Al-Salam Journal for Engineering and Technology
Journal Homepage: http://journal.alsalam.edu.iq/index.php/ajest
ISSN: 2790-4822

Review : Methods of Cryptography

Saja Jumaa Hammad [1], Dr.Qusay Abboodi Ali [2], Dr. Mshari A.Alshmmri [1*]

[1]College of Computer Sciences and Mathematics ,Tikrit University, Tikrit , IRAQ

[2]College of administration and economics , Tikrit University , Head of Technical , Tikrit , IRAQ

* Corresponding author: Dr. Mshari A.Alshmmri

DOI: https://doi.org/10.55145/ajest.2022.01.02.006
Received June 2022; Accepted July 2022; Available online July 2022

ABSTRACT: In order to safeguard the information and data that must be protected from any interference or incursion, security is one of the most significant and prominent concepts at the moment. There are several techniques to ensure security and the protection of our data, but cryptography is the most crucial. Because of the importance of the documents and information that institutions must deal with or transport over the Internet, where unauthorized users or hackers can read and manipulate them, these documents must be encrypted using cipher methods and techniques.

Keywords: Security, Cryptography Methods, Data.

1. INTRODUCTION

The study and science of secret writing is known as cryptography. A cipher is a secretive writing technique in which plain text is transformed into cipher text. Decipherment, often known as “encryption”, is the process of converting cipher text back into plain text. Encipherment, on the other hand, is the act of transforming plain text into cipher text. Cryptographic key(s) regulates both encryption and decryption [1].

Highly sensitive data will be encrypted in such a way that even if the data is taken by unauthorised parties, these parties will be unable to determine the true data since the data they steal is encrypted [2] . The original data to be conveyed is known as plaintext in cryptography, while the data that has been encoded is known as ciphertext. The goal of cryptography is to keep the information contained in data private so that unauthorised people cannot access it [3].

2. Cryptographic Classification

Cryptographic algorithms can be categorized in a number of ways:

The number of keys used for encryption and decryption is one way to characterize cryptographic algorithms. Hash functions, symmetric encryption (also known as secret key cryptography), and asymmetric encryption (commonly known as public key cryptography) are the three different types of algorithms [4] , as shown in Fig 1.

*Corresponding author: author@organization.edu.co

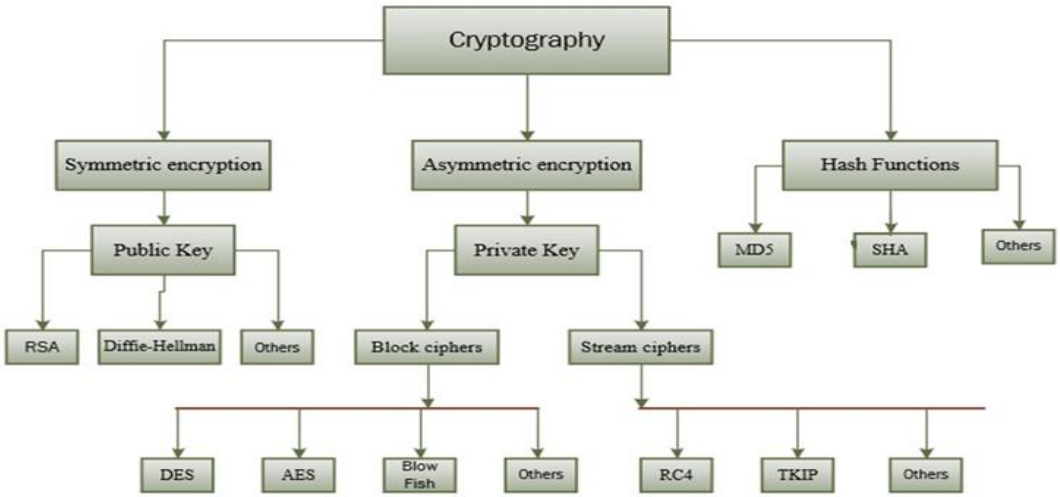

FIGURE 1. Types of Cryptography

2.1 Symmetric Key Encryption

Up until the late 1970s, only symmetric encryption—also referred to as single key encryption, shared key encryption, or secret key cryptography—was employed. [5] . The sender and recipient of the communication could both have access to the secret key, or just one of them might. If two parties utilize private key cryptography to communicate secretly, each party must possess a copy of the secret key. [6] . The encrypted message can be easily deciphered by the attacker if the secret key has been compromised. This type of cryptographic technology must be used since it provides faster service without using a lot of resources [2]. To date, different algorithms have been designed to explain symmetric key cipher.

2.2 Asymmetric Key Encryption

Public-key algorithms and, more generally, public-key cryptography are other names for asymmetric ciphers. With asymmetric ciphers, anyone can encrypt with the public encryption key (which could even be published in a newspaper), but only the intended recipient—who is aware of the decryption key—can unlock the message. The decryption key is often referred to as the private key or secret key, and the “encryption key” is known as the universal public key [7] .

The public key is made available to all entities, but the private key is kept hidden and never disclosed to any communication entities. Either a public key or a private key can be used to encrypt the data, depending on the security target (authentication or confidentiality) that the user wants to achieve [5]. When the data is encrypted using the receiver's public key, confidentiality can be attained. Only the receiver has the necessary key to unlock the encrypted data.

2.3 Hash function

It carries the transformation by employing mathematics to permanently encrypt data. SHA-1, MD5, and more hash functions.[8]. The hash function does not have keys as the ciphertext cannot be transformed to plaintext.

3. Cryptography Techniques

3.1 Substitution Techniques

The substitution technique systematically substitutes alternative letters or symbols for the plaintext's letters. Hill Cipher, Playfair Cipher, Monoalphabetic Cipher, Caesar Cipher, and Polyalphabetic Cipher are a few of the well-known substitution ciphers. [9].

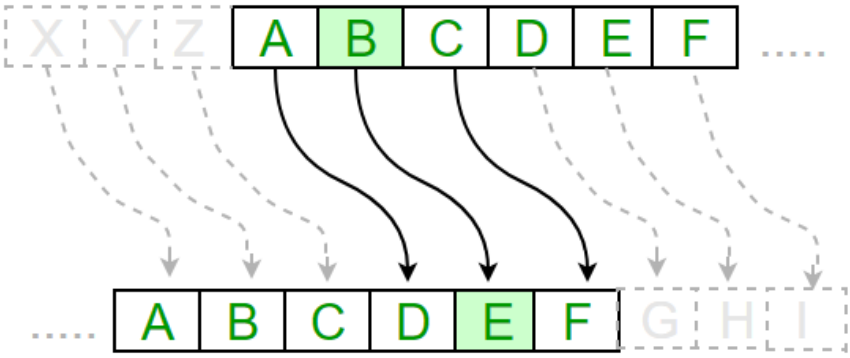

FIGURE 2. Substitution Techniques

3.2 Permutation (Transposition) Techniques

They discuss techniques for changing the order (or sequence) of the characters or components of the entry blocks. Techniques of transposition maintain the frequency distribution of single letters. [10]. A transposition cipher is the term used to describe this method. The simplest of these ciphers are the Column Transposition and Rail Fence techniques..

FIGURE 3. Transposition (permutation) Techniques

4. Cryptography Algorithms

In a cryptographic system, messages are encrypted and decrypted using sets of procedures or rules called cryptographic algorithms. They are techniques that protect data by preventing unauthorized users from accessing it, to put it simply .

Table 1 . Symmetric and Asymmetric Algorithms Types

Symmetric key algorithms	Variations of the DES (Data Encryption Algorithm) and AES (Advanced Encryption Standard) algorithms RC (Rivest Cipher) variants, 3DES, DECX, Blowfish, TwoFish, ThreeFish, IDEA, Serpent, Skipjack, “RC2, RC4, RC5, RC6”, “A5/1, A5/2” (mostly for GSM), and Chach
Asymmetric key algorithms	DSS -Digital Signature Standard, Diffie-Hellman, Elliptic Curve, RSA , ElGamal (based on Diffie-Hellman), and DSA (Digital Signature Algorithm)

4.1 Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES)

IBM created the Data Encryption Standard (DES) in 1975, and the American National Standards Institute (ANSI) published a description of it in 1981 under the name ANSI X3.92. One of the most widely used symmetric key standards now in use is this one [11] [12]. DES encrypts and decrypts data in 64-bit blocks using a 56-bit key. It accepts a 64-bit block of plaintext as input and outputs a 64-bit block of ciphertext, as seen in table 2. DES has 16 rounds, which means the core algorithm is executed 16 times to produce the ciphertext because it uses both permutations and substitutions and always operates on blocks of equal size. It has been found that the number of rounds in a brute-force attack causes the time required to find a key to grow exponentially. Therefore, as the number of rounds increases, the algorithm's security increases exponentially [12]. Triple DES employs three separate keys, each with a

length of 56 bits. Consequently, the final key length is 168 bits. Some authors claim that the key for 3DES uses 112 bits [13].

4.2 AES

The Data Encryption Standard will be replaced with the AES algorithm, a symmetric key encryption method (DES). It is the outcome of an international request for submissions of encryption algorithms launched by the "National Institute of Standards and Technology" (NIST) of the US Government in 1997 and finished in 2000 [12].

The AES encryption ratio is high. It has been shown to work well in 128-bit form. AES also employs keys of 192 and 256 bits for use in high-security encryption. AES operates at a fast speed. For encryption, AES uses various rounds of 10, 12, and 14. [13] Multiple transformations are applied to plaintext, including byte substitution, shifting of rows and columns, mixing of columns, and addition of round key transformations. [11]. Consequently, this is regarded as one of the greatest algorithms to date, according to several publications. Both hardware and software can use it.

4.3 Blowfish

Another algorithm that was primarily created to replace DES is called blowfish. As shown in table 2, this algorithm divides messages into blocks of 64 bits and encrypts each message separately. Some authors claim that blowfish lasts for 14 rounds, while others claim that it lasts for 16 rounds. The blowfish key length is not constant. Between 32 and 448 bits are possible. Utilizing Blowfish has many benefits, one of which is that it protects against dictionary assaults. Some writers claim that among the AES and DES variants, blowfish is a good algorithm [11] [13].

4.4 Variations of RC (RC2, RC4, and RC6)

RC is a block encoding algorithm that has been introduced back in 1987. The letters "RC" stand for either Ron's Code or Rivest Cipher. [11]. According to numerous authors, the range of RC is from RC1 to RC6. However, the majority of authors only discuss RC2, RC4, and RC6. The block size for RC2 is 64 bits, while the key size ranges from 8 to 1024 bits. Key sizes between 40 and 2048 bits can be used with RC4. In 1994, it was leaked. RC5 has a customizable key size (0-2040 bits), block size (32, 64, or 128), and number of rounds (0–255). The initial recommended set of parameters were a block size of 64 bits, a key size of 128 bits, and 12 rounds. RC6 is a descendant of RC5, which supports key sizes of 128, 192, and 256 bits while only supporting block sizes of 128 bits [13]. Some researchers have created RC6e (Enhancement of RC6), which operates on 256-bit blocks, whereas modified RC6 (MRC6) operates on 512-bit blocks .

4.5 RSA

One of the first algorithms, it uses a public encryption key and a secret decryption key to function. The most widely used encryption method up to this point is RSA. RSA uses 1024 bit streams, which can currently also be up to 4096 bytes, for keying purposes. The primary characteristic of RSA is its reliance on huge prime integer values [13]. The primary benefit of RSA is that its security is improved over other algorithms. It is actually one of the safest algorithms. The slow encryption performance, difficult key generation, and vulnerability to assaults are its main drawbacks. Making a public/private key combination, The three steps are: transforming plain text (data) into ciphertext (data), and decrypting the data to recover the original text [11] .

4.6 Diffie-Hellman (DH)

It is a protocol or technique that permits two cooperating entities to compute and exchange a key, then use this key in symmetric algorithms like AES [5]. Benefits include security, a complex enough algorithm, and the fact that the secret key is never broadcast over a channel. However, due to the lack of verification, the method is unreliable, expensive, and inappropriate for the majority of encryption situations [11].

5. Conclusion

Because this data can be accessed by a third party or an outsider, security is critical in transmitting and dealing with it. Cryptography is essential for the secure transmission of data. Many techniques and algorithms are used to encrypt and decrypt data .

The speed of encryption and decryption, the accuracy of encryption, the complexity of the operations, the level of security, and other factors distinguish these techniques .

ACKNOWLEDGEMENT

The authors would like to thank the reviewers for their comments

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

[1] T. M. Aung, H. H. Naing, and N. N. Hla, "A complex transformation of monoalphabetic cipher to polyalphabetic cipher:(Vigenère-Affine cipher)," *Int. J. Mach. Learn. Comput*, vol. 9, pp. 296-303, 2019.

[2] J. Jamaludin and R. Romindo, "Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security," *IJISTECH (International Journal of Information System & Technology)*, vol. 4, pp. 471-481, 2020.

[3] R. Romindo and J. Jamaludin, "Sistem pendukung keputusan menggunakan metode ANP untuk pemilihan toko daring terbaik di Politeknik Ganesha," *REMIK: Riset dan E-Jurnal Manajemen Informatika Komputer*, vol. 4, pp. 99-106, 2019.

[4] M. A. Alrammahi and H. Kaur, "Development of Advanced Encryption Standard (AES) Cryptography Algorithm for Wi-Fi Security Protocol," *International Journal of Advanced Research in Computer Science*, vol. 5, pp. 62-67, 2014.

[5] J. O. Olwenyi, A. T. Thomas, and A. Barsoum, "Modern Cryptographic Schemes: Applications and Comparative Study," *Journal of Network and Information Security*, vol. 7, pp. 28-34, 2019.

[6] S. Naser, "Cryptography: From The Ancient History to Now, It's Applications and a New Complete Numerical Model," *International Journal of Mathematics and Statistics Studies*, vol. 9, pp. 11-30, 2021.

[7] M. C. PRAKASH, "Performance evaluation of cloud data security framework using symmetric key algorithm," *IJCSMC*, vol. 8, pp. 25-33, 2019.

[8] Z. Al-Odat and S. Khan, "The sponge structure modulation application to overcome the security breaches for the md5 and sha-1 hash functions," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, 2019, pp. 811-816.

[9] D. V. V. Deepthi, B. H. Benny, and K. Sreenu, "Various ciphers in classical cryptography," in *Journal of Physics: Conference Series*, 2019, p. 012014.

[10] A. Salai and T. Nadu, "Evaluative study on substitution and transposition ciphers," *IJCRT*, vol. 6, pp. 155-160, 2018.

[11] M. Al-Shabi, "A survey on symmetric and asymmetric cryptography algorithms in information security," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 9, pp. 576-589, 2019.

[12] B. E. H. H. Hamouda, "Comparative study of different cryptographic algorithms," *Journal of Information Security*, vol. 11, pp. 138-148, 2020.

[13] N. Advani, C. Rathod, and A. M. Gonsai, "Comparative study of various cryptographic algorithms used for text, image, and video," in *Emerging Trends in Expert Applications and Security*, ed: Springer, 2019, pp. 393-399.