American Journal of Sciences and Engineering Research
E-ISSN -2348 – 703X, Volume 3, Issue 1, 2020

Open Access

Application of Game Theory to Select the Most Suitable Cryptographic Algorithm in Asymmetric Conditions

Saeed Seyed Agha Banihashemi [1], Eman visheh [2]
North Azad university of Theran.

ABSTRACT: *The cryptographic systems used in an organization use a fixed cryptographic algorithm and the specific procedures of that system. Due to the fact that the algorithm is fixed in these systems, the probability of failure or success of such systems depends on human resources, hardware resources and work environment so that it can be said that the probability of success or the failure of these systems is 50%. Also, in this kind of systems, there are no other algorithms based on the needs of the user. This research addresses the question of how we can use multiple asymmetric algorithms in a cryptographic system that does not defeat the algorithm by the opponent. In this research, selection of algorithms based on some environmental parameters and the possibility of breaking the algorithm by the opponent should be selected. This will be done using game theory. The problem is modeled as a model of solvable problems by game theory and generated outputs will be use by Gambit software which is especial for Game theory. The results obtained from this study indicate the ease of choosing the algorithm based on the need and with regard to the attack on the opponent and how to reduce the likelihood of breaking the algorithm.*

Keywords: *Encryption and Decryption, Game Theory, Overcoming Strategy, Nash Function, Gametheory, Gambit, crypto tool, cryptology*

I. INTRODUCTION

The simplest definition of Game theory is study of strategic situations. The game theory examines the impact of two or more interactions on the basis of extracted parameters from the environment. Based on the conditions in each engagement, each player has some choices that can be profitable or damaging to him. The science of game theory allows each player to choose the best choice in choosing his actions in response to choosing a player's strategy in playing situations. This science is a subcategory of applied mathematics and is used in different fields such as economics and political science, Law, Biology, Army, management, facing terrorism and so on. The cryptographic science studies the methods of concealing information in sending and receiving messages from origin to destination. The methods presented in cryptanalysis sometimes modify the content of the message, only the authorized agents can be informed of the contents of the message, and access to the content of the message is not possible or hardly feasible. In this paper, we try to create a kind of interaction between science of cryptography and science of game theory. With the aim of analyzing the existing strategies in the situation and using a set of algorithms, the best cryptographic algorithm can be selected and used.

Due to conditions in the environment, usable algorithms and requirements that are created in the situation, it is not possible to change and use different encryption algorithms dynamically in cryptographic systems. Changing the algorithm without regard to some conditions may cause the algorithm to be misused and weaken the system. The idea behind this is based on how the best algorithm can be chosen if there are different usable algorithms and environmental conditions. In this paper, we try to evaluate a sample of situation conditions and present the results of the evaluation as a strategy to the theory of games. Under these conditions, the task of science of game theory is to examine the strategies and determine the best strategy for the player using this method.

Gilatt Col, and Mannie nowar, discuss the design of the protocol for information conversion. This article seeks to design a proper protocol for secure sharing and multi-party computing (7). Ali Atk iddin in an article on digital cryptography, based on the RSA algorithm, investigated the algorithms of RSA, DES, and Blowfish algorithms in image

 Received- 02-02-2020, Accepted- 13-02-2020

cryptography (8).Julie Shah and Vikas Saxina, have devoted a comprehensive study on video cryptography (9).Nicholas McDonald examines the history of cryptography in the past, present and future (10).Majid Bakhtiari and Mohammad Eizini, famously in his article on the issue of serious security weaknesses in the RSA encryption system, initially introduced the RSA algorithm and further describes its application (11). Jean Francois Raymond and Anton Stiglitz discuss the weaknesses in the Diffieel Hillman key transform protocol (12).

Veronika Stolbikova An article in the ISACA Journal entitled "Cryptography of elliptical bends?" Has provided a general overview of the security of encryption systems (13).

II. MAIN PROBLEM

Under the normal conditions of a cryptographic system, the solution to secure the system depends on the parameters associated with the structure of the system. This means that there are no rules in this system. In this structure, there is only one strategy for defense (encryption) and a strategy for attacking. For observing the conditions without the use of game theory, C

rypTool encryption software was used for both RSA and ECC prototyping. Prototyping done in both ways is based on a file size of 497 KB. The results are as follows:

First Review of the RSA Algorithm: The results of the first review in the field are summarized as follows:

	Length of key	Encryption	decryption
	512	0.354	4.769
RSA	768	0.48	7.757
	1024	0.525	11.336
	2048	0.956	39.079

Table 1 - Results obtained from the encryption process with the RSA algorithm

Table 1 shows the time required for the encryption process in the second column and the decryption time in the third column based on the key length indicated in the first column. In fact, by observing this table, the key-length relationship is determined by encryption and decryption processes.

Table 1 shows that in the encryption process, very little time is consumed for data encryption. This time will not make much difference with the increase in key length so that in using the maximum key length that can be implemented by the software (2048 bits) the time taken is less than one second. It is seen in the review of the time taken for the decoding process to increase by increasing the key length of time spent reopening the cipher text. Increasing the time spent in the decoding process draws attention to the fact that the increase in key length can have a significant effect at the time of opening the encrypted texts so that the decoding time of a text with a 2048-bit key is 8 times the decoding of the same text with 512-bit key length (Figure 1).

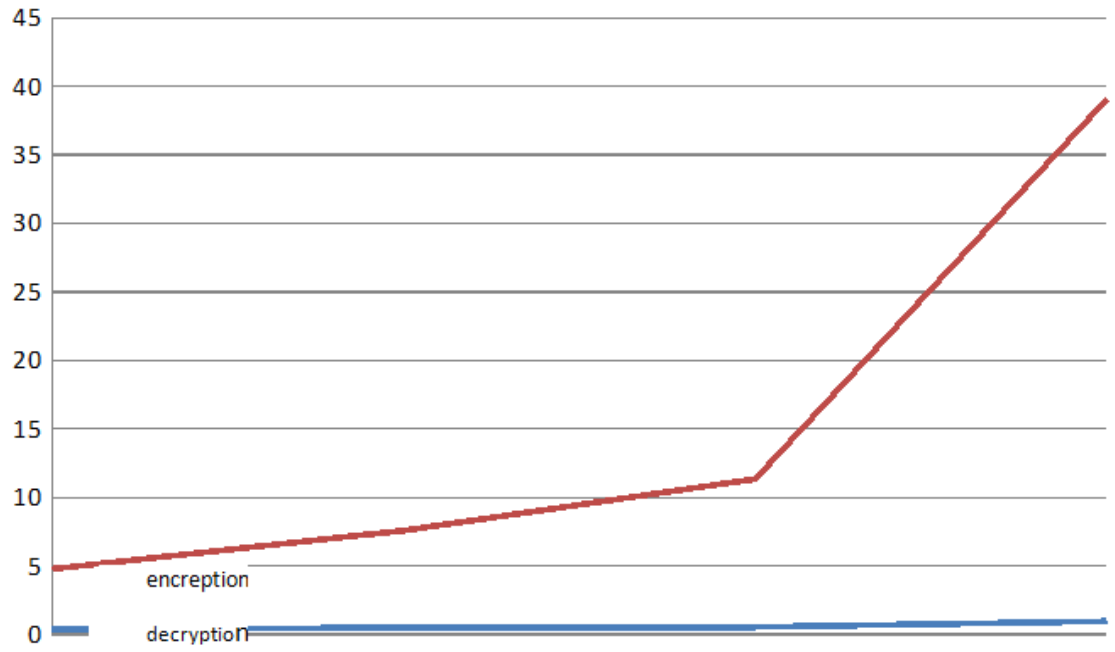

Figure 1: Comparison of encryption timing and RSA algorithm decoding based on key length.

This review specifies that the use of the RSA method is not a suitable option for choosing when the time for opening the encrypted text is important for the user.

The second study of ECSP-DSA: algorithm was investigated in the second study of ECSP-D

decryption	encryption	Length of key	
0.093	10.33	192v1	
0,086	10.08	192v2	
0.081	9,996	192v3	
0.099	10.22	239v1	ecsp-dsa
0.091	10.292	239v2	
0.091	10,103	239v3	
0.096	10.156	256v1	

Table 2 - Results obtained from the encryption process with ellipticity algorithm

Table 2, like Table 1, shows the decoding and encryption process based on the key length. In the study of ellipticity algorithm we observe that, unlike the RSA algorithm, a lot of time is spent in the cryptographic process. It is noteworthy that the increase in key length does not have much effect on the encryption process. Decoding time is much less than encryption time. This difference is well seen in Chart 2.

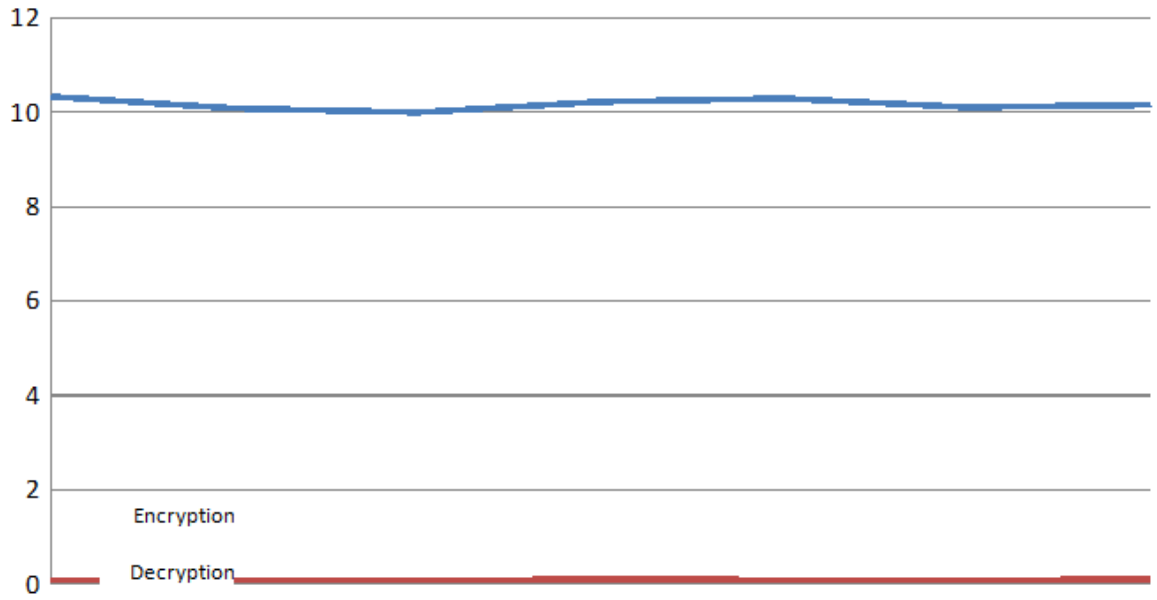

Figure 2 Comparing the timing of encryption and decoding of the ECSP-DSA algorithm based on the key length.

In situations where time of encryption is important for the user, this method will not be the right option for cryptographic operations.

By studying two RSA patterns, ECC can be observed if a cryptographic protocol is designed based on one of these two at the beginning of the work, the required work must be specified and based on the required hardware requirements to be provided. . For example, if the data used is of a video type, the time at which the data is retrieved in the destination takes a lot of time. In the current situation where game theory is not used to select an encryption algorithm, we cannot change the choice of our algorithm.

III. THE RESULT OBTAINED FROM THIS METHOD

• In Situations without Using Game Theory as we can see, in each encryption process, we can only use a cryptographic algorithm based on the requirements specified in the system design stage.

• In this situation, we will not be able to evaluate and select any other algorithm for encryption.

IV. PROBLEM SOLVING METHOD WITH THE HELP OF GAME THEORY

In the first method, it is only possible to use an algorithm for cryptographic operations. Note that in the method of conditions, without the use of game theory, a cryptographic system is chosen with an algorithm. In the first method, we have to do the feasibility study first, and then proceed with the design of the encryption protocol. The simplest evaluation in the first method is to examine decoding and encryption time in both RSA and ECC methods. But in this assessment only one criterion is used and other effective measures can not be involved in this assessment. In the status quo test method, using the game theory, not only a prior assessment criterion is also considered, but we can also apply other criteria in the assessment of the conditions.

The tips below are a brief description of the characteristics of cryptographic algorithms. Although there may be controversy over some of the characteristics in different sources, a general overview of these issues can be considered. In general, if we want to list common features of the items listed, we can list the following:

• Lower key length: One of the issues in key cryptography is asymmetric. By increasing the key length, the resources used to construct the key will increase

• The speed of cryptography operations: This property has a significant impact on cryptographic operations, so that the increase in the cryptographic operation time can affect the destination message or the process execution cycle.

• Performance Multiplication: Some algorithms are one-stop and some are multifunctional. The performance

multiplicity may improve the performance or performance weakness of an algorithm from the perspective of the execution speed of the algorithm.

• Exclusive use: Some algorithms may be used in certain circumstances. The exclusivity of this group makes it impossible in general terms to use the algorithms we seek. Of course, in general terms and in certain circumstances, the algorithm can be considered as a suitable parameter.

•Multiple methods of attacking the algorithm: If there are multiple attack methods for an encryption algorithm, there are more weaknesses for this algorithm, so this property can be one of the characteristics of the algorithm's attack evaluation.

• Less memory consumption: Memory is considered as one of the bottlenecks in the calculations. The need to fetch a large amount of data to implement a cryptographic process can be considered as one of the problems associated with the complexity of the cryptographic algorithm.

• Independence of the algorithm: Independence of the algorithm in execution and its need to use the other algorithm can be considered as one of the positive characteristics. Some algorithms need to be used along with another algorithm.

The specification can be summarized as follows:

	Positive feature	Negative feature		
Length of key	Short key length	Long key length		
Operation speed	Too much	Being low		
Performance multiplicity	Multiple use	Exclusive use		
Exclusive use	No limitation to a specific tool	Limitations for use for certain tools		
Multiple methods of attack	Lack of methods	Many methods		
Memory consumption	Low	Much		
Independence on the run	Independent	Along with the other algorithm		

Table 3 - Checking some of the features

Characteristics listed in table3 can to evaluate the algorithm used for asymmetric cryptography.

No	properties	DSA	ECC	ELG	DH	RSA
1	Length of key	low	low	a lot	a lot	a lot
2	Speed of operation	a lot	moderate	low	low	low
3	Dimensions of performance	no	yes	no	no	yes
4	Exclusive use	no	no	yes	no	no
5	The multiplicity of attack methods	Low	moderate	low	a lot	moderate
6	Memory consumption	a lot	a lot	low	low	low
7	Independence on the run	no	yes	no	no	yes

Table 4 – evaluation of cryptographic algorithms

This table is a simple example of the evaluation of encryption algorithm for that every individual which can use to regard environmental conditions .The multiplicity of the above characteristics to show differ behavior indifferent algorithm .For example, in the absence of proper use of hardware encryption algorithm RSA with the problem encountered and the resources to overcome this problem short-length keys should be easier to use encryption or in the absence of a secure channel using password algorithms Delfi - Hillman seems reasonable .The middle man attack may face algorithm by danger. However this should be consider that table 4 of simple sample assessment that a person should be in terms of implementation. As mentioned, the most simple features that can be fitted to evaluate the algorithm used for the encryption is the minimum key length attribute. The evaluation of this attribute with the result that we fitted in the comparison of two or more of the algorithm, each algorithm that requires greater key length for the encryption and security, power loaders, poor performance than others. Table 5 of this subject makes clear.

key equivalent to the Symmetric encryption	elliptic curves	The dimension group in the aljmal	Cup of RSA
64	128	816	816
72	144	1008	1008
80	160	1248	1248
96	192	1776	1776
112	224	2432	2432
128	256	3248	3248
256	512	15424	15424

Table 5-comparison algorithm key length

With a view of table 5 we fitted to a minimum key length for the security of the data encrypted in the asymmetric algorithms relative to average much more than symmetric algorithm for.64-bit versus the length of the symmetric algorithm keys, with a minimum length of 128 bits for asymmetric algorithms we face that corresponds to elliptical curves ELGmalو for RSA algorithm and key length 816 bit to cover this level of security fitted used up. with the uptrend in the length of the key in the algorithm in along with the symmetric algorithm key length for the elliptic curve to form a symmetrical algorithm and fixed double fitted increased though two ELGmal and RSA algorithm with more to follow the slope of the fitted to this increase. Documented to ability of the public key in addition to the ability to provide a method of calculating a minimum key length of table 6 to other species is described.

System requirements for resistance to attack	Length of symmetric key	Length of block of DH,RSA	Length of subgroup of DSA
70	70	947	129
80	80	1228	148
90	90	1553	167
100	100	1926	186
150	150	4575	284
200	200	8719	383
250	2502	14596	482

Table 6 compares the key length needed in encryption algorithm

In this documentary in one level we calculate RSA,DH but also we calculate length key of DSA in another pillars separately.

in comparison of algorithm of DSA,ECC with same symmetric algorithm of key length we keep for ECC 160 bit for DSA 148 bit. We must be pay attention to this point, although the criteria for the evaluation of algorithm can be the key length but in real conditions other factors are effected to selection of algorithm.

V. PROBLEM SOLVING USING THE GAME THEORY

To explain how to use the game theories have to use a simple example. A profile table that can be read as a simple example would be that any person can be based on existing conditions in the desired evaluation to do.

Reviews profile and evaluating conditions in method profile table: to review the existing situation and the third chapter of the rate they are paid. Get result of bulging study conducted in chapter III on the table was set the following profile:

		Second player (attacks)				
		AT1	AT2	AT3	AT4	
First player algorithm	AT1RSA	(75,25)	(50,50)	(50,50)	(50,50)	(50,50)
	AT2DH	(50,50)	(25,75)	(50,50)	(50,50)	(50,50)
	AT3ECC	(50,50)	(50,50)	(25,75)	(050,50)	(50,50)
	AT4ELG	(50,50)	(50,50)	(50,50)	(75,25)	(50,50)
	AT5DSA	(0,100)	(0,100)	(0,100)	(0,100)	(25,75)

7- Profile of game

In this table the first player strategy algorithms encryption and the second player's strategy to attack the existing algorithms methods. In this table of the algorithm a limited number (five algorithm) is used, however this should be consider that this table can also be generalized to more.

How to insert information a land value to it in table. For the existing table rate we act as follows:

- In case of attack to an algorithm we consider probability of winning of each player

50,50

- If you are being a versatile algorithm is due to cover the needs there will be more points for player using the algorithm .
- When there is no probability of attack for for algorithm we consider (100,0) value
- when we consider algorithm which is not good for encryption we give value (0,100).

In the event that one of the attacks can be used for other algorithms available on the basis of probability is the percentage share of existing attack techniques with other algorithms will be calculated (for example,(25, 75)).

A question that gets raised is that what causes factor gets along with a host of options available to the players is the first player selected second in the interest of the player or at odds with it. Determine the selections (strategies) to help the existing methods in the theory of games will be available. In the first method, which examined the possibility of a strategy change dynamically are not there so the system is used only on the basis of a protocol.

To calculate and analysis results we use Gambit software which is special for game theory. This software easily can present dominated and Nash equilibrium.

To calculate the game situation we must insert info, to Gambit software. The primary input of information is

as follow:

Second player

First Playe	AT1		AT2		AT3		AT4		AT5	
RSA	75	25	50	50	50	50	50	50	50	50
DH	50	50	75	25	50	50	50	50	50	50
ECC	50	50	50	50	50	50	50	50	50	50
ELG	50	50	50	50	25	75	25	75	50	50
DSA	100	0	100	0	100	0	100	0	75	25

4-4 first table of Gambit

This table is base of our future calculation.

we can see dominated strategies in this matrix

Second Player

First Playe	AT1		AT2		AT3		AT4		AT5	
RSA	75	25	50	50	50	50	50	50	50	50
DH	50	50	75	25	50	50	50	50	50	50
ECC	50	50	50	50	50	50	50	50	50	50
ELG	50	50	50	50	25	75	25	75	50	50
DSA	100	0	100	0	100	0	100	0	75	25

Table 5-4

In the matrix view cells that have been marked with a tick mark. The cells removed by software because of this is that if one of the players selected by the respective cells will fail .For the first player that is marked with red color DSA is best strategy and for second player AT3, AT4, AT5 are good strategy if second player choose AT1,AT2 is looser.

Now DSA is dominated strategy for first player and when first player choose DSA best strategy for second player is AT5.

VI. CHOOSING THE BEST STRATEGY GAME THEORY BASED ON THE ENCRYPTION ALGORITHM

As in the previous section to answer the issue of choosing the best encryption algorithm to help game theory we have, in this section want to answer the questions to choose the best strategy game theory based on the encryption algorithm .Answer questions to choose the best encryption algorithm based on the theory of games as a basis to respond to the question about the comment.

As in the previous question on the basis of the conditions related to any strategy to assess together the right algorithm, in this situation and it turns out the strategy initially based on the desired selection algorithm. In this situation the available strategies are defined as follows:

1- The dominant strategy: the player decides to use this strategy

2- Nash equilibrium: if there is not dominated strategy then player use Nash equilibrium

3- Best response: If there is not dominated strategy and Nash equilibrium then player choose BR .

VII. CONCLUSIONS

This is the use of the game theory to determine the most appropriate symmetric encryption algorithm is done using these two Science together can be certain points of interest was acquired in the different results that could give them the following :

1- In the normal situation that only a strategy or method of working there, the first player to reach the goal of maximum security in cryptographic operations; based on human resources, have been hardware and will form the infrastructure. In this situation the second player who also tried to break the encryption system is only available a set

of instructions for the attack.

2-If contrary to the procedure before use the game theory to determine the strategies, our choice is not limited to a single procedure and that the first player has a few strategies, the second player will also play different strategies will be presented

3- The existence of different strategies with more action to select a player puts more weaknesses may also create, so the correct conditions for evaluation can play a major role in the results of the game.

4. Game theory based on mathematical science building has been built, with the description of the output based on input parameters are calculated correctly, factors and put for use of us. What you should take into consideration is that game theory is no help in estimating the parameters.

5. Convert concepts to a numeric value or vice versa is based on perceptions of the individual and may vary from one person to the person .So create a different person by the profile table two different results.

6. Assessment of environmental conditions on the basis of the parameters available in the environment and may be based on different factors such as time, human resources, psychological factors present in the environment and hardware has undergone a change. With this account can be firmly said that the evaluation of the environmental conditions will be a function of time.

7-Assessment of environmental conditions on existing conditions need full peers in the executive environment of the opponent. There may be some factors that in normal circumstances are estimated due to the lack of appropriate peers on environmental conditions has not properly evaluated. As well as some of the parameters to the public because the classifications will not be assembled.

8. As I mentioned in the article, can we trust to encryption elliptical curves? In the case of existence of a backdoor in the case of elliptical curves as there may be some benefits to the influential parameters for hostile because there is virtually hidden, there remain these parameters can be the result of a game as a way to return the favor of the opponent.

9-To wrap some of the attacks may be carried out without informing the first opponent. It this is the only method based on probability of occurrence and the second player moves to achieve results is calculated.

VIII. SOURCES

1. **Pham, Viet Hoang.***Applications of Game Theory in Information Security.* London : University of London, 2015.
2. *Adaptive Selection of Cryptographic Protocols in Wireless Sensor Networks using Evolutionary Game Theory.* **Arora, Srishti, Singh, Prabhjot and Gupta, Ashok Ji.** Nagpur, INDIA : elsevier, 2015. ICISP2015. p. 358.
3. **Bitansky, Nir, Panethy, Omer and Rosen, Alon.***On the Cryptographic Hardness of Finding a Nash Equilibrium.* boston : boston University, 2015.
4. **Liao, Xiaojua and Hasegawa, Ryuzo.***Maximum Satisfiability Approach to Game Theory and Network Security.* s.l. : Graduate School in Information science and Electrical Engineering, 2014.
5. **Dodis, Yevgeniy, Halevi, Shai and Rabin, Tal.***A Cryptographic Solution to a Game Theoretic Problem.* New York : MIT, 2008.
6. **Katz, Jonathan.***Bridging Game Theory and Cryptography: Recent Results and Future Directions.* Maryland : Department of Computer Science University of Maryland, 2008.
7. **Kol, Gillat and Naor, Moni.***Cryptography and Game Theory: Designing Protocols for Exchanging Information.* Israel : Department of Computer Science and Applied Mathematics Weizmann Institute of Science, Rehovot 76100 Israel, 2008.
8. *Digital Image Encryption Based on RSA Algorithm.* **Taki El_deen, Ali E, El_badawy, El_sayed A and gobran, Sameh N.** 1, egypt : IOSR Journal of Electronics and Communication Engineering, 2014, IOSR-JECE, Vol. 9, pp. 69-73. 2278-8735.
9. *Video Encryption: a Survey.* **Saxena, Vikas and Shah, Jolly.** 2, Uttare Paradesh : IJCSI, 2011, Vol. 8. 1694-0814.
10. **McDonald, Nicholas G.***Past Present And Future methoeds Of cryptoghraphy And Data Encryption.* Utah : University Of

Utah.

11. *Serious Security Weakness in RSA Cryptosystem.* **Bakhtiari, Majid and Maarof, Mohd aizaini.** 1, Skudai : IJCSI, 2012, IJCSI, Vol. 9. 1694-0814.
12. **Raymond, Jean-Franc¸ois and Stiglic, Anton.***Security Issues in the Diffie-Hellman Key Agreement Protocol.*
13. *Can Elliptic Curve Cryptography Be Trusted? A Brief Analysis of the Security of a Popular Cryptosystem.* **Stolbikova, Veronika.** s.l. : ISACA, ISACA, Vol. 3, p. 30.