International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319 – 6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 4; April 2017; Page No. 3382-3387
DOI: http://dx.doi.org/10.24327/ijcar.2017.3387.0280

Research Article

ENHANCED SECURITY OF BLOWFISH USING GAME THEORY'S OPTIMAL ONE-SHOT CATEGORY OF NASH EQUILIBRIUM IN AVALANCHE EFFECT

Shamina Ross B[1] and Josephraj V[2]

[1]Department of Computer Applications Scott Christian College Manonmaniam Sundaranar University Nagercoil-629001, India
[2]Department of Computer Science Kamaraj College Manonmaniam Sundaranar University Thoothukudi-628003, India

A R T I C L E I N F O

Article History:

Received 20th January, 2017
Received in revised form 19th February, 2017
Accepted 22nd March, 2017
Published online 28th April, 2017

Key words:

Avalanche Effect, Blowfish, Cryptanalysis, Feistel Network, Nash Equilibrium

A B S T R A C T

Internet and network applications are growing rapidly in this modern world. The need to secure these applications is increasing day by day. Security is one of the most challenging aspects in the communications and electronic applications. Cryptography is a way to make sure that confidentiality, authentication, integrity, availability and identification of user data can be maintained as well as security and privacy of data can be provided to the user. There are a variety of crypto systems. Of all the crypto systems available, Blowfish block cipher is the best. As of today, the Blowfish has no cryptanalysis. An effort is made to enhance the security of the Blowfish cryptography algorithm by making modifications to the Feistel (F) function by combining the Blowfish and the Game Theory's one-shot category in Nash Equilibrium (GNE). The outcome of the proposed optimal hybrid GNE-Blowfish and the existing Blowfish algorithm are analyzed using Avalanche effect and the better performance of GNE-Blowfish is reported. GNE-Blowfish can be widely used in the field of electronics and communication which involves high level of data security.

INTRODUCTION

Cryptography plays an important role for protecting data from destructive forces and the unwanted actions of unauthorized users. Encryption is the process of transforming plain text data into cipher text in order to conceal its meaning and prevent any unauthorized user to retrieve the original data. Nowadays, the mathematical complexity of the cryptographic algorithms is increasing which results in more computation. This in turn leads to more execution time and high energy consumption recent years. Successful studies have been made to speed up the execution of cryptographic algorithms. The Blowfish algorithm was designed by Bruce Schneier to replace Data Encryption Standard, which was the Federal Information processing Standard Cryptography [1]. It is a symmetrical block cipher [2] having the advantages of secure, fast, easy to implement etc. The operation part of Blowfish consists of XORs and additions on 32-bit words, and only 4KB or even less memory is needed when it runs. The key length of Blowfish can vary from 32 bits to 448 bits, which makes datum secure enough. In the security domain, the defenders often deploy defense counter measures based on the value of the assets they try to protect and potential threats from attackers. Game theory studies interactions between players with the same or conflicting interests. The proposed optimal hybrid GNE-Blowfish algorithm obtained by combining Nash Equilibrium and Parallel Blowfish algorithm enhance the performance over Blowfish by modifying the function F of the existing Blowfish. There are a lot of benefits from parallel computing. The advantage of this system is its ability to handle large and extremely complex computations. The basic idea of this research is to develop a simple, stronger and safer cryptographic algorithm. We have implemented parallel processing technique. Amdhal's law states that the speed of an algorithm can be increased by parallel processing [3]. The Blowfish and Nash Equilibrium concept in Game Theory are combined so that the security is increased. The Avalanche effect is used to show that the proposed GNE-Blowfish algorithm possess good diffusion characteristics as that of original Blowfish algorithm [4]. The Nash Equilibrium concept makes sure that it is unbreakable in any situation. The objective of this research paper is to study the blowfish and enhance its strength using Parallel processing and Game Theory's One-shot category of Nash Equilibrium. As GNE-Blowfish using optimal one-shot category in Nash Equilibrium is a variable length key block cipher, it is most suitable for communications link or automatic file encryptor where the key does not change often. The new hybrid GNE-Blowfish algorithm can be widely used in Electronic

Corresponding author:* **Shamina Ross B
Department of Computer Applications Scott Christian College Manonmaniam Sundaranar University Nagercoil-629001, India

communications, E-Commerce Software, E-Mail encryption, Online chat, Password Management, etc.

Related Work

System Specification

For this research a Laptop with Intel Pentium T4500 @ 2.30 GHz CPU, 4.00 GB Dual-Channel DDR3 and Linux Mint 17.1 is used to collect the performance data. Experimentation is done on text file of fifteen different file sizes ranging from 50 bytes to 208942 bytes. The performance metrics used for comparison are the encryption speed, decryption speed, execution time, encryption throughput, decryption throughput, execution throughput and avalanche effect. The GNE-Blowfish cryptosystem was implemented using the C programming language in gcc compiler.

Game Theory

The field of game theory and cryptographic protocol design are both concerned with the study of interactions among mutually distrusting parties. A great deal of effort was invested in trying to capture the nature of rational behavior, resulting in a long line of stability concepts. Cryptographic protocols are designed under the assumption that some parties are honest and faithfully follow the protocol, while some parties are malicious and behave in an arbitrary fashion. The game-theoretic perspective is that all parties are simply reasonable and behave in their own best interests. This viewpoint is incomparable to the cryptographic one, although no one can be trusted to follow the protocol unless it is in their own best interests, the protocol need not prevent un-reasonable behavior.

Nash Equilibrium

In game theory Nash Equilibrium is a state where each player's strategy is the best given the strategies of all other players. A Nash Equilibrium exists when there is no one way beneficiary deviation from any of the players involved. In other words, no player in the game would take a different move until every other player remains in the same state. Nash Equilibria are self-regulating. At Nash Equilibrium state the players have no desire to move because they will not get a better position than the existing one. An individual will not receive any uplifted benefit from changing actions with the assumption that other players remain constant in their strategies. A game may or may not have Nash equilibria. It can also have multiple Nash equilibria. The unique Nash equilibrium of the game is where both players concede. Both would be better positioned, if neither of them conceded. Nash equilibrium is as a stable state in which neither of the players can improve the outcome for themselves given what the other players are doing. Nash equilibrium is the best known notion of equilibrium. It corresponds to a strategy profile in which strategies of players are independent. More precisely, the induced distribution over the pairs of actions, must be a product distribution, $s(A1 \times A2) = s_1(A_1) \times s_2(A2)$. Deterministic are a special case of strategies, where s_i assigns probability 1 to some action. For strategies s_1 and s_2, we denote by $u_1(s_1,s_2)$ the expected payoff for player i when players independently follow s_1 and s_2.

A Nash equilibrium of a game G is an independent strategy profile such that for any $a_1 \in A_1$, $a_2 \in A$, we have $u_1(s_1^*, s_2^*) \geq u_1(a_1, s_2^*)$ and $u_2(s_1^*, s_2^*) \geq u_2(s_1^*, a_2)$.

At the Nash Equilibrium, the attacker and the defender have no incentive to device from their strategies unilaterally. The Nash Equilibrium consists of the optimal acceptable strategies for both players. In the worst case where the attacker has sufficient attack resources, the defender's Nash Equilibrium strategy is his best response to the attacker's strategy [5]. In a Stackleberg game we have a leader and a follower. A leader chooses his strategy first. Afterwards, the follower, notified by the leader's choice, chooses his strategy [6]. In our case, the defender is the leader who tries to configure encryption rates on each device in order to protect the confidentiality.

Parallel processing

Parallel processing is the process of dividing the program instructions among multiple processors to reduce the execution time of a program. In parallel processing, each processor works the same as any other microprocessor. The processors act on instructions written in assembly language. Based on these instructions, the processors perform mathematical operations on data retrieved from computer memory. The processors can also move data to a different memory location.

Processors rely on software to send and receive messages. The software allows a processor to communicate information to other processors. By exchanging messages, processors can adjust data values and stay in sync with one another. This is important because once all processors finish their tasks, the CPU must reassemble all the individual solutions into an overall solution for the original computational problem. There Latency and bandwidth are the two major factors that can impact system performance. A good parallel processing system must have low latency and high bandwidth.

Blowfish Algorithm

The Feistel Structure of Blowfish Algorithm is shown in Fig.1.

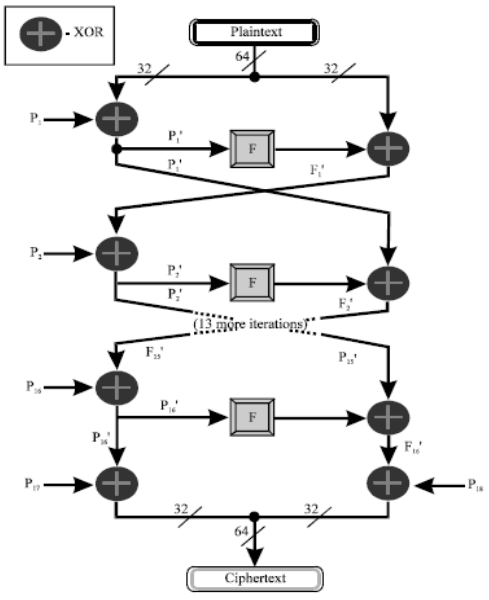

Fig 1 Feistel Structure of Blowfish Algorithm

The Blowfish algorithm inputs a 64-bit plaintext and then outputs a 64-bit cipher text. The key length is variable from 32 bits to 448 bits [7]. The algorithm can be split into two divisions such as a key expansion part and a data encryption part. Key expansion converts a key of maximum size 448 bits

into several sub key arrays to a total of 4168 bytes. The original sub key p-box and s-box are fixed. They are initialized in order with a fixed string that consists of hexadecimal digits of Pi less the initial 3. Data encryption takes place in a 16 round Feistel network [8] after key expansion. Each round consists of a key-dependent permutation and a key- and data-dependent substitution. The sub keys are generated before data encryption or decryption. Function F is obtained by dividing XL into four eight-bit quarters a, b, c, and d

F(XL) = ((S1,a +S2,b mod2^32) XOR S3,c) + S4,dmod2^32
In the above F function, "+" is addition on 32-bit words, and XOR represents Exclusive OR. S1, a represents key s-box [1] [a], S2, b represents key s-box [2] [b], S3, c represents key s-box [3] [c], and S4, d represents key s-box [4] [d]. The key p-box is used in the reverse order for decryption process. The process of decryption is the same as encryption but key p-box is used in the reverse order.

Fig.2 shows the calculation of the function F(XL) using Blowfish algorithm.

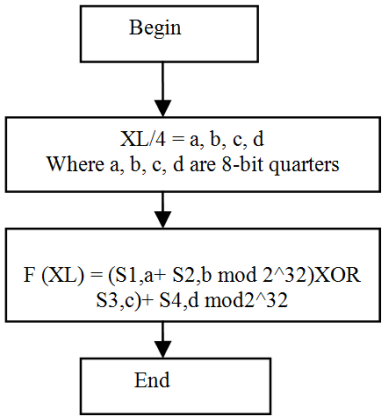

Fig.2 Feistel Function F in Blowfish Algorithm

The principle of Blowfish algorithm is both easy to understand and easy to implement. All sub keys of Blowfish are influenced by every bit of the key, that makes the key and the data mingled together completely, which makes it quite difficult to analyze the key [9]. The function F gives the Feistel network a great avalanche effect.

Blowfish cipher is not only secure, but also fast, and suitable for different platforms. This gives Blowfish a high recognition in the field of information security. Blowfish is among the fastest block ciphers available. Blowfish is used in wide range of applications such as bulk encryption of data files, remote backup of hard disk. Also multimedia applications use blowfish for encryption of voice and media files. It is now being used in biometric identification and authentication, using voice, facial or fingerprint recognition. Geographical information system uses blowfish for cryptographic protection of sensitive data. These applications run in high-end servers, workstations, process bulk amount of data and demand high speed encryption and higher throughput [9]. A study was conducted for different popular key algorithms such as DES, 3DES, AES and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were tested on two different hardware platforms. On comparing their performance it was found that Blowfish had a very good performance than the other algorithms [10]. Bruce Schneier made a block cipher speed comparison among Blowfish, RC5, DES, IDEA, 3DES algorithms. The speed comparison was made using the parameters, number of clock cycles per round, number of rounds and number of clock cycles per byte of output. The results showed the advantage of Blowfish among block ciphers in terms of speed. The results are tabulated in Table I. From Table I, it is clear that Blowfish is a fast and highly secure algorithm. The speed and the security strength of Blowfish algorithm makes it widely used in the field of information security [11].

Proposed Game Theory's Nash Equilibrium Blowfish Algorithm and Analysis

GNE-Blowfish

The block diagram in Fig.3 represents the structure of GNE-Blowfish algorithm.

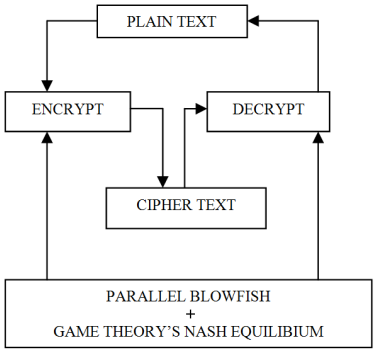

Fig 3 Block Diagram og GNE-Blowfish

A rational attacker attacks only the nodes in the sensible target set. The sensible target is a set of nodes whose security assets are the most attractive to the attacker. The security asset refers to the confidentiality of data processed by the nodes. The objective of the attacker is to collect the maximum amount of information from the defender where the defender tries to protect the data from the attacker by encrypting it. For this research, investigation is done where both the attacker and the defender take the decisions at the same time by taking into account each other's strategy. This type of iterations falls under the one-shot game category [12]. The proposed GNE-Blowfish algorithm is a modified Blowfish algorithm. The modification is done in the F function. Parallel processing and Game Theory's one-shot game category in Nash equilibrium state is incorporated in the blowfish algorithm. The proposed algorithm limits to a range of nodes which are the leaf of a sub tree which consists of sensible nodes to get the optimal strategy in one-shot category. The defender's strategy to encrypt data on node i does not only depend on security asset and the attacker's strategy but on the number and security assets of nodes along the path from node i to the root node. Without violating the security requirements, the Blowfish function F can be modified as follows

*F(XL)=(S1,a/S2,b)+(S3,c/(S2,b*S4,d))*

This modification supports the parallel evaluation of one division operation and one multiplication operation, then one division operation and finally an addition operation. All these

operations take place in 3 steps. Fig.4 shows the calculation of F function using GNE-Blowfish.

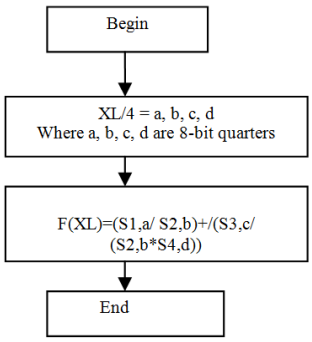

Fig.4 Feistel Function F in GNE-Blowfish Algorithm

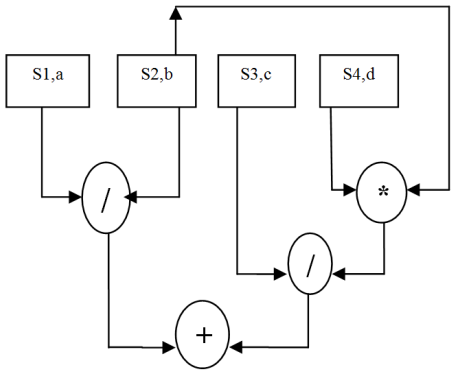

Fig.5 S-Box Substitution in Function F in GNE-Blowfish Algorithm

Performance Comparisons

In this paper the performance metrics execution time, encryption time, decryption time, throughput, avalanche effect, power consumption are used to evaluate the blowfish algorithm and GNE-Blowfish algorithm. The encryption time, the decryption time, the Execution time, is low for Blowfish algorithm than GNE-Blowfish algorithm. But the Avalanche Effect is high for GNE-Blowfish than Blowfish. GNE-Blowfish is the best in terms of security. Blowfish algorithm by itself is highly secure. But above all GNE-Blowfish is unbreakable in any circumstances.

Experimental Results

Encryption Time

Encryption Time is one of the performance metrics which is defined as the amount of time required for converting plaintext message to cipher text at the time of encryption. Tabulation of results of encryption time with fifteen different packet sizes for Blowfish algorithm is shown in Table II and GNE-Blowfish algorithm in Table III. The encryption time of GNE-Blowfish algorithm is reasonable.

Decryption Time

Decryption Time is one of the performance metrics which is defined as the amount of time required for converting the cipher text into the plain text at the time of decryption. Tabulation of results of decryption time with fifteen different packet sizes for Blowfish algorithm is shown in Table II and GNE-Blowfish algorithm in Table III. The decryption time for GNE-Blowfish algorithm is reasonable.

Execution Time

Execution time of an algorithm directly depends on the functionality of the algorithm and it clearly defines that more complex structure originates poor execution time. Higher the key length provides higher security but increases execution time. The speed of the algorithm is determined by the execution time of the algorithm. Tabulation of results of execution time with fifteen different packet sizes for Blowfish algorithm is shown in Table II and GNE-Blowfish algorithm in TableIII. The execution time taken by GNE-Blowfish algorithm is reasonable.

Throughput

The throughput of the encryption scheme is calculated by dividing the total plaintext encrypted in Megabytes by the total encryption time for each algorithm.

Throughput= Total Plaintext in Mega Bytes / Encryption Time

The higher the value of throughput more is the efficiency of encrypting any text with an encryption algorithm. Tabulation of results of throughput with fifteen different packet sizes for Blowfish algorithm is shown in Table II and GNE-Blowfish algorithm in Table III.

Avalanche Effect

A change in one bit of the plain text or one bit of the key schedule will produce a change in many bits of the cipher text. This change in number of bits in the cipher text whenever there is a change in one bit of the plain text or one bit of the key is called Avalanche Effect [13].

Table I Block Cipher Speed Comparison

Algorithm	Clocks/round	No. of Rounds	Clocks/byte of output
Blowfish	9	16	18
RC5	12	16	23
DES	18	16	45
IDEA	50	8	50
3DES	18	48	108

Table II Speed Analysis of Blowfish Algorithm

Data size in Bytes	Encryption	Decryption	Execution
50	0.7586	0.7602	0.8875
60	0.7709	0.7722	0.9058
100	0.7919	0.7934	0.9543
250	0.8962	0.8978	1.1592
325	0.9486	0.9497	1.2615
700	1.2776	1.2005	1.7646
900	1.3354	1.3364	2.0352
965	1.3741	1.549	2.29
5350	4.5246	4.4654	8.3683
7400	5.9181	5.8499	11.146
9000	6.9128	5.1447	11.4318
51202	20.9473	16.2216	36.5376
61442	23.8123	19.2313	42.4173
102402	37.7555	31.5148	68.651
208942	63.2736	63.159	126.085
Average Time (millisec)	11.41983333	10.25639333	21.05967333
Throughput (MB/sec)	2.500233162	2.783848579	1.3557782

A desirable feature of any encryption algorithm is that a small change in either the plain text or the key should produce a significant change in the cipher text. If the changes are small, this might provide a way to reduce the size of the plain text or key space to be searched thereby making the cryptanalysis

very easy. For a cryptographic algorithm to be secure it should exhibit strong Avalanche effect. For this research, the value of one bit in the input is changed and the resulting avalanche effect for each algorithm is obtained for 20 times and the average value of the avalancheeffect was taken and compared for the two algorithms Blowfish and GNE-Blowfish. Tabulation of results observed by changing one bit of plain text in the sample is shown in TableIV. Fig.2 represents the Avalanche effect of Blowfish algorithm and GNE-Blowfish algorithm. In the bar chart Blowfish is represented as BF and GNE-Blowfish as GNEBF.

The Blowfish algorithm has the least Avalanche effect when compared to the GNE-Blowfish algorithm discussed here. Higher the Avalanche value more will be the security. So it is clear that GNE-Blowfish algorithm is more secure than Blowfish algorithm.

Table III Speed Analysis of GNE-Blowfish Algorithm

Data size in Bytes	Encryption	Decryption	Execution
50	1.091	1.0932	1.2339
60	1.1006	1.103	1.2534
100	1.1378	1.14	1.3303
250	1.2859	1.2886	1.6236
325	1.3562	1.359	1.7658
700	1.7217	1.8954	2.6774
900	1.9177	2.0997	3.0764
965	2.0041	1.9757	3.0951
5350	5.6043	4.2401	8.8831
7400	7.4453	4.8089	11.2961
9000	8.1553	5.3761	12.5759
51202	26.7755	23.3385	49.2568
61442	31.658	27.8036	58.6938
102402	49.6562	45.6026	94.3201
208942	90.5527	90.2677	180.4362
Average Time (millisec)	15.43082	14.22614	28.76786
Throughput (MB/sec)	1.850338867	2.007026924	0.992505038

Table IV Avalanche Effect Comparison

Algorithm	BF	GNEBF
Avalanche	57.1	67.8

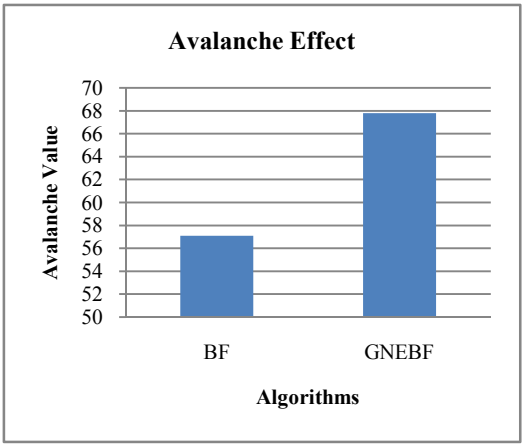

Fig 1 Avalanche Effect Comparison

CONCLUSIONS AND SUGGESTIONS

This paper gives a detailed study of the most popular symmetric key encryption algorithm that is Blowfish and discusses about its advantages. Based on the benefits and bottlenecks of the Blowfish algorithm, a new hybrid method is proposed and implemented to further enhance the existing algorithm to achieve better results in terms of security. The striking feature of GNE-Blowfish encryption algorithm is that for the same input plaintext the cipher text generated at each time will be different. This is because every time a new random number gets generated and as a result this gives a difference in the application of F function over each round. The advantage of different cipher text generated for the same input is, it will greatly enhance the security aspect of the new hybrid GNE-Blowfish algorithm. There are a variety of Game Theory's Nash Equilibrium based on suitable constraints. Blowfish algorithm together with Game Theory's optimal one-shot category in Nash Equilibrium gives an excellent performance in terms of security. The above results clearly indicate that there is a huge variation in the Avalanche value for GNE-Blowfish and Blowfish algorithm. GNE-Blowfish algorithm is highly secure than Blowfish algorithm. So it is clear that GNE-Blowfish algorithm is very strong, secure and unbreakable than the Blowfish algorithm. The research work can be further extended with other optimization techniques which have potential capacities. The s-box calculation can be done using normalization of random value to enhance the speed of the algorithm.

References

1. U.S. National Bureau of Standards, "Data encryption standard", U.S. Fed. Inform. Processing Standards Pub., FIPS PUB 46, January 1977, pp. 2-27.
2. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd Edition, New York, John Wiley and Sons, Inc. 1996, pp. 21-27.
3. Gene M. Adahl, "Validity of the single processor approach to large scale computing capabilities", in proceedings of the April 18-20, 1967, Spring joint computer conference AFIPS'67(spring) ACM, Newyork, NY, USA, pp. 483-485.
4. William Stallings, "Cryptography and Network Security", Fifth Edition, Pearson Education, 2011, pp. 119-120.
5. Yevgeniy Donis Sha Halevi Tal Rabin, "A Cryptographic Solution to a Game Theoretic Problem", Advances in Cryptology 2000, copy right 2000, Publisher-Springer Berlin Heidelberg, pp. 112-130.
6. Ziad Ismail, Jean Leneutre, David Bateman and Lin Chen, "A Game Theoretical Analysis of Data Confidentiality Attacks on Smaret-Grid AMI", IEEE journal on selected areas in communications, vol.32, No.7,July2014, pp. 1486-1499.
7. Bruce Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", in Cambridge Security Workshop on Fast Software Encryption, Cambridge, UK, December 9-11, 1993, pp. 191-204.
8. Bruce.Schneier, "The Blowfish Encryption Algorithm", *Dr. Dobb's Journal*, Vol. 19, No. 4, April 1994, pp. 38-40.
9. T. Srikanthan et al., "Drill – A Flexible Architecture for Blowfish Encryption Using Dynamic Reconfiguration, Replication, Inner-Loop, Pipelining, Loop Folding Techniques", Springer- Verlag Berlin Heidelberg 2005, pp. 6256-639.
10. Aamer Nadeem, Dr.M.Younus Javed, "A Performance Comparison of Data Encryption Algorithms", IEEE,

Information and Communication Technologies, 2005, ICICT 2005, First International Conference, 2006-02-27, pp. 84-89.

11. Mingyan Wang, Yanwen Que, "The Design and Implementation of Password Management System Based on Blowfish Cryptographic Algorithm", IEEE Xplore, International Forum on Computer Science-Technology and Applicatioins, 2009, IEEE Computer Society, 978-0-7695-3930-0/09, pp. 24-28
12. Martin J. Osborne, Ariel Rubinstein, "A Course in Game Theory", Cambridge, MA, USA, MIT Press, 1994.
13. Krishnamurthy G.N., V.Ramaswamy, Leela G.H., Ashalatha M.E., "Performance enhancement of Blowfish and CAST-128 algorithms and Security Analysis of Improved Blowfish Algorithm Using Avalanche Effect", IJCSNS, Vol.8 No.3, March 2008, pp. 244-250.

How to cite this article:

Shamina Ross B and Josephraj V *et al* (2017) ' Enhanced Security Of Blowfish Using Game Theory's Optimal One-Shot Category Of Nash Equilibrium In Avalanche Effect', *International Journal of Current Advanced Research,* 06(04), pp. 3382-3387.DOI: http://dx.doi.org/10.24327/ijcar.2017.3387.0280

****