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

List of Figures

Introduction

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

End to End Encryption means 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 to that data. It is a method of transmitting data where all the users easily send and receive the users only encrypt data Messages.[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 contains the five components: identity and protocols, algorithms, secure implementation, and reliable operation. The Protocol is used to set up everything needed for encryption, like a critical exchange and the algorithms. The algorithm uses mathematical processes to protect the data in such a way that so that it is nearly impossible to decode your data without the predetermined key. Secure implementation and operation are necessary to ensure that the encryption process is not affected to cyberattacks on your hardware sides, such as viruses and malware. [3][4]

The first free, widely used end-to-end encrypted messaging software was PGP, or Pretty Good Privacy, a program coded by Phil Zimmermann and open in 1991. But it's taken Period for that whole encryption channel to reach the masses.[5]

End-to-end encryption blocks third-party users from editing transferred data. In that way, E2EE can support ease risk and protect complex information by preventing third parties from compiling user data when data is moved from one resource to another.[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 reliable 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. [7]

It follows the critical exchange method in which the public key of the communicating user’s sender and receiver are shared. 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. [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.

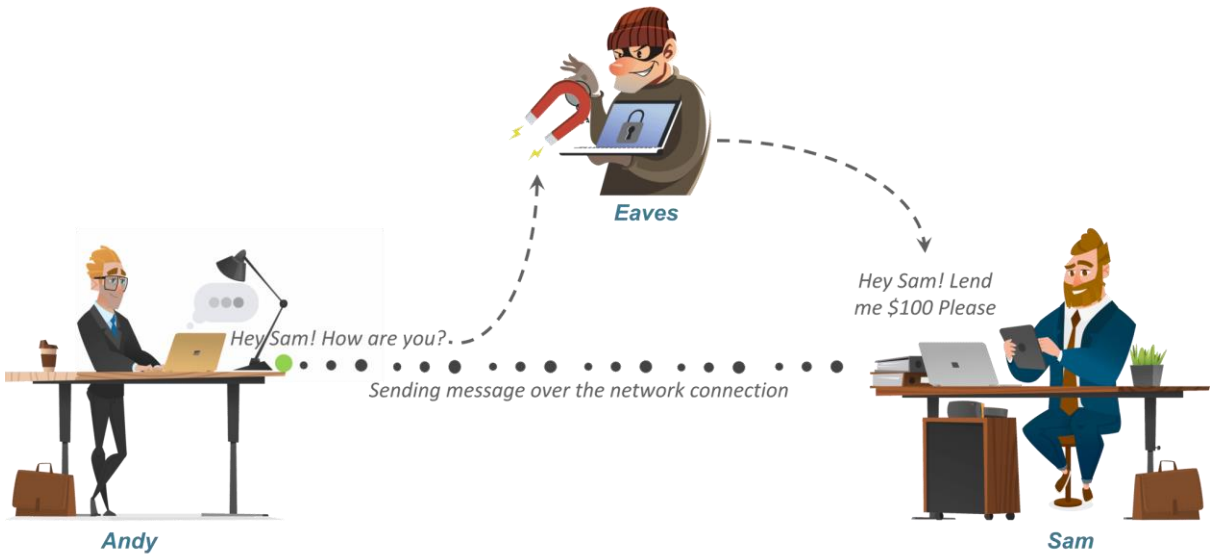

Figure 1. Third-Party interference (Insecure Network) [16]

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 maximised up to some extent. In this way, if some third party retrieves a single key; they can only decrypt a separate message. In this way, we can maximise 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.

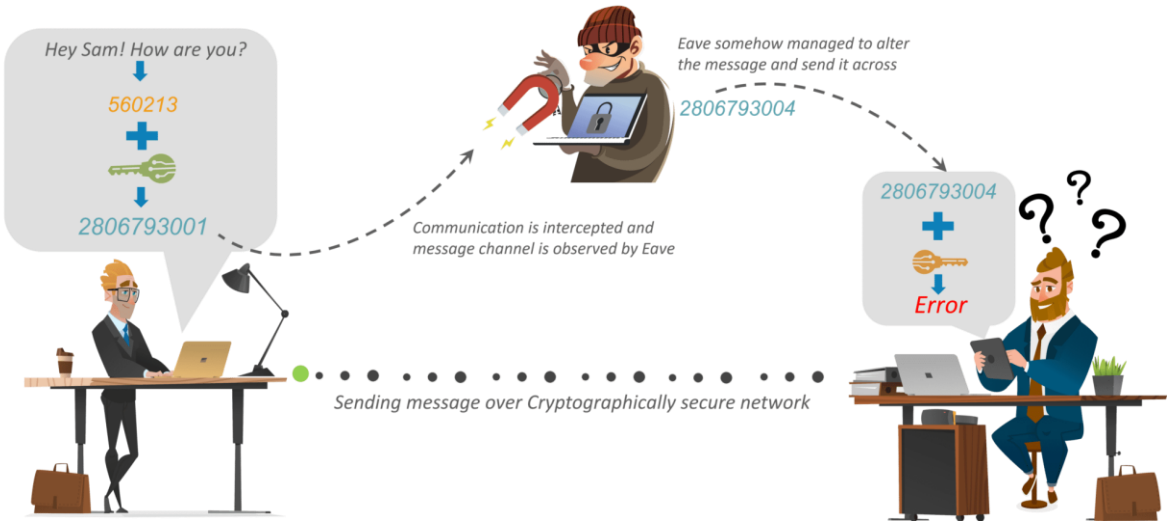

Figure 2. Secure Network using Cipher Technique [16]

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 technique of secure 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 unique 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 standard 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]

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 cyber network attack goes out of the company within six 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 decoded 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]

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]

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 unauthorised 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.

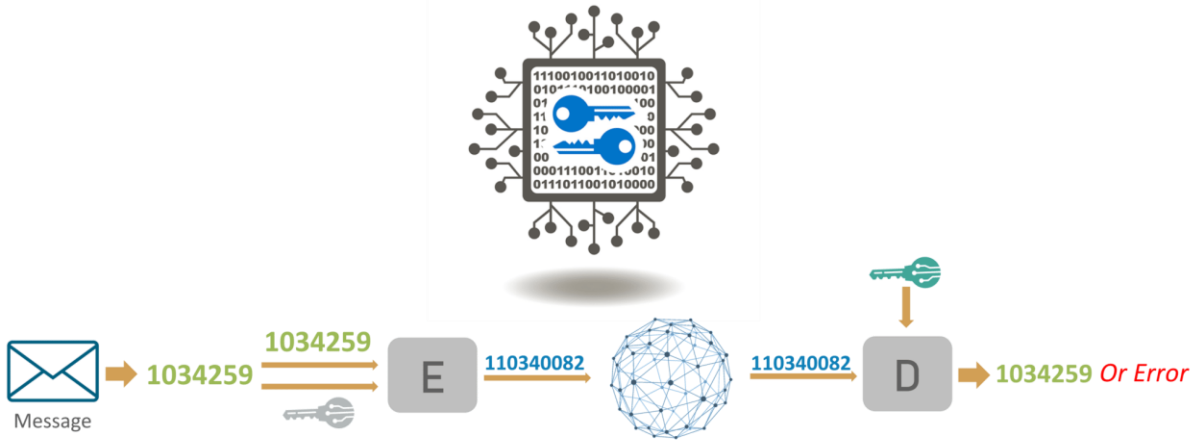

Figure 3. Cryptography Mechanism [16]

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.

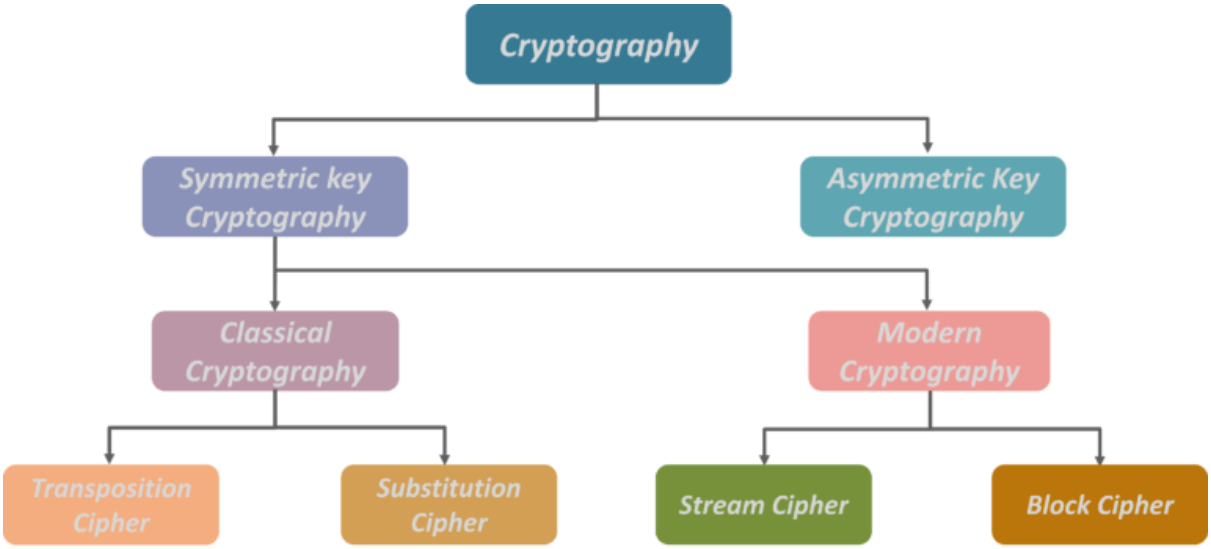

Figure 4. Encryption Algorithms [16]

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

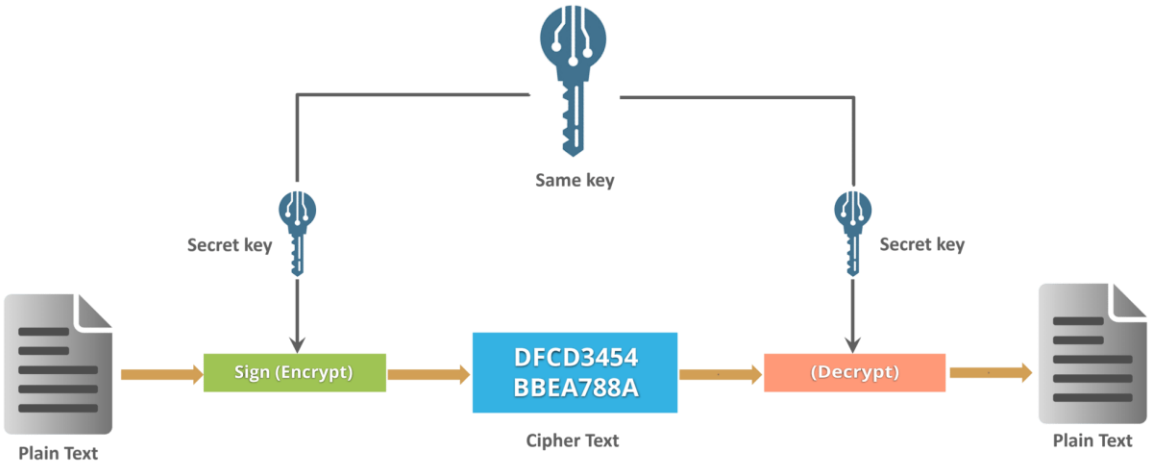

Figure 5. Symmetric Key Cryptography [16]

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

1	2	3	4	5	6
M	E	E	T	M	E
A	F	T	E	R	P
A	R	T	Y		

4	2	1	6	3	5
T	E	M	E	E	M
E	F	A	P	T	R
Y	R	A		T	

Plain Text: MEET ME AFTER PARTY

Key Used: 421635

Cipher Text: TEMEEMEFAPTRYRAT

Figure 6. Transposition Ciphers [16]

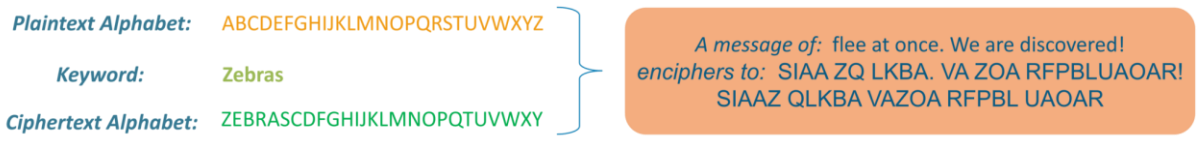

Figure 7. Substitution Cipher [16]

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 ciphers as mentioned in the figure below.

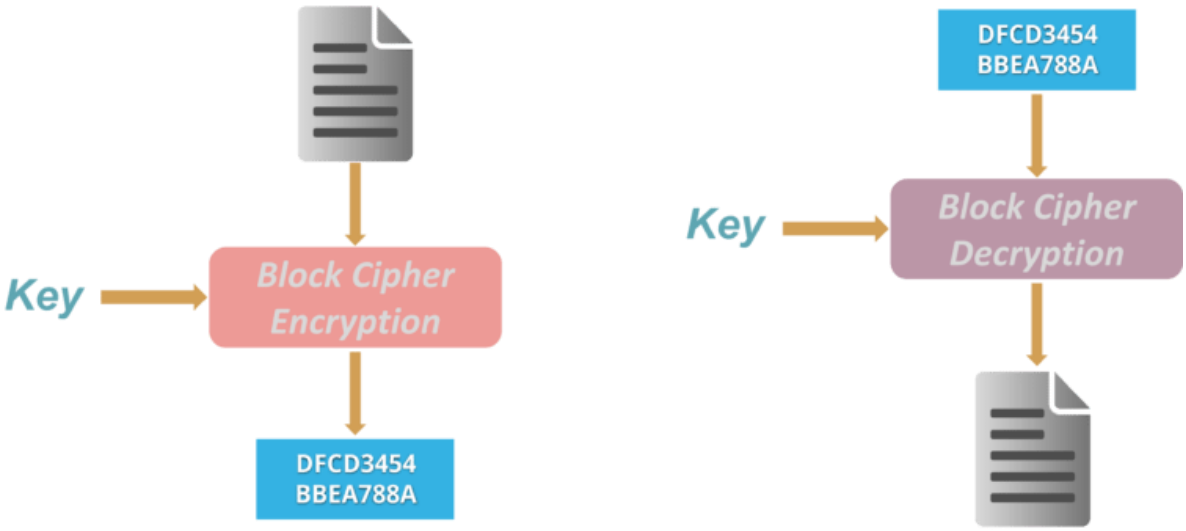

Figure 8. Block Cipher [16]

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.

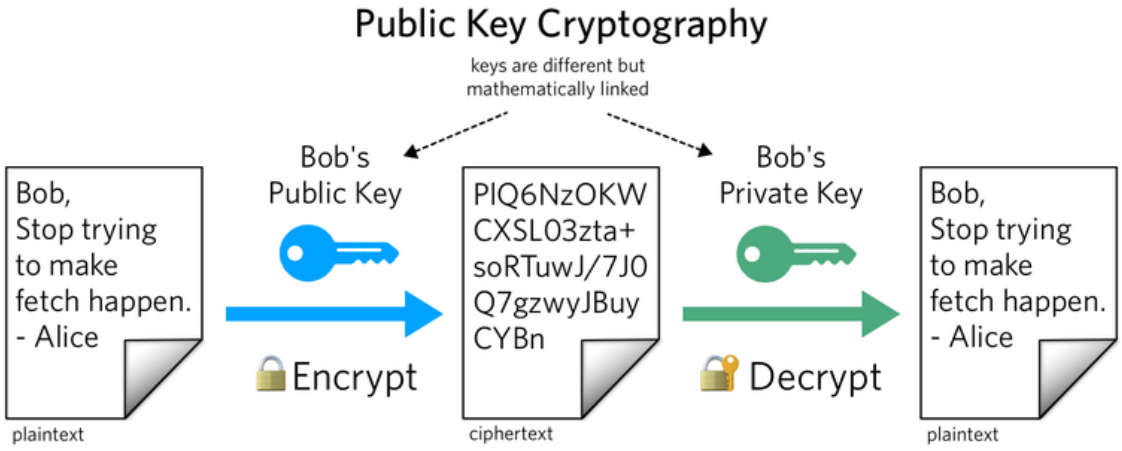

Figure 9. Public Key and Private Key Concept in Cryptography [16]

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]

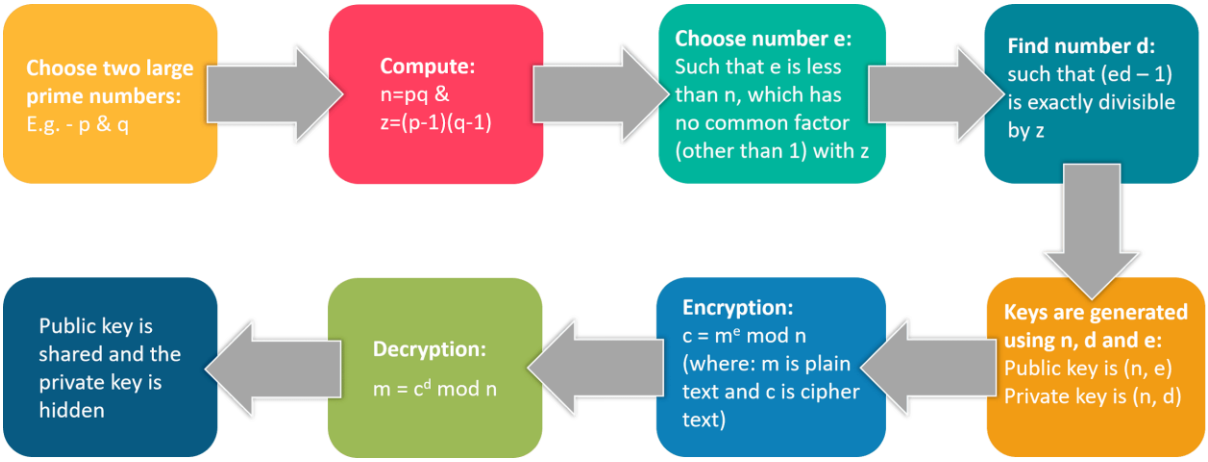

Figure 10. RSA Algorithm [16]

RSA stands for Rivest, Shamir, and Adelman, 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 of 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]

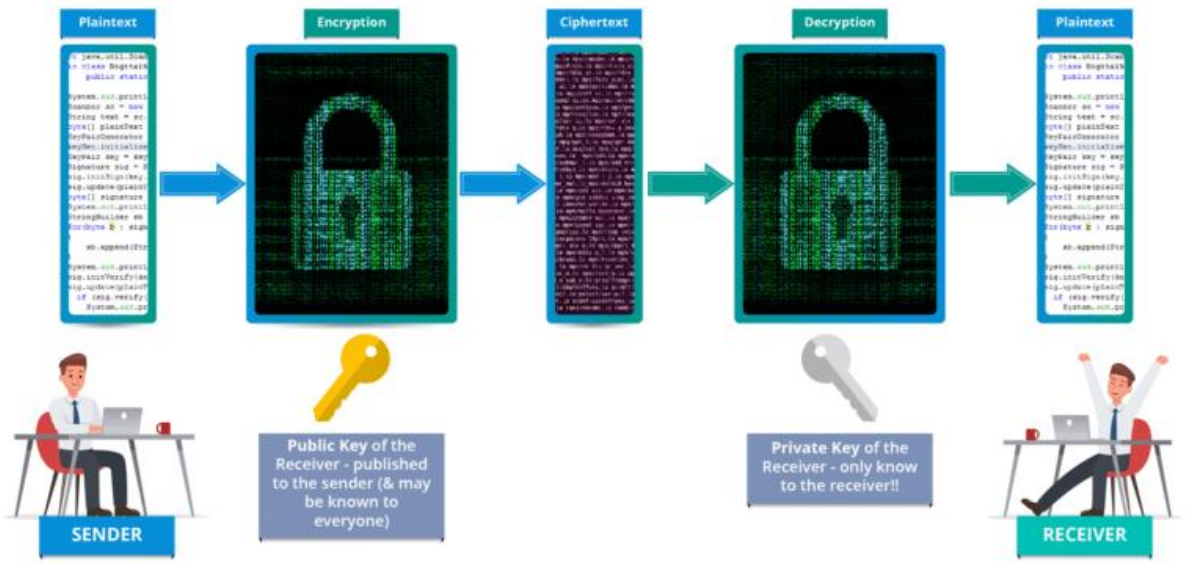

Figure 11. Asymmetric Key Encryption (or Public Key Cryptography) [16]

Outcome/Expected Result

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.

Gantt Chart

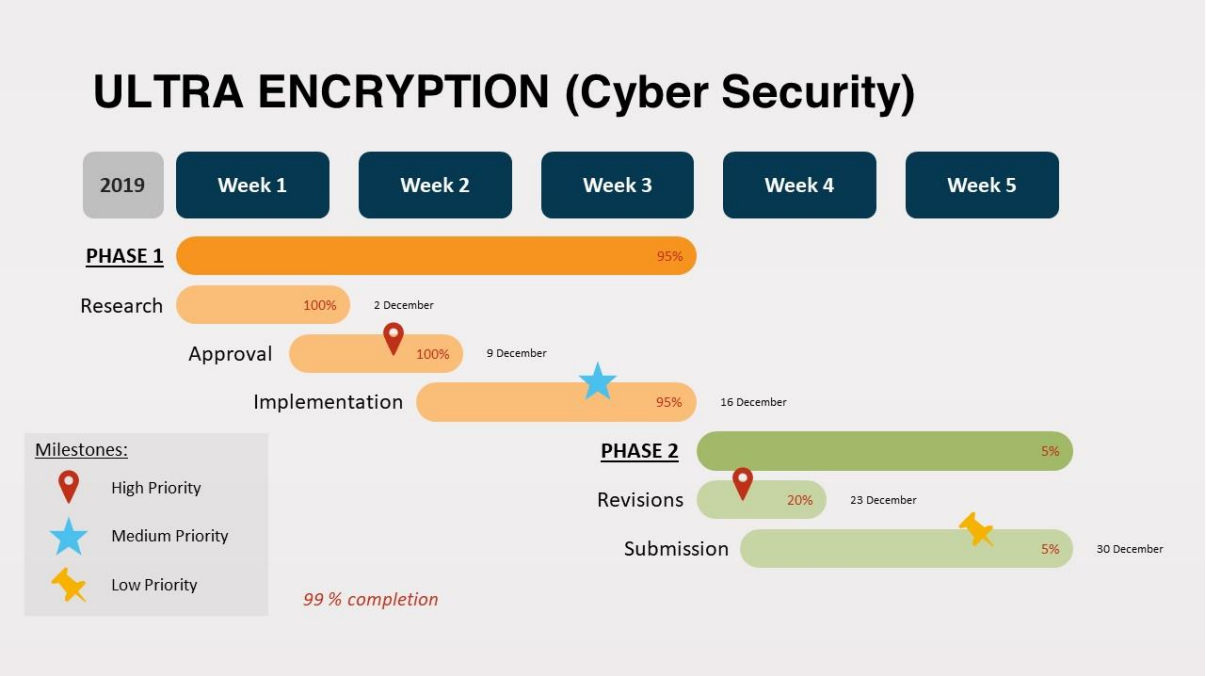

Figure 12. Gantt Chart Ultra Encryption

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 Thom´e, 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/