Journal of the Korea Academia-Industrial cooperation Society
Vol. 22, No. 11 pp. 760-768, 2021

https://doi.org/10.5762/KAIS.2021.22.11.760
ISSN 1975-4701 / eISSN 2288-4688

Research on Improvement of Network Information Security Technology Based on Hybrid Encryption Algorithm

Hye-Jin Kim
Dept. of General Education, Kookmin University

하이브리드 암호 알고리즘 기반 네트워크 정보보호 기술 개선 연구

김혜진
국민대학교 교양대학

Abstract Data encryption is the foundation of information security. With the popularization of computer network applications, the technology has good prospects for development. Due to the sharing characteristics, data transmitted over the Internet is very easily tracked and stolen, so it is necessary to improve security during transmission. Currently, symmetric encryption and asymmetric encryption are most widely used. Symmetric encryption requires algorithms that use the same key for both encryption and decryption, and is commonly implemented when a sender needs to encrypt a large amount of data. Asymmetric encryption is suitable for small amounts of data owing to its long and slow encryption and decryption times. In this paper, by studying both symmetric and asymmetric data encryption algorithms, the advantages of both are combined into a hybrid algorithm. By comparing the hybrid algorithm with DES and DH encryption algorithms, the results prove that the security of the hybrid algorithm exceeds both of them. In particular, under a brute force attack simulation, the hybrid algorithm delivered up to four times better performance than conventional methods.

요 약 데이터 암호화 기술은 정보 보호의 기반이며, 컴퓨터 네트워크 애플리케이션의 대중화와 함께 다양한 분야에서 발전될 것으로 전망된다. 인터넷의 공유 특성으로 인해 인터넷에서 전송되는 데이터는 추적되거나 도난당하기 매우 쉽기 때문에, 데이터 전송 보안을 개선할 필요가 있다. 현재 가장 널리 사용되는 것은 대칭 암호화와 비대칭 암호화이다. 대칭 암호화에는 암호화 및 암호 해독에 동일한 키를 사용하는 암호화 알고리즘이 필요하다. 대칭 암호화는 일반적으로 메시지 발송인이 대량의 데이터를 암호화해야 할 때 사용된다. 비대칭 암호화는 암호화와 암호 해독 시간이 길고 속도가 느려 소량에 적합하다. 본 연구에서는 대칭 데이터 암호화 알고리즘과 비대칭 데이터 암호화 알고리즘의 연구를 통해, 양쪽의 장점을 결합하여 하이브리드 알고리즘을 개발하고자 하였다. 하이브리드 알고리즘을 DES 암호화 알고리즘 및 DH 알고리즘과 비교하였으며, 시뮬레이션을 통해 하이브리드 암호화 알고리즘의 보안이 DES 암호화 알고리즘 및 DH 암호화 알고리즘보다 향상되었다는 것을 보였다. 특히 무차별 공격 시뮬레이션과 관련해 하이브리드 알고리즘이 기존 방식보다 최대 4배 향상된 성능을 보였다.

Keywords : Network, Security, Symmetric, Asymmetric, Encryption, Hybrid Algorithm

*Corresponding Author : Hye-Jin Kim(Kookmin Univ.)
email: khj5187@kookmin.ac.kr
Received October 8, 2021 Revised October 29, 2021
Accepted November 5, 2021 Published November 30, 2021

1. Introduction

Due to the rapid development of the Internet and communication technologies, electronic informatization data has gradually become popular[1-3], but security issues have also become prominent. Therefore, a method that can effectively encrypt data is needed to deal with the problem of information leakage. There are many forms of data encryption technology in modern computer networks. At present, the most widely used are symmetric encryption and asymmetric encryption. Symmetric encryption requires encryption algorithms that use the same key for encryption and decryption. Symmetric encryption is usually used when the message sender needs to encrypt a large amount of data. Commonly used algorithms in symmetric encryption algorithms are: DES, TDEA, RC2, Blowfish, SKIPJACK, RC4, RC5, IDEA, 3DES, etc. The symmetric encryption algorithm is open, the amount of calculation is small, the encryption speed is fast, and the encryption efficiency is high. But before the data is transmitted, the sender and receiver must agree and save the secret key. If the secret key of either party is leaked, the security of encryption is impossible to talk about. In addition, its use is unitary, which also results in a huge number of keys for the sender and receiver, and key management becomes a burden on both parties. Asymmetric encryption uses a public key and a secret key to encrypt and decrypt data, respectively. The public key is public and the secret key is kept by the receiver. Asymmetric encryption has a long encryption and decryption time and slow speed, which is only suitable for small amounts. The main algorithms are: RSA, ECC (elliptic curve encryption algorithm), Rabin, D-H, knapsack algorithm, etc. The advantage of this mode is that the key management mode is relatively simple, and the probability of confusion and errors is small. The disadvantage is that the encryption process must fully consider the "fitness" with the keys held by all users, resulting in a linear increase in the complexity of the encryption algorithm.

There is no secure network in the absolute sense, because data is stored, transmitted, and processed in the computer network system. Any error in any link means that there are insecure factors. Computer network security includes logical security and Physical security. Logical security includes the security of information integrity, confidentiality and availability. Physical security is the protection of network system equipment and related facilities from physical damage. Threats to the logical security of network information include: unauthorized access: identity attacks, fake identities, illegal users entering the network system to perform illegal operations, and legitimate users performing unauthorized operations. Service interference: It refers to stealing the right to use information through illegal means, and maliciously adding, modifying, inserting, deleting or repeating irrelevant information, continuously interfering with the network information service system, slowing down the system response, or even paralyzing it, which has a serious impact Normal use by the user.

Literature[4,5] proposed to use the initial value sensitivity of the chaotic system to increase the complexity of the key and improve the security of data encryption, but this method takes too long to encrypt and decrypt, and the efficiency is too low. Literature[6] uses a ring topology for asymmetric data encryption, but it requires a delay time during operation, which reduces the encryption efficiency. Literature[7] mentions a data encryption method based on SQLite algorithm. Although this method is simple, it is easily affected by external conditions, making the encryption result inaccurate[7].

Based on this, this paper analyzes the advantages and disadvantages of the Blowfish

encryption method and the RSA public key encryption method, combines the two, and proposes a hybrid algorithm[8].

2. Hybrid Data Encryption Method

2.1 Blowfish encryption algorithm

The Blowfish encryption algorithm is a symmetric encryption algorithm that can quickly encrypt 64-bit strings. The Blowfish encryption algorithm can quickly encrypt and decrypt[9], and the key length is variable.

Using the Blowfish encryption algorithm to encrypt and decrypt data requires two steps: pre-processing the encryption algorithm key. In the design of the Blowfish encryption algorithm, it will provide the source keys pbox and sbox of the Blowfish algorithm, and they are fixed. Each user uses the same set of source keys pbox and sbox[10]. When encrypting data, you need to prepare a key for encryption, and combine this key with the source keys pbox and sbox to generate subkeys key_pbox and key_sbox. Encrypt data through key_pbox and key_sbox. The encryption process of the Blowfish encryption algorithm is shown in Fig. 1.

As shown in Fig. 1, since Blowfish is a symmetric encryption algorithm, it is also necessary to generate subkeys key_pbox and key_sbox through key preprocessing during decryption, but the order of encryption and decryption using subkeys is reversed.

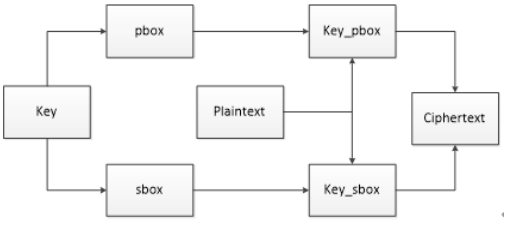

Fig. 1. Blowfish algorithm encryption flow chart

In the Blowfish encryption algorithm, since the length of the encryption key is uncertain, its length can be changed. Although this brings great convenience to the user when designing the key, it also brings great hidden dangers to the security of the data. Since the core of Blowfish encryption and decryption lies in the selection and confidentiality of the key, it is necessary to improve the selection and confidentiality of the Blowfish encryption algorithm.

2.2 RSA public key encryption algorithm

Among the current asymmetric encryption algorithms, the RSA algorithm is the most mature public key encryption algorithm[11-16]. It is an asymmetric algorithm that uses a public encryption key cryptosystem. The cipher system of public encryption key is by adopting an encryption algorithm method in which the encryption key is different from the decryption key, and the irreversible algorithm in mathematics, so that the known encryption algorithm key or decryption algorithm key is not used. It is possible to derive another algorithm key method, and its encryption algorithm key can be disclosed for data transmission. The core of the RSA public key encryption algorithm is to use the factorization of the product of two large prime numbers, which is a type of np problem, so as to realize the unsolvability of the encryption key to the decryption key. The RSA encryption algorithm generates the public key and the private key of the encryption algorithm through two large prime numbers and some related data. The public key is used for the encryption algorithm of the data, and the private key is only used for the decryption algorithm of the data. The detailed structure of the RSA encryption algorithm is shown in Table 1.

Table 1. Detailed composition of RSA

Name	Constitute
Prime number	P and Q
Common modulus	$N=P^*Q$
Euler function	$F(N)=(P-1)(Q-1)$
Public key E	$1<E<F(N)$ and with $F(N)$ relatively prime
Private key D	$D=E^{-1}(\mathrm{mod}(P-1)(Q-1))$
Encryption	$c\equiv m^E \mathrm{mod}(N)$
Decrypt	$m\equiv c^D \mathrm{mod}(N)$

As shown in Table 1, two prime numbers P and Q need to be selected first. In order to increase the difficulty of cracking, a prime number with a larger number of digits and the same number of digits is generally selected; the common modulus N is equal to the product of P and Q. Euler function $F(N) = (P - 1)(Q - 1)$. The public key E is expressed as a random number with $1<E<F(N)$ and relatively prime to F(N). The private key D is expressed as $D = E^{-1}(\mathrm{mod}(P-1)(Q-1))$, where mod is the remainder; suppose c is ciphertext, m is plaintext, and the encryption method is $c\equiv m^E \mathrm{mod}(N)$. The decryption method is $m\equiv c^D \mathrm{mod}(N)$. The public key is composed of E and N, and the private key is composed of D and N [17,18].

In the RSA public-key encryption algorithm, if there is only one set of keys, this can only complete the transfer of information from one party to the other, and at least two sets of keys are required to transfer information to each other. The basic flow chart of using the RSA encryption algorithm to transfer encrypted data between users is shown in Fig. 2.

As shown in Fig. 2, if user A wants to receive information from user B, he first needs to upload his public key A to the public network. User B obtains the plaintext 1 that needs to be sent for A public key encryption from the public network, and puts the secret After text 1 is uploaded to the public network, user A can use his A private key to decrypt, decrypt the ciphertext 1 into plaintext, and then obtain the plaintext 1 sent by user B. A user's sending file also requires such a step, and requires the use of another set of keys.

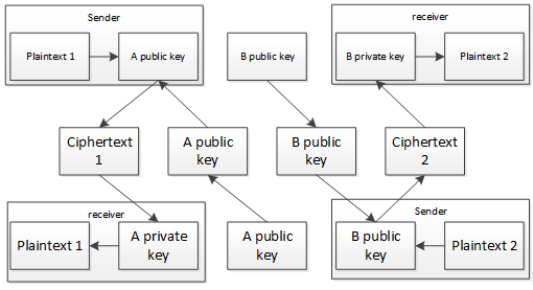

Fig. 2. Basic flow chart of information transfer between users

With the continuous development of human ability to seek prime factors, in order to ensure the security of the RSA encryption algorithm, the public modulus N must be at least 600 bits of complexity. The data operation cost during encryption and decryption is very high, and the efficiency of encryption and decryption is very low. Compared with the symmetric encryption algorithm, the efficiency will be hundreds of times lower, and with the rapid development of the large number decomposition factor technology, the length of the public modulus N is also increasing rapidly, which is not conducive to the standardization of the data format[19,20].

2.3 Hybrid encryption algorithm

Through the above analysis, it can be found that the use of Blowfish algorithm and RSA public key algorithm to encrypt data has their own shortcomings. Therefore, this article will combine these two methods and introduce the MD5 algorithm to digitally sign the ciphertext to verify the integrity of the file. It can prevent data loss and improve the security of encrypted data

transmission and the efficiency of data encryption and decryption. Now suppose that user A needs to transmit some data information to user B, and the data information is M.

To send data message M to user B, user A needs to prepare the public key of Blowfish encryption algorithm, MD5 algorithm and user B's RSA encryption algorithm. The operation process of the sender is shown in Fig. 3[21,22].

As shown in Fig. 3, the sending end of user A needs to encrypt the electronic file by using the Blowfish encryption algorithm to obtain the ciphertext of the official document; then encrypt the key of the Blowfish encryption algorithm with the public key of the RSA encryption algorithm received from the public network. The ciphertext of the Blowfish key will be obtained; finally, the ciphertext of the official document is digitally signed by the MD5 algorithm, which can verify the integrity of the data transmission. The security is very high.

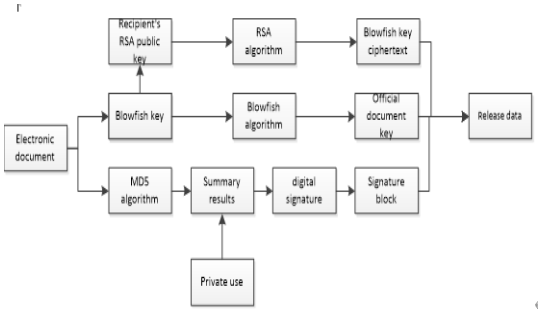

Fig. 3. Flowchart of the sender operation

There are five data that user B needs to receive, which are Blowfish key ciphertext, official ciphertext, MD5 algorithm public key, signature block, and hash function for digest. Fig. 4 below shows the operation flow of the receiving end.

As shown in Fig. 4, it is first necessary to verify the security and integrity of the source of the official ciphertext. Use the MD5 algorithm public key to decrypt the signature block and compare it with the ciphertext digested by the hash function. If the same, then the source is safe and the file is complete. Otherwise, the sender needs to resend it; then decrypt the key ciphertext with the private key of the RSA encryption algorithm to obtain the key of the Blowfish encryption algorithm; finally, pass the key pair of the Blowfish encryption algorithm. By decrypting the ciphertext of the official document, the electronic file M can be obtained.

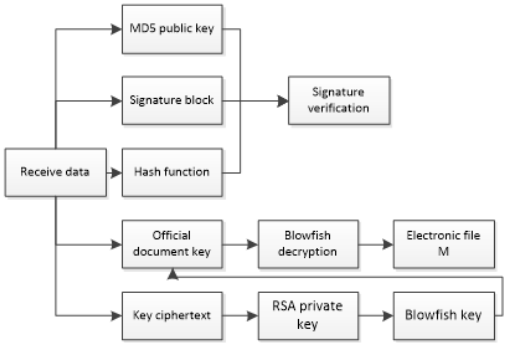

Fig. 4. Flow chart of receiver operation

2.4 DES encryption algorithm principle

The DES encryption algorithm is mainly derived from the Lucifer algorithm. This algorithm is a block encryption algorithm. It uses 64 bits as the data packet unit to encrypt and protect the grouped data. Then, the 64-bit group of data is encrypted and protected. It is input into the system in the form of plain text, and the system uses the DES encryption algorithm to convert the plain text into cipher text, and outputs the cipher text from the other end. The DES encryption algorithm is a symmetric algorithm, and the same algorithm is used in both data encryption processing and data decryption processing. The length of the key is usually 56 bits, and 56 bits of data can be arbitrarily selected. Therefore, a small amount of data is called a "weak key". Therefore, in order to improve the confidentiality of data, technical personnel should pay attention to the application of the key. In addition, when the DES encryption

algorithm performs block encryption processing on 64-bit plaintext, it needs to use data replacement to divide the plaintext into the following two types, one is the left half of the data, and the other is the right half of the data. The length of these two types of data is 32 bits. Then, the key is used to effectively combine the left half of the data and the right half of the data, and the inverse permutation method is used to realize the encryption and protection of the data, in order to further improve the stability, reliability and security of data transmission lay a solid foundation. It can be seen that the DES encryption process mainly involves the following points: (1) Re-ordering is used to group the plaintext in a group of 64 bits, and then initialize it and replace it, so that the length is 32. The left half of the data and the right half of the data. (2) Iteratively process the two halves of the data to obtain 16 transformations. (3) Using inverse permutation, the two halves of the data are swapped to generate the corresponding ciphertext.

3. Analysis of Experimental Results

In data information communication, the advantages and disadvantages of encryption systems are mainly reflected in two aspects: security and data encryption and decryption time. In order to verify the effectiveness of the hybrid data encryption technology designed in this article, the hybrid encryption algorithm designed in this article is combined with DES encryption. The algorithm is compared with the DH encryption algorithm, and the efficiency and security of encryption and decryption are analyzed[23,24].

3.1 Encryption and decryption work efficiency test

Three algorithms were used to encrypt and decrypt the data volume of 0.5G, 1G, 2G, 5G, 10G and 20G, and many experiments were carried out. The average time for encryption and decryption of these three data encryption algorithms is shown in Table 2[25,26].

The DES encryption algorithm is compared with the hybrid encryption algorithm. Because the hybrid encryption algorithm has more operation steps than the DES encryption algorithm, and the asymmetric encryption algorithm RSA is required to distribute and manage the keys of the Blowfish encryption algorithm, more additions are needed.

Table 2. Statistics of the average time of encryption and decryption

Data size	*DES*	*DH*	Hybrid algorithm
$0.5G$	77	7,789	152
$1G$	103	12,534	167
$2G$	212	25,765	251
$5G$	389	42,376	412
$10G$	613	65,786	630
$20G$	1,031	124,679	989

Decryption time, but because the Blowfish algorithm in the hybrid algorithm itself is shorter than the encryption and decryption time of the DES algorithm, as the amount of data increases, the efficiency of the hybrid algorithm gradually exceeds the DES algorithm. Compared with the DH algorithm and the hybrid algorithm, the efficiency of the hybrid algorithm is more than 100 times that of the DH algorithm. Because the asymmetric algorithm involves the calculation of large prime numbers and requires a large amount of calculation, the DH algorithm is not suitable for large data files. Encryption[27,28].

3.2 Data encryption security test

It is tested by checking the balance of ASCII value of cipher text characters and brute force cracking. In order to test the ability of the hybrid algorithm designed in this paper in terms of data

balance, this article counts the ASCII value of the ciphertext characters of the hybrid algorithm, DES algorithm and DH algorithm, and the distribution results are shown in Fig. 5 [29].

Analyzing Fig. 5, it can be concluded that the distribution of the characters in the ciphertext encrypted by the hybrid algorithm is relatively balanced, while the distribution of the characters in the other two methods is relatively scattered, with relatively large fluctuations. Analyze the distribution law of the ASCII value of the ciphertext data, and then use the statistical distribution law of the frequency of use of each character in life, and the password can be deciphered. If the frequency distribution cannot be changed, there will be a risk of being cracked, but the hybrid encryption algorithm designed in this article can prevent this cracking method well.

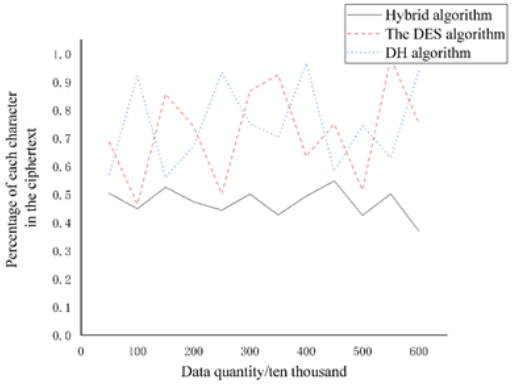

Fig. 5. Statistics of ciphertext ASCII value

In order to test the effect of the hybrid algorithm against deciphering in practice, the brute force deciphering method is used to test its safety. This article uses DES encryption algorithm, DH encryption algorithm and hybrid algorithm to encrypt 200K data, text files, pictures and multimedia videos, and then uses FTP protocol to make it transmitted in the local area network. Perform data interception, and then brute force the four types of data. The brute force data packet uses a desktop computer with Intel i7-10700K processor, and it is set to repeatedly decode it five times within 15 minutes. The results are shown in Table 3.

Table 3. Statistics of brute force cracking

Type of data	*DES*	*DH*	Hybrid algorithm
Data	4	1	1
Text file	4	1	0
Picture	2	0	0
Multimedia video	0	0	0

It can be seen from the data in Table 3 that the hybrid algorithm designed in this paper has a better data security effect than DES and DH algorithms. From the principle of data encryption, the Blowfish encryption algorithm used by the hybrid encryption algorithm has higher security than the DES encryption algorithm, and it manages the key of the Blowfish encryption algorithm through the RSA encryption algorithm, which can further improve the security. The RSA encryption algorithm and the DH encryption algorithm have similar core theories. They are both derived from the mathematical theory that large prime numbers cannot be decomposed into prime factors. The hybrid encryption algorithm adds the Blowfish encryption algorithm to this layer of encryption, so hybrid encryption The security of the algorithm surpasses the DES encryption algorithm and the DH encryption algorithm.

4. Conclusion

Network security has become an important issue in people's lives. Aiming at the hidden dangers of information security in computer networks, a new type of data encryption technology is proposed. This technology combines the Blowfish encryption algorithm and

the RSA encryption algorithm to solve the problem of symmetric algorithms in conventional technologies. Security issues, difficult key management, and low efficiency of asymmetric algorithm encryption and decryption. By comparing the hybrid algorithm in this study with the DES algorithm and the DH algorithm, in the encryption and decryption efficiency and security test, the efficiency of the hybrid algorithm is increased by 100 times and the security level is high. When considering average time of encryption and decryption of 20G Data, Hybrid algorithm(989) showed better result than DES(1,031) and DH(124,679).

References

[1] Meng Li, Zhang Shuang, Wang Fuqiang, "Influence of Internet-based Social Big Data on Personal Credit Reporting", *Asia-pacific Journal of Convergent Research Interchange*, Vol.6, No.7, pp.39-57, July 2020.
DOI: http://dx.doi.org/10.47116/apjcri.2020.07.05

[2] N. Thirupathi Rao, "Performance Evaluation of Optimized Tandem Communication Network Model", *Asia-pacific Journal of Convergent Research Interchange,* Vol.5, No.3, pp.211-220, September 2019.
DOI: http://dx.doi.org/10.21742/apjcri.2019.09.21

[3] Jung-Ha Park, "Comparison between eLearning video and Smartphone Application for Information Technology Use in Nursing Education", *Asia-pacific Journal of Convergent Research Interchange*, Vol.5, No.4, pp.39-47, December 2019.
DOI: http://dx.doi.org/10.21742/apjcri.2019.12.05

[4] Sundarapandian V, Pehlivan I., "Analysis, control, synchronization, and circuit design of a novel chaotic system", *Mathematical & Computer Modelling,* Vol.55, No.7-8, pp.1904-1915, April 2012.
DOI: https://doi.org/10.1016/j.mcm.2011.11.048

[5] Viet-Thanh Pham, Christos Volos, Sajad Jafari, Zhouchao Wei and Xiong Wang, "Constructing a Novel No-Equilibrium Chaotic System". *International Journal of Bifurcation and Chaos*, Vol.24, No.5, 2014, 1450073.
DOI: https://doi.org/10.1142/S0218127414500734

[6] Andreas Pommer, Andreas Uhl., "Selective encryption of wavelet-packet encoded image data: efficiency and security", *Multimedia Systems*, Vol.9, pp.279-287, 2003.
DOI: https://doi.org/10.1007/s00530-003-0099-y

[7] Bensikaddour E. H., Bentoutou Y., Taleb N., "Satellite image encryption method based on AES-CTR algorithm and GEFFE generator", *Proceedings of 8th International Conference on Recent Advances in Space Technologies (RAST),* IEEE, Istanbul, Turkey, pp.247-252, 19-22 June 2017.
DOI: https://doi.org/10.1109/RAST.2017.8002953

[8] Wook-Lae, Cho, Kyung-Wook, et al., "2,048 bits RSA public-key cryptography processor based on 32-bit Montgomery modular multiplier", *Journal of the Korea Institute of Information and Communication Engineering*, Vol.21, No.8, pp.1471-1479, 2017.
DOI: https://doi.org/10.6109/jkiice.2017.21.8.1471

[9] Noah Oluwatobi Akande, Christiana Oluwakemi Abikoye, Marion Olubunmi Adebiyi, Anthonia Aderonke Kayode, Adekanmi Adeyinka Adegun, Roseline Oluwaseun Ogundokun, "Electronic Medical Information Encryption Using Modified Blowfish Algorithm", *Proceedings of International Conference on Computational Science & Its Applications,* Lecture Notes in Computer Science, vol.11623. Springer, Cham., Saint Petersburg, Russia, pp.166-179, July 1-4, 2019.
DOI: https://doi.org/10.1007/978-3-030-24308-1_14

[10] R. Mahaveerakannan and C. Suresh Gnana Dhas, "Customized RSA public key cryptosystem using digital signature of secure data transfer natural 22 number algorithm", *International Journal of Computer Technology & Application,* International Science Press, Vol.9, No.5, pp.2627-2632, 2016. WEB: https://www.researchgate.net/publication/309103706_Customized_RSA_public_key_cryptosystem_using_Digital_Signature_of_secure_data_transfer_natural_number_algorithm

[11] Jung Hyun Kim, "Proposal for Advanced Attribute-based Encryption in Mobile Cloud Computing", *Asia-pacific Journal of Convergent Research Interchange*, Vol.1, No.4, pp.45-51, December 31, 2015.
DOI: http://dx.doi.org/10.21742/apjcri.2015.12.07

[12] Pavan Yadav, "Advanced Looping Broadcast Proxy Re-Encryption in Cloud computing", A*sia-pacific Journal of Convergent Research Interchange*, Vol.2, No.1, pp.21-28, March 2016.
DOI: http://dx.doi.org/10.21742/APJCRI.2016.03.04

[13] Jae Yoon Lee, Mounika Durbha, "Customary Broadcast Encryption with Advanced Encryption and Short ciphertexts", *Asia-pacific Journal of Convergent Research Interchange,* Vol.2, No.2, pp.27-33, June 2016.
DOI: http://dx.doi.org/10.21742/APJCRI.2016.06.04

[14] Bhargavi Nadella, "Data Encryption using Geometric Range", *Asia-pacific Journal of Convergent Research Interchange*, Vol.2, No.3, pp.21-28, September 2016.
DOI: http://dx.doi.org/10.21742/APJCRI.2016.09.03

[15] Su Min Shin, Vandana Roy, "Hybrid key-Based

Encryption in Cloud Storage", *Asia-pacific Journal of Convergent Research Interchange*, Vol.2, No.3, pp.29-34, September 2016.
DOI: http://dx.doi.org/10.21742/APJCRI.2016.09.04

[16] V. Sujatha, "Auditing of Storage Security on Encryption", *Asia-pacific Journal of Convergent Research Interchange*, Vol.3, No.2, pp.1-9, June 2017.
DOI: http://dx.doi.org/10.21742/APJCRI.2017.06.01

[17] Shailendra Kumar Tripathi, Bhupendra G., Pandian S., "An alternative practical public-key cryptosystems based on the Dependent RSA Discrete Logarithm Problems", *Expert Systems with Applications*, Vol.164, February 2021.
DOI: https://doi.org/10.1016/j.eswa.2020.114047

[18] I. Jaya, S. M. Hardi, J. T. Tarigan, E. M. Zamzami and P. Sihombing, "Distributed Factorization Computation on Multiple Volunteered Mobile Resource to Break RSA Key", *Journal of Physics Conference Series*, Vol.801, No.1, 012081, pp.1-6, 2017.
DOI: https://doi.org/10.1088/1742-6596/801/1/012081

[19] Siregar H. , Junaeti E. , Hayatno T., "Implementation of digital signature using AES and RSA algorithms as a security in disposition system AF letter", *IOP Conference Series: Materials Science and Engineering*, Vol.180, No.1, pp.12-55, 2017.
DOI: http://dx.doi.org/10.1088/1757-899X/180/1/012055

[20] Gulen U., Alkhodary A., Baktir S., "Implementing RSA for Wireless Sensor Nodes", *Sensors*, Vol.19, No.13, pp.1-15, June 2019.
DOI: https://doi.org/10.3390/s19132864

[21] Avudaiappan T., Ba Lasubramanian R., Pandiyan S. S., et al. "Medical Image Security Using Dual Encryption with Oppositional Based Optimization Algorithm", *Journal of Medical Systems*, Vol.42, No.11, pp.1-11, September 2018.
DOI: https://doi.org/10.1007/s10916-018-1053-z

[22] Mansour A. H, "Encryption and decryption analysis of the RSA digital signature based on MD5 and SHA hash functions using strong prime", *Journal of Soft Computing and Decision Support Systems*, Vol.4, No.1, pp.7-15, 2017.
WEB: https://jscdss.utm.my/index.php/files/article/view/125

[23] Hamdi M., Miri J., Moalla B., "Hybrid encryption algorithm (HEA) based on chaotic system", *Soft Computing*, Vol.25, No.7, pp.1847-1858, February 2021.
DOI: https://doi.org/10.1007/s00500-020-05258-z

[24] Chalee Thammarat, Werasak Kurutach, "A lightweight and secure NFC-base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification", *International Journal of Communication Systems*, Vol.32, No.12, pp.e3991.1-e3991.21, June 2019.
DOI: https://doi.org/10.1002/dac.3991

[25] Vikas Goyal, Chander Kant, "An Effective Hybrid Encryption Algorithm for Ensuring Cloud Data Security", *Big Data Analytics*, Vol.654, pp.195-210, October 2017.
DOI: https://doi.org/10.1007/978-981-10-6620-7_20

[26] Marwan Ali Albahar, Olayemi Olawumi, Keijo Haataja, Pekka Toivanen, "Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption", *Journal of Information Security*, Vol.9, No.2, pp.168-176, April 2018.
DOI: https://doi.org/10.4236/jis.2018.92012

[27] Pasquale Memmolo, Maria Iannone, Maurizio Ventre, Paolo Antonio Netti, Andrea Finizio, Melania Paturzo, and Pietro Ferraro, "Quantitative phase maps denoising of long holographic sequences by using SPADEDH algorithm", *Applied Optics*, Vol,52, No.7, pp.1453-1460, 2013.
DOI: https://doi.org/10.1364/AO.52.001453

[28] L. Vinodhkumar, S. Vinoth B., S. Sivaganesh, "In-dependable Data hiding in an Encrypted Image using FCM-DH Algorithm", *International journal of scientific research in science, engineering and technology*, Vol.1, No.1, pp.159-161, 2015. WEB: https://www.semanticscholar.org/paper/In-Dependable-Data-hiding-in-an-Encrypted-Image-Vinodhkumar-VinothB/66ad16a44848c8aa2330d7501016f5d1d80ba317

[29] R, Sudhakar, P. V. Venkateswara Rao, "Optimized Video Image Security and Compression Using DCT and Depth Hexagon Based Search (DHEXBS) Algorithm", *International Journal of Applied Engineering Research*, Vol.13, No.7 pp.4776-4781, 2018. WEB: https://www.ripublication.com/ijaer18/ijaerv13n7_23.pdf

Hye-Jin Kim [Regular member]

- Feb. 2007 : Woosuk Univ., Education, MEdu
- Jul. 2017 : Univ. of Bristol, Education, PhD
- Sep. 2020 ~ current : Kookmin Univ., Dept. of General Education, Assistant Professor

〈Research Interests〉
U-learning, Education Technology, Artificial Intelligence, IoT, Remote Education Management Technology