(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2004-502379
(P2004-502379A)
(43)公表日　平成16年1月22日(2004.1.22)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/16	H04L 9/00	643	5B017
G06F 12/14	G06F 12/14	310K	5J104
H04L 9/08	G06F 12/14	320B	
	H04L 9/00	601F	

審査請求 未請求　予備審査請求 未請求　（全 29 頁）

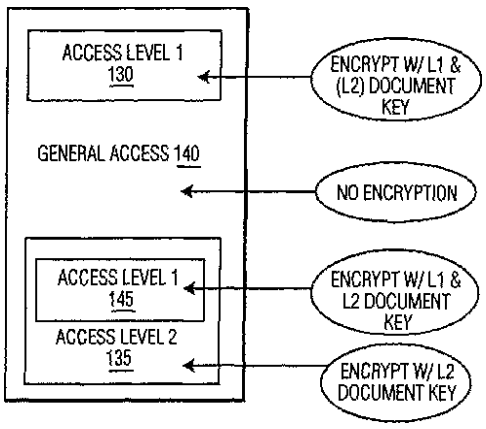
(21)出願番号　特願2002-506149(P2002-506149)
(86)(22)出願日　平成13年6月22日(2001.6.22)
(85)翻訳文提出日　平成14年2月27日(2002.2.27)
(86)国際出願番号　PCT/EP2001/007090
(87)国際公開番号　WO2002/001271
(87)国際公開日　平成14年1月3日(2002.1.3)
(31)優先権主張番号　09/606,339
(32)優先日　平成12年6月29日(2000.6.29)
(33)優先権主張国　米国(US)
(81)指定国　EP(AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),CN,JP,KR

(71)出願人　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
Ｋｏｎｉｎｋｌｉｊｋｅ　Ｐｈｉｌｉｐｓ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｎ．Ｖ．
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　１
Ｇｒｏｅｎｅｗｏｕｄｓｅｗｅｇ　１，５６２１　ＢＡ　Ｅｉｎｄｈｏｖｅｎ，Ｔｈｅ　Ｎｅｔｈｅｒｌａｎｄｓ
(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】多重レベルアクセス特権を付与する単一文書の多重暗号化

(57)【要約】
文書の種々のセクションを選択的に暗号化し復号化する方法及びシステムは、種々の鍵を利用する技術において種々のアクセスレベルを与える。文書は、文書セクションレベル（ここで、「セクション」は一般的な意味で使用されている）で暗号化され、セクション毎に語となる暗号鍵の組を使用する。アクセスレベル１をもつユーザＡは、アクセスレベル１で符号化されたセクションと、暗号化されていないセクションとだけを利用する。本技術のアプリケーション例は病院である。患者の記録は、看護師には適切な素材だけへのアクセスを許可し、医師にはより広いアクセスを許可するように別々に暗号化された部分に区分される。看護師は、自分に権利が与えられている文書の部分にアクセスできるように自分のアクセスレベル秘密鍵が与えられる。プラマリ・ケア医師又は健康ケア・プロキシだけが権利を与えられているレベルも存在する。



【特許請求の範囲】
【請求項１】
第１の文書を安全に送る方法であって、
第１レベルの文書鍵及び第２レベルの文書鍵を生成する手順と、
該第１の文書の第１セクションを該第１レベルの文書鍵で暗号化し、該第１の文書の第２セクションを該第２レベルの文書鍵で暗号化する手順と、
該第１レベルの文書鍵及び該第２レベルの文書鍵を収容する第２の文書又は該第１の文書の一部を形成する手順と、
該第２の文書又は該第１の文書の一部を形成する手順における選択に応じて、該第１の文書又は該第１の文書及び該第２の文書を送る手順と、
を有する方法。
【請求項２】
該第１レベルの文書鍵及び該第２レベルの文書鍵は対称鍵である、請求項１記載の方法。
【請求項３】
受取側から少なくとも二つの公開鍵を受け取る手順を更に有し、
該第２の文書又は該第１の文書の一部を形成する手順は、該第１レベルの文書鍵及び該第２レベルの文書鍵の対応した組が該少なくとも二つの公開鍵の中の一方を用いる復号化によって利用可能にされ、該第１レベルの文書鍵及び該第２レベルの文書鍵の対応した別の組が該少なくとも二つの公開鍵の中の他方を用いる復号化によって利用可能にされるように、該第２の文書を暗号化する手順を含む、
請求項１記載の方法。
【請求項４】
該第２の文書を暗号化する手順は、
該第２の文書の第１の部分又は第１の文書部分における該少なくとも二つの公開鍵の一方を暗号化する手順と、
該第２の文書の第２の部分又は第１の文書部分における該少なくとも二つの公開鍵の両方を暗号化する手順と、
を含む、
請求項３記載の方法。
【請求項５】
該第１レベルの文書鍵及び該第２レベルの文書鍵は対称鍵である、請求項３記載の方法。
【請求項６】
該文書を送る手順は、該第２の文書又は該第１の文書の一部を形成する手順における選択に応じて、該第１の文書、又は、該第１の文書及び該第２の文書を暗号化する手順を含む、請求項１記載の方法。
【請求項７】
文書を暗号化する方法であって、
第１の鍵を用いて文書の第１の部分を暗号化する第１の手順と、
第２の鍵を用いて該文書の第２の部分を暗号化する第２の手順と、
受信側の公開鍵である第３の鍵を用いて、該第１の手順及び該第２の手順の結果を暗号化する手順と、
を有する文書を暗号化する方法。
【請求項８】
該第１の鍵は該受信側の第１の公開鍵であり、該第２の鍵は該受信側の第２の公開鍵である、請求項７記載の文書を暗号化する方法。
【請求項９】
該第１の鍵は第１の対称鍵であり、該第２の鍵は第２の対称鍵であり、
公開鍵を用いて該第１の対称鍵を暗号化する手順を更に有する、
請求項７記載の文書を暗号化する方法。
【請求項１０】

該第２の部分は該第１の部分の一部分を含み、
該一部分は該第１の対称鍵で暗号化されている、
請求項９記載の文書を暗号化する方法。
【請求項１１】
第２の公開鍵を用いて該第２の対称鍵を暗号化する手順を更に有する、請求項９記載の文書を暗号化する方法。
【請求項１２】
文書の第１の受け手側及び第２の受け手側に安全に文書にアクセスさせる方法であって、
該文書の受け手側に対応し該文書を暗号化するため使用される公開鍵を、文書の送り手側へ送る手順と、
該送り手側から暗号化されたデータを受ける手順と、
該公開鍵の一方に対応した秘密鍵を用いて該暗号化されたデータの一部分を復号化する第１の手順と、
該第１の手順の結果として、該公開鍵の該一方に対応した該データの一部分にアクセスする手順と、
該公開鍵の他方に対応した秘密鍵を用いて該暗号化されたデータの一部分を復号化する第２の手順と、
該第２の手順の結果として、該公開鍵の該他方に対応した該データの一部分にアクセスする手順と、
を有する方法。
【請求項１３】
該第１の手順及び該第２の手順は、暗号鍵の対応した組を開くため、該データの一部分を復号化する手順を含む、請求項１２記載の方法。
【請求項１４】
該第１の手順及び該第２の手順は、該文書の一部分だけへのアクセスを許可すべく、該暗号化されたデータの少なくとも一部分を開くため、暗号鍵の該対応した組を使用する手順を含む、
請求項１２記載の方法。
【請求項１５】
該第１の手順及び該第２の手順は、該文書へのアクセスを許可すべく、該暗号化されたデータの少なくとも一部分を開くため、暗号鍵の該対応した組を使用する手順を含む、
請求項１２記載の方法。
【請求項１６】
鍵部分及び暗号文書部分を含む暗号保護付き文書を収容し、
該鍵部分は、第１の対称鍵にアクセスするため、第１の公開鍵を用いて少なくとも部分的に復号化可能であり、
該鍵部分は、第２の対称鍵にアクセスするため、第２の公開鍵を用いて少なくとも部分的に復号化可能であり、
該暗号文書部分の第１の部分は、該第１の対称鍵を用いて復号化可能であり、
該暗号文書部分の第２の部分は、該第２の対称鍵を用いて復号化可能である、データファイル。
【請求項１７】
暗号文書及び少なくとも二つの暗号鍵を収容し、
該暗号鍵は、少なくとも二つの公開鍵を用いてアクセスできるように暗号化され、
該暗号文書の第１の部分は、該少なくとも二つの公開鍵のうちの一方を用いて復号化可能である該暗号鍵の第１の部分集合を用いて復号化することによりアクセス可能であり、
該暗号文書の第２の部分は、該少なくとも二つの公開鍵のうちの他方を用いて復号化可能である該暗号鍵の第２の部分集合を用いて復号化することによりアクセス可能である、
データファイル。
【請求項１８】

部分毎に対応した鍵を用いて暗号化された文書を含み、
該文書の第１の部分は、該対応した鍵のうちの第１の鍵を用いて暗号化され、
該文書の第２の部分は、該対応した鍵のうちの第２の鍵を用いて暗号化され、
該第１の鍵及び該第２の鍵は、第１の秘密鍵によって該第１の鍵を復号化することができ、第２の秘密鍵によって該第２の鍵を復号化することができるように、ファイル内で暗号化されている、
データ記憶媒体に格納されたデータセット。
【請求項１９】
部分毎に対応した鍵を用いて暗号化された文書を含み、
該文書の第１の部分は、該対応した鍵のうちの第１の鍵及び第２の鍵を用いて暗号化され、
該文書の第２の部分は、該対応した鍵のうちの該第１の鍵を用いて暗号化され、
該第１の鍵及び該第２の鍵は、第１の秘密鍵によって該第１の鍵及び該第２の鍵を復号化することができ、第２の秘密鍵によって該第１の鍵を復号化することができるように、ファイル内で暗号化されている、
データ記憶媒体に格納されたデータセット。
【請求項２０】
各鍵を用いて復号化することによって更なる各鍵の組が得られるデータセットの一部分を選択的に復号化するプロセスを定義するコードと、
各鍵に対応した該文書の一部分だけにアクセスできるようにするため、該データセットから該更なる各鍵の組に対応した文書の部分を獲得する更なるプロセスを定義するコードと、
を含む、データ記憶媒体に格納された文書復号化プログラム。
【請求項２１】
該各鍵は公開鍵である、請求項２０記載の文書復号化プログラム。
【請求項２２】
該更なる鍵の組の各鍵は該文書に対して固有の鍵である、請求項２０記載の文書復号化プログラム。
【発明の詳細な説明】
【０００１】
［発明の背景］
［発明の分野］
本発明は、文書暗号化及び文書に関するアクセス制限に係り、特に、暗号化された文書の部分へのアクセス権が対応した鍵によって獲得される文書の部分毎の暗号化に関する。
【０００２】
［背景技術］
文書アクセス保護に関する多数の技術が公知である。一例として、文献：ＥＰ ０ ８４８ ３１４ Ａ１，”ＤＯＣＵＭＥＮＴ ＳＥＣＵＲＩＴＹ ＳＹＳＴＥＭ ＡＮＤ ＭＥＴＨＯＤ”では、ユーザが権利をもつ文書だけがデータベースから生成される。可変のセキュリティレベルが与えられる。米国特許第５，０５２，０４０号、”ＭＵＬＴＩＰＬＥ ＵＳＥＲ ＳＴＯＲＥＤ ＤＡＴＡ ＣＲＹＰＴＯＧＲＡＰＨＩＣ ＬＡＢＥＬＬＩＮＧ ＳＹＳＴＥＭ ＡＮＤ ＭＥＴＨＯＤ”に記載された別のシステムは、種々のユーザが同じファイルを利用することを許容する。このシステムは、コンフィギュレーション能力と、ユーザの権利及び特権を含むファイルラベルの拡張を利用する。この例における別々のユーザの権利及び特権は、読み出し専用、読み書き、削除などのように文書全体に関係する。文書は暗号化される。別の従来技術のシステムは、米国特許第６，００１，８４７号、”ＣＲＹＰＴＯＧＲＡＰＨＩＣ ＡＣＣＥＳ ＡＮＤ ＬＡＢＥＬＩＮＧ ＳＹＳＴＥＭ”に記載されている。このシステムの場合、ファイルの暗号化及び復号化は、システムによって生成された関係鍵を使用する。コンピュータプログラムは、暗号化され、暗号化されたメッセージへの終端部（トレーラ）として付加された一連のラベルを生成する。暗号化された

ラベルは、特定の暗号化の来歴を与え、全ファイルから個別に選択され、分離され、復号化される。アクセス制御モジュールは、生成されたベクトル若しくは鍵を、フレキシブルディスクのような可搬型記憶媒体に格納された第２のベクトル若しくは鍵の部分的に復号化された変形バージョンと比較することにより、ユーザにパスフレーズによる文書の暗号部分へのアクセスを許可する。これに応答して、主鍵は、ラベルを暗号化若しくは復号化するため生成される。後者のシステムは、主として、記述的なラベルを暗号化された文書の最後に付加することに関心があり、サーバーとクライアントの間で記述鍵を渡す鍵交換方法を含む。

【０００３】

その他の従来技術によるシステム及び方法が公知ではあるが、アクセス特権に基づいて文書の種々の部分の暗号化・保護を行なう非常に便利で、頑強性があり、かつ、簡単な方法は存在しない。

【０００４】

［発明の概要］

文章の種々のセクションを選択的に暗号化し復号化する方法及びシステムは、種々の鍵を利用する技術において、種々のアクセスレベルを実現する。文書は、文書セクションレベル（ここで、「セクション」は一般的な意味で使用されている）で暗号化され、セクション毎に語となる暗号鍵の組を使用する。アクセスレベル１をもつユーザＡは、アクセスレベル１で符号化されたセクションと、暗号化されていないセクションとだけを利用する。本技術のアプリケーション例は病院である。患者の記録は、看護師には適切な素材だけへのアクセスを許可し、医師にはより広いアクセスを許可するように別々に暗号化された部分に区分される。このようにして、本例は、特定の環境内で認められた予め決められた役割に基づく、文書に含まれる情報へのアクセス制御を例示する。看護師は病院によって決められたアクセス制御ルールに基づいてアクセスレベル鍵が付与される。プラマリ・ケア医師又は健康ケア・プロキシだけが権利を与えられているレベルも存在する。

【０００５】

鍵を識別する方法も提供される。この方法は、文書のセクションを符号化するため使用される鍵を保持するため作成された鍵ボックスを利用する。鍵ボックスは、アクセスレベル毎にスロットを格納する。所与のレベルのユーザが必要とする鍵の組が対応したスロットに収容される。各スロットは、ユーザの秘密鍵を用いて復号化したときにユーザに適切なスロット内の鍵へのアクセスを許可するアクセスレベル公開鍵を用いて符号化される。

【０００６】

更なる特徴によれば、要求側機関に対する公開鍵を用いる暗号化の外層が得られる。要求側機関が自分の秘密鍵を用いて文書を開くと、受信側機関の人は誰でも自分のアクセスレベル秘密鍵を鍵ボックスへ適用することができ、次に、対応したスロット内の鍵を文書に適用する。これにより、各ユーザは、自分がアクセス権を保有する文書の一部を閲覧、変更することが可能になる。

【０００７】

以下では、ある種の好ましい実施例に関して、理解がより深まるように例示的な添付図面を参照して、本発明を説明する。本発明の説明では、非対称アルゴリズムを実現するため従来技術において使用される公開・秘密鍵ペアの公開部に対応させるため、公開鍵の定義を使用する。本発明の説明は、非対称アルゴリズムを実現するため従来技術において使用される公開・秘密鍵ペアの秘密部に対応させるため、秘密鍵の定義を使用する。本発明の説明は、対称アルゴリズムを実現するため従来技術において使用される単一鍵を表わすため、対称鍵の定義を使用する。

【０００８】

図面に関しては、図示された具体例は、例示として用いられて、本発明の好ましい実施例を具体的に説明することだけを意図し、本発明の原理及び概念的な局面が最も有効に、かつ、最も容易に理解できるように提示されている。この点に関して、本発明の構造的な細部は、本発明の基本的な理解に必要な程度以上には図示されていない。添付図面を参照し

て以下の詳細な説明を読むことによって、当業者は、本発明の幾つかの実施形態を実際に実現できることが明らかである。

【０００９】

［好ましい実施例の詳細な説明］

図１によれば、本発明は、電子文書転送の環境で使用される。このような環境の一例は、ネットワーク１００によって、或いは、フレキシブルディスクのような不揮発性データ記憶装置９０の物理的な運搬によって接続された送信側コンピュータ１１０及び受信側コンピュータ１２０である。

【００１０】

図２Ａを参照するに、文書９５は、種々のセクション１３０、１３５、１４０及び１４５を含む。各セクションは、セクションに含まれる情報が特定の人（機関若しくはその他の実体）或いは人のクラスによってアクセスできるようにするために望ましい方式に従って区分される。文書９５は、送信側１１０によって受信側１２０へ転送されるよう意図されている。受信側は、各人又は人のクラスを含む。セクション１３０及び１４５は、第１のユーザ若しくはユーザクラスに値対応した公開鍵Ｌ１によって暗号化される。セクション１３５は、第２のユーザ若しくはユーザクラスに対応した公開鍵Ｌ２によって暗号化される。セクション１４５は、セクション１３５に埋め込まれているため、Ｌ２公開鍵を用いて暗号化される。

【００１１】

図２Ｂを参照するに、種々のセクションは、対応したアクセスレベルから最低のアクセスレベルまでの全てのアクセスレベルからの１個の鍵だけ、又は、全ての鍵を用いて暗号化される。かくして、本例の場合、文書セクション１４５は、Ｌ１鍵及びＬ２鍵の両方を用いて暗号化され、文書１３０はそうではない。或いは、各セクションは、唯一の鍵によって暗号化されるので、レベル２セクションに現れるレベル１セクションは、レベル２とは全く別のセクションとして取り扱われ、Ｌ２暗号化に対するセクションとは別のセクションに分離される。上述の暗号方式は、意図された対象者の公開鍵に基づいて文書への多重レベルアクセスを認める。ユーザに基づいて、並びに、次の実施例で説明するように特定の文書に基づいてアクセスを制限することが可能である。

【００１２】

図３及び４を参照するに、文書セクションは、それぞれの文書鍵によって暗号化され、各文書鍵は文書の範囲内で定義された各アクセスレベルに対応する。文書鍵は対称鍵でもよい。対称鍵は、文書使用の前後関係の範囲外では共用されないので、ユーザは、対称鍵が何であるかを知る必要が無い。文書鍵は、文書鍵を別々の文書（図７に示されたファイルヘッダのように元の文書の一部でも構わない）に暗号化することにより、受信側で利用できるようにされる。鍵ボックスは、そのような文書を要求する機関の範囲内で定義された各アクセルレベルに対応したスロットを有する。第１のスロット１（２１０）は、ユーザに両方のレベルへのアクセスを許可するアクセスレベル１及び２に対する文書鍵を格納する。第２のスロット１（２１５）は、アクセスレベル２に対する文書鍵を格納する。各スロットは、スロットのアクセスレベルに対応した機関の公開鍵を用いて暗号化される。全鍵ボックスファイル及び文書は、文書及び鍵ボックスの伝送の機密性を保証するため、ユーザの公開鍵を用いて暗号化される。さらに、鍵ボックス及び文書は、文書の伝送の完全性及び真実性を保証するため、送信側１１０によって署名される。

【００１３】

上記の実施例は、暗号を準備する文書の送信側と、文書を受け取る機関との間に同意があることを前提としている。この同意によって、文書を暗号化する際に使用されるアクセスレベルは、受信側に与えられるアクセスレベルにマッピングされる。特定の文書に対し、特定の機関のレベルは、単一の文書アクセスレベルに位置付けられる。或いは、特定の機関のレベルは、多数の文書アクセスレベルに位置付けられる。

【００１４】

好ましくは、データの完全性及び否認防止を保証するため、文書供給側は、秘密鍵を用い

て文書にハッシュを署名する。これにより、文書を署名と共に受け取った要求側は、供給側の正当性を保証できる。文書のコンテンツを認証するその他のメカニズムも使用される。

【００１５】

アクセスレベルＮを与えられた人が文書を開くとき、その人は、対称鍵ペアに対応した自分の機関のアクセスレベル秘密鍵を、その鍵を用いて鍵ボックス内の適当なスロットへアクセスする復号化プロセスに提示する。対称鍵は、ユーザからは見えないように、文書の適切なレベルにアクセスするためプロセスによって使用される。ユーザは、対称文書鍵を決して取り扱うことが無く、自分がアクセスを許可されている文書の部分へアクセスするだけである。

【００１６】

図５を参照するに、文書を作成、送信、受信及び使用する詳細な手順は、ステップ１０で、文書及び適当な情報の要求を受信することで始まる。適当な情報には、ユーザの公開鍵、ユーザのアクセスレベルへのマップなどが含まれる。つぎに、ステップ２０で、要求されたアクセスレベル毎に鍵が作成される。ステップ３０において、文書は、次に、最上位（最高特権）アクセスレベルから始めて、徐々に下のレベルへ暗号化される。これにより、図２Ａ及び２Ｂの何れかの階層型暗号化が行なわれるか、或いは、各レベルが１回だけ暗号化される別のプロセスが行なわれる。鍵は鍵ボックス文書に形成され、各組はアクセスレベルの公開鍵を用いて別々に暗号化される（ステップ４５）。次に、文書及び鍵ボックスは、一つにまとめられ、受信側の公開鍵を用いて随意的に暗号化される（ステップ５５）。

【００１７】

受信側が暗号化された文書及び鍵ボックスを含むファイルを受け取ったとき、パッケージは、別々にされ、随意的に復号化される（ステップ６０）。文書及び鍵ボックスは、ユーザ側で利用できるようになる（ステップ７０）。ユーザが文書にアクセスしたとき、ユーザは、自分の機関のアクセスレベル秘密鍵を、受信側コンピュータ（たとえば、コンピュータ１２０）の復号化プロセスへ与え、受信側コンピュータは、鍵ボックスの適当なスロットを復号化するためこの鍵を使用する（ステップ７５）。このプロセスは、鍵ボックス内の復号化されたスロットから獲得された対称鍵を文書へ適用し（ステップ８０）、ユーザは文書にアクセスできるようになる（ステップ８５）。ユーザは、対称アクセスレベル鍵に直接アクセスすることはなく、或いは、自分にとって必要な鍵の個数を気にすることさえない。

【００１８】

図６を参照するに、他の一実施例において、受信側の公開鍵は、文書を暗号化するため使用されない。ステップ４５は飛ばされ、鍵ボックスは、機関の公開鍵だけを用いて暗号化される。受信側機関では、ステップ６５とステップ７０の間に更なるステップ９０が追加され、ステップ９０において、鍵ボックスのスロットが機関に存在するアクセスレベルへマッピングされ、ユーザ若しくはユーザのグループの適当な公開鍵を用いて暗号化される。

【００１９】

当業者には、本発明が上記の例示的な実施例の細部に限定されないこと、並びに、本発明は、本発明の精神若しくは不可欠な条件を逸脱することなく他の具体的な形態で実施され得ることが明らかである。したがって、本発明の実施例は、全ての観点において、上記の詳細な説明ではなく請求項に記載された事項によって示された発明の範囲を例示するものであり、限定するものではないと考えられるべきであり、また、請求項に記載された事項の均等物の意味及び範囲が請求項の記載に包摂されることが意図されている。

【図面の簡単な説明】

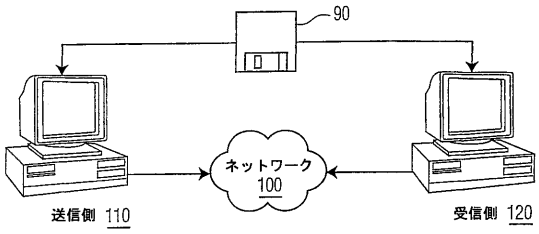
【図１】

本発明が使用されるコンピュータ環境を示す図である。

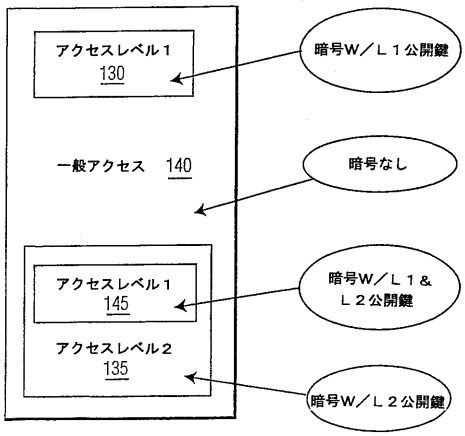
【図２Ａ】

暗号化のため公開鍵が使用される本発明の第１の実施例による別々のセクションを示す文書と各セクションに適用される暗号化処理とを示す図である。
【図２Ｂ】
暗号化のため公開鍵が使用される本発明の第２の実施例による別々のセクションを示す文書と各セクションに適用される暗号化処理とを示す図である。
【図３】
文書固有鍵が使用される本発明の第３の実施例による別々のセクションを示す文書と各セクションに適用される暗号化処理とを示す図である。
【図４】
図３の実施例と共に使用される鍵ボックス文書の説明図である。
【図５】
第１～第３の実施例と互換性のある一実施例による文書暗号化処理の説明図である。
【図６】
第１～第３の実施例と互換性のある一実施例による文書暗号化処理の説明図である。
【図７】
鍵ボックスを単一文書内に組み込むことにより伝送情報に鍵ボックスをパッケージングする他の方法の説明図である。

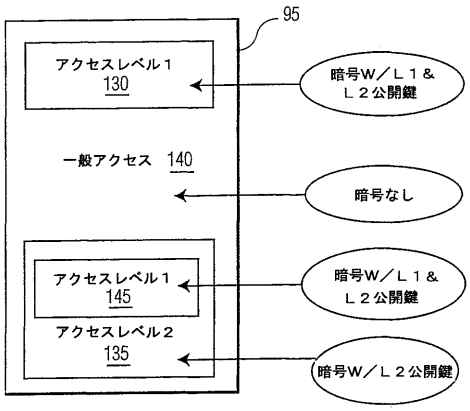
【図１】



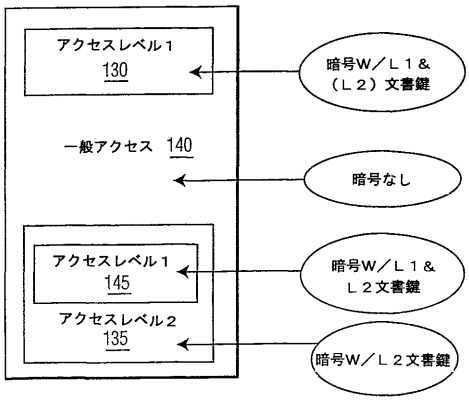
【図２Ａ】



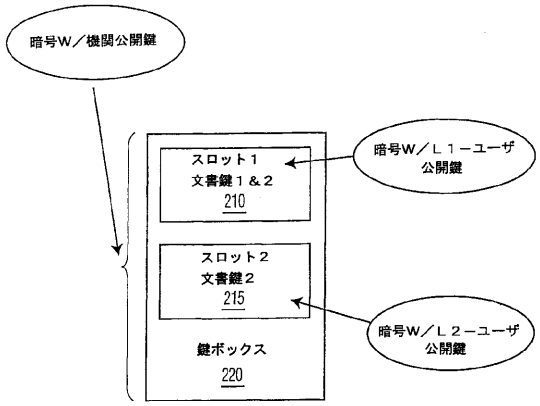
【図２Ｂ】



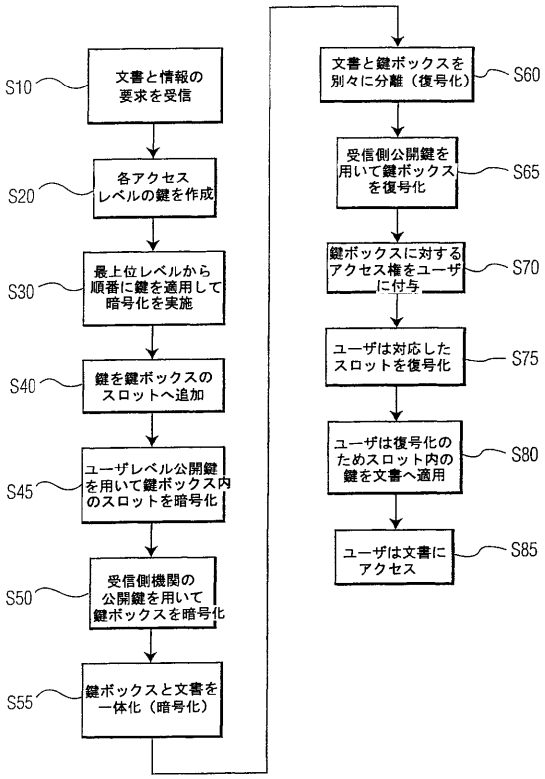
【図３】



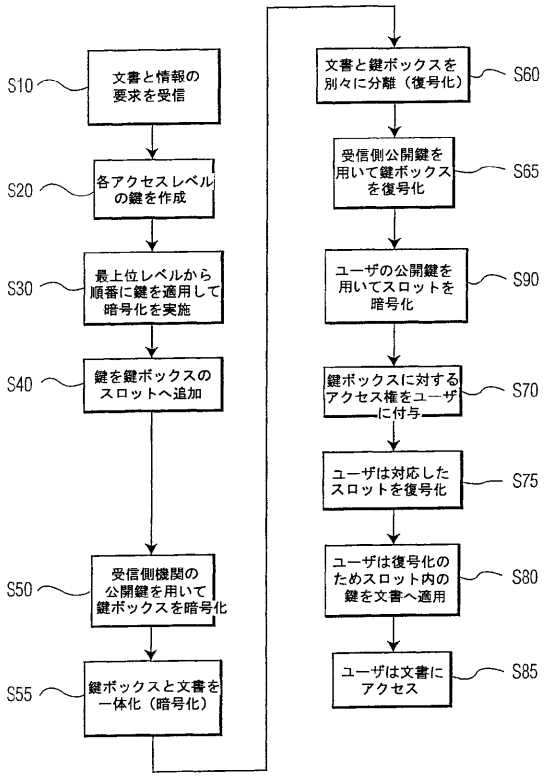
【図４】


暗号W／機関公開鍵
スロット１
文書鍵１＆２
210
暗号W／Ｌ１－ユーザ
公開鍵
スロット２
文書鍵２
215
暗号W／Ｌ２－ユーザ
公開鍵
鍵ボックス
220

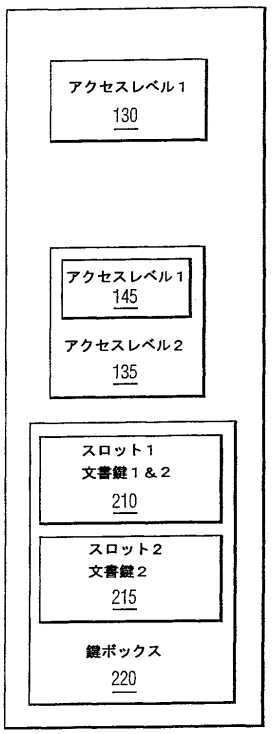
【図５】


S10
文書と情報の
要求を受信
S20
各アクセス
レベルの鍵を作成
S30
最上位レベルから
順番に鍵を適用して
暗号化を実施
S40
鍵を鍵ボックスの
スロットへ追加
S45
ユーザレベル公開鍵
を用いて鍵ボックス内
のスロットを暗号化
S50
受信側機関の
公開鍵を用いて
鍵ボックスを暗号化
S55
鍵ボックスと文書を
一体化（暗号化）
S60
文書と鍵ボックスを
別々に分離（復号化）
S65
受信側公開鍵を
用いて鍵ボックス
を復号化
S70
鍵ボックスに対する
アクセス権をユーザ
に付与
S75
ユーザは対応した
スロットを復号化
S80
ユーザは復号化の
ためスロット内の
鍵を文書へ適用
S85
ユーザは文書に
アクセス

【図６】


S10
文書と情報の
要求を受信
S20
各アクセスレベル
の鍵を作成
S30
最上位レベルから
順番に鍵を適用して
暗号化を実施
S40
鍵を鍵ボックスの
スロットへ追加
S50
受信側機関の
公開鍵を用いて
鍵ボックスを暗号化
S55
鍵ボックスと文書を
一体化（暗号化）
S60
文書と鍵ボックスを
別々に分離（復号化）
S65
受信側公開鍵を
用いて鍵ボックス
を復号化
S90
ユーザの公開鍵を
用いてスロットを
暗号化
S70
鍵ボックスに対する
アクセス権をユーザ
に付与
S75
ユーザは対応した
スロットを復号化
S80
ユーザは復号化の
ためスロット内の
鍵を文書へ適用
S85
ユーザは文書に
アクセス

【図７】


アクセスレベル１
130
アクセスレベル１
145
アクセスレベル２
135
スロット１
文書鍵１＆２
210
スロット２
文書鍵２
215
鍵ボックス
220

【国際公開パンフレット】

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2002 (03.01.2002)

PCT

(10) International Publication Number
WO 02/01271 A1

(51) International Patent Classification[7]: G02B 21/00, 21/16

(21) International Application Number: PCT/EP01/07090

(22) International Filing Date: 22 June 2001 (22.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/606,339 29 June 2000 (29.06.2000) US

(71) Applicant: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: **KRASINSKI, Raymond**; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **ROSNER, Martin**; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: **HOEKSTRA, Jelle**; Internationaal Octrooibureau B.V., Prof Holstlaan 6, NL-5656 AA Eindhoven (NL).

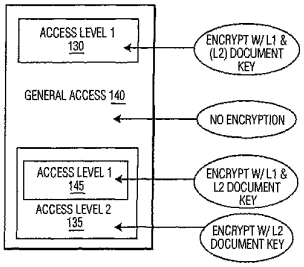
(81) Designated States *(national)*: CN, JP, KR.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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: MULTIPLE ENCRYPTION OF A SINGLE DOCUMENT PROVIDING MULTIPLE LEVEL ACCESS PRIVILEGES



(57) Abstract: A method and system for selectively encrypting and decrypting different sections of a document provides different access levels in a technique employing different keys. The documents may be encrypted at a document section level ("section" here used according to its general meaning) and uses a different set of encryption keys for each section. A user A with an access level 1 may access only those section encoded with access level 1 plus unencoded sections. An application example of this technique is in hospitals. A patients records may each be segmented into separately-encrypted portions giving access to nurses for only suitable material while giving broader access to doctors. The nurse would be provided with his/her access level private key to gain access to those parts of the document for which nurses have rights. There could also be a level to which only the primary care physician or health care proxy has access.

WO 02/01271 A1

Multiple encryption of a single document providing multiple level access privileges

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The invention relates to document encryption and access restrictions on documents and more particularly to the encryption of each portion of a document such that access rights to respective portions may be obtained with corresponding keys.

BACKGROUND

Various kinds of document access protection are known. In one example, EP 0 848 314 A1 for DOCUMENT SECURITY SYSTEM AND METHOD only documents to which the user has rights are generated from a database. Varying security levels are provided. Another system described in US Patent No. 5,052,040 for MULTIPLE USER STORED DATA CRYPTOGRAPHIC LABELING SYSTEM AND METHOD permits different users to utilize the same files. The system exploits an extension of the file label which contains configuration capabilities and user rights and privileges. The separate user rights and privileges in this case relate to the entire document such as read only, read and write, deletion, etc. The document is encrypted. Another prior art system is described in US Patent No. 6,011,847 for CRYPTOGRAPHIC ACCESS AND LABELING SYSTEM. In this system, encryption and decryption of files uses a relational key generated by the system. A computer program also generates a series of labels that are encrypted and appended as a trailer to the encrypted message. The encrypted labels provide a history behind the particular encryption and they can be individually selected, separated, and decrypted from the total file. An access control module provides access to an encryption portion of the document to users with passphrases by comparing a generated vector or key with a partially decrypted version of a second vector or key stored on a portable storage medium such as a floppy disk. In response, a main key can be generated to encrypt or decrypt the labels. The latter system is mainly concerned with adding descriptive labels to the end of an encrypted document and contains a key exchange method for passing the decryption key between a server and a client.

Other prior art systems and methods are known, but none contain a very convenient, robust, and straightforward method for encryption-protection of different parts of a document based on access privileges.

SUMMARY OF THE INVENTION

A method and system for selectively encrypting and decrypting different sections of a document provides different access levels in a technique employing different keys. The documents may be encrypted at a document section level ("section" here used according to its general meaning) and uses a different set of encryption keys for each section. A user A with an access level 1 may access only those sections encoded with access level 1 plus unencoded sections. An application example of this technique is in hospitals. A patients records may each be segmented into separately-encrypted portions giving access to nurses for only suitable material while giving broader access to doctors. Thus, this example illustrates access control to information contained inside a document based on pre-defined roles accepted within a specific environment. The nurse would be provided with an access level key based on the access control rules defined by the hospital. Such key would allow the nurse to gain access to those parts of the document for which nurses have rights. There could also be a level to which only the primary care physician or health care proxy has access.

A method for distributing keys is also provided. This method utilizes a key box which is created for holding keys used to encode the sections of the document. The key box contains a slot for each level of access. The set of keys that a user at a given level requires is placed in a corresponding slot. Each slot is encoded using the access level public key giving the user access to the keys in the appropriate slot when decrypted using the user's private key.

An additional feature provides an outer layer of encryption using a public key for a requesting organization. Once the requesting organization opens the document using its private key, anyone in the receiving organization can apply their access level private key(s) to the key box, which in turn applies the keys in the corresponding slot to the document. This allows each user to view/modify the parts of the document to which they have access rights.

The invention will be described in connection with certain preferred embodiments, with reference to the following illustrative figures so that it may be more fully understood. The description of this invention uses the definition of public key to correspond to the public portion of the public/private key pair that is used in the art to realize asymmetric algorithms. The description of this invention uses the definition of private key to correspond to the private portion of the public/private key pair that is used in the art to realize asymmetric algorithms. The description of this invention uses the definition of symmetric key to refer to the a single key that is used in the art to realize symmetric algorithms.

With reference to the figures, it is stressed that the particulars shown are by way of example and for purposes of illustrative discussion of the preferred embodiments of the present invention only, and are presented in the cause of providing what is believed to be the most useful and readily understood description of the principles and conceptual aspects of the invention. In this regard, no attempt is made to show structural details of the invention in more detail than is necessary for a fundamental understanding of the invention, the description taken with the drawings making apparent to those skilled in the art how the several forms of the invention may be embodied in practice.

BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 is an illustration of a computer environment in which the invention may be used.

Fig. 2A is an illustration of a document indicating separate sections and the encryption processes to be applied to each section according to first embodiment of the invention in which public keys are used for encryption.

Fig. 2B is an illustration of a document indicating separate sections and the encryption processes to be applied to each section according to second embodiment of the invention in which public keys are used for encryption.

Fig. 3 is an illustration of a document indicating separate sections and the encryption processes to be applied to each section according to third embodiment of the invention in which document-specific keys are used.

Fig. 4 is an illustration of a key box document used with the embodiment of Fig. 3.

Fig. 5 is an illustration of a process for encrypting a document according to an embodiment compatible with any of the foregoing embodiments.

Fig. 6 is an illustration of a process for encrypting a document according to an embodiment compatible with any of the foregoing embodiments.

Fig. 7 is an alternative way of packaging the key box in a transmission by including it within a single document.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring to Fig. 1, the invention may be used in the environment of electronic document transfer. An example of such an environment is a sending computer 110 and a

receiving computer 120 connected by a network 100 or simply by physical transfer of a non-volatile data store 90 such as a floppy disk.

Referring to Fig. 2A, a document 95 contains various sections 130, 135, 140, and 145. Each section is divided according to how the information contained in the section is desired to be made available to a particular person (organization or other entity) or class of persons. The document 95 is intended to be transferred by the sender 110 to the receiver 120, the receiver including each of the persons or classes of persons. The sections labeled 130 and 145 are encrypted with a public key L1 corresponding to the first user or class of users. The section labeled 135 is encrypted with a second public key L2 corresponding to the second user or class of users. By virtue of being embedded in the section 135, section 145 is also encrypted with the L2 public key.

Referring to Fig. 2B, the various sections may be encrypted with only one key or all keys from the access level to which they correspond down to the lowest level of access. Thus, in this example, document section 145 is encrypted with both the L1 and L2 keys, but so is document section 130. Alternatively, each section may be encrypted with only a single key, so that a level 1 section appearing in a level 2 section is simply treated as a completely separate section with the level 2 section being broken into separate subsections for L2 encryption. The encryption methods described above permit multilevel access to a document based on the public keys of the intended audience. It is possible to limit access based on the user as well as the particular document as shown in the next embodiment.

Referring now to Figs. 3 and 4, the document sections are encrypted with respective document keys, a respective one for each access level defined within the scope of the document. The document keys may be symmetric keys. The latter are not shared outside of the context of use of the document and the user need never directly know what the symmetric keys are. These document keys are then made available to the recipients by encrypting them into a separate document (which could be part of the original document as in a file header as illustrated in Fig. 7) called a key box. The key box has a slot corresponding to each access level defined within the scope of the organization that is requesting such document. A first slot 1 210 contains document keys for access levels 1 and 2 giving the user access to both levels. A second slot 1 215 contains document keys for access level 2. Each slot is encrypted using the public key of the organization that corresponds to the access level of the slot. The entire key box file and the document may be encrypted using the public key of the user to ensure confidentiality of the transmission of the document and the key box.

Additionally, the key box and the document may be signed by the sender 110 to ensure integrity of the transmission and authenticity of the document.

The preceding embodiment contemplates an agreement between the sender of the document who prepares the encryption and the organization receiving the document. This agreement would map access levels used in encrypting the document to the access levels in place at the receiver. For a given document, a given organization level may map to a single document access level. Alternatively, a given organization level may map to multiple document access level.

Preferably, to assure data integrity and non-repudiation, the document source may sign the document hash with a private key. The requestor receiving the document together with the signature can then vouch for the validity of the source. Other mechanisms for authenticating the document's contents may also be used.

When a person with access level N opens the document, he/she presents his/her organization access level private key, which corresponds to the asymmetric key pair, to a decryption process that uses the key to access the appropriate slot in the key box. The symmetric keys may be used by the process to access the appropriate levels of the document transparently to the user. The user never "handles" the symmetric document keys and simply accesses the portions of the document the user has permission to access.

Referring now to Fig. 5, the detailed steps for creating, sending, receiving, and using a document begin with the receipt of a request S10 for the document and the appropriate information such as the public keys of the users, a map of users to access levels, etc. Next, a key is created for each access level required S20. The document is then encrypted starting with the highest (most privileged) access level and going down S30. This may result in the layered encryption of either of Figs. 2A and 2B or the alternative process where each level is only encrypted once. The keys are formed into a key box document and each set separately encrypted using the public keys of the access levels S45. Then the document and key box are bundled and optionally encrypted using the public key of the receiver S55.

When the receiver receives the file containing the encrypted document and the key box, the package is unbundled and optionally decrypted S60. The document and key box are then made available to the users S70. When a user accesses the document, the user provides his/her organization access level private key to a decryption process on a receiving computer (e.g. 120) which uses the key to decrypt the appropriate slot of the key box S75. The process then applies the symmetric keys, obtained from the decrypted slot in the key

box, S80 to the document to allow the user to access the document S85. The user never directly accesses the symmetric access level keys or even concerns him/herself with how many keys are involved.

Referring to Fig. 6, in an alternative embodiment, the public keys of the receivers are not used to encrypt the document. Rather step S45 is skipped and the key box is simply encrypted using the organization's public key. At the receiving organization, an additional step S90 between S65 and S70 is added wherein the slots of the key box are mapped to the access levels present in the organization and encrypted with the appropriate public keys of the users or group of users.

It will be evident to those skilled in the art that the invention is not limited to the details of the foregoing illustrative embodiments, and that the present invention may be embodied in other specific forms without departing from the spirit or essential attributes thereof. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the appended claims rather than by the foregoing description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

CLAIMS:

1. A method of securely transmitting a first document, comprising the steps of:
- generating first and second level document keys;
- encrypting a first section (130) of said first document with said first level document key and encrypting said first and a second section (135) of said first document with said second level document key;
- forming a second document (220) or a portion (520) of said document, said second document or said portion containing said first and second level document keys;
- transmitting said first document or said first and second documents as appropriate to the choice in said step of forming.

2. A method as in claim 1, wherein said first and second level document keys are symmetric keys.

3. A method as in claim 1, further comprising receiving at least two public keys from a recipient, said step of forming including encrypting said second document such that a corresponding set of said first and second level document keys is made available by decryption using a first of said at least two public keys and such that a corresponding other set of said first and second level document keys is made available by decryption using said second of said at least two public keys.

4. A method as in claim 3, wherein said step of encrypting including encrypting a first of said at least two public keys in a first portion of said second document or first document portion and encrypting a first and second of said at least two public keys in a second portion of second document or first document portion.

5. A method as in claim 3, wherein said first and second level document keys are symmetric keys.

6. A method as in claim 1, wherein said step of transmitting includes encrypting said first document or said first and second documents as appropriate to the choice in said step of forming.

7. A method of encrypting a document, comprising the steps of:
- encrypting a first portion of a document using a first key;
- encrypting a second portion of said document using a second key;
- encrypting a result of said first and second steps of encrypting using a third key, being a public key of a recipient.

8. A method of encrypting a document as in claim 7,wherein said first key is a first public key of said recipient and said second key is a second public key of said recipient.

9. A method of encrypting a document as in claim 7, wherein said first key is a first symmetric key and said second key is a second symmetric key, and the method includes the step of encrypting said first symmetric key with a public key.

10. A method as in claim 9, wherein said second portion includes a part of said first portion, said part having been encrypted with said first symmetric key.

11. A method of encrypting a document as in claim 9, comprising the step of encrypting said second symmetric key with a second public key.

12. A method of securely providing access to first and second readers of a document, comprising the steps of:
- transmitting to a sender of a document, public keys corresponding to readers of said document, said public keys being used to encrypt said document;
- receiving encrypted data from said sender;
decrypting a portion of said encrypted data using a private key corresponding to one of said public keys;
- a result of said first step decrypting being the accessing of a portion of said data corresponding to said one of said public keys;
- decrypting a portion of said encrypted data using a private key corresponding to another of said public keys;

- result of said second step decrypting being the accessing of a portion of said data corresponding to said other of said public keys.

13. A method as in claim 12, wherein said first and second steps of decrypting each include decrypting a portion of said data to unlock a respective set of encryption keys.

14. A method as in claim 12, wherein said first and second steps of decrypting further include using said respective set of encryption keys to unlock at least a portion of said encrypted data to provide access to only a portion of said document.

15. A method as in claim 12, wherein said first and second steps of decrypting further include using said respective set of encryption keys to unlock at least a portion of said encrypted data to provide access to said document.

16. A data file (95+220), comprising:
an encryption protected document (95, 595) containing a key portion (520) and an encrypted document portion (585);
- said key portion being at least partly decryptable with a first public key to provide access to a first symmetric key;
- said key portion being at least partly decryptable with a second public key to provide access to a second symmetric key;
- a first portion (210) of said encrypted document portion being decryptable with said first symmetric key and a second portion (215) of said encrypted document portion being decryptable with said second symmetric key.

17. A data file containing:
- an encrypted document (95) and at least two encryption keys;
- said encryption keys being encrypted such as to be accessible using at least two public keys and such that a first portion (130) of said encrypted document is accessible by decrypting with a first subset of said encryption keys, said first subset being decryptable using a first of said at least two public keys, and such that a second portion of said encrypted document is accessible by decrypting with a second subset of said encryption keys, said second subset being decryptable using a second of said at least two public keys.

18. A data set stored on a data storage medium, comprising:

- a document encrypted in portions using respective keys to encrypt said portions;
- a first portion of said document being encrypted with a first of said respective keys;
- a second portion of said document being encrypted with a second of said respective key;
- said first and second respective keys being encrypted in a file such as to permit decryption of said first key by a first private key and to permit decryption of said second key by a second private key.

19. A data set stored on a data storage medium, comprising:

- document encrypted in portions using respective keys to encrypt said portions;
- a first portion of said document being encrypted with first and second of said respective keys;
- a second portion of said document being encrypted with said first respective key;
- said first and second respective keys being encrypted in a file such as to permit decryption of said first and second keys by a first private key and to permit decryption of said first key by a second private key.

20. A document decrypting program stored on a data storage medium, comprising:

- code defining a process capable of selectively decrypting a portion of a data set using a respective key, said portion yielding a respective set of further keys upon decryption;
- code defining a further process capable of retrieving from said data set portions of a document corresponding to said respective set of further keys to provide access to only portions of said document corresponding to respective key.

21. A stored program as in claim 20, wherein said respective key is a public key.

22. A stored program as in claim 20, wherein each of said set of further keys is unique to said document.

23. A stored program as in claim 20, wherein each of said set of further keys is a symmetric key.

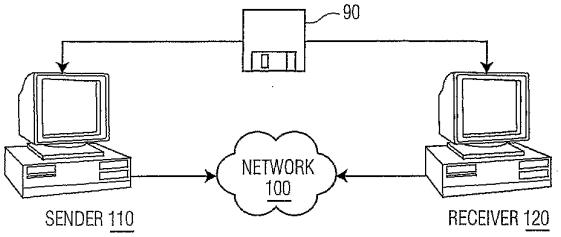

90
NETWORK
100
SENDER 110
RECEIVER 120

FIG. 1

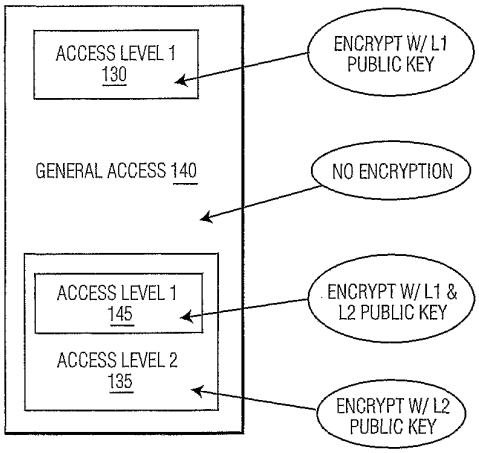

ACCESS LEVEL 1
130
ENCRYPT W/ L1
PUBLIC KEY
GENERAL ACCESS 140
NO ENCRYPTION
ACCESS LEVEL 1
145
ENCRYPT W/ L1 &
L2 PUBLIC KEY
ACCESS LEVEL 2
135
ENCRYPT W/ L2
PUBLIC KEY

FIG. 2A

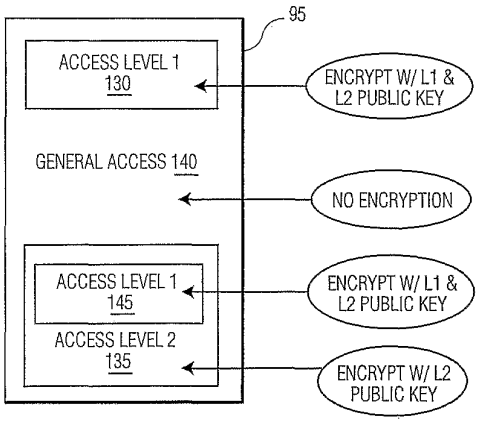

95
ACCESS LEVEL 1
130
ENCRYPT W/ L1 &
L2 PUBLIC KEY
GENERAL ACCESS 140
NO ENCRYPTION
ACCESS LEVEL 1
145
ENCRYPT W/ L1 &
L2 PUBLIC KEY
ACCESS LEVEL 2
135
ENCRYPT W/ L2
PUBLIC KEY

FIG. 2B

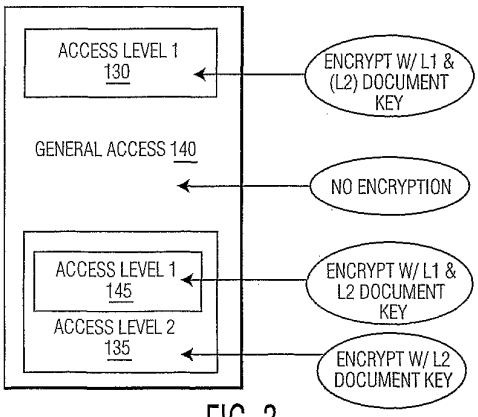

ACCESS LEVEL 1
130
ENCRYPT W/ L1 &
(L2) DOCUMENT
KEY
GENERAL ACCESS 140
NO ENCRYPTION
ACCESS LEVEL 1
145
ENCRYPT W/ L1 &
L2 DOCUMENT
KEY
ACCESS LEVEL 2
135
ENCRYPT W/ L2
DOCUMENT KEY

FIG. 3

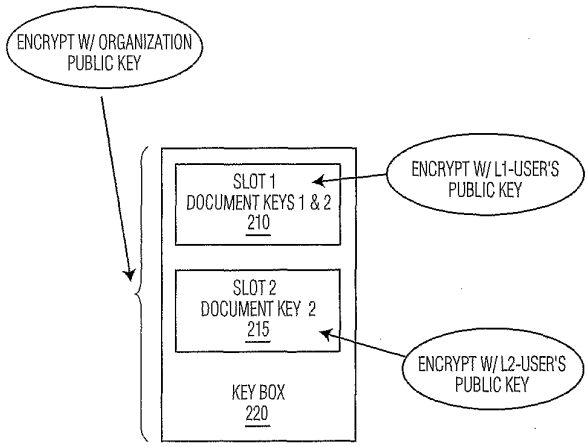

ENCRYPT W/ ORGANIZATION PUBLIC KEY
SLOT 1
DOCUMENT KEYS 1 & 2
210
ENCRYPT W/ L1-USER'S PUBLIC KEY
SLOT 2
DOCUMENT KEY 2
215
ENCRYPT W/ L2-USER'S PUBLIC KEY
KEY BOX
220

FIG. 4

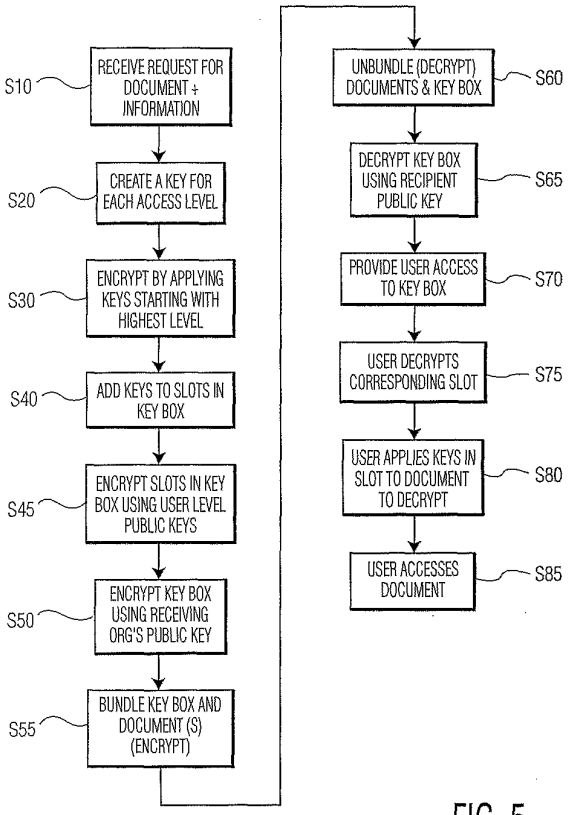

S10
RECEIVE REQUEST FOR DOCUMENT + INFORMATION
S20
CREATE A KEY FOR EACH ACCESS LEVEL
S30
ENCRYPT BY APPLYING KEYS STARTING WITH HIGHEST LEVEL
S40
ADD KEYS TO SLOTS IN KEY BOX
S45
ENCRYPT SLOTS IN KEY BOX USING USER LEVEL PUBLIC KEYS
S50
ENCRYPT KEY BOX USING RECEIVING ORG'S PUBLIC KEY
S55
BUNDLE KEY BOX AND DOCUMENT (S) (ENCRYPT)
S60
UNBUNDLE (DECRYPT) DOCUMENTS & KEY BOX
S65
DECRYPT KEY BOX USING RECIPIENT PUBLIC KEY
S70
PROVIDE USER ACCESS TO KEY BOX
S75
USER DECRYPTS CORRESPONDING SLOT
S80
USER APPLIES KEYS IN SLOT TO DOCUMENT TO DECRYPT
S85
USER ACCESSES DOCUMENT

FIG. 5

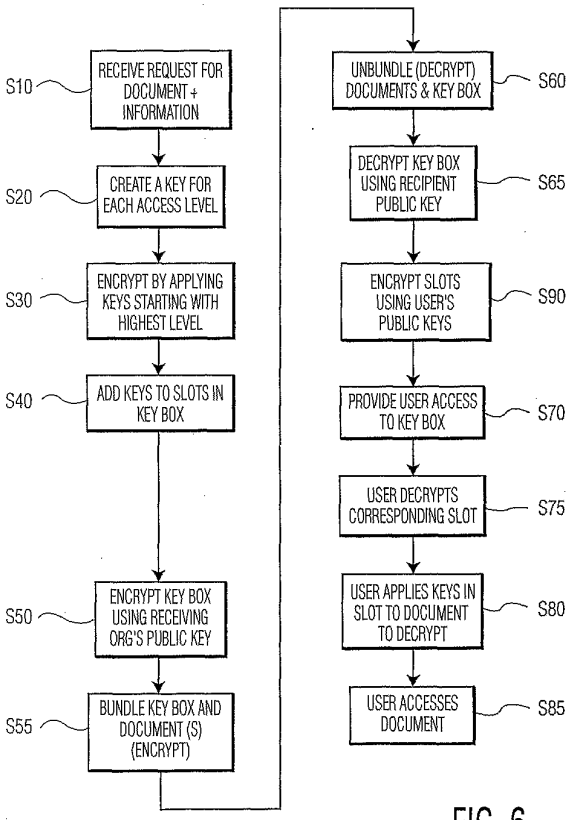

S10
RECEIVE REQUEST FOR DOCUMENT + INFORMATION
S20
CREATE A KEY FOR EACH ACCESS LEVEL
S30
ENCRYPT BY APPLYING KEYS STARTING WITH HIGHEST LEVEL
S40
ADD KEYS TO SLOTS IN KEY BOX
S50
ENCRYPT KEY BOX USING RECEIVING ORG'S PUBLIC KEY
S55
BUNDLE KEY BOX AND DOCUMENT (S) (ENCRYPT)
S60
UNBUNDLE (DECRYPT) DOCUMENTS & KEY BOX
S65
DECRYPT KEY BOX USING RECIPIENT PUBLIC KEY
S90
ENCRYPT SLOTS USING USER'S PUBLIC KEYS
S70
PROVIDE USER ACCESS TO KEY BOX
S75
USER DECRYPTS CORRESPONDING SLOT
S80
USER APPLIES KEYS IN SLOT TO DOCUMENT TO DECRYPT
S85
USER ACCESSES DOCUMENT

FIG. 6

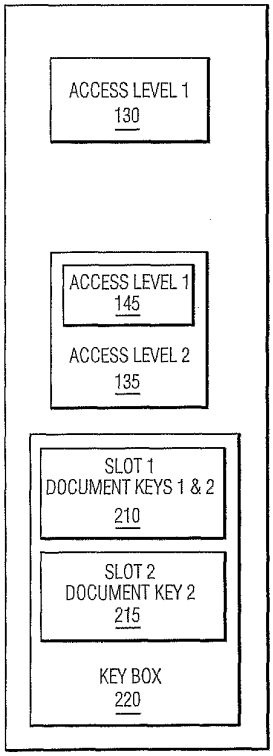

ACCESS LEVEL 1
130
ACCESS LEVEL 1
145
ACCESS LEVEL 2
135
SLOT 1
DOCUMENT KEYS 1 & 2
210
SLOT 2
DOCUMENT KEY 2
215
KEY BOX
220

FIG. 7

【国際公開パンフレット（コレクトバージョン）】

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

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2002 (03.01.2002)

PCT

(10) International Publication Number
WO 02/01271 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/EP01/07090

(22) International Filing Date: 22 June 2001 (22.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/606,339 29 June 2000 (29.06.2000) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: KRASINSKI, Raymond; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). ROSNER, Martin; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: HOEKSTRA, Jelle; Internationaal Octrooibureau B.V., Prof Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(national)*: CN, JP, KR.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

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

(48) Date of publication of this corrected version:
7 February 2002

(15) Information about Correction:
see PCT Gazette No. 06/2002 of 7 February 2002, Section II

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 02/01271 A2

(54) Title: MULTIPLE ENCRYPTION OF A SINGLE DOCUMENT PROVIDING MULTIPLE LEVEL ACCESS PRIVILEGES

(57) Abstract: A method and system for selectively encrypting and decrypting different sections of a document provides different access levels in a technique employing different keys. The documents may be encrypted at a document section level ("section" here used according to its general meaning) and uses a different set of encryption keys for each section. A user A with an access level 1 may access only those section encoded with access level 1 plus unencoded sections. An application example of this technique is in hospitals. A patients records may each be segmented into separately-encrypted portions giving access to nurses for only suitable material while giving broader access to doctors. The nurse would be provided with his/her access level private key to gain access to those parts of the document for which nurses have rights. There could also be a level to which only the primary care physician or health care proxy has access.

フロントページの続き

(72)発明者　クラシンスキ，レイモンド
オランダ国，５６５６　アーアー　アインドーフェン，プロフ・ホルストラーン　６
(72)発明者　ロスナー，マーティン
オランダ国，５６５６　アーアー　アインドーフェン，プロフ・ホルストラーン　６

Ｆターム(参考) 5B017 BA07 CA16
5J104 AA07 AA12 AA16 DA02 EA04 EA18 JA03 JA21 JA31 KA01
KA05 MA05 NA02 PA14