International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

A Research Paper on Cryptography

Ardalkar Shivam Dhanaji, Kaduskar Praful Gajanan, Kate Abhijit Pandurang
Department of Computer Engineering, Zeal College of Engineering and Research, Pune, Maharashtra, India

Article Info
Volume 8, Issue 1
Page Number : 328-336

Publication Issue :
January-February-2022

Article History
Accepted :20Feb2022
Published: 28 Feb2022

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.

Keywords — Cryptography, Security, Algorithm, Cipher, Decryption, Data Security.

I. INTRODUCTION

Cryptography is a technique to achieve 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 [1]. 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 [2].

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 [3].

II. LITERATURE REVIEW

Susan et al. [4] 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. As crackers find ways to hack network systems, new courses are created that cover the latest type of attacks, but each of these attacks become outdated daily due to the responses from new security software. With the continuous maturity of security terminology, security techniques

and skills continue to emerge in the practice of business, network optimization, security architecture, and legal foundation.

Othman O. Khalifa et al. [5] 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.

Nitin Jirwan et al. [6] 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. They also demonstrated the various cryptographic techniques that are used in the process of data communication, such as symmetric and asymmetric methods.

In a review on network security and cryptography, Sandeep Tayal et al. [7] 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. With more users connecting to the internet, this issue further demonstrates the necessity of cryptography techniques. This paper provides an overview of the various techniques used by networks to enhance security, such as cryptography.

Anjula Gupta et al. [8] 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, J. [9] 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. Additionally, the future of cryptography relies on a management system generating strong keys to ensure that only the right people with the right keys can gain access, while others without the keys cannot. Finally, Callas indicated that people's perspectives and thoughts about security and communication privacy are a mirror of the changes that occur in laws that came into existence through events such as the terrorist attacks of September 2001.

Therefore, cryptography will always play a role in the protection of data and information, for now and in the future.

Moving forward with the goals of cryptography, James L. Massey [10] 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.

Lastly, Schneier [11] 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. The only

reliable way to make more improvements in security is to embrace public scrutiny.

Varol, N. et al. [12] 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 chipher that cannot be understood by a cipher algorithm.

Chachapara, K. et al. [13] examined secure sharing with cryptography in cloud computing and demonstrated a framework that makes use of cryptography algorithms like RSA and AES, with AES been the most secure algorithm in cryptography. The cloud users can generate keys for different users with different permissions to access their files.

Orman, H. [14] mentioned that many discussions and developments are generated about cryptography, as the author stated the hash functions are playing a vital role in cryptography by supplying nearly number to any piece of data and by the years that MD5's weaknesses became known, it led to an unsettled feeling about how to design hash functions.

Gennaro, R. [15] discussed randomness in cryptography and explained that a random process is one whose consequences are unknown, and mentioned that this is why randomness is vital in cryptography since it provides a way to create information that an adversary can not learn or predict it.

Preneel, B. [16] demonstrated cryptography and information security in the post-Snowden era, where he discussed mass surveillance practices and the security of ICT systems as well as known ways in which sophisticated attackers can bypass or undermine cryptography.

Sadkhan, S. B. [17] pointed to the main process and trends of the fields in cryptography the time of Julius Cesar till the modern era, as well as mentioning the current status of the Arabic industrial and academical efforts in this field in the past that is related to thee existing cryptographic and search for new evaluation methods for the security of information.

CRYPTOGRAPHY CONCEPT

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" [18].

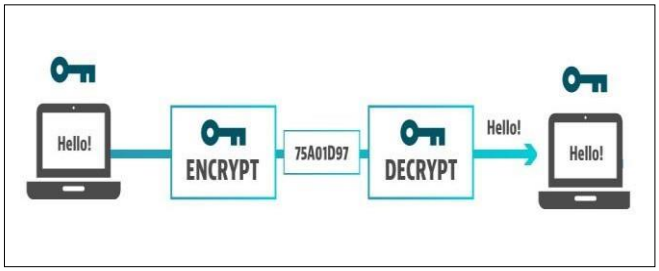

Fig. 1. Cryptography concept

III. HISTORICAL ALGORITHMS

In this section, a few historical algorithms will be introduced, along with pencil and paper examples for a nonmathematical reader. These algorithms were designed and used long before public key cryptography was proposed.

A. 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 [18].

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 [19].

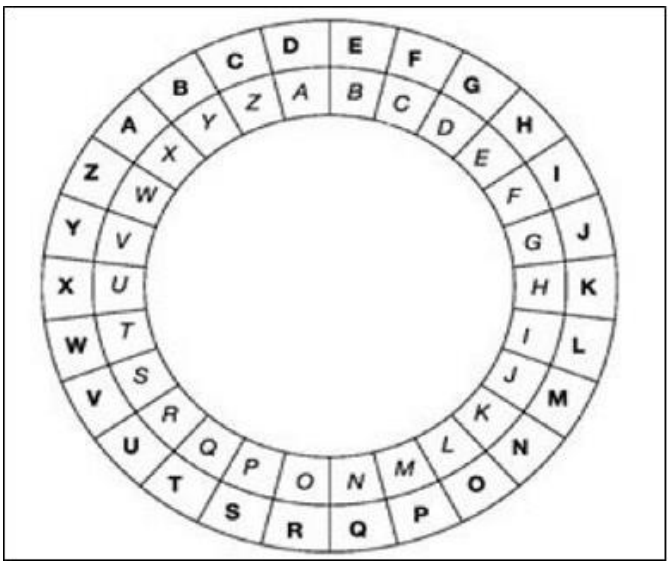

Fig. 2. Caesar Cipher encryption wheel

B. 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	Q	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]

C. 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. For example:

s e c o n d d i v i s o n a d v a n c i n g t o n i g h t x

The cipher text is then derived from the columns depending on the key. In this example, if we used the key "321654", the cipher text is going to be:

cvdng eiaii sdncn donox nsatt oivgh

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 [20].

IV. MODERN ALGORITHMS

A. Stream ciphers

Stream ciphers operate on pseudorandom bits generated from the key, and the plaintext is encrypted by XORing both the plaintext and the pseudorandom bits. Stream ciphers were sometimes avoided in the past, as they were more likely than block ciphers to be broken. Nowadays, however, after years of developing designs, the stream cipher has become more secure and can be trusted and relied on to be used in connections, Bluetooth, communications, mobile 4G, TLS connections, and so on.

In a stream cipher, each bit is encrypted individually. There are two types of stream ciphers: the first is the synchronous stream cipher, in which the key stream relies on the key; in the asynchronous cipher, though, the ciphertext is dependent on the key stream. In Figure 3, we have a dotted line. If it was present, the stream cipher would be asynchronous; otherwise it would be synchronous. The cipher feedback (CFB) would be an example of an asynchronous cipher [2].

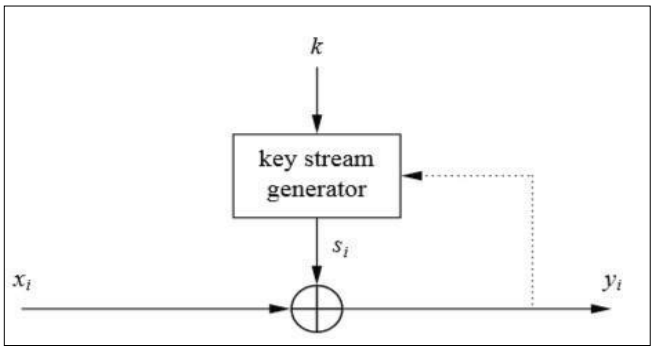

Fig. 3. Asynchronous and synchronous types of stream ciphers

B. Block ciphers:

This type of cipher consists of both an algorithm for encryption and an algorithm for decryption:

- A key (K) is given to the encryption algorithm (E) and a block of plaintext (P), of which C is the product that consists of a ciphertext block. The encryption operation can be expressed as: C = E (K, P).
- As for the decryption algorithm (D), this is the inverse of the previous operation in which the ciphertext is decrypted for the plaintext, P. It can be written as: P = D (K, C).

A pseudorandom permutation (PRP) is used in order to make the block cipher more secure. This means that if the key is kept secret, an attacker will not be able to decrypt the block cipher and compute the output from any input. This is as long as the secrecy of K and its randomness is assured from the attacker's view. In a general form, this means that the attacker would not have the ability to find any pattern in the values that are either input to or output from the block cipher.

In a block cipher, two values are generally referred to: the size of the block and the size of the key. The security relies on the value of both. Many block ciphers use a 64-bit block or a 128-bit block. As it is crucial that the blocks are not too large, the memory footprint and the ciphertext length are small in size. Regarding the ciphertext length, blocks instead of bits are processed in a block cipher. That is, if we wanted to encrypt a 16-bit message and the blocks with 128-bit blocks, we first need to the message to be converted to 128-bit blocks; only if this condition is met will the block cipher start processing and output a 128-bit ciphertext. When it comes to a memory footprint, we need a memory of at least a 128-bit size in order to work and process a 128-bit block. The register of most CPUs is small enough to fit. Otherwise, dedicated hardware circuits can be used for this to be implemented. A 68 bits, 128 bits and even blocks with a size of 512 bits are still short enough in most cases for efficient implementation.

However, as the blocks get larger, (i.e. kilobytes long), the cost and performance of the implementation can be noticeably impacted [19].

C. Hash functions:

Previously known as pseudo random functions (PRF), they work by mapping an arbitrarily-sized input for a fixed-size output in a process called compression. This is not the same as the compression used in .zip or .rar files, however. Instead, it is a mapping that is non-invertible. A hash function must align with two properties in order to be useful:

- The first property is that it must be one-way.
- The second property is that it must be collisionresistant.

Implying one-way output of a hash function can be considered as an important characteristic of it as well as being collision resistant, in which for another input to be found that generates the same output (known as collision) would be nontrivial. Two forms of collision resistance can be introduced:

1) Preimage collision resistance: this form of hash function operates on an output Y, which is given by finding another input M in such a way that the hash of M is the same as Y, nontrivially.

Fig. 5. Preimage collision resistance

2) Second preimage collision resistance: this the second form of hash function in which two messages are given (M1 and another, M2 that is chosen randomly) in which the match would be nontrivial [21].

Fig. 6. Second preimage collision resistance

D. Public key systems:

The invention of public key encryption can be considered a cryptography revolution. It is obvious that even during the 70s and 80s, general cryptography and encryption were solely limited to the military and intelligence fields. It was only through public key systems and techniques that cryptography spread into other areas.

Public key encryption gives us the ability to establish communication without depending on private channels, as the public key can be publicized without ever worrying about it. A summary of the public key and its features follows:

1) With the use of public key encryption, key distribution is allowed on public channels in which the system's initial deployment can be potentially simplified, easing the system's maintenance when parties join or leave.
2) Public key encryption limits the need to store many secret keys. Even in a case in which all parties want the ability to establish secure communication, each party can use a secure fashion to store their own private key. The public keys of other parties can be stored in a non-secure fashion or can be obtained when needed.
3) In the case of open environments, public key cryptography is more suitable, especially when parties that have never interacted previously want to communicate securely and interact. For example, a merchant may have the ability to reveal their public key online, and anyone who wants to purchase something can access the public key of the merchant as necessary when they want their credit card information encrypted [3].

V. DIGITAL SIGNATURES

Unlike cryptography, digital signatures did not exist before the invention of computers. As computer communications were introduced, the need arose for digital signatures to be discussed, especially in the business environments where multiple parties take place and each must commit to keeping their declarations and/or proposals. The topic of unforgeable signatures was first discussed centuries ago, except those were handwritten signatures. The

idea behind digital signatures was first introduced in a paper by Diffie and Hellman titled "New Directions in Cryptography" [22].

Therefore, in a situation where the sender and receiver do not completely trust each other, authentication alone cannot fill the gap between them. Something more is required, i.e. the digital signature, in a way similar to the handwritten signature [23].

A. Digital Signature Requirements:

The relationship that created the link between signature and encryption came into existence with the "digitalization" era that we are currently witnessing and living in. The requirements for an unforgeable signature schema would be:

- Each user should have the ability to generate their own signature on any selected document they chose.
- Each user should have the ability to efficiently verify whether or not a given string is the signature of another particular user.
- No one should have the ability to generate signatures on documents that the original owner did not sign [24].

B. Digital Signature Principles:

Being able to prove that a user or individual generated a message is essential both inside and outside the digital domain. In today's world, this is achieved through use of handwritten signatures. As for generating digital signatures, public-key cryptography is applied, in which the basic idea is that the individual who signs a document or message uses a private key (called private-key), while the individual receiving the message or document must use the matching public-key. The principle of the digital signature scheme is demonstrated in Figure 7.

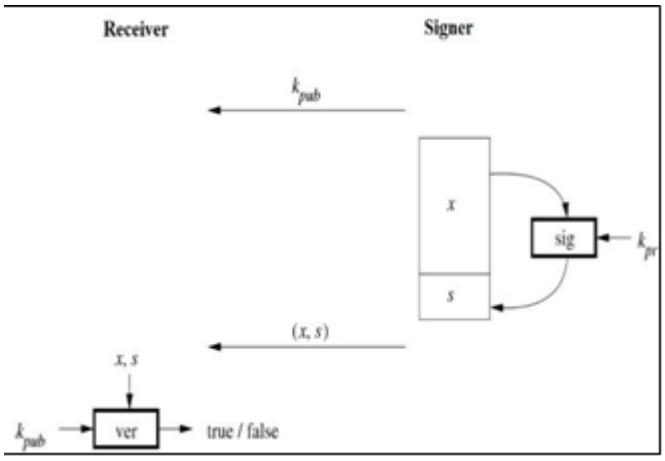

Fig. 7. Digital signature principle (signing and verifying)

This process starts with the signer, who signs the message x. The algorithm used in the signing process is a function that belongs to the signer's private key (kpr), assuming that the signer will keep the private key secret. Thus, a relation can be created between the message x and the signature algorithm; the message x is also given to the signature algorithm as an input. After the message has been signed, the signature s is attached to the message x, and they are sent to the receiver in the pair of (x, s). It must also be noted that a digital signature is useless without being appended to a certain message, similar to putting a handwritten signature on a check or document.

The digital signature itself has an integer value that is quite large, e.g. a string with 2048 bits. In order for the signature to be verified, a verification function is needed in which both the message x and the signature s are given as inputs to the function. The function will require a public key in order to link the signature to the sender who signed it, and the output of the verification function would be either "true" or "false". The output would be true in a case in which the message x was signed through the private key that is linked with the other key, i.e. the public verification key. Otherwise, the output of the verification function would be false [2].

C. Difference between Digital Signature and Message Authentication:

When parties are communicating over an insecure channel, they may wish to add authentication to the messages that they send to the recipient so that the recipient can tell if the message is original or if it has been modified. In message authentication, an authentication tag is generated for a given message being sent; the recipients must verify it after receiving the message and ensure that no external adversary has the ability to generate authentication tags that are not being used by the communicating parties.

Message authentication can be said to be similar to digital signature, in a way, but the difference between them is that in message authentication, it is required that only the second party verify the message. No third party can be involved to verify the message's validity and whether it was generated by the real sender or not. In digital signature, however, third parties have the ability to check the signature's validity. Therefore, digital signatures have created a solution for message authentication [24].

VI. CONCLUSION

Cryptography plays a vital 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.

VII. REFERENCES

[1]. N. Sharma , Prabhjot and H. Kaur, "A Review of Information Security using Cryptography Technique," International Journal of Advanced Research in Computer Science, vol. 8, no. Special Issue, pp. 323-326, 2017.

[2]. B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.

[3]. J. Katz and Y. Lindell, lntroduct:ion t:o Modern Cryptography, London: Taylor & Francis Group, LLC , 2008.

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

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

[6]. N. Jirwan, A. Singh and S. Vijay , "Review and Analysis of Cryptography Techniques," International Journal of Scientific & Engineering Research, vol. 3, no. 4, pp. 1-6, 2013 . [7] S. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal, "A Review paper on Network Security and Cryptography," Advances in Computational Sciences and Technology , vol. 10, no. 5, pp. 763770, 2017.

[7]. A. Gupta and N. K. Walia, "Cryptography Algorithms: A Review," NTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, vol. 2, no. 2, pp. 1667- 1672, 2014.

[8]. J. Callas, "The Future of Cryptography," Information Systems Security, vol. 16, no. 1, pp. 15- 22, 2007.

[9]. J. L. Massey, "Cryptography—A selective survey," Digital Communications, vol. 85, pp. 3-25, 1986.

[10]. B. Schneier, "The Non-Security of Secrecy," Communications of the ACM, vol. 47, no. 10, pp. 120-120, 2004.

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

[12]. K. Chachapara and S. Bhadlawala, "Secure sharing with cryptography in cloud," in 2013 Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, 2013. [14] H. Orman, "Recent Parables in Cryptography," IEEE Internet Computing, vol. 18, no. 1, pp. 82-86, 2014.

[13]. R. GENNARO, "IEEE Security & Privacy," IEEE Security & Privacy, vol. 4, no. 2, pp. 64 - 67, 2006.

[14]. B. Preneel, "Cryptography and Information Security in the PostSnowden Era," in IEEE/ACM 1st International Workshop on TEchnical and LEgal aspects of data pRivacy and SEcurity, Florence, 2015.

[15]. S. B. Sadkhan, "Cryptography : current status and future trends," in International Conference on Information and Communication Technologies: From Theory to Applications, Damascus, 2004. [18] F. Piper and S. Murphy, Cryptography: A Very Short Introduction, London: Oxford University Press, 2002. [19] J. P. Aumasson, SERIOUS CRYPTOGRAPHY A Practical Introduction to Modern Encryption, San Francisco: No Starch Press, Inc, 2018 .

[16]. J. F. Dooley, A Brief History of Cryptology and Cryptographic Algorithms, New York: Springer, 2013. [21] T. S. Denis and S. Johnson, Cryptography for Developers, Boston: Syngress Publishing Inc, 2007 .

[17]. W. D. A. M. E. HELLMAN, "New directions in cryptography," IEEE Transactions on Information Theory, Vols. IT-22, no. 6, pp. 644-654, 1976.

[18]. W. Stallings, Cryptography and Network Security Principles and Practices, New York: Prentice Hall, 2005. [24] O. Goldreich, Foundations of Cryptography Basic Tools, Cambridge: Cambridge University Press, 2004.