Best Strategies of Choosing Crypto-System's Key for Cryptographer and Attacker Based on Game Theory

Dr.Sattar B. Sadkhan[1] and Dhilal M. Reda[2]
[1,2]IT College , University of Babylon, IRAQ
[1]drengsattar@ieee.org , [2]dhilal.mohammad@yahoo.com

***Abstract*— One of the most important strength features of crypto-system's is the key space. As a result, whenever the system has more key space, it will be more resistant to attack. The weakest type of attack on the key space is Brute Force attack, which tests all the keys on the ciphertext in order to get the plaintext. But there are several strategies that can be considered by the attacker and cryptographer related to the selection of the right key with the lowest cost (time). Game theory is a mathematical theory that draws the best strategies for most problems. This research propose a new evaluation method which is employing game theory to draw best strategies for both players (cryptographer & attacker) .**

***Keywords*— game theory; security evaluation; crypto-system; key space .**

I. INTRODUCTION

In cryptology, there are three types of sciences (cryptography, cryptanalysis, evaluation) [1]. What distinguishes the cryptographer from the cryptanalyzer is the possession of the key. While the first converts the plaintext to ciphertext using a secret key and cryptosystem, the second converts the ciphertext to the plaintext using the same cryptosystem without having the key, and this requires an extraordinary effort.

On the subject of evaluation, it is defined as the systematic acquisition and assessment of information to provide influence useful feedback about some object [2] and evaluation is an independent and supportive phase for cryptography.

The understanding of any problem and knowledge of the stages of the problem and what variables that affect the problem and the weight or impact of each variable can be considered a kind of evaluation. Therefore, game theory was chosen as a mathematical tool that accurately contributes to the analysis of the problem and to know the effect of each variable on the problem as a whole. In order to formulate any conflicting positions mathematically, game theory provides a general and accurate framework to describe the best behavior of players involved in such situations. One of the lawyers said, when I am getting ready to reason with a man, I spend one-third of my time thinking about myself and what I am going to say and two-thirds about him and what he is going to say [3]. this indicate to, that game theory is applied in our life without feeling it. Depending on the type of crypto-system, specific security evaluation's model can used. In order to evaluate security of crypto-system using various models, different particles (elements) of the crypto-system are dealt with. For example, in [4] the outputs of the crypto-system are sometimes used as in the evaluation of the stream cipher using statistical tests. Also, in [5], inputs (plain space & key space) and output (cipher space) of crypto-system are employed for information theory to evaluate the security of symmetric crypto-systems.

Game theory is an effective and an accurate tool, so it can be used as a security evaluation model. It reveals what are the best behaviors for players involved in the game (problem), by reaching a state of balance in which each player is convinced of what he has, and there is no intention to change his state. The first player is convinced of the minimum profit he earns and the second player is convinced of the maximum loss he loses. Game theory explains the best behavior for cryptographer and attacker during choosing their keys from key space in order to achieve their goals with minimum cost (time) [6].

Various researches are used the game theory in the evaluation process such as researcher in [7] showed a survey on using game theory for network security. Also, an attractive chapter showed a detailed source about using game theory in network security can be found in [8]. Researchers suggested an evaluation security model of crypto-systems, has been employed game theory (diagonal game) and information theory, can be found in [9]. Also, another evaluation model for crypto-system security which is employed game and information theories is suggested by researchers in [10].In this paper, security evaluation is applied on the key space of crypto-system using only game theory as a new evaluation model.

In this paper gambit software (software tools for game theory graphical interface, Version 15.1.1), is used to solve the matrix game[11].

The structure of this paper includes an overview of cryptography and cryptanalysis is showed in section II, specific type of game theory related to the proposed model is clarified in section III, section IV consists of two sections handles the basic steps of the proposed mathematical model and case study. Results of the proposed model are showed in section V. and conclusions in the last section.

978-1-5386-8452-8/18/$31.00 ©2018 IEEE

II. An Overview Of Cryptography And Cryptanalysis

Under the umbrella of cryptology, there are three types of sciences: cryptography which is related to making secret codes, cryptanalysis which is related to breaking secret codes and evaluation which is related to evaluate the security of secret codes. Theses secret codes are also known as crypto-systems [1]. In Cryptography, two parities (sender and receiver) are securely intended to communicate with each other using crypto-systems over insecure channel. In cryptanalysis, parities other than sender and receiver are securely access the channel and trying to get information about what is being sent.

The purpose of applying cryptography is to achieve the following objectives: confidentiality (keeping information secret from unauthorized parities), data integrity (keeping information unaltered by unauthorized parities), entity authentication (verifying the identity of entity), non-repudiation (preventing an entity from denying its previous commitments).

The basic component that makes cryptography, cryptanalysis and evaluation under one umbrella is the crypto-system. The crypto-system consists of: plaintext space, ciphertext space, keytext space, encryption algorithm and decryption algorithm [12]. Cryptographer Auguste Kerckhoffs was stated its principle related to cryptography: A crypto-system should be secure even if everything about the system, except the key, is public knowledge [13], and this saying indicates to the security of crypto-system heavily depending on keytext space.

In cryptanalysis, attacker analyzes crypto-system, taking advantage of weaknesses in the crypto-system that he can detects, to restore plaintext and/or key from ciphertext. This weakness can be interpreted as (statistical properties of plaintext's language, internal structure of encryption system (software or machine), information that is believed to be contained in the plaintext(cribs)) [14].

Information theory provided an important model to prove the security of the crypto-system called provable security. There is no crypto-system throughout the ages that verifies provable security except one-time pad which was invented by engineer Gilbert Vernam in 1917. One-time pad was proved to be provable secure in 1947 by scientist Claude Shannon. This leads to the fact that there is no secure developed crypto-system unless it achieves the provable security concept and consequently it can withstand the attacks [15]. At each time different crypto-system was appeared and on the other hand, there was an attack to thwart it, e.g. In classical cipher such as transposition cipher (scytale, column transposition, keyword columnar transposition), where the letters of the plaintext are rearranged in order to get a ciphertext and key must has information about how to get back plaintext from ciphertext. Transposition cipher was exposed to divide and conquer attack. Substation cipher such as, viginere cipher, is exposed to statistical attacks (index of coincidence). Hill cipher was exposed to attack exploiting the linearity of the underlying cipher. Weakness of codebook ciphers concentrated around preserving the codebook and it also exposed to statistical attacks.

In world war II, different ciphers such as enigma, purple and sigaba were appeared in German, Japan and America respectively. One of the weaknesses in these machine ciphers was the key space, i.e. engima is monoalphabetic substitution cipher with permutation representing by the initial setting of enigma. Germans were confident that the system was unbreakable because it had a large key space (2^{366}), but in fact the effective key space (2^{77}) was far less effective than they thought, and thus the system was broken [16].

Consequently, modern crypto-systems have tended to increase the effective key space to ensure that the system would not be broken. E.g. when applying brute force attack using a supercomputer to crack the 128-bit AES key, it would take 1 billion billion years i.e. more than the age of the universe (13.75 billion years). If one uses a supercomputer to recover a DES key in a second , it would takes 149 trillion years to crack a 128-bit AES key using the same supercomputer [17].

In this paper, the relation between attacker and cryptographer in choosing the appropriate key from the key space will be investigated using game theory.

III. Two-Persons Zero-Sum Game (Game Theory)

Game theory is a mathematical theory that examines situations involving conflict over limited resources by two or more competitors. These competitors or so-called players are characterized by being rational, i.e. every player tries to achieve the greatest profit for himself and avoid the least lost. When the game theory consists of one player, it is called decision theory. Game theory differs from decision theory in which the decision-maker, the first player, makes a decision versus an irrational player (nature), the second player, who makes his decisions randomly.

There are three formulations of games in game theory: characteristic function game, extensive form game and strategic form game. In this paper, the simplest type, strategic form game or so called matrix game is used.

In order to formulate a problem or competitive situation in strategic form game, four elements must be specified:

1) Number of players.
2) Strategies of each player.
3) Payoff table, the entries of payoff table representing the payoff for each combination of players' strategies.
4) Utility function to compute the payoff value in the payoff table.

Two-persons zero-sum game, as its name stated, consists of two non-cooperative players. The profit for one player considers as a loss for the other and consequently their summation is zero [6][18].

In order to formulate the problem of this research as two-persons zero-sum game, two players are represented by attacker (guesser) and cryptographer (chooser). The attacker continuously guesses what is the used key by the cryptographer

to encrypt the plaintext and get the available ciphertext. At the other side, the cryptographer chooses only one key to encrypt the plaintext from a position in the key space that makes its competitor (attacker) in a confused state.

Game theory accurately determines what is the best situations for attacker and cryptographer to choose their keys from the key space of any crypto-systems.

IV. A Proposed Mathematical Model For Studying The Behavior of Crypto-system's Players Based on Game Theory

A. Basic Steps to describe The Proposed Mathematical Model

The proposed system employs one of the important mathematical theories, namely the game theory. This system examines the behavior of both cryptographer and attacker in how to choose the appropriate key to encrypt plaintext or to decrypt ciphertext related to a particular crypto-system .

1) Choose a specific crypto-system (Affine, Additive, Multiplicative) and specify its own key space.
2) Choose how many times the key space is divided.
3) Determine the type of the game that will be used in order to study Player's behavior.
4) Define the players of the game .
5) Define players' strategies .
6) Determine how the payoff function is calculated.
7) Build a game matrix that contains payoff values for both players.
8) Solve the game based mixed strategies (using gambit software).

B. Case Study

1) Assuming that the chosen crypto-system is the affine, so the key space is equal to *312*, since $E(x) = (ax+b) \bmod m$, the key space of $a=12$ the key space of $b=26$, so *total key space =312*.
2) Suppose the key space is divided into three parts (the number of divisions is determined as the evaluator wants), so that each part contains *104* keys. i.e. key space
$K=\{(1,2,\ldots 104),(105,106,\ldots,208),(209,210,\ldots,312)\}$
3) Two-person zero-sum game is used to build the proposed mathematical model.
4) The players of the game are the attacker and the cryptographer. The cryptographer has one key to encrypt plaintext. The attacker has no specific key and needs to think about strategy that make him choose the right key with minimum cost (time).
5) The two players have the same three strategies (the number of strategies are as much as the number of divisions in the key space) .

Referring to TABLE I., The three strategies of the players are the extent to which the player chooses the key. The first strategy is to experiment the keys sequentially within the range of 104 to 1. The second strategy is to experiment the keys sequentially within the range of 208 to 1. The third strategy is to experiment the keys sequentially within the range from 312 to 1.

TABLE I. PLAYERS'S STRATEHIES OF AFFINE CIPHER

S3		
S2		
S1		
1,2,3,…,104	***105,106,107,…,208***	***209,210,211,..312***

Because both the functions of the cryptographer and the attacker are completely different, the number of attempts to select the key is different. Where the cryptographer knows the section of the key space in which the key will be chosen. Also he knows what is the key needed to convert the plaintext to the ciphertext. Conversely, the attacker does not know what is the key. Also, he does not know in which section of the key space he must searches the keys (i.e. what is the strategy has been used by the cryptographer), as shown in TABLE II. .

TABLE II. NUMBER OF ATTEMPTS FOR BOTH PLAYERS

	Attacker(guesser)		
Cryptographer(chooser)	***S1***	***S2***	***S3***
S1	***1,104***	***1, 208***	***1, 312***
S2	***1,-104***	***1,104***	***1, 208***
S3	***1, -104***	***1, -208***	***1, 104***

6) To calculate the Payoff function , one must consider the number of attempts of both players and whether these attempts led to access the correct key or not.

$$Payoff\ function = A+R+P \qquad (1)$$

Where variable A is the number of attempts without access to the right key. Due to the nature of two-person zero-sum game which requires the amount of what the first player earns is a loss for the second player. The variable A will take positive sign for cryptographer and negative sign for attacker.

The variable R means a reward for getting the right key and the variable P means a punishment for losing the right key. The variables R and P must have the same values, but one of them is negative when it is a punishment P and a positive when it is a reward R. In addition, these values are imposed on the condition that their values are higher than all the values in the TABLE III., here it is imposed as much as the

size of the key space, where imposed as much as the size of the key space.

TABLE III. APPLYING PAYOFF FUNCTION FOR PLAYERS' STRATEGIES

		Attacker(guesser)		
Cryptographer(chooser)		S1	S2	S3
	S1	103+P , -103+R	207+P, -207+R	311+P, -311+R
	S2	104+R , -104+P	103+P,-103+R	207+P, -207+R
	S3	104+R, -104+P	208+R, -208+P	103+P, -103+R

7) In TABLE IV. the values of the game matrix are computed using the payoff function in the previous step.

TABLE IV. GAME MATRIX OF AFFINE CIPHER

		Attacker(guesser)		
Cryptographer(chooser)		S1	S2	S3
	S1	-209 , 209	-105, 105	-1, 1
	S2	416, -416	-209, 209	-105, 105
	S3	416, -416	520 , -520	-209, 209

8) To solve this game, gambit software is used as illustrated in table. I.

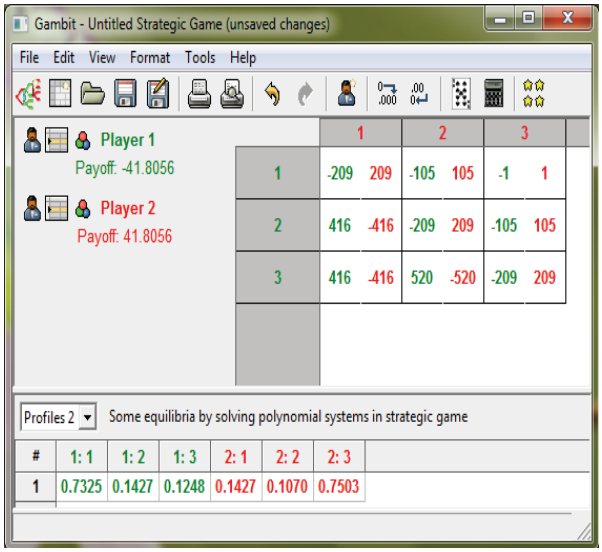

Fig. 1. Values of solving matrix game using gambit.

So the probabilities for playing the strategies of the first player (attacker) and the second player (cryptographer) will be illustrated in TABLE V.

Here the imposed values of reward and punishment respectively: $R=+312, P=-312$.

TABLE V. PROBABILITIES OF PLAYERS' STRATEGIES

Cryptographer(chooser)		
S1	S2	S3
0.7325	0.1427	0.1248
Attacker(guesser)		
S1	S2	S3
0.1427	0.1070	0.7503

V. RESULTS OF PROPOSED BEHAVIORAL MATHEMATICAL MODEL

A. *Results of applying proposed model on Additive cipher:*

In TABLE VI., Players' strategies, i.e. the available range of keys that can be used by players.

TABLE VI. PLAYERS'S STRATEHIES OF ADDITIVE CIPHER

S3		
S2		
S1		
1,2,3,…,8	9,10,11,…,16	17,18,19,..25

In TABLE VII., the number of attempts for both players, in which the first player (cryptographer) needs only one attempt and the second player (attacker) needs one or more than attempts, in order to achieve their goals.

TABLE VII. NUMBER OF ATTEMPTS FOR BOTH PLAYERS

		Attacker(guesser)		
Cryptographer(chooser)		S1	S2	S3
	S1	1,8	1, 16	1, 25
	S2	1,-8	1,8	1, 17
	S3	1, -8	1, -16	1, 9

In TABLE VIII., applying the payoff function which consist of adding the number of failure attempts and the punish or reward to the players in case they find a key or not according to their preferences.

TABLE VIII. APPLYING PAYOFF FUNCTION FOR PLAYERS' STRATEGIES

		Attacker(guesser)		
Cryptographer(chooser)		S1	S2	S3
	S1	7+P , -7+R	15+P, -15+R	24+P, -24+R
	S2	8+R , -8+P	7+P,-7+R	16+P, -16+R
	S3	8+R, -8+P	16+R, -16+P	8+P, -8+R

In TABLE IX., the payoff values for both players.

TABLE IX. GAME MATRIX OF ADDITIVE CIPHER

		Attacker(guesser)		
Cryptographer(chooser)		S1	S2	S3
	S1	-18 , 18	-10, 10	-1, 1
	S2	33, -33	-18, 18	-9, 9
	S3	33, -33	41 , -41	-17, 17

In TABLE X., the probabilities values for both players. These values showed that the payoff for one player is the reverse payoff value of the other player and this due to the nature of the game, two person zero sum game. Also the values (0.7301, 0.1356, 0.1343) indicate to the probabilities that the first player (cryptographer) must be followed in order to achieve the available payoff. Assuming that the number of attempts to be made by the first player is n, the game theory shows that the best behavior of the first player is to choose his or her keys from the range of the first strategy with a number of attempts equal to $n*0.7301$, from the range of the second strategy with a number of attempts equal to $n*0.1356$ and from the range of the third strategy with a number of attempts equal to $n*0.1343$. The same thing for the values (0.1356, 0.1032, 0.7612) which are indicate to the probabilities that the second player (attacker) must be followed in order to achieve the available payoff.

TABLE X. PROBABILITIES OF PLAYERS' STRATEGIES

Cryptographer(chooser)		
S1	S2	S3
0.7301	0.1356	0.1343
Attacker(guesser)		
S1	S2	S3
0.1356	0.1032	0.7612

B. Results of applying proposed model on Multiplicative cipher:

In TABLE XI., Players' strategies, i.e., the available range of keys that can be used by players.

TABLE XI. PLAYERS'S STRATEHIES OF MULTIPLICATIVE CIPHER

S3		
S2		
S1		
1,2,3,4	5,6,7,8	9,10,11

In TABLE XII., the number of attempts for both players, in which the first player (cryptographer) needs only one attempt and the second player (attacker) needs one or more than attempts, in order to achieve their goals.

TABLE XII. NUMBER OF ATTEMPTS FOR BOTH PLAYERS

		Attacker(guesser)		
Cryptographer(chooser)		S1	S2	S3
	S1	1,4	1, 8	1, 11
	S2	1,-4	1,4	1, 7
	S3	1, -4	1, -8	1, 3

In TABLE XIII., applying the payoff function which consist of adding the number of failure attempts and the punish or reward to the players in case they find a key or not according to their preferences.

TABLE XIII. APPLYING PAYOFF FUNCTION FOR PLAYERS' STRATEGIES

		Attacker(guesser)		
Cryptographer(chooser)		S1	S2	S3
	S1	3+P , -3+R	7+P, -7+R	10+P, -10+R
	S2	4+R , -4+P	3+P,-3+R	6+P, -6+R
	S3	4+R, -4+P	8+R, -8+P	2+P, -2+R
	S3	4+R, -4+P	8+R, -8+P	2+P, -2+R

In TABLE XIV., the payoff values for both players.

TABLE XIV. GAME MATRIX OF MULTIPLICATIVE CIPHER

		Attacker(guesser)		
Cryptographer(chooser)		S1	S2	S3
	S1	-8 , 8	-4, 4	-1, 1
	S2	15, -15	-8, 8	-5, 5
	S3	15, -15	19 , -19	-9, 9

The interpretation of results in TABLE X. is also applied on the values in TABLE XV. .

TABLE XV. PROBABILITIES OF PLAYERS' STRATEGIES

Cryptographer(chooser)		
S1	S2	S3
0.7551	0.1481	0.0968
Attacker(guesser)		
S1	S2	S3
0.1481	0.1099	0.7419

Also it can be seen form TABLE V., TABLE X., TABLE XV., that the probabilities' values of the first player's strategies vary from the greater value of the first strategy to the median value of the second strategy, down to the small value of the third strategy. Also the probabilities' values of the second player's strategies vary from the greater value of the third strategy to the median value of the first strategy, down to the small value of the second strategy. In TABLE XVI. the model is applied on some chosen crypto-systems. The key space of crypto-systems is divided into four parts in order to investigate the best behavior for the players.

TABLE XVI. PROBABILITY OF PLAYERS' STRATEGIES WITH KEY SPACE DIVIDED INTO FOUR DIVISIONS

Multiplicative	*Cryptographer(chooser)*			
	S1	*S2*	*S3*	*S4*
	0.7187	*0.1154*	*0.1034*	*0.0625*
	Attacker(guesser)			
	S1	*S2*	*S3*	*S4*
	0.1154	*0.0915*	*0.0744*	*0.7188*
Additive	*Cryptographer(chooser)*			
	S1	*S2*	*S3*	*S4*
	0.6980	*0.1053*	*0.0952*	*0.1014*
	Attacker(guesser)			
	S1	*S2*	*S3*	*S4*
	0.1053	*0.0852*	*0.0704*	*0.7391*
Affine	*Cryptographer(chooser)*			
	S1	*S2*	*S3*	*S4*
	0.6984	*0.1110*	*0.0999*	*0.0908*
	Attacker(guesser)			
	S1	*S2*	*S3*	*S4*
	0.1110	*0.0888*	*0.0727*	*0.7276*
	S1	*S2*	*S3*	*S4*
	0.1110	*0.0888*	*0.0727*	*0.7276*

The results of applying the proposed model on the same chosen crypto-systems with key space divided into four parts are showed in TABLE XVI.. the probabilities' values of the second player's strategies vary from the greater value to the small value for the strategies third, first, second and fourth.

VI. CONCLUSIONS

Since the security evaluation of crypto-system is an important subject, a new mathematical model based game theory is proposed. Game theory draws the best behavior (i.e. nash equilibrium) of choosing key from the key space for both players (cryptography and attacker). Since the modern approach to achieve the security of the crypto-system based on increasing the key space, it was necessary to create a mathematical model to evaluate the security of the crypto-system concentrating on the used key space. The proposed model draws for both players, the best strategies that must be followed. Suppose a specific cryptosystem exposes to brute force attack, instead of an attacker employs its hardware abilities to search the all the key space of specific cryptosystem, he/she can concentrate on specific section of the key space using the same abilities. And consequently, he/she can achieve his/her goal with minimum time. The same thing for cryptographer who wishes to follow a strategy that leaves attacker with worst case. It is necessary to said that when the number of divisions in the key space increase, it will be useful to determine best strategies for both players.

REFERENCES

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

[2] Available at http://www.socialresearchmethods.net/kb/intreval.php

[3] Availableat https://www.brainyquote.com/quotes/abraham_lincoln_164051

[4] S. B. Sadkhan and D. M. Reza, " Investigation of the Best Structure for the Nonlinear Combining Function", Annual Conference on New Trends in Information & Communications Technology Applications-(NTICT'2017), IEEE, 7 - 9 March 2017.

[5] D. M. Reda, "Security Evaluation of Cryptosystems Based on Information Theory", M.Sc. Thesis, University of Babylon, Science College, 2013.

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

[7] X. Liang and Y.Xiao, "Game Theory for Network Security", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, IEEE, 2012.

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

[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 , 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] Free software, available at: http://www.gambit-project.org.

[12] D.R. Patel, "Chapter 1- Overview of Information Security and Cryptography", from book, "INFORMATION SECURITY- Theory and Practice", Prentice-Hall of India Private Limited, 2008

[13] Kerckhoffs's principle – Wikipedia, Available At https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle

[14] A. G. Konheim, "Chapter 1- APERITIFS", from book, "COMPUTER SECURITY AND CRYPTOGRAPHY", A JOHN WILEY & SONS, INC., PUBLICATION, 2007

[15] D. R. Stinson, "Chapter 2- Shannon's Theory", from book, "Cryptography: Theory and Practice", CRC Press, 2007.

[16] M. Stamp and R. M. Low, "Chapter 1- Classic Ciphers" and "Chapter 2-World War II Ciphers" ,from book, "APPLIED CRYPTANALYSIS Breaking Ciphers in the Real World", A JOHN WILEY & SONS, INC., PUBLICATION, 2007

[17] Availableat https://www.eetimes.com/document.asp?doc_id=1279619

[18] F. S. Hillier and G. J. Lieberman, "Chapter 14- Game Theory", from book, ITRODUCTION TO OPERATIONS RESEARCH, McGraw-Hill Series in Industrial Engineering and Management Science, 2008.