Cryptography

Waliyullahi Zakariyah
University of Ilorin
2 PUBLICATIONS **0** CITATIONS

Cryptography

Waliyullahi O. Zakariyah

Department of Telecommunication Science, University of Ilorin

18-52hp066@students.unilorin.edu.ng

***Abstract*—The wide use of cryptography is a necessary consequence of the information revolution. With the existence of electronic transmissions on computer networks, individuals need a way to ensure that their conversations and transactions remain confidential i.e. untouched by any intruder, and that is the essence of Cryptography. This paper will be looking at what cryptography implies, its nexus with the word encryption, how it has evolved with time, some critical axioms that govern encryption will also be looked at, keeping in mind its grand essence and practical applications in our real-life (stressing as much on WhatsApp messaging app as a case study and some other impacts).**

***Keywords*— Cryptography, Encryption, Decryption, Algorithm, Cipher, Applications, Cryptosystem, Authentication, Electronic, Cryptogram**

I. INTRODUCTION

Is increased security reassuring to paranoid individuals? Or, instead, does security provide some fundamental safeguards that we are naive enough to believe we don't need or want? A significant issue to address at a time when the Internet is essential for communication between tens of millions of people and is increasingly being utilized for business is the issue of security. Securing transactions and payments, as well as private conversations and password protection, are just a few of the many aspects and applications of security. To maintain secure communications, cryptography is an essential component, and it is the subject of this paper.

Cryptography, according to its definition, is the science of protecting information by converting it into a format that can only be processed and read by the individuals who are intended to receive it. The first known use of the symbol goes back to 1900 BC when it was found in hieroglyphics in an Egyptian burial chamber. The phrase is derived from the Greek terms Kryptos and Graphein, which translate as "hidden" and "to write," respectively [1], [2].

Some of its ultimate goals are to ensure secured computer networks, internet systems, and digital data through the use of code. It is a concept whose ultimate intention is to keep necessary records invulnerable and private in the tournament of an information breach. While the phrase is frequently linked with the cutting-edge digital era, the idea has been used extensively in military and government operations for millennia. For instance, World War II Navajo code talkers who communicated in their very own tongue used cryptography to transmit necessary information [3].

It is both a science and an academic discipline dedicated to the learn about secret writing. A cipher is a secure technique of writing that converts plaintext to ciphertext (sometimes regarded as a cryptogram). Encryption is a way of converting simple textual content to ciphertext whilst decryption is the reverse process of converting ciphertext lower back to simple text.

Ciphers are categorized into two vast categories: transpositions and substitutions. Transposition ciphers reorientate the data's bits or characters. With the resource of a "rail-fence" [3], [4]

Table 1 suggests the four-floor concepts of cryptography which are:

Confidentiality	Defines a set of rules that limits the access or adds a restriction to certain information
Data Integrity	Ensures data consistency and correctness throughout its life cycle.
Authentication	Confirms the truth of an attribute of a datum that is claimed to be true by some entity, Alice should be Alice, Bob should be Bob
Non-Repudiation	Ensures the inability of a writer of a statement to deny a piece of records

II. DEFINITION AND ORIGIN OF ENCRYPTION TECHNIQUE

Encryption is stated to be a technique of changing messages or information in a form that cannot be studied by using an unauthorized character barring decrypting or interpreting it. Encryption is derived from a root phrase crypt which comes from the Greek word kryptos, which means hidden or secret[5]. The study and exercise of encryption and decryption are called the science of cryptography. Scientists who studied exclusive methods to shield and ensure the integrity, confidentiality, and authenticity of information are known as cryptologists.

Cryptologists also engage themselves in cryptanalysis to locate ways to ruin encryption methods. For many years earlier than the digital conversation and computers age, individuals, militaries, and different businesses write records in a coded way. As digital varieties of conversation and statistics storage and processing have developed, the opportunities to modify, intercept, use, disclose, and read exclusive data have grown outrageously, and the want for effective encryption methods has increased. Government agencies, banks, and many companies now routinely ship a superb deal of private data from one computer to another. Such information are been transmitted thru smartphone traces or other non-private channels, such as the Internet. Constant improvement of secure laptop structures and networks will make sure that personal facts are securely transferred throughout computer networks.

III. HOW ENCRYPTION WORKS

Encryption utilizes a systematic or step-by-step procedure referred to as an algorithm to convert statistics or the textual content of an original message, whichis regarded as plaintext, into ciphertext, which is its encrypted structure [6]. Cryptographic algorithms usually require a string of characters referred to as a key to encrypt or decrypt data. Those who have the key and the algorithm can encrypt the plaintext into ciphertext and then decrypt the ciphertext returned into plaintext [7], [8].

Cryptologists interact themselves in an unending competition to create stronger cryptographic techniques and to break them. Many latest cryptography techniques are nearly unbreakable even with the most powerful computers. These structures produce ciphertext that seems to be random characters. These systems withstand most existing methods for interpreting again into plaintext.

The exceptional sorts of new cryptosystems use exceptionally complex mathematical language and face up to breaking even although cryptologists may recognize the methods used in creating them. Pretty Good Privacy (PGP) helps customers of e-mail hold their communications private. Using this two-key method, which is also known as the public key system, the computer transmitting an encrypted message employs a selected personal key that is never shared, and as a result, only the computer delivering the encrypted message is aware of the personal key. All the authorized computers to acquire and decrypt the message are given the matching public key. This method also unravels whomsoever behind the message transmission. If a sending laptop first encrypts the message with the supposed receiver's public key and again with the sender's secret, non-public key, then the receiving laptop can also decrypt the message, first the use of its secret key and then the sender's public key. Using this public-key cryptographic method, the sender and receiver are capable to authenticate one another as nicely as shield the secrecy of the message [9].

IV. COMMON ENCRYPTING SYSTEM

The three of the common cryptography systems used are as follows:

1. Data Encryption Standard (DES)
2. Pretty Good Privacy (PGP)
3. Rivest, Shamir, Adleman (RSA) system.

DES makes use of a single key for each encrypting and decrypting. It was once first developed by International Business Machines Corporation (IBM) and it was once permitted via the United States National Institute of Standards and Technology in 1976 [10].

In private-key cryptography, a secret key may also be held by using one person or exchanged between the sender and the receiver of a message. For example, if Alice encrypts information for storage on a hard drive, he remembers the key and generally does now not supply it to every other person. But if Alice favors sending invulnerable messages to a business companion named Bob using symmetric cryptography, Alice needs to make sure Bob knows the key that will decrypt the messages. The secret (or private) key in a public-key cryptographic device is by no means transmitted nor shared. For instance, when using the technique for client-side authentication, the server transmits some facts to your purchaser program. The purchaser uses your non-public key to encrypt that data. Using your public key, the server then strives to decrypt the again data, and, if successful, be aware that it has established a conversation with you [11], [12].

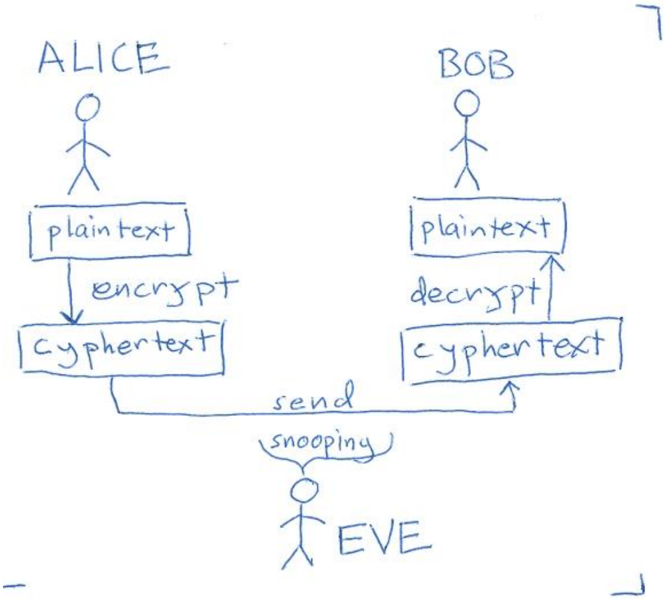


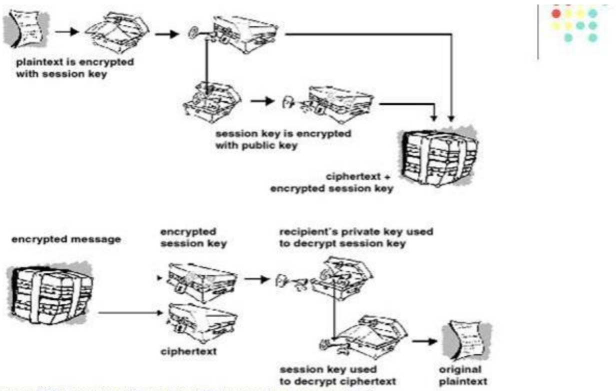
Fig.1 is a pictorial representation of how plain text is encrypted and decrypted [7].

If private-key cryptography is utilized in transmitting secret messages between two events Alice and Bob, both the sender and receiver need to have a copy of the secret key. However, the key may additionally be compromised all through transit. If you comprehend the celebration you are replacing messages with, you can provide them the key in advance. However, if you want to send an encrypted message to someone, you have never met, you will need to determine a way to change keys in an invulnerable way. One technique is to send it by using every other tightly closed channel.

The Rivest, Shamir, Adleman (RSA) algorithm is a famous encryption method that makes use of two keys. It was designed for familiar use in 1977 and was named after the three pc scientists Ronald L. Rivest, Adi Shamir, and Leonard Adleman who introduced it to existence. The RSA Data Security Company has been rather profitable in licensing its algorithm for others to use. Unlike symmetric cryptography, the keys are mathematically related, yet it is computationally infeasible to differentiate one from the other. Alice with the public key can encrypt a message however cannot decrypt it. Only the character with the personal key can decrypt the message. One of the most frequent makes use of public-key science is to furnish a tightly closed verbal exchange channel between computer programs, though private-key techniques can be used for this too. Public key shape additionally presents the foundation or secure emails because public-key cryptography is used to distribute symmetric keys, which are then used to encrypt and decrypt real messages. For example, in using a public-key gadget for personal authentication or impenetrable messaging, you maintain one key secret. The 2nd (public) key can then be disbursed to anyone. An ordinary example of public key infrastructure is the SSL(Secure Socket Layer) protocol.

SSL is often used to shield statistics sent between Web browsers and net servers; this is regularly used in e-commerce systems.

PGP is an encryption system that additionally uses two keys. It is based on the RSA algorithm. PGP used to be invented via a software program developer Philip Zimmerman and is one of the most common cryptosystems used on the Internet because it is effective, free, and simple to use. PGP is such a wonderful encryption tool that the United States government sued Zimmerman for releasing it to the public, alleging that making PGP available to enemies of the United States would endanger country-wide protection [9].


plaintext is encrypted with session key
session key is encrypted with public key
ciphertext + encrypted session key
encrypted message
encrypted session key
recipient's private key used to decrypt session key
ciphertext
session key used to decrypt ciphertext
original plaintext

Source: PGP International Organization, http://www.pgpi.org/doc/pgpintro/#p9

Fig. 2 indicates how the recipient's replica of PGP uses his or her private key, which PGP then makes use of to decrypt the conventionally encrypted ciphertext [7].

The lawsuit was dropped, however, it is nevertheless illegal in some international locations to use PGP to speak with humans in different countries. In the two-key system, moreover diagnosed as the public key system, one key encrypts the data, and another, mathematically associated key decrypts it. Alice uses a laptop to send an encrypted message the use of a chosen private key that is never shared and so is recognized solely to Alice. All computers licensed to obtain and decrypt the message are given the matching public key. This technique additionally discloses who dispatched the message. If a sending pc first encrypts the message with the meant receiver's public key and again with the sender's secret, personal key, then the receiving computer might also decrypt the message, first the usage of its secret key and then the sender's public key [10].

Using this public-key cryptographic method, the sender and receiver can authenticate one another as nicely as defend the secrecy of the message. Single key methods, in contrast, require extremely good secrecy in conveying a key from the sender to the recipient.

V. OTHER CRYPTOSYSTEMS

Secure Sockets Layer (SSL): This protocol was once developed by Netscape Communications Corporation for transmitting non-public files by the Internet, and Secure Hypertext Transfer Protocol (S-HTTP), designed to shipman or woman messages, also use encryption system. The size or complexity of the key (along with the difficulty of the algorithm) generally indicates the effectiveness of the encryption. DES, for example, makes use of fifty-six bits in its key to trade 8-character message segments into 64-bit segments of ciphertext.

In 1997 the National Institute of Standards and Technology started out coordinating the improvement of a new encryption laptop called Advanced Encryption Standard (AES). AES is to exchange DES, as it will use an improved algorithm, based totally on a 128-bit encryption general alternatively of the 64-bit general that DES now uses.

Another superior encryption gadget employs the International Data Encryption Algorithm, or IDEA, based on 128-bit segments. The Swiss Federal Institute of Technology developed the IDEA popular in the 1990s. Banks in the United States and numerous nations in Europe use the IDEA properly known.

VI. KERBEROS

Kerberos is another impervious encryption method. It used to be developed at the Massachusetts Institute of Technology (MIT) in the 80s. Kerberos is one hand in support of business software. Kerberos employs a client/server structure and gives user-to-server authentication as an alternative to host-to-host authentication. In this model, safety and authentication are based totally on secret key technology where each host in the community has its secret key. It would definitely be unmanageable if each host were able to comprehend the keys of all other hosts so a secure, relied-on host someplace on the network, known as a Key. Distribution Center (KDC), knows the keys for all of the hosts (or at least some of the hosts within elements of the network, called a realm). In this way, when a new node is brought online, only the KDC and the new node want to be configured with the node's key; keys can be distributed physically or by some other impervious means [13].

VII. TYPES OF CRYPTOGRAPHY

There are many sorts of cryptography, together with codes, Steganography (hidden or secret writing), and ciphers. Codes rely on codebooks. Steganography relies on special ways to hide or conceal writing. Ciphers are each computer-generated ciphers and those created via encryption methods. The unique kinds of ciphers rely on alphabetical, numerical, computer-based, or other scrambling methods.

.

Codes and Codebooks: A well-constructed code can characterize phrases and entire sentences with symbols, such as five-letter groups, and is often used greater for an economic system than for secrecy. A right-built code can give a high diploma of security, but the issue of printing and distributing codebooks beneath prerequisites of absolute secrecy limits their use to places in which the books can be correctly guarded[11].

Steganography is a method of hiding the existence of a message, the use of equipment such as invisible ink, microscopic writing, or hiding code phrases within sentences of a message (such as making every fifth word in a text section of the message).

Cryptographers may also follow Steganography to digital communications. This software can be referred to as transmission security. Steganography in any other case recognized as secret writing seems to have originated almost as early as writing itself did. Even in ancient Egypt, the place writing itself was a thriller to the common person, two awesome types of writing had been used. The priests used hieratic or sacred writing for secret communication, and other literate people used demotic writing. The historic Greeks and Romans as properly as different civilizations that flourished at around the same time used types of Steganography.

VIII. ENCRYPTION IN WHATSAPP

WhatsApp is one of the most famous mobile messaging functions handy these days owned by Facebook Inc. It is well-matched with a range of platforms, together with Android, Windows Phone, and iPhone. Additionally, WhatsApp enables users to make free calls to different users. It utilizes end-to-end encryption technology to encrypt chats and calls.

End-to-End (E2EE) encryption encrypts solely the data. No encryption is used for the headers, trailers, or routing information. WhatsApp’s end-to-end encryption used to be developed in collaboration with 'Open Whisper Systems'. It ensures that a message is acquired solely by way of only the supposed recipient, averting any structure of data breach or listening [4].

The end-to-end is performed through the use of uneven cryptography or public-key systems.

Working principle: Once WhatsApp is set up on a user's smartphone, the WhatsApp server registers the public keys of WhatsApp clients. It's integral to preserve in mind that the personal key is now not stored on WhatsApp's servers. Having registered the client, an encrypted session is installed between two consumers willing to participate in a conversation. Only when the gadget is changed or the WhatsApp software program is reinstalled does a session need to be re-created. If customer 1 needs to send a message to client 2, its public keys are retrieved from the WhatsApp server and used to encrypt and ship the message to patron 2. The message is then decrypted via Client2 the use of his private key.

Once a session is established, customers alternate messages that are blanketed by a Message Key and encrypted the usage of AES256 in CBC mode, Curve25519 and authenticated using HMAC-SHA256 (WhatsApp Encryption Overview 2016) [4], [14] [15], [16], [17].

IX. OTHER APPLICATIONS OF CRYPTOGRAPHY

Cryptography is one of those oddities that benefit everybody daily, whether in business or as customers, yet most of us are not conscious of it. Some of its essence other than the previously stressed are:

1. Authentication/Digital Signatures:

Authentication is any manner that establishes and verifies the authenticity of data. At times, it may additionally be imperative to affirm the origin of a document, the sender's identity, the time and date on which a record was once despatched and/or signed, the identification of a laptop or user, and so forth. A digital signature is a cryptographic technique that may be used to validate several of these types of information. The digital signature of a document is a piece of information that is generated from each report and the signer's private key to authenticate the document. The majority of the time, it is produced by combining the hash and private signing characteristics of two different cryptographic protocols (algorithms that create encrypted characters containing unique facts about a report and its private keys) [13]. Fig.3 below is a typical example.

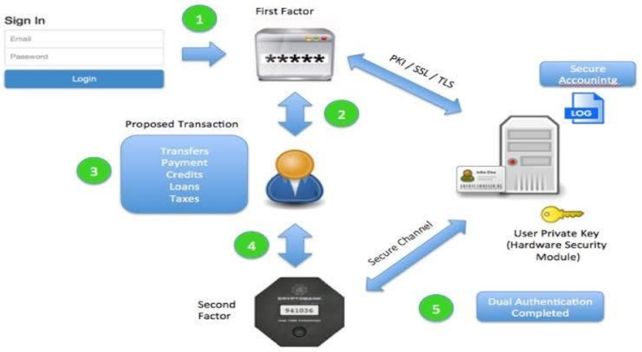


Fig.3 Copied from [13].

2. Electronic money:

Electronic cash (alternatively referred to as digital money or digital cash) is a term that is still evolving. It encompasses digital transactions involving the net switch of money from one celebration to another, which may also be debit or credit and may be nameless or identified.

There are implementations in both hardware and software. When it comes to electronic money (sometimes referred to as electronic cash or digital currency), the word is still in the early stages of development. It encompasses digital transactions involving the net switch of funds from one birthday celebration to another, which may also be debit or credit score and might also be nameless or identified. There are implementations in each hardware and software. Anonymous purposes conceal the customer's identification through the use of blind signature schemes. Identified spending schemes expose the customer's identity and are based totally on more widespread signature schemes. Anonymous schemes are characteristic in a similar way to cash, whereas recognized schemes are characteristic similar to a debit or savings card. There are also some hybrid techniques in which payments can be anonymous to the service provider but not to the bank; or where payments can be anonymous to anybody however traceable (a sequence of purchases can be associated however now not immediately linked to the spender's identity) [13].

Encryption is used in digital money schemes to guard typical transaction data, such as account numbers and transaction amounts; digital signatures can be used in the location of handwritten signatures or savings card authorizations, and public-key encryption can provide confidentiality. There are quite a few systems that cover this range of applications, from transactions that resemble standard paper transactions with values of various dollars and up to several micropayment schemes that batch extraordinarily low-cost transactions into amounts adequate to cover the cost of encryption and clearing the bank. Fig.3.1 is a normal illustration [13].

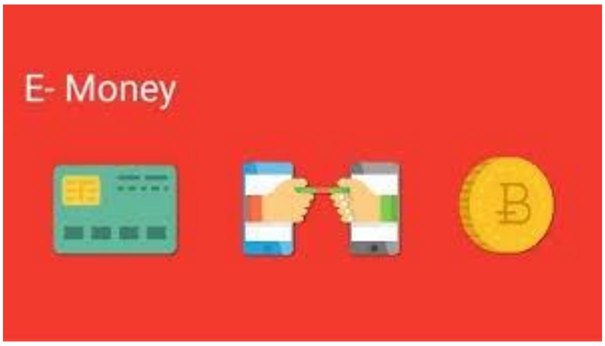
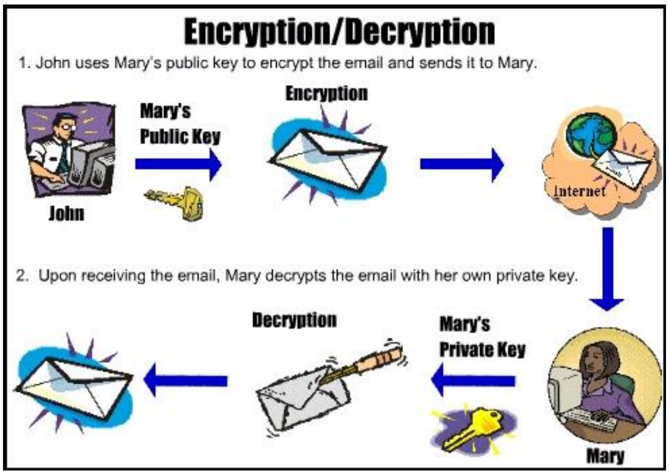


Fig.3.1 Copied from [13].

3. Secure Email communications

Email encryption protects the content of emails from absolutely everyone looking to reap a participant's information from backyard the electronic mail conversation. When an email is encrypted, it becomes unreadable to humans. Your emails can only be unlocked and decrypted by the usage of your email key [13] [18]. Descriptively, Fig.3.2 expounds what is been implied as far as secure email communications are concerned.



Encryption/Decryption

1. John uses Mary's public key to encrypt the email and sends it to Mary.

2. Upon receiving the email, Mary decrypts the email with her own private key.

Fig.3.2 Copied from [13].

4. HTTP Secure—Securing websites:

HTTP stands for 'Hypertext transfer protocol' and is a protocol adapted for communication over the Internet. It is the underlying structure of the World Wide Web. HTTP is a stateless protocol, as the server discards the customer at the conclusion of every transaction.

HTTPS, on the other hand, is HTTP walking over SSL (Secure Sockets Layer). The majority of our each day activities, such as buying or paying bills, are conducted online. As a result, vital and quintessential statistics such as credit score cards and bank account numbers are transmitted online. These imperative facts can't fall into the wrong palms and be used maliciously. This ensures the absolute necessity of impervious communication between the server and the client. SSL utilizes cryptography to ensure this impervious channel of communication. The majority of customers are guaranteed the SSL warranty by using the presence of the "padlock" in the tackle bar's left section, along with the "HTTPS" as an alternative to "HTTP." [13] [18]

X. CONCLUSIONS

Encryption methods have come to continue to be in the digital world. Since every information, that is transmitted via a pc network is no longer protected. The cryptography method is developed to defend records from been vulnerable to assaults and to permit secure and invulnerable communication.

In the end, it is evident that this paper has looked at the semantics, evolution, and syntax of cryptography to some quite extent. Establishments were made on some critical axioms, various flavors, and the importance of cryptography (taking WhatsApp as the main case study).

REFERENCES

[1] Ajay Ohri *What is cryptography*, date published: Feb 2, 2021, [online]: https://www.google.com/amp/s/www.jigsawacademy.com/blogs/cyber-security/what-is-cryptography date accessed: 20/08/21

[2] Kathleen Richards *Definition of cryptography*, date published: April 6, 2021, [online]: https://www.google.com/amp/s/searchsecurity.techtarget.com/definition/cryptography%3famp=1 date accessed: 20/8/21

[3] SoPA *What is cryptography*, year published: 2021, [online]: https://sopa.tulane.edu/blog/what-is-cryptography date accessed: 20/82021

[4] Jayanthi Manikandan *Basics of cryptography* date published: April 7, 2018, [online]: https://resources.infosecinstitute.com/topic/basics-of-cryptography-the-practical date accessed: 22/08/2021

[5] Gary C. Kessler, 1998, an overview of cryptography, [online]: http://www.garykessler.net/library/crypto date accessed: 29/08/21

[6] Jennifer Tauser, 2005, *Encryption is the most important tool for*

Internet security and privacy

[7] PGP Corporation "An Introduction to Cryptography, version 8.0. Released Oct. 2002"

[8] R. E. Frazier, 2004, *data encryption techniques*, [online]: http://catalog.com/sft/encrypt date accessed: 2/09/21

[9] http://www.rsasecurity.com/rsalabs/node.asp?id=222 date accessed: 22/08/21

[10] http://searchsecurity.techtarget.com/sDefinition/0sid14_gci 21195300 dates accessed: 27/08/21

[11]http://www.linktionary.com/p/priv_key_cryp.htmhttp://web.mit.edu/rhel-doc/3/rhel-rg-en-3/s1-kerberos-works.hZ date accessed: 1/09/21

[12]http://www.washington.edu/computing/windows/issue22/encryption date accessed: 5/09/21

[13] Prashanth_*Reddy* *Real Life Applications of Cryptography* date published: Nov 8, 2019 [online]: https://medium.com/@prashanthreddyt1234/real-life-applications-of-cryptography-162ddf2e917d date accessed: 29/08/21

[14] Vamsi Krapa, S.Prayla Shyry, M.Rahul Sai Krishna, July 2019, *WhatsApp Encryption – A Research*

[15] Technical white paper *WhatsApp Encryption Overview*
Version 3 Updated October 22, 2020 Version 2 Updated December 19, 2017
Version 1 Originally published April 5, 2016

[16] Anushka Xavier k Computer Science Engineering, Karunya Institute of Technology and Science *Cryptography Used in WhatsApp*

[17] Calvin Li, Daniel Sanchez, Sean Hua *WhatsApp Security Paper Analysis*

[18] Ronan *Everyday Applications of Cryptography* Date published: June 9, 2020, [online]: https://ronanthewriter.com/applications-of-cryptography-in-daily-life date accessed: 29/08/21