

APPARATUS AND METHOD FOR ENCRYPTION

CROSS-REFERENCE TO RELATED APPLICATION

[1] This application claims priority to and the benefit of Korean Patent Application No. 10-2016-0142391, filed on October 28, 2016, the disclosure of which is incorporated herein by reference in its entirety.

BACKGROUND

1. Field

[2] Embodiments of the present disclosure relate to encryption technology.

2. Discussion of Related Art

[3] A conventional white box cipher implementation method has a structure in which an entire implementation of a cipher algorithm cannot be divisionally changed. Thus, the entire implementation should be simultaneously shared to perform encryption or decryption.

[4] Accordingly, an encryption function can be illegally used by a user having no authority to use a service or can be stolen by an unauthorized terminal utilizing the entire implementation.

[5] Korean Patent No. 10-1580879 proposes a method of updating a white box encryption implementation (including a key update). However, the update is made without analysis and authentication of attributes, and all entire information is shared. Thus, the method has weakness in that an unauthorized user uses an encryption function and an entire implementation thereof is exposed due to a lost terminal or a malicious attack.

SUMMARY

[6] Embodiments of the present disclosure are directed to providing an apparatus

and method for encryption.

[7] According to an aspect of the present disclosure, there is provided an encryption apparatus including a storage configured to store a static key table, and at least one processor configured to implement: an authenticator configured to perform authentication with an external apparatus and acquire authentication information and a key table generator configured to generate a dynamic key table using the authentication information acquired through the authenticator authentication.

[8] The key table generator may generate the dynamic key table using the static key table and the authentication information.

[9] The at least one processor may further implement a key table provider configured to provide the dynamic key table to the external apparatus.

[10] The at least one processor may further implement an encryption/decryption unit configured to perform encryption or decryption using the static key table and the dynamic key table.

[11] According to another aspect of the present disclosure, there is provided an encryption apparatus including a storage configured to store a static key table, and at least one processor configured to implement: an authenticator configured to perform authentication with an external apparatus, and a key table acquirer configured to transmit the authentication information acquired through the authenticator to a key table generation sever and receive a dynamic key table generated using the transmitted authentication information from a key table generation server.

[12] The key table acquirer may receive a dynamic key table generated using a static key table stored in the key table generation server and the transmitted authentication information from the key table generation server.

[13] The at least one processor may further implement an encryption/decryption

unit configured to perform encryption or decryption using the static key table and the dynamic key table.

[14] According to another aspect of the present disclosure, there is provided an encryption apparatus including a storage configured to store a static key table, and at least one processor configured to implement: an authenticator configured to perform authentication with an external apparatus and acquire authentication information from the external apparatus and a key table acquirer configured to acquire a dynamic key table generated using the authentication information acquired through received by the authentication authenticator from the external apparatus.

[15] The key table acquirer may receive a dynamic key table generated using a static key table stored in the external apparatus and the authentication information from the external apparatus.

[16] The at least one processor may further implement an encryption/decryption unit configured to perform encryption or decryption using the static key table and the dynamic key table.

BRIEF DESCRIPTION OF THE DRAWINGS

[17] The above and other objects, features and advantages of the present disclosure will become more apparent to those of ordinary skill in the art by describing in detail exemplary embodiments thereof with reference to the accompanying drawings, in which:

[18] FIG. 1 is a block diagram of an encryption apparatus according to an embodiment of the present disclosure;

[19] FIG. 2 is a diagram showing an example of a cipher algorithm according to an embodiment of the present disclosure;

[20] FIG. 3 is a diagram showing an example of a cipher algorithm according to

another embodiment of the present disclosure;

[21] FIG. 4 is a block diagram of a key table generator according to an embodiment of the present disclosure;

[22] FIG. 5 is a diagram showing an example of a round function used in an operation unit according to an embodiment of the present disclosure;

[23] FIG. 6 is a block diagram of an encryption apparatus according to an additional embodiment of the present disclosure;

[24] FIG. 7 is a block diagram of an encryption apparatus according to another embodiment of the present disclosure;

[25] FIG. 8 is a flowchart of an encryption method according to an embodiment of the present disclosure;

[26] FIG. 9 is a flowchart of an encryption method according to an additional embodiment of the present disclosure;

[27] FIG. 10 is a flowchart of an encryption method according to another embodiment of the present disclosure; and

[28] FIG. 11 is a flowchart of an encryption method according to still another embodiment of the present disclosure.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

[29] Hereinafter, embodiments of the present disclosure will be described in detail with reference to the accompanying drawings. The following detailed description is provided to assist the reader in gaining a comprehensive understanding of the methods, apparatuses, and/or systems described herein. However, the description is only an example, and the present disclosure is not limited thereto.

[30] In describing embodiments of the present disclosure, when it is determined

that a detailed description of known techniques associated with the present disclosure would unnecessarily obscure the subject matter of the present disclosure, the detailed description thereof will be omitted. Also, terms used herein are defined in consideration of the functions of the present disclosure and may be changed depending on a user, the intent of an operator, or a custom. Accordingly, the terms must be defined based on the following overall description of this specification. The terminology used herein is for the purpose of only describing embodiments of the present disclosure and should not be restrictive. The singular forms "a," "an," and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It should be understood that the terms "comprises," "comprising," "includes," and/or "including" specify the presence of stated features, integers, steps, operations, elements, and/or components when used herein, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[31] FIG. 1 is a block diagram of an encryption apparatus according to an embodiment of the present disclosure.

[32] Referring to FIG. 1, an encryption apparatus 100 according to an embodiment of the present disclosure includes a storage 110, an authenticator 120, a key table generator 130, and an encryption/decryption unit 140.

[33] The storage 110 stores a portion of a cipher algorithm for encryption or decryption. In detail, the cipher algorithm may be implemented to perform encryption or decryption with at least one static key table and at least one dynamic key table, and the storage 110 may store the remaining portion of the cipher algorithm other than the dynamic key table. For example, when the cipher algorithm is composed of at least one static key table and at least one dynamic key table, the storage 110 may store the static key table.

[34] In this case, the key table may refer to a lookup table composed of random

values induced from a seed value. Also, the static key table may refer to an unchanged key table that is applied in advance during generation of the cipher algorithm, and the dynamic key table may refer to a key table that is generated later and then added to or updated.

[35] The static key table may be independent of the dynamic key table. In this case, the static key table being independent means that the static key table is independently generated irrespective of the dynamic key table, and thus is not changed according to a change of the dynamic key table in the cipher algorithm.

[36] According to an embodiment of the present disclosure, the cipher algorithm may be a white-box cipher algorithm that is implemented by applying at least one static key table and at least one dynamic key table to a block cipher algorithm.

[37] For example, the cipher algorithm may be a white-box cipher algorithm that is implemented by applying a plurality of key tables to a block cipher algorithm such as an Advanced Encryption Standard (AES) algorithm, a Data Encryption Standard (DES) algorithm, an International Data Encryption (IDEA) algorithm, and a Blowfish algorithm.

[38] For example, as shown in FIG. 2, the cipher algorithm may be a cipher algorithm generated by alternately and repeatedly combining a substitution function F and a plurality of key tables on the basis of the Even-Mansour scheme. In this case, the plurality of key tables may include a static key table and a dynamic key table.

[39] The substitution function F may refer to any form of function that is cryptographically safe and configured to output input values as different values having the same length, and may include a block cipher algorithm such as, for example, an AES algorithm, a DES algorithm, a 3DES algorithm, an IDEA algorithm, and a Blowfish algorithm.

[40] As another example, the cipher algorithm may be a cipher algorithm obtained by applying the key tables to each round function F of a Feistel structure of a Feistel-

structured block cipher algorithm such as, for example, a DES algorithm, as shown in FIG. 3. In this case, the key tables applied to each round function may include a static key table and a dynamic key table.

[41] In an implementation step for a cipher algorithm, a developer may predetermine the number of static key tables and dynamic key tables included in the cipher algorithm and positions at which the static key tables and the dynamic key tables are to be applied. Also, the remaining portion of the cipher algorithm other than the dynamic key tables may be stored in advance in the encryption apparatus 100 and provided to a user or may be received from a separate server through a safe channel and then stored.

[42] The authenticator 120 performs authentication with an external apparatus. In this case, the external apparatus may be an apparatus that shares the remaining portion of the cipher algorithm stored in the storage 110.

[43] In order to perform the authentication, the authenticator 120 may use various well-known authentication methods for sharing authentication information between both parties through authentication, for example, a password-based authentication method, a challenge-response authentication method, etc.

[44] The key table generator 130 generates at least one dynamic key table using authentication information acquired through the authentication performed by the authenticator 120.

[45] In detail, the key table generator 130 may generate the at least one dynamic key table using authentication information shared with the external apparatus through the authentication performed by the authenticator 120. In this case, the authentication information may be different depending on an authentication method used for the authentication.

[46] In detail, referring to FIG. 4, the key table generator 130 according to an

embodiment of the present disclosure may include a random number generator 131 configured to generate a random number from the authentication information, and an operation unit 133 configured to generate a dynamic key table using the generated random number.

[47] The random number generator 131 may receive the authentication information from the authenticator 120 and repeatedly generate a random number k_i .

[48] For example, when it is assumed that three random numbers are generated, the random number generator 131 may generate a first random number from the received authentication information and then generate a second random number from the generated first random number. Subsequently, the random number generator 131 may generate a third random number from the generated second random number.

[49] The operation unit 133 may generate random values for configuring a dynamic key table from the random numbers generated by the random number generator 131, and may generate at least one dynamic random key table including the generated random values.

[50] In detail, the operation unit 133 may generate random values by using a round function for generating a random value and apply the random number k_i generated by the random number generator 131 to the round function every round.

[51] In detail, FIG. 5 is a diagram showing an example of a round function used by the operation unit 133.

[52] Referring to FIG. 5, the operation unit 133 may perform an XOR operation between the random number k_i generated by the random number generator 131 and a random value a with the same size as the random number k_i , and may divide a result of the XOR operation into two parts and apply the two parts to S-boxes.

[53] Subsequently, the operation unit 133 may perform a matrix operation between output result values of the two S-boxes to generate a random value r_i . In this case, various

matrix operations with characteristics for maximizing a diffusion effect on an input value, such as a matrix operation using a maximum distance separable (MDS) matrix, may be used as the matrix operation.

[54] The generation of a dynamic key table performed by the key table generator 130 is not necessarily limited to the examples shown in FIGS. 4 and 5. For example, the key table generator 130 may generate a dynamic key table from authentication information in various methods having a one-way property other than those shown in FIGS. 4 and 5.

[55] Also, according to an embodiment of the present disclosure, the key table generator 130 may additionally use a variety of information shared with the external apparatus other than the authentication information acquired through the authentication process to generate the dynamic key table. As a detailed example, since the external apparatus pre-shares the remaining portion of the cipher algorithm other than the dynamic key table as described above, the key table generator 130 may use a static key table stored in the storage 110 as well as the authentication information shared through the authentication process performed with the external apparatus to generate a dynamic key table.

[56] The encryption/decryption unit 140 performs encryption or decryption using the dynamic key table generated by the key table generator 130 and the static key table stored in the storage 110.

[57] In detail, the encryption/decryption unit 140 may add at least one dynamic key table generated by the key table generator 130 to the remaining portion of the cipher algorithm stored in the storage 110. In this case, a position at which the dynamic key table is applied in the cipher algorithm may be preset by a developer of the cipher algorithm, and the encryption/decryption unit 140 may add the dynamic key table to the remaining portion of the cipher algorithm stored in the storage 110.

[58] In an embodiment, the storage 110, the authenticator 120, the key table

generator 130, and the encryption/decryption unit 140 shown in FIG. 1 may be implemented in at least one computing apparatus including at least one processor and a computer-readable recording medium connected with the processor. The computer-readable recording medium may be disposed inside or outside the processor, and may be connected to the processor using various well-known means. The processor in the computing apparatus may enable the computing apparatus to operate according an example embodiment described in this specification. For example, the processor may execute an instruction stored in the computer-readable recording medium, and the instruction stored in the computer-readable recording medium may be configured to enable the computing apparatus to perform operations according to an example embodiment described in this specification when the instruction is executed by the processor.

[59] FIG. 6 is a block diagram of an encryption apparatus according to an additional embodiment of the present disclosure.

[60] Referring to FIG. 6, an encryption apparatus 600 according to an additional embodiment of the present disclosure includes a storage 110, an authenticator 120, a key table generator 130, an encryption/decryption unit 140, and a key table provider 150.

[61] In the example shown in FIG. 6, the storage 110, the authenticator 120, the key table generator 130, and the encryption/decryption unit 140 have the same configurations as shown in FIG. 1, and thus redundant descriptions thereof will be omitted.

[62] When a dynamic key table is generated by the key table generator 130, the key table provider 150 provides the generated dynamic key table to an external apparatus. In detail, the encryption apparatus 100 and the external apparatus share the same dynamic key table in the embodiment shown in FIG. 1 by using the authentication information shared through the authentication process to generate the dynamic key table, but the encryption apparatus 100 and the external apparatus share the same dynamic key table in the

embodiment shown in FIG. 6 by the key table provider 150 providing the dynamic key table generated by the key table generator 130 to the external apparatus.

[63] In an embodiment, the storage 110, the authenticator 120, the key table generator 130, the encryption/decryption unit 140, and the key table provider 150 shown in FIG. 6 may be implemented in at least one computing apparatus including at least one processor and a computer-readable recording medium connected with the processor. The computer-readable recording medium may be disposed inside or outside the processor, and may be connected with the processor using various well-known means. The processor in the computing apparatus may enable the computing apparatus to operate according an example embodiment described in this specification. For example, the processor may execute an instruction stored in the computer-readable recording medium, and the instruction stored in the computer-readable recording medium may be configured to enable the computing apparatus to perform operations according to an example embodiment described in this specification when the instruction is executed by the processor.

[64] FIG. 7 is a block diagram of an encryption apparatus according to another embodiment of the present disclosure.

[65] Referring to FIG. 7, an encryption apparatus 700 according to an embodiment of the present disclosure includes a storage 710, an authenticator 720, a key table acquirer 730, and an encryption/decryption unit 740.

[66] In the example shown in FIG. 7, the storage 710, the authenticator 720, and the encryption/decryption unit 740 have the same configurations as shown in FIG. 1, and thus redundant descriptions thereof will be omitted.

[67] The key table acquirer 730 acquires at least one dynamic key table from an external apparatus or a key table generation server.

[68] For example, the key table acquirer 730 may receive at least one dynamic key

table generated using authentication information shared through an authentication process with an external apparatus. In this case, the external apparatus may be, for example, the encryption apparatus 600 shown in FIG. 6. Depending on the embodiment, the dynamic key table received from the external apparatus may be generated using a static key table and the authentication information shared through the authentication process.

[69] As another example, the key table acquirer 730 may provide authentication information shared with an external apparatus through the authentication process to a key table generation server. In this case, the key table generation server may generate at least one dynamic key table using the provided authentication information, and the key table acquirer 730 may receive the dynamic key table generated by the key table generation server. Also, the external apparatus may receive the dynamic key table generated by the key table generation server. Accordingly, the external apparatus and the encryption apparatus 700 share the same dynamic key table.

[70] In an embodiment, the storage 710, the authenticator 720, the key table acquirer 730, and the encryption/decryption unit 740 shown in FIG. 7 may be implemented in at least one computing apparatus including at least one processor and a computer-readable recording medium connected with the processor. The computer-readable recording medium may be disposed inside or outside the processor, and may be connected with the processor using various well-known means. The processor in the computing apparatus may enable the computing apparatus to operate according an example embodiment described in this specification. For example, the processor may execute an instruction stored in the computer-readable recording medium, and the instruction stored in the computer-readable recording medium may be configured to enable the computing apparatus to perform operations according to an example embodiment described in this specification when the instruction is executed by the processor.

[71] FIG. 8 is a flowchart of an encryption method according to an embodiment of the present disclosure.

[72] For example, the method shown in FIG. 8 may be performed by the encryption apparatus 100 shown in FIG. 1.

[73] Referring to FIG. 8, first, the encryption apparatus 100 performs authentication with an external apparatus that shares the remaining portion of a cipher algorithm implemented to perform encryption or decryption using at least one static key table and at least one dynamic key table, other than the dynamic key table (810).

[74] In this case, when the authentication is successful (820), the encryption apparatus 100 generates at least one dynamic key table using the authentication information shared with the external apparatus through the authentication (830).

[75] In this case, according to an embodiment, the encryption apparatus 100 may generate the at least one dynamic key table using the shared authentication information and the static key table of the cipher algorithm.

[76] Subsequently, the encryption apparatus 100 adds the generated dynamic key table to the remaining portion of the cipher algorithm (840).

[77] Subsequently, the encryption apparatus 100 performs encryption or decryption using the cipher algorithm to which the dynamic key table is added (850).

[78] FIG. 9 is a flowchart of an encryption method according to an additional embodiment of the present disclosure.

[79] For example, the method shown in FIG. 9 may be performed by the encryption apparatus 600 shown in FIG. 6.

[80] Referring to FIG. 9, first, the encryption apparatus 600 performs authentication with an external apparatus that shares the remaining portion of a cipher algorithm implemented to perform encryption or decryption using at least one static key table

and at least one dynamic key table, other than the dynamic key table (910).

[81] In this case, when the authentication is successful (920), the encryption apparatus 600 generates at least one dynamic key table using the authentication information shared with the external apparatus through the authentication (930).

[82] In this case, according to an embodiment, the encryption apparatus 600 may generate the at least one dynamic key table using the shared authentication information and the static key table of the cipher algorithm.

[83] Subsequently, the encryption apparatus 600 adds the generated dynamic key table to the remaining portion of the cipher algorithm (940).

[84] Subsequently, the encryption apparatus 600 provides the generated dynamic key table to the external apparatus (950).

[85] Subsequently, the encryption apparatus 600 performs encryption or decryption using the cipher algorithm to which the dynamic key table is added (960).

[86] FIG. 10 is a flowchart of an encryption method according to another embodiment of the present disclosure.

[87] For example, the method shown in FIG. 10 may be performed by the encryption apparatus 700 shown in FIG. 7.

[88] Referring to FIG. 10, first, the encryption apparatus 700 performs authentication with an external apparatus that shares the remaining portion of a cipher algorithm implemented to perform encryption or decryption using at least one static key table and at least one dynamic key table, other than the dynamic key table (1010).

[89] In this case, when the authentication is successful (1020), the encryption apparatus 700 receives at least one dynamic key table generated using the authentication information shared through the authentication process from the external apparatus (1030).

[90] In this case, depending on the embodiment, the received dynamic key table

may be generated using the static key table and the shared authentication information.

[91] Subsequently, the encryption apparatus 700 adds the received dynamic key table to the remaining portion of the cipher algorithm (1040).

[92] Subsequently, the encryption apparatus 700 performs encryption or decryption using the cipher algorithm to which the dynamic key table is added (1050).

[93] FIG. 11 is a flowchart of an encryption method according to still another embodiment of the present disclosure.

[94] For example, the method shown in FIG. 11 may be performed by the encryption apparatus 700 shown in FIG. 7.

[95] Referring to FIG. 11, first, the encryption apparatus 700 performs authentication with an external apparatus that shares the remaining portion of a cipher algorithm implemented to perform encryption or decryption using at least one static key table and at least one dynamic key table, other than the dynamic key table (1110).

[96] In this case, when the authentication is successful (1120), the encryption apparatus 700 provides authentication information shared with the external apparatus through the authentication process to the key table generation server (1130).

[97] Subsequently, the encryption apparatus 700 receives at least one dynamic key table generated using the authentication information from the key table generation server (1140).

[98] Subsequently, the encryption apparatus 700 adds the received dynamic key table to the remaining portion of the cipher algorithm (1150).

[99] Subsequently, the encryption apparatus 700 performs encryption or encryption using the cipher algorithm to which the dynamic key table is added (1160).

[100] In the flowcharts shown in FIGS. 8 to 11, the methods have been described as having a plurality of steps. However, at least some of the steps may be performed in a

changed order, performed in combination with another step, omitted, divided into sub-steps, or performed in addition to one or more steps that are not shown.

[101] Embodiments of the present disclosure may include a computer-readable recording medium including a program for executing the methods described herein on a computer. The computer-readable recording medium may include any one or a combination of a program instruction, a local data file, a local data structure, etc. The medium may be designed and configured specifically for the present disclosure or can be typically available in the field of computer software. Examples of the computer-readable recording medium include a magnetic medium, such as a hard disk, a floppy disk, and a magnetic tape, an optical recording medium, such as a CD-ROM and a DVD, a magneto-optical medium, such as a floptical disk, and a hardware device specially configured to store and perform a program instruction, such as a ROM, a RAM, and a flash memory. Examples of the program instruction may include a machine code generated by a compiler and a high-level language code that can be executed in a computer using an interpreter.

[102] According to embodiments of the present disclosure, by sharing only a portion of an implementation of a cipher algorithm, instead of sharing the entire implementation of the cipher algorithm, and then generating the remaining portion through authentication when an encryption/decryption service is applied to share the generated portion, it is possible to prevent use of an unauthorized user and enhance safety in various embodiments including an Internet of things (IoT) that is vulnerable to an attack such as an attack for stealing an algorithm.

[103] Although example embodiments of the present disclosure have been described in detail, it will be understood by those skilled in the art that various changes may be made without departing from the spirit or scope of the present disclosure. Thus, the scope of the present disclosure is to be determined by the following claims and their equivalents, and shall

not be restricted or limited by the foregoing detailed description.

WHAT IS CLAIMED IS:

1. An encryption apparatus comprising:
a storage configured to store at least one static key table;
an authenticator configured to perform authentication with an external apparatus;
and
a key table generator configured to generate at least one dynamic key table using the at least one static key table and authentication information acquired through the authentication,
wherein each of the at least one static key table and at least one dynamic key table is a lookup table.

2. The encryption apparatus of claim 1, further comprising a key table provider configured to provide the at least one dynamic key table to the external apparatus.

3. The encryption apparatus of claim 1, further comprising an encryption/decryption unit configured to perform encryption or decryption using the at least one static key table and the at least one dynamic key table.

4. An encryption apparatus comprising:
a storage configured to store at least one static key table;
an authenticator configured to perform authentication with an external apparatus;
and

a key table acquirer configured to transmit authentication information acquired through the authentication to a key table generation server and receive, from the key table generation server, at least one dynamic key table generated using at least one static key table stored in the key table generation server and the transmitted authentication information,

wherein each of the at least one static key table and at least one dynamic key table is a lookup table.

5. The encryption apparatus of claim 4, further comprising an encryption/decryption unit configured to perform encryption or decryption using the at least one static key table stored in the storage and the at least one dynamic key table.

6. An encryption apparatus comprising:

a storage configured to store at least one static key table;

an authenticator configured to perform authentication with an external apparatus;

and

a key table acquirer configured to acquire, from the external apparatus, at least one dynamic key table generated using at least one static key table stored in the external apparatus and authentication information acquired through the authentication,

wherein each of the at least one static key table and at least one dynamic key table is a lookup table.

7. The encryption apparatus of claim 6, further comprising an encryption/decryption unit configured to perform encryption or decryption using the at least one static key table stored in the storage and the at least one dynamic key table.

8. An encryption method comprising:
storing at least one static key table;
performing authentication with an external apparatus; and
generating at least one dynamic key table using the at least one static key table and authentication information acquired through the authentication,
wherein each of the at least one static key table and at least one dynamic key table is a lookup table.

9. The encryption method of claim 8, further comprising providing the at least one dynamic key table to the external apparatus.

10. The encryption method of claim 8, further comprising performing encryption or decryption using the at least one static key table and the at least one dynamic key table.

11. An encryption method comprising:
storing at least one static key table;
performing authentication with an external apparatus;

transmitting authentication information acquired through the authentication to a key table generation server; and

receiving, from the key table generation server, at least one dynamic key table generated using at least one static key table stored in the key table generation server and the transmitted authentication information,

wherein each of the at least one static key table and at least one dynamic key table is a lookup table.

12. The encryption method of claim 11, further comprising performing encryption or decryption using the at least one static key table stored in the storing step.

13. An encryption method comprising:

storing at least one static key table;

performing authentication with an external apparatus; and

acquiring, from the external apparatus, at least one dynamic key table generated using at least one static key table stored in the external apparatus and authentication information acquired through the authentication,

wherein each of the at least one static key table and at least one dynamic key table is a lookup table.

14. The encryption method of claim 13, further comprising performing encryption or decryption using the at least one static key table stored in the storing step and the at least one dynamic key table.