ISSN 2395-1621

Data Encryption and Decryption using ASCCI Values

Prof. Rupali Deshmukh, Vinayak J. Amritwar, Mahesh D. Irlapalle, Sonam S. Narkhede

Department of Electronics and Telecommunication Engineering
Dr. D. Y. Patil Institute and Engineering Pimpri , Pune-18

ABSTRACT

In this paper, we proposed Data Encryption and Decryption Using RF module. Radio Frequency (RF) is any of the electromagnetic wave frequencies that lie in the range extending from around 3KHz to 300KHz, which includes those frequencies used for communication. Cryptography techniques provide high security to store secret and sensitive data, to transmit to receiver by sender and vice versa. Data encryption is the process of converting message(plaintext) into meaningless text(cipher text).Decryption is reverse meaningless data back to the original data (plaintext)that can read or understand to the receiver. The security is dependent on the key and algorithm, which are used to encrypt and decrypt the message.

Key Words: RF Module, CP Module, Encryption Algorithm, Decryption Algorithm.

ARTICLE INFO

Article History

Received: 11th June 2020

Received in revised form :

11th June 2020

Accepted: 14th June 2020

Published online :

15th June 2020

I. INTRODUCTION

The main advantage of this project is that the data cannot be received until and unless you don't have receiver code that is compatible to transmitter. At the transmitter, keyboard will be attached to microcontroller which is used to input the message. Data encryption and decryption is the process of converting ordinary information or message (plaintext) into meaningless text (cipher text).Decryption is reverse or moving from the random, meaningless data back to the plaintext that can read and understand to the computer. This message is encrypted and then it is transmitted using radio frequency transmitter. The data which will be entered at the transmitter will also be displayed on screen for convenient entry. At the receiving end when the encrypted message is received then this message is decrypted by the microcontroller and is displayed on screen.

For example:

In encryption if we have message h and key is P so encryption process as follows:

h = 104 = 01101000

P = 80 = 01010000 XOR

00111000=56 = 8

To decrypt the cipher text is applied the operation XOR on the cipher text, so that plain text back to its original data.

The resulting cipher text is 8, as for the decryption process then performed the operation XOR between cipher text with a key so that it returns to the original message.

8 = 56 =00111000

P = 97 = 01100001 XOR

01101000=104=h

Data Encryption and Decryption provide high security which is depends on the algorithm which is used. The basic principle of Cryptography is defined as: A message being sent is known as plaintext. The message is then coded using a cryptographic algorithm. This process is called encryption. An encrypted message is known as cipher text, and is turned back into plaintext by the process of decryption. The method for decryption is the same as that for encryption but in reverse direction. It is applicable in each phase of encryption.

There are two algorithms used for encryption and decryption, which is mainly done by using ASCII value. In encryption ASCII value of each character in string is encrypted using subtraction of ASCII values of 1(49), 2(50),

3(51) respectively. In decryption original data can be derived by addition of ASCII values of 1, 2, 3 resp.

In second method X-OR operation is used for encryption and decryption. In encryption take a binary equivalent of ASCII value of each character in sting and perform the X-OR operation binary equivalent of ASCII value of key "P".

Security is essential factor during communication among the people and in e-commerce for the internet user applications such as private communication, password protection and secured e-commerce. The need of secure communication i.e., with Cryptography techniques provides high security like internet banking, ATM"s and Satellite transmission etc.

II. METHODOLOGY

At transmitter side we are using Laptop, CP module, Microcontroller and RF transmitter. First data will be send to controller through the CP module. CP module is used for the serial communication. The data will encrypt and it will transmitted through RF transmitter Module. At receiver end the data is received by RF receiver module. That data will send to the microcontroller. Then data will decrypt and it will send through the CP module to the laptop. Hence the data will get in original form.

ENCRYPTION ALGORITHM

For method 1.

1. START

2. Fetch the string to be encrypts

3. Calculate the ASCII value of each character in the string

4. Calculate the ASCII value of 1

5. Subtract ASCII value of 1from each character in the string

6. Put the NO or character which shows the ASCII value after subtraction

7. STOP

DECRYPTION ALGORITHM

For method 1.

1. Receive the string to be decrypts

2. Calculate the ASCII value of each character or symbol in string

3. Calculate ASCII value of 1

4. Add ASCII value of 1 in each character or symbol in the string

5. Put the NO or character which shows the ASCII value after addition

6. STOP

ENCRYPTION ALGORITHM

For method 2

1.START

2.Fetch the string to be encrypts

3.Calculate the ASCII value of each character in the string

4.Calculate the binary equivalent of ASCII value

5.Take a key "P" & calculate the ASCII value of "P"

6. Calculate the binary equivalent of ASCII value of "P"

7. Perform XOR operation between each character in the input string to the binary equivalent of "P" 8.Calculate ASCII value after XOR operation

8.Calculate ASCII value after XOR operation

9. Note the NO or character which shows the resultant ASCII value

10.STOP

DECRYPTION ALGORITHM

For method 2.

1. Receive the string to be decrypts

2. Calculate the ASCII value and corresponding binary equivalent of each character or symbol in string

3. Calculate the ASCII value & corresponding binary equivalent of "P"

4. Perform XOR operation between each character or NO in string to the binary equivalent of "P"

5. Calculate the ASCII value of binary equivalent after XOR operation

6. Note the NO or character which shows the resultant ASCII value

7. STOP.

Example to demonstrate the Encryption:

Break up of „hello" in char	h	e	l	l	o
ASCII values	104	101	108	108	111
ASCII value of 1	49	49	49	49	49
Subtracting	55	52	59	59	62
Encrypted data	7	4	;	;	>

Decryption

Break up of „74;;>"	7	4	;	;	>
ASCII value	55	52	59	59	62
ASCII value of 1	49	49	49	49	49
Adding	104	101	108	108	111
Decrypted data	h	e	l	l	o

III. RESULT

TRANSMITTED DATA

RECEIVED DATA

IV. CONCLUSION

Data encryption and decryption systems are used to improve information security to secure data that, thereby providing enhanced level of assurance such that the data that are encrypted cannot be viewed by unauthorized receivers in the event of theft or loss.

REFERENCES

[1]Ankit Dhamija, Research Scholar- A Novel Cryptographic and Steganographic Approch for Secure Cloud for Data Migration, IEEE paper, Amity University, April 2016.

[2] Dain Rachmawati, Super-Encryption Implementation Using Monoalphabetic algorithm and XOR Algorithm for Data Security, Journal of Physics, 2018.

[3] A.VIjayan. et. Int. Journal of Engineering Research and applications ASCII Value Based Encryption System, April 2016.

[4] International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013

