Symmetric Encryption Algorithm using ASCII Values

Uma Pujeri, Ramachandra Pujeri

Abstract**:** ***Cryptography at its very core is nothing but math - pure, simple, undiluted math. Math created algorithms that are basics for various encryption algorithm. Encryption is a method in which user's confidential data or private data is encoded to cipher text and this text can be read only if it is decrypted by authorized user using the right key. Cipher text can be decoded back to plain text, only by the authorized users using a right key. Various encryption algorithm are used to encrypt the plain text to cipher text and the cipher text is decrypted back to plain text by authorized user using right key. The symmetric key algorithm uses the same key to encrypt the plain text and decrypt the cipher text. In this paper we have proposed new symmetric algorithm using ASCII value. The plain text using key and ASCII values is converted to cipher text. Encryption algorithm sends cipher text and minimum value to the authorized receiver. Receiver decrypts the cipher text to plain text using same key and minimum value. In this algorithm sequence of five pseudo random number is generated and sum of this five pseudo random number is added to the obtained decimal value. Seed to generate common sequence of pseudo random number is kept secret between sender and receiver. Proposed algorithm support variable key length and plain text size. This algorithms performs faster when text is small message, but the execution time increases as the plain text size increases. This algorithm can be used to send small messages in a secured way. .***

Keywords **:** ***ASCII key, Cipher text, Decryption algorithm, Encryption algorithm, Plain text, Symmetric Key algorithm.***

I. INTRODUCTION

Everyone is a proponent of strong encryption.

Dorothy Denning

Cryptography is practice and technique to secure users confidential data in the presence of adversaries. The main goal of cryptography are Confidentiality/Privacy, Integrity, Authentication, Non repudiation. Encryption is a subset of cryptography. Encryption converts plain text to unreadable format called as cipher text. Encryption can also be called as actual process of applying cryptography. Decryption is simply the inverse of encryption following the same steps in reverse order. Figure 1.1 and 1.2 shows encryption and decryption process.

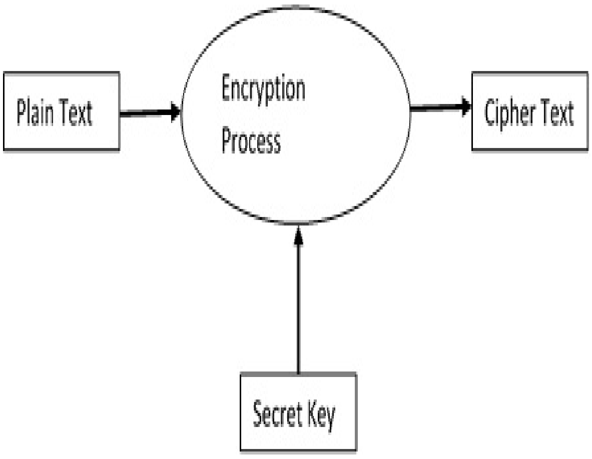


Fig. 1. Encryption Process.

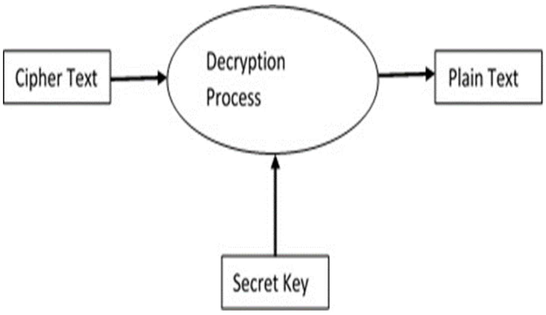


Fig.2. Decryption Process.

Today's most widely used encryption algorithm fall in two categories.

- **Symmetric Key encryption algorithm**: In symmetric key encryption algorithm secret key is shared secretly using various key exchange algorithms like RSA, Diffie- Hellman, and ECC Diffie-Hellman etc. between sender and receiver. Both sender and receiver use the same key for encryption and decryption process. Since key used by sender to encrypt plain text to cipher text and key used by receiver to decrypt cipher text to plain text is same, the algorithm is called symmetric key encryption algorithm.

Manuscript published on January 30, 2020.
* Correspondence Author

Dr. Uma Pujeri*, School of Computer Engineering and Technology, MIT World Peace University, Pune - 411038, India. Email: umaresearch81@gmail.com; uma.pujeri@mitwpu.edu.in

Dr. Ramachandra Pujeri Director MIT ADT, Computer Engineering, MIT ADT, Loni Campus, Pune, India. Email: sriramu.vp@gmail.com

- **Asymmetric key encryption algorithm**: In asymmetric key encryption algorithm two keys public key and private key are used for encryption and decryption process. Public key is used to encrypt the plain text to cipher text. The receiver can decrypt the cipher text by using private key. Private Key is also called as secret key and public key are stored in public databases and anyone can see it. RSA, digital signatures are the example of asymmetric algorithm.

In this paper we have proposed the symmetric key encryption algorithm which uses the same key for encryption and decryption process. Our proposed algorithm uses ASCII values and secret keys for encryption and decryption process. Length of plain text and length of key are independent of each other. The proposed algorithm is implemented in Java and can be used to send small text message, chat message securely in a much faster way. Section II of the paper dis- cusses the past and present history of symmetric algorithms, Section III discusses the algorithm, Section IV discusses the results and finally section V discusses conclusion and future work.

II. History of Past and Present Symmetric Algorithm

Cipher codes and many ancient encryption algorithm were used throughout his- tory to prevent non-authorized people from understanding the message. Simple historical cipher systems are discussed in this session and how these cipher lead to to the design of modern cipher is also discussed.

A. Caesar Shift Cipher Used by Roman Army

Caesar Cipher is an example of symmetric cipher. Caesar Cipher was named in honor of Julius Caesar who used this encryption algorithm to encrypt the military and official message. Algorithm C= P + key mod 26 P = C key mod 26

Suppose key is 3 and plaintext is ABCD then the cipher text will be DEFG.

B. Simple Substitution Cipher

This is also an example of symmetric key cryptography where sender and receiver decides on randomly selected permutation of letters of alphabets. Sender replaces each plain text letter by substituting permutation that is directly beneath its table while receiver on receiving cipher text replaces each cipher text letter with the corresponding plaintext in the top row.

Table 1. Simple Substitution Cipher.

PT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CT	C	F	J	L	O	B	P	R	U	V	X	Z	D	Y	W	T	G	I	M	N	A	Q	S	H	K	E

C. The Pigpen Cipher

The pigpen cipher is simple geometric substitution cipher which substitutes English alphabets with fragments of grid.

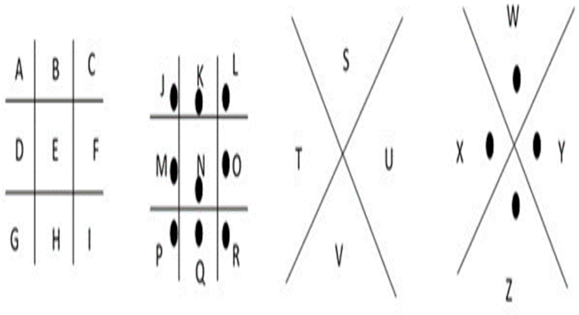


Fig. 3. Pigpen Cipher.

Example India plain text then cipher text will be

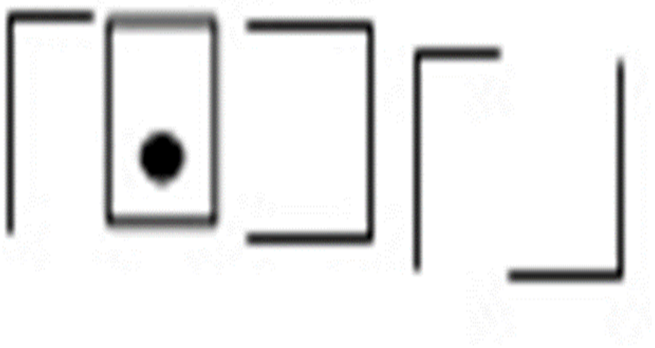


Fig. 4. Pigpen Cipher for text INDIA

D. Play fair Cipher

Play fair cipher was first developed by Charles Wheatstone in 1854, the play fair cipher was named after its promoters Lord play fair.. The play fair cipher uses pairs of letters rather than single letter substitution cipher making the cipher text complex and harder to guess. The play fair cipher is based of 5 * 5 matrix of alphabets constructed using keyword. Rules of play fair cipher to construct cipher text from plain text.

1. Break the plain text into pair of alphabets
2. If both the alphabets are same then add filler alphabet x after the first alphabets, thus making new pair and continue for example ballons will be ba lx lo on.
3. If both the alphabets of plaintext fall in same column then replace it by the letter beneath it, with the top element of the column circularly following the last.
4. If both the alphabet of the plain text fall in the same row then replace it by the letter to the right, with the first element of the row circularly following the back.
5. If both the alphabets of the plain text fall in different column then replace by the letter that lies in its own row and the column occupied by the other plain text.

Thus if the keyword is domestic and the plain text is The key is hidden under the door then the keyword matrix is

Retrieval Number: E5980018520/2020©BEIESP
DOI:10.35940/ijrte.E5980.018520
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Table 2. Play fair Cipher Example with keyword domestic

D	O	M	E	S
T	I	C	A	B
F	G	H	K	L
N	P	Q	R	U
V	W	X	Y	Z

And the cipher text will be **cf ar ae bo gc mv os pn vt ay cf so mw ep.**

E. Modern Symmetric Cipher

In this session all symmetric algorithms developed in modern cryptographic era are discussed.

DES Data encryption standard one of the well-known algorithm of modern cryptographic era was developed in 1970 by IBM in the United States of America. It was replaced by AES in the early 21st century. DES was fortified with new modification which were called as double-DES and triple DES. Double DES decrypt twice to each data block while triple DES decrypts thrice to each data block. DES and double DES are no longer used today but triple DES which is slower than AES is still used today in many electronic payment industry, NIST SP 800-57, Microsoft One note and Outlook 2007 to protect user's system private confidential data.

AES The Advanced encryption standard algorithm was established by the National Institute of Standard and Technology (NIST) in 2001 in United States of America. AES has been adopted worldwide with key length of 128,192 and 256 bits. AES is still widely used today for its better processing power in wide range of hardware like smart card and high performance computers.

RC2 RC2 is symmetric block designed by RON Rivest in 1987. It is a 64-bit block cipher with variable key size and 18 rounds arranged by heavy unbalanced Feistal network with 16 rounds of one type (MIXING) and two rounds of another type (MASHING). RC2 is vulnerable to related key attack using 234 chosen plain text.

RC4 RC4 was designed by Ron Rivest in 1987 is a stream cipher. RC4 was remarkable for its simplicity, speed in software, but multiple vulnerabilities were discovered in RC4 making it insecure. The algorithm was used in some encryption protocols and standards such as WEP in 1997, WPA in 2003, SSL in 1995 and TLS in 1999 and RC4 was prohibited in all the versions of TLS RFC 7465 in 2015.

RC5 It was invented by Ron Rivest in 1994 which had as block size which may vary from 32, 64 or 128 bits and key size from 0 to 2040 bits and rounds from 0 to 255. The original suggestion for parameters was 64 bit block, 128 bit key and 12 rounds

RC6 The main goal for implementation of RC6 was RSA competition and managed to become one of the five finalist. RC6 was invented by Ron Rivets and his colleagues which was derived from RC5. RC6 has a block size of 128 bits and supported key size 128,192, 256 bits and up to 2040 bits. RC6 like RC5 uses data dependent rotations, modular addition and XOR operation

Blowfish Blowfish was invented by Bruce Schneider which is a symmetric block cipher. Blowfish has variable key size from 32 bits to 448 bits is 64 bits and has 16 rounds. Blowfish is not used today because it is vulnerable to sweet32 attack, birthday attack and plain text attack.

Twofish Twofish publish in 1998 which was successor of Blowfish. Twofish has 256 bit key size, 128 bit block size and 16 rounds. Two fish could be implemented on hardware smart card as well as large microprocessors. Twofish is still used today.

III. PROPOSED SYSTEM

Proposed algorithm is implemented in Java. One of the main reason java was chosen because it is platform independent language and run on different types of computers. Since it is symmetric key encryption algorithm 128 bit key ”123@in- dia123456dfgbjcnbvcxzlkjh6 is secretly shared between sender and receiver using various key sharing algorithm. In this algorithm both sender and receiver pseudo random sequence of five numbers and to generate the pseudo random sequence the seed is common between the sender and receiver and kept secret and key size can be variable. Algorithm takes Input text and key convert it to cipher text using ASCII values of the text. Algorithm works faster smaller text but execution time increase as the text size increases. This algorithm can be used to send small messages securely. Algorithm is secured and cannot be easily hacked until attacker knows the key value and constant value.

A. Encryption Algorithm

Step 1 - Scan the input text.

Step 2 - Calculate the length of the text and store it in variable len.

Step 3 - Calculate the ASCII value of every text

Step 4 - Find the minimum ASCII value from the inputted text Store the minimum value to a variable min.

Step 5 - Subtract the min ASCII value from other ASCII value of the text and store the values in array arr

Step 6 - Input the symmetric key

Step 7 - Convert the inputted key to its ASCII

Step 8 - Find the minimum ASCII value of the inputted text

Step 9 -Mod with minimum ASCII value with other ASCII values

Step 10 - If the result of minimum ASCII value with other ASCII values is greater than 16 then mod it again with 16

Step 11 - Calculate mean

Step 12 - Add mean value to elements of an array arr and store the result in an array named arr1.

Step 13 - Convert the values of arr1 to binary (Note append zeros to make it equal digits) max values of binary digit is 5 store it variable x.

Step 14 - Concatenate all binary values of arr1 and make one binary string names as binarr1

Step 15 - Rotate the binary value of binarr1 to right 3 times

Step 16 - Covert the value of rotated rightmost bit of binarr1 to len(len is calculated in step 2) subarray of x digit(x is calculated in step 13)

Step 17 - Convert the calculated value to decimal

Step 18 - Add a all the sequence of five pseudo random number generated numbers with secret seed with the converted decimal value of step 17

Step 19 - Convert the value from step 18 to character

Step 20 - Send the cipher text and min value calculated in step 3 to decryption algorithm.

B. Decryption Algorithm

Step 1 - Cipher text and min value is received calculate length of cipher text and store in it len.

Step 2 - Symmetric algorithm hence key is common key

Step 3 - Covert the received cipher text to ASCII values

Step 4 - Subtract with the sum of all the sequence of five pseudo random number generated with secret seed.

Step 5 - Convert it to binary Find max digit of binary and append zeros to make the conversion of equal digit (example 21 has five binary digits and five has three binary digit append two zeros and make it five binary digit) here max = 5

Step 6 - Concatenate and make it a single string as and store it in decryptbin

Step 7 - Rotate the binary value of decryptbin to left 3 times

Step 8 - Covert the value of rotated leftmost bit of decryptbin to len(len is calculated in step 1) subarray of max digit(max is calculated in step 5)

Step 9- Convert the value calculated at step eight to decimal

Step 10 - Subtract it with key mean (key mean is calculated in encryption algorithm refer steps 6 to 11 same steps applicable here too)

Step 11 - Subtract the value of key means with the decimal values ob- tained in step 9

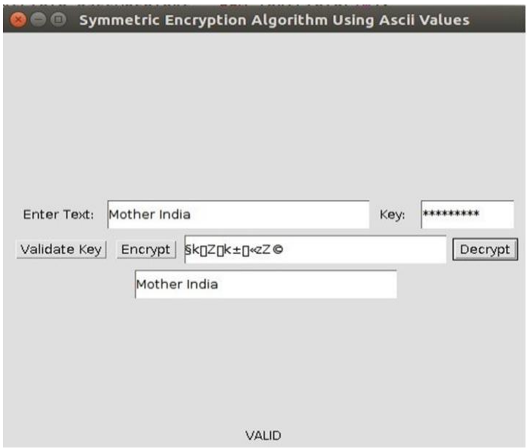
Step 12 - Add min value with the value of step 11

Step 13 - Convert the value from step 12 to character

Step 14 - Cipher text encrypted successfully to the text.

IV. RESULTS.

Program was developed in java and following is the output of the proposed algorithm Proposed algorithm was test with variable plain text size starting from one alphabet to plain text size up to 10 alphabets and output was analyzed.



Enter Text: Mother India

Key: *********

§k▯Z▯k±▯«zZ©

Mother India

VALID

Fig. 6. Output of Proposed Algorithm.

Table depicts conversion of plain text to cipher text from one plain text alphabet to 10 plain text alphabet.

Table 3. Proposed Algorithm output from Plaintext to Cipher text.

Sr. No	Number of letter in Plain text	Plain Text	Cipher Text
1	1	Aa	qu
2	2	IN	ry
3	3	two	NHM
4	4	FOUR	IZ*W*
5	5	EIGHT	UZJBG
6	6	future	Y$_[$*W* [*M*
7	7	ENERGY	IZ][ND
8	8	Question	YvTVFLue
9	9	knowledge	^{W} *CHFY*]*ZE*
10	10	Government	YvwmgNnefo

V. CONCLUSION AND FUTURE WORK

Symmetric key algorithm was implemented in java using a ASCII value of plain text and key. Size of plain text and key are independent of each other. Cipher text produced by the algorithm was really difficult to guess. Algorithm worked faster for smaller plain text, but became slower as the text size increased. Algorithm can be used for send small text message, chats etc. securely over the internet Future scope: Algorithm can be implemented for asymmetric key and execution speed of the algorithm can be improved for larger size of plain text.

REFERENCES

1. Rivest,R.,rfc 2268. MIT Laboratory for Computer Science, March (1998)
2. Milind M,Ayush K, Comparison Between DES 3DES RC2 , RC6 BLOWFISH AND AES .In: Proceedings of National Conference on New Horizons in IT - NCNHIT 2013, pp. 143–148. (2013)
3. Akanksha M,A Research paper: An Ascii Value based data encryption algorithm and its comparision with other symmetric data encryption algorithms .,In: International Journal on Computer Science and Engineering , Vol 4, Issuse 9,pp. 1650–1657. (2012)
4. Sheetal C,A Comparative Study of Rivest Cipher Algorithms.,In: International Jour- nal of Information and Computation Technology. , Vol 4, Issuse 17,pp. 1831–1838. (2014)
5. William S.,Cryptography and Network Security - Principles and Practice. fourth edn. Prentice Hall, (2005)

6. Stavroulakis P.,Kilian D.,Luigi L l.,Handbook of Information and Communication Security.In Review of books,Springer, (2010)
7. https://smallbusiness.chron.com/types-symmetric-encryption-algorithms- 54758.html.
8. https://brilliant.org/wiki/symmetric-ciphers/.
9. https://www.garykessler.net/library/crypto.html.
10. https://crypto.stackexchange.com/questions/68460/difference-between-rc2-rc4- rc5-and-rc6

AUTHORS PROFILE

Dr Uma R Pujeri was born in Sangli, India, in 1981. She has received M.Tech degree from PSG Tech college of Engineering Coimbatore in 2008. She has received doctorate degree from Anna University Chennai in May 2017. Her research area is computer network congestion control algorithm. She has worked as a Assistant Professor in Aditya College of Engineering Coimbatore for six years. Currently she is working as a Associate Professor in MIT College Of Engineering Pune Maharashtra as Associate Professor. She has total ten years of teaching experience. She is a Life Member of the Indian Society for Technical Education (ISTE). She has total 10 publications in International journal.

Dr Ramachandra V Pujeri brings in 21 years of professional experience in teaching and research guidance in networking, management and executive leadership in engineering and technology discipline. Ramachandra V. Pujeri, received the BE in Electronics and Communication Engineering from Karnataka University, Dharwad, ME in Computer Science and Engg from PSG College of Technology, Coimbatore, PhD in Information and Communication Engineering from Anna University, Chennai, MBA in Human Resource Management, from Pondicherry University, Pondicherry, in 1996, 2002, 2007 and 2008 respectively. He is active life member of ISTE, SSI, MIE, ACS and IEE. His has written three textbooks. He is an active expert committee member of AICTE, NBA, DoEACC, NACC and various Universities in India. Currently, under him twenty research scholars pursuing their Ph.D. His research interests lie in the areas of Computer Networking, Operating Systems, Software Engineering, Modeling and Simulation, Quality of Services and Data Mining. He has worked as Vice-Principal of KGiSl Institute of Technology. Currently Dr Ramachandra V Pujeri is working as Director of MIT ADT, Pune, India.