Super-Encryption Cryptography with IDEA and WAKE Algorithm

Dahlan Abdullah¹, Robbi Rahim²*, Andysah Putera Utama Siahaan², Ananda Faridhatul Ulva¹, Zahratul Fitri¹, M Malahayati³ and H Harun³

¹Department of Informatics, Universitas Malikussaleh, Aceh, Indonesia
²School of Computer and Communication Engineering, Universiti Malaysia Perlis, Malaysia
³Department of Law, Universitas Malikussaleh, Aceh, Indonesia

*usurobbi85@zoho.com

Abstract. The security and confidentiality of information becomes an important factor in communication, the use of cryptography can be a powerful way of securing the information, IDEA (International Data Encryption Algorithm) and WAKE (Word Auto Key Encryption) are some modern symmetric cryptography algorithms with encryption and decryption function are much faster than the asymmetric cryptographic algorithm, with the combination experiment IDEA and WAKE it probable to produce highly secret ciphertext and it hopes to take a very long time for cryptanalyst to decrypt the information without knowing the key of the encryption process.

1. Introduction

Encryption is a standard way used to scramble data, so it is unreadable by unidentified parties[1]–[4], there are many cryptographic algorithms that can be used such as Triple DES, RSA, Blowfish, Twofish, AES[5] commonly used to secure data, there are also other symmetric algorithms such as IDEA (International Data Encryption Algorithm)[6] and WAKE (Word Auto Key Encryption)[7] which has a pretty good security process.

Super-Encryption[8] is one technique that can be used to secure data by combining 2 (two) type or more symmetric cryptographic algorithms, this process is commonly used to re-encrypt the encrypted ciphertext result from cryptographic algorithm[9]–[11], the combination of cryptographic algorithms[12] can produce safer ciphertext from various cryptanalyst attacks that want to know data or information from ciphertext, super-encryption in this paper using IDEA and WAKE algorithm.

The IDEA and WAKE algorithm used one by one, the first ciphertext (C1) is generated from the IDEA algorithm encryption process and then re-encrypted using the WAKE algorithm to generate the new Ciphertext (C2), the encryption and decryption process of the IDEA and WAKE algorithms use different keys, using different keys makes cryptanalyst take a longer time to know the data or information from the ciphertext, the use of cryptography does not guarantee data or information free from attacks but can make irresponsible parties be longer in getting the data.

2. Methodology

Super-Encryption in this paper perform step by step where plaintext encrypted with IDEA algorithm and then re-encrypted with WAKE algorithm, for process IDEA algorithm as in the following function:
a. **Key Formation**
This formation process begins by splitting 128-bit keys into eight pieces of 16-bit sub-key, key rotated 25 bits to the left and divided into eight subkeys again[13], [14].

![Key Formation Diagram](image)

**Figure 1. Key Formation**

b. **Encryption Process**
64-bit plaintext is divided into four sub-blocks of 16 bits used for the first iteration. At each iteration, four sub-blocks are XOR-aligned, added, multiplied by another and with six pieces 16-bit sub-keys, next is the sequence of the IDEA algorithm process:
1. Multiply X1 with K1 mod (216 + 1).
2. Add X2 with K2 mod 216.
3. Add X3 with K3 mod 216.
4. Multiply X4 with K4 mod (216 + 1).
5. XOR results from step 1 and 3.
6. XOR results from step 2 and 4.
7. Multiply the result from step 5 with K5 mod (216 + 1).
8. Add the result from step 6 and 7 mod 216.
9. Multiply the result from step 8 with K6 mod (216 + 1).
10. Add the result from step 7 and 9.
11. XOR results from step 1 and 9.
12. XOR results from step 3 and 9.
13. XOR results from step 2 and 10.
14. XOR results from step 4 and 10.

c. **Decryption Process**
The decryption process is precisely the same as the encryption process. The difference lies only in the rules of the sub-key. The encryption process reverses the order of the sub-key, and the sub-key is inverse. The sub-key on the output transformation step of the encryption process is invoked and used as a sub-key in round 1 of the decryption process [11].
Next is how WAKE algorithm works on the encryption and decryption process [6]:

a. A process of forming table S-Box (Substitution Box).
b. A process for forming the key.
c. Encryption and decryption process.

The core of the WAKE method lies in the process of forming the S-Box table and the critical building process. The S-Box table of the WAKE method is flexible and different for each round. Super-encryption IDEA and WAKE algorithm can be seen in Figure 2 below:

![Diagram of Super-Encryption IDEA and WAKE Algorithm]

Figure 2. Super-Encryption IDEA and WAKE Algorithm

3. Result and Discussion
The experiment performed by step by step, for the first stage determines the plaintext and key as below:
Plaintext = DAHLANRR
Key = InternationalCon
The first step is to do the process of forming the key with the IDEA algorithm based on the process of figure 1 so the results obtained as follows:
Key = InternationalCon = 195C9B985D1A5BDB985B10DBDB925B9D
Encryption by using IDEA algorithm using a key that has been formed got a result as follows:
Ciphertext = IðŽÁ¿

The ciphertext of the IDEA algorithm results is then re-encrypted with the WAKE algorithm by using different keys as follows:
Plaintext = IðŽÁ¿
Key = Dahlanabdullahok
Encryption process from WAKE algorithm can be seen below:
ASCII from 'I' = 49
ASCII from ' ' = 20
ASCII from 'Ž' = F0
ASCII from 'Á' = C1
ASCII from '¿' = BF

3
Super-encryption algorithm IDEA and WAKE can be done well in the experiments performed, the combination of these two algorithms is very suitable because the ciphertext of the IDEA algorithm in the form of ASCII can be re-encrypted with WAKE algorithm that changes the plaintext into the new hexadecimal form and then re-encrypted, for more details of the combination of these two algorithms can be seen in table 1 below:

| No | Plaintext   | Key               | IDEA                      | WAKE                      | Combination  |
|----|-------------|-------------------|---------------------------|---------------------------|--------------|
| 1  | ICCAI USU   | uzumakinarutooke | ì',w)žæ                  | p½_YpY_.l                 | åñZENÖEx     |
| 2  | Conference  | uzumakinarutooke | 'Ýñt6• á                 | zºı,✓1SZō>\±MP$          | «i×<MEU_    |
| 3  | Kolaborasi  | uzumakinarutooke | Ÿ!g”~6                   | r*8["&...J”tLY8®Re’      | _ząÅ“åiHš_  |
| 4  | Scopus Conference | scopusindexingok | ]Èä]Gl                    | Ûú†¹yêöööö·+öý’,î         | †Å “>å "    |
| 5  | GWA Scopus  | scopusindexingok | &O–«®3©                   | II—nUú†¹yêöö¸îé            | ¬YmØ•Fåå    |

The result of the combination of IDEA and WAKE algorithm produces different ciphertext, with this combination is probably make cryptanalyst difficult to know the plaintext of ciphertext.

4. Conclusion
The IDEA and WAKE algorithm used in this paper can be combined as well, the use of different keys on each algorithm can also be done, the next development of the encryption process can be a mixed mode where the encryption process is done simultaneously for two different algorithms or more materials.

References
[1] Rahim R and Ikhwan A, 2016 Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher Int. J. Sci. Res. Sci. Technol. 2, 6 p. 71–78.
[2] Putera A Siahaan U and Rahim R, Aug. 2016 Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm Int. J. Secur. Its Appl. 10, 8 p. 173–180.
[3] Rahim R and Ikhwan A, Nov. 2016 Study of Three Pass Protocol on Data Security Int. J. Sci.
Res. 5, 11 p. 102–104.

[4] Rahim R, 2017 Man-in-the-middle-attack prevention using interlock protocol method ARPN J. Eng. Appl. Sci. 12, 22 p. 6483–6487.

[5] Tange H and Andersen B, 2013 Attacks and countermeasures on AES and ECC in 16th International Symposium on Wireless Personal Multimedia Communications (WPMC) p. 1–5.

[6] Chen J Xue D and Lai X, 2008 An analysis of international data encryption algorithm(IDEA) security against differential cryptanalysis Wuhan Univ. J. Nat. Sci. 13, 6 p. 697–701.

[7] Legito L and Rahim R, 2017 SMS Encryption Using Word Auto Key Encryption Int. J. Recent Trends Eng. Res. 3, 1 p. 251–256.

[8] Iswahyudi C Setyaningsih E and Widyastuti N, 2012 Pengamanan kunci enkripsi citra pada algoritma super enkripsi menggunakan metode end of file Pros. Semin. Nas. Apl. Sains Teknol. Periode III November p. 278–285.

[9] Kartikadarma E Listyorini T and Rahim R, 2018 An Android mobile RC4 simulation for education World Trans. Eng. Technol. Educ. 16, 1 p. 75–79.

[10] Rahim R Hartama D Nurdiyanto H Ahmar A S Abdullah D and Napitupulu D, 2018 Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm J. Phys. Conf. Ser. 954, 1 p. 12008.

[11] Nurdiyanto H Rahim R and Wulan N, Dec. 2017 Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement J. Phys. Conf. Ser. 930, 1 p. 12005.

[12] Yu L Wang Z and Wang W, 2012 The Application of Hybrid Encryption Algorithm in Software Security Fourth Int. Conf. Comput. Intell. Commun. Networks p. 762–765.

[13] Ludwig G A and Alegre P, 2007 International Data Encryption Algorithm (IDEA) 8, 1 p. 6–11.

[14] Daemen J Govaerts R and Vandewalle J, 1993, Weak Keys for IDEA, in Advances in Cryptology — CRYPTO’ 93, (Berlin, Heidelberg: Springer Berlin Heidelberg), p. 224–231.