International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1385-1391 www.ijaem.net ISSN: 2395-5252

Cryptography: A Review

[1]Amosa Babalola, [2]Ekuewa Bamidele, [2]Olatunbosun Esther and [2]Oyetunji Olumayowa

[1]*Allbytes Consults, Gbagada Lagos, Nigeria*
[2]*Department of Computer Science, The Federal Polytechnic Ede, Nigeria*

Submitted: 15-10-2021 Revised: 28-10-2021 Accepted: 30-10-2021

ABSTRACT: Cryptography can be defined as the practice and study of hiding information. Disciplines such as mathematics, computer science, and are intersected with cryptography. Some applications of cryptography include ATM cards, computer passwords, and electronic commerce. Some of the key words in this term paper are: Plaintext i.e. information to be transmitted, Ciphertext i.e. plain text rendered unintelligible by the application of a mathematical algorithm, Cryptographic Algorithm i.e. a mathematical formula used to scramble the plain text to yield ciphertext and Key which is a mathematical value, formula, or process that determines how a plaintext message is encrypted or decrypted. The three types of cryptography are: Secret Key Cryptography (SKC), Public Key Cryptography (PKC), and Hash Functions. All these shall be explained in details.

KEYWORDS: Cryptography, Secret key, Hash Key, Public Key

I. INTRODUCTION

Cryptography is the area of constructing cryptographic systems [1]. Cryptography is closely associated with modern electronic communication. It should be noted that, cryptography is a rather old business, with early examples dating back to about 2000 B.C., when non-standard “secret” hieroglyphics were used in ancient Egypt. Since Egyptian days cryptography has been used in one form or the other in many, if not most, cultures that developed written language [2].

Cryptography can be defined as the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science, and engineering. Some applications of cryptography include ATM cards, computer passwords, and electronic commerce [3].

It can also be defined as the art and science of preparing coded or protected communications intended to be intelligible only to the person possessing a key. Cryptography refers both to the process or skill of communicating in or deciphering secret writings (codes, or ciphers) and to the use of codes to convert computerized data so that only a specific recipient will be able to read it using a key [3].

In its broadest sense, cryptography includes the use of concealed messages, ciphers, and codes. Concealed messages, such as those hidden in otherwise innocent text and those written in invisible ink, depend for their success on being unsuspected. Once they are discovered, they frequently are easy to decipher. Codes, in which predetermined words, numbers, or symbols represent words and phrases, are usually impossible to read without the key codebook. Cryptography also includes the use of computerized encryption to protect transmissions of data and messages.

Today most communication leaves some kind of recorded trail. For example, communications over telephone lines, including faxes and e-mail messages, produce a record of the telephone number called and the time it was called. Financial transactions, medical histories, choices of rental movies, and even food choices may be tracked by credit card receipts or insurance records. Every time a person uses the telephone or a credit card, the telephone company or financial institution keeps a record of the number called or the transaction amount, location, and date. In the future, as telephone networks become digital, even the actual conversations may be recorded and stored. All of this amounts to a great potential loss of privacy. Cryptography is one tool that will be able to ensure more privacy. The ability to encrypt data, communications, and other information gives individuals the power to restore personal privacy [4].

Cryptography is important for more than just privacy, however. Cryptography protects the world’s banking systems as well. Many banks and other financial institutions conduct their business over open networks, such as the Internet. Without the ability to protect bank transactions and communications, criminals could interfere with the transactions and steal money without a trace.

Generally, all cryptographic processes have four basic parts:

a. Plaintext - Unscrambled information to be transmitted. It could be a simple text document, a credit card number, a password, a bank account number, or sensitive information such as payroll data, personnel information, or a secret formula being transmitted between organizations.
b. Ciphertext - Represents plain text rendered unintelligible by the application of a mathematical algorithm. Ciphertext is the encrypted plain text that is transmitted to the receiver.
c. Cryptographic Algorithm - A mathematical formula used to scramble the plain text to yield ciphertext. Converting plain text to ciphertext using the cryptographic algorithm is called encryption, and converting ciphertext back to plain text using the same cryptographic algorithm is called decryption.
d. Key - A mathematical value, formula, or process that determines how a plaintext message is encrypted or decrypted. The key is the only way to decipher the scrambled information [4].

Cryptography is a fundamental technology used to provide security of computer networks; it also provides means of detection and remediation of security breach and vulnerabilities [5]. The focus of this paper is to review the concepts behind basic cryptographic methods, and to offer a way to compare the myriad cryptographic schemes in use today. The second is to provide some real examples of cryptography in use today.

II. THE PURPOSE OF CRYPTOGRAPHY

Cryptography as earlier defined as the science of writing in secret code is an ancient art; the first documented use of cryptography in writing dates back to 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet [6]

Within the context of any application-to-application communication, there are some specific security requirements, including:

a. Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak) .
b. Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver
c. Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
d. Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into ciphertext, which will in turn (usually) be decrypted into usable plaintext [3].

III. TYPES OF CRYPTOGRAPHY

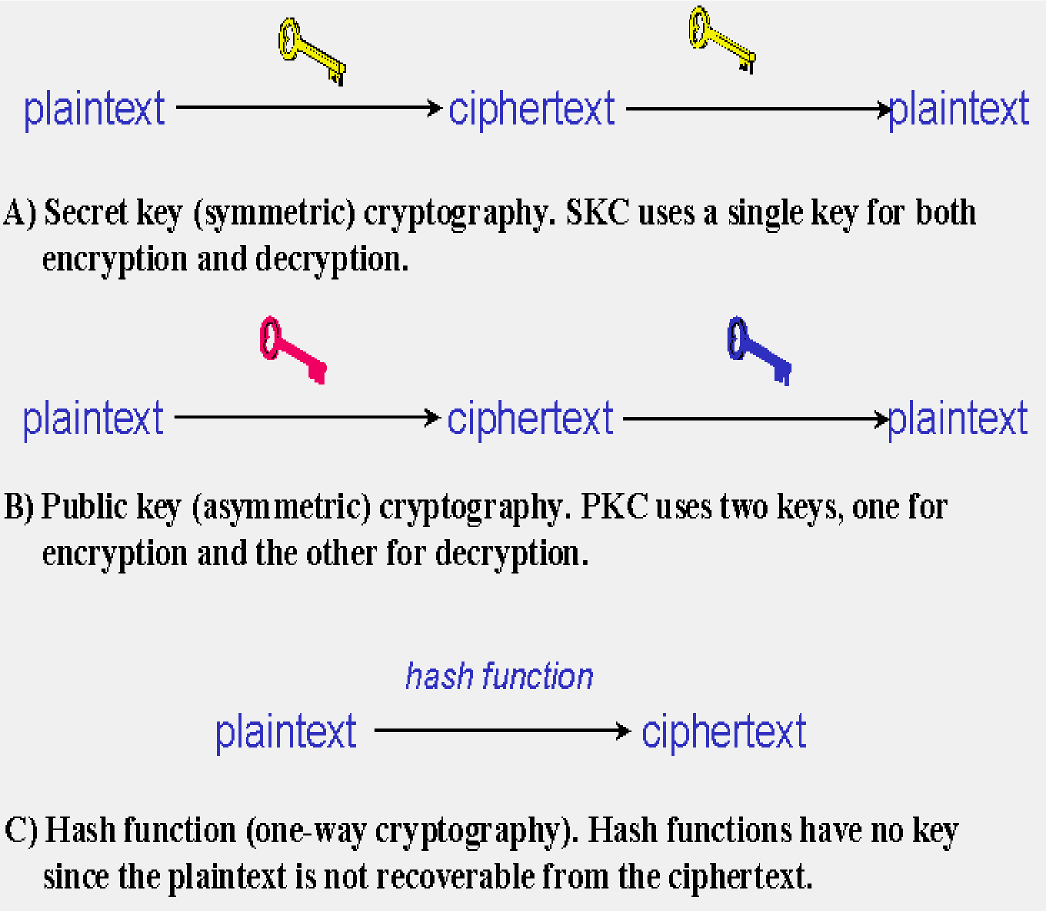
Cryptography is categorized based on the number of keys that are employed for encryption and decryption. The three types are:

a. Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
b. Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
c. Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

Secret Key Cryptography

With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 1, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or ruleset) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing [7]. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher. Stream ciphers come in several flavors but two are worth mentioning here. Self-synchronizing stream ciphers calculate each bit in the keystream as a function of the previous n bits in the keystream. It is termed "self-synchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the n-bit keystream it is.

One problem is error propagation; a garbled bit in transmission will result in n garbled bits at the receiving side. Synchronous stream ciphers generate the keystream in a fashion independent of the message stream but by using the same keystream generation function at sender and receiver. While stream ciphers do not propagate transmission errors, they are, by their nature, periodic so that the keystream will eventually repeat [7].

Block ciphers can operate in one of several modes; the following four are the most important:

a. Electronic Codebook (ECB) mode is the simplest, most obvious application: the secret key is used to encrypt the plaintext block to form a ciphertext block. Two identical plaintext blocks, then, will always generate the same ciphertext block. Although this is the most common mode of block ciphers, it is susceptible to a variety of brute-force attacks.
b. Cipher Block Chaining (CBC) mode adds a feedback mechanism to the encryption scheme. In CBC, the plaintext is exclusively-ORed (XORed) with the previous ciphertext block prior to encryption. In this mode, two identical blocks of plaintext never encrypt to the same ciphertext.
c. Cipher Feedback (CFB) mode is a block cipher implementation as a self-synchronizing stream cipher. CFB mode allows data to be encrypted

in units smaller than the block size, which might be useful in some applications such as encrypting interactive terminal input. If we were using 1-byte CFB mode, for example, each incoming character is placed into a shift register the same size as the block, encrypted, and the block transmitted. At the receiving side, the ciphertext is decrypted and the extra bits in the block (i.e., everything above and beyond the one byte) are discarded.

d. Output Feedback (OFB) mode is a block cipher implementation conceptually similar to a synchronous stream cipher. OFB prevents the same plaintext block from generating the same ciphertext block by using an internal feedback mechanism that is independent of both the plaintext and ciphertext bitstreams.

Secret key cryptography algorithms that are in use today include:

a. Data Encryption Standard (DES)
b. Advanced Encryption Standard (AES)
c. CAST-128/256
d. International Data Encryption Algorithm (IDEA):
e. Rivest Ciphers (aka Ron's Code)
f. Blowfish
g. Twofish
h. Camellia
i. MISTY1
j. Secure and Fast Encryption Routine (SAFER)
k. KASUMI
l. SEED
m. ARIA
n. Skipjack

Public-Key Cryptography

Public-key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976 [8]. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key. PKC depends upon the existence of so-called one-way functions, or mathematical functions that are easy to computer whereas their inverse function is relatively difficult to compute. Let me give you two simple examples:

a. Multiplication vs. factorization
b. Exponentiation vs. logarithms

Public-key cryptography algorithms that are in use today for key exchange or digital signatures include:

a. RSA: The first, and still most common, PKC implementation. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. The public key information includes n and a derivative of one of the factors of n; an attacker cannot determine the prime factors of n (and, therefore, the private key) from this information alone and that is what makes the RSA algorithm so secure. (Some descriptions of PKC erroneously state that RSA's safety is due to the difficulty in factoring large prime numbers. In fact, large prime numbers, like small prime numbers, only have two factors!) The ability for computers to factor large numbers, and therefore attack schemes such as RSA, is rapidly improving and systems today can find the prime factors of numbers with more than 200 digits. Nevertheless, if a large number is created from two prime factors that are roughly the same size, there is no known factorization algorithm that will solve the problem in a reasonable amount of time; a 2005 test to factor a 200-digit number took 1.5 years and over 50 years of compute time. Regardless, one presumed protection of RSA is that users can easily increase the key size to always stay ahead of the computer processing curve. As an aside, the patent for RSA expired in September 2000 which does not appear to have affected RSA's popularity one way or the other.
b. Diffie-Hellman: After the RSA algorithm was published, Diffie and Hellman came up with their own algorithm. D-H is used for secret-key key exchange only, and not for authentication or digital signatures.
c. Digital Signature Algorithm (DSA): The algorithm specified in NIST's Digital Signature Standard (DSS), provides digital signature capability for the authentication of messages.
d. El Gamal: Designed by Taher El Gamal, a PKC system similar to Diffie-Hellman and used for key exchange.

e. Elliptic Curve Cryptography (ECC): A PKC algorithm based upon elliptic curves. ECC can offer levels of security with small keys comparable to RSA and other PKC methods. It was designed for devices with limited compute power and/or memory, such as smartcards and PDAs.

f. Cramer-Shoup: A public-key cryptosystem proposed by R. Cramer and V. Shoup of IBM in 1998.

i. Key Exchange Algorithm (KEA): A variation on Diffie-Hellman; proposed as the key exchange method for Capstone.

j. LUC: A public-key cryptosystem designed by P.J. Smith and based on Lucas sequences. Can be used for encryption and signatures, using integer factoring.

IV. ADVANTAGES OF PUBLIC-KEY CRYPTOGRAPHY SECRET-KEY CRYPTOGRAPHY

a. The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone. In a secret-key system, by contrast, there is always a chance that an enemy could discover the secret key while it is being transmitted [9].

b. Another major advantage of public-key systems is that they can provide a method for digital signatures. Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well. A sender can then repudiate a previously signed message by claiming that the shared secret was somehow compromised by one of the parties sharing the secret [9].

c. Furthermore, digitally signed messages can be proved authentic to a third party, such as a judge, thus allowing such messages to be legally binding. Secret-key authentication systems such as Kerberos were designed to authenticate access to network resources, rather than to authenticate documents, a task which is better achieved via digital signatures [9].

V. DISADVANTAGES OF PUBLIC-KEY CRYPTOGRAPHY

A major disadvantage of using public-key cryptography for encryption is speed (i.e. transmission time for documents encrypted using public key cryptography are significantly slower then symmetric cryptography. In fact, transmission of very large documents is prohibitive.): there are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method.

VI. THE ENCRYPTION TECHNIQUES

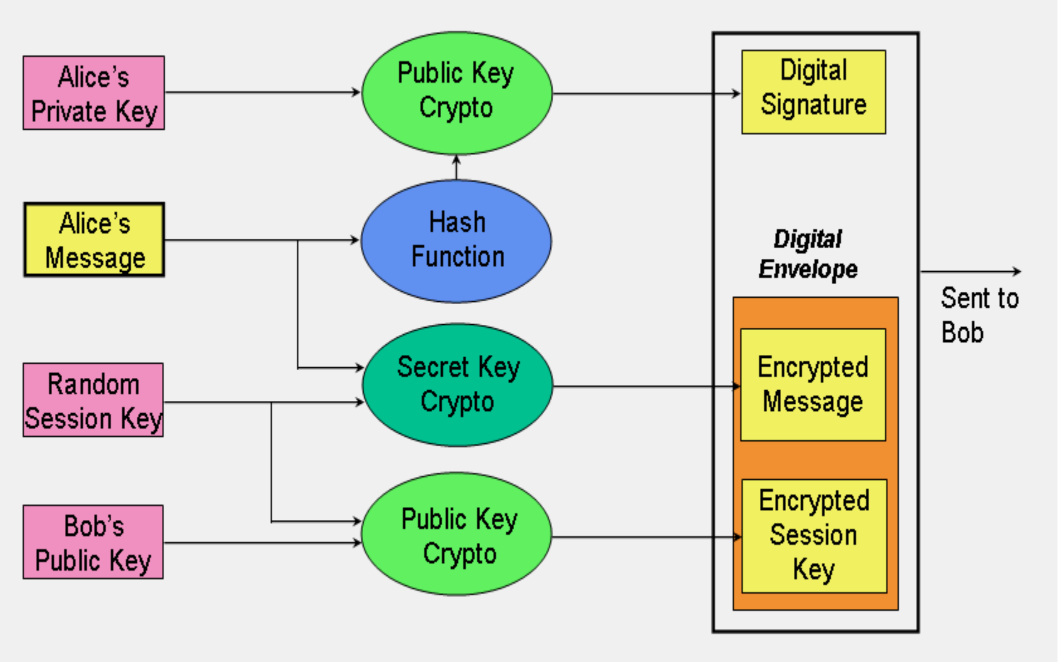
The three encryption techniques as presented in Figure 2 are;

a. Hash functions: are well-suited for ensuring data integrity because any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender. Since it is highly unlikely that two different messages will yield the same hash value, data integrity is ensured to a high degree of confidence [10].

b. Secret key cryptography: is ideally suited to encrypting messages, thus providing privacy and confidentiality. The sender can generate a session key on a per-message basis to encrypt the message; the receiver, of course, needs the same session key to decrypt the message.

c. Key exchange is a key application of public-key cryptography (no pun intended). Asymmetric schemes can also be used for non-repudiation and user authentication; if the receiver can obtain the session key encrypted with the sender's private key, then only this sender could have sent the message. Public-key cryptography could, theoretically, also be used to encrypt messages although this is rarely done because secret-key cryptography operates about 1000 times faster than public-key cryptography.

In figure 2 all the three techniques are put together and it shows how a hybrid cryptographic scheme combines all of these functions to form a secure transmission comprising digital signature and digital envelope. In the example, the sender of the message is Alice and the receiver is Bob. A digital envelope comprises an encrypted message and an encrypted session key. Alice uses secret key cryptography to encrypt her message using the session key, which she generates at random with each session.



Alice then encrypts the session key using Bob's public key. The encrypted message and encrypted session key together form the digital envelope. Upon receipt, Bob recovers the session secret key using his private key and then decrypts the encrypted message.

The digital signature is formed in two steps. First, Alice computes the hash value of her message; next, she encrypts the hash value with her private key. Upon receipt of the digital signature, Bob recovers the hash value calculated by Alice by decrypting the digital signature with Alice's public key. Bob can then apply the hash function to Alice's original message, which he has already decrypted (see previous paragraph). If the resultant hash value is not the same as the value supplied by Alice, then Bob knows that the message has been altered; if the hash values are the same, Bob should believe that the message he received is identical to the one that Alice sent.

This scheme proves that Alice sent the message; if the hash value recovered by Bob using Alice's public key proves that the message has not been altered, then only Alice could have created the digital signature.

Bob also has proof that he is the intended receiver; if he can correctly decrypt the message, then he must have correctly decrypted the session key meaning that his is the correct private key [11].

VII. USES OF CRYPTOGRAPHY

Cryptography can;

a. Provide secrecy.
b. Authenticate that a message has not changed in transit.
c. Implicitly authenticate the sender.
d. Hides words
e. Protect ordinary commerce and ordinary people.
f. Hide secrets, either from others, or during communication.

VIII. SHORT-COMINGS OF CRYPTOGRAPHY

Cryptography can only hide information after it is encrypted as long as it is encrypted, but it cannot hide:

a. Physical contraband,
b. Cash,
c. Physical meetings and training,
d. Movement to and from a central location,
e. An extravagant lifestyle with no visible means of support, or
f. Actions.

And cryptography simply cannot protect against:

a. Informants,
b. Undercover spying,
c. Bugs,
d. Photographic evidence, or
f. Testimony.

IX. APPLICATIONS OF CRYPTOGRAPHY

Typical cryptographic applications and analyzed scenarios based on them that are used in practice are discussed in [12]. While most widely application of cryptography is on electronic commerce which deals with payment systems and transactions over open networks which are:

a. Electronic Money
b. Internet Keyed Payment Protocol (Ikp)
c. Set
d. Mondex
e. Micropayments

X. CONCLUSION

We have reviewed the concept of cryptography in this study. Advantages and disadvantages were also stated. Cryptography is complex, this is because humans recognize numbers as digits from 0 to 9, but the computer can only recognize 0 and 1, and because of this binary system uses bits instead of digits. This will then provide the user with a good estimation of what it stands for. This is why so much education is needed to be able to work as a cryptographer.

REFERENCES

[1] Mohamed Barakat; Christian Eder; and Timo Hanke, 2018, "An Introduction to Cryptography" www.mathematik.uni-kl.de/~ederc/download/Cryptography.pdf Accessed on 15th June 2021

[2] Christof Paar; and Jan Pelzl, 2010, "Understanding Cryptography; A Textbook for Students and Practitioners". Springer-Verlag Berlin Heidelberg.

[3]. Cheswick, W.R; and Bellovin, S.M., 2003, "Firewalls and Internet security". Addison-Wesley, USA

[4]. Davies, D.W; and Price, W.L., 1989, "Security for Computer Networks". John Willey & Sons, Inc., Second Edition

[5] Savu, L., 2013, "Cryptography Role in Information Security". University of Bucharest, Romania

[6]. Davis, D; and Swick, R., 1990, "Network Security via Private-Key Certificates. ACM SIGOPS Operating Systems Review Volume 24, Issue 4, pp 64–67 https://doi.org/10.1145/94574.94579

[7]. Waleffe D. de; and Quisquater, J.J.,1993,"Computer Security and Industrial Cryptography". Springer, VIII.

[8]. Diffie, W; and Hellman, M.E., 1976, "New Directions in Cryptography Theory". IEEE Transaction on Information Theory, VOL IT-22, No 6, pp 644 - 654

[9]. Fiat, A; and Shamir, A., 1987, "How to prove yourself, Advances in Cryptology" - Proc. Of Crypto 86, pp. 641-654

[10]. Krawczyk, H; Bellare,M; and Canetti, R., 1997, "HMAC: Keyed-hashing for Message Authentication".https://www.rfceditor.org/rfc/p dfrfc/rfc2104.txt.pdf' Accessed on 21st May,2021

[11]. Menezes, A.J; Van Oorschot,P.C; and Vanstone, S.A., 1997, "Handbook of Applied Cryptography". https://citeseerx.ist.psu.edu/viewdoc/download?d oi=10.1.1.99.2838&rep=rep1&type=pdf Accessed on 24th May, 2021

[12] Vangelis Karatsiolis; Lucie Langer; Axel Schmidt; Erik Tews; and Alexander Wiesmaier, 2020, "CryptographicApplicationScenarios".https://www.researchgate.net/publication/228559803_Cryptographic_Application_Scenarios? Accessed on 5th May 2020