Abstract: This is the algorithm in which arbitrarily generated numbers are used with the help of modulus and remainder by making program in any language i.e. C, C++ and Java. Carefully, using these modulus & remainder for getting a new method for encrypting and decrypting the message. Though complex encryption techniques have been employed in protection data. Three or more keys can also be used to make the enciphering process more complicated. The main focus of this paper is to provide with an encryption decryption algorithm with secure strength, bringing failure to the intruder effort to break the cipher.

Keywords: Substitution Array, Encryption, Decryption, Secret key, Plaintext, Cipher text.

I. INTRODUCTION

As our main keywords are encryption and decryption so, firstly we understand what is encryption and decryption? Encryption and decryption are used under the topic cryptography. So, cryptography [1, 5, 6, 9] is the branch of art and science of keeping secret messages secret by which unauthorized users can’t access that secret message. So, to make message secret we use encryption i.e. convert plain-text or message into some other code called cipher-text and decryption i.e. convert that cipher-text into original readable form. For encryption and decryption we need two party sender and receiver. The given input on which encryption is to be done and obtain ASCII [7, 8] value for it. Then perform ASCII code to numerical value conversion. Their respective numeric code will be converted into ASCII characters. This conversion is very simple. Then add the character into the command window and press the ok button. After that automatically gives out the resultant numeric code. From the generated substitution array Substitute the numbers sequentially on a one-to-one basis at the place of character of the plain text. Now divide the number chosen with the ASCII value of the plain text character and calculate the Quotient and the Remainder and store it in the Array. The message will now be the series of Quotient followed by the Remainder. A substitution array approach used ASCII values for the encryption and decryption process. ASCII stands for American standard code for information interchange has been adopted by several American computer manufactures as their computer’s internal code American standard association developed ASCII. ASCII value of each character is different.

As A-65, B-66, C-67, …., Z=90 or a -97, b-98, …., z=122 and so on.

Basic Terminology

Plain text: The original intelligible message.
Cipher text: The transformed or coded message.
Cipher: An algorithm for transforming an intelligible message into one.

Key: Some critical information used by cipher.
For Encryption: Y = EK(X)
Where Y=cipher text, E= encryption, K= key, & X= plaintext
For Decryption: X = DK(Y)
Where X= plain text, D= decryption, K= key, Y= cipher text

II. ENVIRONMENT

Cryptography, used for the purpose of security. Nowadays need of security is necessary to make the data secure for the unauthorized users to access. Firstly, security is needed for military communication but day by day as the world, People’s becoming modern and smart, it is necessary to our general economy also both for business application and other application also. Business application includes the security among the data of the company in which information about of the employees, manager workers and owner’s profit is itself stored and similarly, application i.e used by the user’s according to their use is also require security. So, security [2, 3, 8, 10] plays a vital role our day to day life cryptographers are the people who wants to make secure system for the purpose of communication by which information is transmitted securely. But there are some hackers called crypto-analysis wants to develop.

The word cryptography comes from the Greek word kryptos, which is meant for hidden and graphein, which is meant for writing. Always there has been need for exchanging information secretly. The first algorithm and technology to make system more & more complicated and confusing by which hackers can hack. Cryptography is the science of encrypting and decrypting information can be traced back all the way to year 2000 BC in Egypt. Julius Caesar (100-44 BC)
used a simple substitution cipher which has been named after him today. During the first and the second war the demand for secrecy increased dramatically and all kinds of new cryptographic techniques evolved. There are many examples in history where people have tried to keep information secret from enemies or strangers.

III. STRUCTURAL DESIGN

The structural design consists of the following steps:

- Firstly select any number randomly
- After selection use starting and ending number and make subset, followed selection of modulus and remainders well
- When subset is selected then it is divided by mode
- After division take only those number which gives remainder
- Finally selected numbers will be resumed as substitution array

```plaintext
SYSTEM:
Remainder Mode (Subset A [1------n-1])
// computes the substitution array
by dividing it by mode first
//input: A subset A [1------n-1] of
orderable elements
// output: The substitution array
which gives remainder
for (i=1; i <= number; i++)
{
    Take a number, mode & remainder
    if (mode>=number)
    {
        Mode should be less than number;
        Remainder should be less than mode;
    }
    else if (mode < number) || (remainder < mode)
    {
        for (i=R; i<=number; i++)
        {
            Calculate the subset of number (snum);
            Snum/mode;
            if (Rem == Remainder)
            {
                Print the Substitution_array
            }
        }
    }
    Randomly select a number, modei = R; and remainder value
    if (mode >= number) || (remainder >= mode)
    {
        Mode should be less than number;
        Remainder should be less than mode;
    }
    else if (mode < number) || (remainder < mode)
    {
        for (i=R; i<=number; i++)
        {
            Calculate the snum;
            //Snum=subset of number
            Snum /mode;
            if(R=remainder)
            {
                Print the Substitution_array
            }
        }
    }
}
```

Figure 2: Procedure of Substitution Array

Figure 3: Procedure of Encryption and Decryption

Encryption & Decryption Procedure:-

For Encryption
Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

IV. FUTURE SCOPE

This algorithm is developed for the purpose of security. There are many future scope of substitution array using ASCII value for Encryption & Decryption. Firstly it certified that any other third person don’t hack the data between the gap of plain text and cipher text. Secondly receiver gets the cipher text as it’s is as the senders send the plain text. Thirdly in the modern world, new technologies upgraded day by day so we can make changes this algorithm according to the need. This work can be further improvised upon in the future in a number of ways.

CONCLUSION

The Proposed methodology will give the new area of research on cryptography and ASCII algorithms. This new methodology for text encrypts and decrypt using ASCII algorithm is definitely an effective method while compared with other cryptography systems. This algorithm is very fast, secure and reliable.

References