Dynamic Crypto Algorithm for Real-Time Applications DCA-RTA, Key Shifting

Ahmad H. Al-Omari
Computer Science Division, Science College
Northern Border University
ArAr, KSA

***Abstract*—The need for fast and attack resistance crypto algorithm is challenging issue in the era of the revolution in the information and communication technologies. The previous works presented by the authors "Dynamic Crypto Algorithm for Real-Time Applications DCA_RTA", still need more enhancements to bring up the DCA_RTA into acceptable security level. In this work, the author added more enhancements on the Transformation-Table that is generated by the Initial-Table IT, which affects the overall encryption/decryption process. The new TT generation proven to be less correlated with the IT than using the previous TT generation processes. The simulated result indicates more randomness in the TT, which means better attack resistance algorithm. More room for algorithm enhancements is still needed.**

***Keywords*—Dynamic crypto algorithm; real time applications; shared key generation; symmetric key encryption**

I. INTRODUCTION

The Internet and related Internet services are rapidly changing, in the next era of computing things will be outside the realm of the traditional desktops. Many of the objects surrounding us will be on the network, in which Information and Communication Technologies (ICT) are invisibly embedded in the environment surrounding us [1]. The fast momentum in modern computing toward the Internet of Things (IoT), wherein, different objects like home appliances, processors, TVs, cars, furniture, goods and others, blend seamlessly with the environment around us. [2], the shift toward using mobile computing, mobile applications, smartphones, smarts systems and cloud computing. This for sure results in new challenges to the ICT and enforces researchers to find creative solutions to fulfil the increasing demands of higher performance, low latency, more bandwidth and acceptable level of security, or what we call it the network Quality of Service QoS.

One of the main challenges to the (IoT) and the Future Internet (FI), is how to employ the concept of Internet anytime, anywhere and any service without compromising the security and QoS in resource constrained technologies [3]. Most of the proposed security solutions consider privacy, which is the main concern for Internet users. The current Internet privacy implementations mainly employ the existing known security standards, and it needs improvements [4]. Cryptology is the science that aims to provide information security in the digital environment. Cryptology details can be found in the Handbook of Applied Cryptography by [5].

A lot of improvements and (QoS) enhancements are needed to the current Internet privacy, these enhancements should focus on creative solutions that is able to maintain acceptable level of privacy without affecting the processing time. The researchers of this work, have been working since the first release of the proposed algorithm, to add more enhancements over the previous work shown in [6] [7] [8] [9] [10]. Two conference papers, one journal paper and two master students were working on the algorithm, we believe, there are many enhancements areas could be added to the original proposed algorithm, the enhancements for sure will end up with a solid algorithm that can be used in the (IoT/FI). The promising results achieved out of the previous works, provide the researchers with strong confidence of the algorithm success.

The experiment results show a faster encryption/decryption algorithm with minimal processing delay compared to the well-known algorithms, the algorithm still needs a lot of improvements to be robust and durable.

The rest of the paper is structured as follows. Section II presents general cryptographic background, a brief definition of different types of cryptographic techniques were shown. Sections III show the importance and motivation behind the work, the need for fast, secure and attack resistance symmetric algorithm is discussed. Section IV introduces the enhancements proposed by the researchers on the previously published work, the enhancements are supposed to solve some of the short comes of the previous work. Section V presents the main contribution of this paper, namely, the shifting process on the Transformation Table (TT) to eliminate the table deficiencies. Finally, section VI concludes the paper and outlines the future work.

II. BACKGROUND

A. Some Definitions

Cryptology is the study of secret codes, it involves two main branches: cryptography; concerned with writing of a plain text messages using secret code to produce a decrypted message and the creation of these methods, while cryptanalysis; concerned reading encrypted message by breaking the secret code. [11].

Cryptosystem is the method of securing communication. The sender encrypts (or enciphers) a message using an encryption algorithm together with a secret key. This produces a ciphertext which is sent to the recipient. The recipient, who

also possesses a key, receives the ciphertext and decrypts (or deciphers) using the key to recover the original message, called the plaintext. [11].

B. Block Cipher

"An n-bit block cipher divides the plaintext into blocks of n-bits, and encrypts one block at a time with a fixed key-dependent invertible transformation. In practice, the block size n is often 64 or 128 bits. A block cipher is a function E: P χ K→C, with P, K and C the sets of all possible plaintext blocks, keys and ciphertext blocks. M = C = $\{0,1\}^n$; and K = $\{0,1\}^k$. For every key Kϵ K, the encryption function E(.,K) = $E_K(.)$ is invertible and its inverse is denoted D(.,K) = $D_K(.)$. In a secure block cipher it is infeasible to determine K from a number of plaintext/ciphertext pairs faster than trying all possible K, and the permutation on all n-bit words denoted by $E_K(.)$ should be indistinguishable from a random permutation". [12].

C. Cryptanalysis Techniques

Block (or Symmetric) Ciphers are subjected to some popular cryptanalysis techniques. These techniques are differential cryptanalysis, linear cryptanalysis and algebraic cryptanalysis [12]. Any encryption technique should be cryptanalysis resistance.

III. Research Motivation

The need for fast, secure and resistant to attacks cryptography technique is highly required, nowadays many secure encryption techniques used in RTA (for example 3-DES and AES) provide acceptable security level, but the problem becomes clear when QoS is major requirement [10]. The proposed algorithm, once it is gets completed is expect to be provide noticeably high security level for many reasons; to mention some, it is fast, secure, use variable key size, can change the system key frequently with no extra time overhead, flexible and can be used in the IoT/FI regardless of using desktop, laptop, smartphone or handheld devices.

The problem of having an algorithm that is resistant to Cryptanalysis, Differential Power Analysis (DPA) and Simple Power Analysis attacks (SPA) need to be investigated more. The researchers think that, the proposed algorithm is equipped with an acceptable level of cryptanalysis attacks (the proof needs more investigations), but the DPA and SPA are still major challenges to the algorithm. Resistance to cryptanalysis is not sufficient to have secure cryptosystem [13], where, cryptanalysis attacks since vulnerabilities can raise from other layer of implementations. Cryptanalysis can test cryptographic algorithms in isolation using differential or linear cryptanalysis exploiting statistical characteristics of the algorithm, DPA and SPA can exploit vulnerability of other components and parts of the algorithm rather than statistical and mathematical parts of the system [13].

In [14], the researchers proposed to use conventional encryptions to solve the problem of long processing time instead of modern encryptions, the claimed that "Some of the conventional encryption techniques are very weak and brute force attack and traditional cryptanalysis can be used to easily determine the plain text from encrypted text" [14].

This work is consider a block cipher, but doesn't share the common characteristics and definitions of the block cipher, so it is a novel idea of symmetric encryptions. And the promising results that we had in [10], armed the researches with solid background to proceed further enhancing the algorithm to get a trusted secure and fast one.

IV. Related Work

This work is a contribution to the ongoing research on the original work [6]; our objectives were to build a concrete solid algorithm that can be used in the (IoT/FI) as trusted privacy solution, which is characterized by being transparent to the public, secure and faster than the known algorithms.

The work presented here, tries to achieve better encryption/decryption performance while keeping overhead processing to minimal levels and preserving an acceptable security level. The proposed algorithm is not complicated, so, the operations performed, the key selection process, the key size, the plaintext size, the key insertion process, the encryption and decryption processes make it simple and secure technique.

The proposed algorithm consists of three components, the Index Generation Process (IGP), Encryption Process (EP) and Decryption Process (DP) component. The IGP is common between EP and DP. The steps briefly describe the algorithm:

1) The IGP is used in both the EP and DP; where the Initiate Table (IT) is shared and announced, it uses a random Shared Value to generate the Transformation Table (TT), and the Table of Indexes (TI) is generated by randomizing the table content.

2) The Encryption/Decryption Process EP/DP, followed by Key Insertion process, the result of the final step is the Ciphertext. The inputs to the EP are the plaintext, system key and the table of indexes. The System Key is randomly generated by the user; the key is 1024-bit size. The Scrambled text; is the result of the XoR operation performed over the plaintext and the key. The system Key is inserted inside the scrambled text (XoRed table) according to the value of the Index values.

3) The Decryption Process DP starts upon receiving the Ciphertext, then the algorithm extracts the Key out of the Ciphertext, this is called Key-Recovery (KR); the extraction process is the inverse of the key insertion process used in the EP, once the key is retrieved, the DP is performed by XoRing the scrambled message and the system key to obtain the original plaintext.

The original work was described in [6], [8] and [7] the Dynamic Cryptographic Algorithm for Real Time Applications (DCA-RTA). It consists of three main processes, the Encryption Process (EP), the Decryption Process (DP) and the Index Generation Process (IGP).

The EP, takes the *Plaintext* (P) and the *System-Key* as input, then it performs XoR operations to produce the *Scrambled-Text*, then the EP inserts the *System-Key* inside the *Scrambled-Text* according to the *Table-of-Indexes* (from the IGP process), then the *Cipher-Text* which contains the *system-*

key inside are send to the receiver, who is responsible to extract the key from the received *Cipher-Text* and decrypts the message see Encryption Process (EP) below.

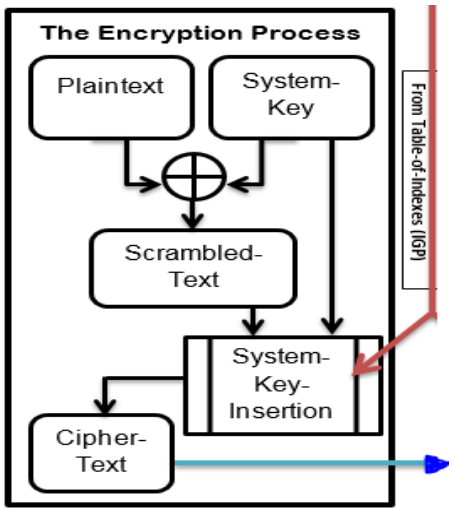

Fig. 1. Encryption Process (EP), [9]

The DP receives the *Cipher-Text* from the (EP) step, it consults the *Table-of-Transformation* to extract the *System-Key* from the received *Cipher-Text*, and then it performs XoR operation between the recovered *System-Key* and the *Scrambled-Text* to get the *Plaintext* (P), see Decryption Process (DP), [9] below.

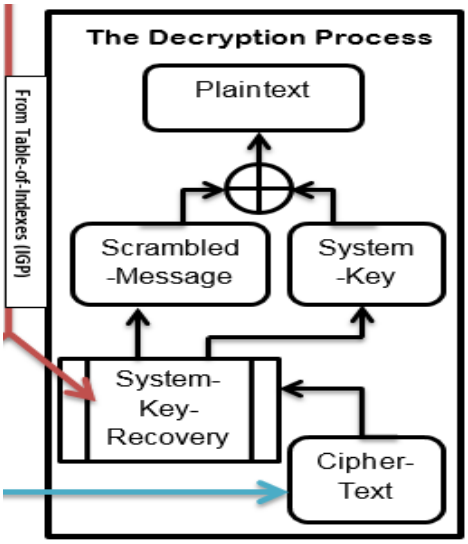

Fig. 2. Decryption Process (DP), [9]

The Index Generation Process (IGP), starts with a fixed announced $(16*16)_{16}$ table, then a randomly generated *Shared-Value* is used to mix up the initial table to produce *Transformation-Table*, then the table is used as a Table-of-Indexes, which is used in both (EP) and (DP) processes. See Index Generation Process (IGP), [9].

The complete architecture of the algorithm is summarized in

Complete DCA-RTA Architecture Algorithm, [9]

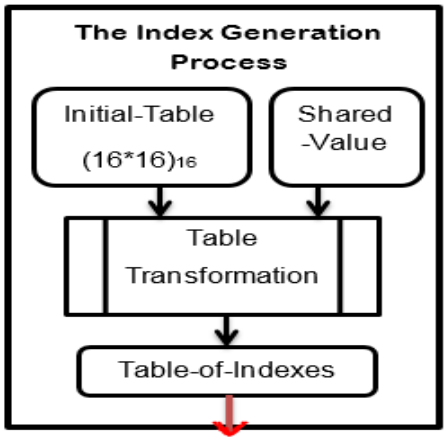

Fig. 3. Index Generation Process (IGP), [9]

In [6], the complete architecture was proposed as described above, the researchers achieved promising results, and the DCA-RTA algorithm was compared with the Advanced Encryption Standard (AES), where DCA-RTA found to be in average ten times faster than AES in Encryption/Decryption processes. In spite of the promising results, the algorithm at that time was seeking for proof of concepts, and finally it works and gave positive results.

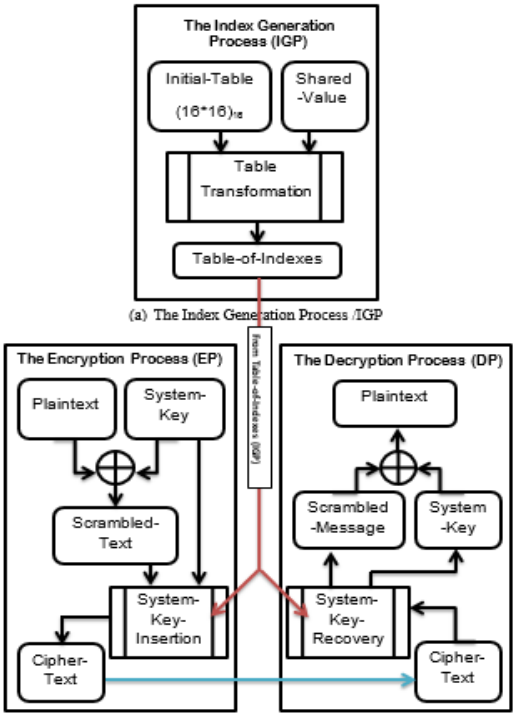

Fig. 4. Complete DCA-RTA Architecture Algorithm, [9]

In [8], the researchers proposed a ten digit shared-key value and the use of different sequences of Indexes to insert the *System-Key* inside the *Scrambled-Text* table that represents the *Cipher-Text* to be send.

In [7], the researchers implements the suggested enhancements on the DCA-RTA, and they improve the use of the Table of Indexes, in this work, no significant

enhancements were achieved, the aim of the work is to prove the correctness of the enhanced algorithm.

In [9], major enhancements on the original DCA-RTA were achieved, the researchers believe that, the initial algorithm parameters should base on scientific background, for this reason, the following parameters were tackled:

1) The System-Key-Insertion sub-process needs more tests, to prove the algorithm requirements according to the modern symmetric algorithms requirements.

2) The best Shared-Value length needs to be examined and set; since it was set to 10-digits without enough proves.

3) The best Plain-Text size should be determined.

4) Table-Transformation generation needs more intelligent processing in order to get rid of repeated patterns or segmentations problems.

Abeer A. Al-Omari, studied the algorithm from different perspectives and proposed some modifications and enhancements on the original DCA-RTA. From the performance perspective, she compared her work using the default key size (128 bytes) with AES under standard key size used in AES (16, 24 and 32 bytes), she found that her approach outperforms AES more than seven times for both encryption and decryption processes.

Abeer has added the following enhancements on the original DCA-RTA, the *Table-Transformation* building process now based on swapping one row with one column based on the *Shared-Value*. The *System-Key-Insertion*, was suffering from bad segmentation, or the *System-Key* was not distributed efficiently inside the Plain-Text, Abeer enhanced the *System-Key-Insertion* process by inserting the System-Key inside the *Scrambled-Text* from both sides. Abeer found that the proper *key-size* of 128 byte is enough to produce the required level of performance and complexity, Abeer also defined the plain-text size to be *190-bytes* long, this size guarantees the insertion process will always be within the Plain-Text boundaries.

V. Research Improvements

A. Reasons for Improvements

An encrypted message must not reveal any information about its origin, so the cryptosystem must make it look as random as possible [15]. In [9] The *Table-Transformation* (TT) is used to produce the *Table-of-Indexes* (TI) which affects the overall security of the proposed encryption algorithm. The researchers proposed five methods to produce the (TI); the methods were Circular Shifts, Swap Cells, Columns Row Swapping (CRSw), same Column Row Swapping or Row Column Swapping (RCSw). The researchers found that the (RCSw) is the best method could be used to produce the (TI). The work presented in [9], suggested randomizing the Initial Table (IT) by swapping one complete row with one complete column, the idea is to add more complexity and randomization on the resulting Transformation Table (TT). The Row Columns Swapping process (RCSw) used in [7] was excluded in [9] since it produced a segmented (TI). The swapping method (RCSw) was considered the best method for the following reasons:

- RCSw was proven to be the best method among other five methods used.
- Using 10-digit Shared-Value (SV), and no need to go beyond this value.
- RCSw using 10-digit Shared-Value produces more segments than the other proposed methods. (More segments mean more cells displacements).

In this work, the researchers believe, more enhancements can be added to the (RCSw) process to get rid of the deficiencies appear on the Transformation Table (TT). The resulted (TT) suffers from the stationary of some cells, they didn't move, also, the resulted (TT) is still segmented, where group of cells were moved for the same distance. By combining the (RCSw) and gets benefits of the idea of the method used in [7] and [9], we could find an optimal method that can eliminate stationary cells and cells segmentations. The optimal method that is free of stationary cells and has less cells segmentations might help to defend the algorithm against cryptanalysis and brute force attacks.

B. The Proposed Improvements

Although, the Row Column Swapping (RCSw) process presented in [9] was used; the proposed enhancement in this work, suggests not only to shift some selective rows and columns, but to shift the entire table including all rows and columns. The researchers believe shifting the whole table contents even for at least one cell distance will add more complexity and randomness over the TT and the TI as well.

The original proposed algorithm consists of many steps; one of them (which are used here) is to generate the *Table-Transformation* (TT) out of the *Initial-Table* (IT), the generation process based on the *random Shared-Value* as an input to produce the *Table-of-Indexes* that is used by *System-Key-Insertion* and *System-Key-Recovery*. The *System-Key-Insertion* inserts the *System-Key* inside the *Scrambled-Text*. The insertion process employs the *Table-of-Indexes* to decide where the *System-Key* is to be inserted, the extracted index is a two-digit length extracted out of the *Table-of-Indexes*.

The new improved process is basically based on the RCSw process, the row column shifting process depends on the value of the last two digits of the Shared-Value. The new method is called Row Colum Shifting (RCSf).

After performing the RCSw process, the whole columns are circularly shifted to the right according to the value of *(n-1)* digit of the Shared-Value, also the whole rows are circularly shifted down according to the value of the (n^{th}) digit of the Shared-Value. The shifting processes the Columns Right Circular Shifts (CRCS) and the Rows Down Circular Shifts (RDCS), guarantee the movement of each individual cell of the IT.

Our hypothesis says, Columns Right Circular Shifts (CRCS) and Rows Down Circular Shifts (RDCS) on the whole table (IT), will produce more randomize (TT) than using (RCSw) only.

The new method formula representation is RCSf = (RCSw followed by CRCS and RDCS); Row Column Shifting is the process of Column Right Circular Shifts followed by Row Down Circular Shifts

C. The Implementation

To validate the correctness of the proposed method, we performed the tests on the same (IT) using two transformation methods RCSw and RCSf methods. We run both methods using seven different Shared-Value lengths (10, 20, 30, 40, 80, 100 and 1000) digits respectively, each Shared-Value was run 30 times, the total number of runs was (7 Shared-Values * 30 runs *2 methods) = 420 runs. After the completing the 30 runs of each individual Shared-Value length, we calculated the new cells locations, then, we ascendingly ordered the resulting TT based on the number of cell displacement, we noticed that, some cells didn't move while others were moved to 1, 2, 3 up to 29 cells, the cells movement ranged from (0 to 29), then we indexed each cell in the new TT table starting from 1 to 256 (the total number of cells are 256 cells). For each Shared-Value runs (30 runs), we calculated the average cells displacement, cells variances, variances between groups and within groups and correlations for each method

D. Research Analysis

RCSw was the best of other 4 methods specially in generating the will-mixed-table [], Method-1 could not generate the will-mixed-table but it had one positive advantage over than RCSw, all the cells of table-of-indexes resulted from Method-1 were changed their location while in RCSw some cells were not changing their initial location specially when using shore Shared-Value length (e.g. 10 or 20).

Since RCSw was the best and Method-1 had one advantage over RCSw, we decided to improve RCSw by taking advantage of Method-1.

The new method was called RCSf, by comparing the Table-of-Indexes resulted from two methods we find that:

- RCSf is better than RCSw when using short Shared-Value-Length, (Fig.5) shows that when using Shared-Value-Length 10, all cells were displaced and changed their location in RCSf, while about 66 cells were not displaced in RCSw, (Fig. 6) shows the resulted tables for both RCSw and RCSf when Shared-Value-Length = 20, it's obvious that increasing Shared-Value-Length improve results of RCSw in terms of number of displaced cells.
- From the correlation table (Table 1), it is obvious that the Shared-Value length = 10, in RCSW indicates very strong correlation between the TT and IT tables, while RCSF shows week correlation between the tables.
- It is notes that while extending the Shared-Value to longer length size, RCSF overweight RCSW obviously for the rest of the Shared-Value lengths.
- The negative correlation in RCSF indicates the randomness of the resulted TT using Shred-Value more than 30 digits length.

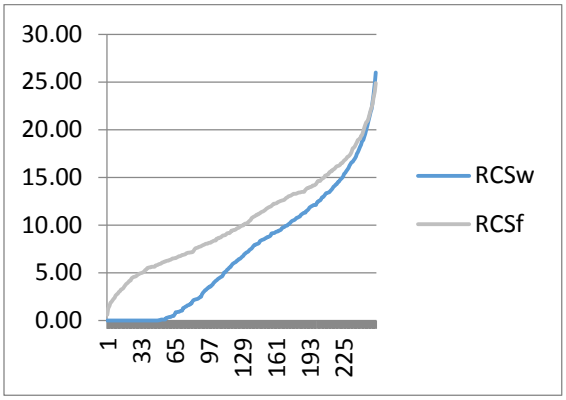

Fig. 5. Shared-Value Length 10

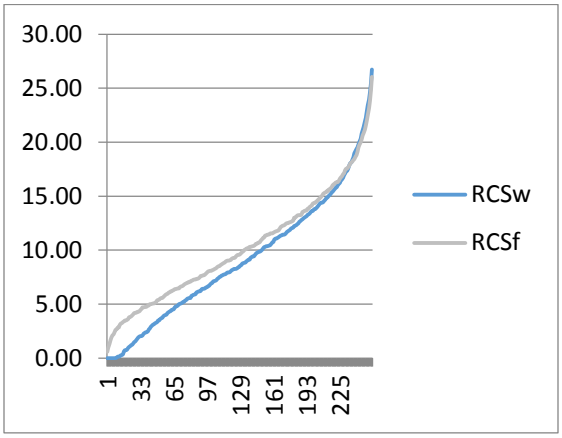

Fig. 6. Shared-Value Length 20

TABLE I. CORRELATION TABLE

Shared Value Length	RCSW	RCSF
10	0.430432021	0.031555991
20	0.149981165	0.00909278
30	0.112991412	-0.029247134
40	0.040089742	-0.008268769
80	-0.007915713	-0.024461118
100	0.002503195	-0.012060659
1000	0.025229386	0.006841883

- The overall assessment of the resulted TT tables by both methods (RCSw and RCSf), definitely indicates the adoption of the new method RCSF.

VI. CONCLUSION

Row Column Swapping followed by Shifting on the Initial Table IT to produce the Transformation Table TT, based on the random values generated by the Shared-Value, even with a relatively small value length (i.e. 10 digits length) produces randomized table, which makes it harder to the cryptanalysis attacks to break the algorithm.

The authors recommend to use Shared-Key value length not less than 30 digits length, in this case the correlation between the IT and TT is weak, here, the attacker will face attack resistance algorithm.

VII. Future Work

More enhancements on the algorithm are exists, where researchers can add substitution techniques, transformation methods, determine the best time to change the Shared-Value or the encryption key, the key exchanging scheme and the best message size to maintain less processing delay.

References

[1] E. J. Gubbi, "Internet Of Things (Iot): Avision, Architectural Elements, And Futuredirections," Future Generation Computer Systems, Pp. 1645-1660 (2013).

[2] E. A. F. D., Internet Of Things (Iot): A Vision, "Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, And Marimuthu Palaniswami," Arxiv Preprint Arxiv, P. 1207, (2012).

[3] N. A. J. Lopez, "Analysis And Taxonomy Of Security/Qos Tradeoff Solutions For The Future Internet," Security And Communication Networks, Security. Com Networks, Pp. 00:1-25, (2013).

[4] G. W. -. Ietf, "Ietf Organisation," 7 Novemebr 2013. [Online]. Available: Https://Www.Ietf.Org/Media/2013-11-07-Internet-Privacy-And-Security.Html. [Accessed 8 Jan 2015].

[5] P. V. O. A. S. V. Alfred Menezes, Handbook Of Applied, Crc Press, (1977).

[6] H. O. B. M. A.-K. R. E. A.-Q. A. M. I. M. Ahmed, "A New Cryptographic Algorithm For The Real Time Applications," In Proceedings Of The 7th Wseas, International Conference On Information Security And Privacy , Cairo, (2008).

[7] B. M. A.-K. A. A. O. Ahmad H. Omari, "Dynamic Cryptography Algorithm For Real-Time Applications Dca-Rta," , Asmcss'09 Proceedings Of The 3rd International Conference On Applied Mathematics, Simulation, Modelling, Circuits, Systems And Signals, P. 1,(2009).

[8] H. O. B. M. A.-K. R. E. A.-Q. A. M. I. M. Ahmad, "Dea-Rta: A Dynamic Encryption Algorithm For The Real-Time Applications," . International Journal Of Computers. 1(3), Pp. 191-199 (2009).

[9] A. Al-Omari, Investigating A Dynamic Crypto Algorithm For Real Time Applications (Dca-Rta), Amman: The University Of Jordan, Master Thesis, (2012).

[10] M. Al-Qaysi, A Shared Value Based Symmetric Crypto System, Amman: Princess Sumaya University For Technology (Psut), Master Htesis, (2014).

[11] G. Durfee, Artist, Cryptanalysis Of Rsa Using Algebraic And Lattice Methods. [Art]. Stanford University, Department Of Computer Science .

[12] J. Lano, Artist, Cryptanalysis And Design Of Synchronous Stream Ciphers. [Art]. Katholieke Universiteit Leuven- Faculteit Ingenieurswetenschappen Arenbergkasteel, B-3001 Heverlee.

[13] J. J. B. J. P. R. Paul Kocher, "Introduction To Differential Power Analysis," J Cryptogr Eng, P. (1):5–27, (2011).

[14] D. N. A. C. M. Yashpalsingh Rajput, "An Improved Cryptographic Technique To Encrypt Text Using Double Encryption," International Journal Of Computer Applications, 86 (6), 24-28, (January 2014).

[15] D. Khovratovich, "Methods Of Symmetric Cryptanalysis," Microsoft Research , Redmond, Usa, (2011).

[16] E. A. Federica Torri, "Next Generation Sequence Analysis And Computational Genomics Using Graphical Pipeline Workflows," Genes, 545-575, (2012).

AUTHOR PROFILE

Ahmad H. Al-Omari, Associate professor of Computer Networks Security, in Science College, Northern Border University, Arar, Kingdom of Saudi Arabia, he received his Ph.D. in computer Information Systems in 2004, he also has long teaching and training record that demonstrates teaching by example, do it yourself training, and hands-on training in attractive ways. He Published research papers in MANET, Encryption, RTA, and e-government. The researcher has more 17 years of business and working experience in the fields of IT, business management, leadership, planning, budgeting, project management, recruitment, E.government and many others. Also he has long academic and teaching experience.