Analysis of Brute-Force Attack in UES over DES

P. Sri Ram Chandra, G.Venkateswara Rao, M. S. Chakravarthy, T .V. Prasad

Abstract*— Data transferring by means of internet has acquired a considerable significance in the recent times which in turn demands interchanging of enormous quantities of information on frequent basis. Vital information always looks for a enhanced stage of protection where cryptography is one such principle which is reliable enough to arrange the same for that data. A new cryptosystem "Ultramodern Encryption Standard (UES)" was proposed by us in our earlier research articles in order to provide a considerable level of protection. Brute-force attack is the most dangerous one where every cryptosystem is expected to with stand over this attack. In this paper we depicted the quality the proposed cryptosystem UES against brute-force attack via the estimated cracking time of the keys used and the experimental results projected here are evident that UES can with-stand to this attack in a better way when compared to the existing Data Encryption Standard-DES.

Keywords*— Brute-force attack, Data Encryption Standard (DES), Plain text, Ultramodern Encryption Standard (UES), Encryption, Cipher text, key, Decryption.

I. INTRODUCTION

Information hiding through encryption i.e., changing the state of the information so that it not possible to get accessed is the crucial aspect of cryptography. The abilities of the sender includes encrypting the information to avoid the illegal access is the basic goal. Better phase of steps must be taken into the consideration so that an enhanced level of protection is enabled for the data. An authentic stage , which takes the accountability for the protection of the data by means of encryption and decryption procedures are considered with or without a secret key is called as cryptography[1] .In the realm of PC security, one of the regularly discussed points is whether n-bit key, used for any cryptosystem is computationally secure against brute force attack or not. Normally Brute-force attack includes efficient checking of all conceivable key mixes until the point that the right key is found and is one approach to attack when it isn't conceivable to exploit the other shortcomings in any cryptosystem. It is also known as Exhaustive-Key search.

II. BACK GROUND STUDY

This section depicts the literature survey regarding quality of the cryptosystem against brute force attack with various key sizes and the estimated cracking time. Brute force attack's practical feasibility is based on the key length used for the encryption i.e., the longer keys are more efficient than shorter ones. If we assume the key size as 4-bit, then the sample brute force attack can be shown in table 1 [1]. As shown, it will have a maximum 16 phases to check each and every possible key combinations found that an 8-bit key can have 256 combinations i.e., simply 2^8.

0000	0001	0010	0011
0100	0101	0110	0111
1000	1001	1010	1011
1100	1101	1110	1111

Table 1: Sample Brute-Force attack on 4-bit Key

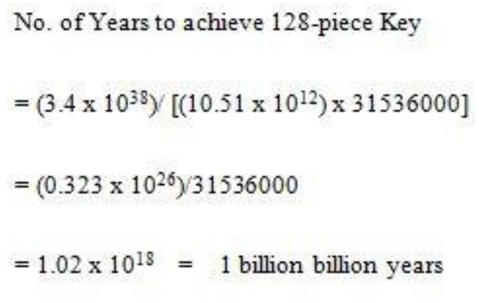
Notice the exponential increase in conceivable blends as the key size increments. There is also a physical dispute that a 128-piece symmetric key is computationally secure against brute-force assault.

Let us assume a Personal Computer with 10.51 Penta flops = 10.51 x 10^{15} Flops [Flops = Floating point operations per second] [1].

No. of Flops required per mix check: 1000 (exceptionally idealistic however simply accept for the time being)

No. of combination checks every second can be given as 10.51 x 10^{12}

No. of seconds in a single Year can be described as 365 days multiplied by 24 hours multiplied by 60 minutes multiplied by 60 seconds is equal to 31536000.



No. of Years to achieve 128-piece Key

$= (3.4 \times 10^{38}) / [(10.51 \times 10^{12}) \times 31536000]$

$= (0.323 \times 10^{26}) / 31536000$

$= 1.02 \times 10^{18}$ = 1 billion billion years

Thus the time estimated to crack the 128-bit key is equivalent to 1.02×10^{18} years [1].

III. THE UES ALGORITHM

During the processes of encryption and decryption, to perform the operations of binary and gray code a set of keys need to be achieved which is done by Ultramodern Encryption Standard (UES) through prolic series number. A number is stated as prolic series number if it fits the relation "$T_n = n*(n+1)\ n \geq 0$" where T_n is n^{th} term of the prolic series.

Revised Manuscript Received on April 12, 2019.

Mr. P. Sri Ram Chandra, Computer Science & Engineering, GIET (A), Rajahmundry, AP, India.(Email : psrgietcse@gmail.com)

Dr.G.Venkateswara Rao, Information Technology Department, GITAM, Visakhapatnam, AP, India

Mr. M. S. Chakravarthy, Computer Science & Engineering, GIET (A), Rajahmundry, AP, India.

Dr. T .V. Prasad, Professor and Principal, GIET (A), Rajahmundry, AP, India.

Actual text of 8 bit is designated as the intake along with two more 8 bit keys which are utilized for the conversion process in the initial round, correspondingly the procedure continues for 16 more rounds of encryption and two other transforms of 8 bit keys each i.e., a total of 34 blocks of keys 8 bit each are necessary [2].

A. Key generation process

Actual process in generating the key of UES algorithm is initiated by considering an random prolic series number proceeded by the relation “T_n= n*(n+1)” such that $0 \leq n \leq 255$, which is the range of ASCII character ,generally represented using binary code of 17 bit. This particular code is further transformed into gray code of 17 bit making the total number of bits to be considered as 34. Further the process goes on until a 272 bit key is achieved. Thereupon for generating a set of keys for encryption and decryption processes the obtained 272 bits are categorized into 34 blocks of 8 bits each and name them as $K_{n,}$ $1 \leq n \leq 34$ [2].

B. Encryption process

Encryption is stated as the procedure in which transforming of message ‘m’ corresponding proper key(s) ‘k’ through encryption algorithm ‘E’ in order to provide access to the users who are authorized, which is further represented as cipher text c=E(k, m).

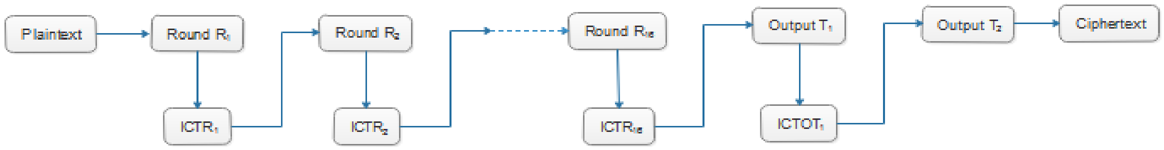


Figure.1 Encryption of UES

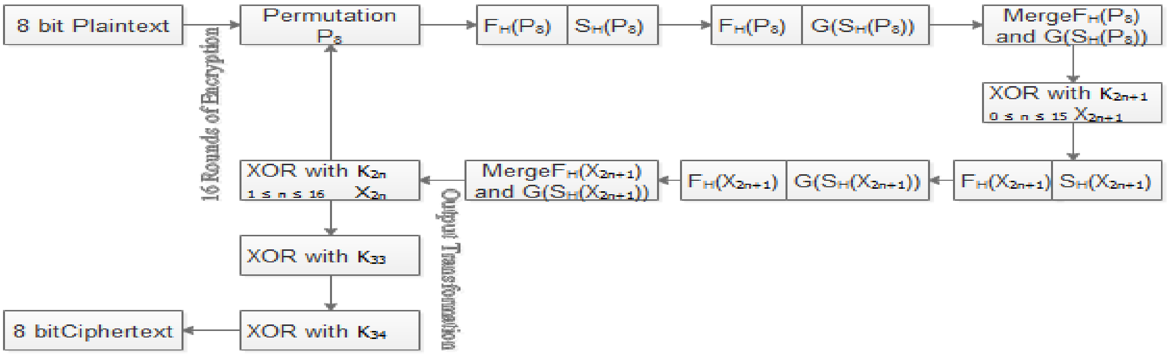


Figure.2 Detailed Execution of one round of Encryption in UES

Initiation of the encryption process considers the input of 8 bit actual text where it further goes encryption of 16 rounds resulting in 32 blocks of keys with 8 bits each are being utilized. The concluding stage of this procedure includes performing operations by means of two output transformation using 2 blocks of key 8 bits each [2]. The detailed encryption process is shown in Figure 1 and Figure 2.

IV. EXPERIMENTAL RESULTS

Based on the brief study of estimated cracking time of n-bit key shown in back ground study, we have tabulated few of the values based on practical notion of cracking the 128-bit key, we included the estimated cracking times of the proposed cryptosystems also.

Key Size	Estimated Time to Crack the key in years
128-bit	$1.02x10^{18}$ years
192-bit	$1.872x10^{37}$ years
256-bit	$3.31x10^{56}$years
272-bit (UES)	$5.32x10^{76}$years

Table 2: Key size Vs. Estimated Cracking time

The encryption process of UES ignites by considering the 272 bit key, thus our proposed cryptosystem Ultramodern Encryption Standard can have 2^{272} combinations of keys and the estimated cracking time can be $5.32x10^{76}$years. As we are using the unique keys for every possible encryption, the encrypted messages can be transmitted safely to the destination with in estimated cracking time. The following table 3 gives us the comparison of Brute-Force attack between DES and UES.

Cryptosystem	Key Size	No. of possible Keys	Estimated key Cracking time
DES	56 bits	2^{56}	399 Seconds
UES	272 bits	2^{272}	$5.32x10^{76}$years

Table 3: Analysis of Brute-Force attack DES vs. UES

V. CONCLUSIONS

In this research article we have analyzed the proposed cryptosystem “Ultramodern Encryption Standard-UES”. Based on the literature survey, we estimated the key cracking time of UES and compared with the existing DES.

The results tabulated in table 3 clearly depicts that the proposed cryptosystem UES can with stand to brute-force attack in a better way when compared to the existing DES.

REFERENCES

1. The article "How Secure is AES against brute-force attacks " written by Mohit Arora was identified via the following link https://www.eetimes.com/document.asp?doc_id=1279619
2. P. Sri Ram Chandra, G. Venkateswara Rao, G.V. Swamy, 'Ultramodern Encryption Standard Cryptosystem using Prolic Series for Secure Data Transmission', International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137 Volume – 02, Issue – 11, November – 2017, PP – 29-35.
3. William Stallings ―Cryptography and network security Pearson education, 2nd Edition.

1*Authors Profile

Sri Ram Chandra. P has received his Bachelor's Degree in Computer science and Engineering from Andhra University, Master' s Degree from GITAM University in the years 2010 and 2012 respectively. He is a member of CSI. He has published 05 research papers in reputed International journals. He has 6.8 Years of Teaching Experience. At present he is working as Associate Professor in the department of CSE, Godavari Institute of Engineering and Technology (A), Rajahmundry, Andhra Pradesh, INDIA.

2 Authors Profile

Dr.G.Venkateswara Rao has received his Master' s Degree with Computer Science and Engineering as stream from Andhra University in 1999. He was awarded with Ph.D. from A.N.U. Guntur in 2010. He is serving the society with teaching as his profession past 20 years and had around 30 research articles published in journals of international repute. Currently he is working in the department of Information Technology, GITAM-Deemed to be University, Andhra Pradesh, INDIA.

3 Authors Profile

M. Srinivasa Chakravarthy has received his Bachelor' s Degree, Master' s Degree in Computer Science and Engineering from JNTU-Kakinada in the years 2008 and 2011 respectively. At present he is working as Associate Professor in the department of CSE, Godavari Institute of Engineering and Technology (A), Rajahmundry, Andhra Pradesh, INDIA.

4 Authors Profile

Dr. T. V. Prasad currently works at Godavari Institute of Engineering and Technology, Rajahmundry, AP, India as Principal.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication