(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4392808号
(P4392808)

(45)発行日　平成22年1月6日(2010.1.6)　(24)登録日　平成21年10月23日(2009.10.23)

(51)Int.Cl.		F I		
G06F 13/00	(2006.01)	G06F	13/00	351E
G09C 1/00	(2006.01)	G09C	1/00	610A
H04L 9/16	(2006.01)	G09C	1/00	660D
H04L 9/18	(2006.01)	H04L	9/00	643
H04L 9/36	(2006.01)	H04L	9/00	651

請求項の数 2　(全 6 頁)　最終頁に続く

(21)出願番号　特願平10-220198
(22)出願日　平成10年8月4日(1998.8.4)
(65)公開番号　特開2000-59355(P2000-59355A)
(43)公開日　平成12年2月25日(2000.2.25)
審査請求日　平成16年10月6日(2004.10.6)
審判番号　不服2007-16173(P2007-16173/J1)
審判請求日　平成19年6月11日(2007.6.11)

(73)特許権者　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100092495
弁理士　蛭川　昌信
(74)代理人　100088041
弁理士　阿部　龍吉
(74)代理人　100095120
弁理士　内田　亘彦
(74)代理人　100095980
弁理士　菅井　英雄
(74)代理人　100094787
弁理士　青木　健二
(74)代理人　100097777
弁理士　韮澤　弘

最終頁に続く

(54)【発明の名称】暗号化処理システム

(57)【特許請求の範囲】
【請求項１】
ＩＣカードに格納されているファイル分割方法に従ってファイルを分割する分割手段と、
ＩＣカードに格納されているファイルの暗号化方法、暗号鍵により前記分割手段で分割した各ファイルを暗号化する暗号化手段と、
各ファイルの暗号化前、或いは暗号化後に各ファイルの順番を維持するか、並び替えを行い、並び替えた場合、それらの順番や最終子ファイルを表す指標を付加する並び替え手段と、
暗号化された各ファイルを別々のファイルにして送信する送信手段と、
前記送信手段で送信され、並び替えが行われて各ファイルの順番或いは最終子ファイルを表す指標が付されているときその指標を削除し、暗号化時の条件を用いて分割された個々のファイルを復号化し、全ファイル復号化後、各ファイルを再統合する復号化手段とを備え、
暗号化処理に際して、前記分割手段で分割して細分化するファイルの長さを求める数式とその初期値、細分化されたファイルの暗号化方式を決定する数式とその初期値、それぞれの暗号化に用いる鍵を求める数式とその初期値を設定することを特徴とする暗号化処理システム。
【請求項２】
前記分割したファイルに、さらにダミーファイルを付加することを特徴とする請求項１

記載の暗号化処理システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は送信データを暗号化し、通信回線を通して受信側にデータを伝送する暗号化処理システムに関するものである。
【０００２】
【従来の技術】
一般に、任意のファイルについて暗号化を行う場合、当該ファイルに対して１つの暗号鍵を用い、１つの暗号方法により一括して暗号化が施される。また、第３者による暗号文への攻撃に対応するため、暗号化された文をさらに分割し、分割したデータを、順次、回線上に分配し、回線上を伝送されてくる分配されたデータを再び元の順番に並べ変える手法も提案されている（特開平３―１０８８３０号公報）。
【０００３】
【発明が解決しようとする課題】
何らかの暗号解読方法、例えば既知の平文攻撃（電子メール等の場合、書き出し部分には定型的な文章が多く現れることを利用し、攻撃者にとって既知の平文と暗号文の対を基に共通鍵を導き出す攻撃）により、ファイルの一部について暗号が破られた場合、ファイルの全体についても同様の手法で暗号が破られる危険性がある。
また、特開平３―１０８８３０号公報で提案されているように、暗号化してからファイルを分割した場合、これを第３者が解読することは困難にはなるが、ファイルの一部の解読が全体に波及することには変わりない。
本発明は上記課題を解決するためのもので、ファイル全体としての隠蔽性を高くし、高い安全性を保つことができるようにすることを目的とする。
【０００４】
【課題を解決するための手段】
本発明は、ＩＣカードに格納されているファイル分割方法に従ってファイルを分割する分割手段と、ＩＣカードに格納されているファイルの暗号化方法、暗号鍵により前記分割手段で分割した各ファイルを暗号化する暗号化手段と、各ファイルの暗号化前、或いは暗号化後に各ファイルの順番を維持するか、並び替えを行い、並び替えた場合、それらの順番や最終子ファイルを表す指標を付加する並び替え手段と、暗号化された各ファイルを別々のファイルにして送信する送信手段と、前記送信手段で送信され、並び替えが行われて各ファイルの順番或いは最終子ファイルを表す指標が付されているときその指標を削除し、暗号化時の条件を用いて分割された個々のファイルを復号化し、全ファイル復号化後、各ファイルを再統合する復号化手段とを備え、暗号化処理に際して、前記分割手段で分割して細分化するファイルの長さを求める数式とその初期値、細分化されたファイルの暗号化方式を決定する数式とその初期値、それぞれの暗号化に用いる鍵を求める数式とその初期値を設定することを特徴とする。
また、本発明は、前記分割したファイルに、さらにダミーファイルを付加することを特徴とする。
【０００５】
【発明の実施の形態】
以下、本発明の実施の形態について説明する。
図１は本発明の暗号化処理システムの全体図である。
送信側は送信端末装置１と暗号化装置２からなり、送信端末装置１は暗号化装置２を介して、暗号化した送信データを通信回線５に送出する。受信側は復号装置３、受信端末装置４からなり、暗号化されたデータを受信端末装置４で受信して復号装置３で復号する。
【０００６】
図２は本発明の暗号化装置２の機能を示すブロック図である。
暗号化装置２には送信するデータファイルを分割するファイル分割手段２１、必要に応じ

てダミーファイルを付加するダミーファイル付加手段２２、分割ファイルを並び替える並び替え手段２３、分割したファイルを個々に暗号化する分割ファイル暗号化手段２４を備えている。

【０００７】

ファイル分割手段２１は、例えば分割するための数式を１つまたは複数有していて、使用する数式をランダムに決定し、初期値を任意に設定して数式よりファイルの分割位置を決定する方式、あるいは乱数を発生させ、これを利用してファイルの分割位置を決定する方式等、適宜の方式を用いる。分割した各ファイルには、その分割位置を示す指標を付したり、あるいは分割位置を示すテーブルを作成する。

【０００８】

ダミーファイル付加手段２２は、一定数、一定サイズのダミーファイルを生成して付加したり、ファイル分割数に応じて付加するダミーファイルの数やそのサイズを変えて付加するものであり、ダミーファイルには、そのこと示す何らかの情報、例えば指標を付加する。

【０００９】

並び変え手段２３は、乱数を発生させてファイルを並べる順番を決めたり、或いは１つまたは複数の数式をもっておき、任意に初期値を設定すること等により順番を決定する。

【００１０】

分割ファイル暗号化手段２４は、複数の暗号化方式、暗号鍵を有していて、分割ファイル全体を１つの暗号化方式、暗号鍵で暗号化したり、各分割ファイル毎、或いはいくつかのファイル毎に暗号化方式、暗号鍵を変えて暗号化を行う。また、暗号化はファイルの一部に行ってもよい。

【００１１】

図３に模式的に示すように、暗号化装置２のファイル分割手段２１により元のデータＦは複数のファイルF_1、F_2……F_nに分割され、ダミーファイル付加手段２２により、必要に応じてダミーファイルF_Dが付加され、並び変え手段２３により必要に応じて並び変えが行われ、分割ファイル暗号化手段２４により暗号化されて送信される。ファイルの並び変えは暗号化の前であっても、後であってもよく、また、ファイルの分割と並び替え、暗号化は並列的に処理を行ってもよい。

【００１２】

図４は復号装置３の機能ブロック図である。

受信した各分割ファイルを復号する分割ファイル復号手段３１と、復号した手段を再統合するファイル統合手段３２とを備えている。

分割ファイル復号手段３１には、送信側での各ファイルごとの暗号化方法、暗号鍵等の情報、暗号化を行ったファイルか否か等の情報があらかじめ設定される。

ファイル統合手段３２には、ファイル単位の分割の仕方、ファイル単位の分割位置の情報を知る必要があり、そのため、例えば分割のための数式だけを決めておき、送信側から初期値を設定すると、受信側ではその初期値を基に順次分割位置を計算によって求めるようにする等の方法が採用可能である。

また、ファイル分割方法、各分割ファイルの暗号化方法、暗号鍵等をＩＣカードに格納しておき、これを送信側、受信側に配布するようにしてもよい。このようなＩＣカードを利用すれば、回線上に暗号化に関する情報が流れないので、一層秘密性を保持することができる。

【００１３】

次に、図５により暗号化／復号処理フローの例を説明する。

暗号化処理を説明すると、図５（ａ）において、先ず、用いる暗号の方式、分割して細分化するファイルの長さを求める数式とこれの初期値、細分化されたファイルを暗号化する方式を決定する数式とこれの初期値、それぞれの暗号化に用いる鍵を求める数式とその初期値を設定する（Ｓ１）。次いで、与えられたファイルを規則に従って分割し（Ｓ２）、これに暗号化を施す（Ｓ３）。分割された個々のファイル（以下、子ファイル）について

はその順番を維持するか、何らかの規則に従って並び替えを行う。並び替えた場合、それらの順番や最終子ファイルを表わす指標を付加する（Ｓ４）。子ファイルは外部から個々のファイルとして認識されるか、あるいは全体が１つのファイルとして認識される。子ファイルに指標を付けず、これらを管理し、最後の子ファイルを認識するためのテーブルを用意しておいても良い。こうしてファイルが最後か、否か判断し（Ｓ５）、最後になるまで以上の処理を繰り返す。

【００１４】

次に、復号処理を説明すると、図５（ｂ）において、先ず、順番や最終子ファイルを表わす指標を削除し（Ｓ１１）、暗号化した時のそれぞれの条件を用いて個々の子ファイルの復号を行い（Ｓ１２）、その結果を出力し（Ｓ１３）、この処理を最後まで繰り返し（Ｓ１４）、最後まで復号処理したらファイルを再統合する（Ｓ１５）。

【００１５】

【発明の効果】

以上のように、本発明によれば、ファイル全体としての隠蔽性が高くなるため、高い安全性を保つことができる。また、暗号手法の強度、例えば暗号鍵の長さ等に関して、何らかの制限があり、十分安全な暗号方式を使用できない場合にもファイル全体として高い安全性を保つことが可能となる。

【図面の簡単な説明】

【図１】　本発明の暗号化処理システムの全体図である。

【図２】　本発明の暗号化装置２の機能を示すブロック図である。

【図３】　ファイル分割を模式的に示す図である。

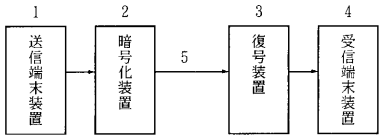
【図４】　復号装置の機能ブロック図である。

【図５】　暗号化／復号処理フローの例を説明する図である。

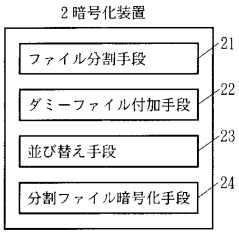
【符号の説明】

１…送信端末装置、２…暗号化装置、３…復号装置、４…受信端末装置、５…通信回線、２１…ファイル分割手段、２２…ダミーファイル付加手段、２３…並び替え手段、２４…分割ファイル暗号化手段、３１…分割ファイル復号手段、３２…ファイル統合手段。

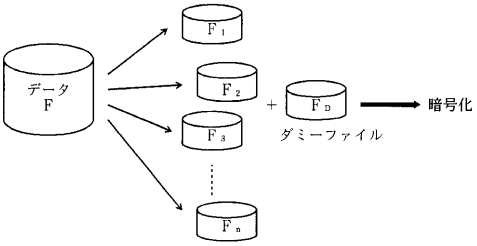
【図１】


1
送信端末装置
2
暗号化装置
5
3
復号装置
4
受信端末装置

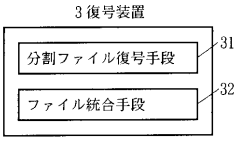
【図２】


2暗号化装置
ファイル分割手段
21
ダミーファイル付加手段
22
並び替え手段
23
分割ファイル暗号化手段
24

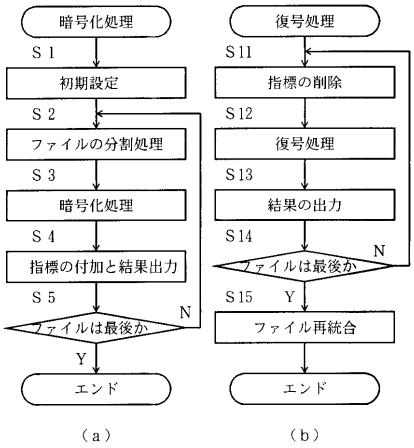
【図３】


データ
F
F1
F2
F3
Fn
+
FD
ダミーファイル
暗号化

【図４】


3復号装置
分割ファイル復号手段
31
ファイル統合手段
32

【図５】


暗号化処理
S1
初期設定
S2
ファイルの分割処理
S3
暗号化処理
S4
指標の付加と結果出力
S5
ファイルは最後か
N
Y
エンド
（a）
復号処理
S11
指標の削除
S12
復号処理
S13
結果の出力
S14
ファイルは最後か
N
S15
Y
ファイル再統合
エンド
（b）

フロントページの続き

(51)Int.Cl. FI
H04L 9/00 685

(74)代理人 100091971
弁理士 米澤 明
(72)発明者 矢野義博
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内
(72)発明者 松田雅之
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内
(72)発明者 半田富己男
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内
(72)発明者 柴田直人
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内

合議体
審判長 吉岡 浩
審判官 石田 信行
審判官 冨吉 伸弥

(56)参考文献 特開平７－２８８７６２（ＪＰ，Ａ）
特開平９－２００１９５（ＪＰ，Ａ）
特開平１０－２７１１０７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/16
H04L 9/18
H04L 9/36
G09C 1/00
G06F 13/00
G06F 21/24