**SECURING BLUETOOTH WITH THE HELP OF CRYPTOGRAPHY AND MULTI-FACTOR AUTHENTICATION**

**Vikaskumar Darji1**, **Ramani.S2**

**1 Student, VIT, School of Computer Science and Engineering, Tamil-Nadu, India.**

**2 Professor, VIT, School of Computer Science and Engineering, Tamil-Nadu, India.**

***ABSTRACT: -***

*From many years, people are using Bluetooth for transmission and receiving data. Moreover, Bluetooth security is to safeguard administrations presented by gadgets as well as allow without a doubt. However, just like Wi-Fi Bluetooth can be very risky at some times. A few individuals don’t turn off Bluetooth after utilizing it they think that's not imperative that's where they are off-base. There are many attacks can be possible on Bluetooth like Eavesdropping, Denial of Service, Impersonation attack, etc. In this paper, it implements an encryption algorithm to protect Bluetooth transmissions, so even if an attacker attacks an open Bluetooth device, your data will be protected.* *In this algorithm, first the sender will authenticate the receiver if the receiver is legitimate user, then the sender will start encryption of data and start sending to the receiver. The receiver will start collecting the data which coming from the sender’s side. we are converting each character into number then arranging them again converting those number to different number. This algorithm is much more time-complex and hides a lot of data complex then Caesar ciphers, rail fence ciphers, and Playfair ciphers.* *Many of them can be brute force decoded, but this algorithm cannot. Here we use authentication with an encryption algorithm to prevent impersonation attacks.* *Even if the attacker is someone known to our device, the data will also be backed up. This eliminates the risk of data being stolen.*

***Keywords: -*** CRYPTOGRAPHY, MULTI-FACTOR AUTHENTICATION, BLUETOOTH

***INTRODUCTION: -***

A WPAN means wireless personal area network, which is designed for portable and mobile computing devices. Bluetooth technology is one of them. Bluetooth is a fascinating technology that uses in daily life. We can say this because when you play video or music on your wireless headphone or transmit those files to another device your device transmits around a million 0s and 1s to your headphones or other devices every second using Bluetooth. Bluetooth is license-free and used in the world usually and it uses a 2.4 GHz frequency-hopping spread spectrum. It is used for data transmission and can transmit voice. Bluetooth uses three kinds of security pairing processes. One is SSP (Secure Simple pairing), the second is LMP (Link Manager Protocol) also known as PIN-code based, and the third is None standard pairing. The SSP uses a very complex mechanism, which is known as elliptic curve cryptography. LMP establishes links between two Bluetooth devices and maintains the links for communication. LMP's main function is authentication, encryption, and negotiation of packet size. In the past many technologies are being found, modified, and is secured by developers, as we know whenever new technology comes same old technology will be forgotten, this same thing happens with Bluetooth technology. For the last few years, many people are neglecting the security of Bluetooth or we can say Bluetooth security. However, neglecting Bluetooth security can be a risk at the same time. For example, people forgot to turn off their Bluetooth the attacker can do an impersonation attack them, in impersonation attack attacker act like a previous paired person and steal data or can send the malicious virus to the victim's device and that can be very dangerous for victim's data. Not just that there are many more attacks on Bluetooth pairing such as method confusion attacks, etc. To secure any type of data we need cryptography. Cryptography is very important because it allows us to securely protect data that we want to hide from others. There are three types of encoding algorithms in cryptography. They are Symmetric-key Cryptography, Asymmetric key Cryptography, Hybrid key Cryptography. Symmetric-key Cryptography is also known as secret-key Cryptography. In this Cryptography, Encode and Decode will use the same key. Asymmetric key Cryptography is known as public-key Cryptography. In this Cryptography, Encode and decoding will happen with different keys. And third hybrid key Cryptography is a combination of Symmetric and Asymmetric Key Cryptography. So here, we are proposing a new cryptographic algorithm for encoding in Bluetooth data transmission. Along with a cryptographic algorithm, we are also adding authentication. Over here we are trying to implement new algorithms for encoding and decoding. This algorithm will use the same key for encoding and decoding. As it's working, for now, we are going to call this algorithm spiral algorithm. We are Here in this sender turn on Bluetooth, will select a receiver, after selection system will generate a one-time password, the receiver will enter that on-time password into their device after that sender and receiver will be connected. For the transmission, the sender will write a message/ select file, according to that another password will generate by a system for encoding, the receiver will enter this password for decoding the massage or file and this is how the transaction will be done by the system. Bluetooth is a wireless technology that allows the exchange of data between different devices.While Bluetooth uses wavelength to transmit information, it generally only works within a short distance for the devices to stay connected. Chances are good that you are familiar with how Bluetooth technology works – you probably have used it to pair your iPhone with your Air Pod or connect your favorite music program with a speaker. In the simplest terms, Bluetooth is the technology that enables exchange of data between devices within a short amount of distance. What separates Bluetooth radio waves from the broadcast sent out by your favorite pop station is the fact that Bluetooth waves don't travel very far and are constantly switching frequencies. Most Bluetooth devices have a **maximum connectivity range of about 30 feet,** and that distance is reduced when obstacles (such as a wall) are present.

***LITERATURE SURVEY: -***

In this paper, the author's Peter Cope, Joseph Campbell, Thaier Hayajneh are doing a security analysis of Bluetooth. Then they are discussing the vulnerability of all Bluetooth versions, their performance analysis, and the result of all versions. principle destinations for this paper were to concentrate on Bluetooth innovation and to play out an involved examination of the different security weaknesses related to Bluetooth. By using the Ubertooth One instrument related to Kismet, Wireshark and Pop, they had the option to perform range investigation, parcel sniffing, and bundle unraveling [1]. In this paper, Shaikh Shahriar Hassan, Soumik Das Bibon, Md Shohrab Hossain, Mohammed Atiquzzaman, the authors are doing a comprehensive survey on Bluetooth vulnerabilities. First, they are trying to explain how Bluetooth works, its making, architecture, etc. they have illustrated the attacks on Bluetooth, malware in Bluetooth. They have also provided a probable solution for those attacks. Clients don't appear to be greatly fixed on these security dangers. Thus, large numbers of Bluetooth assaults are going undetected or unreported. A programmer's most noteworthy benefit would be the absence of worry for Bluetooth dangers. With a touch of information concerning those dangers, clients can stay safe. That reviewing work can be assisted specialists with finding other kinds of dangers that are at this point unclear through the information on those current dangers and further investigation and potential blends of controls [2]. In this papers authers are Maximilian von Tschirschnitz, Ludwig Peuckert, Fabian Franzen, and Jens Grossklags. the authors are trying to attack Bluetooth. The name of that attack given by authors is Method confusion attack. In this attack, the attack will get access as Man-In-The-Middle. Furthermore, the authors have also provided changes that would help to mitigate the attack. They exhibited a clever assault on the BLE matching in BT variant 5.2. The assault uses a strategy they call Method Confusion to acquire a MitM position between two matched Bluetooth gadgets. It mishandles a basic plan defect that upon their revelation was recognized by the Bluetooth SIG. The assault's fittingness was confirmed by embracing a normally utilized BLE driver into their system BThack, equipped for playing out the MitM assault. Utilizing that, they assaulted various cell phones, a smartwatch, and a financial gadget. All assaults succeeded and they were anticipating that numerous different gadgets should be powerless against this assault [3]. The authors A.S.Diallo, Wajdi Fawzi M. Al-Khateeb, R.F. Olanrewaju, F. Sado have proposed a protocol that uses more than one encryption to verify pairing another device. They are rehearsing Arduino IDE as programming, Bluetooth safeguard associated with an Arduino Uno R3 as equipment. The security issues in SSP, for example, detached and dynamic snooping are totally blocked by forestalling the trading of public keys and passwords in cleartext. Involved passwords and public keys are privately put away and the mysterious boundaries (IV and mystery keys) are produced arbitrarily by utilizing a solid irregular generator number then, at that point, safely traded with the RSA calculation. Other traded figures can't be altered because of the non-accessibility of the encryption keys to a third utilized and furthermore the strength of the pre-owned encryption frameworks [4]. In the paper, the authors Da-Zhi Sun, Yi Mu, Willy Susilo is discussing security in Bluetooth standard V5.0 and implement a Man-In-The-Middle attack on Bluetooth. they are likewise talking about weakness in secure straightforward matching in Bluetooth standard V5.0. they are likewise giving an answer for that assault in Bluetooth utilized in a home organization application. The MITM (Man-In-The-Middle) assaults can be conceivable, at whatever point the host reuses the passkey or when the gadget utilizes a nonrandom passkey age calculation rather than an irregular passkey age calculation in the passkey passage affiliation model. they further superior the passkey section convention to forestall the MITM assaults on the passkey passage affiliation model. The better convention can be effectively adjusted to the Bluetooth standard since it just utilizes the essential cryptographic parts that existed in the Bluetooth standard [5]. In this paper, the authors Samta Gajbhiye, Sanjeev Karmakar, Monisha Sharma, Sanjay Sharma is adding two new security levels in SSP (Secure Simple Pairing) to prevent MITM (Man-In-The-Middle) attacks. the creator is adding confirmation ease in that level to get the matching gadget. Same time one of the interfacing gadgets brings its security level down to match the security level of the most un-strong gadget and that is an issue. Most of the assaults depend on these issues. Accordingly, analysts are dealing with a convention that gives high security to delicate and secret data of gadgets. The SSP-APKE-DECE was working effectively with assistance in the improvement of two greater security layers in the current SSP. The convention conveys wonderful forward mystery, with respect to each matching meeting the new nonce was produced. Subsequently, every time the new meeting/interface key is created. Besides, the convention fights off from reflection assault, as the series of changes of nonce and the responsibility values are won't allow the aggressor to synchronize their gadget with the real gadgets. On account of the additional security layers, the blending season of SSP-APKE-DECE is more than SSP when contrasted with SSP. Regardless, the upgraded security of the proposed convention compensates for the upward of extra blending time [6]. In this paper, the authors Daniele Antonioli, Nils Ole Tippenhauer, Kasper Rasmussen was implementing BIAS (Bluetooth Impersonation Attacks) on Bluetooth. The authors developed an attack that would have affected each version of Bluetooth, the security mode, the manufacturer. their assaults permit them to imitate Bluetooth gadgets by taking advantage of weaknesses in the particular of Bluetooth validation and secure association foundation. they observed such weaknesses by manual review of the Bluetooth standard and utilizing their earlier business related to Bluetooth security. Because of a BIAS assault, an aggressor finishes secure association foundation while mimicking Bluetooth expert and slave gadgets, without knowing and validating the drawn-out key divided among the people in question. The BIAS assaults are standard agreeable and are successful against Legacy Secure Connections (utilizing the inheritance verification strategy) and Secure Connections (utilizing the protected confirmation method). The BIAS assaults are quick to reveal issues connected with Bluetooth's solid association foundation validation techniques, antagonistic job switches, and Secure Connections downsize. The BIAS assaults are covert, as Bluetooth secure association foundation doesn't need client communication. The BIAS assaults are at the design level of Bluetooth [7]. In this paper, the authors Moneer Fakroona, Fayez Gebali, Mohammad Mamun are using physical unclonable functions for Multifactor authentication. PUF (Physical Unclonable Functions) is physically given input of a condition (challenge) for digital devices for example fingerprints, etc. here, PUF is used to enable mutual authentication and key exchange. In this work, powerful lightweight validation and key trade plot are proposed among four elements engaged with a telehealth framework. when a series of secure verification is laid out between a cell phone, server, door, and an IoT edge gadget, a symmetric meeting key. The security of the proposed conspire is demonstrated officially utilizing the BAN rationale. Also, a casual security check guarantees obstruction of the proposed plot despite the most well-known assaults [8]. In this paper, the author An Braeken is comparing public keys and symmetric keys for client-server authentication. The author is comparing them by security-related, by performance-related. The creator is contrasting them in by client type like a client as client and gadget as the client. And furthermore, doing an examination of contrasting of in advance distributed writing. this paper starts with complete cryptanalysis of the benefits of public key-based cryptography contrasted with symmetric key-based cryptography. Truth be told, the benefits generally descend on the insurance against a semi-confined TTP or the evasion of one older sibling in the framework. To completely take advantage of that benefit, both client and server ought to have their own private key, just known without help from anyone else and not imparted to the TTP. a convention ought not to be planned with the plan to have a public key (generally ECC)- based convention, however with the plan to involve it in a savvy way to such an extent that all extra upward (contrasted with more lightweight symmetric key-based other options) is completely persuaded [9]. In this paper, the authors Sourabh Chandra, Smita Paira, Sk Safikul Alam, Goutam Sanyal are first introducing symmetric keys and asymmetric keys and all algorithms of these cryptography keys. From that point forward, the creators are contrasting Hilter kilter key calculations by highlights, benefits, drawbacks, security arrangements. Furthermore, symmetric key calculations by technique, attributes, Advantages, entanglements, execution. Both Symmetric and Asymmetric Key calculations are profoundly productive in getting them moved information over any correspondence medium. They have featured the essential as well as proposed calculations connected with these cryptographic strategies. In Symmetric Key Cryptography, a solitary key is for both encryption and unscrambling purposes. The sharing of this calculation's key turns out to be now and again uncertain. Then again, Asymmetric Key Cryptography utilizes two separate keys to forestall any unscrupulous admittance to the information. The public key lives public to the and the private key isn't imparted to anybody. This procedure guarantees preferable security over the previous [10]. Here in the paper, the authors Fursan Thabit, Sharaf Alhomdy, Abdulrazzaq H.A. Al-Ahdal, Dr. Sudhir Jagtap are proposing a new cryptographic algorithm that is lightweight. The author uses 128 bits block cipher and 128 bits key for encryption. They are dividing 128 bits blocks into 16 bits blocks after this they start encrypting the blocks. They have also compared this algorithm with algorithms like AES, DES, 3DES, LED, and many more. In the paper, another lightweight cryptographic calculation has been proposed. It is known as a New Lightweight Cryptographic Algorithm (NLCA) for expanding information security in a distributed computing climate. It scrambles and unscrambles information in view of symmetric cryptography. The calculation is utilizing a 16 bytes (128-bit) block code and 16 bytes (128-digit) key to encode and decode the information. The calculation is utilized for straightforward and incredibly secure encryption-unscrambling of information. It is propelled by Feistel and SP structural techniques to upgrade the intricacy of encryption. The proposed calculation has likewise been contrasted and the presentation of a few regularly utilized cryptographic calculations to be specific DES, AES, HIGHT, Blowfish, LED which are utilizing different boundaries that are block size, key length, conceivable key, numerical tasks, figure type, and security power [11].

***OVERVIEW: -***

A WPAN means wireless personal area network, which is designed for portable and mobile computing devices. Bluetooth technology is one of them. Bluetooth is a fascinating technology that uses in daily life. We can say this because when you play video or music on your wireless headphone or transmit those files to another device your device transmits around a million 0s and 1s to your headphones or other devices every second using Bluetooth. Bluetooth is license-free and used in the world usually and it uses a 2.4 GHz frequency-hopping spread spectrum. It is used for data transmission and can transmit voice. Bluetooth uses three kinds of security pairing processes. One is SSP (Secure Simple pairing), the second is LMP (Link Manager Protocol) also known as PIN-code based, and the third is None standard pairing. The SSP uses a very complex mechanism, which is known as elliptic curve cryptography. LMP establishes links between two Bluetooth devices and maintains the links for communication. LMP's main function is authentication, encryption, and negotiation of packet size. In the past many technologies are being found, modified, and is secured by developers, as we know whenever new technology comes same old technology will be forgotten, this same thing happens with Bluetooth technology. For the last few years, many people are neglecting the security of Bluetooth or we can say Bluetooth security. However, neglecting Bluetooth security can be a risk at the same time. For example, people forgot to turn off their Bluetooth the attacker can do an impersonation attack them, in impersonation attack attacker act like a previous paired person and steal statistics or can dispatch the virus to the victim's device and that can be very dangerous for victim's data. Not just that there are many more attacks on Bluetooth pairing such as method confusion attacks, etc.

To secure any type of data we need cryptography. Cryptography is very important because it allows us to securely protect data that we want to hide from others. There are three types of encoding algorithms in cryptography. Symmetric-key Encryption-Decryption algorithm is designated secret-key Encryption-Decryption. In this Encryption-Decryption algorithm, Encode and Decode will use the same key. Asymmetric key Encryption-Decryption is designated public key Encryption-Decryption algorithm. In this Encryption-Decryption algorithm, Encode and decoding will happen with different keys. And third hybrid key Encryption-Decryption algorithm is a mixture of symmetric key Encryption-Decryption algorithm and asymmetric key Encryption-Decryption algorithm.

***LIMITATIONS OF THE EXISTING SYSTEM: -***

In the past many technologies are being found, modified, and is secured by developers, as we know whenever new technology comes same old technology will be forgotten, this same thing happens with Bluetooth technology. For the last few years, many people are neglecting the security of Bluetooth or we can say Bluetooth security. However, neglecting Bluetooth security can be a risk at the same time. For example, people forgot to turn off their Bluetooth the attacker can do an impersonation attack them, in pantomime assault assailants behave like a past matched individual and take data or can advance the infection to the casualty's gadget and that can be extremely risky for casualty's information. Not just that there are many more attacks on Bluetooth pairing such as method confusion attacks, etc.

***PROPOSED SYSTEM: -***

We are proposing a new cryptographic algorithm for encoding in Bluetooth data transmission. Along with a cryptographic algorithm, we are adding authentication. Over here, we are trying to implement new algorithms for encoding and decoding. This algorithm will use the same key for encoding and decoding. We are as sender turns on Bluetooth, will select a receiver, after selection the system will generate a one-time password, the receiver will enter that on-time password into their device after that sender and receiver will be connected. For the transmission, the sender will write a message/ select file, according to that another password will generate by a system for encoding, the receiver will enter this password for decoding the massage or file and this is how the transaction will be done by the System.

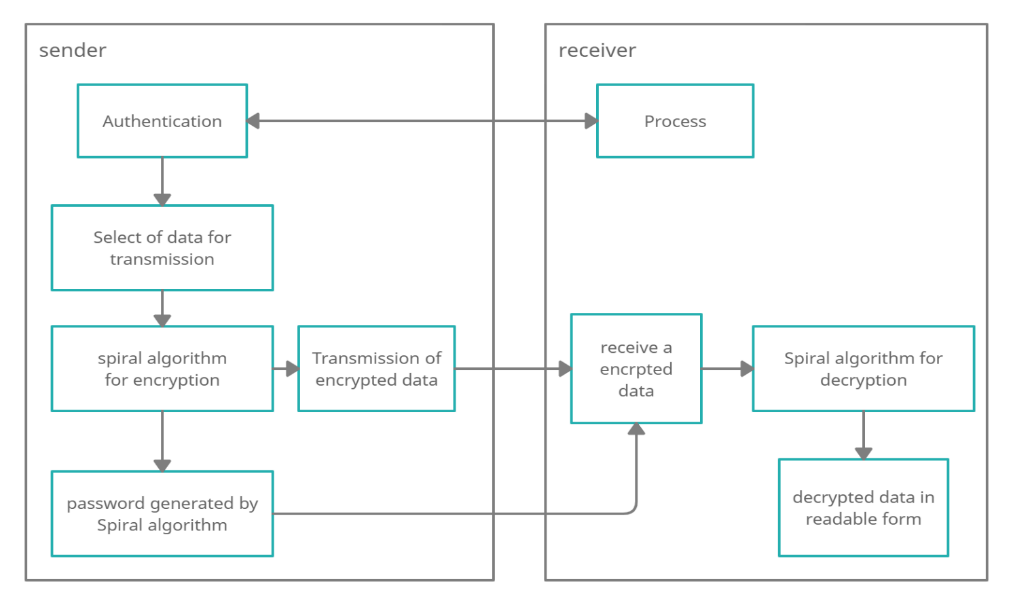
****

Figure 1: Proposed System Architecture

this system model sender will do authentication of the Receiver first then the sender will select the data which the receiver wants to receive and do encryption with key. Now sander’s system will sand encrypted data and key to the receiver. The receiver will receive that encrypted data and store it in a temporary space along with the key. Now receiver will enter the key and the receiver’s system will verify the key and start doing decryption of encrypted data with the key. After decryption, the receiver’s system will store that data permanently.

***AUTHENTICATE BLUETOOTH DEVICE: -***

Both the sender and the receiver will start their Bluetooth devices for authentication. First, the receivers Bluetooth device will sand request to the senders Bluetooth device for authenticate itself. the senders Bluetooth device will generate password which will generate whenever the senders Bluetooth device will start its process. After that, the senders Bluetooth password. Where the receivers Bluetooth device will enter that password and tries to verify itself to the senders Bluetooth device. If the entered password is current, then the authentication is done. If not, then the receivers Bluetooth device will get message that entered password is incorrect.

***CONNECTING OF BLUETOOTH DEVICE: -***

Above mentioned process is continued here. the senders Bluetooth device is going to connect with the receivers Bluetooth device if the senders Bluetooth device is authenticating the receivers Bluetooth device and the authentication is verified successfully.

***ENCRYPTION WITH NEW ALGORITHM: -***

The selected data is going to be encrypted with help of new algorithm. In the algorithm, first we will replace a space with string which is XdX from that selected data. Here, we have selected XdX because XdX cannot occurred in normal data so. we are converting each and every character in number form here we have use ascii value of each character as number. For separate that ascii value from each other we are using any random character after each ascii value. Then the converted number will set in a matrix into spiral from first down then left to right then up then right to left. Then each and every position value will be converted to ascii value again and we will do addition of that ascii value and their row and columns value respectively then store it into same position. Now, collect data row wise with any random character after each ascii value. This will be our encrypted data. As par row and column of matrix we will generate decryption key for each and every encrypted data.

***SEND AN ENCRYPTED DATA TO THE RECEIVER SIDE: -***

After establishment of the connection of the senders Bluetooth device and the receivers Bluetooth devices. We have selected the data to be transfer and then we have done encryption of that selected data. Now, we have encrypted data to be send and we will start sending encrypted data to receivers Bluetooth device and receiver side will receive it and store encrypted data in temporary space. Along will encrypted data we will send key to decrypt that encrypted data.

***DECRYPTION WITH NEW ALGORITHM: -***

After receiving encrypted data and store it in temporary space we will start decrypting the encrypted data. In the decryption part, receiver will enter key for decryption. Now algorithm will verify the entered key with key received from sender’s side. If the entered key and received key are same then algorithm will start decryption. As we have seen that the key generated from row and columns by key, we can determine row and columns value and form matrix from them. Now, after removing random character from encrypted data and adding that encrypted data in array or list. We will set that array or list elements in matrix row wire as we have retrieved data from matrix at encryption time. After setting up encrypted data, we will subtract each and every value with their row and columns value respectively and store it into same position again. And we will separate those value with random character. After that we will retrieve data form matrix in spiral from first down then left to right then up then right to left and store it into single string. Now, we will remove character and add the number value into array or list and convert those ascii number into characters. We will do same process twice. Here our decryption part is over after that whatever character will left is encrypted data or we can say data which sender has sent to us. after decryption process is completed, we have got our encrypted data in decrypted from we will save that data.

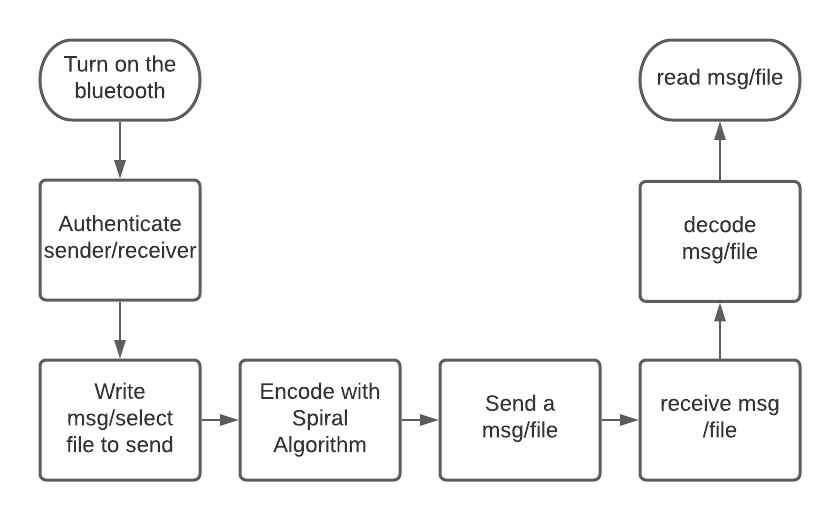


Figure 2: Flow-chart Diagram

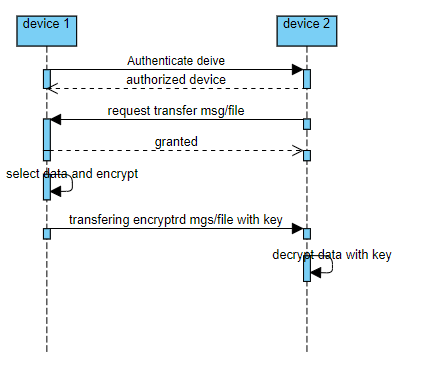


Figure 3: Sequence Diagram

|  |  |
| --- | --- |
|  | *Algorithm: sender side* |
| 1 | Spiralencode(msg) |
| 2 | { |
| 3 | Encry = “” |
| 4 | For j in msg |
| 5 | Encry = Encry + ASCII value (j) + random char |
| 6 | L <- Length of Encry |
| 7 | Arr1[] <- Fectors of L |
| 8 | Do { |
| 9 | Random(row) of factors |
| 10 | } while (row ==0 | row ==1| row ==L) |
| 11 | Column <- L/row |
| 12 | Matrix (row, Column) |
| 13 | t<-0, b <- rows – 1, lt <- 0, rt<- columns – 1, index <-0 |
| 14 | while(true) |
| 15 | If(t>b) |
| 16 | Break |
| 17 | for loop (t to b) |
| 18 | add row and column into element of msg and add in to matrix column t to b |
| 19 | index ++ |
| 20 | ++lt |
| 21 | If (lt > rt) |
| 22 | Break |
| 23 | for loop (lt to rt+1) |
| 24 | add row and column into element of msg and add in to matrix row lt to rt |
| 25 | index ++ |
| 26 | --b |
| 27 | If(t>b) |
| 28 | Break |
| 29 | For loop (b to t-1) |
| 30 | add row and column into element of msg and add in to matrix column b to t |
| 31 | index ++ |
| 32 | --rt |
| 33 | If (lt > rt) |
| 34 | Break |
| 35 | for loop (rt to lt-1) |
| 36 | add row and column into element of msg and add in to matrix row rt to lt |
| 37 | index ++ |
| 38 | ++t |
| 39 | For i (0 to row) |
| 40 | for j (0 to column) |
| 41 | encode <- encode + matrix [i][j] + random char |
| 42 | Return (encode + row + three random chars + column) |
| 43 | } |

|  |  |
| --- | --- |
|  | *Algorithm: receiver side* |
| 1 | Spiraldecode(encode) |
| 2 | { |
| 3 | L <- Length of encode |
| 4 | K <- 0 |
| 5 | Row and col <- enter |
| 6 | Matrix (row, Column) |
| 7 | For I in encode |
| 8 | If i is digit |
| 9 | K0 = K0 + i |
| 10 | Else |
| 11 | K0 =K0+ empty string |
| 12 | L = split the K0 |
| 13 | For i (0 to row) |
| 14 | for j (0 to column) |
| 15 | matrix [i][j] <- kth position element of L |
| 16 | k++ |
| 17 | t<-0, b <- rows – 1, lt <- 0, rt<- columns – 1, index <-0, |
| 18 | str <- “” |
| 19 | While(true) |
| 20 | If(t>b) |
| 21 | Break |
| 22 | for I (t to b) |
| 23 | subtract of row and column from matrix[i][lt] after that concatenation str and matrix [i][lt] |
| 24 | index ++ |
| 25 | ++lt |
| 26 | If (lt > rt) |
| 27 | Break |
| 28 | for i lt to rt+1 |
| 29 | subtract of row and column from matrix[b][i] after that concatenation str and matrix[b][i] |
| 30 | index ++ |
| 31 | --b |
| 32 | If (t>b) |
| 33 | Break |
| 34 | for I (b to t-1) |
| 35 | subtract of row and column from matrix[i][rt] after that concatenation str and matrix[i][rt] |
| 36 | index ++ |
| 37 | ++rt |
| 38 | If (lt > rt) |
| 39 | Break |
| 40 | for i (rt to lt-1) |
| 41 | subtract of row and column from matrix[t][i] after that concatenation str and matrix [t][i] |
| 42 | index ++ |
| 43 | ++t |
| 44 | For I in str |
| 45 | If I is digit |
| 46 | K1 = K1 + I |
| 47 | Else |
| 48 | K1 =K1+ empty string |
| 49 | L = split the K1 |
| 50 | For i in L |
| 51 | Sd = Sd + convert ASCII to chars (i) |
| 52 | For i in Sd |
| 53 | If i is digit |
| 54 | K2 = K2 + i |
| 55 | Else |
| 56 | K2 =K2+ empty string |
| 57 | L2 = split the K2 |
| 58 | For i in L2 |
| 59 | String2 = String2 + convert ASCII to chars (i) |
| 60 | Return String2 |
| 61 | } |

***RESULT: -***

Many algorithms have been introduced for encryption and decryption in past times. With this algorithm Bluetooth device and our data will be safe. There is no such algorithm which get complex with length of data. This algorithm is first converting each data in ASCII value then set them up and then again convert that data into ASCII value so algorithm would do Encryption of the given data. None of the past introduced algorithm are capable of such things. This algorithm also increases length of data after encryption of the data which is giving boost to hiding data. So, transferring data will be very secure Using Bluetooth without warring about attacker or impersonator.

If we are do encryption of “he”

First, we convert hello in number format here we are using ASCII value

So ‘h’s ASCII value is 104 and random character is ‘U’,

‘e’s ASCII value is 101 and random character is ‘g’,

so now data will be

104U101g

And suppose random generated matrix is 4 X 2 means 4 row and 2 columns

Now set them in spiral format

1 g

0 1

4 0

U 1

Now

Covert character int ASCII again and set them in their respective position

‘1’s ASCII value is 49 and random character is ‘y’, position is (0,0)

‘g’s ASCII value is 103 and random character is ‘e’, position is (0,1)

‘0’s ASCII value is 48 and random character is ‘x’, position is (1,0)

‘1’s ASCII value is 49 and random character is ‘H’, position is (1,1)

‘4’s ASCII value is 52 and random character is ‘L’, position is (2,0)

‘0’s ASCII value is 48 and random character is ‘x’, position is (2,1)

‘U’s ASCII value is 85 and random character is ‘v’, position is (3,0)

‘1’s ASCII value is 49 and random character is ‘x’, position is (3,1)

Now on position (0,0) instead of 1 we will put 49 + 0 + 0 = 49

position (0,1) instead of ‘g’ we will put 103 + 0 + 1 = 104

position (1,0) instead of ‘0’ we will put 48 + 1 + 0 = 49

position (1,1) instead of ‘1’ we will put 49 + 1 + 1 = 51

position (2,0) instead of ‘4’ we will put 52 + 2 + 0 = 54

position (2,1) instead of ‘0’ we will put 48 + 2 + 1 = 51

position (3,0) instead of ‘U’ we will put 85 + 3 + 0 = 88

position (3,1) instead of ‘1’ we will put 49 + 3 + 1 = 53

49y 104e

49x 51H

54L 51x

88v 53x

So, the Encrypted data will be “49y104e49x51H54L51x88v53x” and generated key will be 4IJT2 for this encryption.

And for decryption

First, we will generate a matrix from key we will consider only numbers in key except them ignore other characters so number s or 4 and 2 so our matrix will be 4 X 2

In the encrypted data we will consider only numbers except them ignore other characters and for separation of the number from the data we will add those number in array. Whenever character occur number before that character is whale element like this, we will separate all numbers.

we will arrange Encrypted data’s array in spiral format in matrix,

49 104

49 51

54 51

88 53

Now on position (0,0) instead of 49 we will put 49 - 0 - 0 = 49 and random character is ‘y’

position (0,1) instead of 104 we will put 104 - 0 - 1 = 103 and random character is ‘c’

position (1,0) instead of 49 we will put 49 - 1 - 0 = 48 and random character is ‘v’

position (1,1) instead of 51 we will put 51 - 1 - 1 = 49 and random character is ‘F’

position (2,0) instead of 54 we will put 54 - 2 - 0 = 52 and random character is ‘K’

position (2,1) instead of 51 we will put 51 - 2 - 1 = 48 and random character is ‘a’

position (3,0) instead of 88 we will put 88 - 3 - 0 = 85 and random character is ‘h’

position (3,1) instead of 53 we will put 53 - 3 - 1 = 49 and random character is ‘E’

“49y103c48v49F52K48a85h49E”

Now, again separate numbers and convert that numbers into character consider numbers as ASCII value and convert into respective characters and ignore character.

104U101g

Repeat above mansion step again

convert that numbers into character consider numbers as ASCII value and convert into respective characters and ignore character.

‘he’ this is decrypted data.

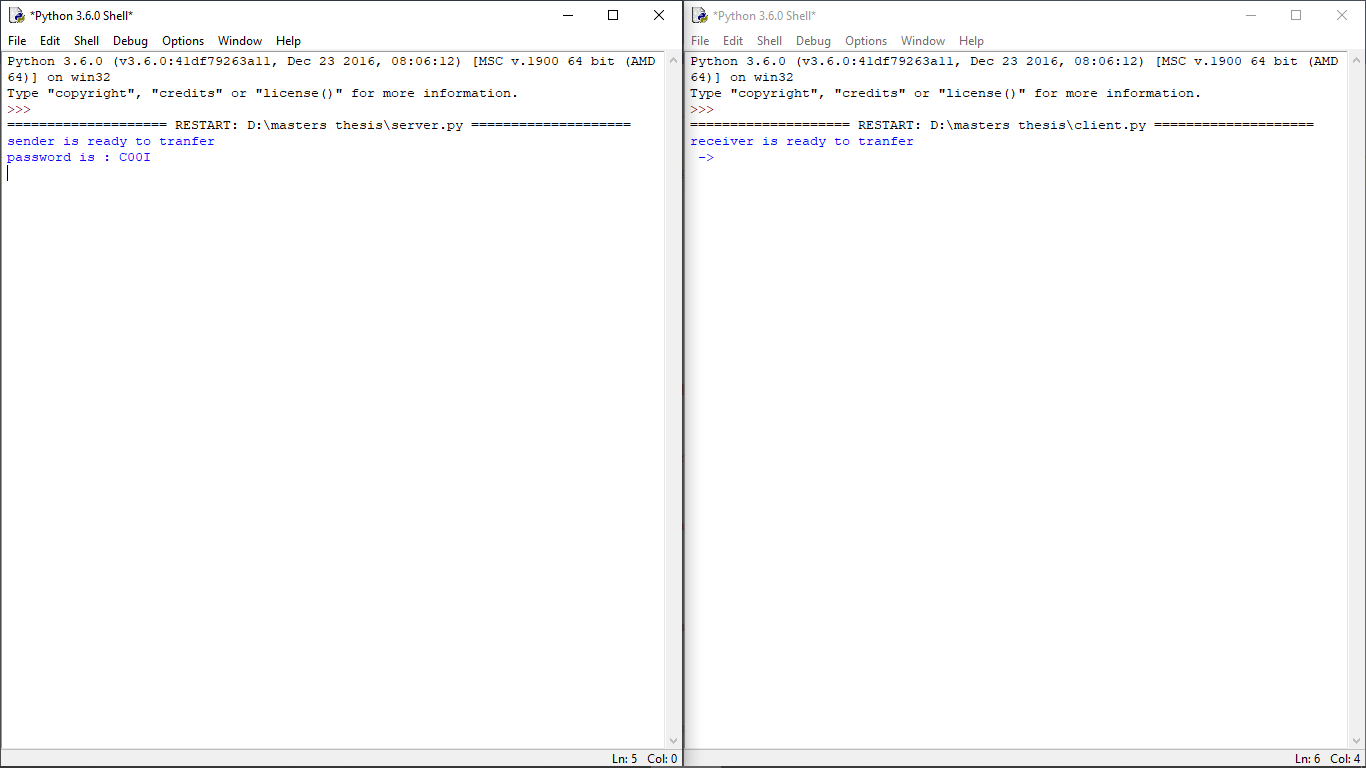


Figure 4: Home page

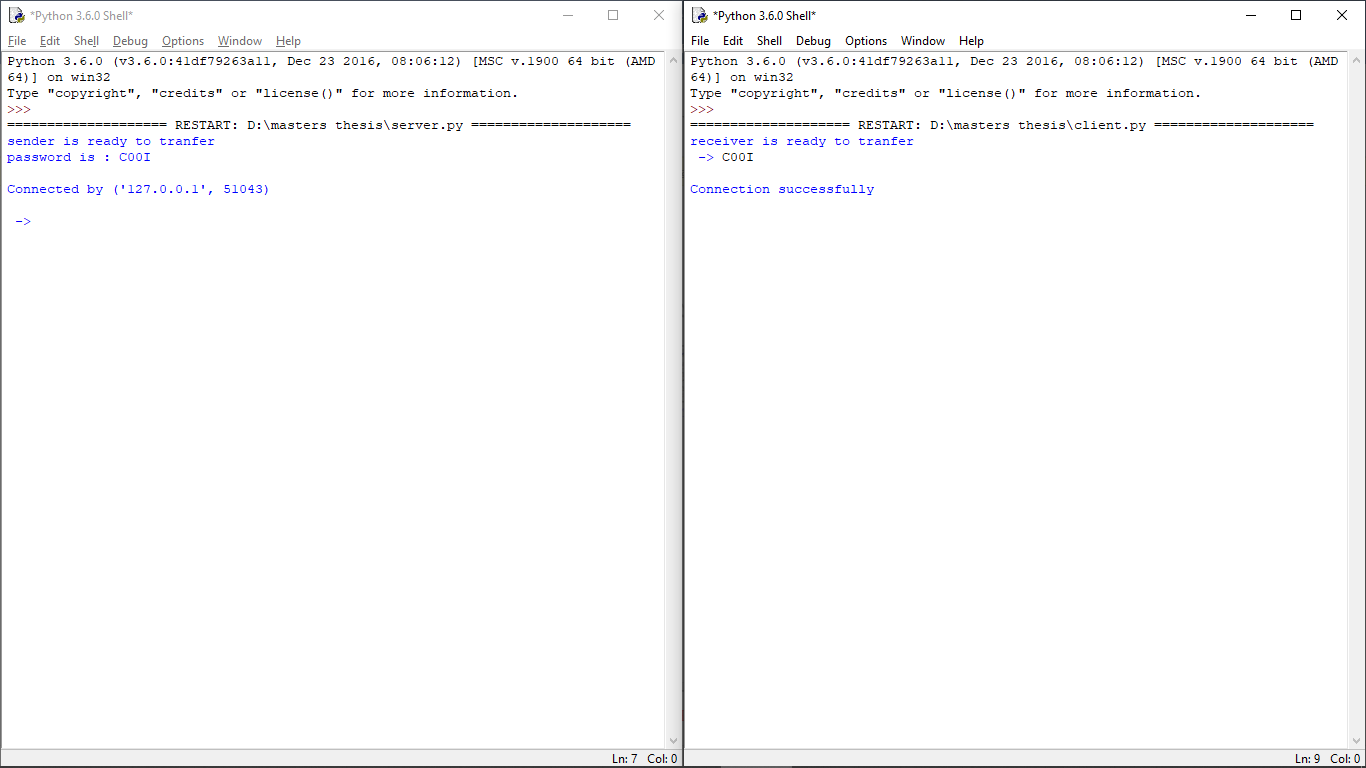


Figure 5: Receiver enters password and Establishment of connection

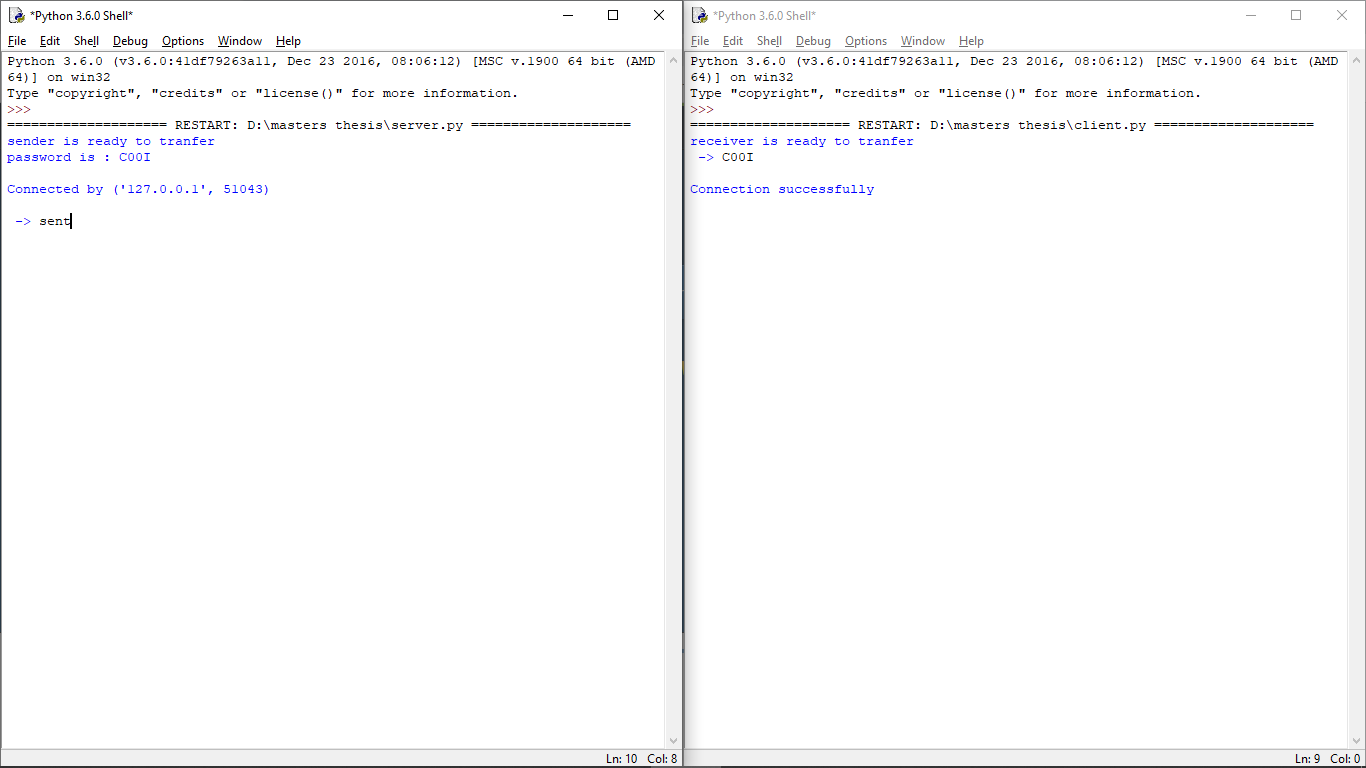


Figure 6: Sender enter sent to a start sending



Figure 7: Senders Encrypted data and key generation



Figure 8: Receivers received encrypted data



Figure 9: Receiver enters key to decrypt the data



Figure 10: Receives get decrypted date

***ANALYSIS: -***

As we know the time complexity and space complexity is very important in any algorithm. We also know that Smaller the time complexity the better the algorithm and same for space complexity Smaller the space complexity the better to use that algorithm. But in this encryption algorithm longer data the more confuse data this algorithm is going on this moto. So along with time complexity this algorithm is very good even better. There is only problem with this algorithm that is space complexity we have compromise space complexity in this algorithm little bit except that algorithm is very good. In this brute force attack is worthless because of randomness of algorithm. with this algorithm many attacks are useless on Bluetooth device. We can avoid been attack by attacker and impersonator. Below we have present same of the graph of comparison of AES-128, Playfair cipher, new algorithm, and Caesar cipher. Comparison of length of key used in that algorithms and length of encrypted data. We have used “new cryptographic algorithm” for data in all algorithms. only key value of been change for AES128 we are using “1234567890ABCDEF”, Playfair cipher we are using “Gravity Falls”, new algorithm we are using “4HXV29”, Caesar cipher we are using “3” as key.

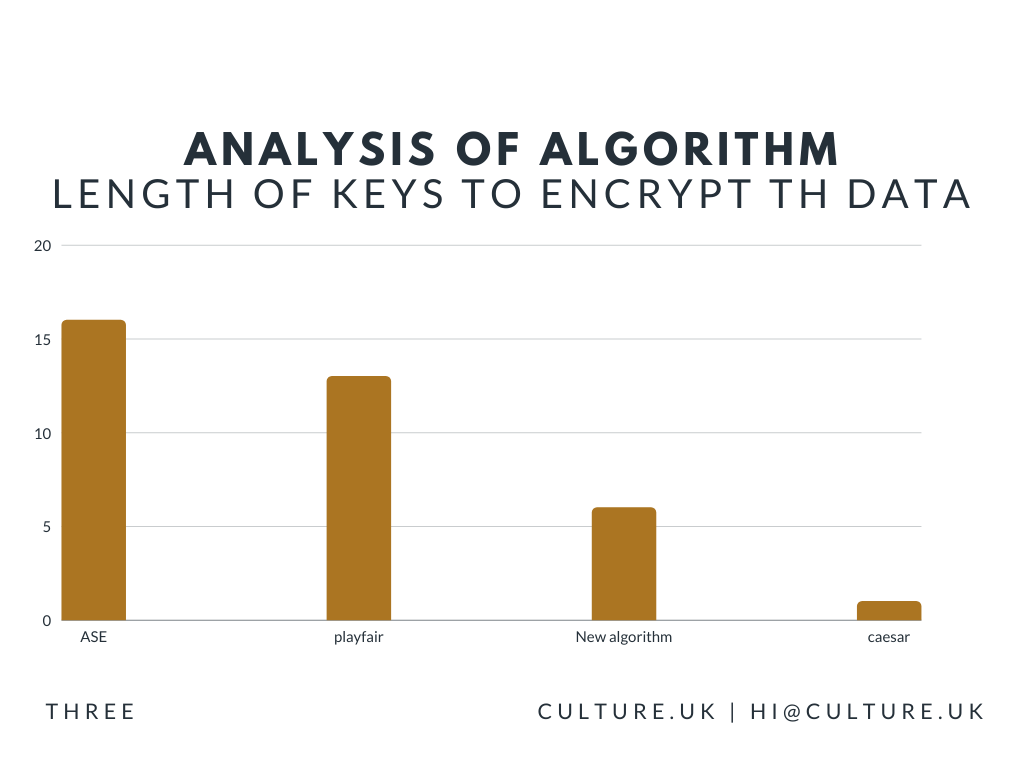


Figure 11: comparison of length of keys

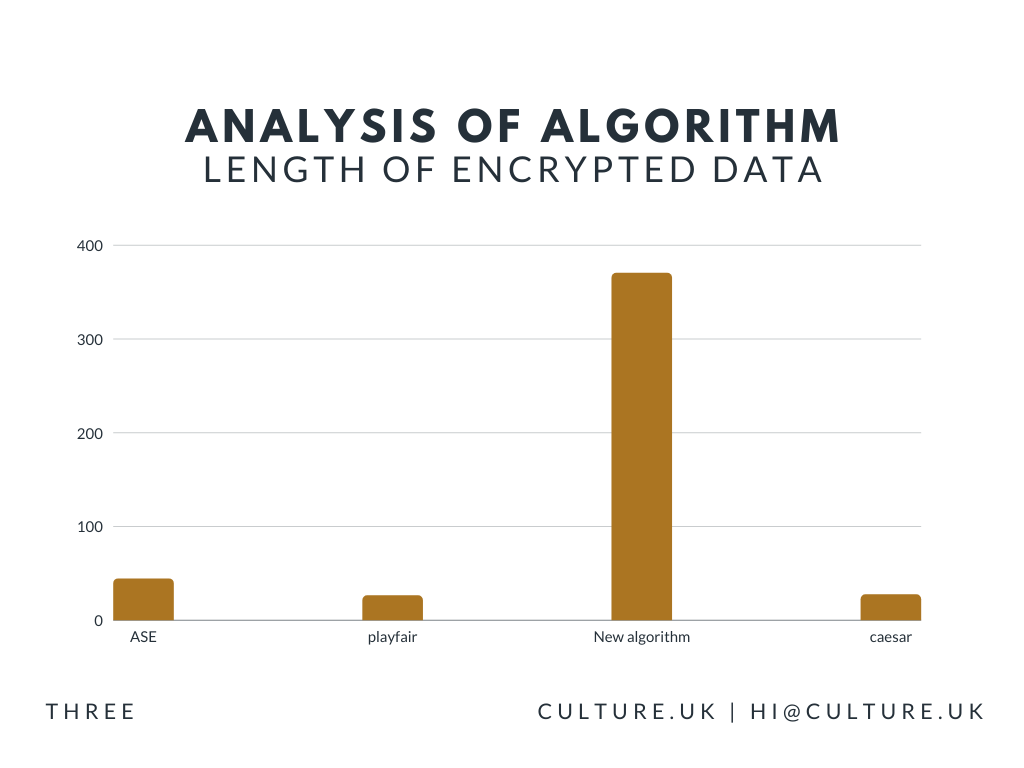


Figure 12: comparison of length of Encrypted data

***CONCLUSION: -***

For a short-range data transmission and data receiving we are using Wi-Fi, Bluetooth, and many other technologies. Same time, people don’t consider them as risk. Many people, after trans receiving won’t turn off that technology that can be very risk for peoples. Most likely people don’t turn off their Bluetooth device. That where attacker start their work to steal data form victim’s device. Here, we have fund solution for that. We have found an algorithm specially for transmitting and receiving of data. With this project, victim’s device won’t sand data without victim’s acknowledgement so attacker can’t steal data. This algorithm is also had good accuracy. The algorithm will help us to security data of our device.

***REFERENCES: -***

[1] Peter Cope, Joseph Campbell, Thaier Hayajneh, “An Investigation of Bluetooth Security Vulnerabilities”, 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), **DOI:**10.1109/CCWC.2017.7868416

[2] Shaikh Shahriar Hassan, Soumik Das Bibon, Md Shohrab Hossain, Mohammed Atiquzzaman, "Security threats in Bluetooth technology", Elsevier Computers & Security 74 (2018) 308–322, https:/doi.org/10.1016/j.cose.2017.03.008

[3] Maximilian von Tschirschnitz, Ludwig Peuckert, Fabian Franzen, and Jens Grossklags, “Method confusion Attack on Bluetooth pairing”, 2021 IEEE Symposium on Security and Privacy (SP), **DOI:**10.1109/SP40001.2021.00013

[4] A.S.Diallo, Wajdi Fawzi M. Al-Khateeb, R.F. Olanrewaju, [F. Sado](https://ieeexplore.ieee.org/author/37085338087), “A secure Authentication scheme for Bluetooth connection”, 2014 IEEE International Conference on Computer and Communication Engineering, **DOI:** 10.1109/ICCCE.2014.29

[5] [Da-Zhi Sun](https://link.springer.com/article/10.1007/s00779-017-1081-6#auth-Da_Zhi-Sun), [Yi Mu](https://link.springer.com/article/10.1007/s00779-017-1081-6#auth-Yi-Mu), Willy Susilo, "Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard V5.0 and its countermeasure”, Springer Link Personal and Ubiquitous Computing volume 22, pages 55–67 (2018), https:/link.springer.com/article/10.1007/s00779-017-1081-6

[6] Samta Gajbhiye, Sanjeev Karmakar, Monisha Sharma, Sanjay Sharma, “Bluetooth Secure Simple Pairing with enhanced security level ”, Journal of Information Security and Applications Volume 44, February 2019, Pages 170-183, https:/doi.org/10.1016/j.jisa.2018.11.009

[7] [Daniele Antonioli](https://ieeexplore.ieee.org/author/37072641000), [Nils Ole Tippenhauer](https://ieeexplore.ieee.org/author/37546904700), [Kasper Rasmussen](https://ieeexplore.ieee.org/author/37969691300), “BIAS: Bluetooth Impersonation AttackS”, 2020 IEEE Symposium on Security and Privacy (SP), **DOI:**10.1109/SP40000.2020.00093

[8] Moneer Fakroona, Fayez Gebali, Mohammad Mamun, “Multifactor authentication scheme using physically unclonable functions”, Elsevier [Internet of Things](https://www.sciencedirect.com/science/journal/25426605) Volume 13, March 2021, 100343, [https:/doi.org/10.1016/j.iot.2020.100343](https://doi.org/10.1016/j.iot.2020.100343)

[9] An Braeken, “Public key versus symmetric key cryptography in client-server authentication protocols”, Springer International Journal of Information Security published march 2021, https:/doi.org/10.1007/s10207-021-00543-w

[10] Sourabh Chandra, Smita Paira, Sk Safikul Alam, Goutam Sanyal, “Comparative survey of symmetric and asymmetric key cryptography”, IEEE 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), DOI: [10.1109/ICECCE.2014.7086640](https://doi.org/10.1109/ICECCE.2014.7086640)

[11] Fursan Thabit, Sharaf Alhomdy, Abdulrazzaq H.A. Al-Ahdal,Dr Sudhir Jagtap, “A new lightweight cryptographic algorithm for enhancing data security in cloud computing”, Elsevier Global Transitions Proceedings Volume 2, Issue 1, June 2021, Pages 91-99, https:/doi.org/10.1016/j.gltp.2021.01.013

[12] Samta Gajbhiyea, Sanjeev Karmakarb, Monisha Sharmac, Sanjay Sharma, “Two-party secure connection in Bluetooth-enabled devices”, information security journal: a global perspective 2018, Volume. 27, NO.1,42–56, https:// doi.org / 10.1080 / 19393555.2018.1423714

[13] Yu Xin, Yan Ting, “A Security Architecture Based on User Authentication of Bluetooth”, 2009 International Forum on Information Technology and Applications, DOI: 10.1109/IFITA.2009.115

[14] Li Juan, Chen Bin, Li Kun “Study on the Improvement of Encryption Algorithm of Bluetooth”, 2009 International Conference on Networking and Digital Society, DOI: 10.1109/ICNDS.2009.28

[15] D.Sharmila, R.Neelaveni, K.Kiruba, “Bluetooth Man-In-The-Middle Attack Based on Secure Simple Pairing using Out Of Band Association model”, INTERNATIONAL CONFERENCE ON “CONTROL, AUTOMATION, COMMUNICATION AND ENERGY CONSERVATION -2009, 4th-6th June 2009, KEC/INCACEC/332

[16] Dr.M.Tanooj kumar, Revanth Kumar Katragadda, Vishnu Srujan Kolli, Shaik Lahir Rahiman, “A Hybrid Approach For Enhancing Security In Internet Of Things (IoT)”, International Conference on Intelligent Sustainable Systems (ICISS 2019) IEEE Xplore Part Number: CFP19M19-ART; ISBN: 978-1-5386-7799-5

[17] https:// www.bluetooth.com / learn-about-bluetooth / key-attributes / Bluetooth-security / reporting-security /

[18] https:// www.globalsign.com / en-in/blog / top-5-bluetooth-security-vulnerabilities

[19] https:// www.webroot.com / in / en / resources / tips-articles / a-review-of-bluetooth-attacks-and-how-to-secure-mobile-workforce-devices