Ultra Encryption

Cyber Security

**COMSATS University Islamabad**

Sahiwal Campus



**Group Members**

**Usama Sarwar**

FA17-BCS-090

**Alina Raza**

FA17-BCS-072

**Maryam Zia**

FA17-BCS-055

**Rimsha Bilal**

FA17-BCS-062

**Supervisor**

**Mr Usman Nasir**

Introduction to Computing

December 11, 2019

Table of Contents

[**Abstract**](#_4pr0envxgft3) **4**

[**Introduction**](#_dfsxnwsfqs76) **1**

[**Problem Statement**](#_lmfjjjxjbi8a) **3**

[**Solution**](#_34u56smpjkv3) **4**

[**Objectives**](#_fzwr2vyirhy9) **5**

[**Literature Review**](#_otkdah9zvnt) **6**

[**Methodology**](#_dxi0uli9bspg) **8**

[**Applications**](#_eftgxv1ozjnt) **13**

[**Challenges**](#_7xpn8unoianr) **14**

[**Limitation**](#_vbziq1n4cbi1) **15**

[**Conclusion**](#_a5bzni53moj0) **16**

[**Gantt Chart**](#_qqkkvovoka50) **17**

[**References**](#_75n9v0jmrjp7) **18**

List of Figures

Figure 1. Third-Party interference (Insecure Network) 5

Figure 2. Secure Network using Cipher Technique 6

Figure 3. Cryptography Mechanism 10

Figure 4. Encryption Algorithms 10

Figure 5. Symmetric Key Cryptography 11

Figure 6. Transposition Ciphers 11

Figure 7. Substitution Cipher 11

Figure 8. Block Cipher 12

Figure 9. Public Key and Private Key Concept 12

Figure 10. RSA Algorithm 13

Figure 11. Asymmetric Key Encryption 13

Figure 12. Gantt Chart Ultra Encryption 15

# Abstract

Personal online safety is becoming a very important issue in the field of engineering. This is due to the growing demand of online communication. The best technology to establish the security of user data is end-to-end encryption.Thus email services became available to the public.. Online shopping, banking and other online financial business have "led" to an even greater demand for internet security. An example of a technology that offers a high profile of data protection is end-to-end encryption. The hardware built into the phones and computers allows the locks and random keys that make up end-to-end encryption to work only on the devices involved in the discussion. This means that the communicated data is completely secured. End-to-end encryption is very useful for the feasible of online data protection as it protects users from attacks and is difficult to decrypt. WhatsApp Messenger is the best example of this important technology in large-scale use. End-to-end message encryption makes it almost impossible to cut off a WhatsApp Messenger message. In addition, the encryption history related to the public use of this software is important to understand how end-to-end encryption has developed gradually to become popular in applications like WhatsApp Messenger today. WhatsApp Messenger software is one of the most popular public messaging programs, so it reflects the productiveness of end-to-end encryption technology. WhatsApp Messenger is the world’s top-rated chatting App. Today, people are concerned with their privacy a lot, so their privacy can’t be compromised. WhatsApp Messenger uses end-to-end encryption and claims to ensure users’ privacy. Their methodology uses two keys; one is a public key, that is a part of the encryption protocol and the other one is a private key that is never shared. These two keys when combine, you get access to the WhatsApp Messenger Account data. There is a loophole detected in WhatsApp Messenger end-to-end encryption. If the private key of a WhatsApp Messenger account is retrieved in some ways; all chats can be easily decrypted. In the current algorithm, WhatsApp Messenger uses a private key at the user level. If we generate this key at each chat/message level then the security can be maximized up to some extent. In this way, if a single key is retrieved by some third party; they can only decrypt a single message. In this way, we can maximize the security level of WhatsApp Messenger Messenger. In this method, if someone attacks on the network, the network will be smart enough to trace the error. Although this technology enables an extremely high level of security for users, it poses certain problems, such as the encryption limits imposed on government surveillance.

# 

# Introduction

//Encryption links to the coding of the information to keep your data secured. Encryption technique is accomplished by transforming the string of characters and words comprising the data to produce a new series that is the coded form of data.[1]

End to End Encryption defines that the message or data sent by one person to another person can only be understood by two of them.No Third Person read that data even if he gets access that data. It is a method of transmitting data where all the users easily send and receive data Messages are only encrypted by the users.[2] No third person can encrypt that information at the same time. If any communication app is encrypted it doesn't mean that the owner company cannot view this message. E2EE consists of five parts: identity, protocols, algorithms, secured implementation, and secure operation. This Protocol is needed to set up everything required for encryption, like a key exchange technique and the algorithms. This algorithm implements mathematical processes to protect the data in a way that so that it is almost impossible to decode your data without the predefined key. Secure implementation and operation are necessary to confirm that the encryption process is not affected to cyberattacks on your hardware sides, such as the viruses and malware program. [3][4]

In 1991 free first widely used end to end encryption messages program software known as PGP or we said Pretty Good Privacy a coded program invented by the Phil Zimmermann.

But it takes long years for that overall encryption channel to reach the large masses.[5]

Data and information encryption are known to protect user-information from other peoples. It Converts data from a specific format, called plain text, to another type of format, called encrypted text, using an encryption key approach. Compression and encryption methods are now performed separately. Pre-modern cryptography was practically synonymous with encryption method, the conversion of information from a readable format to apparent unreadable format. Modern cryptography technique relies mostly on mathematical theory, algorithms and computer knowledge. Cryptographic algorithms were based on assumptions of the calculation hardness, which makes it difficult for every opponent to put these algorithms into real practice. As we know Theoretically, it is possible to destroy the system, but it is impossible to do so by any known in the practical means. The growth of cryptographic technology leads to several legal problems in the information age.

Secured operations and implementation are required to confirm that the E2EE process is not vulnerable to cyber attacks of hardware such as viruses program, and malware program. All these factors work together to provide a fluid system that works more efficiently and provide possible security for end-users. It helps E2EE to adapt the various threats imposed by hackers, since a single factor can evolve to correct a single vulnerability, rather than having to re-invent the whole system. There are many different categories of each of the factor that has developed for different applications over, the years.//

//End-to-end encryption blocks third-party users from editing transferred data. In such a way, E2EE can support ease risk and secure complex information and data by blocking third parties from editing user data when it is moved from one resource to another resourse[6]

E2EE is used to make the business and private communication of the users more secure. It allows the data or information communicating between the users is more secure so that it is hard to crack for the third party. This technique gave peace or relaxation of mind to the users because now their data is secured to transmit only the receiver can decrypt it whom they want to send it.. [7]

It follows the key exchange method in which the public key of the communicating user’s sender and receiver are shared with each other. These shared public keys combined with the private keys of sender and receiver and make a shareable key which is required to encrypt the message of the user and that message is only decrypted by the receiver's private key which is non-shareable key. [8]//

# Problem Statement

WhatsApp Messenger is the world’s top-rated chatting App. Today, people are concerned with their privacy a lot, so their privacy can’t be compromised. WhatsApp Messenger uses end-to-end encryption and claims to ensure users’ privacy. Their methodology uses two keys; one is a public key, that is a part of the encryption protocol and the other one is a private key that is never shared. These two keys when combine, you get access to the WhatsApp Messenger Account data. There is a loophole detected in WhatsApp Messenger end-to-end encryption. If the private key of a WhatsApp Messenger account is retrieved in some ways; all chats can be easily decrypted as shown in figure 1.

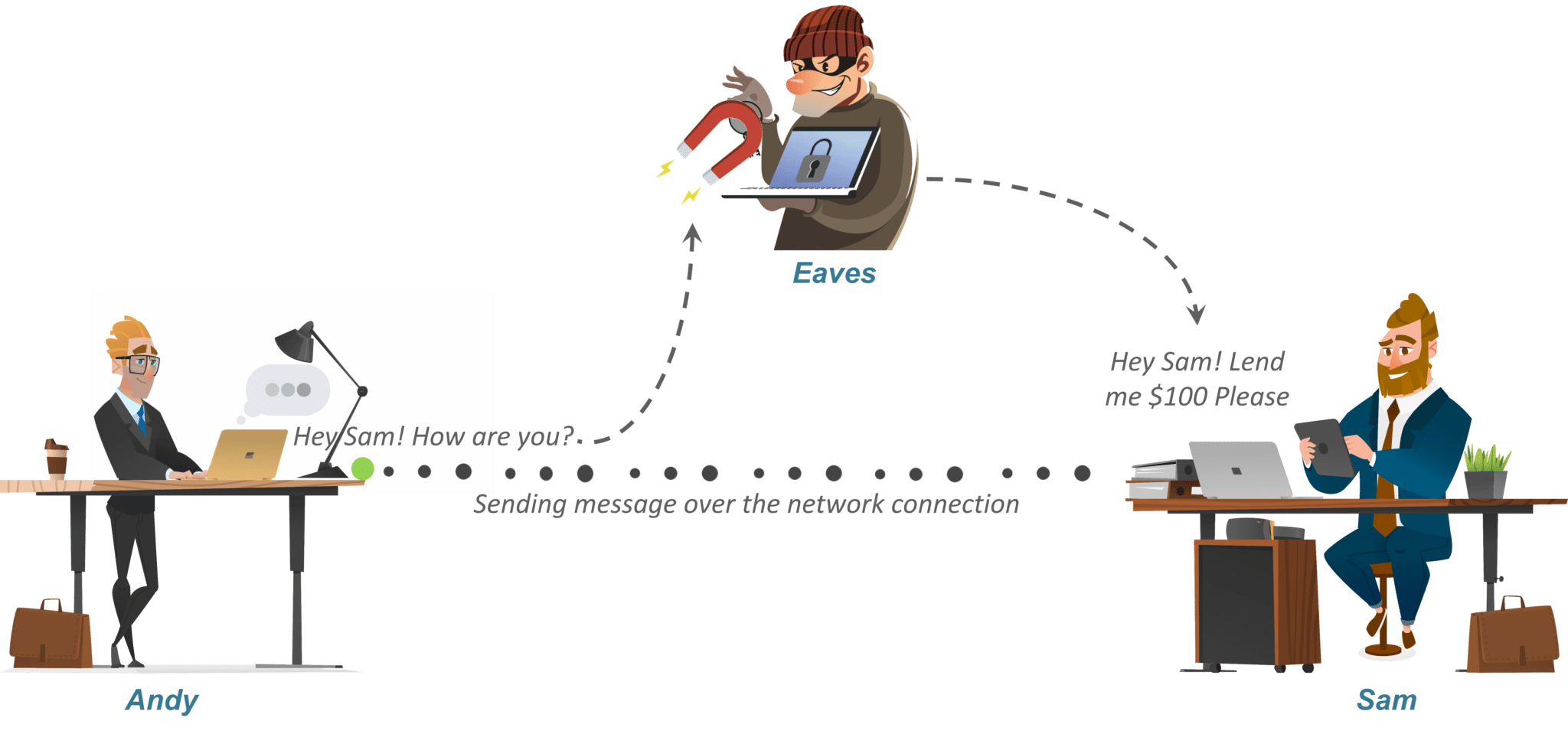


Figure 1. Third-Party interference (Insecure Network) [16]

# Solution

In the current algorithm, WhatsApp Messenger uses a private key at the user level. If we generate this key at each chat/message level then the security can be maximized up to some extent. In this way, if a single key is retrieved by some third party; they can only decrypt a single message. In this way, we can maximize the security level of WhatsApp Messenger Messenger. In this method, if someone attacks on the network, the network will be smart enough to trace the error as shown in figure 2.

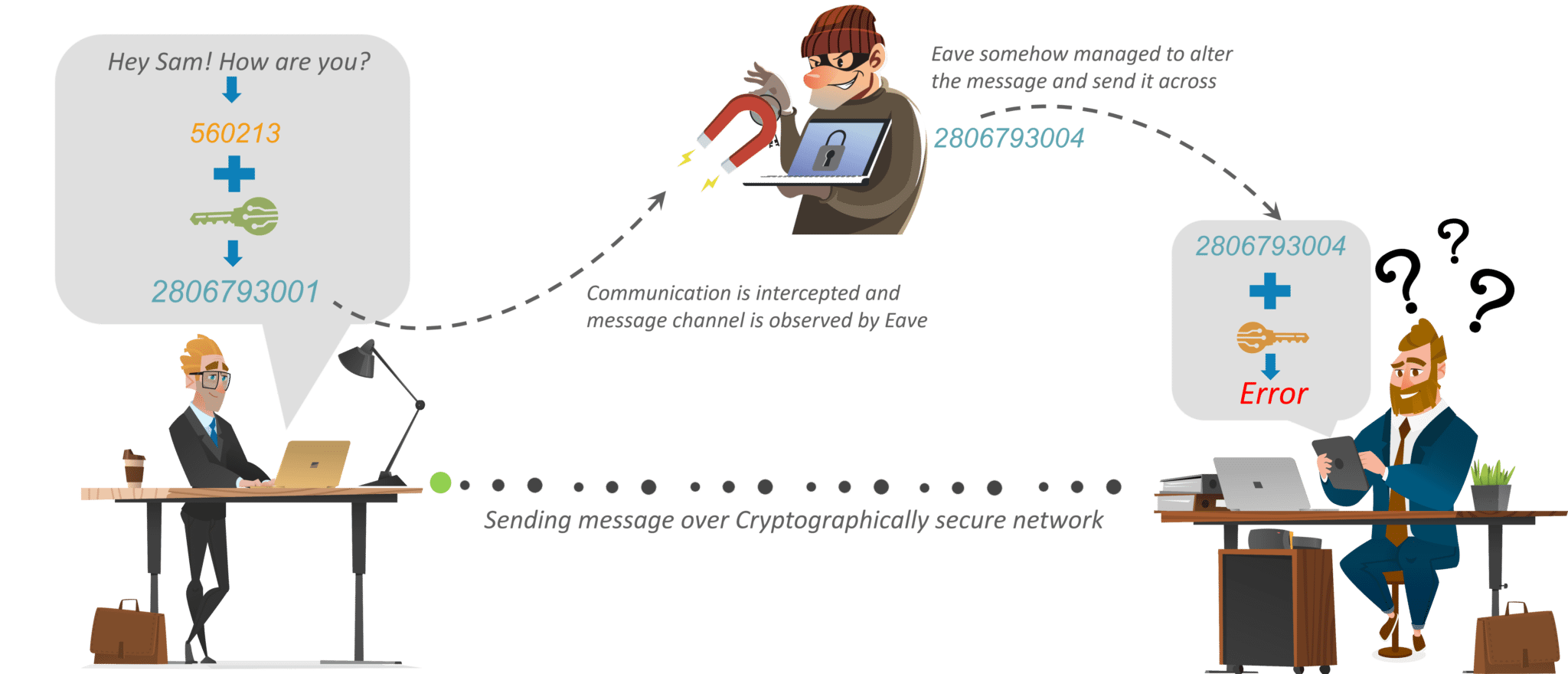


Figure 2. Secure Network using Cipher Technique [16]

# Objectives

1. Improvement in Data Privacy
2. Improvement of Network Security
3. Creating difficulty for the third-party attacks.
4. Solution for Backdoor Access.
5. Building a secure network.

# Literature Review

//End-to-end encryption is a method of a secure way of communication that prevents third parties to access that data. It can allow the user to encrypt that data so it cannot be accessed by other people. The messages are secured with locks and the targeted user has a special key to access that data. No one else, including the hackers, can access or read the encrypted data. [1]

Probably 4000 years ago in Egypt. End to end is the normal way encryption works the sender encrypts a message, passes it to a courier or postal service. The systems invented before end user are some drawbacks due to which data encryption is not possible and the user comes into beginning to overcome these drawbacks and to make sure to data more secure during communication. [2]

End-to-end encryption was implemented by exchanging keys to allow the key pair that is interchanged between the two parties to generate the secure common key that is used as the key for the encryption algorithms.// The proposed secure chat application provides confidentiality, confidentiality, and integrity. Users can be sure that no one, not even the service provider, can read their messages. The algorithm used to encrypt text messages is the AES standard, which is slower than other encryption blocks but offers greater security.

Data security is essential for protecting customers’ private information such as passwords, debit or credit card information, mailing addresses, or birthdays. Data security measures such as using products and services that employ encryption moderate the risk of a breach. Cyber Security found that sixty per cent of all small businesses that suffer due to network cyber attack goes out of business within 6 months of the breach. [3]

End to end encryption provides two types of keys public and private key for encryption and decryption of data or messages to both user’s sender and receiver who want to communicate. Both sender and receiver shared their public keys to encrypt the information. If the sender wants to send some secret data to receiver he will encrypt this information by using the receivers public key and send data to the server it does not decrypt this information and send it to the receiver the encrypted information is decrypted by receiver using his own private key which is only known by the receiver, not the sender. [4]

Some limitations on end to end-user encryption are government policies. [5] Government is banning the strong encryption for the user and only allows implementing weak encryption so that intelligence can access the encrypted data by secret techniques. [6] By creating software and hardware backdoor techniques they can access the encrypted data. [7][8] The mandatory -key Escrow allows the government to bring court orders and to force companies to give an extra key to intelligence agencies to access the encrypted data. [9]

A secure implementation is an essential element to ensure the security of the E2EE process. For example, if the malware was installed on a client's computer that can steal data from the computer's memory, the full encryption process is not necessary because the hacker has access to the data after decryption. Behringer also mentions malware that can record keystrokes. Its means that passwords and usernames can be stolen and used to pretend to be users. Because of this vulnerability, companies using E2EE often require network users to install an antivirus service on their computers to prevent malware attacks that compromise the security offered by E2EE. In general, E2EE is an extremely secure way to send information over the Internet and the best solution to improve online privacy. It is due to its adaptability, the use of privately generated keys and complex algorithms that enable maximum security.

The first free, widely used end-to-end encrypted messaging software was PGP, or Pretty Good Privacy, a program coded by Phil Zimmermann and free in 1991. But it's taken Period for that whole encryption channel to reach the masses. [10]

End-to-end encryption blocks third-party users from editing transferred data.[11] In that way, E2EE can support ease risk and protect complex information by blocking third parties from editing user data when data is moved from one resource to another. [12]

The signal protocol introduced the chain concept Essential to support outdoor message reception and a rare form of secret retransmission. Instead of using a shared secret Encrypt messages directly; signal derives a new encryption key for Each message applies an essential derivation function to the current one Key to generate a new chain in the process. The shared secret from sharing keys from our group can be used directly as the beginning of a keychain. Indeed, our implementation derives its message key from a hash string to ensure that each key. It is used only once and offers a kind of secret after committing a chain key

E2EE is used to make the business and private communication of the users more secure. It allows the data or information communicating between the users is more secure so that it is hard to crack for the third party. This technique gave peace of mind to the users because their data is secured to transmit only the receiver can decrypt it. [13]

It follows the key exchange method in which the public key of the communicating user’s sender and receiver are shared with each other. [14] These shared public keys combined with the private keys of sender and receiver and make a shareable key which is used to encrypt the message and the message is decrypted by the receiver's private key which is not shareable key. [15]

# Methodology

Encryption secures data and information from unauthorized access and keeps it confidential. If there is no encryption between sender and receiver, the third-party may fetch the data or even may alter the data. Cryptography is a technique for securing communication and data in the presence of adversaries or third parties. [3] In this way we secure our conversations.

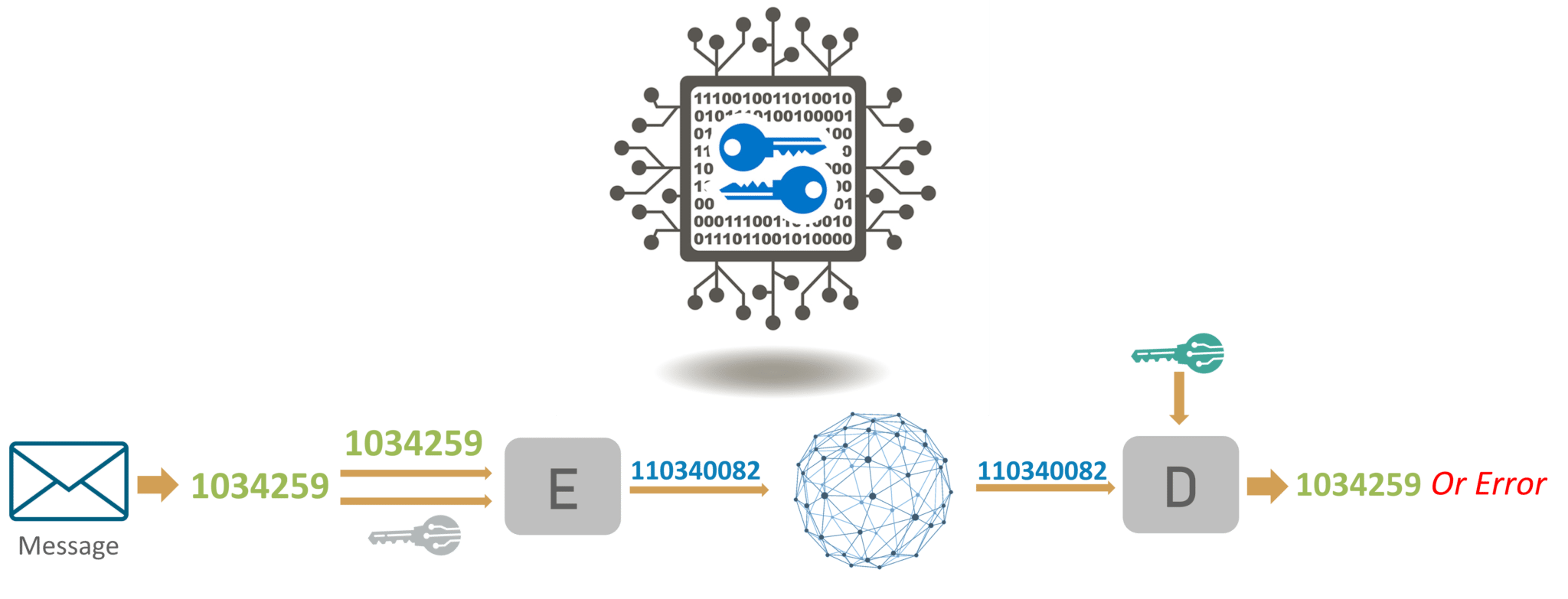


Figure 3. Cryptography Mechanism [16]

It follows the key exchange technique. Both users who are communicating have two types of keys public key and private key. Public keys are the shareable keys. [7] Cryptography has two categories: Symmetric key Cryptography and Asymmetric Key Cryptography.

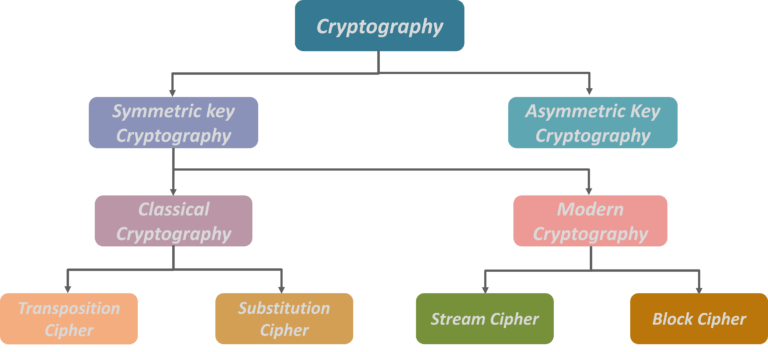


Figure 4. Encryption Algorithms [16]

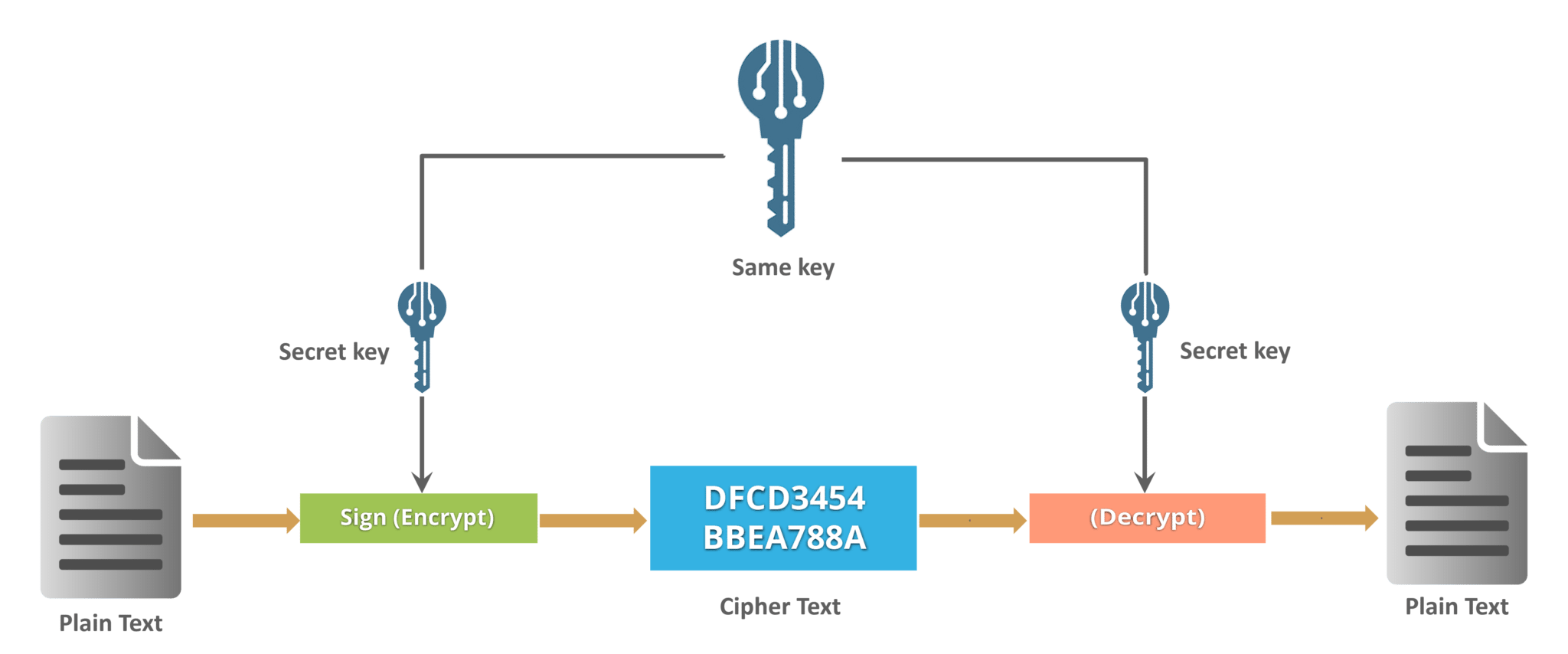
An encryption technique in which the sender and receiver share a single, common key that is used to encrypt as well as decrypt the data or a message.

Figure 5. Symmetric Key Cryptography [16]

Cryptography uses a transposition cypher by which the positions held by units of plain-text are shifted according to a regular system and the ciphertext constitutes a permutation of the plain-text. In this way data is encrypted. [6]

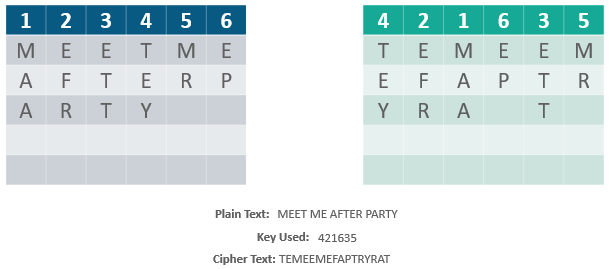


Figure 6. Transposition Ciphers [16]

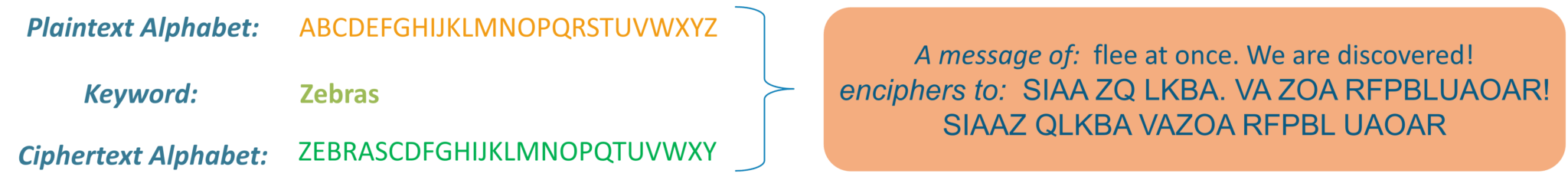


Figure 7. Substitution Cipher [16]

An encryption technique that implements a deterministic algorithm along with another symmetric key to encrypt a block of text or data, rather than encrypting one bit at a time as in-stream cyphers as mentioned in the figure below.

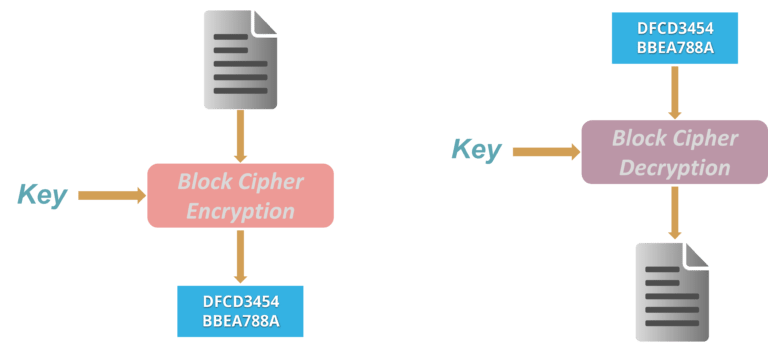


Figure 8. Block Cipher [16]

In this way, we ensure that the message is delivered safely without modification. This also helps us to identify the loopholes in a weak security system.

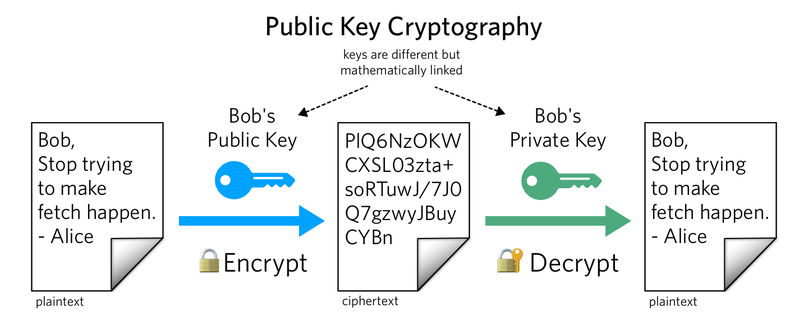


Figure 9. Public Key and Private Key Concept in Cryptography [16]

Public keys of both sender and receiver are shared with each other. These public keys which are shared combined with the private keys of both users which are communicating and make a shareable key. [9]

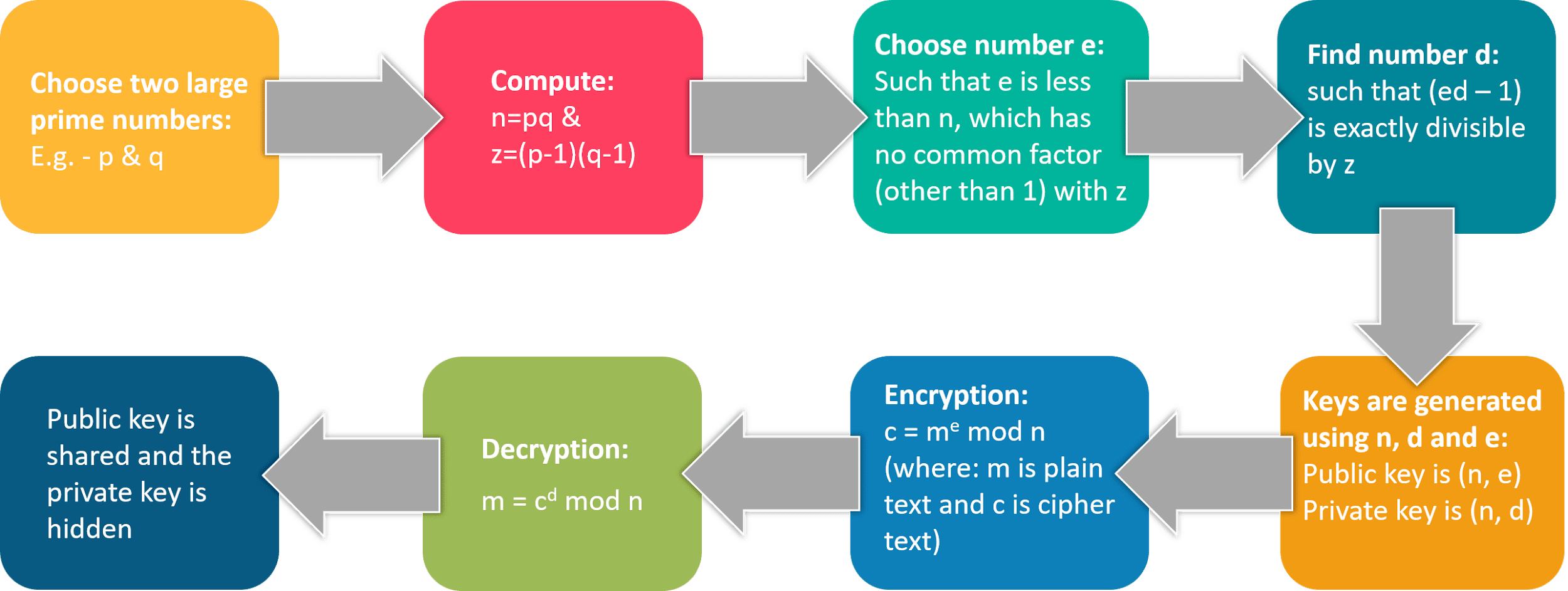


Figure 10. RSA Algorithm [16]

RSA stands for Rivest, Shamir, and Adelman, the inventors of this technique. Both public and private key are interchangeable. Variable Key Size (512, 1024, or 2048 bits). These shareable key are used to encrypt the data users are communicating.[13] If a hacker successfully gets the private key, he can read the text messages and even can alter the messages as shown in the figure. The data is decrypted by the receivers private key which is not even available to the sender and the organization which used this technique. WhatsApp claims that it doesn’t store any data on its servers but third parties may interact with the data to manipulate it. WhatsApp uses end-to-end encryption on the user-level interface. If we implement the same mechanism on each message level instead of user-level, we can then maximize the security level. [8]

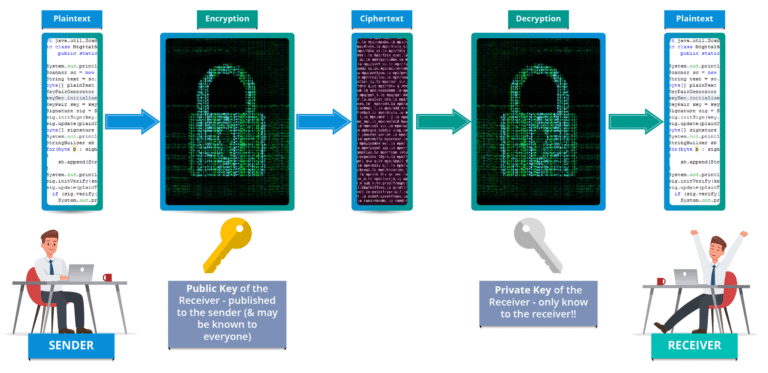


Figure 11. Asymmetric Key Encryption (or Public Key Cryptography) [16]

# Applications

**Communication on Messaging Platforms**

Phil Zimmerman published PGP (Pretty Good Privacy)because he thought that all earn space. When Apple WhatsApp Messenger began in 2011, end-to-end encryption was incorporated due to the launch of the platform. WhatsApp, a popular Facebook messaging service, also implemented the system in 2014. WhatsApp is another of the main platforms for end-to-end encryption.

**Encryption on Additional Platforms**

Moreover to various messaging products, various methods utilize end-to-end encryption on various platforms. End-to-end encryption is commonly found in email, on the phone and even on radio. The various email programmes include GnuPG, Protonmail, Mailfence, S / MIME, Inky and pEp. For end-to-end encryption of the phone, software such as ZRTP and FaceTime make use of the Tone across the Internet or VoIP etiquette, which depends on the immediate transportation protocol. The software which uses the end-to-end encryption for the broadcasting is called TETRA. Various requests and local services make use of end-to-end encryption for interaction and instant messaging. Encryption on all these proposals is critical as it allocates reliable and private communication techniques between two or more people.

**Encryption of Patient Data and Medical Records**

Confidential personal data can not just be found on interaction programs. It can also be observed in clinics where patient records used to follow long-suffering history, difficulties and documents. There are regularly robbers who are taking advantage of undiscovered data, who go to take data or contact medications or anything that persons, in general, do not have contact to. On the way to solve this problem, documents and data are first converted with a cypher with the purpose of cannot be interrupted by the incorrect eyes. The future recipient also has a key that can decrypt the data, that can use information that is encrypted and that can help the patient. It is an end-to-end encryption process that also directly helps persons by protecting their health data and protecting them from bad persons.

# 

# Challenges

//As we know that end-to-end encryption is an extremely secure method of communication, but there are still ways to access the information in an encrypted file using techniques like as “Man in the Middle Attacks”. These attacks point on messages from the sender to the receiver and receiver to the sender, but it takes the edge because of the use of the Internet connection that depends on the network.

Man in the Middle attacks technique is keystrokes on a communication network with which the hackers or third party can intercept and manipulate all message sent from the sender to a receiver. In a man attack in the middle technique, the attacker could fetch the message of the person sent using a set of public keys. After opening the message, the hacker or third party can see the data and even change the personal data or message. After intercepting the message and doing what you want to do, you can send data with a similar set of keys that sends it to the required receiver, and there is no trace of it. These hacking attacks or data loss are very complicated, but there is an easy method to prevent your data from these attacks. Only by using a set of a private and secure network, it keeps people away from their network connection, and they are not able to intercept data and messages. But Unfortunately, some of the people stay away from public networks without passwords and are get unProtected to these attacks on their personal and digital platform information. Even if they have connections to the public network, there is a high-risk present of being connected, and only a few people know about it.

An encrypted form of the message is sent from a remote type of connection and received over the end user's network. The attacker or third party is also connected to the same type of the network and therefore they get easy access to the encrypted message. With a set of public or the stolen keys, the third parties and attackers can view and even change the information and messages. The hackers can re-encrypts the message and send it to the sender( end-user), who cannot say that a message has been tampered with.

# Limitation

Organizations implement end-to-end backdoor encryption technique and sometimes do not instruct their users to have a backdoor. A back door is a system set up by the service provider, in which they can enter through backdoors and retrieve sent messages, and decrypt them and pass them on to third parties organization such as the ISI, the CIA and other organizations under the government. Generally, consumers ignore this because they do not get a genuinely encrypted end-to-end service. when implementing backdoors, this means that the service which they providing are wasn't end-to-end encrypted and your data is not secured, which means it wasn't as secure as we thought it is protected. However, the back doors also represent a security vulnerability in the software or system through which attackers can access a system's private data or users. If WhatsApp adds a back door to the software or application, it is no longer a secure way of communication method, and the software loses a substantial part of its attractiveness. It is also likely that installing such a mechanism will result in intelligence agencies knocking always on WhatApp door asking them to reveal someone's messages and information.

If anyone thinks that removing WhatsApp encryption might be the solution, they don't understand the real problem. Even if you eliminate WhatsApp end-to-end encryption, the criminals could create their own setup of similar software that they are able to use for communicating securely while due to this the ordinary users lose the technique to send truly private data and messages.

The back door is implemented to protect the public, so Microsoft and Skype had decided to protect the public. In general, Microsoft not required to access sent messages because most of the users have no bad intentions. Understandably, Microsoft and Skype would like to access the records after the fact to provide the government and any intelligence agencies with information that could protect the public data in the future.

# 

# Conclusion

As a result of Ultra Encryption, Security level would be increased up to many extents. Users would be at the freedom of sharing things in private. This will also build their trust in the organization. In this way, the security level is enhanced in its own way. However, there is still a lot of significant risk of putting your private records in a service that is easily accessible to anyone with a connection or a type of device. But unfortunately, many people try to infiltrate and steal private data and records. That is why end-to-end encryption is used when we applied to this type of technology and secure the user's confidential data. Contrary to the already present opinion, some people believe that the risk of mischievous use of end to end encryption technology eliminates the benefits of data protection on the Internet connection. In the previous version of WhatsApp, security was compromised but by using ultra encryption; security level is increased and the difficulty level for third parties and hackers is increased too many times.

# Gantt Chart

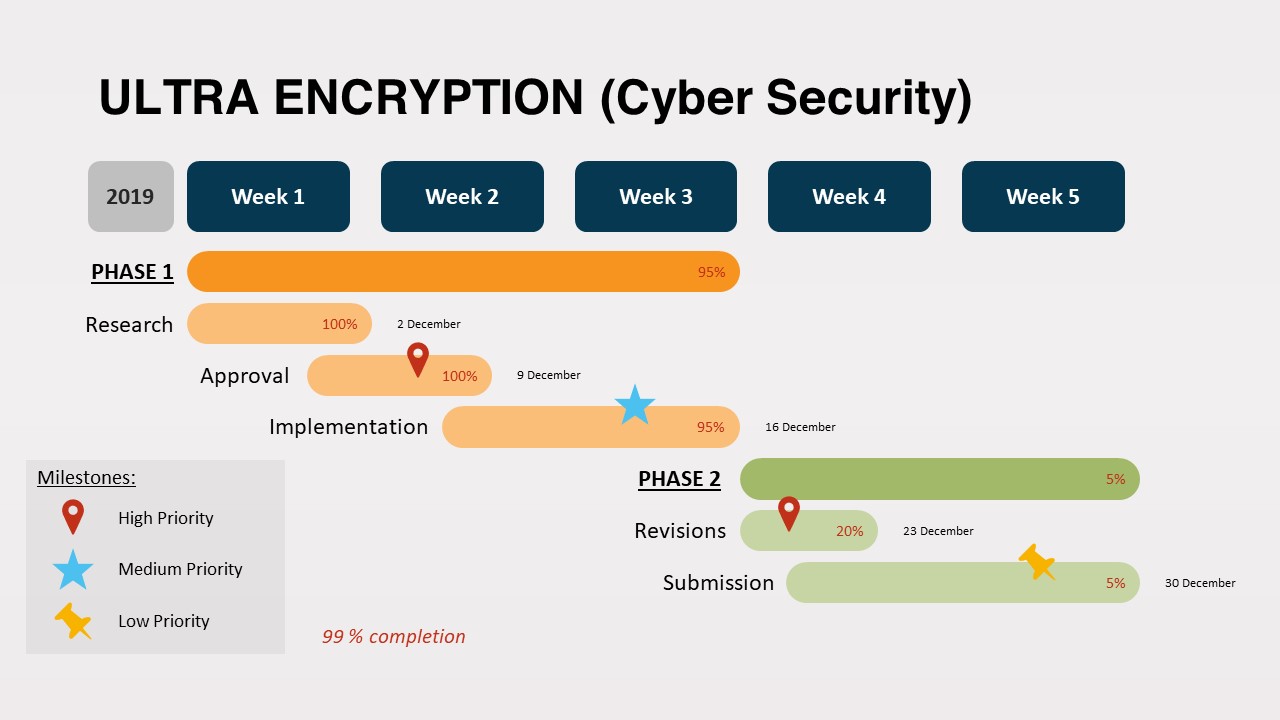


Figure 12. Gantt Chart Ultra Encryption

# References

1. FIPS PUB 197, Advanced Encryption Standard (AES), 2001. U.S.Department of Commerce/National Institute of Standards and Technology.
2. NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation, 2001. U.S.Department of Commerce/National Institute of Standards and Technology.
3. NIST SP 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, 2007. U.S.Department of Commerce/National Institute of Standards and Technology.
4. NIST SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2007. U.S.Department of Commerce/National Institute of Standards and Technology.
5. FIPS PUB 180-4, Secure Hash Standard, 2015. U.S.Department of Commerce/National Institute of Standards and Technology.
6. A new generation of safe messaging: Letter Sealing. LINE Blog, 2015. https://engineering.linecorp.com/en/blog/detail/65.
7. LINE Enters Agreement with Japan’s CAO for Mynaportal Interconnectivity, 2017. https://linecorp.com/en/pr/news/en/2017/1771.
8. Line Will Top 50 Million Users in Japan This Year. eMarketer, 2017. https://www.emarketer.com/Article/Line-Will-Top-50-Million-Users-Japan-This-Year/1016207.
9. 179. David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thome, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella B´eguelin, and Paul Zimmermann. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. In Indrajit Ray, Ninghui Li, and Christopher Kruegel, editors, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015, pages 5{17. ACM, 2015.
10. Nadhem J. AlFardan and Kenneth G. Paterson. Lucky Thirteen: Breaking the TLS and DTLS Record Protocols. In 2013 IEEE Symposium on Security and Privacy, SP 2013, Berkeley, CA, USA, May 19-22, 2013, pages 526{540. IEEE Computer Society, 2013.
11. Mihir Bellare and Chanathip Namprempre. Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. J. Cryptology, 21(4):469{491, 2008.
12. Mihir Bellare, Phillip Rogaway, and David A. Wagner. The EAX Mode of Operation. In Bimal K. Roy and Willi Meier, editors, Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers, volume 3017 of Lecture Notes in Computer Science, pages 389{407. Springer, 2004.
13. Daniel J. Bernstein. Curve25519: New Diffie-Hellman Speed Records. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings, volume 3958 of Lecture Notes in Computer Science, pages 207{228. Springer, 2006.
14. BitcoinWisdom.com. Bitcoin Difficulty, 2017.  
    https://bitcoinwisdom.com/bitcoin/difficulty.
15. Simon Blake-Wilson and Alfred Menezes. Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol. In Hideki Imai and Yuliang Zheng, editors, Public Key Cryptography, Second International Workshop on Practice and Theory in Public Key Cryptography, PKC ’99, Kamakura, Japan, March 1-3, 1999, Proceedings, volume 1560 of Lecture Notes in Computer Science, pages 154{170. Springer, 199
16. Shashank, May 22, 2019, “What is Cryptography? – An Introduction to Cryptographic Algorithms”   
    https://www.edureka.co/blog/what-is-cryptography/