A New Cipher Process With Double Encryption

Addepalli Hari Narayana,
4th year, Electrical Engg.
IIT Indore.

Dr. Addepalli V. N. Krishna,
Professor, CSE, Faculty of Engineering,
CHRIST (Deemed to be university)

ABSTRACT

This paper deals with cryptographic study which involves differentiation and integration process for converting the plain text into a larger number (Cipher Text) with the help of keys. Three Keys are being used for encryption process. A primary Key is used which is to be shared among the sender and receiver which is a onetime process. A random sequence is used as a session key which is to be modified as per encryption of plain text. This Modified session key is encrypted with primary key to be sent to receiver. A secondary key is also to be shared between sender and receiver which help in identifying the number of differentiations and Integrations in the encryption and decryption process. Thus the work generates two cipher texts, one getting converted from plain text and the other by encrypting session key with primary key.

Keywords: Double Encryption, Differentiation, Integration, Session Key, Secondary Key.

I. INTRODUCTION

The significance of encrypting data is of more relevance in the light of Mushrooming applications like Communications, Defense, E commerce, on line voting etc. where vast amounts of data are stored in varied and distributed environment. The security features like Security to data transmitted, Authentication of users and integrity of message is of primary importance.

II. LITERATURE SURVEY

In the past, few works have been developed on the concept of double encryption. In [1], encryption is followed in 2 steps. In the first step the plain text is encrypted using a specific algorithm to generate a first encrypted text then another random number is considered to generate a cipher key which in turn is used to encrypt the first encrypted text to generate the final cipher text. Both the final cipher text and the cipher key are sent to the receiver for decryption. In [2], the plain text is encrypted, many times using different strong encryption algorithms at each phase. In [3], there has been a double encryption of the data by multiplexing the cipher text with a salt cipher text coded with the same setup. In [4], the plain text is encrypted twice using RSA and DES encryption algorithms and the final encrypted text is hidden in a host image using the process of steganography. This helps in increasing the complexity of data retrieval. In [5], to strengthen the already existing DES algorithm the plain text is enciphered 3 times, first encryption with a first key, then decrypt with a second key then again encrypt with the first key.

In our work we have used a different approach for double encryption; three keys are used in our process. The session key is initially developed depending on the plain text and is modified in the process of encryption and the secondary key determines the way in which the encryption process is carried out. The session key is a random number sequence which varies every time we encrypt the data and it gets modified during the process of encryption, the secondary key also helps in altering the encryption process between differentiation and integration. These features help in adding additional complexity to the algorithm.

III. MODELLING OF THE WORK

Three Keys are being used for encryption process. A Primary and Secondary Keys are used which are to be shared among the participants. The primary

Key which is to be shared among the sender and receiver is a onetime process. A random sequence is used as a session key which is to be modified as per the encryption of plain text. This Modified session key is encrypted with primary key to be sent to receiver. The secondary key to be shared between sender and receiver helps to identify the number of differentiations and integrations in the encryption and decryption process.

Thus initially the plain text is encrypted with the help of session key and a secondary key which generates a larger number which is a part of cipher text and the session key is also encrypted simultaneously with the help primary key which forms the other part of cipher text. Thus, this process produces 2 cipher texts.

In the decryption process, primary key is used to decrypt the secondary cipher text to generate the session key. Once the session key is obtained, along with the secondary key we can decrypt the primary cipher text to obtain the plain text.

IV. ENCRYPTION PROCESS

The secondary key and the session key are the 2 important things in this encryption process.

A. Secondary Key

Secondary key is just a string of numbers which helps us understand the way in which the encryption process is carried out. The secondary key can be user defined. In this encryption process as mentioned before differentiation and integration are carried out. Initially the plain text is differentiated for a particular number of steps, and then it is integrated for a particular number of steps and again differentiation is carried out. So, as we can see the encryption process alternates between differentiating and integrating the plain text. The secondary key decides when differentiation is to be carried out and when integration.

Example1: Secondary key: 3, 6
Initially the encryption always starts with differentiation and the secondary key suggests that until the 3^{rd} number of the session key differentiation is carried out and then the encryption process changes to integration which continues from 4^{th} to 6^{th} number of the session key, then it again changes to differentiation which continues till the end of the encryption process.

Example2: Secondary Key: 2, 5, 7, 10
This secondary key suggests that the encryption is followed in the following order

a. Differentiation from 1^{st} to 2^{nd} number of session key
b. Integration from 3^{rd} to 5^{th} number of session key
c. Differentiation from 6^{th} to 7^{th} number of session key
d. Integration from 8^{th} to 10^{th} number of session key
e. Differentiation from 11^{th} number of the session key till the end of encryption.

As we can see, the secondary key decides the order in which differentiation and integration is carried out. So, the secondary key should have the following properties.

a. It should contain a string of numbers that are non-repetitive and are in an increasing order.
b. Secondary key deals with the length of the session key and in the encryption process 6 characters are considered once, so it is advisable that the secondary key has digits that are less than 10 (the process of changing the encryption method between integration and differentiation is done only till the 10^{th} number of the session key).
c. The length of the secondary key should always be even.

B. Session Key

The session key is a string of randomly generated numbers. The randomly generated sequence is taken as the session key initially and the encryption process starts and during the encryption process it is altered and finally after the encryption is completed i.e when the primary cipher text is generated, the final session key is also generated which is again encrypted with the primary key to generate the secondary cipher text. Thus we finally have 2 cipher texts.

The random numbers that are generated in the session key must lie in the range 1-n, where n is the number of characters considered per block, normally we consider 6 characters in a block then n=6, but in certain situations the number of

characters that are left to be encrypted might be less than 6. In such situations the value of n will be number of characters that are left to be encrypted.

Example1: Plain Text - SUNDAY
In the above example, the plain text contains 6 characters, so the value of n=6.
Random number series will look like 3,6,2,2,5,6,1,2,3,5,5,5,4,2,4… which will be the initial session key.

Example2: Plain Text - HELLO
In the above example, the plain text contains 5 characters, so the value of n=5.
Random number series will look like 3,3,4,1,5,1,4,2,1,1,4,1,3,5…which will be the initial session key.

Session key has the following properties.

a. It is an infinite series of randomly generated numbers. The session key is modified during the encryption steps depending on the cipher text and at the end of encryption we have a finite length session key.

b. Session key generated depends only on the number of characters the plain text considered for a block has, and the modification of the session key depends on the encryption process.

C. Process of Encryption

The encryption process mainly consists of differentiation and integration which are carried out in regular steps according to the session and secondary keys.
In this process of encryption, we allocate numbers to characters' like
A-1
B-2
C-3
D-4 and so on like this till Z-26. We also allocate numbers to special characters like Space-27, !-28, @-29 and so on.

Example: SUNDAY
The word "SUNDAY" has 6 characters so we find the corresponding numbers allocated to these characters and raise 6 different variables (say X1, X2, X3, X4, X5, X6) to these corresponding numbers of the characters and then multiply all the variables which have powers.

(X1^19)*(X2^21)*(X3^14)*(X4^4)*(X5^1)*(X6^25).

Now, consider a plain text "SUNDAY IS GOOD" that is to be encrypted. In the plain text there are 3 words and 14 characters. The encryption process is carried out in blocks where in each block we consider 6 characters and encrypt them. So we have to encrypt the above plain text in 3 blocks.
Block 1: Plain Text: "SUNDAY"
Block 2: Plain Text: " IS GO"
Block 3: Plain text: "OD"
We can see that in the 1st block the plain text is the 1st six characters from the original plain text that is "SUNDAY". For the 2nd block the plain text is the next six characters that is " IS GO" and for the 3rd block we have only 2 more characters left, so the plain text is "OD". In this way we divide up the original plain text into blocks having 6 characters each.

So the number of blocks depend on the number of characters the original plain text has.
Number of characters in the original plain text = N.
Number of blocks = (N/6). If N is a multiple of 6
= ((N/6) + 1). Otherwise
Now, we consider the 1st block, we have a plain text corresponding to the 1st block and we carry out the encryption process and generate 2 cipher texts. This process is repeated for all the blocks and corresponding cipher texts are generated.
During the decryption process we consider the 1st two cipher texts and decrypt it to obtain the plain text for the 1st block and the same process is repeated until we have the plain texts for all the blocks. Thus the original plain text is generated by combining the plain texts of all the blocks.

So throughout the process of encryption, the primary key and the secondary key are constant. The plain text and the session key varies for each block and they are encrypted to generate 2 cipher texts each time.

Example

For simplicity we consider a plain text "ABCD". This plain text has only 4 characters so the encryption process can be completed in only 1 block.

Plain text: ABCD

Un modified session key:

3,2,4,3,3,1,2,3,2,1,3,2,4,4,1,3,2,2,1,4,3,3,4,2,1…

Secondary key: 3, 6

Therefore the expression of the plain text will be (X1^1)*(X2^2)*(X3^3)*(X4^4).

Now, from the secondary key, we understand that till the 3rd number of the session key differentiation is to be carried out.

So, consider the first three numbers of the session key 3, 2, 4. It means that the expression is partially differentiated according to the session key in the following manner.

The expression is (X1^1)*(X2^2)*(X3^3)*(X4^4) and the first number of the session key is 3, so the 3rd variable is partially differentiated.

3*(X1^1)*(X2^2)*(X3^2)*(X4^4).

And to the constant of the expression, add the initial power of the variable before it is differentiated.

(3+3)*(X1^1)*(X2^2)*(X3^2)*(X4^4) = 6*(X1^1)*(X2^2)*(X3^2)*(X4^4).

Now the next number in the session key is 2 so partially differentiate the expression with the 2nd variable and add the power of the variable to the differentiated expression constant, which gives

((6*2) + 2)*(X1^1)*(X2^1)*(X3^2)*(X4^4) = 14*(X1^1)*(X2^1)*(X3^2)*(X4^4)

Now, the last number before the process changes to integration is 4, so follow the same procedure which gives

((14*4) + 4)*(X1^1)*(X2^1)*(X3^2)*(X4^3) = 60*(X1^1)*(X2^1)*(X3^2)*(X4^3)

So, we have the expression as 60*(X1^1)*(X2^1)*(X3^2)*(X4^3).

Now according to the secondary key integration applies from 4th number to 6th number of the session key. So the session key that is to be considered is 3, 3, 1.

Expression is 60*(X1^1)*(X2^1)*(X3^2)*(X4^3)

Now, partially integrate the expression with respect to the 3rd variable then subtract the power of third variable from the numerator that is obtained after the integration.

((60-3)/3)*(X1^1)*(X2^1)*(X3^3)*(X4^3) = 57/3*(X1^1)*(X2^1)*(X3^3)*(X4^3)

Note: The constant of the expression should not be simplified at any time of the encryption process the denominator must be left as it is. The constant should not be simplified; it gets cleared out during the decryption process. Anyhow, the denominator is formed only during the integration process. So, only during the integration process of the encryption the denominator is to be considered. During the differentiation part we must consider only the numerator.

Now, the next numbers in the session key are 3, 1. They are integrated in the similar fashion and the powers are subtracted out which finally results in

((57-4)/(3*4))*(X1^1)*(X2^1)*(X3^4)*(X4^3) = 53/12*(X1^1)*(X2^1)*(X3^4)*(X4^3).

((53-2)/(12*2))*(X1^2)*(X2^1)*(X3^4)*(X4^3) = 51/24*(X1^2)*(X2^1)*(X3^4)*(X4^3).

Now, the integration part is also completed according to the secondary key, so again differentiation process again starts.

And the session key remaining part is 2,3,2,1,3,2,4,4,1,3,2,2,1,4,3,3,4,2…where differentiation is carried out.

The expression is

51/24*(X1^2)*(X2^1)*(X3^4)*(X4^3)

Now, as discussed earlier differentiation is carried out along with addition of the power of the variable. Here, the first number is 2. So the expression is differentiated with the second variable and its power is added

Note: Now, here the differentiation process is carried out and it only deals with the numerator part and the denominator part is left untouched and it is not to be disturbed.

(51+1)/24*(X1^2)*(X3^4)*(X4^3) = 52/24*(X1^2)*(X3^4)*(X4^3).

Next number in the session key is 3 so the 3rd variable is to be differentiated, it gives

((52*4)+4)/24*(X1^2)*(X3^3)*(X4^3) = 212/24*(X1^2)*(X3^3)*(X4^3)

Now if we observe the expression, 2nd variable has vanished and the next number in the session key is 2. So if we differentiate the expression with respect to the 2nd variable it gives us 0. So, we need to modify the session key by removing the 2nd variable terms in the session key from now on.

So the session key from the 7th number becomes 2,3,1,3,4,4,1,3,1,4,3,3,4,1…from here on.
So, the next number in the key is 1, the 1st variable is to be differentiated which gives
((212*2)+2)/24*(X1^1)*(X3^3)*(X4^3) = 426/24*(X1^1)*(X3^3)*(X4^3)

Now, this process is continued according to the session key and as soon a variable vanishes all the preceding terms of the variable in the session key are removed, so as to avoid the formation of 0, which means if the 4th variable vanishes at any step all the fourth variable terms in the session key which comes after the step in which the fourth variable got vanished are removed.
By following this process, we get the following expressions
426/24*(X1^1)*(X3^3)*(X4^3)
1281/24*(X1^1)*(X3^2)*(X4^3)
3846/24*(X1^1)*(X3^2)*(X4^2)
7694/24*(X1^1)*(X3^2)*(X4^1)
7695/24*(X3^2)*(X4^1)
15392/24*(X3^1)*(X4^1)
15393/24*(X3^1)
15394/24.
So, we finally obtained the primary cipher text.
The modified and finite length final session key is 3,2,4,3,3,1,2,3,1,3,4,4,1,3,4,3. Now, this final session key is encrypted using the primary key by Matrix Key Multiplication Algorithm [6] and it develops the secondary cipher text. This primary key is shared between both the sender and receiver.

With this both the cipher texts are generated and the encryption process is completed for the 1st block. In our example we have only 4 characters so the encryption is completed. If we have more than 6 characters, then we have to consider the 2nd block and follow the same procedure to get 2 cipher texts.

With this the encryption process is completed and the two cipher texts are sent to the receiver and the receiver receives both the cipher texts and he already has the primary key and secondary key. With the help of primary key, he first decrypts the secondary cipher text to obtain the session key and then he uses both the session key and the secondary keys and decrypts the primary cipher and obtain the plain text.

V. DECRYPTION PROCESS

The receiver already has the primary key and the secondary key. He receives the primary cipher and secondary cipher texts.

Then the receiver uses the primary key and decrypts the secondary key according to the Matrix Key Multiplication Algorithm and retrieves the session key.

Example: Consider the above example
So, if the receiver uses the primary key and secondary cipher text he then retrieves the session key as 3,2,4,3,3,1,2,3,1,3,4,4,1,3,4,3.
Now, this session key shows the direction in which the encryption process is carried out and we also have the secondary key as 3, 6 which shows the way in which differentiation and integration processes are carried out. Now in the decryption process firstly reverse the session key which gives us decryption session key as 3,4,3,1,4,4,3,1,3,2,1,3,3,4,2,3. According to the encryption process differentiation is carried till the 3rd number then integration till 6th number then again differentiation is carried out. So, to decrypt the primary cipher we need to get in reverse pattern and retrieve the encrypted text.
Therefore, firstly we need to integrate until the 6th number from last in the decryption session key then start differentiating until the 3rd last number in the decryption session key and then continue integrating till the end to retrieve the plain text according to the secondary key.

We have the primary cipher text as 15394/24.
And the decryption session key is 3,4,3,1,4,4,3,1,3,2,1,3,3,4,2,3.

So, now we can start integrating according to the session key and then subtract the power the

variable as achieved, since we added its power during encryption process, so now we need to subtract the power. Therefore,
(15394-1)/24*(X3^1) = 15393/24*(X3^1).

Note: We did not consider the denominator of the primary cipher text in the differentiation process of the encryption process we only considered it in the integration part of the encryption. Similarly, we consider the denominator of the cipher text only in the differentiation process of the decryption process and omit it in the integration process of the decryption process.
So now the decryption process involving integration is to be carried out according to the session key till the 6th number from the last of the session key (3,4,3,1,4,4,3,1,3,2) which gives us
15393/24*(X3^1)
(15393-1)/24*(X3^1)*(X4^1) = 15392/24*(X3^1)*(X4^1)
(15392-2)/24*((X3^2)/2)*(X4^1)
=15390/24*((X3^2)/2)*(X4^1) = 7695/24*(X3^2)*(X4^1)
(7695-1)/24*(X1^1)*(X3^2)*(X4^1) = 7694/24*(X1^1)*(X3^2)*(X4^1)
3846/24*(X1^1)*(X3^2)*(X4^2)
1281/24*(X1^1)*(X3^2)*(X4^3)
426/24*(X1^1)*(X3^3)*(X4^3)
212/24*(X1^2)*(X3^3)*(X4^3)
52/24*(X1^2)*(X3^4)*(X4^3)
51/24*(X1^2)*(X2^1)*(X3^4)*(X4^3)
With this we have reached the 6th number from last in the decryption session key now we need to differentiate the expression till the 3rd last number according to the decryption session key (1,3,3).

So, when we are differentiating we need to add the power of the variable with respect to which we are differentiating since we subtracted the power during of the integration part of the encryption process.

((51+2)/24)*(2*(X1^1))*(X2^1)*(X3^4)*(X4^3)
= 53/12*(X1^1)*(X2^1)*(X3^4)*(X4^3)
(53+4)/12*(X1^1)*(X2^1)*(4*(X3^3))*(X4^3) = 57/3*(X1^1)*(X2^1)*(X3^3)*(X4^3)
(57+3)/3*(X1^1)*(X2^1)*(3*(X3^2))*(X4^3) = 60*(X1^1)*(X2^1)*(X3^2)*(X4^3)

Therefore, we have reached the 3rd last number in the decryption session key so now again the integration process continues till the end (4, 2, 3) to achieve the plain text.

60*(X1^1)*(X2^1)*(X3^2)*(X4^3)
(60-4)*(X1^1)*(X2^1)*(X3^2)*((X4^4)/4) = 14*(X1^1)*(X2^1)*(X3^2)*(X4^4)
(14-2)*(X1^1)*((X2^2)/2)*(X3^2)*(X4^4) = 6*(X1^1)*(X2^2)*(X3^2)*(X4^4)
(6-3)*(X1^1)*(X2^2)*((X3^3)/3)*(X4^4) = (X1^1)*(X2^2)*(X3^3)*(X4^4)

So, finally the decryption process according to decryption session key is completed and the final expression is achieved and it is (X1^1)*(X2^2)*(X3^3)*(X4^4).

So, now the powers of the variables are collected and it is associated with their corresponding characters.

The powers of the variables are 1,2,3,4. Therefore the corresponding characters are A,B,C,D. therefore the plain text is ABCD which is decrypted with the help of the session key and according to the secondary key. Therefore, the plain text is ABCD.

VI. COMPLEXITY

In the algorithm discussed above, during the encryption and decryption processes partial differentiation and partial integration of the plain text expression are carried out along with addition and subtraction of the powers to the constant. Partial differentiation and partial integration in our algorithm can be compared to that of simple multiplication and division of the constant term. The time complexity of multiplication and division is O(n^2) and that of addition and subtraction is O(n). So the time complexity of the algorithm for one step of the encryption is O(n^2). If the length of the session key is M, then the overall time complexity of the algorithm is O(M*(n^2)).
The fact that the session key generated will be different each time the data is encrypted and the secondary key helps in changing the encryption mechanism between differentiation and

integration, adds to the complexity of the algorithm.

VII. CONCLUSION

The work considers encryption of plain text with a session key, whose modification depends on the plain text to form one part of cipher text. This session key is also encrypted with the primary key to form other part of cipher text. During decryption process initially the session key has to be generated and using this session key plain text will be restored. The strength with this mechanism is that the session key used is changing for every session as it is dependent on plain text. The primary key used is a onetime exchange among participants. The secondary key can be changed for certain sessions as per the agreement among the participants.

REFERENCES

[1] Sourabh Chandraa, Bidisha Mandalb, Sk. safikul Alamc , Siddhartha Bhattacharyyad (2015) Content based double encryption algorithm using symmetric key cryptography. Presented at International Conference on Recent Trends in Computing (ICRTC 2015).

[2] Himanshu Gupta and Vinod Kumar Sharma, Multiphase Encryption: (2013, August). A New Concept in Modern Cryptography,*International Journal of Computer Theory and Engineering, Vol. 5, No. 4.*

[3] Alejandro Velez Zea, John Fredy Barrera and Roberto Torroba, (2017, September) Cryptographic salting for security enhancement of double random phase encryption schemes. *Journal of Optics, Volume 19, Number 10.*

[4] Mahanth Landu , Sujatha C.N (2017, July), Secured Transmission of Text using Double Encryption Algorithms, International Journal of Engineering Trends and Technology (IJETT) –Volume 49 Number 5.

[5] Ralph C. Merkle Elxsi, Int. Martin E. Hellman (1981, July), On the Security of Multiple Encryption, Communications of the ACM Number 7, Volume 24.

[6] A.V.N. Krishna, S. N. N. Pandit & A. Vinaya Babu (2007), A generalized scheme for data encryption technique using a randomized matrix key, Journal of Discrete Mathematical Sciences and Cryptography, Volume 10.

[7] Rajaram Ramasamy.R, Amutha Prabakar.M, Indra Devi, M and M. Suguna.M (2009). Knapsack based ECC Encryption and Decryption, *International Journal of Network Security, 9(3),* 218-226.

[8] Stallings, W.(2006) *Cryptography and Network Security*, Prentice Hall, 4th Edition.