United States Patent [19]

Rivest et al.

[11] **4,405,829**

[45] **Sep. 20, 1983**

[54] **CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD**

[75] Inventors: **Ronald L. Rivest**, Belmont; **Adi Shamir**, Cambridge; **Leonard M. Adleman**, Arlington, all of Mass.

[73] Assignee: **Massachusetts Institute of Technology**, Cambridge, Mass.

[21] Appl. No.: **860,586**

[22] Filed: **Dec. 14, 1977**

[51] **Int. Cl.**[3] **H04K 1/00**; H04I 9/04
[52] **U.S. Cl.** **178/22.1**; 178/22.11
[58] **Field of Search** 178/22, 22.1, 22.11, 178/22.14, 22.15

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,657,476 4/1972 Aiken 178/22

OTHER PUBLICATIONS

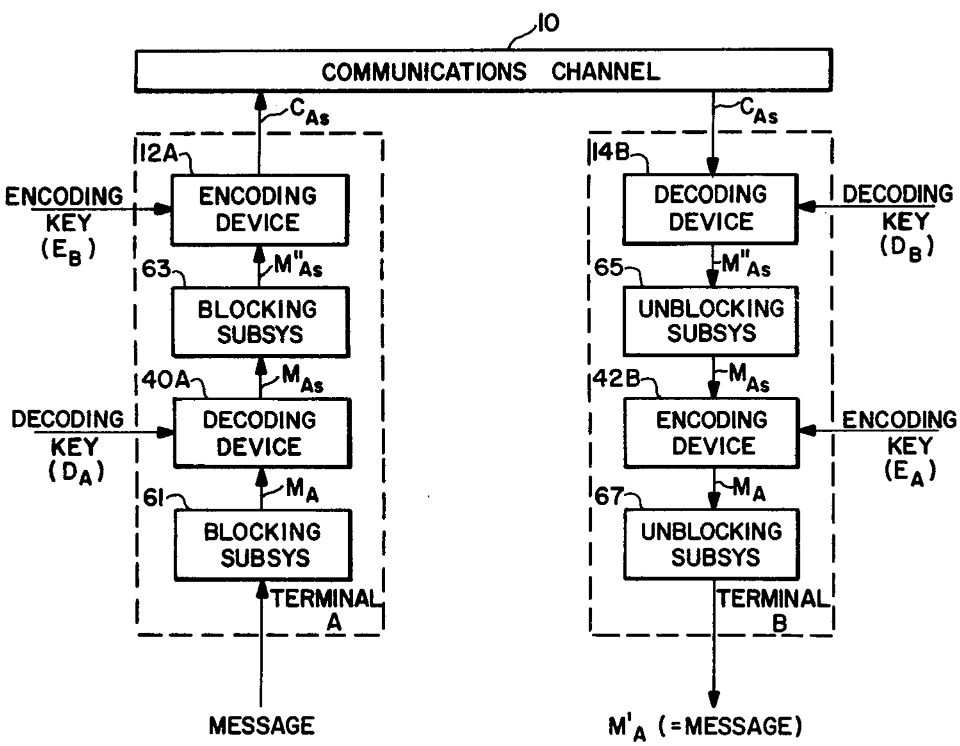
"New Directions in Cryptography", Diffie et al., *IEEE Transactions on Information Theory*, vol. IT-22, No. 6, Nov. 1976, pp. 644-654.
"Theory of Numbers" Stewart, MacMillan Co., 1952, pp. 133-135.
"Diffie et al., Multi-User Cryptographic Techniques", AFIPS. Conference Proceedings, vol. 45, pp. 109-112, Jun. 8, 1976.

Primary Examiner—Sal Cangialosi
Attorney, Agent, or Firm—Arthur A. Smith, Jr.; Robert J. Horn, Jr.

[57] **ABSTRACT**

A cryptographic communications system and method. The system includes a communications channel coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. A message-to-be-transferred is enciphered to ciphertext at the encoding terminal by first encoding the message as a number M in a predetermined set, and then raising that number to a first predetermined power (associated with the intended receiver) and finally computing the remainder, or residue, C, when the exponentiated number is divided by the product of two predetermined prime numbers (associated with the intended receiver). The residue C is the ciphertext. The ciphertext is deciphered to the original message at the decoding terminal in a similar manner by raising the ciphertext to a second predetermined power (associated with the intended receiver), and then computing the residue, M', when the exponentiated ciphertext is divided by the product of the two predetermined prime numbers associated with the intended receiver. The residue M' corresponds to the original encoded message M.

40 Claims, 7 Drawing Figures



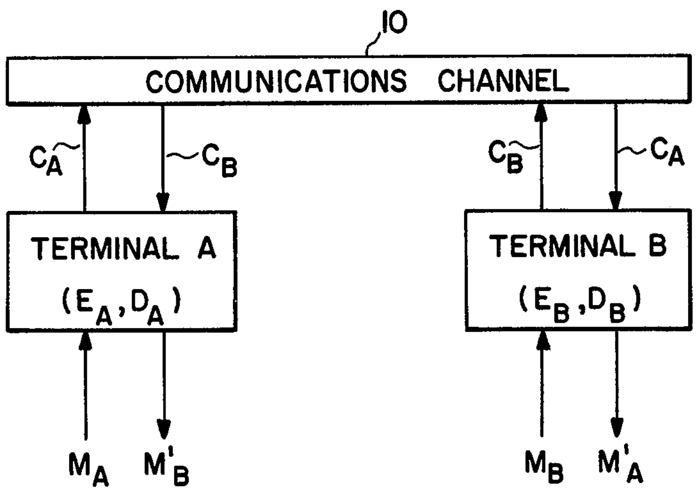

10
COMMUNICATIONS CHANNEL
C_A
C_B
C_B
C_A
TERMINAL A
(E_A, D_A)
TERMINAL B
(E_B, D_B)
M_A
M'_B
M_B
M'_A

FIG. 1

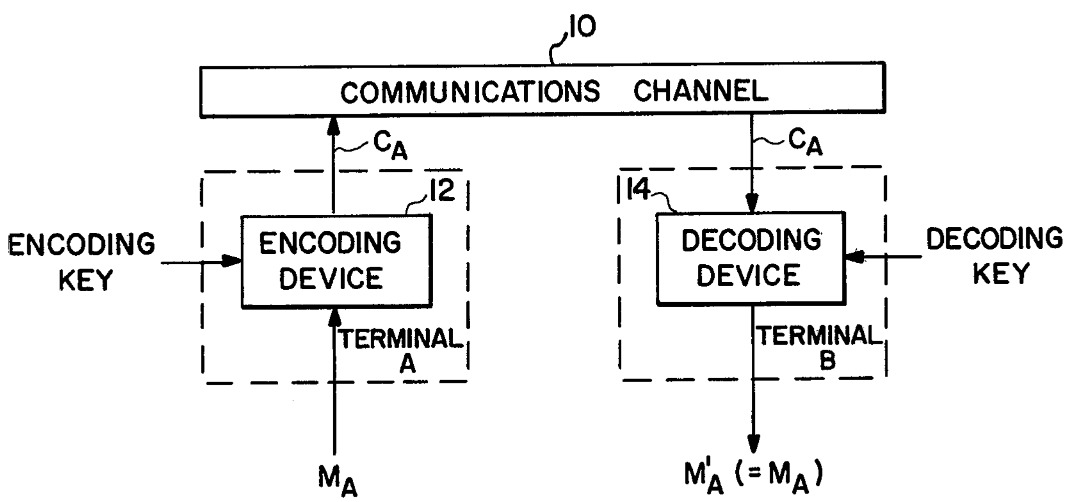

10
COMMUNICATIONS CHANNEL
C_A
C_A
12
14
ENCODING KEY
ENCODING DEVICE
DECODING DEVICE
DECODING KEY
TERMINAL A
TERMINAL B
M_A
M'_A $(=M_A)$

FIG. 2

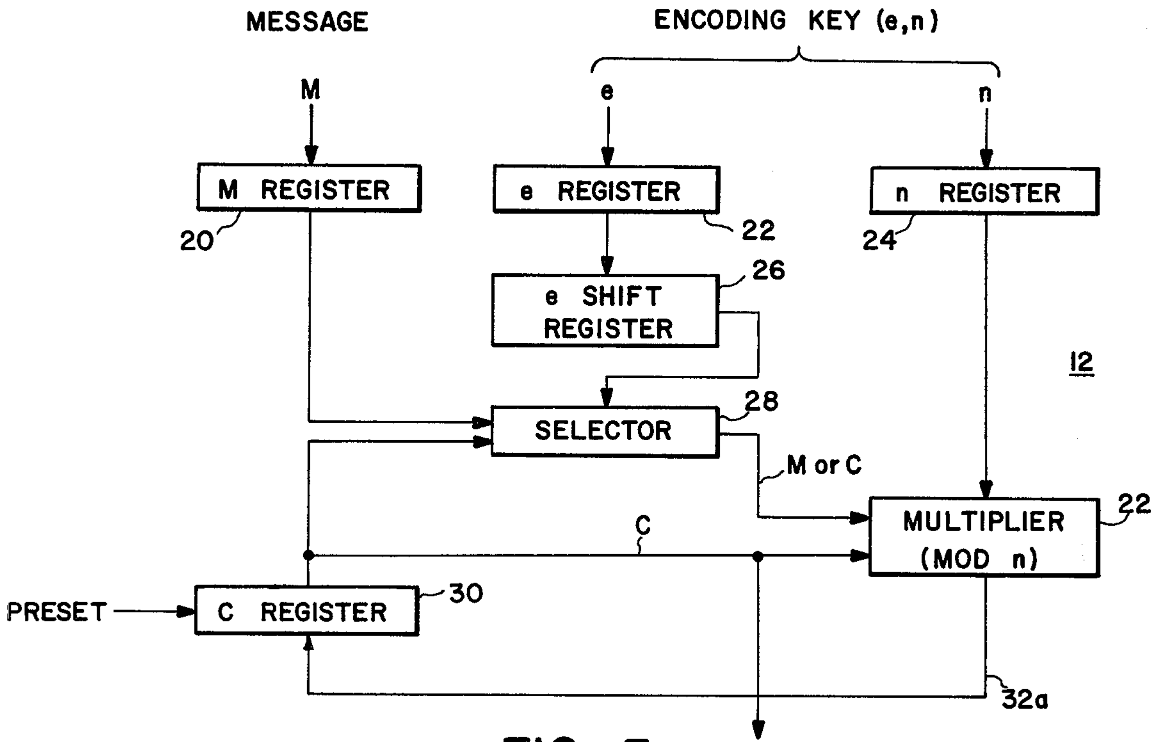


FIG. 3

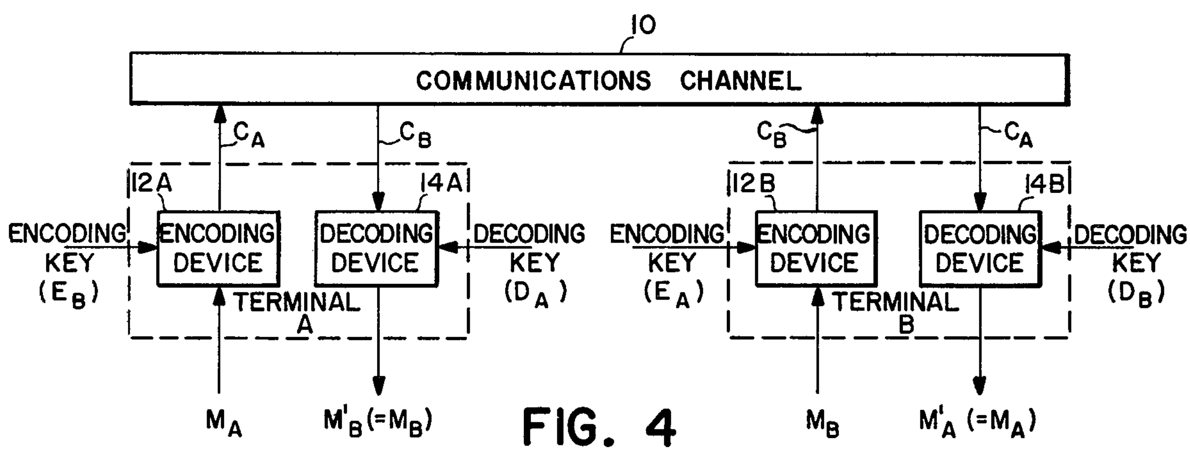


FIG. 4

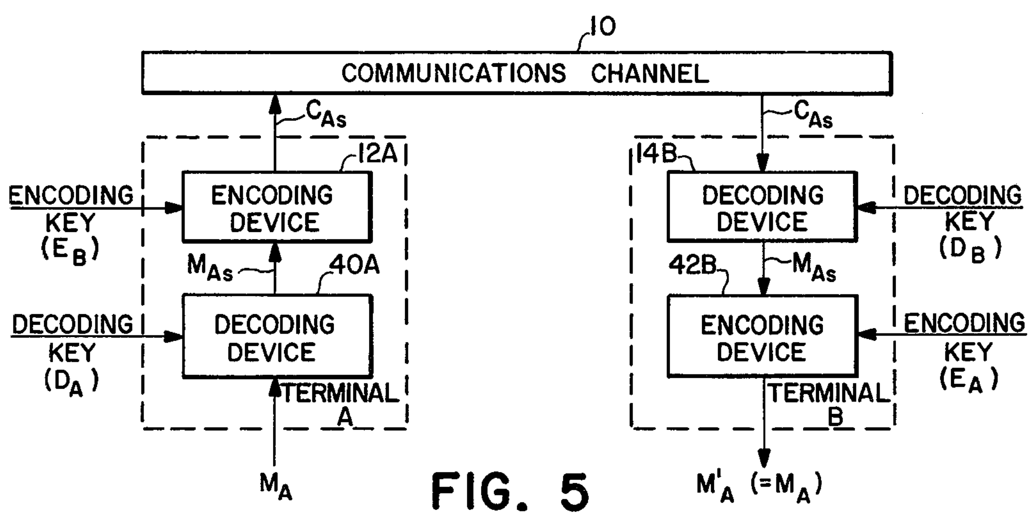


FIG. 5

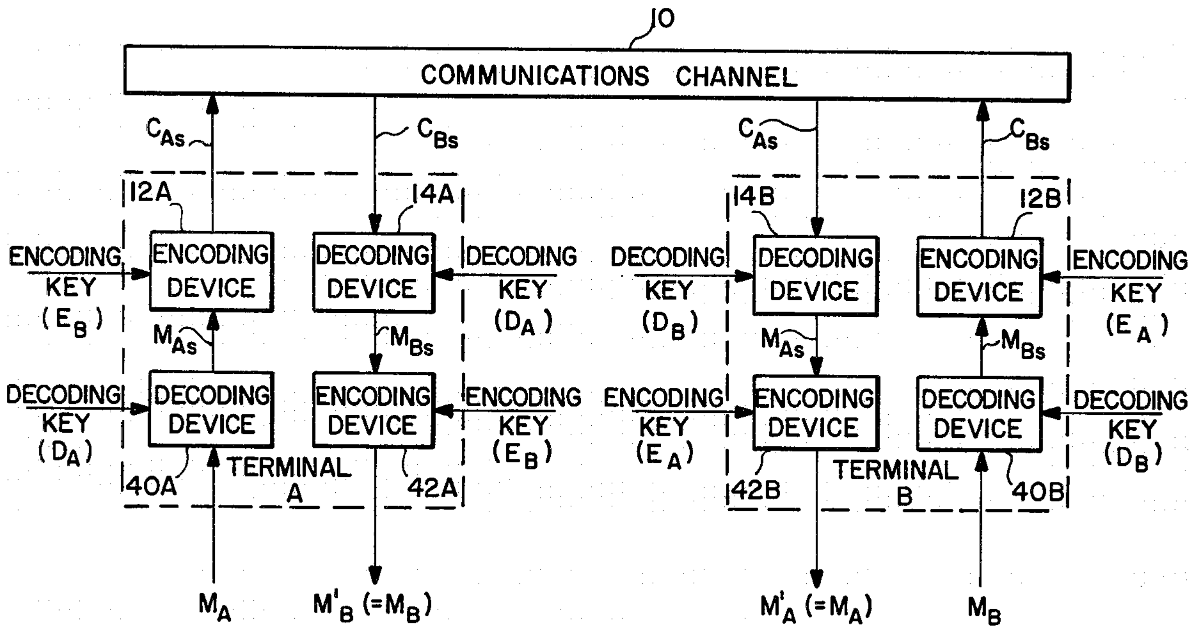

10
COMMUNICATIONS CHANNEL
C$_{As}$
C$_{Bs}$
C$_{As}$
C$_{Bs}$
12A
14A
14B
12B
ENCODING KEY (E$_B$)
ENCODING DEVICE
DECODING DEVICE
DECODING KEY (D$_A$)
DECODING KEY (D$_B$)
DECODING DEVICE
ENCODING DEVICE
ENCODING KEY (E$_A$)
M$_{As}$
M$_{Bs}$
M$_{As}$
M$_{Bs}$
DECODING KEY (D$_A$)
DECODING DEVICE
ENCODING DEVICE
ENCODING KEY (E$_B$)
ENCODING KEY (E$_A$)
ENCODING DEVICE
DECODING DEVICE
DECODING KEY (D$_B$)
40A
TERMINAL A
42A
42B
TERMINAL B
40B
M$_A$
M'$_B$ (=M$_B$)
M'$_A$ (=M$_A$)
M$_B$

FIG. 6

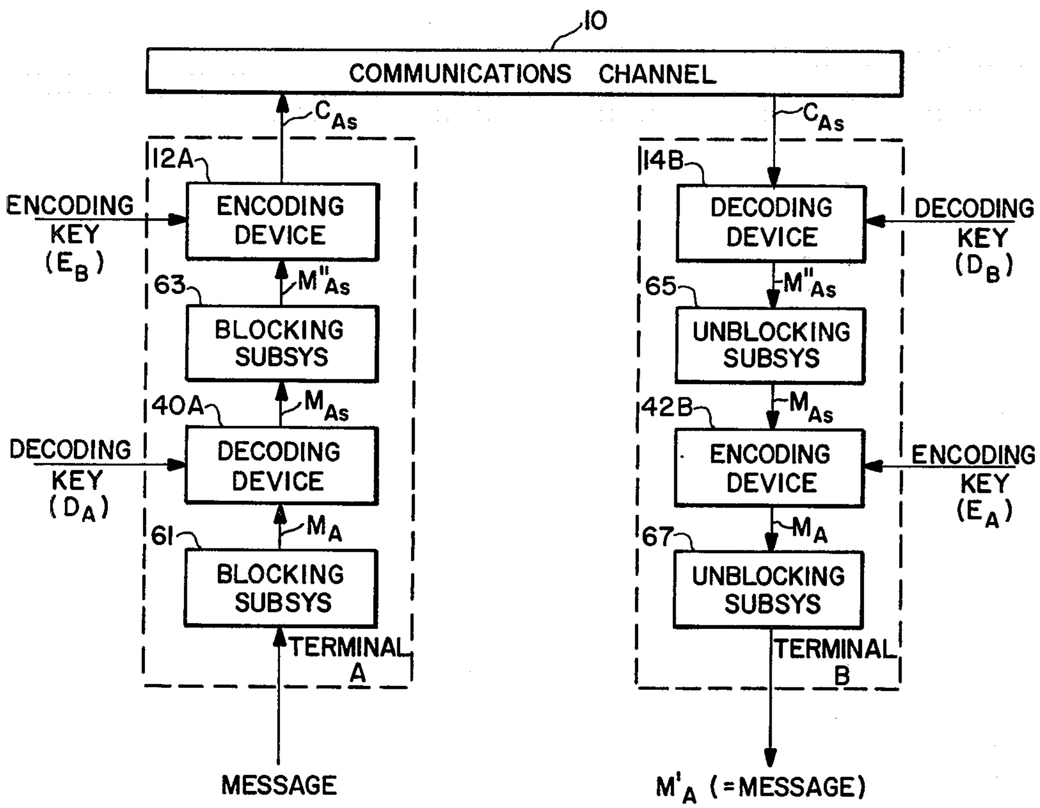

10
COMMUNICATIONS CHANNEL
C$_{As}$
C$_{As}$
12A
14B
ENCODING KEY (E$_B$)
ENCODING DEVICE
DECODING DEVICE
DECODING KEY (D$_B$)
63
M''$_{As}$
65
M''$_{As}$
BLOCKING SUBSYS
UNBLOCKING SUBSYS
40A
M$_{As}$
42B
M$_{As}$
DECODING KEY (D$_A$)
DECODING DEVICE
ENCODING DEVICE
ENCODING KEY (E$_A$)
61
M$_A$
67
M$_A$
BLOCKING SUBSYS
UNBLOCKING SUBSYS
TERMINAL A
TERMINAL B
MESSAGE
M'$_A$ (=MESSAGE)

FIG. 7

CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD

The Government has rights in this invention pursuant to Contract No. N00014-67-A-0204, awarded by the Department of the Navy, and Grant No. MCS76-14249, awarded by the National Science Foundation.

BACKGROUND OF THE DISCLOSURE

This invention relates to communications, and more particularly to cryptographic communications systems and methods.

With the development of computer technology, the transfer of information in digital form has rapidly increased. There are many applications, including electronic mail systems, bank systems and data processing systems, where the transferred information must pass over communications channels which may be monitored by electronic eavesdroppers. While the degree of security required may vary for various applications, it is generally important for all of these examples that the substance of particular communications pass directly from a sender to an intended receiver without intermediate parties being able to interpret the transferred message. In addition, there are further instances where information in computer memory banks must be protected from snoopers who have access to the memory through data processing networks.

In addition to these privacy requirements, authentication of the source of a message must often be insured along with the verification and security of the message content. For example, in banking applications, it is required that a signed document, such as a bank draft, be authenticated as being actually signed by the indicated signator. Furthermore, in many applications, it is desirable to further require safeguards against signature forgery by a message recipient.

In the prior art, a number of cryptographic encoding and decoding techniques are readily available to provide some degree of privacy and authentication for digital communications, for example, the data encryption standards adopted by the National Bureau of Standards, see *Federal Register,* Mar. 17, 1975, Volume 40, No. 52 and Aug. 1, 1975, Volume 40, No. 149.

In general, cryptographic systems are adapted to transfer a message between remote locations. Such systems include at least one encoding device at a first location and at least one decoding device at a second location, with the encoding and decoding devices all being coupled to a communication channel. For digital systems, the message is defined to be a digital message, M, that is, a sequence of symbols from some alphabet. In practice, the alphabet is generally chosen to be the binary alphabet consisting of the symbols 0 and 1.

Each encoding device is an apparatus which accepts two inputs: a message-to-be-encoded, M, and an encoding key or operator, E. Each encoding device transforms the message M in accordance with the encryption operator to produce an encoded version C of the message (which is denoted as the ciphertext) where $C=E(M)$. The encoding key and the ciphertext are also digital sequences.

Each decoding device is an apparatus which accepts two inputs: a ciphertext-to-be-decoded C and a decoding key or operator, D. Each decoding device transforms the ciphertext in accordance with the decryption operator to produce a decoded version M′ of the ciphertext where $M'=D(C)$, or $M'=D(E(M))$. Like the encoding key, the decoding key and decoded message M′ are also digital sequences. The encoding and decoding keys are selected so that $M'=M$ for all messages M.

In operation, a message, once encoded into ciphertext, is transmitted over the channel to a recipient who decodes the received ciphertext to obtain the original message M. Thus, a recipient sees the original message M as the output of his decoding device.

To a large degree, the quality of performance of a cryptographic system depends on the complexity of the encoding and decoding devices. Regarding the problem of ensuring privacy of communications for a system where an eavesdropper can listen to every message transmitted on the communications channel (which might, for example, be a radio link), the effectiveness of the system depends upon the ability to ensure that the eavesdropper is unable to understand any such overheard messages. In the prior art systems, the sender and recipient arrange to have corresponding encoding and decoding keys which are kept secret from the eavesdropper, so that even if the eavesdropper knows the construction of the encoding and decoding devices, he would not be able to decode the messages he hears, even after hearing a large number of messages. In practice, however, this constraint results in extremely complex and correspodingly expensive equipment. A disadvantage of the prior art systems results from the general requirement that the pre-arranged encoding and decoding keys must be delivered in a secure fashion (often by courier) to the sender and receiver, respectively, to enable communication through the systems.

The "public-key cryptosystem" described by Diffie and Hellman, "New Directions In Cryptography", IEEE Transactions on Information Theory (Nov. 1976), in principle, provides enciphered communication between arbitrary pairs of people, without the necessity of their agreeing on an enciphering key beforehand. The Diffie and Hellman system also provides a way of creating for a digitized document a recognizable, unforgeable, document-dependent, digitized signature whose authenticity the signer cannot later deny.

In a public-key cryptosystem, each user (e.g. user A) places in a public file an enciphering operator, or key, E_A. User A keeps to himself the details of the corresponding deciphering key D_A which satisfies the equation

$$D_A(E_A(M))=M,$$

for any message M. In order for the public key system to be practical, both E_A and D_A must be efficiently computable. Furthermore, user A must not compromise D_A when revealing E_A. That is, it should not be computationally feasible for an eavesdropper to find an efficient way of computing D_A, given only a specification of the enciphering key E_A (even though a very inefficient way exists: to compute $D_A(C)$, just enumerate all possible messages M until one such that $E_A(M)=C$ is found. Then $D_A(C)=M$.). In a public key system, a judicious selection of keys ensures that only user A is able to compute D_A efficiently.

Whenever another user (e.g. user B) wishes to send a message M to A, he looks up E_A in the public file and then sends the enciphered message $E_A(M)$ to user A. User A deciphers the message by computing $D_A(E_A(M))=M$. Since D_A is not derivable from E_A in a practical way, only user A can decipher the message

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.