Fifth International Engineering Conference on Developments in Civil & Computer Engineering Applications 2019 - (IEC2019) - Erbil - IRAQ

Hybrid Strategies for Choosing Suitable Cryptosystem Based on Game and Information Theories

Sattar B. Sadkhan- SMIEEE
IT College – Babylon University
Babil- Iraq
drengsattar@ieee.org

Dhilal Mohammad
IT College- Babylon UNiversity
Babil- Iraq
dhilal.mohammad@yahoo.com

Abstract— **This paper provides a new approach for enhancing the security of a computer. This enhancement can be achieved by treatment with the best strategy for executing some chosen crypto-systems on a computer. The enhancement process is done in two stages; the first stage depends on the result of the security evaluation of the crypto-system. The second stage compares several crypto-systems which are evaluated in the first stage.**

This research is a complementary to the previous published papers and focused on comparing different crypto-systems which are strongly different in their securities, and propose the best strategies for their use. The proposed approach used information theory and triangular game as a basic rule in order to provide accurate indicators for the security of crypto-systems, and also used diagonal game to suggest the best strategy to use the cryptosystems.

Keywords— Information Theory; Game Theory; Security Evaluation; Crypto-system.

I. Introduction

Since the beginning of life there is an urgent need to know the value or significance of a particular object in various aspects of human life. Such need is called the evaluation. For example, when buying something from the market, it is necessary to ascertain whether it is valid or not. As a result, the evaluation subject has wide applications in many life aspects, such as education, economics, health, space, industry, computer science, information security and others.

The evaluation process is defined as; the systematic acquisition and assessment information to provide useful feedback about some object [1]. With regard to computer science, cryptology has three basic parts: cryptography, cryptanalysis and security evaluation [2]. The security evaluation of crypto-systems is of great importance not less than cryptography or cryptanalysis.

The wide spread of media technologies has led to an explosion in the use of mobile devices. As a result, the number of connections between individuals increased and the world became like a large village. This requires, all the devices connected to the network to be secure. One method of securing, can be achieved using crypto-systems, which must be evaluated before use to verify the strength of its security.

In order to evaluate the security of cryptosystems, different security evaluation methods have been emerged. At each evaluation method, there are certain parameters related to the evaluated crypto-system that must depend on. These methods have been adopted by several researchers. As an example the researchers in [3] used heuristic security method to evaluate AES, RSA in view point of four attacks (chosen ciphertext, brute force, mathematical, timing). Also researchers in [4][5][6][7] used soft computing techniques to evaluate some symmetric and asymmetric crypto-systems. The unconditional security method was used by researchers in [8].

Researcher in [9], evaluated the security of cryptosystems using the unconditional security and diagonal game. Also researchers in [10], used the unconditional security and triangular game in their evaluation. Researchers in [11], evaluated the key space of cryptosystem based on game theory. In [12], a good resource about using game theory as a security evaluation method for network security.

The structure of this paper is arranged as follows: section II illustrates the security evaluation of cryptosystems. In Section III, the mathematical theories of the proposed system were presented. Section IV is divided into two subsections, the first contains the basic steps of the proposed evaluation method, and the second contains a case study related to the proposed evaluation method. The results can be found in section V, and the last section VI contains the conclusion.

II. Security Evaluation of Cryptosystems

Depending on the type of crypto-system, a specific security evaluation's method has been used. In order to evaluate security of crypto-system using various methods, different particles (elements) of the crypto-system are dealt with.

A. Unconditional Security

This method measures the security of crypto-systems against attacker with unlimited computational resources (time, hardware, software). This method is appeared when scientist Claude Shannon introduced the information theory, which is then known as Shannon's theory. According to Shannon theorem, unconditional security method defines a crypto-system as perfect secrecy system, on the assumption that the length of plain-text, key-text, cipher-text spaces are equal. If the following two conditions are verified: the first, every key in the key space is used with equal probability; The second, there is only unique key for every character's mapping from the plain-text space to the cipher-text space. Based on this

978-1-7281-4377-4/19/$31.00 ©2019 IEEE

method, the limitation of using perfect secrecy crypto-system is the length of the key must be at least as the length of the message and this interpret why one time pad crypto-systems are rarely used [13].

B. Computational Security

This method measures the crypto-system security based on the computational recourses, which are needed by the attacker for breaking it. This method defines a crypto-system as computational secure system from two viewpoints: the concrete approach and the asymptotic approach. In concrete viewpoint, for every attacker, the probability of success for breaking crypto-system is (ε), and the time required is at most (t), then the crypto-system is considered (t,ε)-secure. In asymptotic viewpoint: if the success probability of breaking crypto-system is negligible, for every probabilistic polynomial time attacker, then the crypto-system is secure. This method is practical, but it has not proven assumption. It also weaker than the unconditional security method. Since its strength is measured based on the available computational resources for attacker which are variable with time, i.e. secure computational crypto-system in one time will be insecure computationally with the increased advanced in modern computational technology [14].

C. Provable Security

This method measures the security of crypto-system relative to the difficulty of well-known mathematical problem that the crypto-system rely on. This method is considered as special case of computational security method. The security of crypto-system depends on the computational resources required by the attacker in order to solve its mathematical problems. The most well-known problems that security of the new crypto-systems depend on are the discrete logarithm problem and the integer factorization problem. This security method is very popular and is well known to evaluate public crypto-systems [13] .

D. Heuristic Security

This method measures the security of crypto-system based on its resistance to well-known attacks. This method is considered as weakest method since it does not submit the crypto-system with several possible attacks and consequently it does not consider as formal proof. This method is applied in all types of crypto-systems, each type with its counterpart attacks[15] .

E. Soft Computing Techniques

This method measure the security of crypto-system based on using soft computing techniques such as fuzzy logic, genetic algorithm and NN. Different researchers used one of these techniques or a combination of some of them. In [4], researchers ANFIS evaluator which is a combination of fuzzy logic and artificial neural network. Also they used five parameters in their evaluator to evaluate RSA. In [5], researchers used fuzzy logic to evaluate the security of some chosen block ciphers (RC5, Blowfish, DES). They used key size, number of rounds and block size as inputs to their evaluator. Also researcher in [6] used fuzzy logic to evaluate some knapsack crypto-systems (Luli system, Chor Rivest, Traditional and Advance Adina Diparto Systems). The inputs of the evaluator were the entropy and the density of the knapsack vector.

The ANN is used by researchers in [7] as evaluator. The evaluate the security of the following cryptosystems (Merkle Hellman, Lu-Lee, Goodman-Maculey, Adina di Parto). They considered in their evaluator the density of knapsack vector and the attacking methods applied on the chosen crypto-systems.

F. Statistical Tests

This method measure the security of stream cipher based on the security pseudo-random number generators. This method measures the amount of randomness in the output stream of these generators. Different statistical suits are found such as ENT tests, FIPS 140–1, Diehard battery, NIST Statistical Test Suite, FIPS 140–2 [16].

G. Game Theory

In order to analyze problems of conflict of interest, these problems are formulated as mathematical methods. These methods are known as games under the umbrella of game theory. So different games are used to analyze the conflict of interests between people, groups of people [17]. In Wireless and communication networks, game theory has flourished in this area. Due to this environment reflects different scenarios of competition on limited resources such as frequencies, resources sharing, transmit power, interface management and packet forwarding. Different problems related to network security were analyzed in [12] using game theory.

H. Game Theory and Unconditional Security

This method represents a combination of two security evaluation methods: unconditional security which is represented by information theory and game theory. This method exploits the strength points of both theories. The information theory provides an actual and accurate values related to crypto-system, and game theory analyze the interaction among players which are competed on limited resources. The method includes the values of information theory related to crypto-systems into the framework of game theory and finally solve the game [9],[10].

III. Information and Game Theories

In order to understand the role of information theory in evaluating the security of crypto-systems, the appropriate frame must be considered. The probability theory is the appropriate framework which describes the security of crypto-system against attacker with unlimited resources. Such security is called the unconditional security, information theoretic security or perfect secrecy [13]. The unconditional security has been known after scientific Claude E. Shannon published his paper, "communication theory of secrecy systems", in 1949. In his paper he answered some problems related to perfect secrecy in terms of entropy and redundancy. Such problems are: what is the system's resistance to the attacker when unlimited resources such as time, hardware, software and manpower? Does the encrypted text have a single solution and what is the number of solutions that the encrypted text can carry? How long is the text required for a single solution? [18].

Therefore, the process of evaluating crypto-system begins by calculating set of possibilities from probability theory. These possibilities are related to plain-text, cipher-text and key-text spaces. These possibilities include: plain-text's probability, cipher-text's probability, key-text's probability, joint probability of plain-text and key-text and the conditional probability of plain-text in the presence of cipher-text. The evaluation process continues by calculating a set of entropies from information theory. This set includes plain-text, cipher-text and key-text entropies. Also the joint entropy of the plain-text and key-text, and the conditional entropy of the plain-text given the cipher-text. When the entropies' values of the crypto-system are obtained, the evaluation process using the information theory is done. A detailed example about the security evaluation process of crypto- system can be seen in [8][9].

With regard to the role of game theory in the security evaluation process of crypto-system, there are three abstract methods which are described, by John von Neumann and Oskar Morgenstern, in 1944. These methods represent a general umbrella that encompasses all games in game theory and are formulated to analyze problems in several areas. Depending on the nature of the problem and the factors influencing the problem, the type of adopted method is chosen. The methods are the following: extensive form, characteristic form and normal form [19]. In this paper, emphasis has been placed on games from the normal form method which will be clarified.

The game in this form is characterized by the number of players n, the set of strategies (the strategy space) for each player $N_1, N_2, \ldots\ldots N_n$, and the payoff function that represents a mapping from the Cartesian product of players' strategy spaces $N_1 \times N_2 \times \cdots \times N_n$ into n-dimensional Euclidean space. Games in normal form are used either to study two person's games and are represented by matrix game, or to study n- person's non-cooperative games and are represented by n-dimensional matrix [20].

Solution's methods for static games in normal form can be classified into solutions based on pure strategies and solutions based on mixed strategies as shown in Fig.1. In order to describe these methods, a mathematical definition 1, for non-cooperative static game in strategic must be showed:

Definition 1[20]: Let $G = (\mathcal{N}, (S_i)_{i\in\mathcal{N}}, (u_i)_{i\in\mathcal{N}})$, a non-cooperative game in strategic (or normal) form, where:

- $\mathcal{N}$: finite set of players, i.e., $\mathcal{N} = \{1, \ldots, N\}$.
- S_i : set of player i's strategies.
- $u_i : S \to \mathbb{R}$: player i 's utility function, with $S = S_i \times \ldots \times S_i \times \ldots \times S_N$ (Cartesian product of the strategy sets).

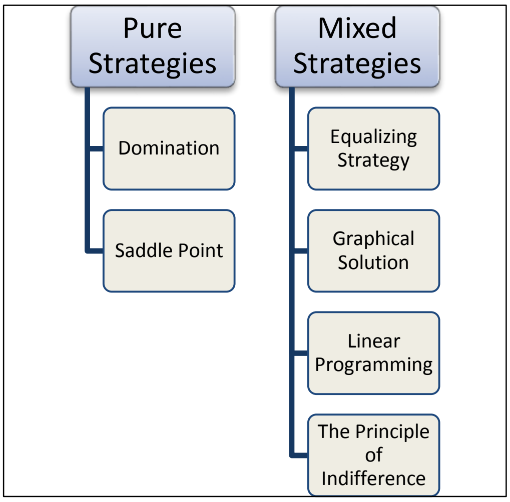

Fig. 1. Solutions' Methods for Normal Form Game

One of the popular games used for analyzing problems in wireless and communication networks is zero- sum game. For example, a security game is zero-sum which is used for representing the interaction between two parities defender and attacker [20]. The solutions' methods in Fig. 1, are only suitable for two person's zero-sum static game in normal form where the strategy set are finite and discrete.

Two games, diagonal game and triangular game, are mentioned in this paper. These games can be solved based on useful principle called the principle of indifference. This principle states that Player1 searches for a strategy that makes Player2 is indifferent as to which of the (good) pure strategies to use. Similarly, Player2 should play in such a way to make Player1 is indifferent among his (good) strategies [21]. These games can be solved based on the ideas in the following theorem.

Theorem (1) [21]: Suppose a game matrix A with $m \times n$, the value of the game V. Let any optimal strategy for player1 be $p = (p_1, \ldots., p_m)^T$ and any optimal strategy for player2 be $q = (q_1, \ldots., q_n)^T$, then $\sum_{j=1}^{n} a_{ij} q_j = V$, for all i for which $p_i > 0$. And $\sum_{i=1}^{m} p_i a_{ij} = V$ for all j for which $q_j > 0$.■

Triangular game is used in the security evaluation process of cryptosystem by including values in certain positions of the triangular matrix. These values are computed from information theory. A detailed example about the security evaluation process can be seen in [10].

Also diagonal game is used in the security evaluation process of cryptosystems by including values in certain positions of the diagonal matrix. These values are computed from information theory. A detailed example about the security evaluation process can be seen in [9].

IV. A Proposed Cryptosystems' Security Evaluation Method

A. *How to Evaluate Cryptosystem's Security Using the Proposed Method*

The proposed system in Fig. 2, employs two of the important mathematical theories, namely the information and game theories.

1) Determine the number of crypto-systems N to be used on a terminal.
2) Evaluate each of the determined crypto-systems using information theory by following these steps.
   a) Specify the space for each of the plain-text, cipher-text and key-text.
   b) Calculate the independent probabilities for the specified spaces, the joint probability and the conditional probability.
   c) Calculate the entropies for the plain-text, cipher-text and key-text.
   d) Calculate the joint and the conditional entropies for the specified spaces. And make sure about the validity of the calculation process.
   e) Include the values of the calculated entropies at specific sites in the triangular matrix of the triangular game.
   f) Solve the triangular game and calculate the value of the game.
3) Repeat the step (2), N times, and store the results' values of evaluation for all chosen cryptosystems.
4) Include values of crypto-systems' security evaluation stored in step (3), in specific locations of the diagonal matrix.
5) Solve the diagonal matrix of the diagonal game and calculate the probabilities of players.

B. *Case Study*

At the beginning, three crypto-systems are chosen for security evaluation, which are additive, multiplicative and affine. Each one of the chosen crypto-systems must be evaluated as it has been explained in [9]. The chosen plaintext was "transposition ciphers rearrange characters according to some scheme".

First, Shannon's entropies for each crypto-systems are computed. The results of computing Shannon's entropies are shown in TABLE I.

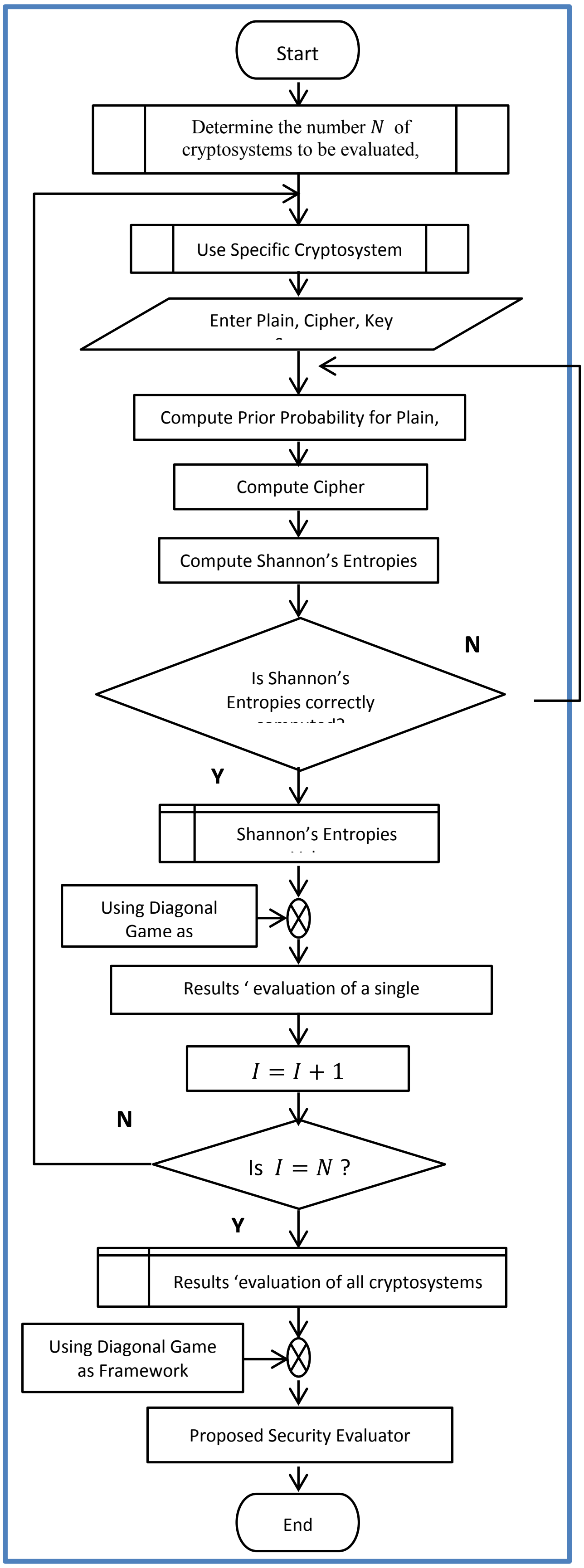
Start
Determine the number N of cryptosystems to be evaluated,
Use Specific Cryptosystem
Enter Plain, Cipher, Key
Compute Prior Probability for Plain,
Compute Cipher
Compute Shannon's Entropies
Is Shannon's Entropies correctly
N
Y
Shannon's Entropies
Using Diagonal Game as
Results ' evaluation of a single
$I = I + 1$
N
Is $I = N$?
Y
Results 'evaluation of all cryptosystems
Using Diagonal Game as Framework
Proposed Security Evaluator
End

Fig. 2. Flow Chart for the Proposed Security Evaluation Method

TABLE I. SHANNON'S CRITERIA OF SOME CHOSEN CRYPTO-SYSTEMS

		Shannon's Criteria				
		plain entropy	key entropy	cipher entropy	joint entropy	conditional entropy
Crypto-system	**Multiplicative**	3.631	3.459	4.576	7.091	2.514
	Additive	3.631	4.644	4.698	8.275	3.576
	Affine	3.631	8.285	4.700	11.916	7.216

As it was explained in [10], and in order to evaluate the security of each chosen cryptosystem, the values of Shannon entropies in TABLE I., will be including in triangular matrix of triangular game for each chosen crypto-systems, as shown in TABLES II. , III, and table IV. respectively.

TABLE II. TRIANGULAR GAME WITH VALUES OF SHANNON'S ENTROPIES FOR MULTIPLICATIVE

	Player2			
Player1	4.576	-2.513	3.459	-3.631
		4.576	-2.513	3.459
			4.576	-2.513
				4.576

TABLE III. TRIANGULAR GAME WITH VALUES OF SHANNON'S ENTROPIES FOR ADDITIVE

	Player2			
Player1	4.698	-3.576	4.644	-3.631
		4.698	-3.576	4.644
			4.698	-3.576
				4.698

TABLE IV. TRIANGULAR GAME WITH VALUES OF SHANNON'S ENTROPIES FOR AFFINE

	Player2			
Player1	4.700	-7.216	8.285	-3.631
		4.700	-7.216	8.285
			4.700	-7.216
				4.700

In order to solve Triangular game of Multiplicative, Additive and Affine crypto-systems in TABLES II. , III., IV. respectively, the method in [10] will be followed, the results of solving these game are shown in TABLE V.

TABLE V. RESULTS OF FIRST PROPOSED METHOD FOR THREE CHOSEN CRYPTO-SYSTEMS

Crypto-systems	Value of Triangular Game
Multiplicative	0.940
Additive	0.908
Affine	0.535

Now, to compute the best strategy for executing the chosen cryptosystems on computer, the method in [9] is followed. And consequently, the values in TABLE V, are included in diagonal matrix of diagonal game as shown in TABLE VI.

TABLE VI. DIAGONAL GAME WITH RESULTS OF FIRST PROPOSED METHOD

PLAYERS	**II (designer)**			
I (Evaluator)	**STRATEGIES**	**Multiplicative**	**Additive**	**Affine**
	Mulipli cative	*0.940*	*0*	*0*
	Additive	0	0.908	0
	Affine	0	0	0.535

Now, it is time for computing strategies vector for Player1 (p1,p2,p3) , for Player2 (q1, q2,q3) and the value of the diagonal matrix in TABLE VI.

$$V = (\sum_{i=1}^{m} 1/d_i)^{-1} \qquad (1)$$

$$= (1/0.940 + 1/0.908 + 1/0.535)^{-1}$$

$$= (4.03431)^{-1}$$

$$= 0.248$$

$$p_i = q_i = \frac{V}{d_i} \qquad \text{for } i = 1, \dots m \quad (2)$$

$$p_1 = q_1 = 0.248/0.940 = 0.262$$

$$p_2 = q_2 = 0.248/0.908 = 0.272$$

$$p_3 = q_3 = 0.248/0.535 = 0.461$$

V. Results of the Proposed Method

The results of solving diagonal game is shown in TABLE VII.

TABLE VII. Results of Second Proposed Method for three Chosen Crypto-systems

Crypto-systems	Values of Triangular Games	Value of Diagonal Game	Players' strategies: The Used Crypto-system	Values of Strategies
Multiplicative	0.940	0.248	**p1, q1: Multiplicative**	0.262
Additive	0.908		**p2, q2: Additive**	0.272
Affine	0.535		**P3, q3: Affine**	0.461

In TABLE VII., three chosen crypto-systems (multiplicative, additive, affine) are evaluated. The values of the triangular games represent the weakness of each chosen crypto-system. Suppose a computer employs more than one cryptosystem, and game theory can be used to draw the best strategy for executing these crypto-systems.

The viewpoint is related to time, suppose a computer uses one crypto-system from the available chosen crypto-system. Game theory advises us instead of using one crypto-system in certain full period of time, it is best to use first crypto-system (multiplicative) with probability (0.262) of full period, second crypto-system (additive) with probability (0.272) of full period and third crypto-system (Affine) with probability (0.461) of full period, to reduce the weakness to (0.248) instead of (0.940, 0.908, 0.535).

VI. Conclusions

Information Theory is used to compute the security criteria for each chosen crypto-system. The results of applying the information theory and triangular game represent an evaluation for each crypto-system. After determining the weakness for each chosen crypto-system. Now diagonal game is used to draw the best strategies for playing the game. Playing the game refers to how can one use the crypto-systems with different security' weakness. Diagonal game in the proposed evaluator, can be seen as search game where two players want to find **something** (**that is, reducing inherent cryptosystems' security weakness**). Diagonal game gives an advice for searching something with minimum resources such as time or hardware. And also it can be used in another application.

References

[1] P. N. Lakshmi Shanmugam, Evaluation of Learning, Laxmi Book Publication, 2016.

[2] S. B. Sadkhan and N. A. Abaas, "Chapter 1- Multidisciplinary in Cryptology", from book, "Multidisciplinary Perspectives in Cryptology and Information Security", IGI Global, 2014.

[3] A. Al Hasib and A. M. Mahmudul Haque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography" Third 2008 International Conference on Convergence and Hybrid Information Technology, IEEE, 2008.

[4] S. B. Sadkhan and F. H. Abdulraheem, " A Proposed ANFIS Evaluator for RSA Crypto-system used in Cloud Networking " 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT), IEEE, 2017.

[5] S. A. Mohammed and S. B. Sadkhan, "Block Cipher Security Evaluation Based on Fuzzy Logic" The First International Conference of Electrical, Communications, Computer, Power and Control Engineering ICECCPCE'13/December 17-18, IEEE, 2013.

[6] S. B. Sadkhan, A. H. Nasef and S. F. Jawad, " Complexity Evaluation of Knapsack Crypto System using Fuzzy Set", Journal of Basrah Researches ((sciences)), 2011.

[7] S. B. Sadkhan, N. A. Abbas and M. K. Ibrahim, "A PROPOSED SECURITY EVALUATOR FOR KNAPSACK PUBLIC KEY CRYPTO-SYSTEMS BASED ON ANN", IEEE, 1997.

[8] D. M. Reda, Security Evaluation of Crypto-systems Based on Information Theory, Master Thesis, College of Science, Babylon University, 2013.

[9] S. B. Sadkhan and D. M. Reda, "Cryptosystem Security Evaluation Based on Diagonal Game and Information Theory", International Conference on Engineering Technologies and their Applications-2018,ICETA-2018, IEEE, 2018.

[10] S. B. Sadkhan and D. M. Reda, " A Proposed Security Evaluator for Cryptosystem based on Information Theory and Triangular Game", International Conference on Advanced Science and Engineering 2018 (ICOASE2018), IEEE, 2018.

[11] S. B. Sadkhan and D. M. Reda, "Best Strategies of Choosing Crypto-System's Key for Cryptographer and Attacker Based on Game theory", New Trends in Computing, Communications, and Information Technology, NTCCIT- 2018, IEEE, 2018.

[12] S. Kim, "Chapter 6- Game Theory for Network Security", from book, "Game Theory Applications in Network Design", IGI Global, 2014, pp. 158-171.

[13] D. Stinson, Cryptography: Theory and Practice. CRC Press, CRC Press LLC, 1995.

[14] J. Katz and Y. Lindell, "Chapter 2- Perfectly-Secret Encryption", from book, "INTRODUCTION TO MODERN CRYPTOCRAPHY", Taylor & Francis Group LCC, 2008.

[15] C. Douligeris and D. N. Serpanos, NETWORK SECURITY Current Status and Future Direction. John Wiley & Sons, Inc., Publication, 2007.

[16] D. Bucerzan, M. Craciun, V. Chis and C. Ratiu, "Stream Ciphers Analysis Methods" Int. J. of Computers, Communications & Control, vol. V(2010), pp. 483-489, 2010.

[17] L.C. Thomas, "Chapter 1- The game's afoot", from book, "GAMES, THEORY AND APPLICATIONS", Dover Publications, 2003

[18] C. E. Shannon, "Communication Theory of Secrecy Systems" Bell System Technical Journal, vol. 28-4, pp. 656-715, Oct. 1949.

[19] W. F. Lucas, "GAME THEORY and its Applications". American Mathematical Society, 1989.

[20] Z. Han, D. Niyato, W. Saad, T. Basar, and A. Hjorungenes, Game Theory in Wireless and Communication Networks Theory, Methods, and Applications. Cambridge University Press, 2012.

[21] T. S. Ferguson, "Chapter 2- Two-Person Zero-Sum Games", from book, GAME THEORY,UCLA, 2008.