IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A SYNTHESIS TEXT ENCRYPTION TECHNIQUE USING DSKE (Deep Substitution and Key Encryption Algorithm)

[1]K.JosephDileep, [2]Jhansi Rani Singothu,

[1]Student (M.Tech) Cyber Security & Data Analytics, [2]Assistant Professor of Dept. Computer Science & System Engineering,
[1]Dept. of Information Technology and Computer Applications,
[1]Andhra University College of Engineering, Visakhapatnam, India

Abstract: Nowadays the usage of computer technology and the internet has increased rapidly. We are using this improvised network in data transfer and storage of data for faster communication. However, where there is a positive there will be negatives also, in this safe communication/transmission of data is always of concern, and new techniques keep developing to safeguard the data. So, to provide secure data transfer we propose a synthesis text encryption technique that is Deep Substitution and Key Encryption algorithm(DSKE).DSKE is the combination of DSEM[1]and RSA. DSKE splits the user data into two parts and one half is sent to DSEM and the other half is sent to the RSA algorithm. This paper comprehensively explains the DSKE cryptic process.

Index Terms - encryption, decryption, DSEM, RSA, Cryptography

I. INTRODUCTION

Cryptography plays a major role in this computerized world, which is like for secure data storage, and data transfer between the networks and cloud safely. In cryptography there were substitution techniques. They encoded data using the substitution of units in the plaintext with the relevant ciphertext units. Here units may be a single letter or pair of letters or mixture of letters. After the substitution the user sends it to the receiver through the network. The receiver decodes ciphertext by performing the inverse substitution. To provide secure data transmission and protect data we proposed the new synthesize encryption algorithm that is Deep Substitution and Key Encryption algorithm (DSKE). DSKE encrypts and decrypts the data using Deep Substitution Encryption Method (DSEM) and RSA. DSEM is a substitution technique. It substitutes the user data with different types of cipher text. RSA is an Asymmetric Cryptic Process And also, Public key Encryption.

DSEM algorithm: In this method, we encode the plaintext using repeated substitution process. It is a bit–by-bit stream algorithm. DSEM performs the five substitution phases. They are first phase is ASCII code substitution phase, second is Periodic element substitution phase, third is Flower name substitution phase, fourth is HTML color name substitution phase and the fifth phase is color hex code substitution phase. The DSEM uses the same key for encryption and decryption.[1]

RIVEST-SHAMIR-ADLEMAN (RSA) : The RSA algorithm is an asymmetric cryptographic algorithm that uses two different keys, the public key and the private key. A public key is a key used to encrypt messages and is known to anyone while a private key is a key used to decrypt the encrypted message and is known only by the sender and receiver.

II.LITERATURE REVIEW:

B. Lavanya, V.Thamizh Thendral, proposed A novel data ciphering method for secure cloud storage. In this they implemented Deep Substitution Encryption Method(DSEM) to encrypt and decrypt the data they perform five different substitution phases using key.[1]

Ghada Farouk Elkabbany and Mohamed Rasslan, stated the security issues in distributed computing system models, explained about distributed system and computing then its types in detail. Some security issues are Confidentiality, Data integrity, Authentication, Authorization and Access control, Non-Repudiation and Accountability. And they mentioned security attacks of distributed systems such as Distributed Denial of Service (DDoS) Attack, Identity Attack in Distributed System and etc., [2].

Manoj Kumar and Nikhil Agrawal analyzed the different security issues and attacks of the distributed system. Authors mainly focused on three securities issues in the distributed system and that security issues concerns about the Security of Information, Physical security in distributed system and Security of network and authentication policy. And describe the few methodologies to solve the issue presents in the distributed system [3].

Eng. Hashem H. Ramadan and Moussa Adamou Djamilou are using AES and RSA algorithms for file encryption and store into cloud storage. First, using AES to encrypt the data and then encode by the RSA algorithm. Decryption also performs the same as encryption technique [4].

Venkat Krishna Pavan Kalubandi and Yamuna M, proposed Byte Encryption of a string using periodic table. The periodic elements are randomly assigned to each character in the original text. Decrypt the encoded text the same way as encoded using key value but in the reverse order. Periodic table not using generally other than it is used in drug encryptions, encode chemical composition of drugs .[5]

Xin Zhou and Xiaofei Tang, propose an implementation of a complete and practical RSA encrypt/decrypt solution based on the study of RSA public key algorithm.[6]

III. ALGORITHMS:

DSEM algorithm:
DSEM key generation: Initially, the key value is fixed as the ASCII value of given user plain text. Then we add that key value with an increment variable so each and every time we get a different key value and there is no repetition will occur for the same letter. To get the inverse key value we subtract the increment variable from the key value.[1].

Deep Substitution Encryption Method:

ASCII code substitution phase: Initially we get the given user plaintext and convert it as ASCII value.[1]
Periodic element substitution phase: Using key value to get the periodic element from the substitution table then we substitute the element in the place of corresponding its ASCII values.[1]
Flower name substitution phase: Based on key value we retrieve the flower name then we replace periodic element as flower name.[1]
HTML color name substitution phase: In this phase, use the key to get the HTML color name from the substitution table then we swap the flower name as HTML color name.[1]
Color hex code substitution phase: This substitution phase is to replace the color name to its corresponding hex code value using key value.[1]

RIVEST-SHAMIR-ADLEMAN (RSA) : Choose two prime numbers p and Q.

1. Multiply p and q to generate n. n will be used as the modulus.
2. Calculate ϕ (n) = (p-1) * (q-1). ϕ (n) is the Euler's totient function. ϕ (p) is the number of positive integers less than p and relatively prime to p.
3. Choose a number e such that it is relatively prime to ϕ (n).
4. Find d such that it is a multiplicative inverse of e, d = e−1 mod ϕ (n).
5. (e,n) is the public key and (d,n) is the private key.
6. To encrypt, we use the formula (Ciphertext) =$(\text{Plaintext})^{e} \bmod n$.
7. To decrypt, we use the formula (Plaintext) = $(\text{Ciphertext})^{d} \bmod n$

IV. PROPOSED METHOD:

The Proposed work is Deep Substitution and Key Encryption algorithm and simply referred to as "DSKE". Deep Substitution and Key Encryption algorithm is a synthesis encryption technique that is synthesis of two algorithms called RSA (**RIVEST-SHAMIR-ADLEMAN**) and Deep Substitution Encryption Method(**DSEM**). From DSKE the word "Deep Substitution" derived from the Deep Substitution Encryption Method and "Key Encryption" originated from the RSA algorithm because it is a public key encryption technique. The proposed method splits the plaintext into two parts and encodes the data by DSEM and RSA algorithms, after encrypting it will send it to the receiver. And the receiver will decrypt it same way by the DSKE algorithm.

DSKE Encryption cryptic steps are:

1) Split plaintext data step,

2)left half encryption/DSEM step,

3) Right half encryption/RSA step, and

4) Merge encrypted data step.

The Deciphering Process Includes:

1) Split encoded data step,

2) Left half/DSEM decryption data step,

3) Right half/RSA decryption and

4) Merge decrypted data step.

The DSKE algorithm is explained step by step in this section.

DSKE encryption procedure: Initially, DSKE gets cloud user data.

Split original text: Equally divide the given user text as Right half and Left half. Example: User text is CLOUD. From CLOUD, CL has left half data and OUD as right half data split by first step. If cannot be divided equally like e.g. CLOUD, DSEM split the "CL" as left half and OUD as right half or "CLO" as left and "UD" as right half.

Left half/ DSEM encryption step: To encode the right half data sent to the Deep Substitution Encryption Method. Right half data is encoding as mentioned in Algorithm.

For an example: Left half "CL"

DSEM cipher is: ['66FF66','C40233']

Right half/RSA encryption step: To cipher, the left half text is directed to the RSA algorithm. Left half data is ciphering as described in Algorithm.

For an example: Right half : "OUD"
RSA cipher: [962, 680, 1139]

Merge cipher data step: In this step, we merge the split encrypted text and upload into the Cloud.

For an example:: "CLOUD" cipher:
['66FF66','C40233',962, 680, 1139]

V.ARCHITECTURE:

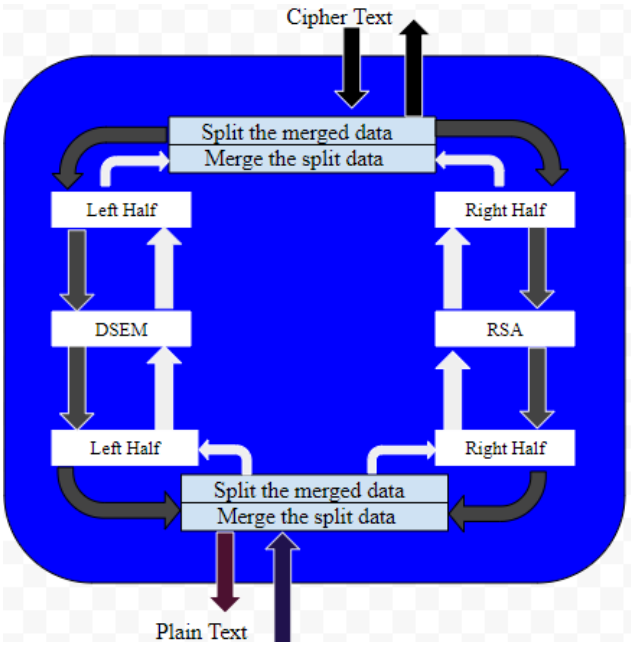

Fig. 1. Architecture of Deep Substitution and Key Encryption

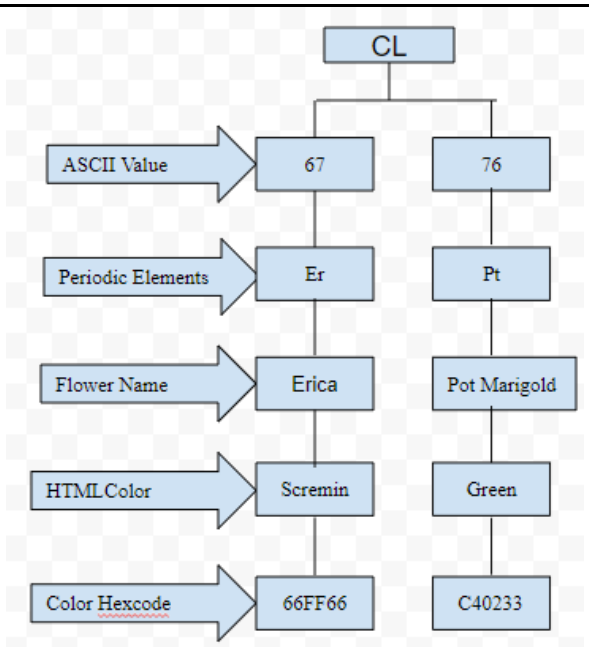

Fig. 2. Encryption process of DSEM

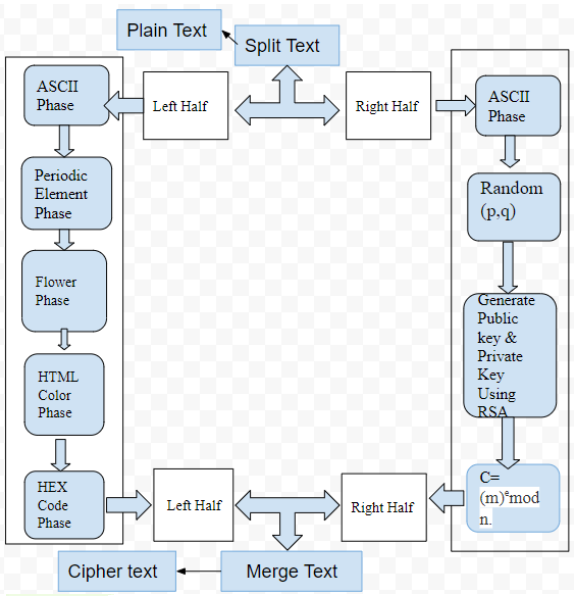

Fig. 3. DSKE encryption

DSKE Decryption Procedure:

To decode the unreadable text, we follow the same procedure as the encryption process of DSKE. Split decrypted Text step: First, the encrypted text is split up as right half and left half. And the below example defines the splitting process.

For an example :: “CLOUD” cipher:
[‘66FF66’,’C40233’,962, 680, 1139]

Splitting Data:
[‘66FF66’,’C40233’,962, 680, 1139]

[‘66FF66’,’C40233’] Left Half

[962,680,1139] Right Half

Left half/ DSEM decryption step: The right half data is sent to DSEM for decipher and decryption perform as defined in Algorithm

For an example: DSEM encoding is:

['66FF66','C40233']

DSEM decoding is: CL

Right half/ RSA decryption step: The left half data is sent to RSA for deciphering the text and decode as defined in Algorithm.

For an example: RSA encryption:
[962, 680, 1139]

RSA decryption: OUD

Merge deciphered data step: Finally, merge the decrypted right half and left half text together and sent to the cloud user.

For an example:
Merged decoded data is CLOUD

IV. RESULTS :

```
In [1]: runfile('C:/Users/DJ/Desktop/prj/DSEMTDES.py', wdir='C:/Users/DJ/Desktop/prj')

Enter 1 For Encryption and 2 for Decryption
1

Enter a TextCLOUD
The original string is : CLOUD
The first part of string : CL
The second part of string : OUD
 ASCII Value is :
[67, 76]
Encryption key:
[68, 78]
Periodic Element Substitution: ['Er', 'Pt']
Flower Name Substitution: ['Erica', 'Potmarigold']
Color Substitution: ['scremin', 'green']
DSEM Encrypted text ['66FF66', 'C40233']
p = 89
q = 17
n=1513
e = 85
d = 381
The original list : OUD
The ascii list is : [79, 85, 68]
Encrypted message = [962, 680, 1139]
['66FF66', 'C40233', 962, 680, 1139]
```

Fig 1: Encryption

```
In [1]: runfile('C:/Users/DJ/Desktop/prj/DSEMTDES.py', wdir='C:/Users/DJ/Desktop/prj')

Enter 1 For Encryption and 2 for Decryption
2

Enter Cipher Text'66FF66','C40233',962,680,1139
The first part of string : ["'66FF66'", "'C40233'"]
The second part of string : ['962', '680', '1139']
['66FF66', 'C40233']
[67, 77]
[66, 75]
Color Substitution: ['66FF66', 'Hydrogen']
Flower Name Substitution: ['Erica', 'Iridium']
Periodic Element Substitution: ['Er', 'Ir']
['Er', 'Ir']
[67, 76]
Ascii List [67, 76]
Decrypt Text CL

Enter d value381

Enter n value1513
[79, 85, 68]
Ascii List [79, 85, 68]
Decrypt Text OUD
OUD
CLOUD
```

Fig 2. Decryption

Conclusion:

In this concept, we split the user text then divided the data and encrypted by two different algorithms so attackers cannot break the DSKE algorithm. Although if they hack the one side of enciphered data and the other half would be near to impossible to decipher. Because the two encryptions are not related to one another and both encoding techniques use different keys. To break DSKE algorithm it takes more time to hack the user data. So practically it is not possible to crack the algorithm. And DSKM methods use the unique kind of substitution techniques so attackers first have to get the knowledge about that substitution techniques otherwise they cannot break the DSKE method. So, considering the above all reasons DSKE is the best encryption algorithm .

REFERENCES

[1] B. Lavanya, V.ThamizhThendral. “A novel data ciphering method for secure cloud storage”, Accepted for publication in “The IEEE sponsored International Carnahan Conference on Security Technology”, 2019 .

[2] El-Kabbany, Ghada & Rasslan, Mohamed. (2016). Security Issues in Distributed Computing System Models. Security Solutions for Hyper connectivity and the Internet of Things, Advances in Information Security, Privacy, and Ethics (AISPE). 36. 211-259. 10.4018/978-1- 5225-0741-3.ch009.

[3] Kumar, Manoj, and Nikhil Agrawal. "Analysis of Different Security Issues and Attacks in Distributed System A- Review." International Journal of Advanced Research in Computer Science and Software Engineering 3.4 (2013).

[4] Eng. Hashem H. Ramadan. “Using Cryptography Algorithms to Secure Cloud Computing Data and Services.” American Journal of Engineering Research (AJER), vol. 6, no. 10, 2017, pp. 334–337

[5] Venkat Krishna Pavan Kalubandi1, Yamuna M2 , Byte Encryption of a String using Periodic Table, International Journal of Computer Science and InnovationVol. 2016,no. 1, pp. 98-106 ISSN: 2458- 6528Copyright © Infinity Sciences.

[6] Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," Proceedings of 2011 6th International Forum on Strategic Technology, Harbin, Heilongjiang, 2011, pp. 1118-1121, doi: 10.1109/IFOST.2011.6021216.