Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Dynamic Permutations

Dr. Sharaf A. Alhomdy[1] and Dr. Saleh N. Abdullah[2]

[1] Faculty of Computer and Information Technology, Sanaa University

Received: 9 December 2014 Accepted: 4 January 2015 Published: 15 January 2015

Abstract

The confidentiality, integrity and authentication of anelectronic documentare necessary in many application systems. The security of confidentiality, integrity and authentication of an electronic document are based on nonlinear functions, in which there is no directrelationship between the inputs and the outputs. This means that the inputs cannot be extracted from the outputs.Indeed, all modern cyphers are based on the concept of substitution transposition. In data encryption standard algorithm, DES, which consists of many functions, only one nonlinear function is used in the algorithm, called substitution boxes, and all other functions are linear, one of these linear functions is called IP, initial permutation function, which performs static permutations. The permutations are replaced by transpositions, based on predefined positions, and the permutation function is used several times in DES algorithm.

Index terms— confusion, diffusion, linear function, nonlinear function, static permutations, dynamic permutations, one-way functions, hash table and complexity.

1 Introduction

n any cryptosystem or message integrity and authentication, the nonlinear functions are the cornerstones because the inputs to the nonlinear functions cannot be extracted from the outputs. In linear function it is possible to obtain the output if both the inputs & the operation are known; also the second input can be obtained if one input & output are known (e.g.

2 XOR function).

A function is called nonlinear if one solution can be retched from several inputs; in other words, if the operations and the outputs of a function are known, and the inputs to a function are not known, the function is callednonlinear. Moreover, if such outputs are produced via nonlinear functions, it becomes difficult to obtain the inputs to the nonlinear functions in a suitable time. For example, the operation mod acts as nonlinear function, because 20 mod 6 =2, also 20 mod 9=2, and 20 mod 3= 2. The value 2 comes from 20 mod 6, 20 mod 9, and 20mod 3. So, if we know one of the inputs and the output along with the operation 'mod', we cannot know the second input.

In this paper, section two provides details about literature review. Section three describes our proposal technique to enhance the security in the confidentiality, integrity and authentication. The conclusion and future works will be found in section four.

3 II.

4 Literature Review

In any cryptography systems, permutation (transposition) is an essential element to remove the relations between the alphabets which formulate the sentences because every language has its own characteristics.

Permutation: refers to mapping a block of length L1 into a block of length L1 [1].

Definition: Permutation denotes ? p . ? p : {1,..,L m }?{1,?,L m1 }is a permutation, where L and m are positive integers. Shannon [2,3] suggests two methods for frustrating statistical cryptanalysis: Diffusion and Confusion. In diffusion, the statistical structure of the plaintext is dissipated into a long range statistics of the cipher text. On the other hand, confusion seeks to make the relationship between the statistics of the cipher text and the value of encryption key as complex as possible. Confusion can be achieved by the use of a complex substitution algo rithm via using substitution boxes [1].For example, if we have the following inputs: 10101101 01001110 10000100 10101111.

The corresponding values in hexadecimal system are AC4E84AF.So every value will take a predefined position as shown in table 1.

Table1 : Shows the Values and Indexes

5 Index output

6 Index input

In this paper, we will try to develop dynamic permutations instead of static permutations, nonlinear factors, which in turn enhance the security system. Keywords: confusion, diffusion, linear function, nonlinear function, static permutations, dynamic permutations, one-way functions, hash table and complexity.

7 Year 2015

The first 4-bit input will be transferred into position 8 of output, and so on.

In DES algorithm [3,4] So far all the processes of any permutations are static, i.e, the permutations are replaced by transpositions, based on predefined positions. However, in this paper we will suggesta new method ”dynamic permutations” to enhance the security in cryptosystems. The main idea for the new method is as follows:

? Constructing a suitable hash table along with suitable hash key.

? Dividing the binary data into groups, each group consists of 8-bits; and each 8-bitscan take values from 00 to FF in hexadecimal system.

? Each group should be hashed into the corresponding value; this value is used as an index to store the group in the hash table. Since the values stored in the hash table are based on randomindexes, each group will take dynamic position.

In this case, the permutations of the inputs are dynamic permutations but not static. Figure (1) shows the suggested method for the construction of the hash table.

Figure1 : Shows the Construction of the Hash Table **??**E, 84, AF. So, every value will take a position in the hash table. If there is more than one value equals, the first one will take the correct position in the hash table and the others will increase the frequency field by 1, and so on, without taking extra positions in the hash table. If there are more than one values hashed to the same index, the second value stays in another node with the same index in the hash table, and so on.V 1 V 2 V 3 V 4 V 5 V 6 V 7 V 8 V 9 V 10 V 11 V 12 V 13 V 14 V 15 V 16 V 17 V 18 V 19 V 20 V 21 V 22 V 23 V 24 V 25 V 26 V 27 V 28 V 29 V 30 V 31 V 32 V 33 V 34 V 35 V 36 V 37 V 38 V 39 V 40 V 41 V 42 V 43 V 44 V 45 V 46 V 47 V 48 V 49 V 50 V 51 V 52 V 53 V 54 V 55 V 56 V 57 V 58 V 59 V 60 V 61 V 62 V 63 V 64 V 58 V 50 V

The length of the hash table is directly proportional to the S. That means, L ? S (1) such that S is the number of characters in the block simultaneously permuted and L is the length of the hash table.

The following equation: pi=(pi-1+ xi)%m (2) Maybe used to produce the hash key, such that p0=7, pi is the index position in the hash table, x0= 11, xi is the value to be hashed, and m is prime number points to the size of the hash table.

The following is a sample of values hashed to the some indexes.

Figure 1:

2

Figure 2: Table 2 :

3

Figure 3: Table 3 :

	value	frequency
0		
1		
2		
3		
..		
m-1		

Example: if we have the following inputs 10101101 01001110 10000100 10101111.The corresponding values in hexadecimal system are AC,

Figure 4: 42 v 34 V 26 v 18 v 10 v 2 v 60 V 52 V 44 v 36 V 28 v 20 v 12 v 4 V 62 V 54 V 46 v 38 V 30 v 22 v 14 v 6 v 64 V 56 V 48 v 40 V 32 v 24 v 16 v 8 V 57 V 49 V 41 v 33 V 25 v 17 v 9 v 1 v 59 V 51 V 43 v 35 V 27 v 19 v 11 v 3 V 61 V 53 V 45 v 37 V 29 v 21 v 13 V 5 v 63 V 55 V 47 v 39 V 31 v 23 v 15 v 7

Complexity means studying each of execution time, input-data, language difficulties, mass storage required by the algorithm etc.

In this study we concentrate on complexity from only three points:

i. Data complexity.

The amount of data needed as input to the attack.

ii. Processing complexity.

The time needed to perform the attack. This is often called the work factor.

iii. Storage requirements.

The amount of memory needed to do the attack [6]. b) Complexity of Algorithms An algorithm's complexity is determined by the computational power needed to execute the algorithm itself. The computation of an algorithm is often measured by two variables: T (for Time Complexity), and S (for Space Complexity). In general, the computational complexity of an algorithm is expressed in what is called "big O" notation: the order of magnitude of the computation complexity.

Generally, algorithms are classified according to their time or space complexity: ? An algorithm is a constant if its time complexity is independent of n: O(1). ? An algorithm is linear, if its time complexity is O (n). ? An algorithms can also be quadratic, cubic, and so on. Like those algorithms, their complexity are polynomial i.e. O (nm), where m is a constant. Algorithms whose complexities are O(cf(n)), where c is a constant and f(n) is more than a constant but less than linear, are called "Supper polynomial" [6].

The suggested algorithm will take extra process more than static algorithm as the following: ? The process of conversion from binary todecimal O (n). ? The computation of indexes O (m). ? It needs also extra storage corresponding to the hash table.

IV.

.1 Conclusion and Future Work

The permutation is an essential factor in many security cryptosystems. Therefore, we developed a new method that uses dynamic permutation for enhancing the security of the system in a way better than using static permutations.

The future work, dynamic permutation can be used to produce one way hash function.

[Schneier ()] 'Applied Cryptography" 3rdEd'. Bruce Schneier . *ASIA) Pvt. Ltd. Singapore* 2010. John Wiley & Sons. 129809.

[Horowitz and Rajasekran ()] *Computer Algorithms*, Ellis Horowitz , Sanguthevar Rajasekran . 2005. New Delhi, India: Galgotia Publication Pvt. Lid.

[Russell et al. ()] *Computer Security Basics" O'*, D Russell , G T Gangemi , Sr . 2009. New York: Reilly& Associates, Inc.

[Stallings ()] *Cryptography and Network Security: Principles and Practice*, William Stallings . 2009. (3rd Ed. India)

[Douglasr and Stinson ()] *Cryptography: Theory and Practice*, Douglasr , Stinson . 2002. Waterloo, Ontario Canada: Chapman & Hall/CRC. University of Waterloo (2nd Ed)

[Thomas et al. ()] *Introduction to Algorithms*, H Thomas , Charles E Cormen , Ronald L Leiseroin , Rivest Clifford Stein . 2002. New Delhi: Prentice, Hall of India, Pvt. Ltd. 110 p. 1. (2nd Ed)

[Dennin ()] *Library of Congress Cataloging in Publication Data*, Dorothy E Dennin . 1983. Addison-Wesley, USA. (Cryptography and Data Security)