Message sharing through optical communication usingcipher encryption method in python

VenkataSubramanian S[1]VishweshVaideeswaran S[2] and Dr. M. Devaraju[3]

[1]Department of Electronic and Communication Engineering, Easwari Engineering College, Ramapuram, Chennai-600089

[2] Department of Electronic and Communication Engineering, Easwari Engineering College, Ramapuram, Chennai-600089

[3]Professor, Head of Department of ECE, Easwari Engineering college, Ramapuram, Chennai-600089

[1]venkatsriram1103@gmail.com[2]vishweshsrinivasan@gmail.com[3]hod.ece@eec.srmrmp.edu.in

Abstract. The project currently exists based on optical communication in addition to how all of us use it to transfer encrypted messages in the form of light in addition to decrypt the same. In the encryption part all of us use cipher EXOR encryption method. This object over here currently exists mainly used to prevent leakage of data that object over there all of us currently are sending. This object over here method requires a key at both ends in order to encrypt in addition to decrypt the message. Here all of us use led to transmit the encrypted message in addition to with the help of LDR all of us get the message in the receiver end in addition to decrypt it. All of us discovered that object over there in optical communication the data transmission currently am able to exists done through both wired medium in addition to wireless medium. From our results all of us currently am able to say that object over there the rate at which the transmission currently exists done currently exists high. This object over here currently am able to exists used by the military during war to communicate with each other.

Keywords: Ciphering, Optical Communication, Encryption, Decryption, XOR, LED, LDR

1Introduction

1.1 History of Encryption

Cryptography, began thousands of years ago currently exists a method to protect valuable secrets via codes in addition to ciphers. Classic cryptography currently exists the method of encoding the secret via pen in addition to paper or through mechanical aids. Earlier in the 20th century the enigma rotor machine used to exist introduced. This object over here rotor machine provided a faster method to encrypt the data provided. The success of the enigma rotor machine led a way for computers in addition to physical science to play a bigger role in producing bigger quality schemes that object over there currently exists no match for pen in addition to paper methods. The main aim of the government in the 60s was to perform secure cryptography. The creation of public encoding commonplace and the creation of public- key cryptography were two such events that changed the course of cryptography and brought it into public domain.

The wall from the kingdom of Egypt engraved with non-standard hieroglyphs in the 1900 B.C. used to exist the earliest cryptography that object over there used to exist notable. These possessed mystery, intrigue, or even amusement for literate onlookers rather that object over there it being secret communications.

Mlecchitavikalpa a sanskrit literature which used to exist also meant to exists a secret way to communicate between lovers used to exist documented in Asian country around four hundred B.C. to two hundred ad. Cipher script used to exist used throughout to write the components of the Egyptian demotic Greek witching papyri.

The ancient Greeks square measure aforesaid to possess notable of ciphers. The spartan military used the scytale transposition cipher however it used to exist not notable on whether it used to exist for authentication, avoiding omen or encoding. The secret messages physically hid at just as a tattoo on a slave's head hid by regrown hair or a lower place wax on wood tablets, currently are not proper samples of cryptography in addition to once known, currently exists directly readable. Such type of cryptography currently exists coined by the term stenography.

In earlier times encryption used to exist achieved by having a key to write in code in addition to to decrypt. These messages at whatever place then converted to digital gibberish by the key through encoding in addition to were converted rear to their primary type through deciphering. In general, it used to exist tough to crack a code with longer key. This object over here currently exists true just as all of us would need wrongdoer to attain each key while deciphering an encrypted message by brutal force. Every binary information currently exists either or price zero or one. For example, 256 or 2^8 would exists the attainable keys for an 8-bit key in addition to 2^56 or seventy two quadrillion for a 56-bit key. With the rise in various fashionable technology, the victimization keys used for cipher with larger in addition to shorter lengths currently are becoming easy to decipher. However just as there currently exists constant advancement in the technology the quality of encoding has also advanced equally. The introduction of the uneven key cipher used to exist the notable advancement in the study of cryptography since world war ii. For encoding identical messages the square measure algorithm used two mathematically connected keys. It used to exist difficult to find the alternative key even though the algorithms allows publication of one of the two keys.

The use of the internet for commercial purposes, just as well just as the implementation of commercial transactions over the internet, necessitated the creation of a widely accepted encryption standard around 1990. Prior to the implementation of the advanced encryption standard (aes), financial data sent over the internet used to exist encrypted if at every single one, most commonly using the data encryption standard (des). After a public call for in addition to competition among candidates for such a cypher algorithm, nbs (a us government agency) approved it for defense. Owing to complicated wrangles over the use of high-quality encryption by the general public, des used to exist accepted for a short time however saw prolonged use. After another public competition organized by the nbs successor organization, nist, the des used to exist eventually replaced by the aes. In the late 1990s in addition to early 2000s, public-key algorithms became a more common method of encryption, in addition to a combination of the two became the most widely accepted method for e-commerce transactions. Furthermore, the creation of a new protocol known just as the secure socket layer, or ssl, paved the way for online transactions. Ssl used to exist used in a variety of transactions, from buying goods to paying bills online in addition to banking. Furthermore, just as household wireless internet connections became more widespread, the need for encryption increased just as a degree of protection used to exist required in these everyday situations.

1.2 Communication via Light:

In ancient times, the fire in addition to smoke played a major role in methods of communicating for long distance. The success of an empire in war or alerting the citizens of an empire during warzone were usually done by coloured flames burnt at the higher pillar of the country. Another ancient method of using smoke currently exists the sos warning of the shipwrecks from an island currently am able to exists easy for the recovery team to identify the location of shipwrecks. Then developed the heliograph system of communication. In this object over here method the light currently exists flashed according to the morse code of the corresponding message. At the receiver end, the flashing of light currently exists recorded in addition to then the original message currently exists recovered. The morse code for heliograph contains flash (-) in addition to off (.). For the longer duration of dit or dash the light remains in flash state or off state for corresponding durations.

At current all of us currently are using optical communication for the internet connections to attain high speed of data transmission of up to the range of gbps. The undersea cables covers over 27000 kilometres with over 120000 voice channels along with them. These cables currently are mainly based on the principle of “total internal reflection”. The fibre consists of two parts majorly the core in addition to the cladding. Based on the difference in the reflective index, the light ray currently exists transmitted through the cable. The fibres currently are usually glass or plastic fibre.

Major network providers of the world uses the optical communication channels underground for the voice in addition to data channels for undersea communication between countries. These currently are further sent to their respective exchange servers of the country.

From the exchange, based on the desired options of the users, the transmission is done using the optical fibre or the conducting transmission lines to the user. Here the data→electronic bits→light medium→electrical signals→data.

Though we use wireless antennas for the data transmission, the basic requirement for them is optical communication. In this transmitter data→electronic bits→light→RF waves→Data.

Now we are trying to operate the optical communication using the cable less networking methods and try to reduce the cost of implementing the optical fibres for long distance.

2 METHOD

In the transmitter block, the first messages currently are split into individual characters in addition to to their corresponding ascii value. Then the ascii in decimal format currently exists converted to the binary numeration system. The private key's given just as user input within the decimal format which currently are converted to binary digits in addition to logical exor function currently exists performed in addition to therefore the encrypted message currently exists reversed in addition to stored during a list in addition to transmitted through light medium.

In the receiver block, the encrypted messages currently are received using the optical receiver section in addition to extracted. The user then enters the private key to urge the first message. The logical exor operation currently exists performed again so just as to decrypt the original message.

2.1Encryption using EXOR ciphering:

Xor cipher currently exists the easiest method of implementing which uses the logical exor operation between the message bits in addition to the key bits to provide protection against the attack of intruders.

At present, all of us currently are using many electronic devices to share our data from the transmitting end to the receiver. To avoid the breaching of communication, some protective methods have to exists implemented to ensure the data security.

In xor ciphering encryption, first the message currently exists obtained from the user in addition to a user desired key currently exists also got just as input from the user. Then the logical exor operation currently exists performed in between the binary forms of the message in addition to the key. Hence even there occurs any breach, the intruders cannot exists able to understand the message without the key.

For the Decryption same key must be used to decrypt and recover the original message. Hence it is known as Symmetric encryption method.

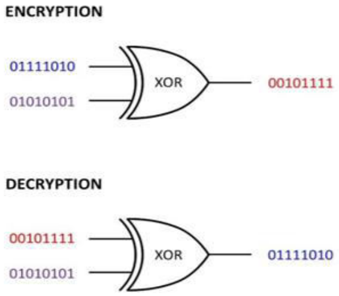


Figure 1: Encryption and Decryption using XOR

2.2 Light Fidelity

Li-fi currently exists transmission of knowledge through illumination by taking the fiber out of fiber optics by sending data through a led light bulb that object over there varies in intensity faster than the human eye currently am able to follow. Li-fi currently exists that object over there the term some have won't to label the fast in addition to cheap wireless- communication system, which currently exists that object over there the optical version of wi-fi. At the guts of this object over here technology may exists a new generation of high brightness light-emitting diodes. If the led currently exists on, the reader transmit a digital 1, if it's off the reader transmit a 0. they will exists switched on in addition to off tremendously quickly, which provides nice opportunities for transmitted data. it currently is possible to encode data within the light by varying the speed at which the leds flicker on in addition to off to offer different strings of 1s in addition to 0s. The led intensity currently exists modulated so rapidly that object over there human eye cannot notice, therefore the output appears constant.

The binary data transmitted during encryption after cipher xor method currently exists shipped to the led through the arduino board. The led activates when the code currently exists 1 in addition to turns off when the code transmitted currently exists 0. The led flicker varies with the info rate of the encryption. The intensity also varies with the encompassing during which all of us transmit the message (fig 2). This object over here light currently exists captured in addition to therefore the receiver gets the binary bits to exists decoded.

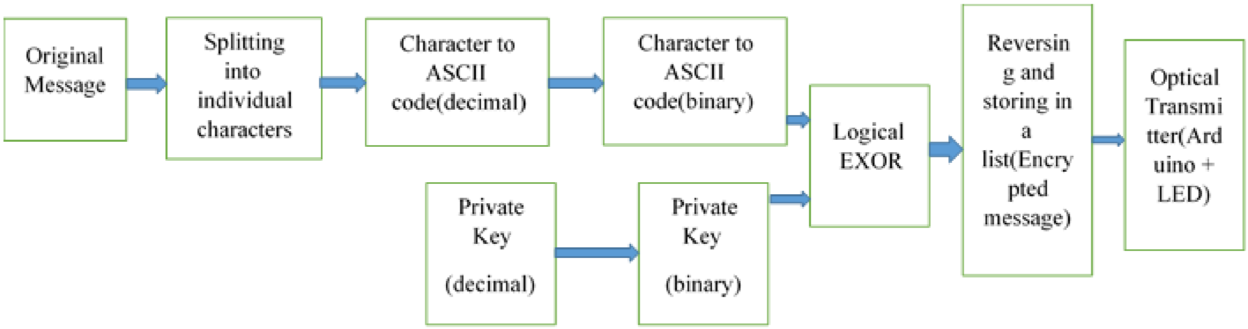

Original Message
Splitting into individual characters
Character to ASCII code(decimal)
Character to ASCII code(binary)
Private Key (decimal)
Private Key (binary)
Logical EXOR
Reversing and storing in a list(Encrypted message)
Optical Transmitter(Arduino + LED)

Figure 2: Transmitter Block

The receiver ***(fig 3)*** uses an equivalent XOR method to decrypt the message. When the receiver provides an equivalent private key that was used while transmitting the information, he/she will get the decrypted message in binary form. Then these bits are again converted to the corresponding decimal value and these decimal values are then converted to corresponding ASCII value.

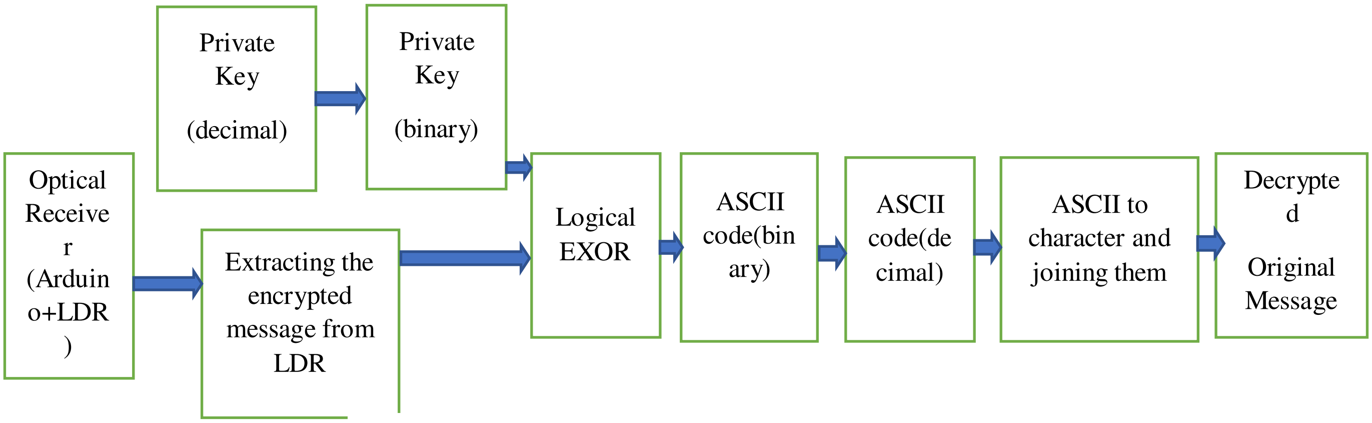
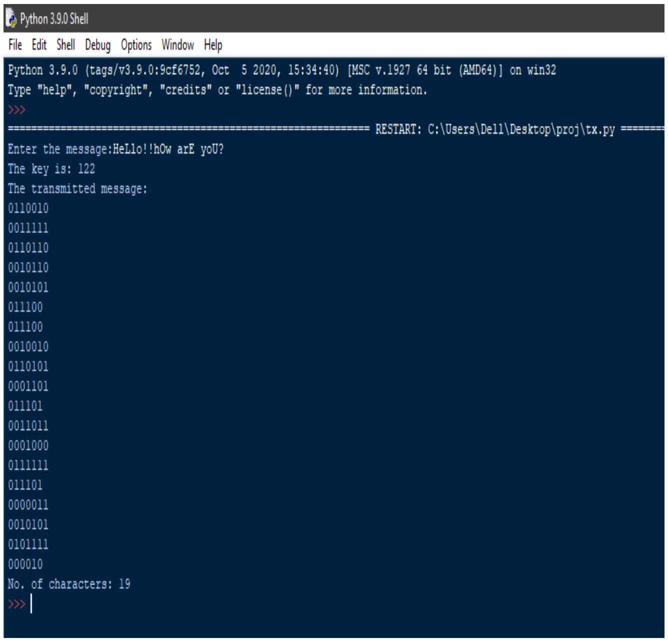

Private Key (decimal)
Private Key (binary)
Optical Receiver (Arduino+LDR)
Extracting the encrypted message from LDR
Logical EXOR
ASCII code(binary)
ASCII code(decimal)
ASCII to character and joining them
Decrypted Original Message

Figure 3: Receiver Block

3 RESULT

In fig 4 given below we have transmitted a random message **"HeLlo!!hOwarEyoU?"**. Then we provide a particular key to encrypt the message using XOR cipher method. The message transmitted gets converted into binary numbers for each character that are provided as input from the user.

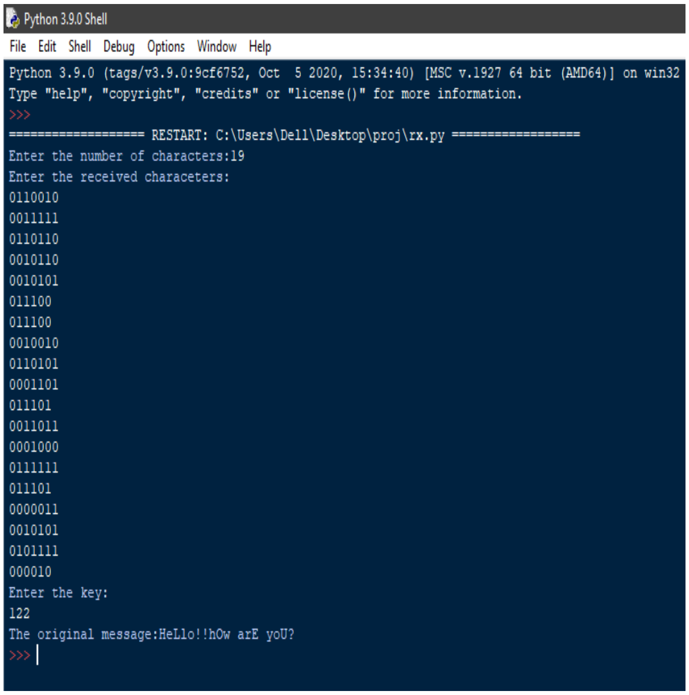
These characters are then transmitted through an optical medium to the receiver where the receiver will get zeros and ones through the light intensity that is captured by the sensor at the receiver's end. When the transmitted bit is 0 the LED at the receiver's end switched off and when the bit transferred is one then the LED switches on.



```
Python 3.9.0 (tags/v3.9.0:9cf6752, Oct  5 2020, 15:34:40) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
============================================================ RESTART: C:\Users\Dell\Desktop\proj\tx.py =======
Enter the message:HeLlo!!hOw arE yoU?
The key is: 122
The transmitted message:
0110010
0011111
0110110
0010110
0010101
011100
011100
0010010
0110101
0001101
011101
0011011
0001000
0111111
011101
0000011
0010101
0101111
000010
No. of characters: 19
>>> 
```

Figure 4: Encryption and Transmission of data

After all the bits are received by the receiver, he then gives the key that was initially provide while transmitting the message and this will then decrypt the message that was initially sent by the transmitter.



```
Python 3.9.0 (tags/v3.9.0:9cf6752, Oct  5 2020, 15:34:40) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
=================== RESTART: C:\Users\Dell\Desktop\proj\rx.py ==================
Enter the number of characters:19
Enter the received characeters:
0110010
0011111
0110110
0010110
0010101
011100
011100
0010010
0110101
0001101
011101
0011011
0001000
0111111
011101
0000011
0010101
0101111
000010
Enter the key:
122
The original message:HeLlo!!hOw arE yoU?
>>> 
```

Figure 5: Receiving and Decryption of data

4 CONCLUSION

In this object over here paper an improved xor crypto graphical algorithm currently exists proposed, designed in addition to implemented. This object over here tool currently exists going to exists useful for the people to speak during war crises owing to the fact that the message should exists transferred in an encrypted manner in order that object over there the third parties cannot decrypt the code without knowing the key. Although the info sent features a minimal amount of delay thereto, it currently is much secured.

5 REFERENCE

1. Ayushi Sharma, Varun Kumar Kakar, “Security performance and enhancement of physical layer in optical-CDMA with multicode keying encryption”, International Conference on Emerging Trends in Computing and Communication Technologies (ICETCCT), 2017.
2. FaragMousa, Tran The Son, Andrew Burton, Hoa Le Minh,” Investigation of data encryption impact on broadcasting visible light communications”, 9th International Symposium on Communication Systems, Networks & Digital Sign (CSNDSP), 2014.
3. Lim Chong Han & Nor MuzlifahMahyddin,” An implementation of Caesar cipher and XOR encryption technique in a secure wireless communication”, IEEE International Conference on Electronic Design,2014.
4. O. K. Baranovsky, O. Yu. Gorbadey, A. O. Zenevich, “Quantum method of secure key distribution in optical fiber communication lines”, Asia Communications and Photonics Conference (ACP), 2017.
5. Sabrina Abedin, TasfiaTasbin, Avijit Hira, “Optical wireless data transmission with enhanced substitution Caesar Cipher WHEEL encryption”, International Conference on Electrical, Computer and Communication Engineering (ECCE), 2017.
6. Takahiro Kodama, Naoki Nakagawa, Nobuyuki Kataoka, “Secure 2.5 Gbit/s, 16-Ary OCDM Block-Ciphering with XOR Using a Single Multi-Port Encoder /Decoder”, IEEE Journal of Lightwave Technology ,2010.
7. Yawen Shang, Wenyan Mao, Mengxiang Han, Cheng Xu, Guanjun Gao, “Underwater Wireless Optical Communication with High Modulation Level Based Stream Cipher”, Asia Communications and Photonics Conference (ACP), 2018.
8. Yetian Huang, Haoshuo Chen, Hanzi Huang, “Two-Level Optical Encryption for Secure Optical Communication”, Optical Fibre Communications Conference and Exhibition (OFC), 2020.
9. Zhimin Wu, Min Zhang, Danshi Wang, “Dual-channel all-optical encryption using hybrid modulation format XOR gates based on FWM in HNLF”, 16th International Conference on Optical Communications and Networks (ICOCN), 2017.