

Encryption and Decryption Algorithm using ASCII values with substitution array Approach

Vineet Sukhraliya¹, Sumit Chaudhary², Sangeeta Solanki³

Assistant Professor, Electronics & Communication, VKIT, Bijnore, India¹

Assistant Professor, Computer Science, Shri Ram Group of Colleges, Muzaffarnagar, India²

Assistant Professor, Computer Science, Shobhit University, Meerut, India³

Abstract: This is the algorithm in which randomly 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 safeguarding 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, 11, 17] 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 inter change 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 or a -97, b-98 and so on.

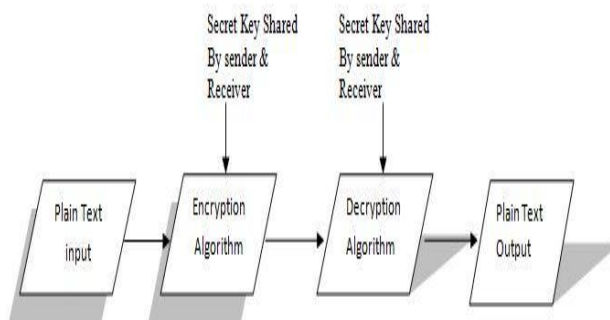


Figure 1: Conventional Encryption Model

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= plain text

For Decryption: $X = DK(Y)$

Where X= plain text, D= decryption, K= key, Y= cipher text



II. BACKGROUND

Cryptography, used for the purpose of security. Now –a-days 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 crypta-analysis wants to develop. The first algorithm and technology to make system more & more complicated and confusing by which hackers can hack. 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. There are many examples in history where people have tried to keep information secret from enemies or strangers. Cryptography is the science of encrypting and decrypting [11, 13, 14, 16] 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.

III. ARCHITECTURE

The architecture 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 remainder as 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

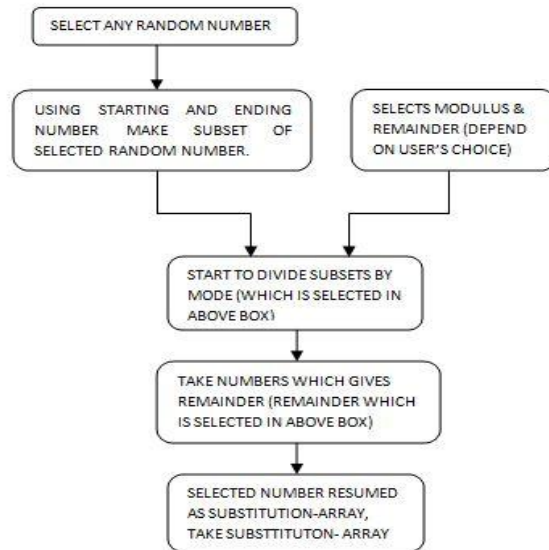


Figure 2: Procedure of Substitution array

MECHANISM:

```

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;
}
}
}
}
}
}
}
}
}

```

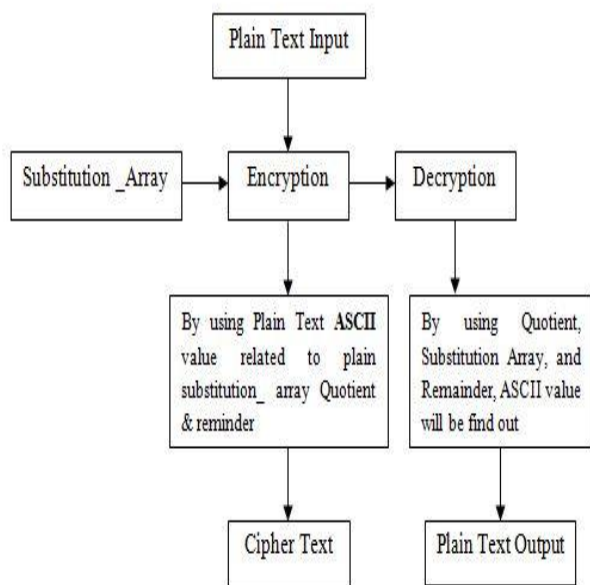


Figure 2: Procedure of Encryption and Decryption

Encryption & Decryption Procedure:-

For Encryption

Character	H	E	L	L	O
ASCII value	72	69	76	76	79
Substitution Array	2627	3747	4867	1227	4027
Division	2627/72	3747/69	4867/76	1227/76	4027/79
Quotient	36	54	64	16	410
Remainder	35	23	03	11	77

For Decryption:

Quotient	36	54	64	16	410
Substitution Array	2627	3747	4867	1227	4027
Remainder	35	23	03	11	77
ASCII value	72	69	76	76	79
Character	H	E	L	L	O

Figure 4: Table Content of Encryption & Decryption

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.

V. 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

[1] Stallings W. Cryptography and Network Security: Principles and Practice, 2/3e Prentice hall, 1999; 30-49.
 [2] Simmons S. Algebraic Cryptanalysis of Simplified AES. Proquest Science Journals 2009; 33(4): 305.
 [3] Satyanarayana MV, Vijaya PA. Variable Size Block Encryption using Dynamic-key Mechanism (VBEDM), Volume 27-7.



- [4] International Journal of Engineering Education, <http://www.ijesr.org.ie>, Accessed 30 december 2012.
- [5] Aleksey Gorodilov, Vladimir Morozenko, 'Genetic Algorithms for finding the key's length and crypto analysis of the permutation cipher', International Journal "Information Theories and Applications vol.15/2008.
- [6] Bethany Delman, 'Genetic Algorithms in Cryptography' published in web; July 2004.
- [7] Darrell Whitley, "A Genetic Algorithm Tutorial", Computer Science Department, Colorado State University, Fort Collins, CO 80523.
- [8] Introduction to Cryptography – Ranjan Bose – Tata Mc-Grew – hill Publisher Ltd, 2001.
- [9] N. Koblitz, 'A course in number theory and Cryptography', Springer-Verlag, New York, INc, 1994.
- [10] Nalani N, G. Raghavendra Rao, 'Cryptanalysis of Simplified Data Encryption Standard via Optimisation Heuristics; IJCSNS, Vol.6 No.1B, January 2006.
- [11] Sean Simmons, 'Algebraic Cryptoanalysis of Simplified AES', October 2009; 33, 4; Proquest Science Journals Pg.305.
- [12] Sujith Ravi, Kevin Knight, 'Attacking Letter Substitution Ciphers with Integer Programming', Oct 2009, 33, 4; Proquest Science Journals Pg.321.
- [13] A K Verma, Mauyank Dave and R.C Joshi, 'Genetic Algorithm and Tabu Search Attack on the Mono Alphabetic Substitution Cipher in Adhoc Networks; Journal of Computer Science 3(3): 134-137, 2007.
- [14] Che-Chern Lin "Study on internet usages, academic achievements, and the exploring capability of regional culture knowledge using internet" WSEAS Transactions on Information Science and Applications Volume 5 Issue 10, October 2008.
- [15] Ross J. Anderson, "Why Cryptosystems Fail", Communications of the ACM, New York, USA, 1994, pp. 32-40.
- [16] Francois-Xavier Standaert, Gilles Piret, Jean- Jacques Quisquater, "Cryptanalysis of Block Ciphers: A Survey", UCL Crypto Group, 2003.
- [17] William C. Barker, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", National Institute of Standards and Technology, NIST Special Publication 800-67, 2008.
- [18] Collins, R.W., "Software localization for Internet software, issues and methods", Software, IEEE, Florida, USA, 2002, pp. 74-80.

BIOGRAPHY



Vineet Sukhraliya is working as a Assistant Professor in ECE Department at VKIT, Bijnore, (U.P.). He completed B-Tech (Electronics and Communication Engineering) with First Division from S.D College of Engineering & Technology, Muzaffarnagar. During teaching He has been coordinated many Technical fests and National Conferences at Institute Level. He has attended several seminars, workshops and conferences at various levels. His area of research includes Wireless Communication, Handoff Management, VHDL and Various Types of Antennas.



Sumit Chaudhary is working as Assistant Professor in CSE department at Shri Ram Group of colleges, Muzaffarnagar (U.P.), INDIA. He obtained his M-Tech (Computer Engineering) with Hons. from Shobhit University and B-Tech (Computer Science) from SCRJET, Meerut (U.P.). He has been in teaching from more than four years. During this short period of time, he has been supervised several dissertation of M.Tech. Students. He has been member of several academic and administrative bodies. During his teaching he has been coordinated many Technical fests and National Conferences at Institute and University Level. He has attended several seminars, workshops and

conferences at various levels. His many papers are published in various national, international journals and conferences. His area of research includes Wireless Sensor Network (WSN), Network Security, Neural Network, Artificial Intelligence and MANET (Mobile Ad-Hoc network).



Sangeeta Solanki is working as Assistant Professor in CSE department at Shobhit University, Meerut, (U.P.), INDIA. She is pursuing her PhD from Shobhit University, Meerut (U.P.). She obtained her M-Tech (Computer Engineering) with Hons. from Shobhit University and B-Tech (C.S.) from IIMT College of Engineering, Meerut (U.P.), INDIA. She has been in teaching from more than four years. Her many papers are published in various national, international journals and conferences. Her area of research includes MANET (Mobile Ad-Hoc network), Wireless Sensor Network (WSN) and Network Security.