JOURNAL PUNJAB ACADEMY OF SCIENCES (Peer Reviewed Open Access Journal)
JPAS, 22: 27-33 (January-December, 2022)
Available online at www.jpas.in
ISSN 2229-7014 (P)

CRYPTOGRAPHY AND ITS TECHNIQUES: A REVIEW

Alka Bamotra
Department of Computer Science and IT, Baring Union Christian College,
Batala, Punjab, India
E-Mail: bamotraalka@gmail.com

ABSTRACT

With the internet having reached a level that merges with our lives, growing explosively during the last several decades, data security has become a main concern for anyone connected to the web. Data security ensures that our data is only accessible by the intended receiver and prevents any modification or alteration of data. In order to achieve this level of security, various algorithms and methods have been developed. Cryptography can be defined as techniques that cipher data, depending on specific algorithms that make the data unreadable to the human eye unless decrypted by algorithms that are predefined by the sender. So for providing data security many cryptography techniques are employed, such as symmetric and asymmetric techniques. Main concentration is on various algorithms including DES, RSA.

Keywords: RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm), ECC (Elliptic curve cryptography), Cryptography, Security, Algorithm, Cipher, Decryption, Data Security.

INTRODUCTION

Cryptography is an approach to accomplish confidentiality of messages. The term has a specific meaning in Greek: "secret writing". Nowadays, however, the privacy of individuals and organizations is provided through cryptography at a high level, making sure that information sent is secure in a way that the authorized receiver can access this information (Perrig *et al*, 2004). With historical roots, cryptography can be considered an old technique that is still being developed. Examples reach back to 2000 B.C., when the ancient Egyptians used "secret" hieroglyphics, as well as other evidence in the form of secret writings in ancient Greece or the famous Caesar cipher of ancient Rome (Massey, 1986). Billions of people around the globe use cryptography on a daily basis to protect data and information, although most do not know that they are using it. In addition to being extremely useful, it is also considered highly brittle, as cryptographic systems can become compromised due to a single programming or specification error (Schneider, 2004). It is the process of transforming the secret data or information into an unreadable or scrambled form. In fact it is the art of writing the message secretly. The concept of cryptography depends on five factors. These are discussed below (Perrig *et al*, 2004).

(a) Plain text: The message or information that we want to send secretly. The set of plain text is represented by P.

(b) Cipher text: It is the scrambled or unreadable form of information or message. The set of cipher text is represented by C.

(c) Key: It is the rule with the help of which data is scrambled. The set of keys is represented by K.

(d) Encryption Function: It is the method using which the cipher text is generated. The set of encryption function is represented by E(x).

(e) Decryption Function: It is the inverse function of E(x). It is the effort to generate the

original message. The set of decryption function is represented by D(x).

Thus, cryptography is depending on {P, C, K, E(x), D(x)}. Every user while communicating wants a secure network so that data communication should secure and no intruder can read their data. For providing secure data communication cryptography is used in wireless and wired network, where cryptography converts to plain text into cipher text and cipher text into a plain text. At a sender side plain text is converted into a cipher text known as encryption and receiver side cipher text is converted into a plain text known as decryption. Cryptography classified as Symmetric cryptography and Asymmetric cryptography techniques. In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. In asymmetric or public-key cryptography, there are two keys: a private key and a public key are used. The private key is kept by the receiver and public key is announced to the public. Further some types of asymmetric cryptography are given by different researchers. Some commonly used asymmetric cryptography techniques are RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm), ECC (Elliptic curve cryptography).The basic concept of a cryptographic system is to cipher information or data in order to achieve confidentiality of the information in a way that an unauthorized person would be unable to derive its meaning. Two of the most common uses of cryptography would be using it to transmit data through an insecure channel, such as the internet, or ensuring that unauthorized people do not understand what they are looking at in a scenario in which they have accessed the information. In cryptography, the concealed information is usually termed "plaintext", and the process of disguising the plaintext is defined as "encryption"; the encrypted plaintext is known as "ciphertext". This process is achieved by a number of rules known as "encryption algorithms". Usually, the encryption process relies on an "encryption key", which is then give to the encryption algorithm as input along with the information. Using a "decryption algorithm", the receiving side can retrieve the information using the appropriate "decryption key" (Jirwan *et al*, 2013).

RESULTS AND DISCUSSION

Linke and Hollan (2007) pointed out that network and computer security is a new and fast-moving technology within the computer science field, with computer security teaching to be a target that never stops moving. Algorithmic and mathematic aspects, such as hashing techniques and encryption, are the main focus of security courses.

Khalifa *et al* (2004) demonstrated the primary basic concepts, characteristics, and goals of cryptography. They discussed that in our age, i.e. the age of information, communication has contributed to the growth of technology and therefore has an important role that requires privacy to be protected and assured when data is sent through the medium of communication.

Jirwan *et al* (2013) referred to data communication as depending mainly on digital data communication, in which data security has the highest priority when using encryption algorithms in order for data to reach the intended users safely without being compromised.

In a review on network security and cryptography, Tayal *et al* (2017) mentioned that with the emergence of social networks and commerce applications, huge amounts of data are produced daily by organizations across the world. This makes information security a huge issue in terms of ensuring that the transfer of data through the web is guaranteed.

Gupta *et al* (2014) showcased the origins and meaning of cryptography as well as how information security has become a challenging issue in the fields of computers and communications. In addition to demonstrating cryptography as a way to ensure identification, availability, integrity, authentication, and confidentiality of users and their data by

providing security and privacy, this paper also provides various asymmetric algorithms that have given us the ability to protect and secure data.

A study conducted by Callas (2014) referred to topics such as cryptography, privacy enhancing technologies, legal changes concerned with cryptography, reliability, and technologies used in privacy enhancement. He noted that it is how society uses cryptography that will determine the future of cryptography, which depends on regulations, current laws, and customs as well as what society expects it to achieve. He indicated that there are many gaps in the field of cryptography for future researchers to fill.

Massey (1986) pointed out that there are two goals that cryptography aims to achieve as they are: authenticity and/or secrecy. In terms of the security that it affords (which can be either practical or theoretical), he discussed both Shannon's theory of theoretical secrecy as well as Simmon's theory of theoretical authenticity (Massey, 1986).

Schneier (2004) concluded that secrecy of security as a good thing is a myth and that it is not good for security to be secret, as security completely relying on secrecy can be fragile. If that secrecy was lost, regaining it would be impossible. Schneier further expressed that cryptography based on short secret keys that can be easily transferred and changed must rely on a basic principle, which is for the cryptographic algorithms to be simultaneously strong and public in order to offer good security.

Varol *et al* (2007) studied on symmetric encryption which is used for the encryption of a certain text or speech. In this study the content to be encrypted is first converted into an encapsulation cipher that cannot be understood by a cipher algorithm.

Cryptography techniques

Caesar Cipher: This is one of the oldest and earliest examples of cryptography, invented by Julius Caesar, the emperor of Rome, during the Gallic Wars. In this type of algorithm, the letters A through We are encrypted by being represented with the letters that come three places ahead of each letter in the alphabet, while the remaining letters A, B, and C are represented by X, Y, and Z. This means that a "shift" of 3 is used, although by using any of the numbers between 1 and 25 we could obtain a similar effect on the encrypted text. Therefore, nowadays, a shift is often regarded as a Caesar Cipher (Jirwan *et al*, 2013). As the Caesar cipher is one of the simplest examples of cryptography, it is simple to break. In order for the ciphertext to be decrypted, the letters that were shifted get shifted three letters back to their previous positions. Despite this weakness, it might been strong enough in historical times when Julius Caesar used it during his wars. Although, as the shifted letter in the Caesar Cipher is always three, anyone trying to decrypt the ciphertext has only to shift the letters to decrypt it (Tanyal *et al*, 2017).

Simple Substitution Ciphers : Take the Simple Substitutions Cipher, also known as Monoalphabetic Cipher, as an example. In a Simple Substitution Cipher, we take the alphabet letters and place them in random order under the alphabet written correctly, as seen here:

A B C D E F G H I J K L M D I
M T B Z S Y K V O F
N O P Q R S T U V W X Y Z
E R J A U W P X H L C N G

In the encryption and decryption, the same key is used. The rule of encryption here is that "each letter gets replaced by the letter beneath it", and the rule of decryption would be the opposite. For instance, the corresponding ciphertext for the plaintext CAN is QDN [18]

Transposition Ciphers: Other cipher families work by ordering the letters of the plaintext to transform it to cipher text using a key and particular rule. Transposition can be defined as the alteration of the letters in the plaintext through rules and a specific key. A columnar transposition cipher can be considered as one of the simplest types of transposition cipher

and has two forms: the first is called "complete columnar transposition", while the second is "incomplete columnar". Regardless of which form is used, a rectangle shape is utilized to represent the written plaintext horizontally, and its width should correspond to the length of the key being used. There can be as many rows as necessary to write the message. When complete columnar transposition is used, the plaintext is written, and all empty columns are filled with null so that each column has the same length. However, when it comes to an incomplete columnar transposition cipher, the columns are not required to be completed, so the null characters are left out. This results in columns of different lengths, which can cause the ciphertext to be more difficult to decipher without the key (Gupta and Walia, 2014).

Rivest Shamir and Adleman (RSA) algorithm: RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message (Perrig *et al*, 2004). RSA algorithm can be used in Wireless Sensor Network (WSN), because WSN is insecure network and vulnerable to many attacks because of broadcast nature of transmission medium. The security requirements of wireless sensor networks are : a. Confidentiality b. Integrity c. Authentication (Massey, 1986).

Diffie-Hellman Algorithm: This algorithm is used for exchanging cryptography keys between two users. Here user doesn't have any knowledge about the keys used by each other and they use a shared secret key over an insecure communication channel, then this key is used to encrypt subsequent communications using a symmetric key cipher. AK (Authenticated Key Agreement) and AKC (Authenticated Key agreement with key confirmation) protocols within a formal model of distributed computing and a unified model of key agreement is proposed with several variants of this model are demonstrated to provide secure AK and AKC protocol in the random oracle model. Here AK and AKC are made secure by providing clear, formal definitions of the goals of AK and AKC protocols, and secondly by furnishing practical, provably secure solutions in the random oracle model (Wilson, 1997).

Digital Signature Algorithm (DSA): It is used by receiver of a message to verify that the message has not been altered during transit as well as certain the sender's identity. A digital signature is an electronic version of a written signature in that the digital signature can be used in proving to the recipient or a third party that the message was, in fact, signed by the sender. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time (Anderson, 2004). One method for sending low size and capacity data by using DSA is proposed by Erfaneh Noorouzil et al. "Hash function" is used in this method and it generates dynamic and smaller size of bits which depends on each byte of data. The main function which is used for hashing is bitwise or and multiply functions. If hashed file sized is 4% of the original file in the messages with size lower than 1600 bytes. This algorithm can be used in several applications which have low file size for sending and want simple and fast algorithms for generating digital signature (Noorouzil et al 2014).

Elliptic Curve Cryptography (ECC): Elliptic curve cryptography is a relatively new family of public-key algorithms that can provide shorter key lengths and, depending upon the environment and application in which it is used, improved performance over system based on integer factorization and discrete logarithms (Lauter, 2004). Here its security, advantages and performance (Amin et al,

2008) are discussed. ECC has its security problems based on some difficult mathematical. Elliptic curve is based on a mathematical structure in which certain operation can be defined. These operations provide a one way function that can be used to produce efficient cryptographic systems. ECC uses this one way function is called Elliptic Curve Discrete logarithm Problem (ECDLP). The ECDLP is similar to the one way function on which DSA and Diffie-Hellman are based, and hence, elliptic curve analogs of each of these algorithms have been defined (Lauter, 2004).

CONCLUSION

Cryptography plays an essential and critical role in achieving the primary aims of security goals, such as authentication, integrity, confidentiality, and no-repudiation. Cryptographic algorithms are developed in order to achieve these goals. Cryptography has the important purpose of providing reliable, strong, and robust network and data security. In this paper, we demonstrated a review of some of the research that has been conducted in the field of cryptography as well as of how the various algorithms used in cryptography for different security purposes work. Cryptography will continue to emerge with IT and business plans in regard to protecting personal, financial, medical, and ecommerce data and providing a respectable level of privacy.

Table1. The various techniques used for cryptography by different researchers.

Year	Researcher	Techniques
2007	S. J. Lincke and A. Hollan	Hashing and Encryption
2004	Othman O. Khalifa	Communication Cryptography
2013	N. Jirwan, A. Singh and S. Vijay	Symmetric and Asymmetric method
2017	S. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal	RSA, DSA
2014	A. Gupta and N. K. Walia	Asymmetric Algorithm
2007	J. Callas	Information System Security
1986	J. L. Massey	Shannon's theory and Simmon's theory
2004	B. Schneier	Secret Keys
2017	N. Varol, F. Aydoğan and A. Varol	Cipher Algorithm

REFERENCES

Abdullah Said Alkalbani et al., 2010. "Comparison between RSA Hardware and Software Implementation for WSNs Security Schemes," In proceeding 3rd International Conference on ICT4M.

Amin, F. Jahangir, A. H. and Rasifard, H. 2008. "Analysis Of Publickey Cryptography For Wireless Sensor Networks Security," In Proceedings of World Academy of Science, Engineering and Technology.

Anderson, H. 2004. Introduction to Computer Security, Prentice Hall. pp 85-86.

Callas, J. 2007. "The Future of Cryptography," Information Systems Security, 16(1): 15-22.

Chandra M. Kota et al., 2002. "Implementation of the RSA algorithm and its cryptanalysis," In proceedings of the ASEE Gulf-Southwest Annual Conference.

David A. Carts. 2001. "A Review of the DiffieHellman Algorithm and its Use in Secure Internet Protocols," SANS institute.

Erfaneh Noorouzil et al, 2011. "A New Digital Signature Algorithm", International Conference on Machine Learning and Computing, IPCSIT vol.3.

Gupta, A. and Walia, N. K. 2014. "Cryptography Algorithms: A Review," International Journal of Engineering Development and Research, 2(2): 1667-1672.

Jirwan, N. Singh, A. and Vijay, S. 2013. "Review and Analysis of Cryptography Techniques," International Journal of Scientific & Engineering Research, 3(4): 1-6.

Khalifa, O. O. Islam, M. R. Khan, S. and Shebani, M. S. 2004. "Communications cryptography," in RF and Microwave Conference, RFM 2004. Proceedings, Selangor.

Lauter, K. 2004. "The Advantages of Elliptic Curve Cryptography for Wireless.

Lincke, S. J. and Hollan, A. 2007. "Network Security: Focus on Security, Skills, and Stability," in 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee.

Massey, J. L. 1986. "Cryptography-A selective survey," Digital Communications, 85: 3-25.

Perrig, A. Stankovic, J. and Wagner, D. 2004. "Security In Wireless Sensor Networks," ACM, 47(653).

Schneier, B. 2004. "The Non-Security of Secrecy," Communications of the ACM, 47(10): 120.

Singh, P Yadav et al., 2012. "Implementation of RSA algorithm using Elliptic Curve Algorithm for security and performance enhancement," International Journal of Scientific & Technology Research 1(4).

Tayal, S. Gupta, N. Gupta, P. Goyal, D. and Goyal, M. 2017. "A Review paper on Network Security and Cryptography," Advances in Computational Sciences and Technology , 10 (5): 763- 770.

Varol, N., Aydoğan F. and Varol, A. 2007. ,"Cyber Attacks Targetting Android Cellphones," in The 5th International Symposium on Digital Forensics and Security (ISDFS 2017), Tirgu Mures.

Wilson, S. B. et al., 1997. "Key agreement protocols and their security analysis."

Zuccherato, R. 2000. "Elliptic Curve Cryptography Support in Entrust," Entrust ltd. in Canada.