ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 12(5), DOI: 10.17485/ijst/2019/v12i5/141758, February 2019* ISSN (Online) : 0974-5645

Securing Sensitive Information Files based on Session Keys using Numeric Encryption and Bit Scrambling

K. N. Sivabalan[1] and S. Balakrishnan[2]

[1]Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore - 641008, Tamil Nadu, India; knsbalan1979@gmail.com

[2]Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore - 641008, Tamil Nadu, India; balkiparu@gmail.com

Abstract

Objectives: The study of proposed method deeply focuses on encrypting and decrypting the file contents using session based keys. **Methods/Statistical Analysis:** Encrypt_transmission and decrypt_receiver algorithms are used. **Findings:** Transmission of information through the network in the highly technological era has become a routine process. Transmission of information includes personal details, credit card and debit card numbers, Account transaction and other sensitive issues. As a result securing this type of sensitive information from hackers is considered as a daunting task. Most of the security techniques are vulnerable these days. Taking into account all the above factors an efficient algorithm has been proposed based on the user login for encryption and decryption. The algorithm works uniquely for every user. **Application/Improvements:** This algorithm is also suitable for financial related transactions.

Keywords: Decryption, Encryption, Key

1. Introduction

Rapid advancement in the spectrum of technology has facilitated communication in a rapid phase despite the distance in geographical locations. As the technology grows threats also grow considerably. The major challenge posed today is how to safeguard sensitive information such as credit card details, personnel details from techies with nefarious intent. Even the most secured and shielded information has been vulnerable to potent hacking tools. The system becomes vulnerable because the same encryption technique or methodology is applied for every content during transmission. So that the brute force attack can be easily done on information to interpret it. Many academicians and professional researchers have done fabulous work for information security. In[1] proposed discussed how the authors of RSA algorithm used public and private key encryption using two keys. He also differentiates between public and private keys. In[2] proposed explained how the security of RSA algorithm can be done by exchanging keys between the users in a transparent way. In[3] proposed discusses the modified and enriched RSA algorithm with security using 'n' prime numbers. And also suggests n prime numbers are not breakable and decomposable and assures high security and reliability. In[4] proposed described the various analysis of RSA algorithm during the securing process compared to other algorithm. She has also used some computational metrics to corroborate her views. In[5] proposed discuss how RSA algorithm can be used to encrypt and decrypt speech data. He initially uses bangla words and stored in Wav file later it is converted and stored in text files. In[6] proposed suggested how RSA algorithm can be used to protect information using specific block size. She also highlighted the issues in other methods related to encryption and decryption. In[7] proposed mentioned about the enhanced RSA algorithm security and also focuses on the computational complexity about the algorithm during the network transmission.

*Author for correspondence

In[8] proposed sheds light on secure communication using digital signatures. Mentions how message authentication code can be used to protect the message integrity. In[9] proposed has done a complete analysis on AES, DES and RSA algorithm. Based on the analysis recommendation has been given which algorithm is best in what category. In[10] proposed mentioned the method of digital image encryption using RSA algorithm. He also makes a complete analysis with blowfish and DES algorithms.

2. Proposed Method

The proposed method deeply focuses on encrypting and decrypting the file contents using session based keys. The user logs in with username and password which fetches him a unique session key. The sensitive information in the file will be read automatically and each character in the file will be assigned a numerical value based on python dictionary data structure the session key is added with numeric value which produces a modified numeric value. Now each numeric value will be represented in binary format and then least and most significant bit will be swapped. This information is transmitted to the receiver end. The receiver module performs bit swapping and the session key is subtracted from the numerical value. After this process the corresponding numerical value will be represented by appropriate character using python dictionary data structure to restore the original information. This method is so secured because session key is unique for every user and the decryption mechanism unlocks only when appropriate session is released.

3. Proposed Algorithm

Algorithm Encrypt_Transmission

```
session_key=Access_Database(userinfo)
dict_encrpt={A:100,B:120,C:123,……..,Z:45}
data=readfile(file)
for i← 1 to len(data) do
    {
    enc_char←dict_encrypt[data[i]]
    enc_char←enc_char + session_key
    enc_char←char_to_binary(enc_char)
    swap_enc←bit_swap_MSB_LSB(enc_char)
    swap_enc←swap_enc||session_key
    transmit_data(swap_enc)
    }
```

END Encrypt_Transmission

Algorithm Decrypt_Receiver

```
data←receive_data(swap_enc)
dict_decrypt={100:A,120:B,123:C,……..,45:Z}
session_key←extract_data(data)
enc_data←extract_data(data)
enc_data←bit_swap_MSB_LSB(enc_data)
enc_data←binary_to_char(enc_data)
for i← 1 to len(enc_data) do
    {
    dec_char←enc_data[i] - session_key
    dec_char←dict_decrypt[dec_char]
   display(dec_char)
    }
```

END Decrypt_Receiver

3.1 Encoding Module

The database contains username and password and also a unique Session key(S) for every user. When the user logs in the unique Session key is taken out and the Algorithm automatically reads the File which is getting transmitted. Each character in the file will be assigned a numeric value which is based on the python dictionary data structure. Encoding module is given in the Figure 1. Let us Assume N is the numeric value X in the character of file and Y is the python dictionary for representing character into number and F is the function for conversion then N can be obtained as

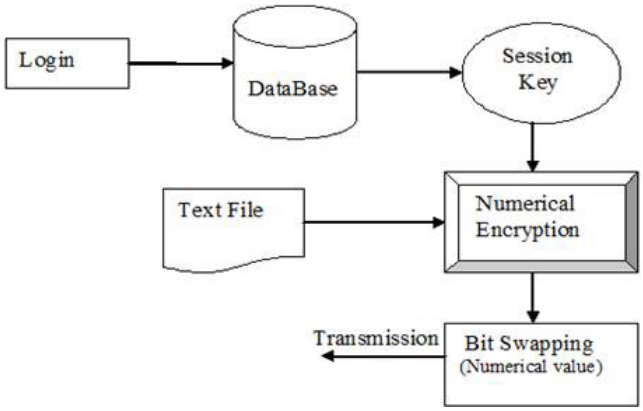

Figure 1. Encoding Module.

N←F(Y[X])

The above process is repeated for each character of file. Let us Assume E is the encrypted character of the file and S is the session key extracted from database then the modified numeric value will be generated as

E=N + S

Now E is the new encrypted character. This number has to be converted into equivalent binary number with the following pattern

$$E=b_7b_6b_5.....b_1b_0$$

Now the binary pattern will be subjected to bit swapping where b7 to b4 is swapped on right and b3 to b0 are pushed on left side. The bit pattern appears as follows

$$E=b_3b_2b_1b_0\ b_7b_6b_5b_4$$

Now the swapped bit pattern is written inside the file and session key is sent as digital signature by merging it inside the file. The process is as follows

W(File[i],E)||S

W mentions write and E mentions the binary pattern of the corresponding character. The above process is repeated for every character in the file and then key is attached with the file and then it will get transmitted.

3.2 Decoding Module

After receiving the file every 8 bit is received in a sequence so that the pattern can be received the format. Let Z be the received binary pattern such as (Figure 2).

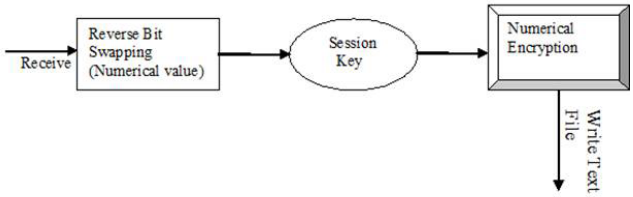

Figure 2. Decoding Module.

$$Z=b_3b_2b_1b_0\ b_7b_6b_5b_4$$

Now interchange the first four and the last four bits which is mentioned as Z1

$$Z1=b_7b_6b_5b_4\ b_3b_2b_1b_0$$

After the particular character is converted after bit swapping the concerned character is subjected to alteration with key value. This character is considered as K1 and new character after applying key is called O,

O=K1 - key value

The converted value O is written back to file to represent the original message in the file,

Alg(W(file(i),O))

W is used to mention write and O is the new character file(i) represents the unique character

4. Experimental Results

The proposed Algorithm is implemented with Python where two modules of python program is developed one focuses on encryption and transmission and the other concentrates on decryption and reception. The transmission module fetch the session key from database after login then it prints the contents of the transmitted file as well as its encrypted contents (shown in the Figure 3).

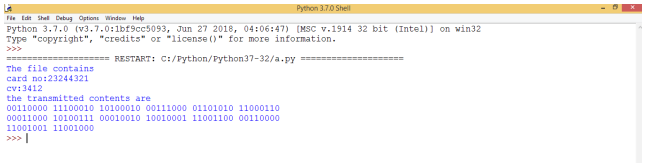

Figure 3. Snap shot of transmission module.

5. Conclusion

The proposed method above can be efficiently used in personnel information transmission through wired or wireless media. Since the method of cryptography is not uniform for every user brute force attack is highly impossible. It is not vulnerable to threats such as rainbow attacks. This algorithm is also suitable for financial related transactions.

6. References

1. RSA Algorithm. Available from: https://www.di-mgt.com.au/rsa_alg.html. Date accessed: 09/06/2018.
2. Saranya, Vinothini, Vasumathi. A Study on RSA Algorithm for Cryptography. International Journal of Computer Science and Information Technologies. 2014; 5(4):5708-9.
3. Vivek TVS, Anandam D, Anil G, Sreenivasulu B, Lakshma Reddy V, Batchnaboyina MR. Modified RSA Algorithm for (Wi-Fi) Security Protocol. International Journal of Computer Science and Information Technologies. 2015; 6(3):2097-8.
4. Preetha M, Nithya M. A Study And Performance Analysis Of RSA Algorithm. International Journal of Computer Science and Mobile Computing. 2013; 2(6):126-39.
5. Rahman M, Saha TK, Bhuiyan AA. Implementation of RSA Algorithm for Speech Data Encryption and Decryption. International Journal of Computer Science and Network Security. 2012; 12(3):74-82.

6. Data Encryption and Decryption Using RSA Algorithm in Network Environment. Available from: https://www.techrepublic.com/resource-library/whitepapers/data-encryption-and-decryption-using-rsa-algorithm-in-a-network-environment/. Date accessed: 2014.
7. Patel SR, Shah K. Security Enhancement and Speed Monitoring of RSA Algorithm. International Journal of Engineering Development and Research. 2014; 2(2):2057-63.
8. Kapoor V. Secure Communication using RSA Algorithm for Network Environment. International Journal of Computer Applications. 2015; 118(7):6-9.
9. Mahajan P, Sachdeva A. A Study of Encryption Algorithms AES, DES and RSA for Security. Global Journal of Computer Science and Technology Network, Web & Security. 2013; 13(15):1-9.
10. El-Deen AET, El-Badawy ESA, Gobran SN. Digital Image Encryption Based on RSA Algorithm. IOSR Journal of Electronics and Communication Engineering. 2014; 9(1):69-73. https://doi.org/10.9790/2834-09146973