Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 5; April-June, 2015 pp. 446-449
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

A New Approach towards Encryption Technique: D's Crypto-Cipher Technique (DCCT)

Darpan D Shah[1], Anamika Mittal[2] and Kuntesh K Jani[3]

[1]Information Technology Government Engineering College Gandhinagar, Sector 28, Gujarat, India.-382028
[2,3]Government Engineering College Gandhinagar, Sector 28, Gujarat, India-382028
E-mail: [1]darpanshah5@gmail.com, [2]anamika@gecg28.ac.in, [3]kunteshjani@gecg28.ac.in

Abstract—*Information Security is a major challenging issue in today's technological world. There is a huge demand for a stronger and secure encryption techniques which are very hard to crack. Earlier so many researcher have proposed various encryption techniques and algorithm such as DES, AES, Blowfish, RSA, Feistel block cipher etc. Some of them are very popular in achieving data security at a great extent like Blowfish and AES. But nowadays as security level is increased the time span and complexity of algorithm to perform various operations is also increased. This is the major cause of decreasing efficiency and speed of an encryption techniques. For this we have proposed a new encryption technique named "D's crypto-cipher technique (DCCT)" with a random key generation which enhance security level as well as speed and efficiency of an encryption system. The (DCCT) is applied on a plaintext block with a random key generation where the key is also encrypted at another location rather than original location. In this abstract we have proposed a new invented encryption technique which is very secure and very efficient. (DCCT) is implemented in a way like 'Hide and Seek.' But to seek by cryptanalyst is very hard and may be not possible.*

Index terms*: Encryption, decryption, random Key generation.*

1. INTRODUCTION

Speed of these systems is low. The main purpose of the cryptography is used not only provide confidentially, but also to provide solutions for other problems. Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new Cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity. Here Fig. 1 is representing Conventional encryption.

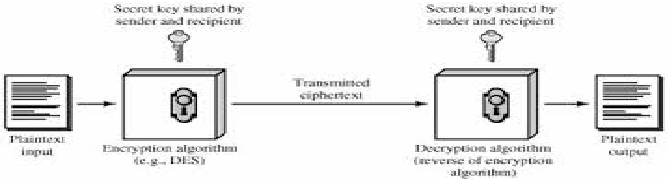
Secret key shared by sender and recipient
Secret key shared by sender and recipient
Plaintext input
Encryption algorithm (e.g., DES)
Transmitted ciphertext
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Fig. 1: A Simplified Model of Conventional Encryption

In this research paper, a new encryption algorithm named "D's Crypto-Cipher Technique (DCCT)" is proposed which is applied on a plaintext block with a random key generation where the key is also encrypted at another location rather than original location. This technique is symmetric encryption technique in which key is same at both sender and receiver side. In this abstract we have proposed a new invented encryption technique which is very secure and very efficient. DCCT is implemented in a way like 'Hide and Seek.' But to seek by cryptanalyst is very hard and may be not possible. In DCCT we are working with a 64 bit of plain text block. Here key generation technique is totally different than we seen in previous encryption technique. We are generating a random key each time when a new plaintext message has to be come. The length of the key is equal to plaintext length. This DCCT has follow randomization technique for key generation. So it is very hard to find the key which has to be used in encryption process.

In the following section we are going in details.

2. RELATED WORK

Cryptography is the study of transmitting secret messages securely from one party to another in a very secure manner.[4] To accomplish this task, the original text or also known as message, called plaintext, is translated into an encrypted version called cipher text, which is sent to the intended recipient. The task of recipient is to decrypts the text that it received and also obtain the original message called as plaintext. For this purpose in this paper I am presenting a new block based symmetric cryptography algorithm. The model has been written into two steps. In the first step, the plaintext has been taken as 64 bit of blocks. Then we generate a random key which is having same length as the length of plaintext. Here a random key generation function is used which generate a new random key every time when a new plaintext will arrive. Here a vital task of function is not only generation of random key but it also comprise length of key which is same as the length of plaintext.

3. PROPOSED D’S CRYPTO-CIPHER TECHNIQUE (DCCT)

The DCCT has the following features:

- It is a Symmetric Key Block Cipher technique.
- Block size is of 8bytes.
- Key size is depend on plaintext bits.
- Key generation is Random.
- Key is also encrypted.
- Location of key where it stored is deleted.

Encryption approach Used

Here we are using symmetric encryption approach. We have already know that symmetric encryption approach is divide in two type one is block cipher symmetric cryptography technique and another is stream cipher symmetric cryptography[1] but there we are choosing block cipher type because its efficiency and security. In the proposed technique we have a common key between sender and receiver, which is known as private key [10]. **Here one main concept is key is also encrypted and its original location is removed.** Basically private key concept is the symmetric key concepts where plain text is converting into encrypted text known as cipher text using private key where cipher text decrypted by same private key into plane text. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain private information [3]. Basic concept of symmetric cryptography is shown in Fig. 2.

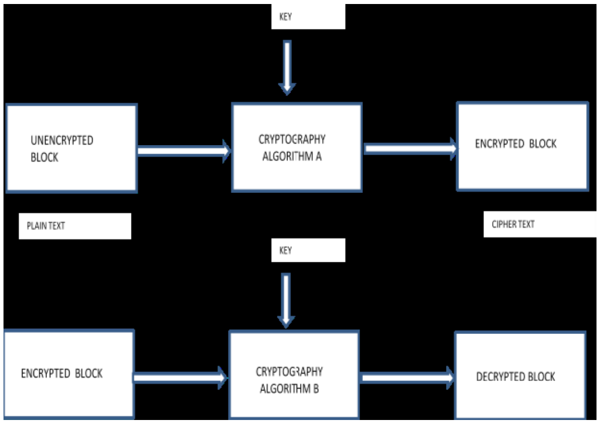

Fig. 2: Basic Concept for Symmetric Cryptography

Reason for Use of Symmetric Approach for Encryption and Decryption

The encryption process is simple.

- Each trading partner can use the same encryption Algorithm no need to develop and exchange secret algorithms.
- Security is dependent on the length of the key.
- High rates of data throughput.
- Keys for symmetric-key ciphers are relatively short.
- Symmetric-key ciphers can be used as primitives to construct various cryptographic mechanisms.
- Symmetric-key ciphers can be composed to produce stronger ciphers.

Proposed Key Generation Steps

- Count the length of plaintext and determine the length of an array which is same as plaintext
- Here size of key is varied from 0 to 64 bits according to the length of plaintext.
- Make a random key generation function which generate key in the form of random number.
- Here key which is generated contain only numbers but random number.
- After generating key we stored it into the predefine array.
- This array is used for encryption. This array is created every time as new plaintext arrived.

Encryption Steps on plaintext in Proposed Algorithm:

- Initially we select a 64 bit block which containing plaintext or message.
- Accept the sender message by counting number of bits in plaintext.
- Generate the key having same length as plaintext and store it in array called key.
- Encrypt the message by applying key number on each bit of plaintext.
- Here first we convert plaintext into number form.
- Then we perform addition by adding each random number of key with each bit of plaintext respectively.
- After performing addition we transform this new form of encrypted plaintext also called as cipher text into ASCII value which would be either number, symbol, character.
- At last final form of cipher text is generated which is stored in the new location and deleting original location here array which holding plaintext.

Encryption on Key

In this technique we also perform encryption operation on random key as describe in below steps.

- First we take the original key array.
- Then we have to make a new array that contain cipher-key.
- Set the length of the new array same as original array Containing key.
- Then we perform encryption on the key by converting number in key to character form and store it into the new array.

- Here we removed the original array of key so opponent can't find original key.
- Stop.

The below Fig. shown key Encryption.

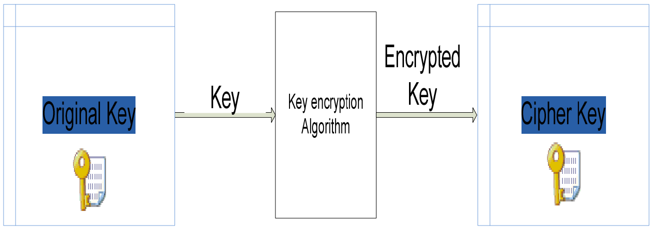

Fig. 3: Key Decryption using key Encryption lgorithm. Exit.

Decryption on Key

Now first we perform decryption on encrypted key as describe in below steps.

- First take the cipher key array.
- Then make a new array that contain plain-key.
- Set the length of the new array same as original array Containing cipher key.
- Then we perform decryption on the key by converting character in array to numeric form and store it into the new array.
- Now we removed the array of cipher-key so opponent can't find cipher key.
- Stop.

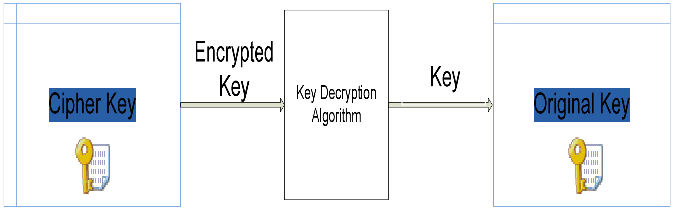

Fig. 4: Key Decryption using key Decryption algorithm.

Decryption Steps on plaintext in Proposed Algorithm:

- Now we perform decryption on cipher-text block which is containing cipher-text.
- Count the number of bit in cipher-text and make a new array which contain length equal to the cipher-text bits.
- Decrypt the message by applying key number on each bit of cipher-text.
- Here we convert cipher-text contain ASCII value to number form.
- Then we perform subtraction operation by subtracting each key bit from cipher-text bit respectively.
- After performing this operation we get an original plaintext.
- At last final form of plaintext text is generated which is stored in the new location and deleting original location here array which holding cipher-text.

Snap of DCCT Encryption and Decryption Technique

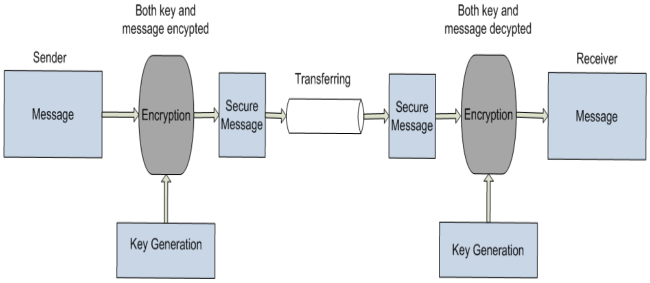

Fig. 5: DCCT Encryption Decryption.

4. ADVANTAGES

DCCT has benefits and features over the old cryptographic technique.

- Here in this technique we perform encryption of key while in previous techniques there is no any such kind of implementation.
- The location of key before and after encryption is deleted.
- So opponent cannot find actual location.
- Key is random for every new time.
- Key length is depended on plaintext length so predict about key is not possible.
- If receiver wants to decrypt message then first it must decrypt key and then it can decrypt plaintext.
- It is develop with the idea of dual encryption technique both plaintext and key.

5. FUTURE ENHANCEMENT

The system can be easily modified to accept any encryption algorithm which would be framed in future. Just by adding or removing another module in the main function, any number of algorithms can be included or reduced. We can implement this algorithm for security purpose on web to store public data in encrypted form. So any attack on their data can be prevented.

6. CONCLUSION

Each algorithm having its own advantages and Disadvantages, our system proposed a good strategy of making most out of the advantages of DCCT while trying to eliminate the limitations. The developed technique encrypt data of person so that security is maintained. The importing thing of our proposed technique is that it is almost impossible to break the encryption technique without knowing exact key value which is also encrypted as well as random and not having fixed length. We propose that this encryption method can be applied for data encryption and decryption in any type of public application for sending confidential data.

7. ACKNOWLEDGEMENTS

I am grateful to many people for their help in writing this paper. First of all I would like to thanks my family who helps me in my every effort behind this precious work. I personally thanks to a special person in my life who appreciate me for my work and she is very lucky for me. Without her appreciation am not able to do this job.

REFERENCES

[1] W.Stallings, “Cryptography and Network Security: Principles and Practices”, Prentice Hall, 1999.

[2] Cryptography and Network Security, Tata Mc Graw Hill, Atul Kahate, 3rd Eddition.

[3] NIST special publication 800-133, Recommendation for cryptography Key Generation by Elain Barker Allen Roginsky.

[4] Technical Publication by V.S. Bagad and I.A. Dhotre.

[5] Information Security (Complete Reference Series 2nd Eddition) By Mark Rhodes-Ousley.

[6] D Walter Tuchman, "A brief history of the data encryption standard", ACM Press/Addison-Wesley Publishing Co. NY, USA, pp. 275–280, 1997.

[7] Neal Koblitz “A Course in Number Theory and Cryptography” Second Edition Published by Springer-Verlag.

[8] National Bureau of Standards, “Data Encryption Standard,” FIPS Publication 46, 1977.

[9] Gast.M.S (2002),"802.11 Wireless Network: The Definitive Guide," O'REILLY.

[10] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e 2005.

[11] Shashi Mehrotra Seth, 2Rajan Mishra,” Comparative Analysis Of Encryption Algorithms For Data Communication”, IJCST Vol. 2, Iss ue 2, June 2011 pp.192-192.

[12] eSTREAM - The ECRYPT Stream Cipher Project, http://www.ecrypt.eu.org/stream/

[13] Prasithsangaree.P and rishnamurthy.P(2003), “Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs,” in the Proceedings of the IEEE GLOBECOM 2003, pp. 1445-1449.

[14] National Institute of Standards and Technology, Advanced Encryption Standard, FIPS-197,http://csrc.nist.gov/archive/aes/index.html, 2000.

[15] D. Stinson, Cryptography, Theory and Practice, CRC Press, Second edition, 2000.