

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
28 September 2006 (28.09.2006)

PCT

(10) International Publication Number
WO 2006/102003 A2

(51) International Patent Classification:
G06F 21/20 (2006.01)

(21) International Application Number:
PCT/US2006/009567

(22) International Filing Date: 16 March 2006 (16.03.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/662,269 16 March 2005 (16.03.2005) US

(71) Applicant (for all designated States except US): **THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK** [US/US]; 412 Low Memorial Library, 535 West 116th Street, New York, New York 10027 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **COOK, Debra, L.** [US/US]; 52 Society Hill Way, Tinton Falls, New Jersey 07724 (US). **YUNG, Marcel, Mordechay** [IL/US]; 750 Columbus Avenue, 4h, New York, New York 10025 (US). **KEROMYTIS, Angelos, D.** [GR/US]; 423 West 120th Street, #102, New York, New York 10027 (US).

(74) Agents: **BYRNE, Matthew, T.** et al.; Wilmer Cutler Pickering Hale And Dorr LLP, 399 Park Avenue, New York, New York 10022 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

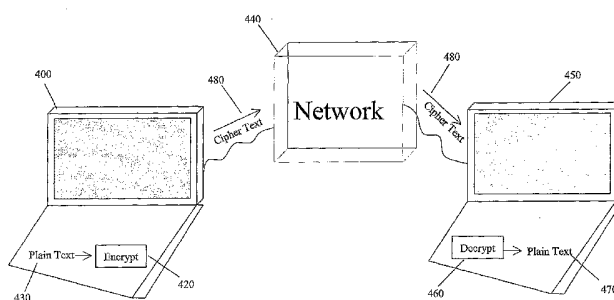
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEMS AND METHODS FOR PERFORMING DOUBLE ENCRYPTION TO INHIBIT MEET-IN-THE-MIDDLE ATTACKS



(57) Abstract: Methods and systems are provided for the encryption of data. In one embodiment, the invention provides a method for performing double encryption and applying whitening while providing a key length of at least $2n$ where the key of the original cipher is n bits. This is provided in a way that requires less work than three applications of the cipher and avoids a meet-in-the-middle attack to which double encryption by itself would be subject.

WO 2006/102003 A2

SYSTEMS AND METHODS FOR PERFORMING DOUBLE ENCRYPTION TO INHIBIT MEET-IN-THE-MIDDLE ATTACKS

Cross-Reference to Related Application

[0001] This application claims the benefit under 35 U.S.C. §119(e) of United States Provisional Patent Application No. 60/662,269, filed March 16, 2005, which is hereby incorporated by reference herein in its entirety.

Field of the Invention

[0002] The present invention relates to the field of encryption. More particularly, this invention relates to increasing the security of encryption while reducing the time required to obtain that security.

Background of the Invention

[0003] Due to the ubiquity of information exchange on the Internet and other computer platforms, it is important to have access to methods of securely transmitting information from one party to another and keeping private information unreadable to all but the those who should be granted rightful access. Encryption is the process of obscuring information to make it unreadable without special knowledge. The data to be encrypted is referred to as plaintext, the encrypted form is referred to as ciphertext, and the secret information used to encrypt the plaintext is known as a key. A simple illustration of encrypting plaintext to ciphertext with a key can be seen FIG. 1. Plaintext **110** is encrypted with a cipher **120** using a key **130** to produce ciphertext **140**. FIG. 2 shows a decryption of ciphertext to plaintext with a key. Ciphertext **210** is decrypted with a cipher **220** using a key **230** to produce plaintext **240**.

[0004] The notation below will be used through out this description:

- $k, k_i, K, \text{ and } K_i$ denote keys, where i is an integer;
- E_k denotes encryption using key k ;
- D_k denotes decryption using key k ;
- P and P_i denote plaintext, where i is an integer;
- C and C_i denotes ciphertext, where i is an integer;

- $H(x)$ denotes a hash of x ;
- whitening is the process of adding some confusion to data;
- whitening may be performed, for example, by exclusive-oring the data with a string of bits generated by a pseudo-random function or a hash function;
- W_k consists of whitening key bits dependent on key k ;
- n denotes the length of a key; and
- the symbol $\oplus$ is used to denote the exclusive-or operation (XOR).

[0005] DES (Data Encryption Standard) is a widely used cipher that employs the DEA (Data Encryption Algorithm) for encrypting information. DES is now considered to be insecure for many applications especially as some modern computers are able to decrypt data encrypted with DES in a matter of hours. As such, enhancements and alternatives are needed.

[0006] Double encryption refers to using two independent keys to encrypt P twice. This may be represented in equation form as $C = E_{k2}(E_{k1}(P))$. Use of double encryption was intended to provide double the security because an exhaustive search of all possible combinations of keys of length n would take 2^{2n} attempts, compared to the 2^n attempts required to break a single encryption.

[0007] However, double encryption alone has long been known to provide little additional security over a single application of a cipher due to its susceptibility to a meet-in-the-middle attack. Given a double encryption, $C = E_{k2}(E_{k1}(P))$, an attacker can compute and store $E_{ki}(P)$ and $D_{kj}(C)$ for all possible keys to find a ki, kj for which $E_{ki}(P) = D_{kj}(C)$. When searching for a match, 2^n memory locations are required to store the values $E_{ki}(P)$ or $D_{kj}(P)$ for every possible key. Upon finding this match, the attacker can then verify it with a second set of P and C . This attack requires only 2^{n+1} attempts for encrypting and decrypting with all 2^n possible keys, and thus double encryption alone is not worth the time needed to perform the second encryption.

[0008] 3DES (Triple DES) is encryption that may be represented by $C = E_{k3}(D_{k2}(E_{k1}(P)))$. Even with a meet in the middle attack, 3DES requires 2^{2n} attempts for an attacker because all possible combinations of $(k1, k2)$ must be tried. However, 3DES requires a large amount of work for encryption and decryption and thus can be too slow in many situations.

[0009] Advance Encryption Standard (AES) is a newer cipher that has, in addition to other differences, a larger block and key size than DES. While this standard offers greater protection over DES, it is not yet implemented everywhere. Further, it is likely that as computer speeds increase, brute force attacks will become practical against AES encrypted data.

[0010] It has been proposed to add initial and final whitening as a way of requiring less work than 3DES while providing a longer key. This construction can be written generically as $C = K_2 \oplus E_k(K_1 \oplus P)$. DESX is the name given to this construction when applied to DES. In DESX, K_1 and K_2 are each 64 bits and k is 56 bits, thus requiring a 184 bit key ($64 + 64 + 56$). As a result of the longer key length compared to the original cipher, this construction increases the security of the cipher against an exhaustive key search without requiring multiple applications of the cipher.

[0011] Further analysis of $C = K_2 \oplus E_k(K_1 \oplus P)$ has demonstrated that without the initial whitening, i.e., $C = K_2 \oplus E_k(P)$, extra security against an exhaustive key search is not provided because $K_2 = C \oplus E_k(P)$. Using two or more known plaintext ciphertext pairs, an attacker can compute $C \oplus E_k(P)$ for each pair and for each k . When the correct k is used, the pairs will produce the same value for K_2 . Additional pairs can be tested to verify the key is correct. This version of DES with only the final whitening was referred to as DESW.

[0012] Therefore, it would be of great benefit to make existing encryption algorithms more secure without having to incur the extra time needed to perform two encryptions.

Summary of the Invention

[0013] Methods and systems are provided for the encryption of data. In some embodiments, methods and systems are provided for encrypting plaintext wherein the plaintext is encrypted with a first key, encrypted with a second key, and then exclusive-ored with a whitening of a third key to produce ciphertext.

[0014] In other embodiments, methods and systems for decrypting ciphertext are provided wherein the ciphertext is exclusive-ored with a whitening of a third key, decrypted with a second key, and then decrypted with a first key to produce plaintext.

[0015] In still other embodiments, methods and systems are provided for encrypting plaintext wherein the plaintext is exclusive-ored with a whitening of a third key, encrypted with a first key, and then encrypted with a second key to produce ciphertext.

[0016] In yet other embodiments, methods and systems for decrypting ciphertext are provided wherein the ciphertext is decrypted with a second key, decrypted with a first key, and then exclusive-ored with a whitening of a third key to produce plaintext.

Brief Description of the Drawings

[0017] The above and other advantages of the present invention will be apparent upon consideration of the following detailed description, taken in conjunction with accompanying drawings, in which like reference characters refer to like parts throughout, and in which:

[0018] FIG. 1 is a simplified illustration of data being encrypted;

[0019] FIG. 2 is a simplified illustration of data being decrypted;

[0020] FIG. 3 is a simplified illustration of a method for encrypting data in accordance with certain embodiments of the present invention;

[0021] FIG. 4 is a simplified illustration of a system that may be used in accordance with certain embodiments of the present invention; and

[0022] FIG. 5 is a simplified illustration of a method for decrypting ciphertext in accordance with certain embodiments of the present invention.

Detailed Description of the Invention

[0023] Methods and systems are provided for the encryption of data. In some embodiments, methods and systems are provided for performing double encryption along with whitening. This is provided in a way that requires less work than triple encryption and avoids a meet-in-the-middle attack to which double encryption alone would be subject. Embodiments of this invention apply not only to, for example, DES and AES, but apply equally well to any encryption cipher.

[0024] In some embodiments, methods and systems are provided for encrypting plaintext wherein the plaintext is encrypted with a first key, encrypted with a second key, and then exclusive-ored with a whitening of a third key to produce ciphertext. In other embodiments, methods and systems for decrypting ciphertext are provided wherein the ciphertext is exclusive-ored with a whitening of a third key, decrypted with a second key, and

then decrypted with a first key to produce plaintext. In still other embodiments, methods and systems are provided for encrypting plaintext wherein the plaintext is exclusive-ored with a whitening of a third key, encrypted with a first key, and then encrypted with a second key to produce ciphertext. In yet other embodiments, methods and systems for decrypting ciphertext are provided wherein the ciphertext is decrypted with a second key, decrypted with a first key, and then exclusive-ored with a whitening of a third key to produce plaintext. For reasons of clarity and consistency, the third key in this description is used in the whitening while the first and second key are used for both encryption and decryption. However, embodiments of the systems and methods of this invention can be practiced with any numbering scheme for the keys.

[0025] In one embodiment, the present invention adds a hash of key material to double encryption:

$$(I) \quad C = H(k1||k2) \oplus E_{k2}(E_{k1}(P)).$$

More generally,

$$(II) \quad C = W_{k3} \oplus E_{k2}(E_{k1}(P))$$

where W_{k3} is whitening based on the key $k3$.

[0026] A simple illustration of equation II can be seen in FIG. 3. Starting with plaintext 310, the first step is to encrypt the data with $k1$ at step 320. The result of that first encryption is then encrypted with $k2$ at step 330. The final step 340 is to XOR the whitening based on $k3$ with the result of the second encryption to produce the ciphertext 350.

[0027] Some embodiments of the present invention may be used to send data over a network as demonstrated in FIG. 4. As shown, plaintext 430 residing on a system 400 comprising a processor may be encrypted 420 using one embodiment of the present invention. The created ciphertext 480 may then be sent over a network 440 to another system 450. That system may then decrypt 460 the ciphertext using an embodiment of the present invention to produce the plaintext 470, which is the same as the plaintext 430 that was originally encrypted. Other embodiments may encrypt data to be stored on media, memory, or any other suitable storage or transfer mechanism. The systems referenced by 400 and 450 may be, for example, laptop computers, mobile phones, personal digital assistants, or any type of device capable of using the underlying cipher for encryption or decryption. Furthermore, they do not have to be the same type of system. Also, the systems may share the first key, second key, and third key using methods known in the art.

[0028] Regardless of whether the whitening is the output of a hash function or some other function, it is preferably computed once during the key expansion and not per plaintext, i.e., the same whitening is preferably used for each plaintext throughout the encryption. However, the whitening of k_3 may be performed either before or after performing the double encryption. The key, k_3 , can either be a combination of k_1 and k_2 , or a third key of length $\geq n$. A block length, b , greater than or equal to n is assumed ($b \geq n$). Both options result in the attacker having to try 2^{2n} key combinations instead of only 2^n combinations. The generic construction is analyzed below and one possible hash for whitening is suggested.

[0029] The following assumptions are made in this discussion:

- W_{k_3} is the output of a pseudo-random function (PRF) acting on input k_3 ;
- W_{k_3} is not part of the key schedule of the block cipher;
- W_{k_3} is independent of the plaintext;
- $|k_3| \geq |k_1|$ and $|k_1| = |k_2| = n$; and

[0030] It should be considered that the placement of the XOR is relevant, as demonstrated in the following equation: $C = E_{k_2}(W_{k_3} \oplus E_{k_1}(P))$. Adding the hash between the two encryptions provides no benefit because a meet-in-the-middle attack using pairs of plaintext and ciphertext is possible. Given plaintext and ciphertext (P_1, C_1) and (P_2, C_2), for each k_1 , an attacker could encrypt P_1 and P_2 then XOR the resulting ciphertext, or similarly, for each k_2 , decrypt C_1 and C_2 then XOR the resulting plaintext. Then the attacker could check for which (k_1, k_2) the two results match and thus achieve a meet-in-the-middle attack. This, specifically, can be seen in the following equation:

$$D_{k_2}(C_1) \oplus D_{k_2}(C_2) = W_{k_3} \oplus E_{k_1}(P_1) \oplus W_{k_3} \oplus E_{k_1}(P_2) = E_{k_1}(P_1) \oplus E_{k_1}(P_2)$$

[0031] The analysis of equation II applies regardless of whether the whitening is added before or after the double encryption. That is, the encryption may also be performed by first XORing a whitening of a third key with the plaintext and then performing the double encryption on that result as demonstrated in the following equation: $C = E_{k_2}(E_{k_1}(W_{k_3} \oplus P))$. Without loss of generality, the construction is analyzed with the whitening at the end, as shown in equation II. When the whitening is added after both encryptions, an exhaustive key search requires 2^{2n} attempts. Attempting to find the keys by applying two encryptions and then applying the whitening directly will require trying keys of length $2n$ (combinations of k_1 and k_2). Given known plaintext and ciphertext (P, C) pairs, by encrypting pairs of plaintexts

with each (k_1, k_2) guess, the resulting ciphertexts can be XORed and matched against the XOR of the known ciphertexts to determine if the guess is correct. Once k_1 and k_2 are known, if (P_1, C_1) are also known, the whitening can be determined by computing $E_{k_2}(E_{k_1}(P_1)) \oplus C_1$. Specifically, encrypting plaintexts P_1 and P_2 results in:

$$C_1 \oplus W_{k_3} = E_{k_2}(E_{k_1}(P_1)) \text{ and } C_2 \oplus W_{k_3} = E_{k_2}(E_{k_1}(P_2)).$$

Therefore, $C_1 \oplus C_2 = E_{k_2}(E_{k_1}(P_1)) \oplus E_{k_2}(E_{k_1}(P_2))$.

[0032] A meet-in-the-middle attack also requires finding 2^n key bits. The goal of an attacker is to find keys such that $D_{k_2}(C \oplus W_{k_3}) = E_{k_1}(P)$. To do this, both $D_{k_2}(C \oplus W_{k_3})$ and $E_{k_1}(P)$ must be computed. The whitening bits must be guessed in order to decrypt. Since W_{k_3} is unknown, the minimum work required to undo the whitening is the minimum of 2^b and $2^{|k_3|}$. Every possible k_2 must be tried with every possible W_{k_3} when performing a meet-in-the-middle attack. If $k_3 = k_1 || k_2$, then there are 2^{2n} possible (k_2, k_3) combinations. If k_3 is independent of k_1 and k_2 then, since both b and $|k_3|$ are greater than n , there are at least 2^{2n} combinations to test. The whitening is independent of the cipher's key schedule so an attacker cannot try all possible k_1 or k_2 values and have the whitening included in the expanded key bits.

[0033] If the cipher includes whitening as its last step, or if the whitening is performed before the two encryptions, then, in theory, there may exist a k_4 that produces the same expanded key bits as k_2 except that the final whitening corresponds to the final whitening of the cipher XORed with W_{k_3} . If this occurs, an attacker can ignore W_{k_3} completely and use a meet-in-the-middle attack to find k_1 and k_4 . This is the same scenario that was described for the equation $C = K_2 \oplus E_k(K_1 \oplus P)$. However, assuming the key schedule is well designed, it would be unlikely that changing any number of bits in the key would impact only a subset of the expanded key bits.

[0034] In another embodiment of this invention, ciphertext can be decrypted. This can be seen by manipulating encryption equations I and II:

$$C \oplus H(k_1 || k_2) = E_{k_2}(E_{k_1}(P)), \text{ and}$$

$$C \oplus W_{k_3} = E_{k_2}(E_{k_1}(P))$$

where W_{k_3} is whitening based on the key k_3 . Therefore,

$$P = D_{k_1}(D_{k_2}(C \oplus W_{k_3}) = D_{k_1}(D_{k_2}(E_{k_2}(E_{k_1}(P))))).$$

[0035] A simple illustration of decryption according to an embodiment of the present invention can be seen in FIG. 5. To decrypt the ciphertext 510, one may first XOR the whitening of a third key with the ciphertext at step 520. The result of that operation may then be decrypted with the second key at step 530. The final step is to decrypt the results of the previous step with the first key at step 540 to produce the plaintext 550. The embodiment used for decryption of the ciphertext depends on whether the whitening of the third key was XORed with the plaintext or if it was XORed with the doubly encrypted data. Accordingly, in some embodiments of the present invention decryption may be performed by first doubly decrypting the ciphertext with a second and first key and then XORing the result with the whitening of a third key. The same details discussed for possible embodiments of methods and systems for encryption also apply to methods and systems for decryption.

[0036] This invention improves a double encryption's resistance to attacks. It relies on the used block cipher having a sufficient level of resistance to attacks aside from an exhaustive key search. This invention provides a way that a double application of DES with a final whitening can be used to achieve the same purpose of 3DES while requiring fewer computations than 3DES. In implementations of 3DES, the initial and final permutations are not required between each pair of applications because sequential applications of DES result in pairs of the permutations that merely undo each other. Likewise, in 2DES, the final permutation of the first encryption and the initial permutation of the second encryption are omitted. Therefore, 2DES with a final whitening step offers a savings over 3DES by eliminating one application of DES minus the initial permutation while adding only the cost of the XOR required for the whitening.

[0037] Although the invention has been described and illustrated in the foregoing illustrative embodiments, it is understood that the present disclosure has been made only by way of example, and that numerous changes in the details of implementation of the invention can be made without departing from the spirit and scope of the invention. For example, although the example underlying encryption used was DES, the invention is not limited in this manner. Rather, according to various embodiments of the present invention, different methods of encryption can be used.

[0038] Therefore, other embodiments, extensions, and modifications of the ideas presented above are comprehended and should be within the reach of one versed in the art upon reviewing the present disclosure. Accordingly, the scope of the present invention in its

various aspects should not be limited by the examples presented above. The individual aspects of the present invention, and the entirety of the invention should be regarded so as to allow for such design modifications and future developments within the scope of the present disclosure. The present invention is limited only by the claims that follow.

Claims

What is claimed is:

1. A method for encrypting data using a first key, a second key, and a third key, comprising:
encrypting the data with the first key to produce a first encryption;
encrypting the first encryption with the second key to produce a second encryption;
and
performing an exclusive-or of a whitening of the third key and the second encryption to produce ciphertext.
2. The method of claim 1, wherein at least one of the first encryption and the second encryption use the Data Encryption Algorithm (DEA) of the Data Encryption Standard (DES).
3. The method of claim 1, wherein the third key is a combination of the first key and the second key.
4. The method of claim 1, wherein the whitening is the output of a pseudo-random function.
5. The method of claim 1, wherein the whitening is the output of a hash function.
6. A method for encrypting data using a first key, a second key, and a third key, comprising:
performing an exclusive-or of a whitening of the third key and the data to produce a first result;
encrypting the first result with the first key to produce a first encryption; and
encrypting the first encryption with the second key to produce ciphertext.

7. The method of claim 6, wherein at least one of the first encryption and the second encryption use the Data Encryption Algorithm (DEA) of the Data Encryption Standard (DES).
8. The method of claim 6, wherein the third key is a combination of the first key and the second key.
9. The method of claim 6, wherein the whitening is the output of a pseudo-random function.
10. The method of claim 6, wherein the whitening is the output of a hash function.
11. A method for decrypting ciphertext using a first key, a second key, and a third key, comprising:
 - performing an exclusive-or of a whitening of the third key and the ciphertext to produce a first result;
 - decrypting the first result with the second key to produce a second result; and
 - decrypting the second result with the first key.
12. The method of claim 11, wherein at least one of the first decryption and the second decryption use the Data Encryption Algorithm (DEA) of the Data Encryption Standard (DES).
13. The method of claim 11, wherein the third key is a combination of the first key and the second key.
14. The method of claim 11, wherein the whitening is the output of a pseudo-random function.
15. The method of claim 11, wherein the whitening is the output of a hash function.

16. A method for decrypting ciphertext using a first key, a second key, and a third key, comprising:

decrypting the ciphertext with the second key to produce a first result;
decrypting the first result with the first key to produce a second result; and
performing an exclusive-or of a whitening of the third key and the second result.

17. The method of claim 16, wherein at least one of the first decryption and the second decryption use the Data Encryption Algorithm (DEA) of the Data Encryption Standard (DES).

18. The method of claim 16, wherein the third key is a combination of the first key and the second key.

19. The method of claim 16, wherein the whitening is the output of a pseudo-random function.

20. The method of claim 16, wherein the whitening is the output of a hash function.

21. A device comprising a processor, including a first key, a second key, and a third key, that:

encrypts data with the first key to produce a first encryption;
encrypts the first encryption with the second key to produce a second encryption; and
performs an exclusive-or of a whitening of the third key and the second encryption to produce ciphertext.

22. The device of claim 21, wherein at least one of the first encryption and the second encryption use the Data Encryption Algorithm (DEA) of the Data Encryption Standard (DES).

23. The device of claim 21, wherein the third key is a combination of the first key and the second key.

24. The device of claim 21, wherein the whitening is the output of a pseudo-random function.
25. The device of claim 21, wherein the whitening is the output of a hash function.
26. A device comprising a processor, including a first key, a second key, and a third key, that:
performs an exclusive-or of a whitening of the third key and the data to produce a first result;
encrypts the first result with the first key to produce a first encryption; and
encrypts the first encryption with the second key to produce ciphertext.
27. The device of claim 26, wherein at least one of the first encryption and the second encryption use the Data Encryption Algorithm (DEA) of the Data Encryption Standard (DES).
28. The device of claim 26, wherein the third key is a combination of the first key and the second key.
29. The device of claim 26, wherein the whitening is the output of a pseudo-random function.
30. The device of claim 26, wherein the whitening is the output of a hash function.

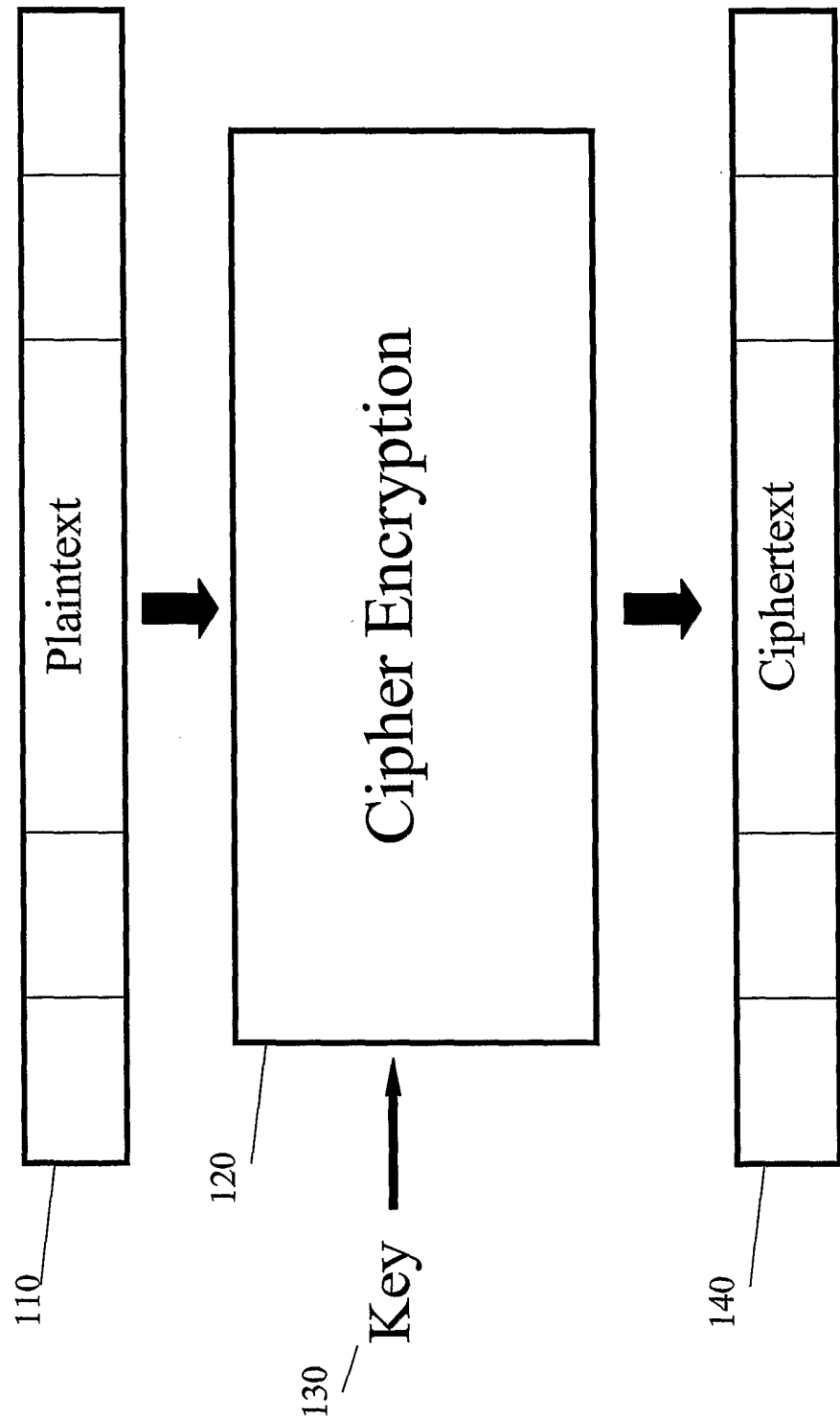


FIG. 1
(PRIOR ART)

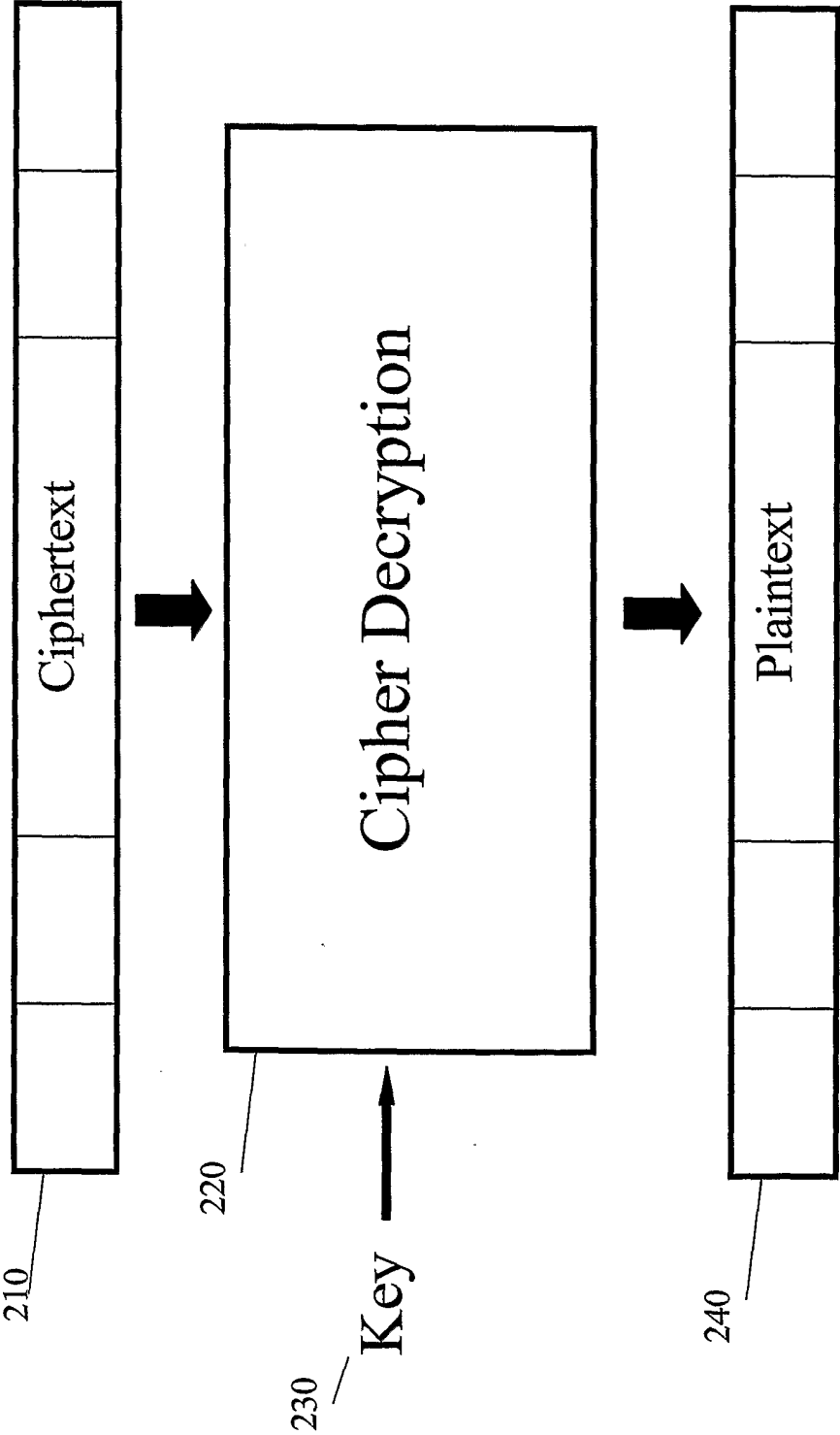


FIG. 2
(PRIOR ART)

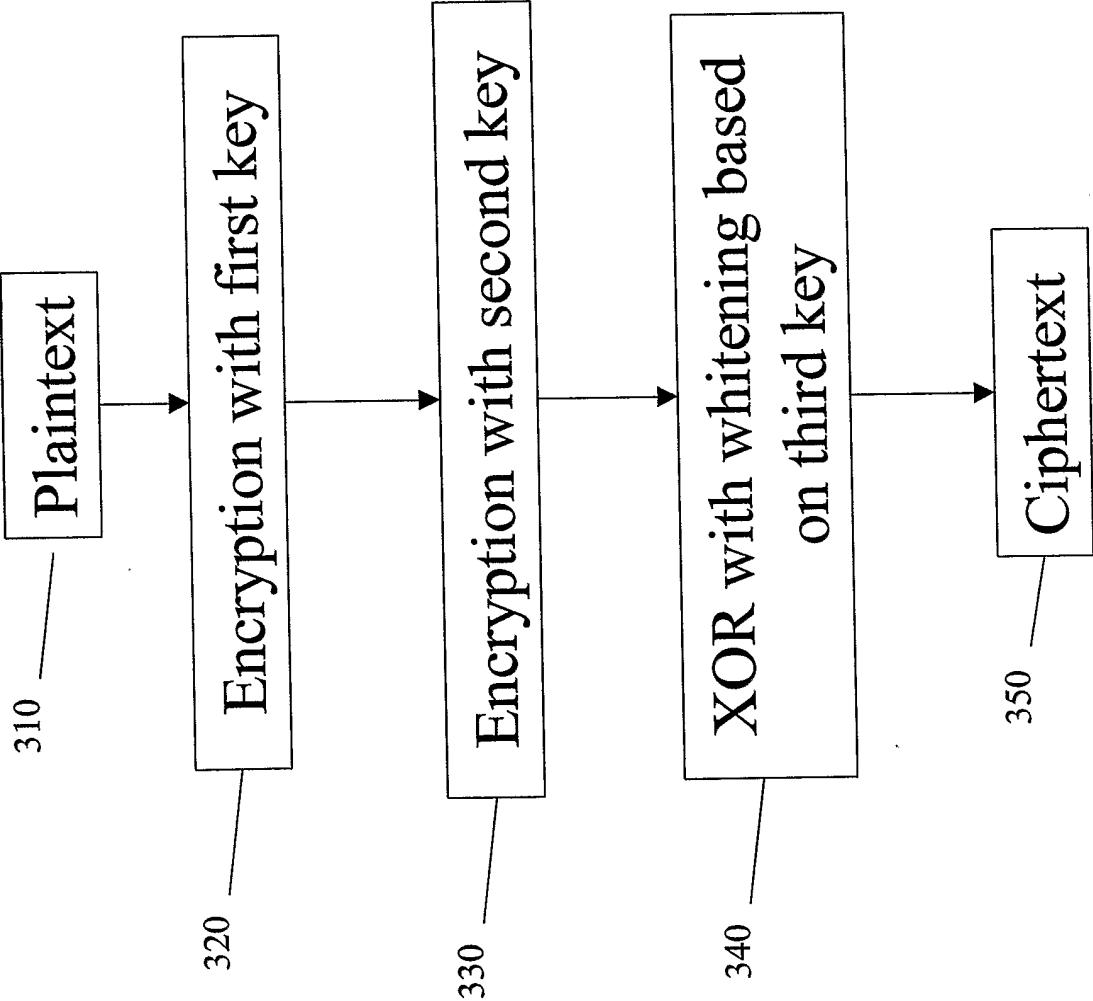


FIG. 3

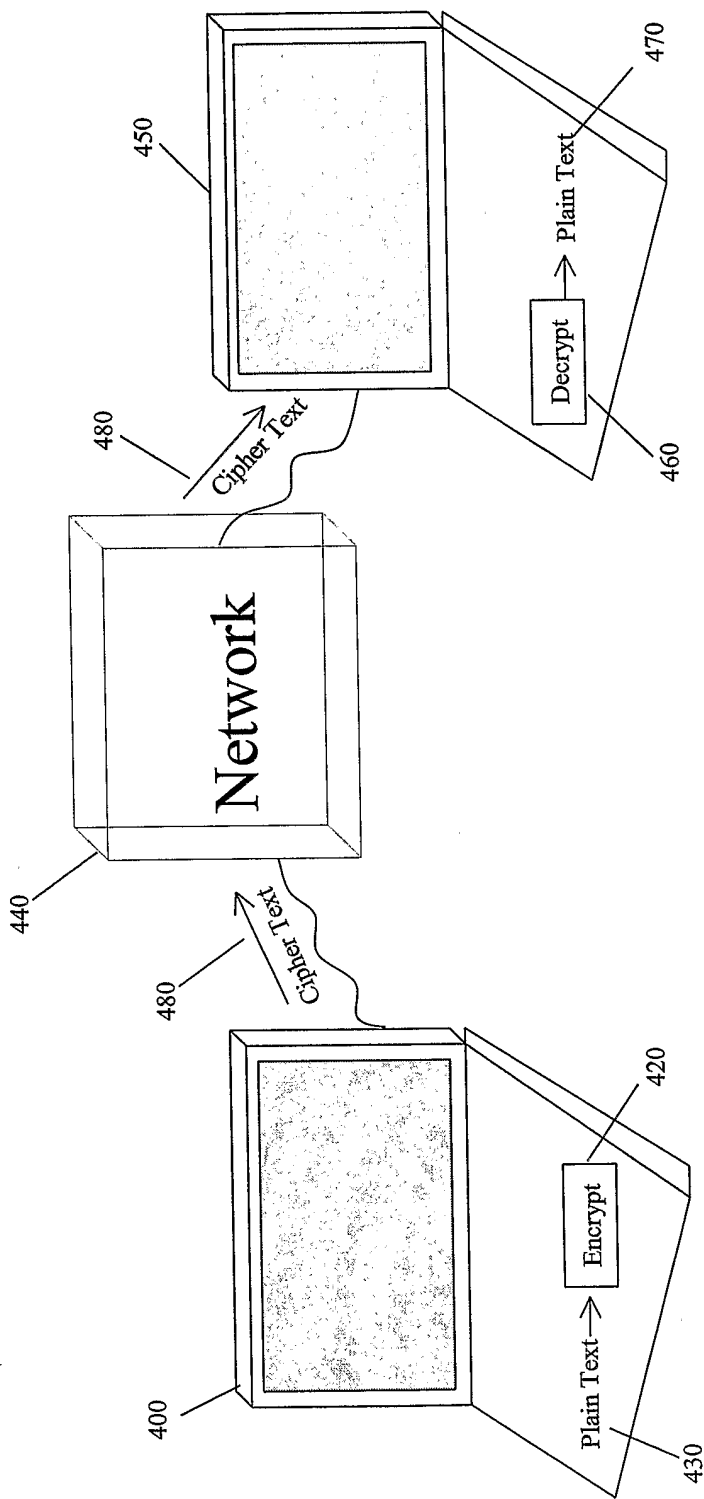


FIG. 4

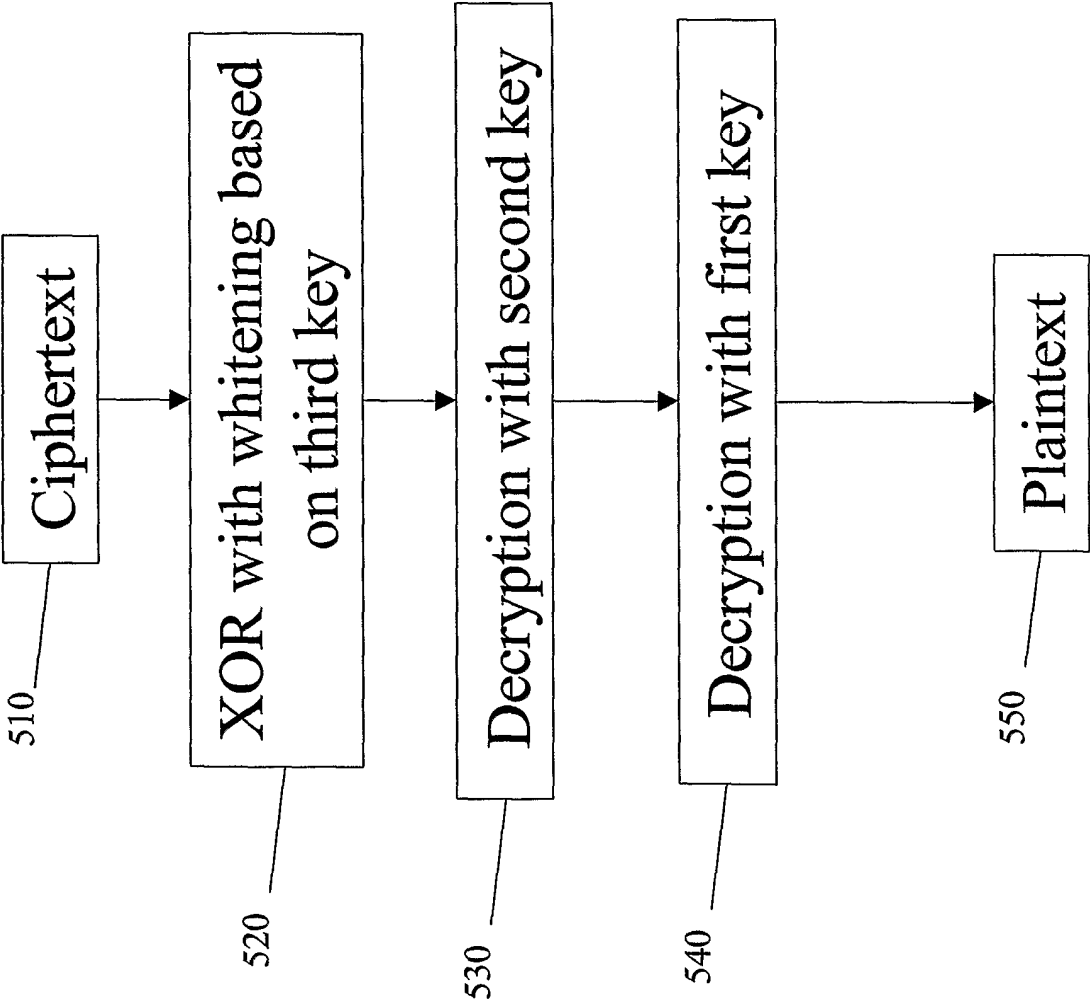


FIG. 5