents a new interesting algorithm of encryption and decryption that is useful to be used nowadays. The main work contribution is focused fundamentally on a new encryption and decryption method that it is used a new algorithm with different types of encryption techniques. In previous some works, it was easy to break or open encrypted words, either by analyzing or by guessing the password, and this facilitates the penetration of the encrypted texts. So, our proposed new method can solve such weak point in previous encryption and decryption techniques. The **motivation** of this research is to overcome one of the most challenges for data security so we need to do a good studying and defining the encryption and decryption noting that these processes take a long time to encrypt it. And **The Objectives** of this research are**: a-**Provide extended with optimized transfer encryption and Decryption Information rates and QoS, **b-**Another important is increasing in manual investigation and decryption of enciphered archives is a repetitive and mistake inclined work, **c-**the demand computerizing the unscrambling of different kinds of figures makes it conceivable to filter through the huge number of encoded messages found in libraries and files. And the **contributions** of this manuscript are: **a-**We propose in this paper new algorithm has been made to encrypt the information, **b-**This algorithm works to shc-ield information from robbery and can't be decrypted in the text, **c-**It is taken care of precisely to very accurately to avoid any penetration to arrive at the first text. **d-**The private key can't be decrypted by the specialist and licensed by the maker of the code in order to protect the data in an excellent manner, **e-**Provide new Method Encryption and Decryption with strong bounds for all versions.

As for this new method, it cannot be analyzed or guessed in any way, and this is what distinguishes it from the rest of the methods the rest of the paper is organized as follows: section 2. Gives an overview Basic Idea for Encryption, Decryption and Cryptography types' Next section 3, provides System Model an Encryption Design Elements In section 4, the steps of the proposed algorithm are explained of Encryption and Decryption Process section 5 shown the results Finally, section 6 introduces the experimental Conclusions for an interesting algorithm of encryption and Decryption that are currently used with other existing techniques.

Basic Idea

In basic Idea we explain Concepts Encryption and Decryption and other Cryptography types.

Concept Encryption

Encryption:- It is security instrument for PC organizes. It is procedure of changing over data recognized as plain text utilizing an algorithm to make it indistinguishable recognized as cipher text to anybody aside from those handling uncommon information, for the most part alluded to as key. It is the best effective technique to accomplish information security. As encryption is the science used to shield the security and protection of information, Crypto assessment is a science to break and break secure correspondence [16].

Concept Decryption

Decryption:- It is procedure in which taking encoded text and changing over it again into (authentic text) and (into text) that you or the PC can peruse and understand. Decryption is utilized for un-encoding the information with keys or the algorithm. Cryptography utilizes the decoding procedure at the collector side to acquire the first message from non-coherent message of Cipher Text. The decoding procedure requires two things- a key and algorithm. A Decryption the algorithm demonstrates the system that has been utilized in Decryption. For the most part, (the decoding algorithm and encryption are same).

Encryption or Cryptography Types

Currently there are two types of encryption:

Traditional Encryption

An encryption system is a methodology which takes the first message “plaintext” and a little snippet of data masterminded ahead of time among sender and recipient the key and makes an encoded rendition of the message cipher text. At the point when we are thinking about the nature of an encryption system, we accept the individual attempting to interpret the message comprehends what the general methodology is and is taking a gander at the cipher text - the main thing he doesn't have is the key. We additionally accept the individual sending messages doesn't invest energy attempting to think up a hard to-peruse message by utilizing letter frequencies or abnormal words the sender is relying on the system to give all the required security.

Traditional Encryption Systems Include

Caesar Code: An old technique made by Tsar Julius to work the encrypted of the messages between the areas of the army has proved effective in his time. But in our time and with the developments everywhere this method cannot be used this way for the speed of detection of the content of encrypted messages. In the following example illustrates how Caesar's code decodes on the off chance that we code the word "SECRET" and utilize the estimation of the key 3, we change the situation of the letters starting with the third letter, "D", so the request for the letters will be as per the following [19]:

(A B C D E F G H I J K L M N O P Q R S T U V W X Y Z)
Characters after putting the new value in the key"3"Is in the current shape:
(D E F G H I J K L M N O P Q R S T U V W X Y Z A B C)

Presently the estimation of (D à A, BE à, F à C) and so on. Thus, along these lines, “SECRET" will be "VHFUHW", to enable any other individual to peruse your scrambled message, you should send it the estimation of the "3" key. Standard Data Encryption (SDE): his system was progressed in the late 1970s by the US National Security Agency, and it is not feasible to use it within nowadays of computer systems and the faster processing of data, as the content of encrypted messages may be detected in a low time. (IDEA), (AES), (3DES) and blowfish, which are new sophisticated and proven nowadays, are coding industry. All of the above examples depend on the one-key principle of encryption and decryption.

Public Key Encryption

“Cryptography Asymmetric” The system was created in the seventies in UK and was used exclusively for specific segments of the legislature and depends on the rule of two keys, namely the private and public keys, as the (public key) is to scramble messages. And the (public key) is sent to all individuals and the private key to decode messages. as the private key is kept by the proprietor and not sent to any individual Who needs to send you an encoded message It utilizes the (public key) to scramble and afterward receive and unscramble it with your (private key) [20][21]. Demonstrates encryption work using (private key) and (public key), and some examples of the (public key) encryption of systems, **(Pretty Good Privacy) (DSA), (PGP), (Deffie-Hellman), (RSA), (Elgamal).**

Every one of these systems depends on the principle of awry encryption or encryption using private key and public key.

System Model

The Design Elements system contains a number of fields designated for encryption and decryption. In the first field: Plaintext: Enter the text to be encoded.The second field is cipher text: the text that is encrypted using the algorithm It contains an interface on a number of buttons dedicated to opening a document and saving a document. It is also possible to save the private encoding code and copy and paste documents. A new page can be created in the areas that have been hidden is the encoding code and the way it was encrypted has been hidden to ensure protection the information in an excellent manner as illustrates in figure 1. The special information was hidden in the program for security of theft, but the texts are clear and encrypted too, and figure.2, Shows Process of Block diagram of Encryption and Decryption.

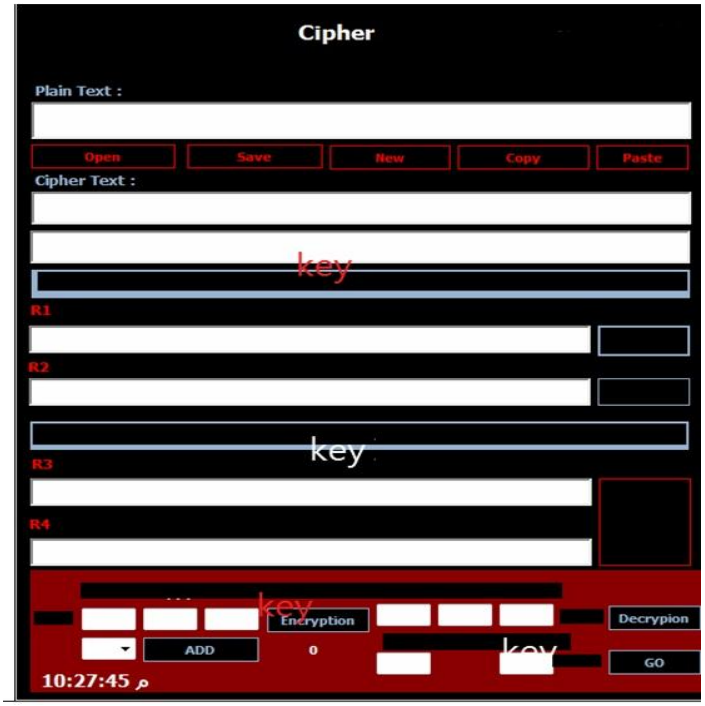

Figure 1 Illustrates Home page of program

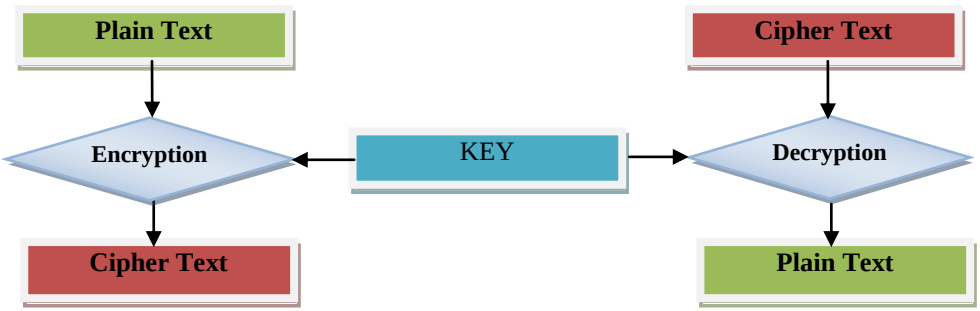

Figure 2 Block diagram of Encryption and Decryption Process

Proposed Algorithm

The process of data encryption is a complex way which is done through a number of attempts and the use of a number of mathematical functions and symbols to work algorithm is specialized in data encryption and therefore a new way was developed to encrypt data fully and through special mathematical equations. When you start encrypting the text, a (public key) and the (private key) are provided as shown in the algorithm. If the condition of the encrypted text is met with the (private key) you will get of the (original text), and final stat can print message. If the encrypted text is available and the private key is not available, the original text cannot be accessed in any way it was known the innovative way enables the user to protect his information completely and perfectly. The algorithm Encryption and Decryption Process as shown in figure.3.

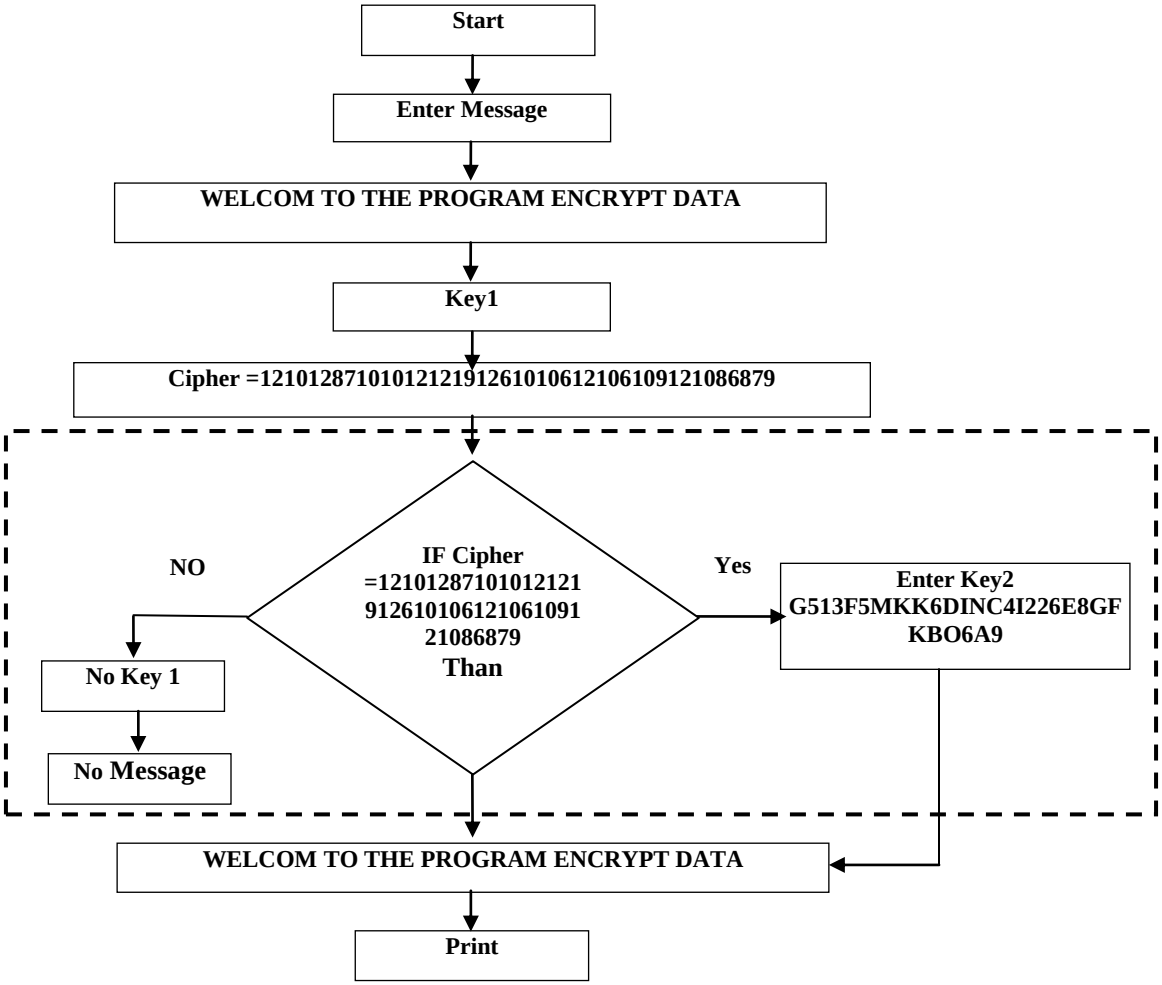

Figure 3 Algorithm of Encryption and Decryption Process

We can more Explain the process of encryption is done through a number of steps if the text encryption or decrypted text as described in the Block diagram in figure.4 in

beginning to enter the text to be encrypted and the status of a general key to be entered, for example we enter the original text and then put the public key and Then the encoded text comes out with the private key and at the end decodes the text.

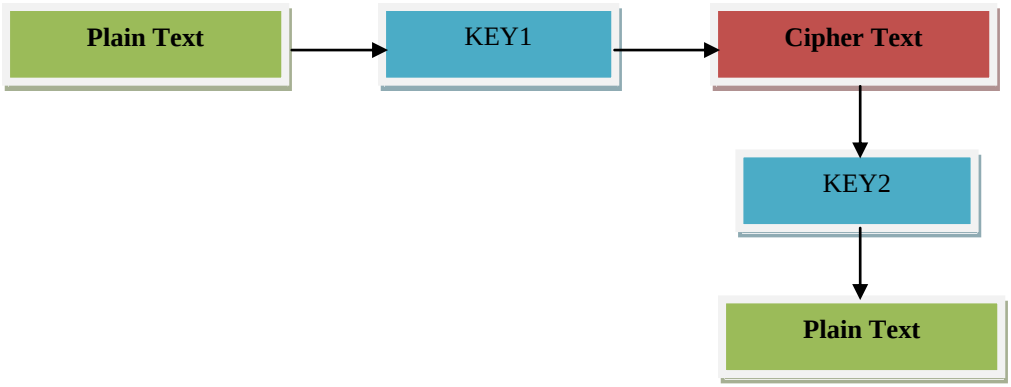

Figure 4 Block diagram of encryption text and decrypted text

Results

The proposed new algorithm has been created to encrypt the data and includes efficient and secure. The results Method of applying the proposed this algorithm works to protect data from theft and cannot be decrypted in the text. It is handled very accurately to avoid any penetration to reach the original text. It can be used in companies or any other system, but it takes a long time to encrypt it. To the original text when encryption to ensure the protection of data in full and security. Encrypted text contains a special key, even when stolen. The private key cannot be decrypted by the specialist and licensed by the creator of the code in order to protect the information in an excellent manner the final result we find new method designated for encryption and decryption and the table.1 as shown below. In the first field, regular text is entered hence; the general code of the first key and the special code of the second key were specified through this process, the encoded text shown.

Table 1 Illustrated the results new method designated for encryption and decryption

State	Results
Plaintext	WELCOM TO THE PROGRAM ENCRYPT DATA
Key1 (Public)	7
Cipher Text	12101287101012121912610106121061091210868 79
Key2	G513F5MKK6DINC4I226E8GFKBO6A9
Plaintext	WELCOM TO THE PROGRAM ENCRYPT DATA

See example below in Figure5.That explained the table above and Shown how encryption of the data is done through encryption process and mathematical operations. Example: - We insert in the text of the original we enter the general key and then enter the text with the public key in a series of mathematical equations to generate encrypted text with a special key for the code.

Plain text = WELCOM TO THE PROGRAM ENCRYPT DATA

Now a general key is being used that is used for camouflage, which is often not the real key

Key1 (Public) =7

When you finish placing the code and the traffic in the mathematical functions, the encrypted text shown is presented to you and it is very difficult to know the number of letters in the existing code.

Cipher Text =121012871010121219126101061210610912108687 9

As mentioned earlier it is difficult to know the number of characters in the encrypted message and this is what distinguishes them. But when you provide the private key for the code will be the number of characters in the code sent but cannot decrypt even if the (private key) and the (public key) because of mathematical equivalent of the special decoding and separation of characters from each other

Key2 = G513F5MKK6DINC4I226E8GFKBO6A9

In the final stat can we will get the original text message

Plain text = WELCOM TO THE PROGRAM ENCRYPT DATA

Here we want to show that all examples are applied in the same Method

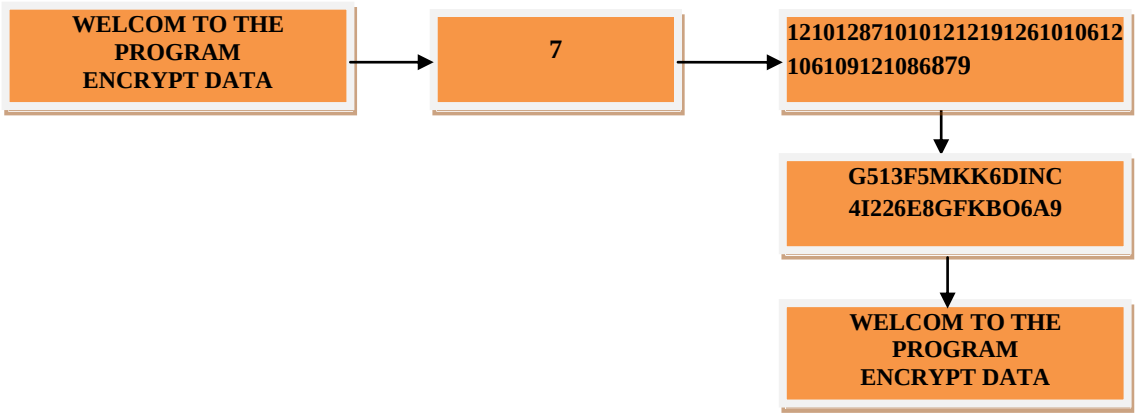

Figure 5 Block diagram is example how Encryption and Decryption of the data

Finally the example in table. 2 as shown the comparison between the new method Cipher and another old method (old and the modern systems), and through the results we notice the difference between them.

Table 2 Comparison between the new methods proposes with old method

A new Method Encryption and Decryption		
Plaintext	Cipher text	KEY1
HI HOW ARE YOU	PPquyrstysr	5
Caesar Cipher		
HI HOW ARE YOU	**kl krz duh brx**	**3**

Conclusions

In this paper, we propose another generally mainstream and intriguing the algorithm of encryption and Decryption that are as of now utilized. And what's more, this paper centers for the most part around as of now. A new Method Encryption and Decryption with different a type of encryption techniques, Encryption and Decryption plays significant job in development expanding of the information stockpiling and correspondence. It is utilized to accomplish the mains of security objectives like secrecy, honesty, confirmation, integrity, and non-renouncement. The utility new Method Encryption and Decryption is great, as it furnishes protection and security with every one of its ideas of information transmitted over open systems. There is a requirement for solid Encryption and Decryption strategies in light of the fact that with the fast advancement of the PC it lessens the quality of Encryption and Decryption; on the grounds that speeding up the PC implies shortening the time required by the PC to break or recognize a key Encryption and Decryption. This methodology is effective for giving higher honesty, privacy, and to achieve data security.

References

Ming-yu, Y. (2011). A new algorithm for encryption/decryption based on artificial immunity theory. *In IEEE International Conference on Electronics, Communications and Control (ICECC)*, 1839-1842.

Abdullah, A.M., & Aziz, R H.H. (2016). New approaches to encrypt and decrypt data in image using cryptography and steganography algorithm. *International Journal of Computer Applications, 143*(4), 11-17.

Beachem, B.R., & Smith, M.K. (2013). *Key management to protect encrypted data of an endpoint computing device.* U.S. Patent No. 8,588,422.

Abbood, E.A., Neamah, R.M., & Abdulkadhm, S. (2018). Text in Image Hiding using Developed LSB and Random Method. *International Journal of Electrical & Computer Engineering, 8*(4), 2088-8708.

Lyakhovitskiy, G.B., & Tsang, M.H. (2014). *Managing self-encrypting drives in decentralized environments.* U.S. Patent No. 8,856,553.

Galbraith, S.D. (2012). *Mathematics of public key cryptography*. Cambridge University Press.

Nuhn, M., Schamper, J., & Ney, H. (2013). Beam search for solving substitution ciphers. *In Proceedings of the 51st Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, 1568-1576.

Ravi, S., & Knight, K. (2011). Bayesian inference for Zodiac and other homophonic ciphers. *In Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies*, 239-247.

Latef, S., Hassan, N.A., & Dhannoon, B.N. (2011). Color image encryption using random password seed and linear feedback shift register. *Al-Nahrain Journal of Science, 14*(1), 186-192.

Furht, B., Muharemagic, E., & Socek, D. (2005). An Overview of Modern Cryptography. *Multimedia Encryption and Watermarking*, 31-51.

Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: a review. *In IEEE international conference on computer science and electronics engineering*, 3, 648-651.

Usman, M., Ahmed, I., Aslam, M.I., Khan, S., & Shah, U.A. (2017). SIT: a lightweight encryption algorithm for secure internet of things. *(IJACSA) International Journal of Advanced Computer Science and Applications, 8*(1), 1-10.

Vaikuntanathan, V. (2011). Computing blindfolded: New developments in fully homomorphic encryption. *In IEEE 52nd Annual Symposium on Foundations of Computer Science*, 5-16.

Adams, C., & Lloyd, S. (1999). *Understanding public-key infrastructure: concepts, standards, and deployment considerations*. Sams Publishing.

Gerhart, D.E., Lappi, C., Lipps, D.R., & Walker, W.J. (2018). *Method and apparatus to generate zero content over garbage data when encryption parameters are changed.* U.S. Patent Application 15/967,033.

Walker, W.J., Lappi, C., Gerhart, D.E., & Lipps, D.R. (2019). *Method to generate pattern data over garbage data when encryption parameters are changed.* U.S. Patent No. 10,372,627.

Zhao, M.W., Mao, R., & Jiang, R.A. (2009). Transparent encryption file system model based on filter driver. *Computer Engineering, 1*, 51.

Yun-Peng, Z., Wei, L., Shui-Ping, C., Zheng-Jun, Z., Xuan, N., & Wei-di, D. (2009, October). Digital image encryption algorithm based on chaos and improved DES. *In IEEE International Conference on Systems, Man and Cybernetics*, 474-479.

Churchhouse, R., Churchhouse, R.F., & Churchhouse, R.F. (2002). *Codes and ciphers: Julius Caesar, the Enigma, and the Internet*. Cambridge University Press.

Hwang, Y.H., & Lee, P.J. (2007). Public key encryption with conjunctive keyword search and its extension to a multi-user system. *In International conference on pairing-based cryptography*. Springer, Berlin, Heidelberg, 2-22.

Baek, J., Safavi-Naini, R., & Susilo, W. (2008). Public key encryption with keyword search revisited. *In International conference on Computational Science and Its Applications, Springer, Berlin, Heidelberg*, 1249-1259.