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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 August 2007 (16.08.2007)

PCT

(10) International Publication Number
WO 2007/092525 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2007/003309

(22) International Filing Date: 7 February 2007 (07.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/765,998 7 February 2006 (07.02.2006) 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, NY 10027 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **STAVROU, Angelos** [GR/US]; 527 W. 113th Street, #1F, New York, NY 10025 (US). **KEROMYTIS, Angelos, D.** [GR/US]; 423 W. 120th Street, #98, New York, NY 10027 (US). **LOCASTO, Michael, E.** [US/US]; 4 Pringle Road, Miller, NY 11764 (US).

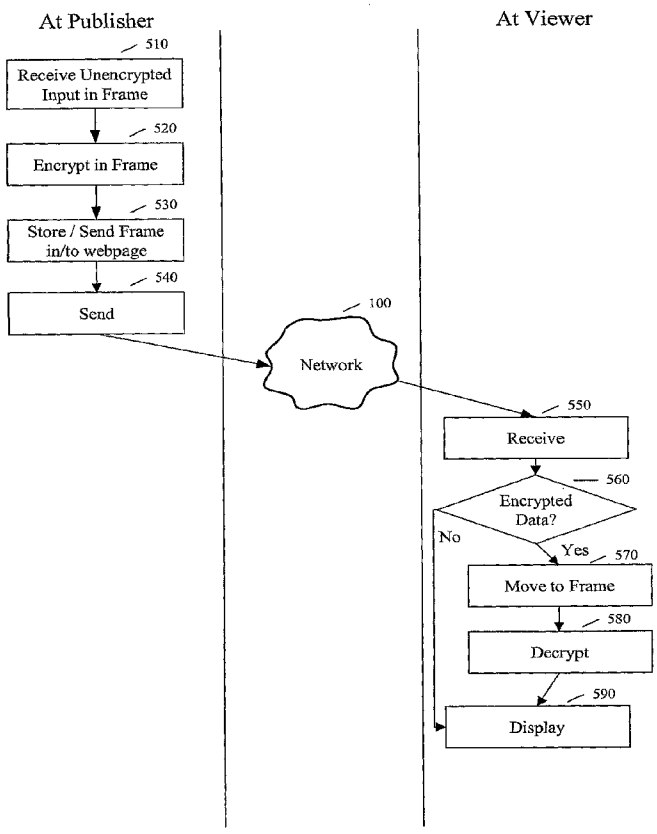
(74) Agents: **HALAS, Michael** et al.; Wilmer Cutler Pickering Hale And Dorr LLP, 399 Park Avenue, New York, NY 10022 (US).

(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, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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,

[Continued on next page]

(54) Title: SYSTEMES, PROCEDES ET SUPPORTS POUVANT INHIBER LES ATTAQUES CONTRE DES DONNEES



(57) Abstract: L'invention concerne des systèmes, des procédés et des supports pouvant inhiber les attaques contre des données. Dans quelques modes de réalisation, les procédés de l'invention consistent à: recevoir des données et au moins une indication selon laquelle les données sont cryptées dans un environnement non protégé dans un navigateur web; déterminer si, d'après au moins ladite ou lesdites indications, cette partie des données est cryptée; créer un environnement protégé dans le navigateur web; rendre automatiquement les données disponibles pour ledit environnement protégé; déchiffrer les données pour former des données déchiffrées dans l'environnement protégé; et présenter les données déchiffrées dans l'environnement protégé.

WO 2007/092525 A2

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.

Express Mailing No. EV 901254893 US
Docket No. 19240.568WO1

SYSTEMS, METHODS, AND MEDIA FOR INHIBITING ATTACKS ON DATA

Cross-Reference to Related Application

[0001] This application claims the benefit of United States Provisional Patent Application No. 60/765,998, filed February 7, 2006, which is hereby incorporated by reference herein in its entirety.

Technology Area

[0002] The disclosed subject matter relates to systems, methods, and media for inhibiting attacks on data.

Copyright Notice

Background

[0004] Users of data communications typically want to ensure that their communications remain private and uncompromised. However, communications between digital processing devices can be intercepted by attacks on, for example, the digital devices themselves or a network that the devices use for communication. While some network communications can be protected, for example, by transport level cryptographic operations (e.g., Secure Socket Layer (SSL), Transport Layer Security (TLS), etc.), there are situations in which a communications infrastructure provider cannot be trusted. For example, an access-restricted webpage intended to be seen only by authorized viewers can be submitted for private publication to a hosting service. However, the hosting service can breach the confidentiality by reading or otherwise using the document. Likewise, a customer purchasing items from an online merchant may have to divulge sensitive personal information (e.g., account numbers, addresses, etc.) to the merchant. Revealing such information to the merchant may be an unacceptable security risk, especially when the merchant may not guarantee the security of its systems against electronic or physical theft.

[0005] In another example, users of webmail services, such as MSN Hotmail, Yahoo Mail, or Google's Gmail may be concerned about keeping their e-mails confidential from the webmail service. In some cases, a user may employ Pretty Good Privacy (PGP) or Secure / Multipurpose Internet Mail Extensions (S/MIME) for e-mail messages, when a trusted mail client is available from a webmail service. However, such a trusted mail client may not be always available. Furthermore, in some cases, even if these services can support, for example, client-side PGP operations (e.g., via ActiveX, Flash or a Java applet), the user may not trust these components with, for example, the user's private key or pass phrase.

[0006] Thus, in many cases, the security and/or privacy of a user's communications are susceptible to vulnerabilities of another's equipment and/or employees, or to the unavailability of adequate technology for protecting those communications.

Summary

[0007] Systems, methods, and media for inhibiting attacks on data are provided. In some embodiments, methods for inhibiting attacks on data are provided. The methods include receiving data and at least one indication indicating that the data is encrypted in an unprotected environment in a web browser; determining whether the at least one indication indicates that the portion of the data is encrypted; creating a protected environment in the web browser; automatically making the data available to the protected environment; decrypting the data to form decrypted data in the protected environment; and displaying the decrypted data in the protected environment.

[0008] In some embodiments, methods for inhibiting attacks on data are provided. The methods include creating a protected environment in a web browser; receiving data in the protected environment; encrypting the data to form encrypted data in the protected environment; associating the encrypted data with an indication that the encrypted data is encrypted; and automatically making the encrypted data and the indication accessible to an unprotected environment in the web browser.

[0009] In some embodiments, computer-readable media containing computer-executable instructions that, when executed by a processor, cause the processor to perform methods for inhibiting attacks on data are provided. The methods include receiving data and at least one indication indicating that the data is encrypted in an unprotected environment in a web browser; determining whether the at least one indication indicates that the portion of the

data is encrypted; creating a protected environment in the web browser; automatically making the data available to the protected environment; decrypting the data to form decrypted data in the protected environment; and displaying the decrypted data in the protected environment.

[0010] In some embodiments, computer-readable media containing computer-executable instructions that, when executed by a processor, cause the processor to perform methods for inhibiting attacks on data are provided. The methods include creating a protected environment in a web browser; receiving data in the protected environment; encrypting the data to form encrypted data in the protected environment; associating the encrypted data with an indication that the encrypted data is encrypted; and automatically making the encrypted data and the indication accessible to an unprotected environment in the web browser.

[0011] In some embodiments, systems for inhibiting attacks on data, including an interface in communication with a network; a memory; and a processor in communication with the memory and the interface are provided, wherein the processor receives data and at least one indication indicating that the data is encrypted in an unprotected environment in a web browser; determines whether the at least one indication indicates that the portion of the data is encrypted; creates a protected environment in the web browser; automatically makes the data available to the protected environment; decrypts the data to form decrypted data in the protected environment; and displays the decrypted data in the protected environment.

[0012] In some embodiments, systems for inhibiting attacks on data, including an interface in communication with a network; a memory; and a processor in communication with the memory and the interface are provided, wherein the processor creates a protected environment in a web browser; receives data in the protected environment; encrypts the data to form encrypted data in the protected environment; associates the encrypted data with an indication that the encrypted data is encrypted; and automatically makes the encrypted data and the indication accessible to an unprotected environment in the web browser.

[0013] In some embodiments, methods for inhibiting attacks on data are provided. The methods include receiving data from a first entity comprising at least a message and an encrypted account number; determining, based on the message, whether the encrypted account number needs to be authorized; if the encrypted account number needs to be authorized, making the encrypted account number available to a second entity; receiving

authorization from the second entity; and sending a response to the first entity based on the message and the authorization.

Brief Description of the Drawings

[0014] FIG. 1 is a schematic diagram of a system suitable for inhibiting attacks on data in accordance with some embodiments of the disclosed subject matter.

[0015] FIG. 2 is an illustration of nodes that can be used in FIG. 1 in accordance with some embodiments of the disclosed subject matter.

[0016] FIG. 3 is a simplified illustration of a method for inhibiting attacks on data by a party that needs information related to the data in accordance with some embodiments of the disclosed subject matter.

[0017] FIG. 4 is simplified illustration of a method for inhibiting attacks on data from a party through which the data is sent in accordance with some embodiments of the disclosed subject matter.

[0018] FIG. 5 is simplified illustration of a method for inhibiting attacks using a protected frame in accordance with some embodiments of the disclosed subject matter.

[0019] FIG. 6 is a "div" tag and associated data that can be used in accordance with some embodiments of the disclosed subject matter.

[0020] FIG. 7 is a screen shot of a pull down menu that can be used to select a cryptographic operation in accordance with some embodiments of the disclosed subject matter.

[0021] FIG. 8 is a screen shot of data signed and encrypted in accordance with some embodiments of the disclosed subject matter.

[0022] FIG. 9 is a simplified illustration of a method for inhibiting attacks on parts of a document which is shared among various entities in accordance with some embodiments of the disclosed subject matter.

Detailed Description

[0023] Systems and methods for inhibiting attacks on data are provided. In some embodiments, end-to-end (E2E) confidentiality and integrity between a producer of content and a recipient of that content are provided. This confidentiality and integrity can be provided, for example, by a mechanism in which content can be encrypted in one client's web browser and then decrypted in another client's web browser without being subject to review and/or modification by an intervening server. Public-key cryptography (e.g., PGP) can be used, although various types of cryptography can additionally or alternatively be used.

[0024] Some embodiments can transform HTML content into, for example, PGP encrypted, ASCII-armored blocks of data when transferring data to a web browser. Sections of a document can be identified for encryption and/or decryption by using, for example, tags or markers, such as the "div tag" (an HTML tag that defines a division/section in a document). For example, encryption can be provided using a style-sheet applied to web-content in a browser by marking div tags with a Cascading Style Sheet (CSS) identifier. In some embodiments, text can be manually selected in objects, such as, for example, "text-areas" and "text-boxes," and a context menu can access PGP to, for example, encrypt, sign, encrypt and sign, decrypt, verify, and decrypt and verify, the selected text.

[0025] Some embodiments can provide cryptographic processing when displaying and/or rendering content. For example, in addition to rendering content for placement, size, and coloring, the content can be decoded into a form that the user is authorized to view. Sections of a document that were identified and encrypted, as discussed above, can be automatically decrypted when received by a user having an appropriate key, for example.

[0026] Some embodiments can provide these functions through an extension to a web browser, such as, for example, Microsoft Internet Explorer (from Microsoft Corporation), Firefox (available from the Mozilla Foundation), Safari (available from Apple Inc.), Opera (available from Opera Software), lynx (available from, for example, http://lynx.browser.org), and wget (available from the Free Software Foundation). The extension can include, for example, extra functionality for a layout engine, additions to the user interface (UI) (e.g., to the selected-text context menu), and/or the addition of key handling (e.g., PGP key handling). Extensions to web browsers can offer, for example, easy deployment and can allow a user to easily enable, disable, or update the extension while requiring only small or no modifications to the browser. In other cases, functions of the disclosed subject can be provided as an

integrated part of a web browser. In some embodiments, new tags can be added to the HTML grammar to identify sections of a document for encryption and/or decription.

[0027] FIG. 1 is a schematic diagram of an illustrative system 100 that may be used for protecting communications between a first entity (e.g., an originator, such as, a customer, a content publisher, a web logger, an e-mail user, etc.) and a second entity (e.g., an intermediary, such as, a banking system, a credit card authorization service, a shipping company, a content reader, an e-mail user, etc.) through a third entity (e.g., an intended recipient, such as, a service provider, a merchant, a web hosting service, etc.) in accordance with some embodiments of the disclosed subject matter. In some embodiments, the above examples of different entities can serve various roles (e.g., a merchant can be any of the first, second, and/or third entities). As illustrated, system 100 can include one or more clients 102. Clients 102 can be connected by one or more communications links 104 to a communications network 106 or connected directly to each other. Communications network 106 can also be linked through a communications link 108 to a server 110. Various embodiments of the disclosed subject matter can be implemented on at least one of the server and the clients. It is also possible that a client and a server can be connected through communication links 108 or 104 directly and not through a communication network 106.

[0028] In system 100, server 110 can be a server or digital processing device for executing an application, such as, for example, a processor, a computer, a data processing device, or a combination of such devices. Communications network 106 can be a data transfer network including the Internet, an intranet, a wide-area network (WAN), a local-area network (LAN), a wireless network, a digital subscriber line (DSL) network, a frame relay network, an asynchronous transfer mode (ATM) network, a virtual private network (VPN), a mobile ad-hoc network (MANET), or a combination of one or more of the same. Communications links 104 and 108 can be communications links suitable for communicating data between clients 102 and server 110, such as network links, dial-up links, wireless links, hard-wired links, etc. Clients 102 can be digital processing devices, such as, for example, personal computers, laptop computers, mainframe computers, data displays, Internet browsers, personal digital assistants (PDAs), two-way pagers, wireless terminals, portable telephones, etc., or a combination of the same. Clients 102 and server 110 can be located at various locations. In some embodiments, clients 102 and server 110 can be located within an

organization. Alternatively, clients 102 and server 110 can be distributed between multiple organizations.

[0029] The server 110 and one of the clients 102, which are depicted in FIG. 1, are illustrated in more detail in FIG. 2. Referring to FIG. 2, client 102 and server 110 can include respectively, among other things, processors 202 and 220, displays 204 and 222, input/output devices 206 and 224, and memory 208 and 226, which can be interconnected. The input/output devices can receive input such as, for example, text from a keyboard, mouse clicks, images from a camera, images from a scanner, audio recordings, voice-to-text translations, etc. The input/output devices can produce output such as, for example, text-to-voice, audio recordings, etc. In one embodiment, memory 208 and 226 contain a storage device for storing a program for controlling processors 202 and 220. Memory 208 and 226 can also contain applications for inhibiting attacks on data. In some embodiments, various applications can be resident in the memory of client 102 or server 110. System 100 can be modified to include additional components or omit components in accordance with various embodiments of the disclosed subject matter. In addition, although some embodiments are described herein as being implemented on a client and/or a server, this is only illustrative. Various components of some embodiments of the disclosed subject matter can be implemented on various platforms.

[0030] As described above, some embodiments provide protection from an untrustworthy service provider. If, for example, the user is a customer of an online merchant, the merchant can attack by misusing information the user disclosed to the merchant. If, for example, a user is a user of a web-mail service, the web-mail service can attack by examining e-mails sent to other users. In some cases, the attacker (e.g., service provider) may be merely curious, however, in other cases the attacker may be compromised, or actively malicious.

[0031] For example, a client 102 may send a message to another client 102 through, for example, a server 110. A server 110 can be, for example, a host for a webmail service, a merchant, and/or a web host for content, such as, blogs. The message may contain personal information, such as, for example, credit card information. Despite not needing the personal information, for example, to satisfy an order, the server 110 may nevertheless examine and/or store the personal information.

[0032] FIG. 3 illustrates a method for addressing this situation in accordance with some embodiments. As shown, for example, a customer (e.g., a client) can send, at 310, a message (e.g., a product request) and encrypted information (e.g., an account number, a credit card number, etc.) to a merchant. The encrypted information can be formed using various techniques. The merchant can determine whether it needs information related to the encrypted information, at 330. If it does not need information, the merchant can for example, send a response and/or the product to the customer, at 390. If it does need information, the merchant can send, at 340, the encrypted account number to an authorizer. The authorizer (e.g., a client or a server) can authorize account transactions. In doing so, the authorizer can decrypt and authorize the account number, at 350, and send, at 360, an authorization message to the merchant. The merchant can then receive the authorization, at 370, and proceed, at 380, by, for example, responding to the customer and/or sending the customer the product. In this way, the account number can be protected from the merchant, but the merchant can still acquire what it needs (i.e., the authorization) to perform the sale.

[0033] As another example, as shown in FIG. 4, a publisher can create a plain text file (e.g., an HTML file), at 410. The publisher can encrypt portions of the plaintext file, at 420, and submit and/or upload the encrypted file, at 430, to a server (e.g., a web server). The server can make the encrypted file 435 available as a webpage, at 440. A viewer can access the webpage, at 450, using, for example, a web browser. The file can be rendered for viewing, including decrypting the encrypted portions of the file, at 460.

[0034] Because some content may be vulnerable when entered into or received from a communications channel, some embodiments can subvert and/or inhibit a communication channel. This subversion and/or inhibition can protect content from a provider of the channel and can include using the channel in a way that the provider did not envision or intend. For example, because some content may be vulnerable when merely entered into a field on a webpage, some embodiments can receive input and/or issue output operations in a, protected area, such as a secure overlay frame. The overlay frame can protect input and output by, for example, not allowing any scripts (e.g., "external" Javascripts) or other code to read or otherwise access data in the frame. In this way, these embodiments can inhibit an attack from accessing data either before or after encryption. In one such attack, a webmail provider can include Javascript (as part of its webmail client) that can log a user's plaintext keystrokes while the user is drafting an e-mail. If the user encrypts the e-mail, the webmail provider

may still have the log of the plaintext that it obtained by keystroke monitoring. To inhibit such an attack, for example, in some embodiments, input operations (e.g., key strokes, pasted images, etc.) can be received and encrypted in an overlay frame and then the encrypted content can be provided to a target in encrypted form.

[0035] For example, as illustrated in FIG. 5, unencrypted data can be received in an overlay frame, at 510. The data can be encrypted in the overlay frame, at 520. The encrypted data can be copied or otherwise entered into a, communications channel, such as a web browser window, at 530, and sent or made available to a viewer, at 540, through network 100. A communications channel, such as a web browser, at the receiver can receive the encrypted data, at 550. The web browser can determine, at 560, whether the received data includes encrypted data. If not, web browser can display the data, at 590. If so, the encrypted data can be moved to an overlay frame, at 570. The data then can be decrypted, at 580, and displayed, at 590. In some embodiments, data may be moved to a frame, at 570, from 550 regardless of whether it contains encrypted data. Various types of data can be protected from various communication channels. For example, a protected frame can be used to protect a text message (e.g., on a cellular phone) from a service provider.

[0036] In order to facilitate encryption and decryption in a document, some embodiments can perform encryption and/or decryption based on an indication in the document. The indication can be, for example, a location of data in a document and can be designated or determined based on, for example, an offset from another location in the document (e.g., the beginning or end), the context of data or surrounding data (e.g., the presence of plain text or the presence of an account number), a string (e.g., "encrypt starting here"), a tag, and/or an element. For example, in order to facilitate automatic decrypting of content in a markup language, such as HyperText Markup Language (HTML), some embodiments can recognize specially marked elements and/or tags. Various elements and/or tags can be used, such as, for example, a "p" (paragraph), "body," "table," "div," and/or "span." These elements can be marked, for example, with the class attribute set to "w3bcrypt," or any other appropriate value, as illustrated in FIG. 6. The class attribute value can be designated by, for example, users, administrators, or a standards committee. The data 610 associated with, for example, the div or span element can then be automatically decrypted. For example, a web browser can finish loading an object module for a page and can request a list of all div or span elements marked with "w3bcrypt" and decrypt them. The

object module can be, for example, the HTML Document Object Model (DOM) (i.e., a collection of objects that represent a page in a web browser and can be used by script programs to examine and dynamically change the page). In some embodiments, the user can be prompted for a pass phrase and/or key to use for decryption.

[0037] To further secure encrypted data, some embodiments can add randomness to the encrypted data. For example, a timestamp, sequence number, and/or randomly generated ticket can be appended to information that will be encrypted (e.g., an account number) and can serve, for example, to identify duplicate transactions. In some embodiments, the use of random data can protect against replay attacks, where, for example, an attacking merchant or service provider sends a user's message multiple times. For example, an attacking merchant may attempt to submit a user's encrypted credit card account number multiple times. However, a customer can include, for example, an encrypted ticket with the credit card number for authorization (at 340 and 350 of FIG. 3). When the authorization service decrypts the account number and the ticket, it can determine that it has already authorized a transaction for this account number and ticket combination. As such, the charge can be denied.

[0038] Some embodiments can provide key management and cryptographic processing, using various key management and cryptographic mechanisms. For example, GnuPG (an implementation of the OpenPGP standard as defined by RFC2440) can be used. Some embodiments, can probe the host at installation time for any already-installed PGP packages, a user can manually select or download a PGP package from a list, or a PGP package can be automatically selected by the system. In some embodiments, a user can enter a key to be used in encryption in a browser window. In some embodiments, for example, where a web content publisher wishes to, for example, forgo or supplement traditional authentication and authorization services, content can be published under an "audience" key (or series of keys).

[0039] In some embodiments, PGP cryptographic operations can be presented as choices in a context menu 701 as show in FIG. 7. As illustrated, these choices can be gathered into a submenu to avoid crowding the regular context menu. A plain text message 702 can be highlighted, at 710. Sign and Encrypt 720 can be selected to both encrypt and digitally sign the message 702. The result can be an encrypted and signed message 801 as illustrated in FIG. 8.

[0040] Some embodiments of the disclosed subject matter can be used to encrypt, decrypt, and/or control access to portions of a document and/or communication. Some embodiments can function with, for example, an integrated development environment (IDE) and/or a revision control system. For example, assume multiple entities are working on software project. If a first entity does not wish a second entity to have access to certain portions of the source code, those portions can be encrypted with, for example, encryption keys. An entity with access to the encrypted source code can be provided with access to encrypted portions of the actual source code by providing the entity with the appropriate decryption key or keys. In some embodiments, a compiler may have access to all the keys so that, for example, an entity with keys to only some portions of the code, but with access to such a compiler, can compile and run the software. The compiler can be available to various of the multiple entities. Such embodiments can allow, for example, multiple entities to work together and still retain control over information that may otherwise need to be shared. The various entities can be, for example, users in the same system, users across multiple systems, companies, authors, programmers, and/or software applications.

[0041] One such embodiment is illustrated in FIG. 9. As shown, a first entity may create a first portion 991 of a document 990, at 910. Portion 991 can be encrypted, at 920, and document 990 can be sent, at 930, to a second entity that can create and encrypt a second portion 992 of the document 990, at 940, but not have a key to decrypt portion 991 created by the first entity. The document can then be sent, at 950, to a third entity that has keys to decrypt portions 991 and 992. The third entity can decrypt the document, at 960, and possibly perform an action on the document, such as, for example, compiling or reading the document. Some embodiments can insert tags (e.g., div tags) into a document to separate the document into various portions that can be encrypted and decrypted using various keys.

[0042] 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, which is limited only by the claims that follow. Features of the disclosed embodiments can be combined and rearranged in various ways within the scope and spirit of the invention.

What is claimed is:

1. A method for inhibiting attacks on data, comprising:

receiving data and at least one indication indicating that the data is encrypted in an unprotected environment in a web browser;

determining whether the at least one indication indicates that the portion of the data is encrypted;

creating a protected environment in the web browser;

automatically making the data available to the protected environment;

decrypting the data to form decrypted data in the protected environment; and

displaying the decrypted data in the protected environment.

2. The method of claim 1, wherein the data is at least part of an HTML document.

3. The method of claim 1, wherein the at least one indication is a div tag or a span tag.

4. The method of claim 1, wherein the at least one indication is a location.

5. The method of claim 1, wherein the protected environment is a frame.

6. The method of claim 1, wherein the protected environment disables scripts.

7. A method for inhibiting attacks on data, comprising:

creating a protected environment in a web browser;

receiving data in the protected environment;

encrypting the data to form encrypted data in the protected environment;

associating the encrypted data with an indication that the encrypted data is encrypted; and

automatically making the encrypted data and the indication accessible to an unprotected environment in the web browser.

8. The method of claim 7, further comprising receiving highlighting of the data and receiving instruction that the data is to be encrypted.

9. The method of claim 7, further comprising receiving highlighting of the data and receiving instruction that the data is to be encrypted and signed.

10. The method of claim 7, further comprising adding random data to the data in the protected environment.

11. The method of claim 7, wherein the indication is a div tag or a span tag.

12. The method of claim 7, wherein the indication is a location.

13. The method of claim 7, wherein the protected environment is a frame.

14. The method of claim 7, wherein the protected area disables scripts.

15. A computer-readable medium containing computer-executable instructions that, when executed by a processor, cause the processor to perform a method for inhibiting attacks on data, comprising:

receiving data and at least one indication indicating that the data is encrypted in an unprotected environment in a web browser;

determining whether the at least one indication indicates that the portion of the data is encrypted;

creating a protected environment in the web browser;

automatically making the data available to the protected environment;

decrypting the data to form decrypted data in the protected environment; and

displaying the decrypted data in the protected environment.

16. The medium of claim 15, wherein the data is at least part of an HTML document.

17. The medium of claim 15, wherein the at least one indication is a div tag or a span tag.

18. The medium of claim 15, wherein the at least one indication is a location.

19. The medium of claim 15, wherein the protected environment is a frame.

20. The medium of claim 15, wherein the protected environment disables scripts.

21. A computer-readable medium containing computer-executable instructions that, when executed by a processor, cause the processor to perform a method for inhibiting attacks on data, comprising:

creating a protected environment in a web browser;

receiving data in the protected environment;

encrypting the data to form encrypted data in the protected environment;

associating the encrypted data with an indication that the encrypted data is encrypted; and

automatically making the encrypted data and the indication accessible to an unprotected environment in the web browser.

22. The medium of claim 21, wherein the method further comprises receiving highlighting of the data and receiving instruction that the data is to be encrypted.

23. The medium of claim 21, wherein the method further comprises receiving highlighting of the data and receiving instruction that the data is to be encrypted and signed.

24. The medium of claim 21, wherein the method further comprises adding random data to the data in the protected environment.

25. The medium of claim 21, wherein the indication is a div tag or a span tag.

26. The medium of claim 21, wherein the indication is a location.

27. The medium of claim 21, wherein the protected environment is a frame.

28. The medium of claim 21, wherein the protected area disables scripts.

29. A system for inhibiting attacks on data, comprising:

an interface in communication with a network;

a memory; and

a processor in communication with the memory and the interface; wherein the processor:

receives data and at least one indication indicating that the data is encrypted in an unprotected environment in a web browser;

determines whether the at least one indication indicates that the portion of the data is encrypted;

creates a protected environment in the web browser;

automatically makes the data available to the protected environment;

decrypts the data to form decrypted data in the protected environment; and

displays the decrypted data in the protected environment.

30. The system of claim 29, wherein the data is at least part of an HTML document.

31. The system of claim 29, wherein the at least one indication is a div tag or a span tag.

32. The system of claim 29, wherein the at least one indication is a location.

33. The system of claim 29, wherein the protected environment is a frame.

34. The system of claim 29, wherein the protected environment disables scripts.

35. A system that for inhibiting attacks on data, comprising:

an interface in communication with a network;

a memory; and

a processor in communication with the memory and the interface; wherein the processor:

creates a protected environment in a web browser;

receives data in the protected environment;

encrypts the data to form encrypted data in the protected environment;

associates the encrypted data with an indication that the encrypted data is encrypted; and

automatically makes the encrypted data and the indication accessible to an unprotected environment in the web browser.

36. The system of claim 35, wherein the process further receives highlighting of the data and receiving instruction that the data is to be encrypted.

37. The system of claim 35, wherein the process further receives highlighting of the data and receiving instruction that the data is to be encrypted and signed.

38. The system of claim 35, wherein the process further adds random data to the data in the protected environment.

39. The system of claim 35, wherein the indication is a div tag or a span tag.

40. The system of claim 35, wherein the indication is a location.

41. The system of claim 35, wherein the protected environment is a frame.

42. The system of claim 35, wherein the protected area disables scripts.

43. A method for inhibiting attacks on data, comprising:

receiving data from a first entity comprising at least a message and an encrypted account number;

determining, based on the message, whether the encrypted account number needs to be authorized;

if the encrypted account number needs to be authorized, making the encrypted account number available to a second entity;

receiving authorization from the second entity; and

sending a response to the first entity based on the message and the authorization.

44. The method of claim 43, wherein the message is a product request.

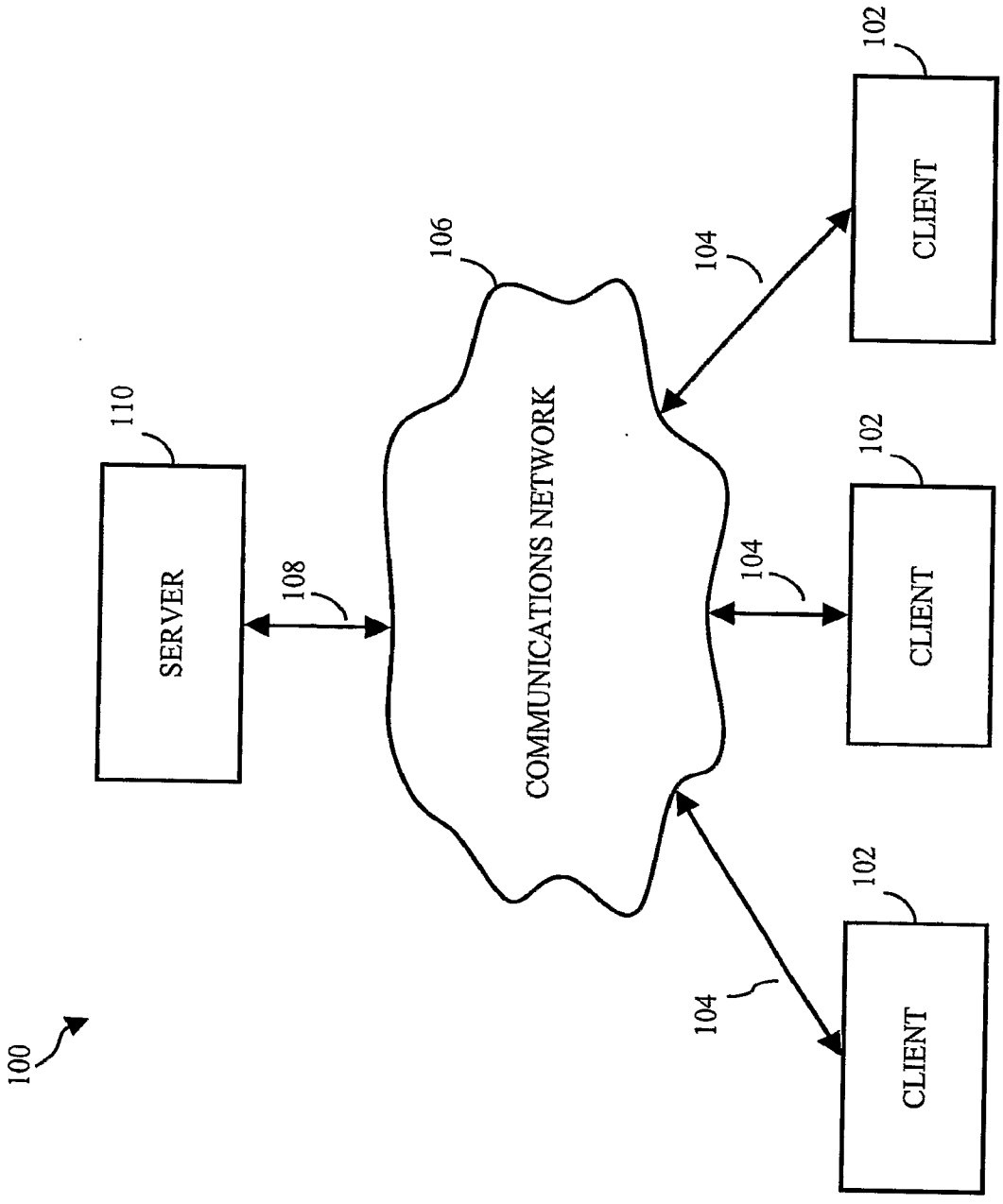

100
SERVER
110
108
COMMUNICATIONS NETWORK
106
104
CLIENT
102
104
CLIENT
102
104
CLIENT
102

FIG. 1

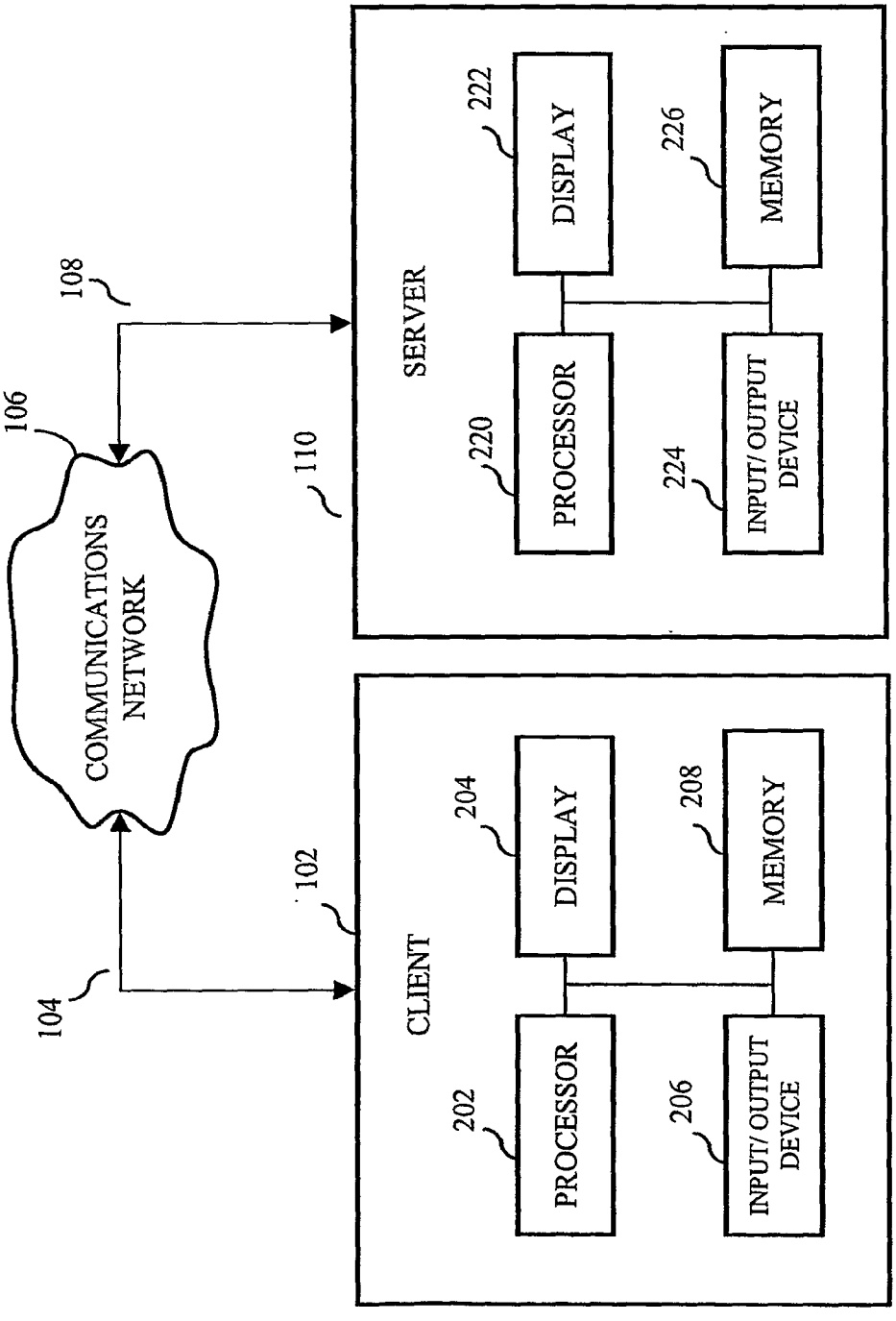

104
106
108
COMMUNICATIONS NETWORK
102
CLIENT
202
PROCESSOR
204
DISPLAY
206
INPUT/ OUTPUT DEVICE
208
MEMORY
110
SERVER
220
PROCESSOR
222
DISPLAY
224
INPUT/ OUTPUT DEVICE
226
MEMORY

FIG. 2

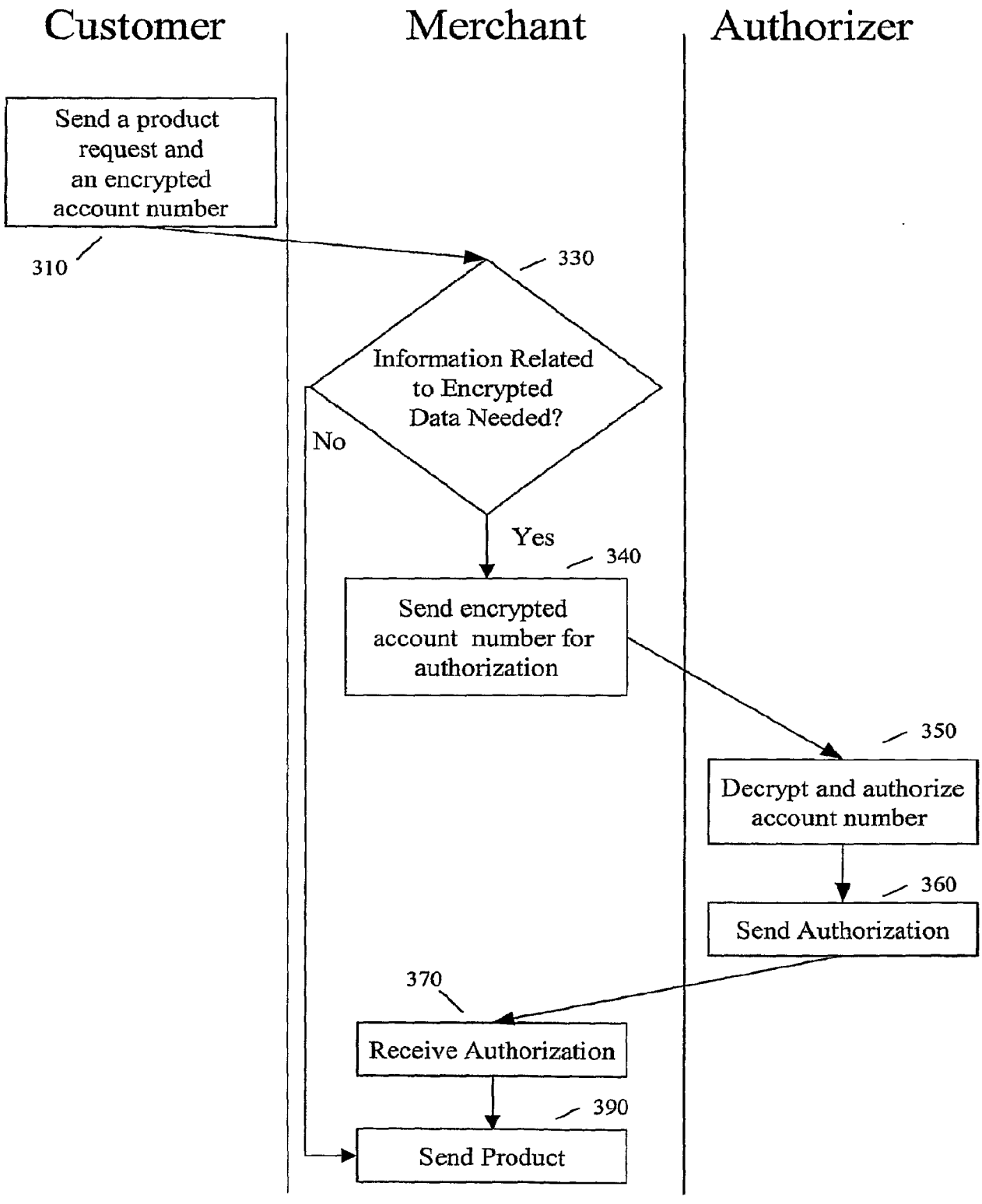

Customer
Merchant
Authorizer
Send a product request and an encrypted account number
310
330
Information Related to Encrypted Data Needed?
No
Yes
340
Send encrypted account number for authorization
350
Decrypt and authorize account number
360
Send Authorization
370
Receive Authorization
390
Send Product

FIG. 3

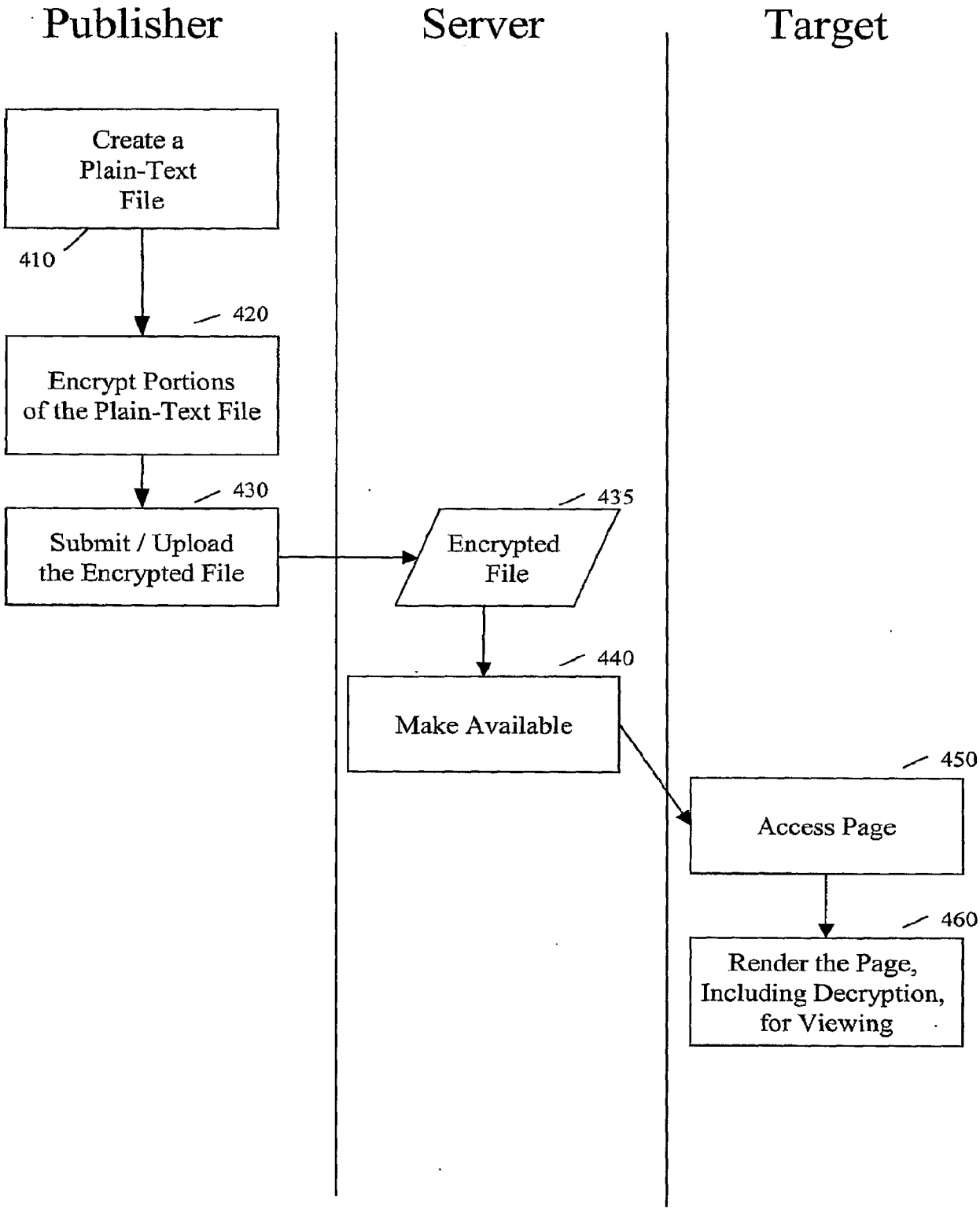

Publisher
Server
Target
Create a Plain-Text File
410
420
Encrypt Portions of the Plain-Text File
430
Submit / Upload the Encrypted File
435
Encrypted File
440
Make Available
450
Access Page
460
Render the Page, Including Decryption, for Viewing

FIG. 4

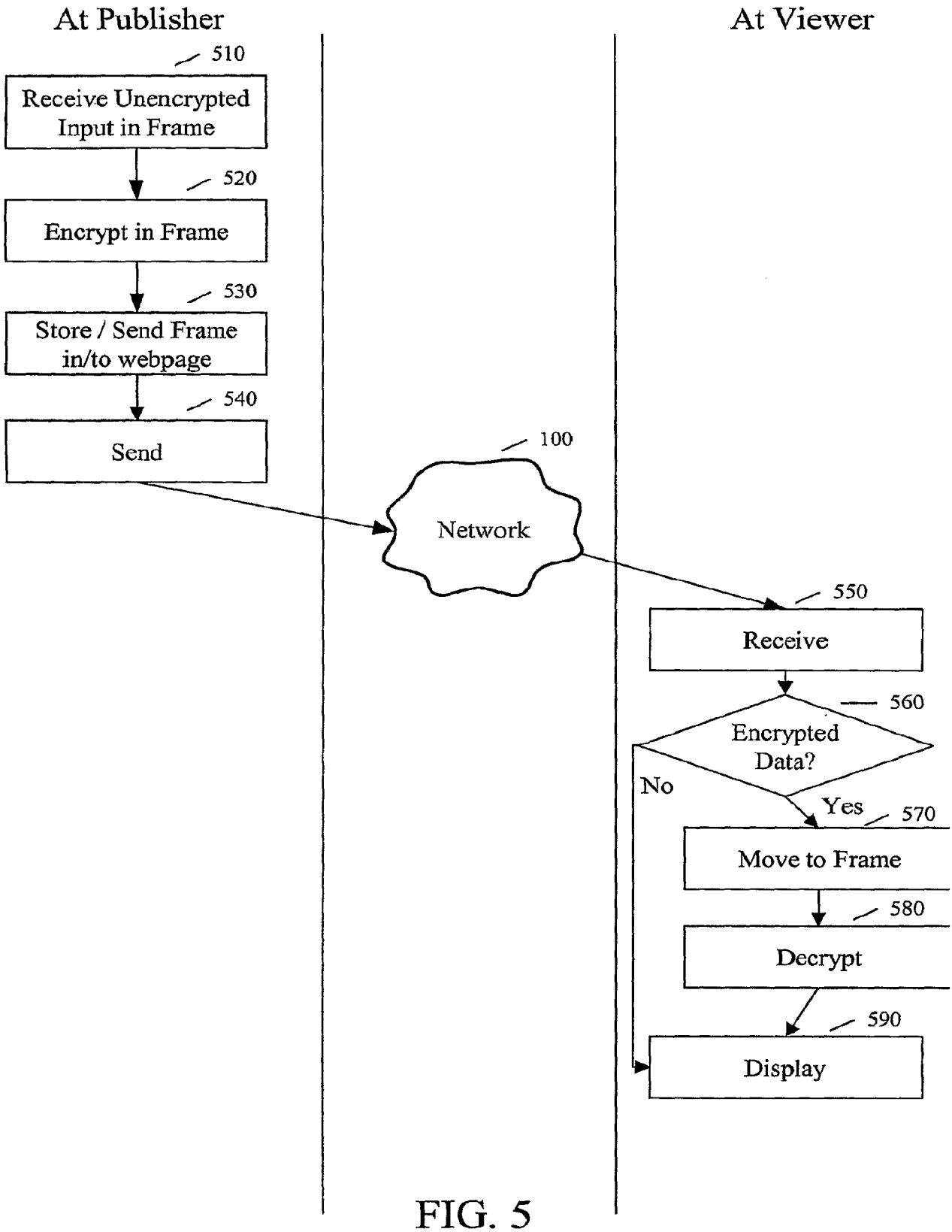

At Publisher
At Viewer
510
Receive Unencrypted Input in Frame
520
Encrypt in Frame
530
Store / Send Frame in/to webpage
540
Send
100
Network
550
Receive
560
Encrypted Data?
No
Yes
570
Move to Frame
580
Decrypt
590
Display

FIG. 5

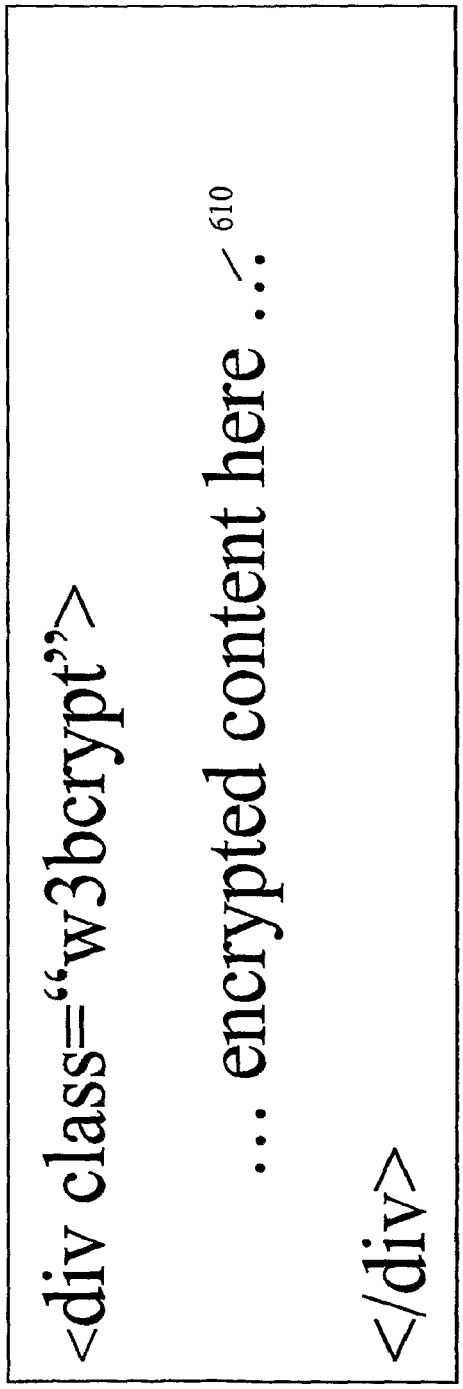


FIG. 6

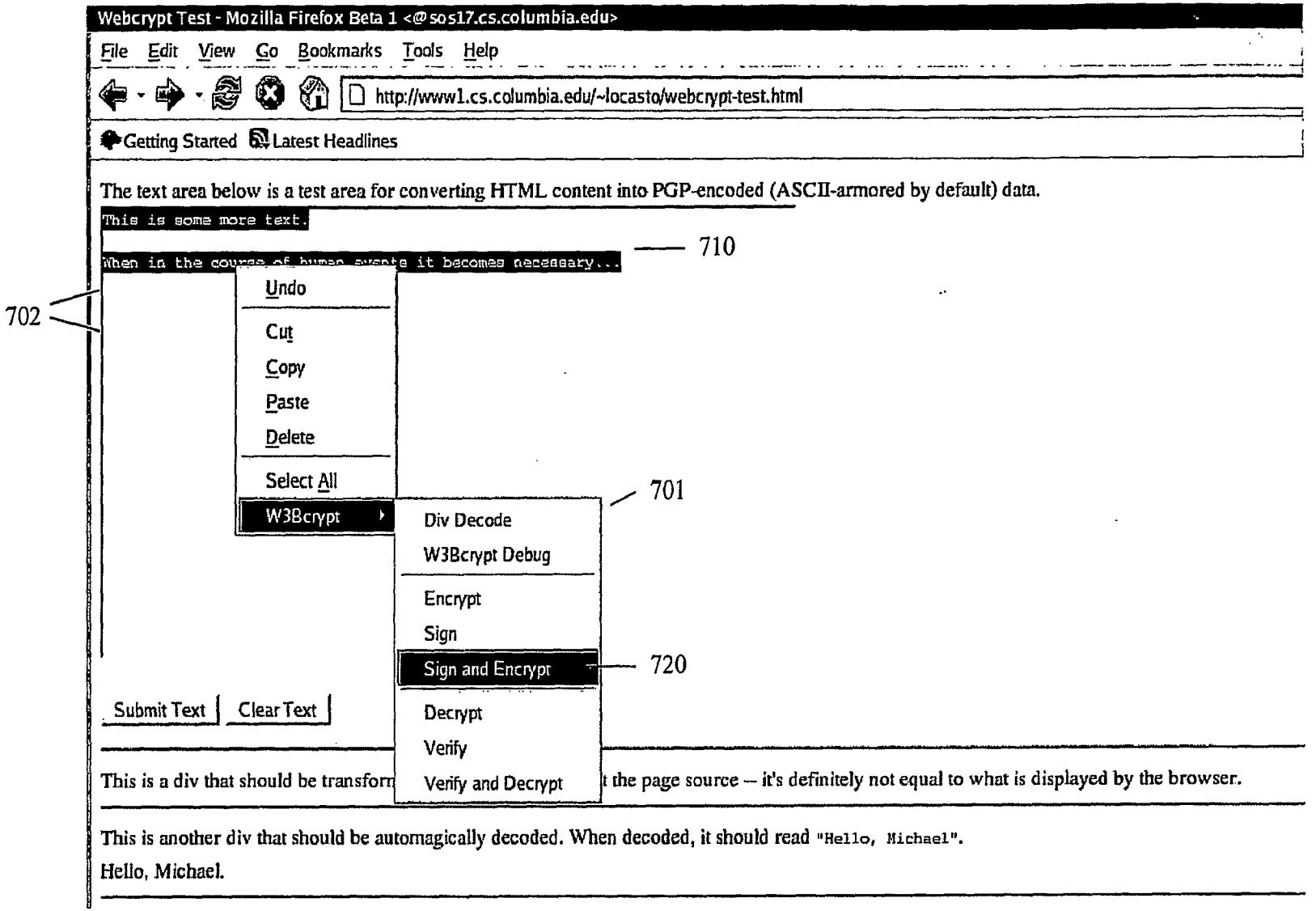
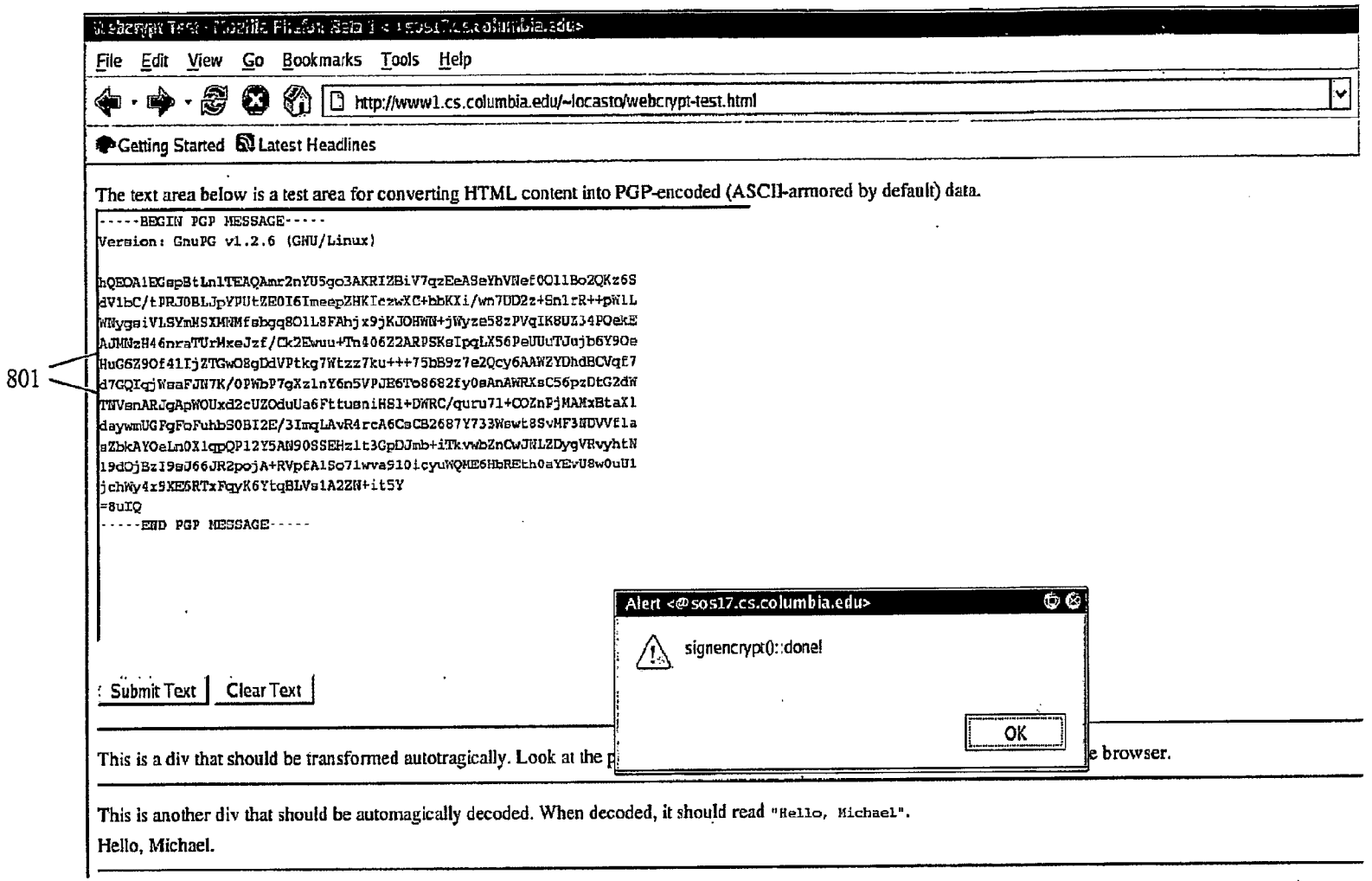


FIG. 7



801

FIG. 8

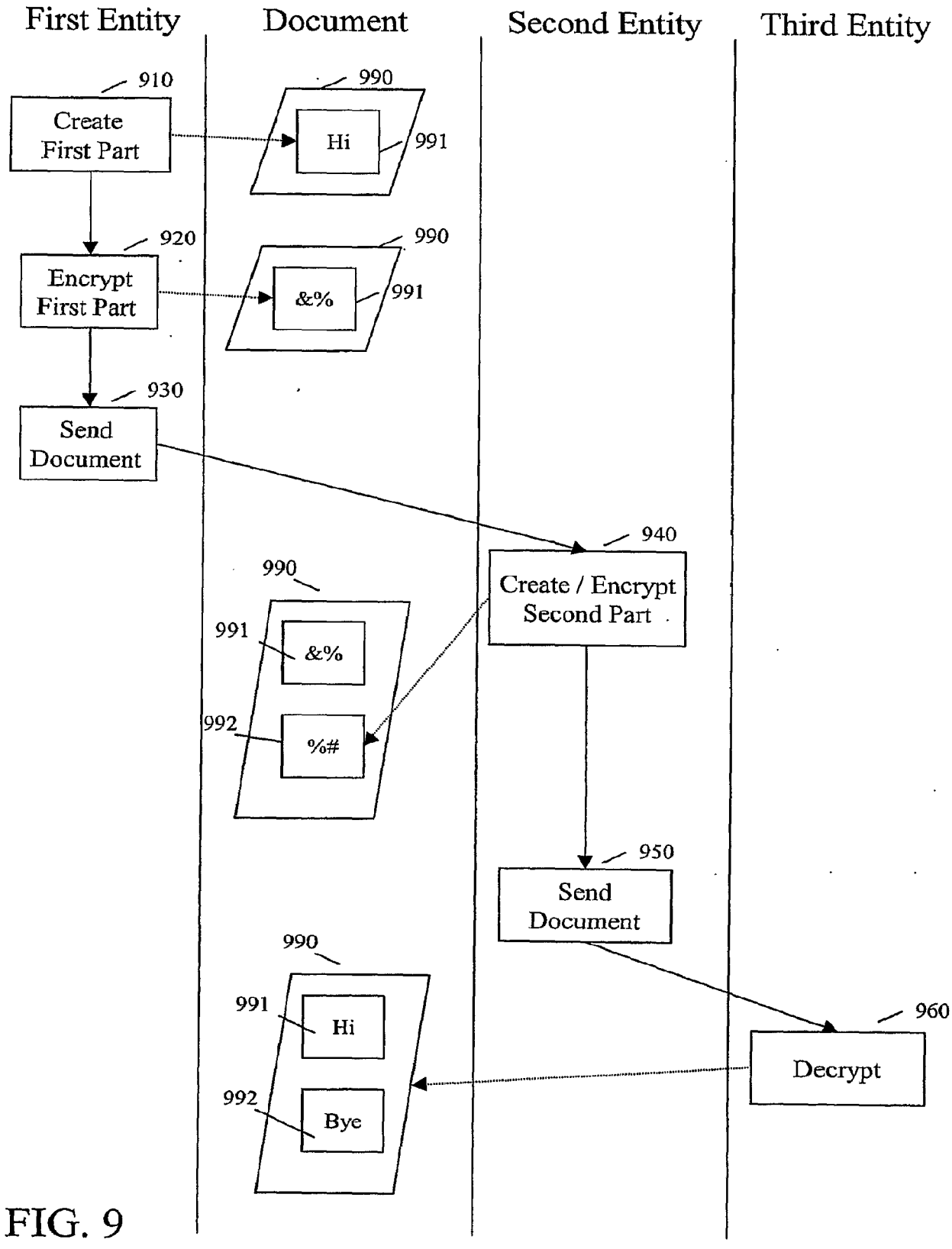

First Entity
Document
Second Entity
Third Entity
910
Create First Part
990
Hi
991
920
Encrypt First Part
990
&%
991
930
Send Document
940
Create / Encrypt Second Part
990
991
&%
992
%#
950
Send Document
990
991
Hi
992
Bye
960
Decrypt

FIG. 9