Scientific Research Publishing

Journal of Information Security, 2018, 9, 168-176
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption

Marwan Ali Albahar, Olayemi Olawumi, Keijo Haataja, Pekka Toivanen

School of Computing, University of Eastern Finland, Kuopio Campus, Kuopio, Finland
Email: Marwana@uef.fi, Olayemo@uef.fi, Keijo.Haataja@uef.fi, Pekka.Toivanen@uef.fi

How to cite this paper: Albahar, M.A., Olawumi, O., Haataja, K. and Toivanen, P. (2018) Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption. *Journal of Information Security*, **9**, 168-176.
https://doi.org/10.4236/jis.2018.92012

Received: February 13, 2018
Accepted: April 6, 2018
Published: April 9, 2018

Abstract

In this paper, we proposed a novel triple algorithm based on RSA (Rivest-Shamir-Adleman), AES (Advanced Encryption Standard), and TwoFish in order to further improve the security of Bluetooth that is currently using only 128-bit AES for encryption in its latest versions (Bluetooth 4.0 - 5.0). Furthermore, older Bluetooth 1.0A – 3.0 + HS (High-Speed) devices use E0 stream cipher for encryption that has been shown to be weak by numerous researchers and thus it could be considered insufficient for high security purposes nowadays. In our novel approach, the triple protection of AES, RSA, and TWOFISH would enhance the level of security, which shields the data transmission in the Bluetooth. As the first step of our novel approach, we first encrypted the message by using AES with 128-bit key and then further encrypted it by using Twofish with the same 128-bit key. Finally, the 128-bit key generated in the beginning will be encrypted by using RSA with 1024-bit key to protect its over-the-air transfer. In the receiving end, the decryption process goes in reverse order compared with encryption process. We showed with experimental figures that our novel algorithm improved the security of Bluetooth encryption by eliminating all known weaknesses and thus made data exchange between Bluetooth devices secure.

Keywords

Bluetooth, Security, AES, Twofish, RSA, Encryption, Decryption

1. Introduction

Bluetooth [1] is a wireless protocol, which is capable of transferring data and real-time two-way audio/video providing data rates up to 24 Mb/s. It connects together two devices when they are close to each other without a wired link, using radio waves as a transmission medium 2.4 GHz frequency band in the free

Scientific Industrial, Scientific, and Medical (ISM) band and can utilize two different frequency hopping methods: AFH (Adaptive Frequency Hopping) or FHSS (Frequency-Hopping Spread Spectrum) in order to avoid "bad" channels that suffer from interference. Nowadays, AFH is supported in all Bluetooth devices, since it was already released with Bluetooth 1.2 version in November 2003 [1] [2] [3].

Several kinds of Bluetooth devices are used globally. In fact, in 2006, the number of shipped devices reached to one-billionth devices [4]. Later in 2012, the annual Bluetooth product shipments exceed 2 billion and in 2016 it is expected that almost 4 billion Bluetooth product will be shipped, thus having 20 billionth Bluetooth device shipped by the end of 2016 [4]. Thus, it is extremely crucial to keep all Bluetooth security issues up to date [1] [2] [3] [4].

As Bluetooth is growing in popularity and it adopts rapidly spreading all around the world, the security of this network is a major source of concern as several threats exist to exploit the vulnerabilities found in this network. Data transmission over Bluetooth network is always at risk of being compromised, as sensitive information and documents are been transmitted over Bluetooth network. Bluetooth being a wireless network can be spied upon from a remote location which may have serious consequences on the integrity of the data being transmitted or the network to which it's being connected. E0 stream cipher is being currently utilized for data encryption in Bluetooth technology; however, there are few weaknesses found in 128-bit E0 stream cipher implementation, and it can be easily cracked, in some cases by 0 (264) mode [5].

Our results: In this paper, we propose a hybrid encryption algorithm to securely communicate in Bluetooth network based on the combination of AES, RSA and Twofish. We demonstrate with experimental figures the effectiveness of this proposed algorithm to protect the confidentiality and integrity of messages transmitted over the Bluetooth network by encrypting the message first with AES Key 128 bits, and then with Twofish and RSA. Our results show that this hybrid algorithm will increase the security level of the encryption mechanism in Bluetooth communications and thus the confidentiality of messages transmitted over the network will be guaranteed.

The rest of the paper is organized as follows. Section 2 provides an overview of Bluetooth security. Our novel secure data transmission technique is proposed in Section 3. Section 4 provides our experimental results and analysis. Finally, Section 5 concludes the paper.

2. Overview of AES, Twofish and RSA Algorithm

In this section we will discuss about the three unique algorithms we implemented in our proposed technique. Sub-section 2.1 discusses about AES, Sub-section 2.2 discusses about Twofish and Sub-section 2.3 discusses about RSA.

2.1. Advanced Encryption Standard (AES)

AES was introduced by NIST in 2001 to replace DES. The AES algorithm is a

symmetric block cipher used to protect important documents by the US government and implemented for data encryption all around the word [6] [7] [8]. AES algorithm comprises of three different ciphers blocks, which are; AES-128, AES-192 and AES-256 which can each encrypt or decrypt data in blocks of 128 bits utilizing 128 bits, 192 bits or 256 bits cryptographic keys. Basically for encryption and decryption process, AES goes through different rounds; it goes through 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys [6] [7] [8]. A 128 bit data length is allowed in AES, which we can further split into four different basic functioning blocks; the blocks represent as range of bytes and are organized as a 4×4 matrix called the state [6]. For encryption/decryption process in AES, AddRoundKey is the first stage that starts the cipher, after which the output goes through additional nine main rounds before it eventually gets to the final round. Four transformations are performed during each of these rounds, they are: 1) Sub-bytes, 2) Shiftrows, 3) Mix-columns, 4) Add round Key [6]. In the (10^{th}) round, which is the final, Mix-column transformation is not performed [9] [10].

2.2. Twofish Algorithm

Twofish algorithm is a symmetric block cipher which has fiestel like structure [7]. It utilizes block ciphering and it is efficient for use in developing software in tiny processor, a good example is Smart cards [7]. In twofish algorithm, it is possible to allow implementers to adapt the code size, encryption speed, key setup time to stabilize performance. Three different key sizes are utilized in Twofish algorithm for encryption, they are 128, 192 and 256 bits and block size of 128 bits are used. Basically, Twofish encryption algorithm has 16 rounds of encryption and the 128 bit cipher text is produced after the 16^{th} round has been completed [7]. Twofish provides efficient security, as it has been extensively cryptanalyzed, that even network Intruders can only break five rounds of the algorithm [11].

2.3. RSA (Rivest-Shamir-Adleman Algorithm)

RSA algorithm is an asymmetric key cryptographic algorithm; it was invented in 1977 by Ron Rivest, Adi Shamir and Len Adlemen. It uses the concept of two keys; the public and the private key; RSA algorithm converts the plaintext into a ciphertext by encrypting the message using the public key, which only the receiver can decrypt with the use of a private key. RSA algorithm's invention is base on the arithmetical concept that it is easy to find and multiply large prime numbers but to factor their product is difficult. Both private key and public keys in RSA algorithm are based on prime numbers that are large (100 or more digits) [12] [13]. There are basically three steps in RSA algorithm; the selection and generation of the public and private keys, encryption and decryption process [12] [13].

The steps below explain RSA algorithm in details [12]:

1) Two prime number p and q are chosen

$$n = p \times q$$

where n represents a large integer whose factorization produce two large prime number p and q.

2) $n = (p-1) \times (q-1)$

3) The encryption key is randomly selected

where $1 < e < \phi(n)$, $\gcd(e, \phi(n)) = 1$.

4) The following equation is solved to compute decryption key d

$de = 1 \bmod \phi(n)$ and $0 \le d \le n$.

5) public key PU = e, n.

6) private key PR = d, n.

3. The Encryption Mechanism in Bluetooth Communication & Drawbacks

Information security in the network has been a challenge, which demands urgent attention. Notably with the rapid development of computer technology, several issues arose to the surface of the Information Security field such as User Authentication, data encryption, data integrity, and access control. Bluetooth is a radio communication standard short-range, which enables electronic devices to be connected as well as communicated wirelessly. Also, Bluetooth functions in the frequency band the 2.4 Hz. It uses FHSS (Frequency Hopping Spread Spectrum) because it makes eavesdropping becomes tough. Frequency Hopping Spread Spectrum, which is a radio transmission process where randomly, chosen frequencies hopping between 79 different frequencies at regular intervals in accordance with a pseudorandom sequence. Further, the transmission range is up to 10 meters, and data can be transmitted over asynchronous (ACL Asynchronous Connection Less) or synchronous channels (SCO, Synchronous Connection-Oriented). In earlier versions of Bluetooth, an E0 stream cipher algorithm is used for encryption process. However, this algorithm has proven to be vulnerable [14], and many attacks in [15] [16] [17] preformed successfully on E0 stream cipher [18]. While in the latest versions (4.0 - 5.0 v), 128-bit AES for encryption is used. Therefore, this study devoted in order to further increase the security of encryption algorithm in Bluetooth.

4. Related Work

Walk through the paper [19]; the authors proposed a hybrid Algorithm based on triple DES algorithm and RSA aiming at enhancing the security of data transmission in Bluetooth communication. Also, they discussed E0 which is the encryption algorithm used by older Bluetooth 1.0A – 3.0 + HS (High-Speed) devices in order to shield the confidentiality and the privacy of data transport in Bluetooth communication. In the same context, the author stated that a proposed algorithm is utilizing RSA and DES protection, which increased the security of algorithm [19].

In this paper [14], a new hybrid encryption scheme proposed based on AES

and RSA for data transmission in Bluetooth communication. In the course of the proposed encryption scheme, the authors explained the encryption process. In the encryption process, RSA will encrypt the key of 128-bit. Then the AES cipher will encrypt the sender's message. In the same matter, the values encrypted will be utilized in order to generate a complex message. In the decryption process, it is simply can be described as a reverse process of the encryption process. However, this hybrid encryption scheme is not destined to detect non-repudiation against cipher-text as well as origin authenticity because it did generate hash function and digital signature.

In [20] the authors proposed a hybrid algorithm, which is based on, AES, RSA, and SHA-1. This algorithm employed the features of three algorithms in order to increase the security. Also, the authors stated that the proposed method is secure and robust because of utilization the advantage of each algorithm. Particularly, the author employed SHA-1 because of the digital signatures, and RSA because it has better key management.

The authors in this paper show a comparison between the RSA public key-based algorithm and DES private key based Algorithm. They found that the central feature that differentiate RSA public key-based algorithm from DES private key based Algorithm was related to the input plain text speed during the encryption and decryption process. Moreover, the authors reported that the time consumed of execution both decryption and encryption process of RSA algorithm is least as compared to DES algorithm. Noteworthy, DES algorithm has a faster speed during encryption and decryption than RSA algorithm [21].

The primary concern of this study is to highlight the weakness of the Bluetooth encryption mechanism and provide a solution. As the aim is pointed towards the interpretation of flaws in the preceding design, Bluetooth E0 algorithm is suffered from a numerous number of attacks and it is proven that E0 algorithm could be broken in 264 operations [14] [15] [16]. Bluetooth encryption mechanism has different vulnerabilities that could be exploited by malicious users to compromise the connection between Bluetooth devices. In this context, we proposed a novel triple algorithm based on RSA, AES, and TwoFish, which increases the level of security of the data transmission using Bluetooth. Furthermore, our triple algorithm provides a convenient and very easy technique for the encryption of transmitted data.

5. Novel Algorithm

As the issue is correlated with the security of the data transmitted via Bluetooth communication, we invariably strive to produce a reliable algorithm for securing data. In this section, we will explain the novel algorithm and the experiment along with the results thoroughly. The reason for employing RSA is that the key management is a primary feature. In addition, the method applied in RSA is relied on the difficulty of factoring large numbers. For AES, it gives a great per-

formance and it is robust as well as efficient. Finally, Twofish comes to be chosen because of its unique combination of conservative design, flexibility and speed. Noteworthy, it is strong and conceptually simple.

5.1. Encryption Process

Figure 1 shows our Hybrid Encryption algorithm, the encryption process as follows.

First plaintext is encrypted with AES and we get a cipher text then again cipher text encrypted with Twofish algorithm. Finally, we get a complex encryption value against plain text passing through two time encryption algorithms.

5.2. Decryption Process

During the decryption of the hybrid encryption algorithm, the process is the reverse of the encryption process (see Figure 2).

5.3. Result

Our proposed hybrid algorithm was successfully implemented, in which we clearly demonstrated the effectiveness of this hybrid technique in efficiently securing the transmission of data and it has shown to be a stronger information security technique for data communications. The combination of AES, Twofish and RSA encryption algorithm formed a strong secured protocol that has increased the security of Bluetooth communication against any known attacks.

Our result is depicted with Figure 3 & Figure 4 below:

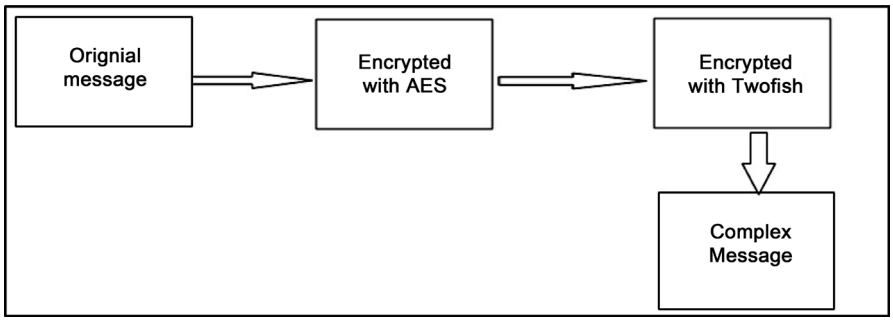

Figure 1. The encryption process of the proposed method.

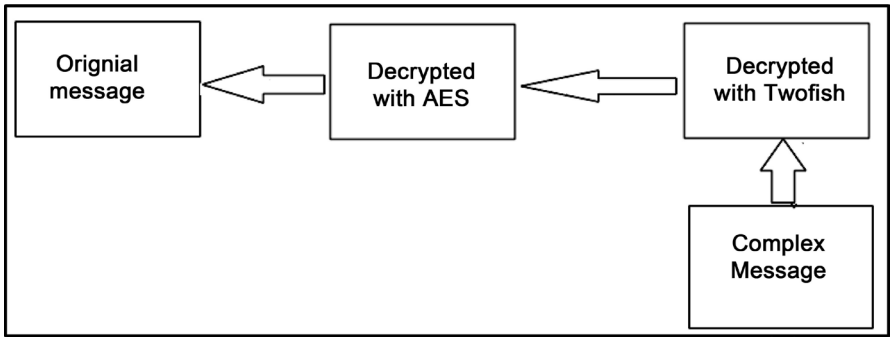

Figure 2. The decryption process of the proposed method.

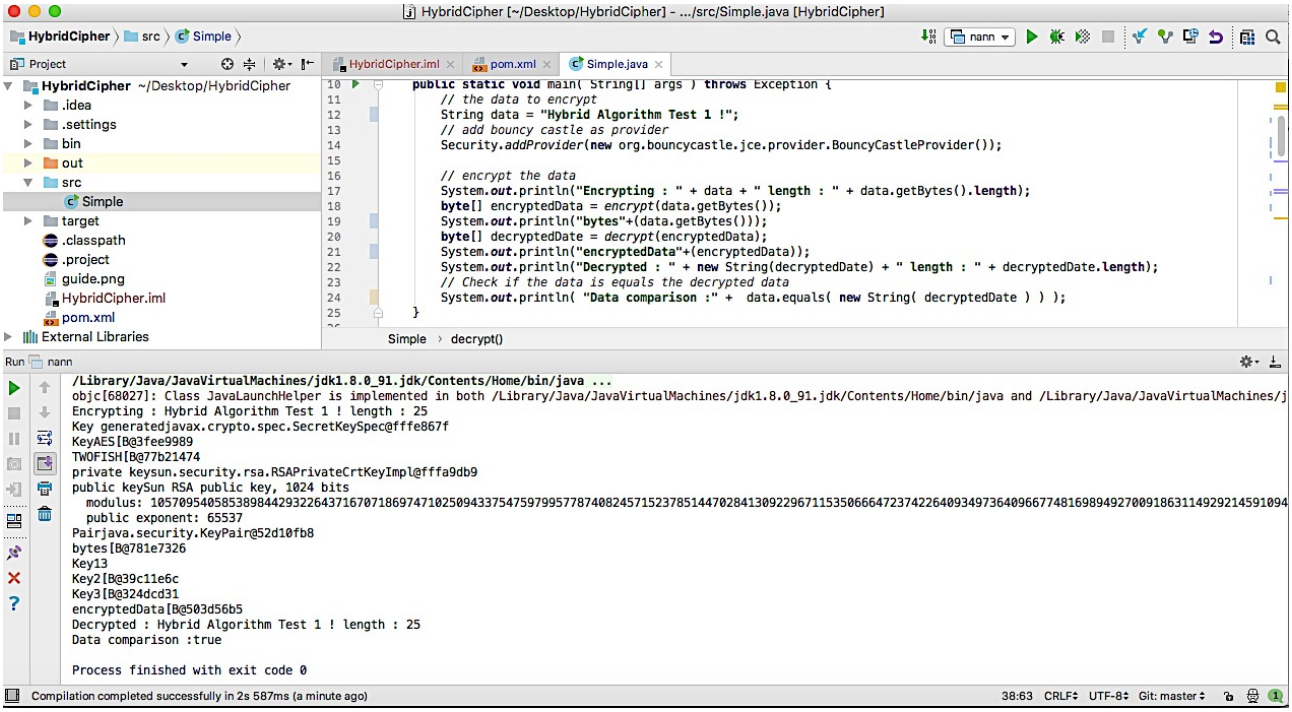

Figure 3. The result of hybrid algorithm.

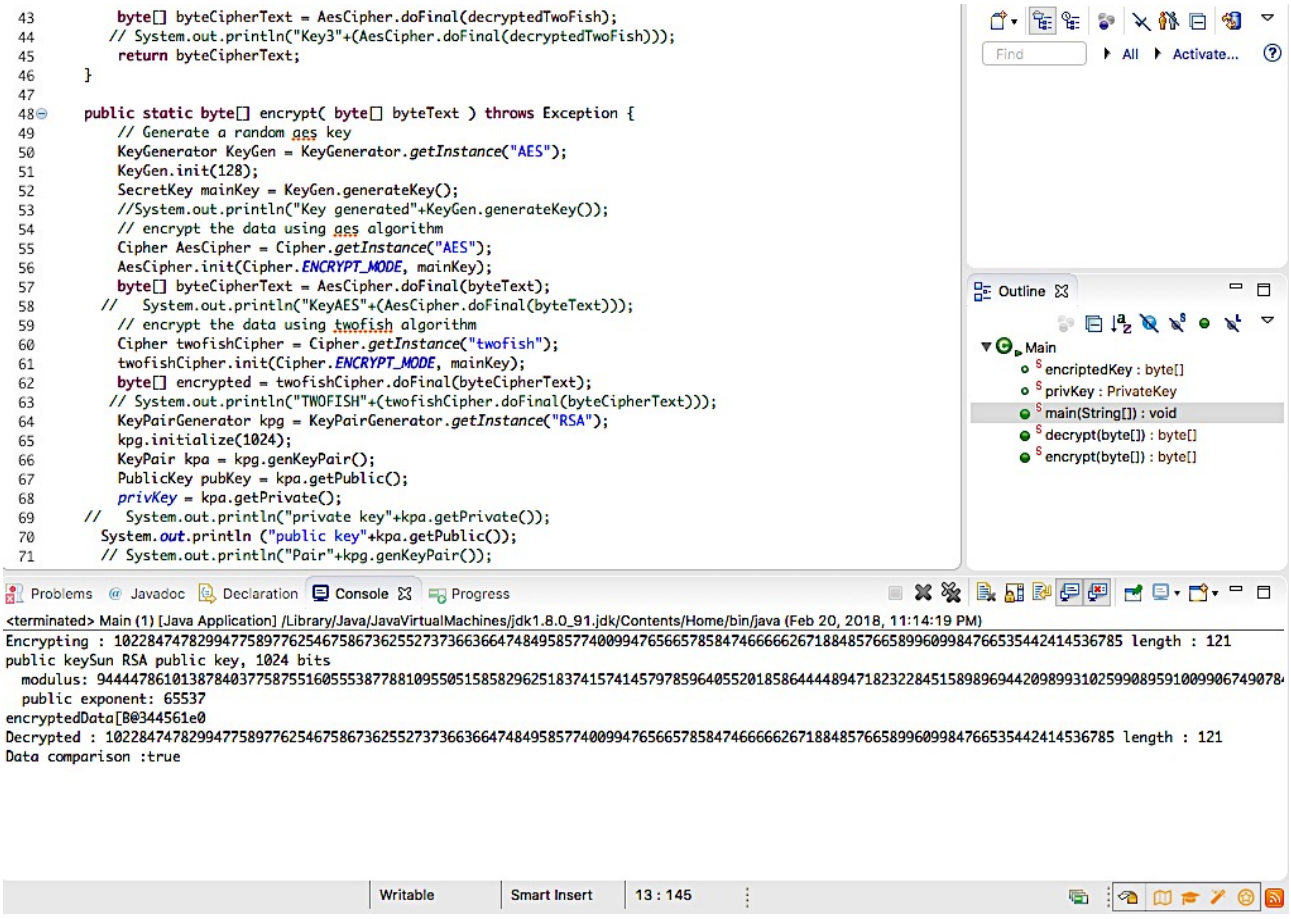

Figure 4. The result of hybrid algorithm.

6. Conclusion

Bluetooth is an inspiring innovative technology, which revolutionizes the way we communicate. However, the security mechanism of earlier versions Bluetooth technology has not been equipped with adequate level of security. Thus, it is more vulnerable to different attacks. Even though the current security mechanism of the latest versions (4.0 - 5.0 v) has been provided an acceptable level of security, however, a high level of security is paramount. In light of this paper, the proposed method was feasible as well as successfully implemented, and it is utilized in live scenarios. In the context of the feasibility of our approach, because the high level of security provided the encryption key remains secret, the original message remains safe. In case of intrusion, the organization of the complex message is intricate, which confused the intruder in understanding which part of the complex message contains the ciphertext and encrypted key. Moreover, the private key of the receiver will not be known. Therefore, the process of transmission data remains secure due to the unique security combination provided by our novel triple algorithm. Indeed, the proposed method has improved the security of encryption algorithm in Bluetooth. In the future, we plan to further develop new ideas concerning the Bluetooth security. First, we plan to analyze the current encryption mechanism weakness, after which we will propose a proper solution. Second, we will propose a geographic pairing based protocol, which will offer resistance against several attacks and add another authentication factor to the pairing process in order to present a strong authentication approach during the Bluetooth pairing process. Positively, these contributions will supply an extra security layer to achieve a high level of security.

References

[1] Bluetooth SIG, Bluetooth Specifications 1.0A-4.2. (2017) https://www.bluetooth.com/specifications

[2] Haataja, K. (2009) Security Threats and Countermeasures in Bluetooth-Enabled Systems. Doctoral Dissertation, University of Eastern Finland.

[3] Haataja, K., Hyppönen, K., Pasanen, S. and Toivanen, P. (2013) Bluetooth Security Attacks—Comparative Analysis, Attacks, and Countermeasures. Springer Briefs Book, Springer Verlag, Berlin, Heidelberg.

[4] Bluetooth SIG, Bluetooth—Our History. (2017) https://www.bluetooth.com/media/our-history

[5] Rege, K., Goenka, N., Bhutada, P. and Mane, S. (2013) Bluetooth Communication Using Hybrid Encryption Algorithm Based on AES and RSA. *International Journal of Computer Applications*, **71**, No. 22.

[6] Singh, G. (2013) A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications*, **67**, 33-38. https://doi.org/10.5120/11507-7224

[7] Bhanot, R. and Hans, R. (2015) A Review and Comparative Analysis of Various Encryption Algorithms. *International Journal of Security and Its Applications*, **9**, 289-306. https://doi.org/10.14257/ijsia.2015.9.4.27

[8] Shanta, J.V. (2012) Evaluating the Performance of Symmetric Key Algorithms: AES

(Advanced Encryption Standard) and DES (Data Encryption Standard). *IJCEM International Journal of Computational Engineering & Management*, **15**, 43-49.

[9] Stallings, W. (2006) Cryptography and Network Security: Principles and Practices. Pearson Education, India.

[10] Chowdhury, Z.J., Pishva, D. and Nishantha, G.G.D. (2010) AES and Confidentiality from the Inside Out. *The* 12*th International Conference on Advanced Communication Technology* (*ICACT*), **2**, 1587-1591.

[11] Gehlot, P., Biradar, S.R. and Singh, B.P. (2013) Implementation of Modified Twofish Algorithm Using 128 and 192-bit Keys on VHDL. *International Journal of Computer Applications*, **70**, 37-42. https://doi.org/10.5120/12024-8087

[12] Singh, S. and Singh, A. (2014) An Information Security Technique Using DES-RSA Hybrid and LSB. *International Journal of Emerging Technologies in Computational and Applied Sciences* (*IJETCAS*), **8**, 187-192.

[13] Singh, S., Maakar, S.K. and Kumar, D.S. (2013) A Performance Analysis of DES and RSA Cryptography. *International Journal of Emerging Trends & Technology in Computer Science* (*IJETTCS*), **2**, 418-423.

[14] Rege, K., Goenka, N., Bhutada, P. and Mane, S. (2013) Bluetooth Communication Using Hybrid Encryption Algorithm Based on AES and RSA. *International Journal of Computer Application*s, **71**, 10-13.

[15] Armknecht, F. and Krause, M. (2003) Algebraic Attacks on Combiners with Memory, in Advances. In: Boneh, D., Ed., *Advances in Cryptology—CRYPTO* 2003, *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 162-175.

[16] Hermelin, M. and Nyberg, K. (2000) Correlation Properties of the Bluetooth Combiner. In: Song, J., Ed., *Information Security and Cryptology—ICISC*'99, *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 17-29.

[17] Lu, Y. and Vaudenay, S. (2004) Faster Correlation Attack on Bluetooth Keystream Generator Eo. In: Franklin, M., Ed., *Advances in Cryptology—CRYPTO* 2004, *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 407-425. https://doi.org/10.1007/978-3-540-28628-8_25

[18] Albahar, M., Haataja, K. and Toivanen, P. (2016) Towards Enhancing Just Works Model in Bluetooth Pairing. *International Journal on Information Technologies & Security*, **8**, 67-82.

[19] Parsharamulu, B. and Krishnaiah, R.V. (2013) A New Design of Algorithm for Enhancing Security in Bluetooth Communication with Triple DES. *International Journal of Science and Research*, **2**, 279-283.

[20] Najar, J.M. and Dar, S.B. (2014) A New Design of a Hybrid Encryption Algorithm. *International Journal of Engineering and Computer Science*, **3**, 9169-9171.

[21] Singh, S., Maakar, S.K. and Kumar, S. (2013) A Performance Analysis of DES and RSA Cryptography. *International Journal of Emerging Trends & Technology in Computer Science*, **2**, 418-423.