**CANARA ENGINEERING COLLEGE**

**BENJANAPADAVU MANGALORE-574219**

****

DEPARTMENT OF ELECTRONICS & COMMUNICATION

**MINI PROJECT**

***RANDOM DATA ENCRYPTION TECHNIQUE AND TRANSMITTING THROUGH LIGHT***

**SUBMITTED BY:**

*Rohit Dattatraya Hegde – 4CB18EC055*

**INDEX**

|  |  |  |
| --- | --- | --- |
| **SL.NO** | **CONTENTS** | **PAGE NO** |
| 1 | Aim | 3 |
| 2 | Components | 3 |
| 3 | Block diagram | 3-4 |
| 4 | Description | 4-5 |
| 5 | Working | 6 |
| 6 | Circuit diagram | 7-8 |
| 7 | Tabulation | 9 |
| 8 | Coding | 10 |
| 9 | Applications | 11 |
| 10 | Result | 11 |

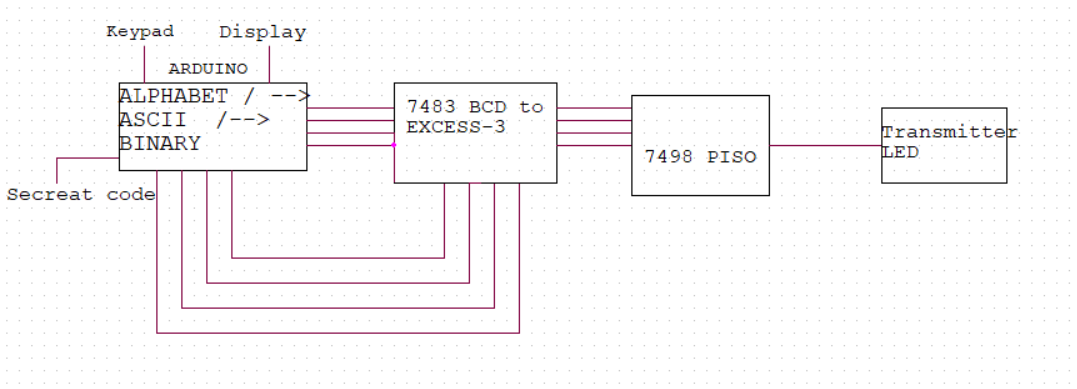
**Aim**: To make the data encrypt and to send it through light and to decrypt.

**Components** :

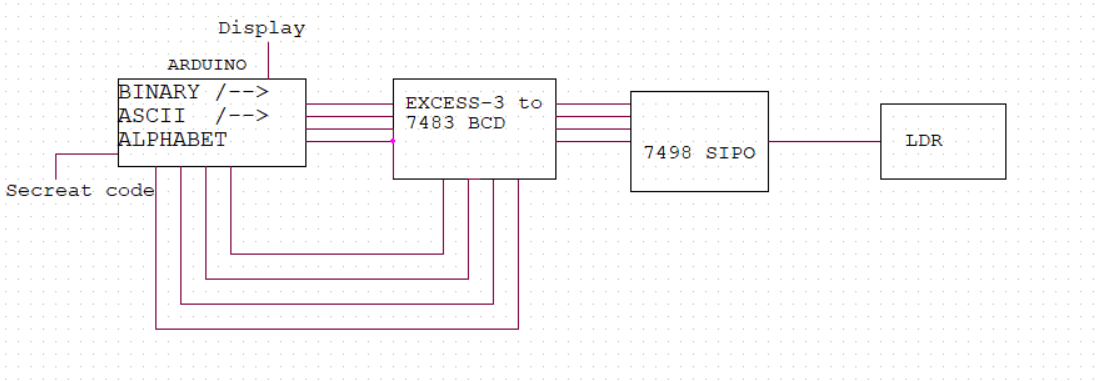
* Arduino - 2
* Ic 74LS83
* Ic 74LS95
* BC548 – transistor
* LDR
* LED

**BLOCK DIAGRAM**

**TRANSMITTER**



**RECEIVER**



The Secure communication is when two entities are communicating and do not want a third party to listen in. For that they need to communicate in a way not susceptible to interception. Secure communication includes means by which people can share information with varying degrees of certainty that third parties cannot intercept what was said. So this encryption system initially converts the data into binary form and than to excess ‘n’ form. Here n stands for the value that has to be added to the binary code that contains the information. So the excess ‘n’ added binary code is encrypted. For every second this encryption ‘n’ value changes. So the combination of all these ‘n’ values gives the encryption key. If both sender and the receiver coordinated this key, then only the proper decryption of data takes place.

**DESCRIPTION**

**History of encryption:**

In 1898, Nikola Tesla demonstrated a radio controlled boat in Madison Square Garden that allowed secure communication between transmitter and receiver.

One of the most famous systems of secure communication was the Green Hornet. During WWII, Winston Churchill had to discuss vital matters with Franklin D. Roosevelt. At first, the calls were made using a voice scrambler as this was thought to be secure. When this was found to be untrue the engineers started work on a whole new system which resulted in the Green Hornet or SIGSALY. With the Green Hornet, anyone unauthorized party listening in would just hear white noise while the conversation was clear to authorized parties. As secrecy was paramount, the location of the Green Hornet was only known by the people who built it and Winston Churchill. To maintain secrecy, the Green Hornet was kept in a closet labeled 'Broom Cupboard.'' The Green Hornet used a one-time pad.

**What is encryption?**

Encryption is a method in which data is rendered hard to read by an unauthorized party. Since encryption methods are created to extremely hard to break, many communication methods either use deliberately weaker encryption than possible, or have backdoors inserted to permit rapid decryption. In some cases government authorities have required backdoors be installed in secret. Many methods of encryption are also subject to "man in the middle" attack whereby a third party who can 'see' the establishment of the secure communication is made privy to the encryption method, this would apply for example to the interception of computer use at an ISP. Provided it is correctly programmed, sufficiently powerful, and the keys not intercepted, encryption would usually be considered secure. The article on key size examines the key requirements for certain degrees of encryption security.

Encryption can be implemented in a way that requires the use of encryption, i.e. if encrypted communication is impossible then no traffic is sent, or opportunistically. Opportunistic encryption is a lower security method to generally increase the percentage of generic traffic which is encrypted. This is analogous to beginning every conversation with "Do you speak Navajo?" If the response is affirmative, then the conversation proceeds in Navajo, otherwise it uses the common language of the two speakers. This method does not generally provide authentication or anonymity but it does protect the content of the conversation from eavesdropping.

An Information-theoretic security technique known as physical layer encryption ensures that a wireless communication link is provably secure with communications and coding techniques.

**Components details**

* **Arduino** refers to an open-source electronics platform or board and the software used to program it. **Arduino** is designed to make electronics more accessible to artists, designers, hobbyists and anyone interested in creating interactive objects or environments.
* It stands for Light Dependent Resistor or Photoresistor, which is a passive electronic component, basically a resistor which has a resistance that varies depending of the light intensity. A photoresistor is made of a high resistance semiconductor that absorbs photons and based on the quantity and frequency of the absorbed photons the semiconductor material give bound electrons enough energy to jump into the conduction band. The resulting free electrons conduct electricity resulting in lowering resistance of the photoresistor. The number of electrons is dependent of the photon’s frequency.
* The **74LS83** is a high speed 4-bit fuller Adder **IC** with carry out feature. The **IC** has four independent stages of full adder circuits in a single package. It is commonly used in applications where arithmetic operations are involved.
* The **74LS95**B is a 4-Bit Shift Register with serial and parallel synchronous operating modes. The serial shift right and parallel load are activated by separate clock inputs which are selected by a mode control input. The data is transferred from the serial or parallel D inputs to the Q outputs synchronous with the HIGH to LOW transition of the appropriate clock input
* The **BC548** is a general-purpose NPN bipolar junction transistor commonly used in European and American electronic equipment. It is notably often the first type of bipolar transistor hobbyists encounter and is often featured in designs in hobby electronics magazines where a general-purpose transistor is required.

**Working of RANDOM ENCRYPTION TECHNIQUE THROUGH LIGHT TRANSFER**

**Sender/ Transmitter:**

* Initially the data is given through the keypad connected to the Arduino. Arduino scans continuously for the input from the keypad.
* The entered data/ an alphabet is converted into the binary form by the Arduino.
* The binary coded of the given data is added with excess ‘n’ bit i.e excess 3, excess 4 any pre defined number which is known only to the sender and receiver.
* The excess bit is changing for each second or for each letter of the data. The whole combination of this ‘n’ bit gives the encryption key.
* Both sender and receiver have to use the same encryption key to send the data in encrypted way
* This encrypted binary parallel data is converted into a serial output.
* Serial output is amplified and converted into the form of light or laser light through led or laser.
* This have to be send through optical fiber for fast communication.

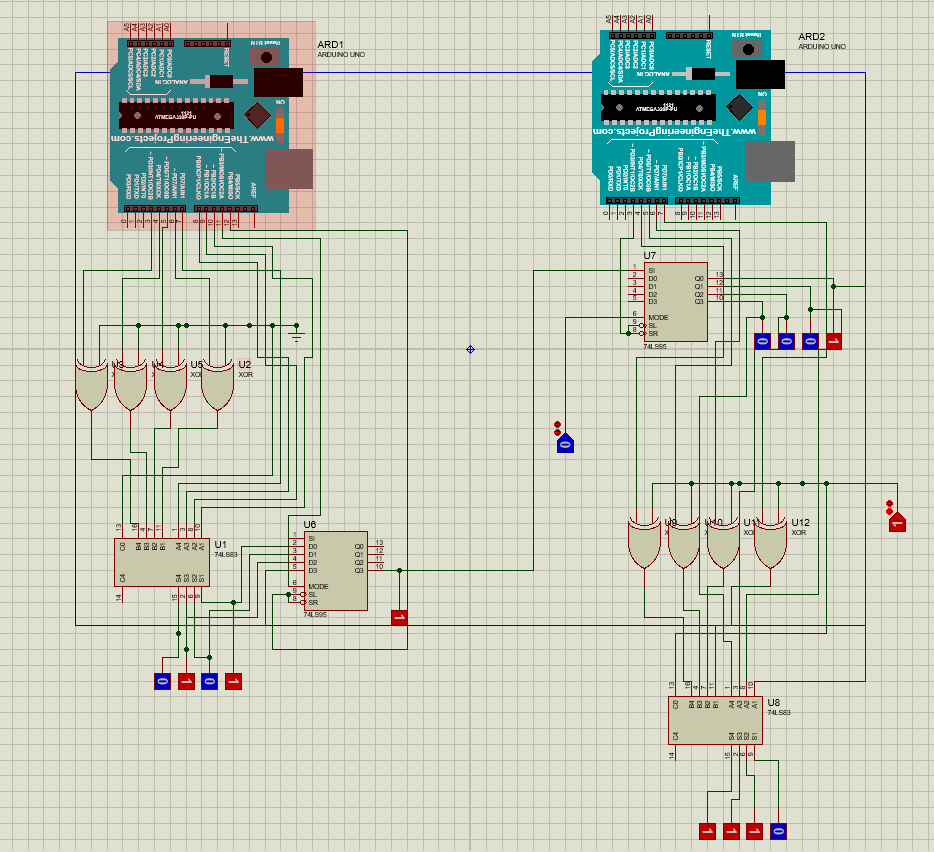
**Channel:**

* Optical fiber is preferred for the fast communication
* Even we can use any electromagnetic waves (radio waves) for transmitting the encrypted data. Here in this case I used light to transfer the data.

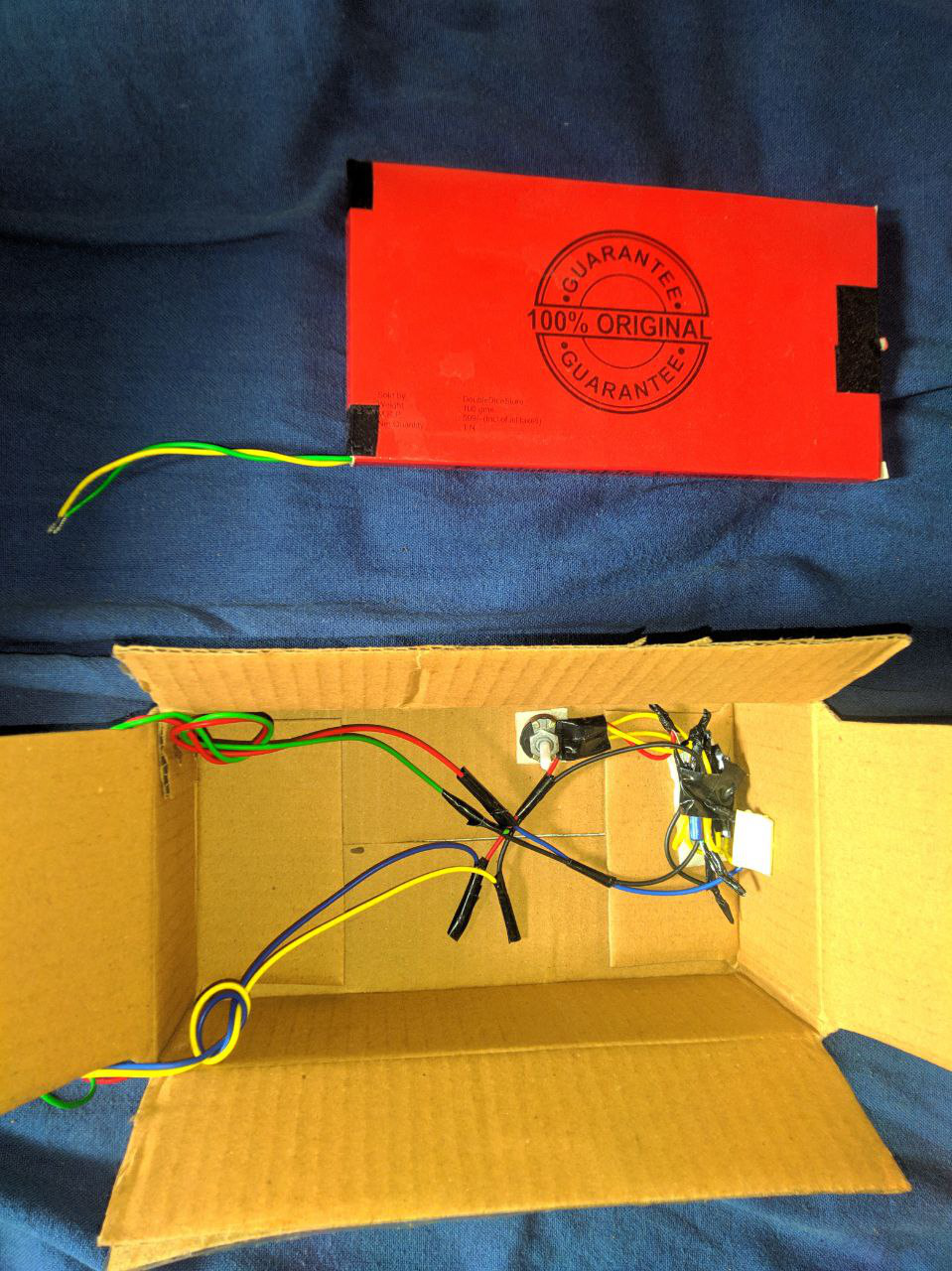
**Receiver:**

* Receiver part receives the light containing encrypted data.
* Here the light is in discrete manner i.e high and low form
* This light is converted back to encrypted binary data
* The binary data is given to subtractor where the excessed ‘n’ but that used by the sender for that data is used to decrypt it. If it’s other than ‘n’ value, the data is different than the sent one. It subtracts that value from the encrypted data.
* By using the encryption key, all encrypted data are decrypted and this is again given to the Arduino and giving a particular time interval for the Arduino to recognize the coming data
* This decrypted binary data is converted back to alphabet/ any data sent by user by Arduino and it is displayed on the LCD display/ screen.

**CIRCUIT DIAGRAM**



{The single line connection between sender and receiver part is the transmitting channel.}



**Transmitting channel setup**

**Tabulation:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DATA | BINARY(assigned) | ‘N’ BIT | ENCRYPTED | DECRYPTED | DATA |
| **A** | **0010** | **3** | **0101** | **0010** | **A** |
| **B** | **0110** | **2** | **1000** | **0110** | **B** |

**Coding for sending 2 ore-defined data**

**Receiver:**

|  |  |
| --- | --- |
| void setup() {  pinMode(3,OUTPUT);  pinMode(4,OUTPUT);  pinMode(5,OUTPUT);  pinMode(6,OUTPUT);  pinMode(7,OUTPUT);  }  void loop() {  //excess 3  digitalWrite(4,LOW);  digitalWrite(5,LOW);  digitalWrite(6,HIGH);  digitalWrite(7,HIGH);  delay(600);  digitalWrite(3,HIGH); //1 shift  delay(100);  digitalWrite(3,LOW);  delay(520);  digitalWrite(3,HIGH); //2 shift  delay(100);  digitalWrite(3,LOW);  delay(520);  digitalWrite(3,HIGH); //3 shift  delay(100);  digitalWrite(3,LOW);  delay(520);  digitalWrite(3,HIGH); //4 shift  delay(100); | digitalWrite(3,LOW);  delay(520);  delay(6000);  ////////////////////////////////////////////////////////////////  //excess 2  digitalWrite(4,LOW);  digitalWrite(5,LOW);  digitalWrite(6,HIGH);  digitalWrite(7,LOW);  delay(600);  digitalWrite(3,HIGH); //1 shift  delay(100);  digitalWrite(3,LOW);  delay(520);  digitalWrite(3,HIGH); //2 shift  delay(100);  digitalWrite(3,LOW);  delay(520);  digitalWrite(3,HIGH); //3 shift  delay(100);  digitalWrite(3,LOW);  delay(520);  digitalWrite(3,HIGH); //4 shift  delay(100);  digitalWrite(3,LOW);  delay(520);  delay(6000);  //By Rohit d h} |

**Sender:**

|  |  |
| --- | --- |
| void setup() {  pinMode(3,OUTPUT);  pinMode(4,OUTPUT);  pinMode(5,OUTPUT);  pinMode(6,OUTPUT);  pinMode(7,OUTPUT);  pinMode(8,OUTPUT);  pinMode(9,OUTPUT);  pinMode(10,OUTPUT);  pinMode(11,OUTPUT);  pinMode(12,OUTPUT);  pinMode(13,OUTPUT);  }  void loop() {  /////////////////////////////////////////1st DATA/////////////////////////////////////  //excess 3  digitalWrite(3,LOW);  digitalWrite(4,LOW);  digitalWrite(5,HIGH);  digitalWrite(6,HIGH);  //data A = 0 0 1 0  digitalWrite(7,LOW);  digitalWrite(8,LOW);  digitalWrite(9,HIGH);  digitalWrite(10,LOW);  //two clock pulse for load  digitalWrite(11,HIGH); //mode 1  delay(100);  digitalWrite(12,HIGH);  delay(100);  digitalWrite(12,LOW);  delay(100);  digitalWrite(12,HIGH);  delay(100);  digitalWrite(12,LOW);  delay(100);  digitalWrite(11,LOW); //mode 0  delay(150); //1 shifted  digitalWrite(12,HIGH);  delay(500);  digitalWrite(12,LOW);  delay(120); //2 shifted  digitalWrite(12,HIGH);  delay(500);  digitalWrite(12,LOW);  delay(120); //3 shifted  digitalWrite(12,HIGH);  delay(500); | digitalWrite(12,LOW);  delay(120); //4 shifted  delay(520);  delay(6000);  ////////////////////////////////////////2nd DATA///////////////////////////////////////  //excess 2  digitalWrite(3,LOW);  digitalWrite(4,LOW);  digitalWrite(5,HIGH);  digitalWrite(6,LOW);  //data B = 0 1 1 0  digitalWrite(7,LOW);  digitalWrite(8,HIGH);  digitalWrite(9,HIGH);  digitalWrite(10,LOW);  //two clock pulse for load  digitalWrite(11,HIGH); //mode 1  delay(100);  digitalWrite(12,HIGH);  delay(100);  digitalWrite(12,LOW);  delay(100);  digitalWrite(12,HIGH);  delay(100);  digitalWrite(12,LOW);  delay(100);  digitalWrite(11,LOW); //mode 0  delay(150); //1 shifted  digitalWrite(12,HIGH);  delay(500);  digitalWrite(12,LOW);  delay(120); //2 shifted  digitalWrite(12,HIGH);  delay(500);  digitalWrite(12,LOW);  delay(120); //3 shifted  digitalWrite(12,HIGH);  delay(500);  digitalWrite(12,LOW);  delay(120); //4 shifted  delay(520);  delay(6000);  ////By ROHIT D H  } |

**Application:**

* Secured communication
* Useful for military data handling
* For encryption of passwords in social media websites like face-book, Instagram etc
* To replace hash format of password saving technology to improved random encryption technology

**Result :**

Given data is encrypted at the receiver side and successfully decrypted at the receiver side.