(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 August 2001 (30.08.2001)

PCT

(10) International Publication Number
WO 01/63831 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US01/06127

(22) International Filing Date: 26 February 2001 (26.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/184,785 24 February 2000 (24.02.2000) US

(71) Applicant: VALICERT CORPORATION [US/US]; 339 N. Bernardo Avenue, Mountain View, CA 94043 (US).

(72) Inventor: JEVANS, David; 530 Menlo Oaks Drive, Menlo Park, CA 94025 (US).

(74) Agent: WOLFELD, Warren, S.; Haynes & Beffel LLP, P.O. Box 366, Half Moon Bay, CA 94019 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

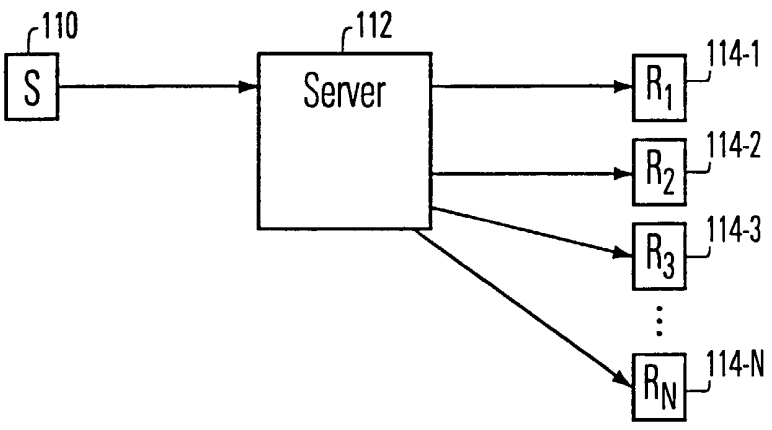
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search 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.

WO 01/63831 A1

(54) Title: MECHANISM FOR EFFICIENT PRIVATE BULK MESSAGING



(57) Abstract: Secure bulk messaging mechanism in which, roughly described, a sender first encrypts a message once. The message can be decrypted with a message decryption key. These can be symmetric or asymmetric keys. For each recipient, the sender (110) then encrypts the message decryption key with the recipient's public key. The sender then sends the encrypted message and the encrypted message decryption keys to a store-and-forward server (112). Subsequently, one or more recipients (114) connect to the server and retrieve the encrypted message and the message encryption key that has been encrypted with the recipient's public key. Alternatively, the server can forward these items to each individual recipient. The recipient then decrypts the encrypted message decryption key with the recipient's private key, resulting in an un-encrypted message decryption key. The recipient then decrypts the message using the message using the un-encrypted message decryption key.

MECHANISM FOR EFFICIENT PRIVATE BULK MESSAGING

[0001] This application claims priority to U.S. Provisional Application Serial No. 60/184,785, filed February 24, 2000, Attorney Docket No. DIFF-01005US0, which is co-pending and incorporated by reference herein.

BACKGROUND

1. Field of the Invention

[0002] The invention relates to secure transmission of documents, and more particularly, to transmission of documents to a large number of recipients, securely and efficiently.

2. Description of Related Art

[0003] The Internet and corporate networks have made the transmission of documents and messages via e-mail commonplace. Bulk messaging has also become commonplace, such as for advertising and promotional purposes. For bulk messaging, typically a user on one computer composes a message and addresses it to an e-mail group. The message is transmitted to a server, which substitutes the individual addresses of all the target recipients in the group, which may number in the thousands, and transmits the message individually to each target recipient.

[0004] Unlike advertising and promotional uses, many businesses require that their communications take place securely. When messages are to be transmitted across an insecure network, such as the Internet, security is typically accomplished by encrypting the message in a manner that can be decrypted only with knowledge of a decryption key. Since only the intended recipient is expected to have the decryption key, only that recipient will be able to open the message and view its contents. Encryption may be performed using a symmetrical encryption algorithm, in which the encryption key matches the decryption key, or by an asymmetric algorithm, in which the encryption key is

different from the decryption key. One popular form of asymmetric encryption is public/private key encryption, described in "Public-key Cryptography Standards," *RSA Data Security, Inc.* (1991), and in Rivest U.S. Patent No. 4,405,829, both incorporated by reference herein.

[0005] According to the public/private key cryptosystem, each target recipient has both a private key that only the recipient knows, and a public key that is publicly available. When a sender desires to send a message securely to one of the target recipients, the sender encrypts the message using the target recipient's public key. Only the target recipient then is able to open the message and view its contents.

[0006] Secure messaging becomes problematical when the sender desires to send the message to a large number of target recipients. If a public/private key cryptosystem is to be used, then the sender must encrypt the message N times, once using the public key of each of the N target recipients, and then send the message separately to each of the target recipients. If the document to be transmitted is large, and/or if N is in the thousands, this can be a formidable task. The encryption part of the task can be minimized if all of the target recipients share a single decryption key, because then the sender need encrypt the message only once. But the need for all recipients to have the decryption key poses risks both in the transmission and in the storage of the key. This solution also does not overcome the need for the sender to transmit the message separately, once to each of the N target recipients.

[0007] Accordingly, there is a need for a more efficient mechanism for secure bulk transmission of messages.

SUMMARY OF THE INVENTION

[0008] According to the invention, roughly described, a sender first encrypts the message once. The message can be decrypted with a message decryption key. These can be symmetric or asymmetric keys. For each recipient, the sender then encrypts the message decryption key with the recipient's public key. The sender

then sends the encrypted message and the encrypted message decryption keys to a store-and-forward server. Subsequently, one or more recipients connect to the server and retrieve the encrypted message and the message encryption key that has been encrypted with the recipient's public key. Alternatively, the server can forward these items to each individual recipient. The recipient then decrypts the encrypted message decryption key with the recipient's private key, resulting in an un-encrypted message decryption key. The recipient then decrypts the message using the un-encrypted message decryption key.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The invention will be described with respect to particular embodiments thereof, and reference will be made to the drawings, in which:

[0010] Fig. 1 is a block diagram of a system incorporating the invention.

[0011] Fig. 2 is a flowchart of basic steps undertaken by a sender in transmitting a secure bulk message using the arrangement of Fig. 1.

[0012] Fig. 3 is a flowchart illustrating the process undertaken by a recipient to retrieve and open the message.

[0013] Fig. 4 illustrates a format by which an encrypted message and the encrypted decryption keys are stored on the server of Fig. 1.

DETAILED DESCRIPTION

[0014] Fig. 1 is a block diagram of a system incorporating the invention. It comprises a sender 110, which sends the encrypted message and encrypted message decryption keys to a server 112, which can then be accessed by each of N target recipients 114-1, 114-2, 114-3, ... 114-N (collectively, target recipients 114). One or more of the transmission paths from the sender 110 to the server 112 or from the server 112 to the recipients 114 are potentially insecure. As used herein, the term "message" is intended to be read broadly to include all kinds of information that might be transmitted, such as e-mail messages, documents, financial transactions, and so on. Also as used herein, the server 112 need not be

limited to a single computer. It can include multiple computers which need not even be located physically together.

[0015] Fig. 2 is a flowchart of the basic steps undertaken by the sender in transmitting a secure bulk message using the arrangement of Fig. 1. In step 210, the sender first creates the message to be sent. In step 212, the sender encrypts the message. As mentioned, encryption at this stage can be either by a symmetric or an asymmetric encryption algorithm. Although there are many examples of acceptable encryption algorithms, one common symmetric algorithm is that described in National Institutes of Standards and Technology, "Data Encryption Standard", FIPS Publication No. 46-1 (January 1988) (hereinafter "DES"), incorporated by reference herein. The encryption process in step 212 can be reversed using a message decryption key known by the sender.

[0016] In step 214, the sender encrypts the message decryption key N times -- once using the public key of each of the N target recipients. This yields N encrypted message decryption keys. In step 216, the sender sends the encrypted message, the addresses of the target recipients, and the list of encrypted message decryption keys to the server 112. It will be appreciated that one of the target recipients could be a third-party monitor, such as a government agency that is permitted to view the message if required by law.

[0017] Optionally, the sender can also send to the server 112 (or the server itself generate) a digital signature protecting all of the encrypted decryption keys associated with a particular encrypted message. The list of encrypted decryption keys thereafter cannot be tampered with without being detectable by reference to the digital signature. A digital signature is created by digesting the list, or significant portions of the list, using a well-known digesting algorithm, and then encrypting the digest with the sender's (or server's) private key of a public/private pair. In order to check for tampering, an auditor repeats the digesting of the list of encrypted decryption keys, to form a new digest, and then decrypts the digital signature using the sender's (or the server's) public key, to recover the original digest, and then compares the two for equality. A satisfactory digesting algorithm

is that describe in R. Rivest, "MD5 Message-Digest Algorithm", *Internet Engineering Task Force RFC No. 1321* (April 1992), incorporated by reference herein.

[0018] On the server 112, the encrypted message and the encrypted decryption keys are stored as illustrated in Fig. 4. The encrypted message is stored at 410. In conjunction with the encrypted message 410, the server stores each of the encrypted decryption keys 412-1, 412-2, ..., 412-N. One of the encrypted decryption keys can, as mentioned above, optionally be a monitor's decryption key 414. Optionally also stored in conjunction with the encrypted message 410, is a digital signature 416 protecting the list of encrypted decryption keys. The elements illustrated in Fig. 4 may be stored all in one contiguous region of computer-readable memory, or across discontiguous regions, or across discontiguous regions of multiple computer-readable media.

[0019] In one embodiment, the server maintains a document management system which not only stores multiple encrypted messages and their associated encrypted decryption keys, but also provides logical and structured restricted access to the various items by individual senders and individual recipients. For example, one such document management system allows senders to change the message stored on the server 112, while not allowing other senders to do so and while not allowing any recipient to do so. Another such document management system allows senders to add, delete or change entries in the list of encrypted decryption keys for messages that were transmitted by the sender, while not allowing such modifications by other senders or by any recipient. Yet another such document management system, when accessed by a particular recipient, shows the recipient only those messages on which the particular recipient is identified as a target recipient, hiding any messages for which there is no encrypted decryption key for the particular recipient.

[0020] Fig. 3 is a flowchart illustrating the process undertaken by a recipient to retrieve and open the message. In step 310, the recipient accesses the server 112, and in step 312, the recipient downloads the encrypted message and at least

the particular recipient's encrypted message decryption key 412. Alternatively, the server 112 can forward these items to the recipient without awaiting action from the recipient. In step 314, the particular recipient decrypts the recipient's encrypted message decryption key, yielding an unencrypted message decryption key. In step 316, the recipient decrypts and views the encrypted message using the now-unencrypted message decryption key.

[0021] It will be appreciated that the above-described mechanism is capable of many variations. As one example, in step 216, the sending of the encrypted message and list of encrypted message decryption keys need not take place in a single transmission. Some of all of the encrypted message decryption keys can be sent earlier or later than the encrypted message.

[0022] As another example, encrypted decryption keys could be bundled into the message and the single message with the encrypted decryption keys could be broadcast to all recipients without compromising the security of the mechanism.

[0023] As yet another example, public and private keys for encrypting the decryption keys could be replaced with symmetric private keys without affecting the security or efficiency of the mechanism.

[0024] As still another example, server 112 could be eliminated and the message with the encrypted decryption keys could be broadcast to all recipients and any other listeners, and only the target recipients will be able to decrypt the message and the security of the mechanism is not compromised.

[0025] As yet another example, for one or more of the target recipients, the sender can multiply encrypt the recipient's message decryption key, thereby requiring multiple entities to be involved in the decryption of the message decryption key. For example, the sender may first encrypt the message decryption key with the target recipient's public key, yielding a "partially-encrypted" message decryption key. The sender may then re-encrypt the partially-encrypted message decryption key, using the public key of an authorizer, thus yielding the final encrypted message decryption key. Upon receipt of the message, the recipient first has the encrypted decryption key decrypted by the authorizer, using

the authorizer's private key. This recovers the partially-encrypted message decryption key. The recipient then decrypts the partially-encrypted message decryption key, using the recipient's private key, thus yielding the un-encrypted message decryption key. Alternatively, the order of encryption for the multiple parties can be reversed, as long as the decryption sequence takes place in the same order as the encryption sequence.

[0026] The foregoing description of preferred embodiments of the present invention has been provided for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Obviously, many modifications and variations will be apparent to practitioners skilled in this art. In particular, and without limitation, any and all variations described, suggested or incorporated by reference in the Background section of this patent application are specifically incorporated by reference into the description herein of embodiments of the invention. The embodiments described herein were chosen and described in order to best explain the principles of the invention and its practical application, thereby enabling others skilled in the art to understand the invention for various embodiments and with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the following claims and their equivalents.

CLAIMS

1. A method for transmitting a message, comprising the steps of:

encrypting said message to develop an encrypted message, said encrypted message being decryptable using a first decryption key;

encrypting said first decryption key with encryption keys of a plurality of target recipients, to develop a plurality of encrypted decryption keys; and

transmitting said encrypted message and said encrypted decryption keys to said target recipients.

2. A method according to claim 1, wherein said step of encrypting said message comprises the step of encrypting said message with a symmetric encryption algorithm.

3. A method according to claim 1, wherein said step of encrypting said message comprises the step of encrypting said message with an asymmetric encryption algorithm.

4. A method according to claim 1, wherein said step of encrypting said first decryption key, with respect to a first one of said target recipients, comprises the step of encrypting said first decryption key with a symmetric encryption algorithm.

5. A method according to claim 1, wherein said step of encrypting said first decryption key, with respect to a first one of said target recipients, comprises the step of encrypting said first decryption key with an asymmetric encryption algorithm.

6. A method according to claim 1, wherein said step of encrypting said first decryption key, with respect to a first one of said target recipients, comprises the steps of:

encrypting said decryption key with a key of an additional party, to develop a partially encrypted decryption key; and

encrypting said partially encrypted decryption key with the key of said first target recipient.

7. A method according to claim 1, wherein said step of transmitting comprises the step of broadcasting said encrypted message and said encrypted decryption keys to a plurality of listeners, not all of which are members of said plurality of target recipients.

8. A method according to claim 1, wherein said step of transmitting comprises the steps of:

sending said encrypted message to a server; and

said server forwarding said encrypted message to each of said target recipients.

9. A method according to claim 8, wherein said step of transmitting further comprises the step of sending said encrypted decryption keys to one of said target recipients bypassing said server.

10. A method according to claim 8, wherein said step of transmitting further comprises the step of sending said encrypted decryption keys to said server.

11. A method according to claim 10, further comprising the step of sending to said server an additional encrypted decryption key, encrypted with a key of an additional target recipient, after said step of sending said encrypted decryption keys to said server.

12. A method according to claim 10, further comprising the step of deleting or changing one of said encrypted decryption keys on said server after said step of sending said encrypted decryption keys to said server.

13. A method according to claim 10, further comprising the step of sending to said server a digital signature covering at least one of said encrypted decryption keys.

14. A method according to claim 10, further comprising the step of sending to said server a digital signature covering all of said encrypted decryption keys.

15. A method for receiving a message, comprising the steps of:

receiving an encrypted message, said encrypted message being decryptable using a first decryption key;

receiving in conjunction with said encrypted message a plurality of encrypted decryption keys for said encrypted message;

decrypting a particular one of said encrypted decryption keys to recover said first decryption key; and

decrypting said encrypted message using said first decryption key.

16. A method according to claim 15, wherein said step of decrypting a particular encrypted decryption key comprises the steps of:

decrypting said encrypted decryption key with a key of a first party, to develop a partially decrypted decryption key; and

decrypting said partially decrypted decryption key with a key of a second party.

17. A method according to claim 15, wherein said step of receiving an encrypted message comprises the step of receiving said encrypted message from a server.

18. A method according to claim 17, wherein said step of receiving a plurality of encrypted decryption keys comprises the step of receiving said plurality of encrypted decryption keys bypassing said server.

19. A method according to claim 17, wherein said step of receiving a plurality of encrypted decryption keys comprises the step of accessing said server, said plurality of encrypted decryption keys being stored on said server.

20. A method according to claim 17, wherein said step of receiving a plurality of encrypted decryption keys comprises the step of a user accessing said server, said plurality of encrypted decryption keys being stored on said server in conjunction with said encrypted message, said server permitting access to only those messages stored thereon for which said user is a target recipient.

21. A method according to claim 15, further comprising the step of downloading said encrypted message from said server prior to said step of decrypting said encrypted message using said first decryption key.

22. Apparatus including at least one computer readable storage medium, said apparatus carrying data comprising:

an encrypted message, said encrypted message being decryptable using a first decryption key; and

a plurality of encrypted decryption keys stored in conjunction with said encrypted message, each of said encrypted decryption keys including said first decryption key encrypted with an encryption key of a respective target recipient of said message.

23. Apparatus according to claim 22, wherein one of said target recipients is a monitor.

24. Apparatus according to claim 22, wherein said data further comprises a digital signature protecting at least a portion of said encrypted decryption keys.

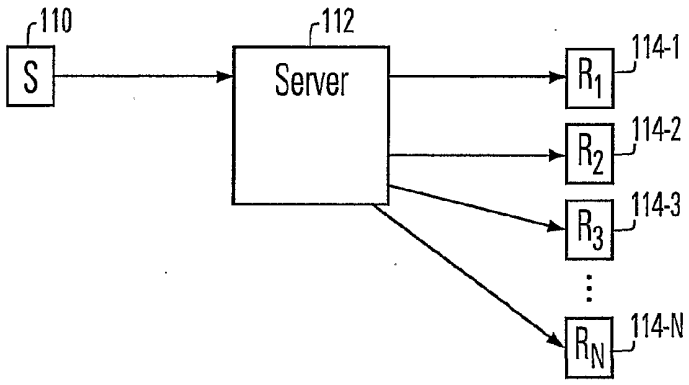


FIG. 1

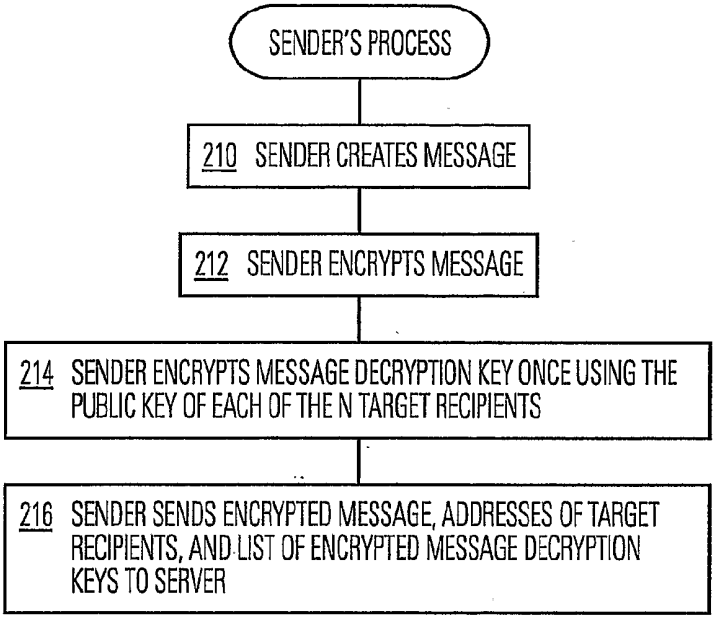

SENDER'S PROCESS
210 SENDER CREATES MESSAGE
212 SENDER ENCRYPTS MESSAGE
214 SENDER ENCRYPTS MESSAGE DECRYPTION KEY ONCE USING THE PUBLIC KEY OF EACH OF THE N TARGET RECIPIENTS
216 SENDER SENDS ENCRYPTED MESSAGE, ADDRESSES OF TARGET RECIPIENTS, AND LIST OF ENCRYPTED MESSAGE DECRYPTION KEYS TO SERVER

FIG. 2

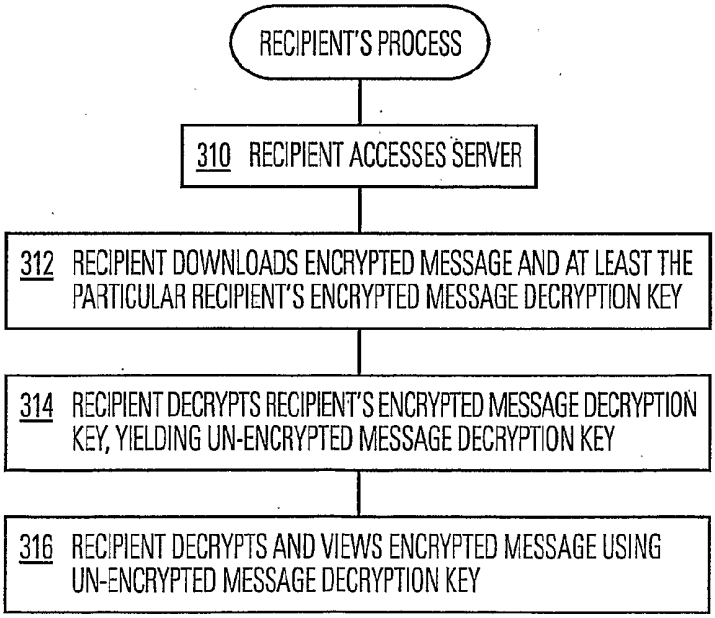

RECIPIENT'S PROCESS
310 RECIPIENT ACCESSES SERVER
312 RECIPIENT DOWNLOADS ENCRYPTED MESSAGE AND AT LEAST THE PARTICULAR RECIPIENT'S ENCRYPTED MESSAGE DECRYPTION KEY
314 RECIPIENT DECRYPTS RECIPIENT'S ENCRYPTED MESSAGE DECRYPTION KEY, YIELDING UN-ENCRYPTED MESSAGE DECRYPTION KEY
316 RECIPIENT DECRYPTS AND VIEWS ENCRYPTED MESSAGE USING UN-ENCRYPTED MESSAGE DECRYPTION KEY

FIG. 3

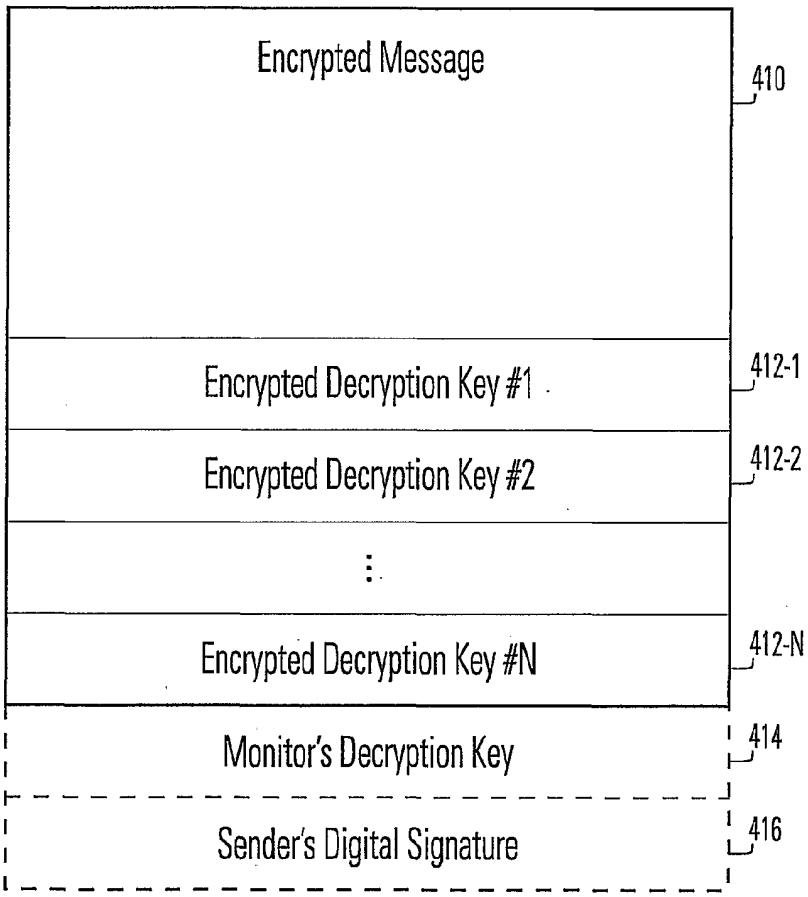

Encrypted Message
410
Encrypted Decryption Key #1
412-1
Encrypted Decryption Key #2
412-2
Encrypted Decryption Key #N
412-N
Monitor's Decryption Key
414
Sender's Digital Signature
416

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/06127

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00
US CL : 380/278

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/278, 279, 282, 284

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST "((electronic or digital) adj signature) near4 ((transmit$4 or send$3 or sent) near4 (encryption adj keys))"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,081,678 A (KAUFMAN et al) 14 January 1992 (14.01.1992), see end of abstract and Fig. 3	1-5, 7, 15
A	US 5,719,938 A (HAAS et al) 17 February 1998 (17.02.1998), see Fig. 1	8-14, 17-24
A	US 5,673,316 A (AUERBACH et al) 30 September 1997 (30.09.1997), see Fig. 6 reference numbers 602-603	6, 16
Y	US 5,956,406 A (MALDY) 21 September 1999 (21.09.1999), see Figs. 4 and 5	6, 8-12, 16-23
A	US 5,633,932 A (DAVIS et al) 27 May 1997 (27.05.1997), see Fig. 2b, reference number 265 and column 4, lines 39-56	1-7, 15
Y	US 5,016,274 A (MICALI et al) 14 May 1991 (14.05.1991), see claim 20 steps (a) through (c)	13, 14, 24
A	Schneier, "Applied Cryptography" 2nd Edition, Section 3.1, 1996, pages 47-52.	1-7, 15
A	Schneier, "Applied Cryptography" 2nd Edition, Section 6.3, 1996, pages 137-139.	7
X --- Y	Schneier, "Applied Cryptography" 2nd Edition, Section 22.7, 1996, pages 523-525.	1-5, 7, 15 --- 6, 8-14, 16-24
A,P	US 6,118,873 A (LOTSPIECH) 12 September 2000 (12.09.2000), abstract and Figs. 3-4	1-24

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
23 April 2001 (23.04.2001)

Date of mailing of the international search report
15 MAY 2001

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703)305-3230

Authorized officer
Tod Swann James R. Matthews
Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)