Comparison and Hybrid Implementation of Blowfish, Twofish and RSA Cryptosystems

Maksim Iavich
Caucasus University
Tbilisi, Georgia
m.iavich@scsa.ge

Sergiy Gnatyuk
Yessenov University
Aktau, Kazakhstan
s.gnatyuk@nau.edu.ua

Elza Jintcharadze
Georgian Technical University
Tbilisi, Georgia
elza.jincharadze@gmail.com

Yuliia Polishchuk
National Aviation University
Kyiv, Ukraine
polishchuk.yu.ya@gmail.com

Andriy Fesenko
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine
aafesenko88@gmail.com

Akmaral Abisheva
Al Farabi Kazakh National University
Almaty, Kazakhstan
ak_maral@mail.ru

***Abstract*—Generally, encryption it's an encoding information process in order to provided security against unauthorized access. Nowadays, there are different types of cryptographic methods to provide high security level. Basically, each of cryptographic algorithms has its own weak and strong points. In this paper, presented the result of implementation and analysis that applied on several cryptographic algorithms such as Twofish, Blowfish, RSA and new hybrid model of those algorithms. The paper presents comparison of two symmetric key algorithms and their hybrid implementation in terms of performances, weaknesses and strengths. Proposed experimental research results on Blowfish and Twofish algorithms shows their advantages, disadvantages and strength against cryptanalysis. JAVA programming language was used to analyze those decryption algorithms.**

Keywords—symmetric cryptography; asymmetric cryptography; data encryption; ciphertext; decryption; hybrid cryptosystem.

I. Introduction

Blowfish it's a variable-length key algorithm with 64-bit block cipher; was created in 1993 by Bruce Schneider to replace the DES (Data Encryption Standard) [3]. Moreover, Blowfish divides a message into blocks of equal size in length, i.e. 64 bits. The algorithm consists of two parts: a key-expansion part and a data-encryption part. By encryption time Blowfish is faster than DES, but the weak key it's the weak point for this algorithm [3]. Nowadays there is no cryptography attack that will break the Blowfish algorithm in a reasonable time. Successful attack may be due to errors in the system. Blowfish wasn't patented and not have a license so it's available for all users. CAST (Carlisle Adams & Stafford Tvares) is similar to DES algorithm and uses 128 or 256 bit key structure. However, CAST less secure than DES and Blowfish algorithms. The table 1 shows the characteristics of these algorithms.

In Cryptography, Twofish algorithm it's symmetrical block algorithm whose block size it's 128 bits, and the key size changes to 256 bits. This algorithm associated with the predecessor Blowfish algorithm [11]. The main characteristic of the Twofish algorithm is the pre-calculated, key-dependent S-blocks and the intricate scheme of encryption. One half of the encryption n-bit keys used as the key to encryption and the remaining half as for algorithm modification. The Twofish algorithm architecture is quite similar the Blowfish algorithm. Twofish may leave behind AES in terms of speed.

RSA has been deemed as a secure and trustworthy algorithm among all asymmetric algorithms which have been proposed up to now. In fact, the RSA algorithm is a compatible asymmetric cipher, since it applies a key with various lengths. In this algorithm security can be assured at the expense of speed. The typical length of RSA keys are 512-2048 bits. Considerable cryptanalysis has approved RSA as a reliable algorithm over the years. It demonstrates that this algorithm has remarkable amount of reliability. Difficulty of factoring large numbers acts as a core component of RSA's security. The efficiency of RSA would be ruined if it was possible to find a simple method for factoring these large numbers. Accordingly, RSA laboratories propounded the term of 'factorization attack' as a challenge in 1991. Timing attack and Cycling attacks are among other attacks on RSA which have been discussed in [9, 10]. RSA believed to be a secure and dependable algorithm among all asymmetric algorithms, which have proposed up to now. Actually, the RSA algorithm presented as asymmetric cipher, which applies a key with various length. In this algorithm, security depends on speed. The usual length of RSA keys are 512-2048 bits. Algorithm was invented in 1978 [12]. Different cryptanalysis has approved RSA as a reliable algorithm over the years. Factoring large numbers is a core component of RSA's security [8]. In RSA, asymmetry based on the difficulty of the factorization of the product of two large prime numbers. Nowadays, RSA encryption it's one of the commonly used asymmetric encryption method, because this algorithm provides a high level of encryption with no known algorithm existing yet to be able to solve it.

II. Comparison and Analyses of Modern Ciphers

RSA it's a relatively slow algorithm, and because of this, it's less used to directly encrypt user data. Usually, RSA encrypted shared keys are used for symmetric key cryptography, which makes encryption-decryption operations to perform with higher speed. On the other hand, Twofish is fast and flexible on different types of CPUs and in hardware. Twofish can be used in network applications where keys are changed frequently and in applications where is little or no RAM and ROM available [15].

A strong side of the blowfish algorithm it's speed and efficiency as well as the ability to produce a large size key and provide high level security. By increasing the speed of data processing process by computer systems, the Blowfish Algorithm is capable of creating and developing a larger and larger length that ensures system security.

Blowfish, Twofish and RSA algorithms have been researched with Java programming language. Developed software code allows to encrypt and decrypt data stored in different size text file. The code describes the amount of time and system memory usage during performance of each algorithm (nanoseconds).

978-1-7281-3882-4/19/$31.00 ©2019 IEEE

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on March 11,2024 at 17:04:40 UTC from IEEE Xplore. Restrictions apply.

Accordingly, these systems are comparable to their encryption with time parameters spent during the decryption process. At the same time, the program code has the ability to encrypt and decrypt the Unicode text (For example Georgian alphabet). Table 1 presents experiment results conducted in different sizes of the file.

TABLE I. EXPERIMENTAL RESULTS OF TWOFISH ALGORITHM

Plaintext size (KB)	Plaintext size (Byte)	Encryption Time (nanoseconds) Twofish	Decryption Time (nanoseconds) Twofish	Twofish Encrypted file size (Bytes)	Used memory Bytes
32	32710	1427393	1344881	65440	2318520
64	65420	2656615	2569520	130848	2236152
128	130840	5124934	4737760	261696	3413776
256	261680	9711774	9532998	523392	5638152
512	523360	19289202	18919306	1046752	10086712
1024	1048460	38495186	38235307	2096928	19013272
2048	2096920	80450602	76949116	4193856	33374336
4096	4193840	177243939	162053556	8387712	67276384

TABLE II. EXPERIMENTAL RESULTS OF BOWFISH ALGORITHM

Plaintext size (KB)	Plaintext size (Byte)	Encryption Time (nanoseconds) Blowfish	Decryption Time (nanoseconds) Blowfish	Blowfish Encrypted file size (Bytes)	Used memory Bytes
32	32710	10753053	1984528	59241	9762104
64	65420	12169867	2743007	119493	10696784
128	130840	12567266	5602025	236670	12556416
256	261680	18200673	9356337	475738	16252696
512	523360	23987822	16802548	954280	23511600
1024	1048460	35550482	26062972	1915678	15407800
2048	2096920	43489299	40463494	3804367	28875368
4096	4193840	62097598	56950097	7552059	55642240

The experiment demonstrated that the encryption of data size increases proportionally with the time of encryption. If compare Blowfish and Twofish algorithms with the time of encryption, will find that the Twofish algorithm needs less time for encryption than the Blowfish algorithm (Fig.1-2).

The size of the encrypted files with the Twofish and Blowfish algorithms are the same as the file size (byte). Analysis of the obtained results demonstrated that Twofish increases encrypted file size averagely and Blowfish 1.8 times (Fig.3-4).

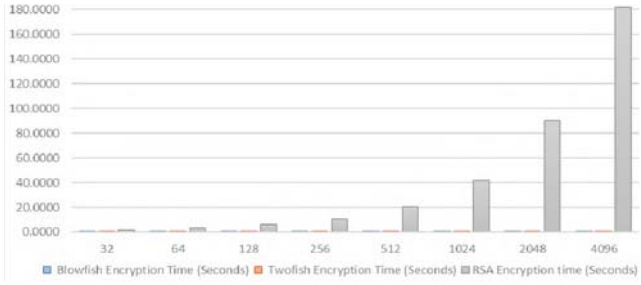

Fig. 1. Twofish, Blowfish and RSA comparison of encryption time

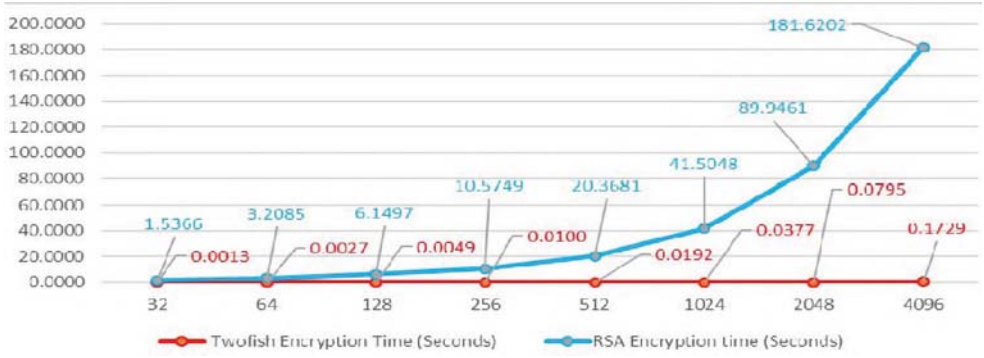

Fig. 2. Twofish and RSA comparison of encryption time

Encryption and decryption experiments, conducted on a different size text file show the following (Fig.5):

1. In encryption process, the encrypted file size of Twofish algorithm exceeds the file size of the Blowfish algorithm encryption result;
2. Small size of plaintext need less time; encryption process with Twofish algorithm is significantly faster. Blowfish algorithm remains stable despite of plaintext file size and it's faster than Twofish.
3. The observation of the memory used was determined that the Twofish algorithm consumed less resources while working with low size files, and Blowfish it's better with large files in the encryption process.

The experimental research has shown that the Twofish algorithm it's more efficient than the Blowfish encryption Algorithm. This result is especially noticeable in case when Twofish needs less encryption time. However, it should be noted that the efficiency of the Twofish algorithm depends on the parameter of the experimental computer memory (RAM) and the used plaintext size.

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on March 11,2024 at 17:04:40 UTC from IEEE Xplore. Restrictions apply.

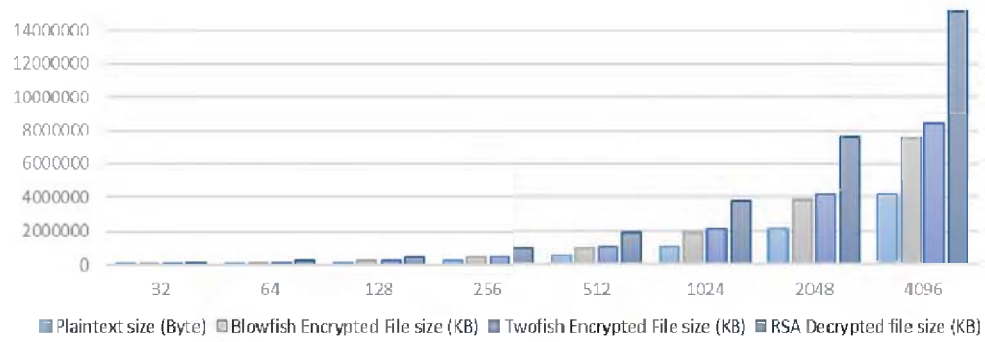

Fig. 3. Blowfish, Twofish and RSA - comparison of plaintext and encrypted file size

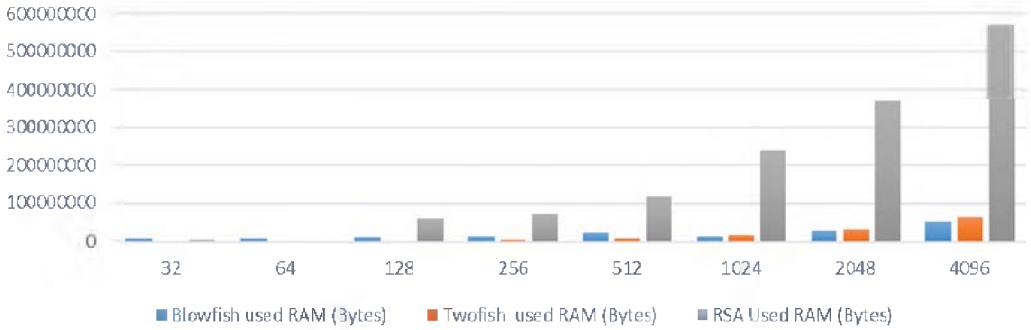

Fig. 4. Blowfish, Twofish and RSA – comparison of memory usage in Bytes

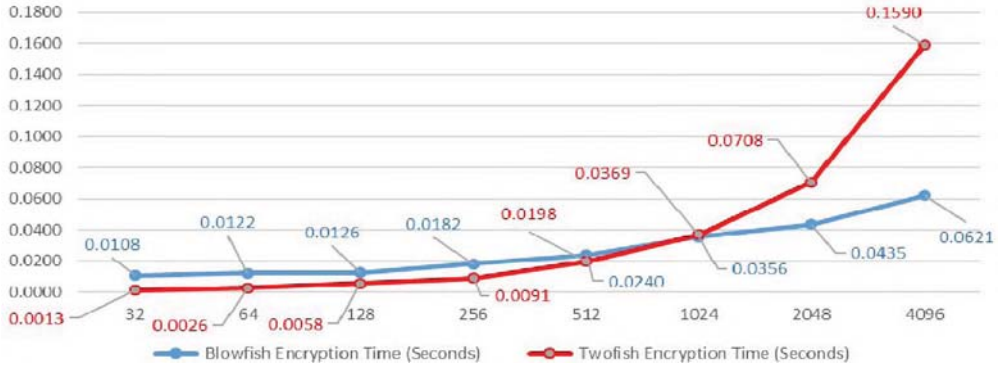

Fig. 5. Encryption time comparison of Blowfish and Twofish algorithms

III. Hybrid Implementation and Comparison of Blowfish+RSA and Twofish+RSA Systems

To create strong encryption algorithm there is proposed hybrid combination of two encryption algorithms -Blowfish + RSA and Twofish+RSA; there was done experiments on proposed algorithms by terms of their encryption speed, used memory and system requirements. The programming language Java was used for implementing the encryption algorithms. To make more calculations was used console work with Java NetBeans IDE.

Fig. 6 shows working process of proposed Blowfish + RSA hybrid cryptosystem. At first, system reads plaintext and generates secret key with RSA; public keys are generated automatically. Next step it's to generate Blowfish symmetric key, which will be encrypted with RSA system. This provides high security for key, because usage of RSA algorithm decreases decryption probability of public key. So, sharing public key, RSA secret key will be shared also. After these steps, plaintext is encrypted using Blowfish, because as other symmetric algorithms Blowfish is fast (Fig.7). Decryption process is reverse process of above described encryption.

IV. Discussion

Comparative analyses of Blowfish, Twofish cryptosystems was presented in paper. Based on those algorithms provides Blowfish+RSA and Twofish+RSA new hybrid cryptosystem model (Fig.8-10). Defined algorithms and hybrid models are evaluated by terms of encryption speed, memory usage, encrypted file size and ensured security level. After conducted experimental testing on those algorithms it's possible to conclude following:

1. If Blowfish, RSA and Blowfish + RSA hybrid algorithms are compared according to the memory used, the highest technical resources require RSA algorithm, and Blowfish are slightly behind the Blowfish + RSA hybrid scheme.

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on March 11,2024 at 17:04:40 UTC from IEEE Xplore. Restrictions apply.

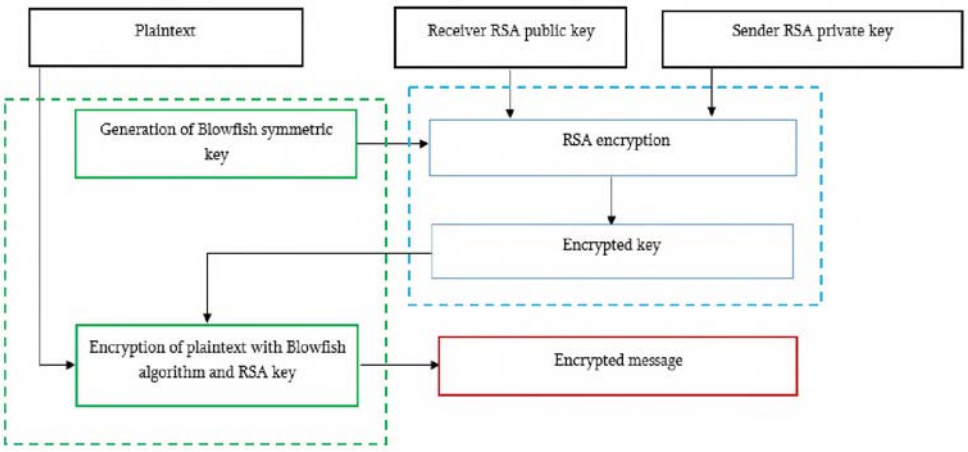

Fig. 6. RSA + Blowfish - the proposed hybrid system architecture

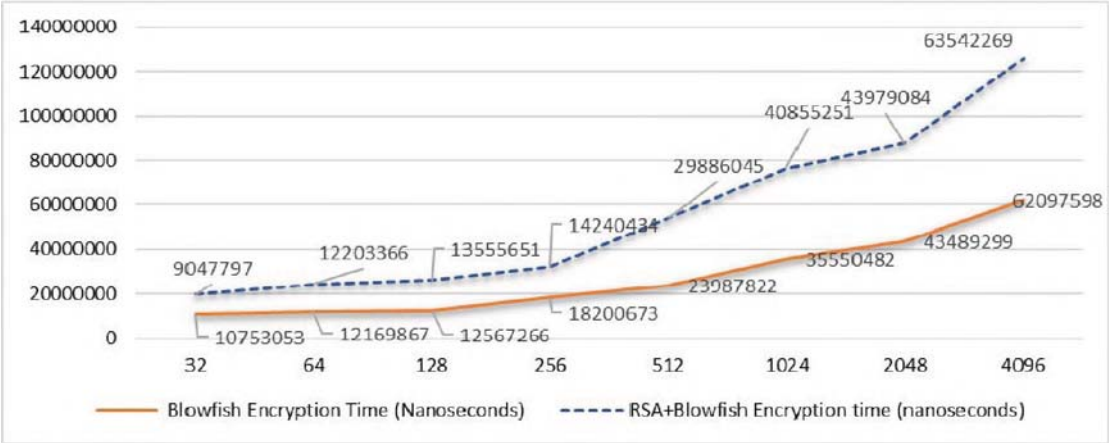

Fig. 7. Comparison of Blowfish and RSA + Blowfish cryptosystems encryption time

2. Considering the option of encryption, Blowfish keeps its initial first position and the fastest of these systems. However, the Blowfish + RSA hybrid algorithm it's far below and significantly faster than RSA; RSA takes the longest time to encrypt.

3. Observation of the decryption time parameters has shown that the Blowfish + RSA hybrid algorithm and the blowfish algorithm are almost equally fast with the decryption process and are faster than the RSA algorithm.

4. As an overview of the encrypted file size setting, the lowest memory needs Blowfish system, the following is Blowfish + RSA, and the RSA algorithm increases the size of an encrypted file with the highest rate.

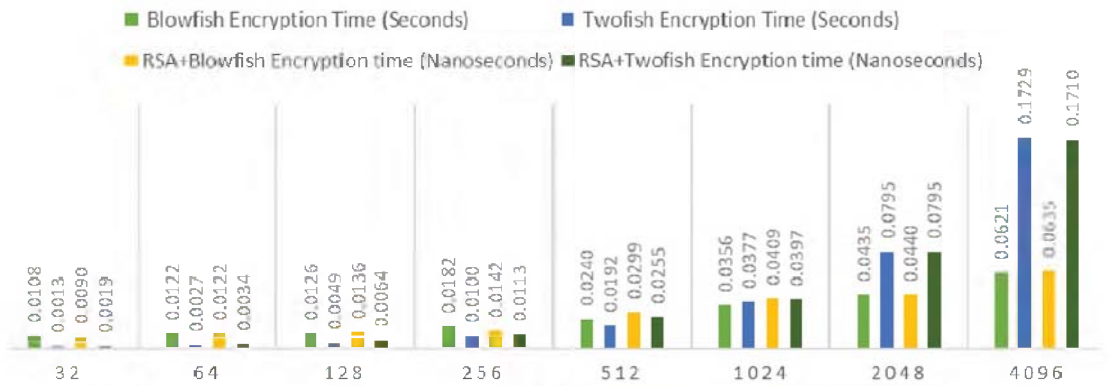

Fig. 8. Comparison of Twofish, Blowfish, RSA+Twofish and RSA + Blowfish cryptosystems encryption time

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on March 11,2024 at 17:04:40 UTC from IEEE Xplore. Restrictions apply.

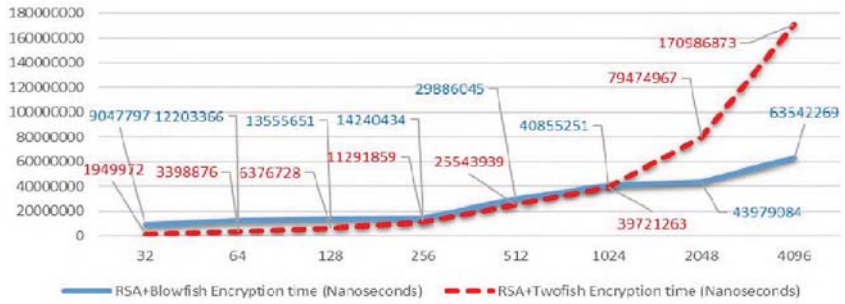

Fig. 9. Comparison of RSA+Twofish and RSA + Blowfish cryptosystems encryption time

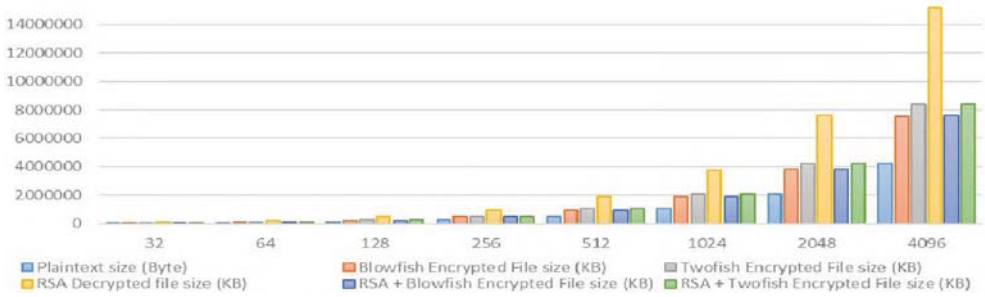

Fig. 10. Comparison of Twofish, Blowfish, RSA+Twofish and RSA + Blowfish cryptosystems encrypted file size

V. Conclusions

This paper presents a performance analysis of selected symmetric and asymmetric encryption algorithms. The selected algorithms are Twofish, Blowfish, RSA and new hybrid model of those algorithms. Along with their working mechanisms severa1points are to be concluded:

First, each of presented cryptographic algorithms has strong and weak points. From the conducted experiment results and the comparison of selected algorithms we conclude that, the blowfish algorithm is the best in case of encryption time and memory usage. Blowfish needs the shortest time among all the presented algorithms.

Second, new hybrid models are significantly secure, because it takes all advantages and strength of symmetric and asymmetric systems.

In the future work it's possible to review another hybrid model of additional symmetric and asymmetric algorithms as well as to conduct a series of entropy research of the different cryptographic algorithms and above-presented hybrid model. This will enable to identify the sustainability of each algorithm against different types of attack, including the frequency analysis of encrypted text. In addition, will able to highlight the highest level of security and speed, including the most efficient encryption algorithm.

Acknowledgment

The work was conducted as a part of joint project of Shota Rustaveli National Science Foundation of Georgia and Science & Technology Center in Ukraine, Project N6321 [STCU-2016- 08].

References

[1] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C — John Wiley & Sons, 1996.

[2] Kelsey J., Schneier B., Wagner D. (1996). Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES.

[3] Meyers R. K., Desoky A. H. An Implementation of the Blowfish Cryptosystem, Signal Processing and Information Technology, 2008. ISSPIT 2008. IEEE International Symposium on — Institute of Electrical and Electronics Engineers, 2008.

[4] R. L. Rivest, A. Shamir and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems," Comm. ACM, 21, pp. 120-126, 1978.

[5] Schneier B. Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), Fast Software Encryption: Cambridge Security Workshop Cambridge, U. K., December 9–11,1993. Proceedings / R. J. Anderson — Berlin: Springer Berlin Heidelberg, 1994.

[6] S. Gnatyuk, V. Kinzeryavyy, M. Iavich, D. Prysiazhnyi, Kh. Yubuzova, High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks, CEUR Workshop Proceedings, Kyiv, Ukraine, May 14-17, 2018), Vol. 2104, pp. 657-668.

[7] Shiho Moriai; Yiqun Lisa Yin (2000). „Cryptanalysis of Twofish (II)"

[8] Hu Z., Gnatyuk S., Kovtun M., Seilova N. Method of searching birationally equivalent Edwards curves over binary fields, Advances in Intelligent Systems and Computing, Vol. 754, pp. 309-319, 2018.

[9] Schneier, Bruce (2005-11-23). „Twofish Cryptanalysis Rumors". Schneier on Security blog.

[10] S. Gnatyuk, A. Okhrimenko, M. Kovtun, T. Gancarczyk, V. Karpinskyi, Method of Algorithm Building for Modular Reducing by Irreducible Polynomial, *Proceedings of the 16th International Conference on Control, Automation and Systems*, Oct. 16-19, Gyeongju, Korea, 2016, pp. 1476-1479.

[11] Niels Ferguson (1999-10-05). "Impossible differentials in Twofish".

[12] R. L. Rivest, A. Shamir and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems," Comm. ACM, 21, pp. 120-126, 1978.

[13] The Twofish Encryption Algorithm, B. Schneier, Dr. Dobb's Journal, December 1998.

[14] M. Iavich, S. Gnatyuk, E. Jintcharadze, Y. Polishchuk, R. Odarchenko, Hybrid Encryption Model of AES and ElGamal Cryptosystems for Flight Control Systems, *Proseedings of the 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control*, October 16-18, 2018. Kyiv, Ukraine, pp. 229-233.

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on March 11,2024 at 17:04:40 UTC from IEEE Xplore. Restrictions apply.