Indian Journals of Science and Technology, Vol 9(20), DOI: 10.17485/ijst/2016/v9i20/70417, May 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Performance Evaluation of Encryption/Decryption Mechanisms to Enhance Data Security

Narander Kumar* and Priyanka Chaudhary

Department of Computer Science, B. B. A. University (A Central University), Lucknow - 226025, Uttar Pradesh India;
nk_iet@yahoo.co.in, cpriyanka22@gmail.com

Abstract

Objective: The foremost goal of this paper is to upgrade the security of information and processing speed utilizing symmetric cryptographic technique based on ASCII value while transferring of information. The idea of this paper is to produce an encoded content by giving plain text enter to symmetric cryptographic based on ASCII value and getting decoded text as original text as original text by giving encrypted text symmetric cryptographic based on ASCII value. **Method:** In this paper, we have proposed an algorithm which is established on the ASCII value to encode a plaintext. This algorithm randomly generates a key for the person having a length equivalent to the length of the plaintext. The randomly generated key is modified to one other key via substitution of position of key utilizing a random number and is used to decode decrypt the message of original plaintext. **Finding**: GUI interface was developed using Java Net Beans IDE 8.0. Entire outcomes have obtained using a computer with the following specifications: Intel Core i3 CPU and 1GB RAM. **Improvement:** Besides the proposed algorithm utilized for this exploration, the other chance of utilizing different algorithm will be executed in future work.

Keywords: Ciphertext, Cryptography, Cyber security, Decryption, Encryption, Plaintext

1. Introduction

Data security problem can be small and loacal and that they can be international in scope, regarding computer systems and business enterprise s on each continent[1]. To avert any type of cataclysm, confidential data must be protected from intruders. Cyber security is an important role[2]. Generally, there's a got to shield info from 'praying eyes'. Within the electronic age, the records that might different wise gain or educate a collection or character also can be used against such institution or people. Industrial spying among extremely competitive businesses usually need that in depth security live ought to be place into the place. And people who desire to exercise their non-public facts to avoid struggling the penalties of going towards the desires of individual who attempt to manage. Encryption is the technique of encoding records to make it unpredictable with out unique understanding decryption is the opposite system. The technique of interpreting or transforming an encrypted message is back to its readable and original shape. In encryption, we use various approach to encode the message while in decryption. The previous understanding of key or password is needed to decode the message. A device for Encryption and decryption is referred to as cryptosystem and approach used for enciphering constitute the location of examine of is referred to as cryptography. Cryptography is that the observe of exploitation encoding to hide text. Cryptographic system are represent as variety of process used for transforming encoded text to decoded text, wide variety of key used, approach that of process the encoded text[3].

A. Mathur proposed, an ASCII value based Symmetric encryption algorithm. In this algorithm length of input data and the length of the key used are same. The key

*Author for correspondence

used in the system is entered through user, manually. For manipulating the key used shift operation depends on the length of the input data. The proposed algorithm in[4] takes more execution time in comparison of the proposed mechanism in this paper. For network security, a system is proposed in which we consider a various layer of security rather than supportive single layer which at once may fall through[5]. For secure communication an ant Colony Optimization Key Generation technique is presented which depending on image encryption technique is defined in[6]. A set of cryptographic algorithm is analyzed for ensuring medical records in the connection of mobile applications[7]. A technique is discussed in[8] which uses three different wavelets for encoding an image along with the password. An algorithm is proposed that is based on Message Encoding Algorithm (MsgEncA) for security purposes which produce better performance to compare than existing is discussed in[9]. A security technique is implemented to hide the information, i.e., based on Advanced Encryption Standard is discussed in[10]. Improved Elliptic Curve Cryptography mechanisms are proposed for security purpose that is proposed in[11]. A cryptography algorithm is implementing using through quasigroup-based endomorphic that is defined in[12].

2. Proposed Mechanism

2.1 Encryption Algorithm

There are following steps are defined in the proposed encryption algorithm.

- Input the plain text without space and find the ASCII code value of each character as well as store it in the ASCII plain content (array variable).
- Find the minimum ASCII value in this data and it store in min ASCII value (variable).
- The ASCII value (the simple text), % (Modulus operation) with the minimum ASCII value (the simple text), store it as the mod value of plain text (array variable). (If the mod value of plain text > 16, then again perform value modulus 16 and store the positions where the value of mod content > 16).
- Find the length of the plain text and save it in length (variable).
- Generate a random no of character according to the length of plain text, i.e., 5 random no of character and store it into the key.
- Find the ASCII value of the key and store it in the ASCII key value.
- Now generate a random no according the number of lengths and store the value in a particular location through the generated no. (If two values is reached in the same value the increase the plus one as well as possible).
- Now apply value on the resultant position and store into the new key value.
- Now find the final encryption key and add the again mod value of plain text in the ASCII value of final encryption key and find the cipher text.

2.2 Decryption Algorithm

- There are find minimum ASCII code values of each character from the cipher text.
- Now performing an operation such as subtraction of the the ASCII code values of final encrypt key from ASCII value of cipher.(Add 16 on stored position where we perform again mod operation so the new differences value i.e. where mod operation >16).
- Add min ASCII value of cipher text with the each value of difference which generate from plaintext.

A sequence diagram is presented in Figure 3 to show the Encryption and decryption process. In this process a precondition is sender and accepter has shared a same key and access a repository of technique.

2.2.1 Encryption Process Description

- Sender sends a message (plain text, key, algorithm identifier) to the encrypter.
- Encryptor encrypt the message using with the algorithm that is specified by the sender
- Encryptor creates the cipher text.

2.2.2 Decryption Process Description

- Accepter sends the cipher text and the shared key to the decryptor.
- Decryptor decrypts the encrypted message using the shared key (If the same key has not used the

one used for encryption, the decryption then the process is failing).

- Decryptor creates the plain text that is send by the sender.
- Decryptor sends the plain Message(i.e., decrypt by algorithm) to the Accepter.

All the above said steps are shown in the sequence diagram to clarify all the process which includes two encryption and decryption the data.

Figure 1. Flow chart of proposed encryption/decryption algorithm.

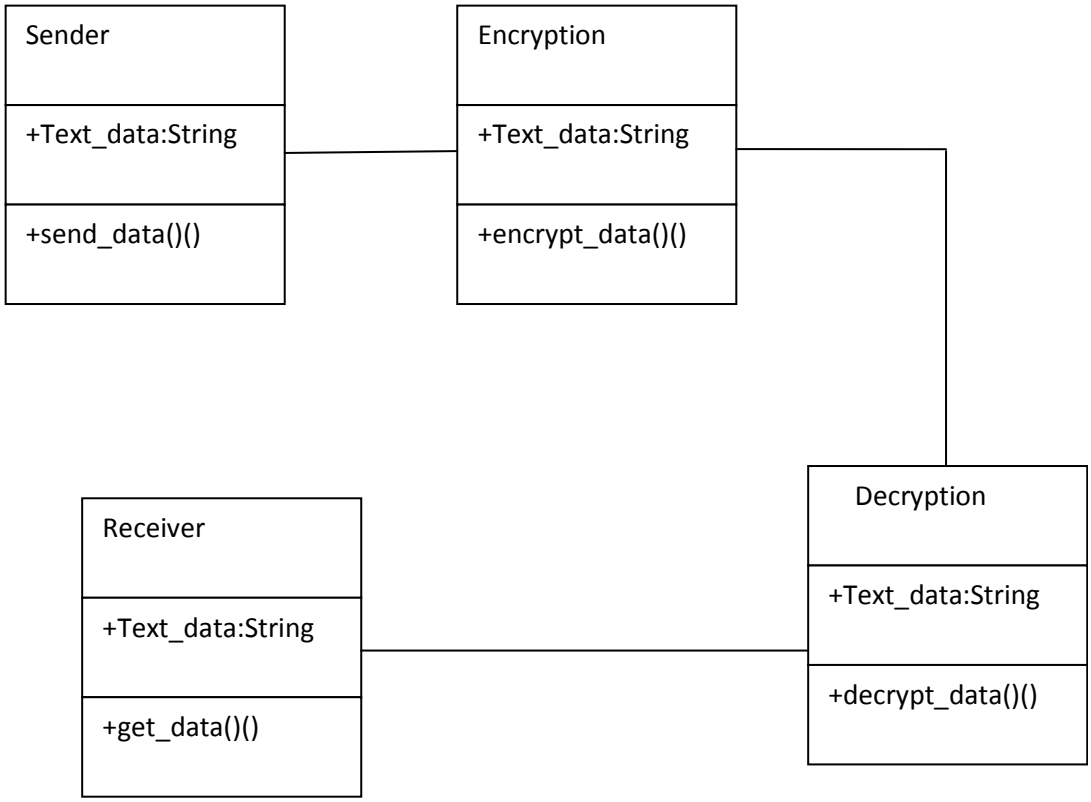

Figure 2. Class diagram for encryption and decryption.

3. Implementation

The algorithm and its GUI interface are developed using Java under Net Beans IDE 8.0. The message is sent into its corresponding ASCII value. The efficiency of the algorithms is defined in this section. All the results have been obtained using a computer with the following specifications: Intel Core i3 CPU and 1GB RAM.

4. Working Example

Now we input a text value is Swati. This is encrypted and decrypted in following manner.

4.1 Encryption Process

Step 1: Input the plain text without space such as swati

Input	s	W	a	t	i
ASCII Content	115	119	97	116	105

Step 2: Find minimum ASCII value

Minimum=97

Step 3: Perform modulus operation on each data

Modvalue[1]	=	115	%	97	=>	18
Modvalue[2]	=	119	%	97	=>	22
Modvalue[3]	=	97	%	97	=>	0
Modvalue[4]	=	116	%	97	=>	29
Modvalue[5]	=	105	%	97	=>	8

In this calculation two location find value more than 16 then again perform mod operation in these two locations.

Modvalue[1]	=	18	%	16	=>	2
Modvalue[1]	=	22	%	16	=>	6
Modvalue[1]	=	29	%	16	=>	13

Step 4: Generate key for encryption (key is generated randomly by system)

Key	A	b	c	d	e
ASCII value	97	98	99	100	101
Genarate random no.	4	2	3	5	1

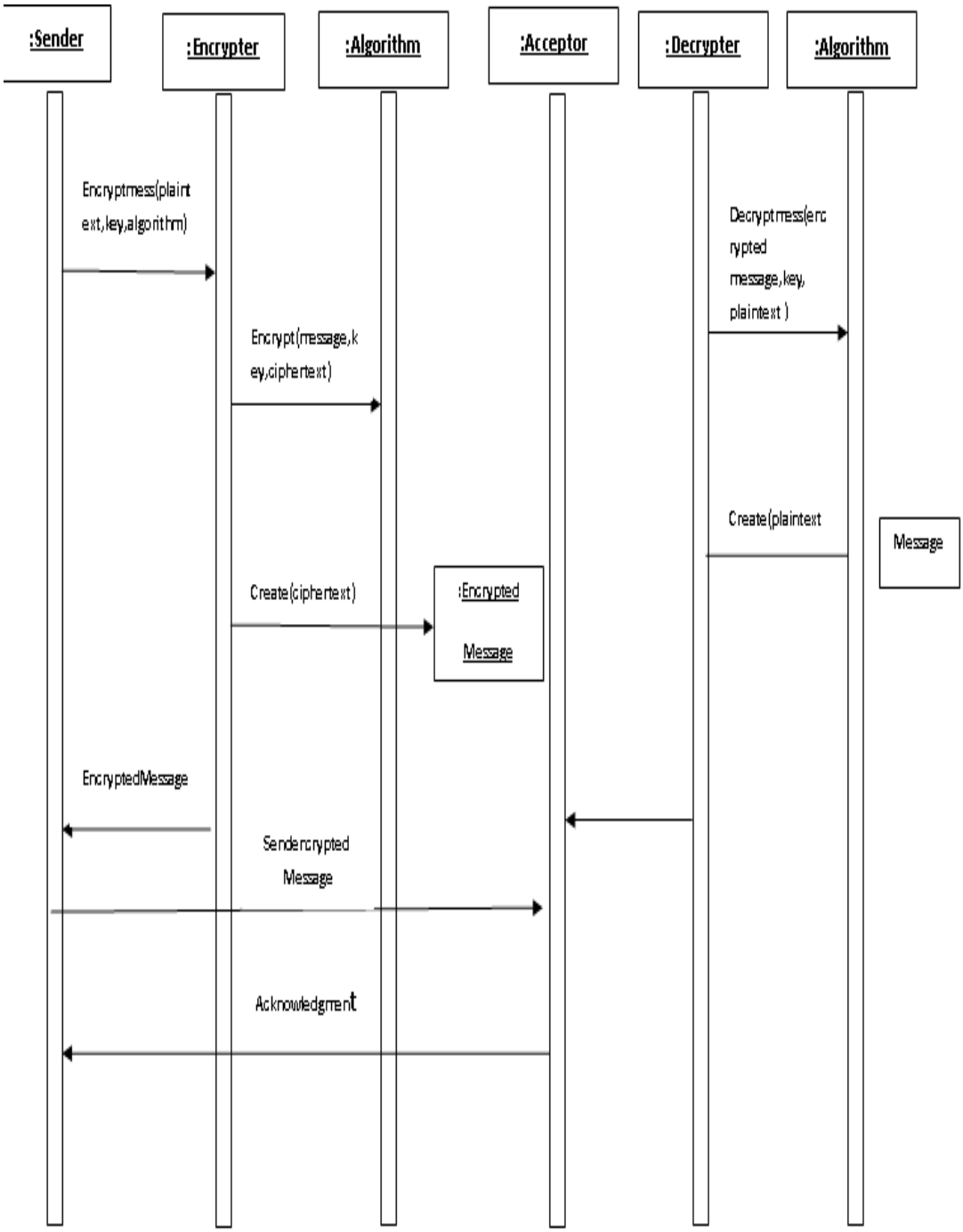

Figure 3. Sequence diagram for encrypting and decrypting a message through proposed algorithm.

Figure 4. Output screen for character input.

Store key value on the particular generated number

Location[1] = 101
Location[2] = 98
Location[3] = 99
Location[4] = 97
Location[5] = 100

Step 5: Add mod value and key value

Location[1] = 101 + 2 => 103
Location[2] = 98 + 6 => 104
Location[3] = 99 + 0 => 99
Location[4] = 97 + 13 => 110
Location[5] = 100 + 8 => 108

Step 6: Find cipher text

Final cipher value	103	104	99	110	108
Cipher text	g	h	c	n	l

4.2 Decryption Process

Step 1:

Final cipher value	103	104	99	110	108
Cipher text	G	h	c	n	l

Step 2: Minimum =97

Step 3: Add 16 on stored position where we perform again mod operation so the new differences value i.e., where mod operation >16)

Location[1]	=	103	+	16	=>	119
Location[1]	=	104	+	16	=>	110
Location[1]	=	110	+	16	=>	126

Step 4: Find plain text

Cipher ASCII value	119	110	97	126	108
ASCII final encrypt key	101	98	99	97	100
Difference	8	12	2	28	7
Plain text ASCII value	115	119	99	125	105
Plain text	s	w	a	t	i

5. Efficiency Analysis

The Figures 1-8 are showing the performance during the implementation of the proposed algorithm with a number of different data values of text and sizes of a wide range. The performance matrics are shown encoding and decoding time. The encryption time is defined as, the time is taken for generating a cipher text from plaintext and decryption time is defined as, the time taken for generating plain text form the cipher text. In Figure 4, author used an input data of variable lengths with key of variable length for generating the cipher text and corresponding execution time has been calculated. The proposed algorithm has taken time for encryption is shown in Figure 5. The proposed algorithm has taken time for decryption is shown in Figure 6. In this algorithm we use the randomly generated a key value instead of shifting to the key value as described in to increase the level of security. In Figure 7, shows the results that time is taken for the encryption or decryption process by Proposed Algorithm are less than encryption or decryption time, which is compared previous proposed an algorithm[4]. In Figure 8, shows the result of throughput of total execution (Encryption/Decryption) time of proposed Mechanism.

6. Performance Factors

There are some performance parameters of proposed algorithm such as security level, key length and execution time has considered evaluating the performance of the proposed algorithm.

Execution Time: In this proposed algorithm execution time (encryption/decryption) is less than previous algorithm which described in[4].

More Secure: With the help of random number generation of the key is more secure cipher text to provide security.

Variable Key length: In this proposed algorithm variable key length is considered which improved level of security and compared with the fixed length variable key mechanism.

Table 1 is defined the encryption and decryption time for proposed algorithm and existing algorithm. The execution is defined as the time is taken for generating a cipher text from plaintext and plain text form the cipher text. Table 2 is defined the comparison between execution time for proposed algorithm and existing algorithm.

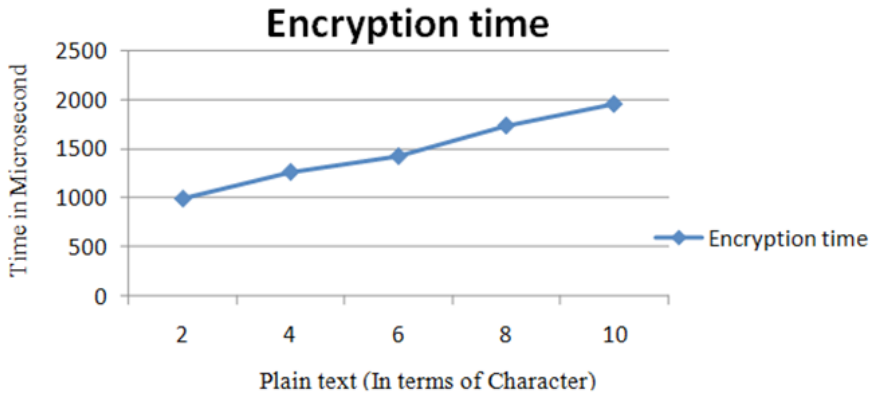

Figure 5. Time taken for encryption in proposed algorithm.

Table 1. Encryption and decryption time of proposed algorithm

Encryption Algorithm (character)	Encryption time (Microsecond)	Decryption time Microsecond)
2	1000	1000
4	1270	1160
6	1430	1230
8	1740	1340
10	1958	1620

Table 2. Execution Time of Proposed and Existing Algorithm[4]

Plain Text (Character)	Previous Algorithm Execution time (Microsecond)	Proposed Algorithm Execution time (Microsecond)
2	3220	2000
4	3679	2430
6	3861	2660
8	4748	3080
10	5543	3578

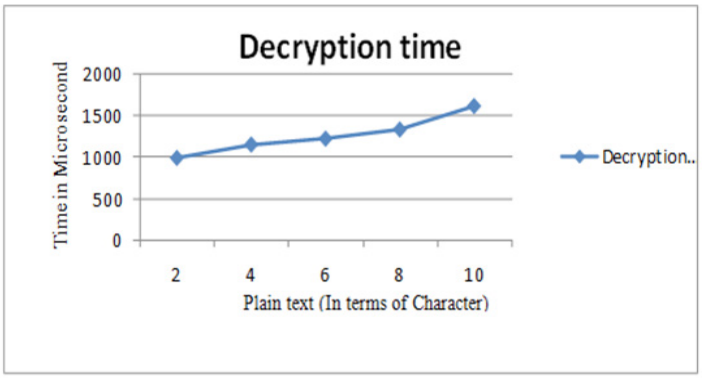

Figure 6. Time taken for decryption in proposed algorithm.

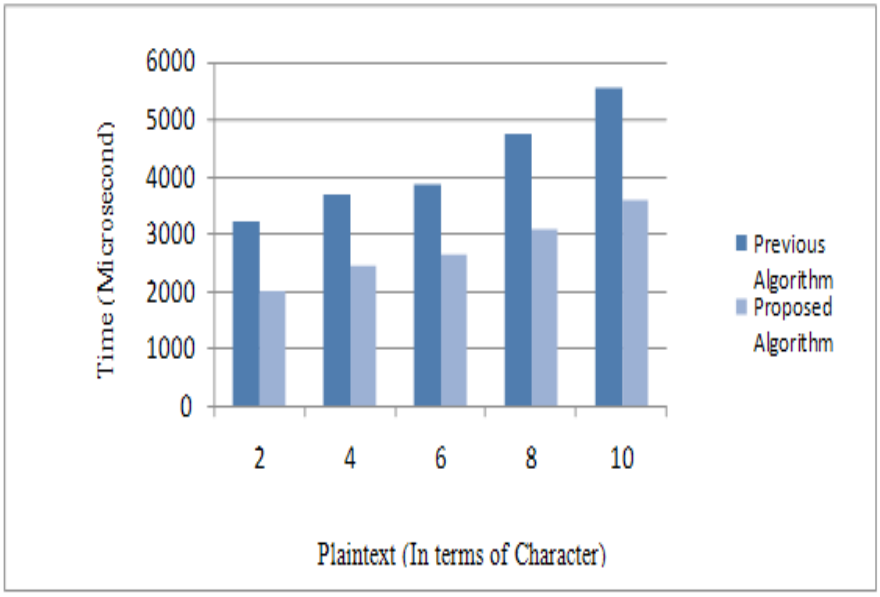

Figure 7. Encryption and decryption time comparison between existing algorithm5 and proposed algorithm.

After find the Encryption and decryption times checked there are also determine throughput that is discussed in[13] how to calculate a through put of particular algorithm.

Where,

$$\text{Throughput} = \frac{\text{Size of encrypted text in megaby}}{\text{Time required for encryption in sec}}$$

After applying this formula in our proposed algorithm, we have found following result that is shown in Table 3.

Table 3. throughput of proposed algorithm

Plain Text (In terms of character	Data (Size in MB)	Execution time (Second)	Throughput
2	.0009550	.002	.4775
4	.0009570	.00243	.3938
6	.0009609	.00266	.3612
8	.0009648	.00308	.3132
10	.0009667	.00358	.2700

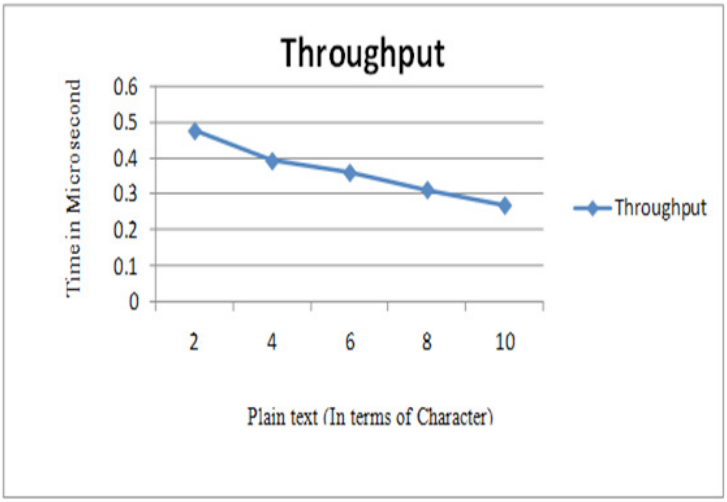

Figure 8. Throughput of total execution (encryption/decryption) time of proposed mechanism.

7 Conclusion

The defined algorithm will gives the advance field of research on cryptography that is based symmetric cryptography based on ASCII code value. These new algorithms for text encrypt and decrypt using ASCII code value that is very efficacious methodology. This algorithm is providing more security and reliability.

8. Comparison and Future Scope

From the results, we've evaluated that our proposed encryption algorithm is furnished better conclusion as compare to the prevailing set of rules so the time taken for encryption and decryption of our designed algorithm is lesser than existing algorithm. In the motive of safety our algorithm boom safety and also time is reduced. If any person gives the focal point on safety of records then they could use our designed technique. The primary benefit is that it's far having variable length key technique to make it difficult for intruder to become aware of. So the element of security is high and the execution time is lesser as compared to above mentioned existing encryption systems. The machine can be in addition prolonged to encrypt the multimedia data including audio documents, video documents and photos and so on. The principle purpose of this proposed algorithm is protection. There are numerous destiny scope of ASCII fee based text statistics encryption and decryption. No unauthorized person can hack the facts. In the current technology, new technologies had been upgraded time to time so there's wanted to changes this algorithm. This algorithm may be similarly progressed through a number of methods in future.

9. References

1. Smith RE. Elementory Information Security. Barlington: Jones and Bartlett Learning; 2013.
2. Elena A. A novel text encryption algorithm. Research in Computing Science. 2013; 68:99–101.
3. Ranjan B. Information theory, coding and cryptography. New Delhi: Tata-McGraw Hill; 2008.
4. Akansha M. An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms. International Journal on Computer Science and Engineering. 2012; 4(9):1650–6.
5. Vincent PMDR. Iqbal SA, Bhagat K, Kushwaha KK. Cryptography: A mathematical approach. Indian Journal of Science and Technology. 2013; 6(12):5607–11.
6. Swapna BS, Emeritus NS. A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology. 2015; 8(3):216–21.
7. Jorge EC, Diego FS, Yeison FT. Study of cryptographic algorithms to protect electronic medical records in mobile platforms. Indian Journal of Science and Technology. 2015; 8(21):1–7.
8. Parthasarathy MB, Srinivasan B. Increased security in image cryptography using wavelet transforms. Indian Journal of Science and Technology. 2015 Jun; 8(12):1–8.
9. George DIA, Geetha JS, Mani K. Analysis and enhancement of speed in public key cryptography using message encoding algorithm. Indian Journal of Science and Technology. 2015 Jul; 8(16):1–7.
10. Thasneem PTS, Vigneswaran. FPGA implementation of hiding information using cryptography. Indian Journal of Science and Technology. 2015; 8(18):1–6.
11. Regina TSR, Britto S, Ramesh K. Enhanced elliptic curve cryptography. Indian Journal of Science and Technology. 2015; 8(26):1–6.
12. Monisha S, Kowar MK. Generation of quasigroup for cryptographic application. Indian Journal of Science and Technology. 2009; 2(11):35–6.
13. Nidhal AKEl. Text encryption based on singular value decomposition. European Academic Research. 2014; 2(4):4631–42.