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

特許第4703805号
(P4703805)

(45)発行日　平成23年6月15日(2011.6.15)　(24)登録日　平成23年3月18日(2011.3.18)

(51)Int.Cl.		F I		
G09C 1/00	(2006.01)	G09C	1/00	610Z
G06K 19/10	(2006.01)	G06K	19/00	R
G06K 19/00	(2006.01)	G06K	19/00	W
H04L 9/10	(2006.01)	H04L	9/00	621A

請求項の数 9　(全 12 頁)

(21)出願番号　特願平11-325836
(22)出願日　平成11年11月16日(1999.11.16)
(65)公開番号　特開2001-142396(P2001-142396A)
(43)公開日　平成13年5月25日(2001.5.25)
審査請求日　平成18年10月18日(2006.10.18)

前置審査

(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　100094053
弁理士　佐藤　隆久
(72)発明者　大島　直行
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　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　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

最終頁に続く

(54)【発明の名称】暗号化装置、暗号化方法、復号化装置、復号化方法および通信システム

(57)【特許請求の範囲】
【請求項１】
任意のデータを所望の符号化方式により符号化する符号化手段と、
前記符号化されたデータを、隣接するデータブロックの長さが異なる複数のデータブロックに仕切り、当該仕切った各データブロックを順次仕切ったデータブロックの数と異なる数の複数のファイルに再配置する、分割手段と、
前記再配置された複数のファイルに対して、各ファイルごとに異なる鍵を用いて、同一の暗号化方式で暗号化処理を行い、暗号化された複数の部分データを生成する暗号化処理手段と、
前記暗号化された複数の部分データをそれぞれ出力する出力手段と
を有する暗号化装置。
【請求項２】
当該暗号化装置は、
前記再配置された複数のファイルに対して、該ファイルと同じサイズで、前記符号化対象のデータとは何ら関わりのないダミーデータを、前記複数のファイルの最後に付加するダミーデータ付加手段と、
前記再配置された複数のファイルと前記付加された前記ダミーデータの順序を乱数を用いて並び替える並び替え手段と
をさらに有し、
前記暗号化処理手段は、前記並べ替え手段において並べ替えられたデータについて前記

暗号化処理し、
前記出力手段は、前記暗号化されたデータを出力する、
請求項１に記載の暗号化装置。
【請求項３】
当該暗号化装置は、前記暗号化されたデータを解読するのに必要な前記鍵のデータをＩＣカードに記録するＩＣカード処理手段をさらに有する、
請求項１または２に記載の暗号化装置。
【請求項４】
符号化部、ファイル分割部、暗号化部、出力部を有する暗号装置において、
前記符号化部が、任意のデータを所望の符号化方式により符号化し、
前記ファイル分割部が、前記符号化されたデータを、隣接するデータブロックの長さが異なる複数のデータブロックに仕切り、当該仕切った各データブロックを順次仕切ったデータブロックの数と異なる数の複数のファイルに再配置し、
前記暗号化部が、前記再配置された複数のファイルに対して、各ファイルごとに異なる鍵を用いて、同一の暗号化方式で暗号化処理を行い、暗号化された複数の部分データを生成し、
前記出力部が、前記暗号化された複数の部分データをそれぞれ出力する、
暗号化方法。
【請求項５】
請求項１の暗号化装置によって生成されて出力された、暗号化された複数のデータを受信する受信手段と、
前記受信手段で受信した前記複数の部分データに分割され暗号化された暗号化データに対して、前記各部分データごとに異なる前記暗号鍵に対応する復号鍵を用いて暗号解読処理を行い解読された複数のデータを生成する暗号解読手段と、
前記解読されて生成された複数のデータについて、請求項１に記載の分割手段の再配置および分割処理と逆の処理を行う、並べ替え手段と、
前記並べ替えられた複数のファイルを前記符号化方式に対応した復号化方式により復号化し、前記任意のデータを生成する復号化手段と
を有する復号化装置。
【請求項６】
前記受信手段で受信した前記暗号化データは、前記任意のデータが分割された前記複数のファイルおよび当該ファイルと同じサイズで前記符号化データとは何の関わりのないダミーデータを有するデータであり、
当該復号化装置は、前記入力される暗号化データより、前記ダミーデータを除去するダミーデータ除去手段をさらに有し、
前記並べ替え手段は、前記ダミーデータを除去された前記生成された複数のデータを並べ替える
請求項５に記載の復号化装置。
【請求項７】
当該復号化装置は、前記各ファイルごと異なる前記暗号鍵に対応する復号鍵の情報が記憶されており、事前に配付されたＩＣカードより、前記暗号化された暗号化データの暗号解読処理に必要な前記復号鍵の情報を読み出すＩＣカード処理手段をさらに有し、
前記暗号解読手段は、前記読みだした前記復号鍵の情報を用いて前記暗号解読処理を行う、
請求項６に記載の復号化装置。
【請求項８】
受信部と、解読部と、並べ替え部と、復号部とを有する復号装置において、
前記受信部が、請求項４の暗号化方法によって生成されて出力された暗号化された複数のデータを受信し、
前記解読部が、前記受信した前記複数のファイルに分割され暗号化された暗号化データ

に対して、前記各ファイルごとに異なる前記暗号鍵に対応する復号鍵を用いて暗号解読処理を行い解読された複数のデータを生成し、
前記並べ替え部が、前記解読されたデータに対して、請求項４に記載のファイル分割部における処理と逆の処理を行い、
前記符号部が、当該処理されたデータを前記符号化方式に対応した復号化方式により復号化する、
復号化方法。
【請求項９】
伝送系統を介して接続される、請求項１～２のいずれかに記載の暗号化装置と、請求項５～６のいずれかに記載の復号化装置とを有し、
前記暗号化装置は、ＩＣカード記録手段を有し、
前記復号化装置は、ＩＣカード読み出し手段を有し、
前記暗号化装置のＩＣカード記録手段は、前記暗号化された複数の部分データを解読するのに必要な鍵データをＩＣカードに記録し、
前記復号化装置内のＩＣカード読み出し手段は、当該復号化装置で復号を行う前に配付された、前記鍵データが記録されたＩＣカードより、当該鍵データを読み出し、
前記復号化装置内の前記暗号解読手段は、前記読みだした前記復号鍵の情報を用いて前記暗号解読処理を行う、
通信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、所望のデータを機密性を保持して伝送する場合などに適用して好適な、暗号化装置とその方法および暗号復号化装置とその方法、および、その暗号化装置と暗号復号化装置とを有する通信システムに関する。
【０００２】
【従来の技術】
情報処理技術や通信技術の進展により、通信網を介した情報の伝送が容易かつ効率的に行えるようになっており、これに伴って、そのような通信網を介して伝送される情報の量も飛躍的に増大している。
通信網としては種々の形態のものがあるが、たとえば、複数のコンピュータシステム、ネットワークが世界的規模で接続されたインターネットは、その規模、通信コストの点などから着目されており、広く利用されている。
【０００３】
ところで、このような通信網を介しては、個人や企業間において種々の機密性を有するデータの通信も行なわれている。しかし、たとえばインターネットのようなオープンなネットワークシステムや無線通信のような通信システムでは、比較的伝送されているデータを傍受し易いという問題がある。
これに対処して機密性の必要なデータを伝送する一般的な方法として、伝送データを暗号化して暗号文を伝送する方法があり、広く利用されている。
なお、この暗号化方法にも種々の方法が考えられており、たとえば、特開平３－１０８８３０号公報には、暗号化した伝送データを複数のデータに分割し、これらを異なる回線を介して伝送することにより、より安全に所望のデータを送信することのできる方法が開示されている。
【０００４】
【発明が解決しようとする課題】
しかしながら、これまでの暗号化方法に対しては種々の解読方法も考えられており、より解読が難しく秘匿性の高い暗号化を行いたいという要望がある。
たとえば、電子メールなどの書き出し部分に定型的な文章が用いられることが多いことを利用し、その文章に相当する既知の平文と暗号文の対を元に共通鍵を導き出すような既知

の平文攻撃という暗号解読方法がある。この方法により一旦データの一部の暗号が解読されていしまうと、これまでの通常の暗号化方法においては、データ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高い。前述した特開平３－１０８８３０号公報に記載されている方法においても、データが分割されているためにその集積に多少の困難さがあるものの、データが見つかれば容易に解読されてしまうことにかわりはない。

【０００５】

したがって本発明の目的は、より秘匿性が高く所望のデータを暗号化することができる、通信に適用して好適な暗号化装置および暗号化方法を提供することにある。

また本発明の他の目的は、そのような暗号化装置および暗号化方法により暗号化されたデータを適切に復号化することができる、通信に適用して好適な暗号復号化装置および暗号復号化方法を提供することにある。

さらに本発明の他の目的は、所望のデータを、より高い秘匿性で伝送することができる通信システムを提供することにある。

【０００６】

本発明によれば、任意のデータを所望の符号化方式により符号化する符号化手段と、

前記符号化されたデータを、隣接するデータブロックの長さが異なる複数のデータブロックに仕切り、当該仕切った各データブロックを順次仕切ったデータブロックの数と異なる数の複数のファイルに再配置する、分割手段と、前記再配置された複数のファイルに対して、各ファイルごとに異なる鍵を用いて、同一の暗号化方式で暗号化処理を行い、暗号化された複数の部分データを生成する暗号化処理手段と、前記暗号化された複数の部分データをそれぞれ出力する出力手段とを有する暗号化装置が提供される。

【０００７】

本発明によれば、符号化部、ファイル分割部、暗号化部、出力部を有する暗号装置において、

前記符号化部が、任意のデータを所望の符号化方式により符号化し、

前記ファイル分割部が、前記符号化されたデータを、隣接するデータブロックの長さが異なる複数のデータブロックに仕切り、当該仕切った各データブロックを順次仕切ったデータブロックの数と異なる数の複数のファイルに再配置し、

前記暗号化部が、前記再配置された複数のファイルに対して、各ファイルごとに異なる鍵を用いて、同一の暗号化方式で暗号化処理を行い、暗号化された複数の部分データを生成し、

前記出力部が、前記暗号化された複数の部分データをそれぞれ出力する、

暗号化方法が提供される。

【０００８】

本発明によれば、上記暗号化装置によって生成されて出力された、暗号化された複数のデータを受信する受信手段と、前記受信手段で受信した前記複数の部分データに分割され暗号化された暗号化データに対して、前記各部分データごとに異なる前記暗号鍵に対応する復号鍵を用いて暗号解読処理を行い解読された複数のデータを生成する暗号解読手段と、前記解読されて生成された複数のデータについて、上記分割手段の再配置および分割処理と逆の処理を行う、並べ替え部と、前記並べ替えられ複数のファイルを前記符号化方式に対応した復号化方式により復号化し、前記任意のデータを生成する復号化手段と

を有する復号化装置が提供される。

【０００９】

本発明によれば、受信部と、解読部と、並べ替え部と、復号部とを有する復号装置において、

前記受信部が、上記暗号化方法によって生成されて出力された暗号化された複数のデータを受信し、

前記解読部が、前記受信した前記複数のファイルに分割され暗号化された暗号化データに対して、前記各ファイルごとに異なる前記暗号鍵に対応する復号鍵を用いて暗号解読処理を行い解読された複数のデータを生成し、

前記並べ替え部が、前記解読されたデータに対して、請求項４に記載のファイル分割部における処理と逆の処理を行い、
前記符号部が、当該処理されたデータを前記符号化方式に対応した復号化方式により復号化する、
復号化方法が提供される。
【００１０】
本発明によれば、伝送系統を介して接続される、上記暗号化装置と上記復号化装置とを有し、
前記暗号化装置は、ＩＣカード記録手段を有し、
前記復号化装置は、ＩＣカード読み出し手段を有し、
前記暗号化装置のＩＣカード記録手段は、前記暗号化された複数の部分データを解読するのに必要な鍵データをＩＣカードに記録し、
前記復号化装置内のＩＣカード読み出し手段は、当該復号化装置で復号を行う前に配付された、前記鍵データが記録されたＩＣカードより、当該鍵データを読み出し、
前記復号化装置内の前記暗号解読手段は、前記読みだした前記復号鍵の情報を用いて前記暗号解読処理を行う、
通信システムが提供される。
【００１１】
【発明の実施の形態】
本発明の一実施の形態について図１～図３を参照して説明する。
本実施の形態においては、所望のデータを任意の伝送路を介して伝送する送信装置および受信装置を有する通信システムを例示して本発明を説明する。
図１は、その通信システム１の構成を示すブロック図である。
通信システム１は、送信装置１０と受信装置３０とが伝送路２０を介して接続された構成である。
【００１２】
送信装置１０は、送信対象の所望のデータに対して、後述する種々の処理を施して所定の形式に変換し、伝送路２０に送出する。
まず、その送信装置１０の構成について説明する。
送信装置１０は、ファイル符号化部１１、ファイル分割部１２、ダミーファイル付加部１３、並び替え部１４、暗号化部１５、送信部１６およびＩＣカード処理部１７を有する。
【００１３】
ファイル符号化部１１は、入力される、あるいは送信装置１０内の図示せぬ記憶装置に予め記憶されている送信対象のデータに対して、所定の符号化処理を行なって符号化する。符号化されたデータは、ファイル分割部１２に供される。
本実施の形態においては、ＬＨＡ３２Ｖｅｒ１．１２により圧縮符号化するものとする。たとえば、図２（Ａ）に示すようなテキストファイルが送信対象のデータであった場合には、このデータは、この圧縮符号化処理により、テキスト表示を行なった場合に図２（Ｂ）に示されるようなデータに変換される。
【００１４】
ファイル分割部１２は、ファイル符号化部１１で符号化が行なわれた送信対象のデータを所定の規則に基づいて複数のファイルに分割する。ファイル分割部１２では、単にファイルの途中に区切りを設けることによりデータを分割するのではなく、ファイル内のデータ列をバイト単位で抽出し、所定の規則で複数のファイルに再配置することによりデータを分割する。
本実施の形態においては、図３（Ａ）に示すように、送信対象のファイルのデータを、順に、１バイト、３バイトごとに区切り、これを順に３つのファイルに再配置することにより、送信対象のデータファイルを３つのファイルに分割する。したがって、この処理により生成された各分割ファイルは、その内容をテキスト表示させると図３（Ｂ）に示すような意味不明の文字の列となり、元のテキストを想像することはできないものとなる。

なお、図３（Ａ）においては、理解を容易にするために分割前のデータとして内容が判るものを示したが、実際には、ファイル分割部１２には、前述したようにファイル符号化部１１で一旦圧縮符号化された、内容が直接的に判らない形式のデータが供給される。

【００１５】

ダミーファイル付加部１３は、ファイル分割部１２で生成された複数のファイルに対して、それらのファイルと同様の形式で、送信対象の元のデータとは何ら関わりの無い内容を有するファイルを付加し、それら全体を送信対象のデータとして並び替え部１４に出力する。付加するダミーファイルは、予め記憶しておいてもよいし、任意の方法で生成してもよい。また、付加する位置も任意の位置に付加してよい。本実施の形態においては、予め容易されたダミーデータの列を用いてファイル分割部１２で生成されたファイルとほぼサイズの等しいダミーデータのファイルを生成し、後段に並び替え部１４が具備されているので、それら生成されたファイルの最後に付加するものとする。

【００１６】

並び替え部１４は、ダミーファイル付加部１３でダミーデータが付加されて供給される送信対象の複数のファイルの順番を、たとえば乱数を用いるなどの方法により変更して、暗号化部１５に出力する。

【００１７】

暗号化部１５は、並び替え部１４より入力される複数のファイルに対して、暗号化処理を施し、暗号化された複数のデータファイルを生成して送信部１６に出力する。本実施の形態において暗号化部１５においては、複数のファイルに対して同一の暗号化アルゴリズムを用いるものの、鍵を各ファイルごとに変えて、各ファイルごとに暗号化処理を行なうものとする。

また暗号化部１５は、この暗号化処理の時に用いる共通鍵、秘密鍵などの情報を、たとえば送信先ごとに予め複数用意し、ＩＣカード２１に記録するべくＩＣカード処理部１７に出力しておく。そして、以後の処理においては、送信先ごとに、この用意された複数の鍵の中のいずれかを用いて暗号化処理を行なう。暗号化処理に用いた鍵は、その鍵のデータではなく、用意された複数の鍵の中のどの鍵を用いたことを示すたとえば鍵の番号など指標を用いて、伝送路２０を介して受信装置３０に通知する。

【００１８】

送信部１６は、送信装置１０が接続されている伝送路２０に応じたインターフェイスおよびプロトコル制御手段などを有しており、暗号化部１５より入力される暗号化された複数のファイルを、伝送路２０を介して受信装置３０に送信する。

【００１９】

ＩＣカード処理部１７は、データの送信に先立って予め暗号化部１５より入力される送信先ごとの共通鍵や秘密鍵などのデータを、装着されたＩＣカード２１に記録する。

なお、これら共通鍵や秘密鍵などのデータが記録されたＩＣカード２１は、データの送信に先立って受信装置３０に搬送される。

【００２０】

このような構成の送信装置１０により、所望の送信対象のファイルが伝送路２０に送出される。

この時の、送信装置１０の動作についてまとめて説明する。

まず、予め暗号化部１５において、暗号化処理に用いる公開鍵および秘密鍵を送信先ごとに複数ずつ決めて、ＩＣカード処理部１７を介してＩＣカード２１に記憶し、受信装置３０に搬送しておく。

そのような状況において、送信装置１０に送信対象のデータファイルが入力されると、ファイル符号化部１１でそのデータを所定の符号化方式により圧縮符号化し、元のデータとは異なり一見して内容を把握できないような符号で表現されたファイルに変換する。

【００２１】

このファイルが、ファイル分割部１２で複数のファイルに分割され、ダミーファイル付加部１３でダミーファイルが付加され、並び替え部１４で並び替えが行なわれる。

そして、この順番が並び替えられた複数のファイルに対して、暗号化部１５で、前述したように送信先ごとに複数決められている公開鍵および秘密鍵のいずれかを用いて暗号化処理を行い、暗号化されたファイルを送信部１６から伝送路２０を介して受信装置３０に送信する。
なお、この時暗号化処理に用いた鍵を示す指標は、その他の、たとえば符号化状態、分割方法、ダミーファイルの識別、並び替えアルゴリズムなど、種々の処理の条件などを示す指標とともに、同じく伝送路２０を介して受信装置３０に送信される。
【００２２】
伝送路２０は、任意の伝送路である。本実施の形態においては、送信装置１０および受信装置３０を含む種々の装置、コンピュータ、ネットワークが世界的規模で接続されたインターネットであるとする。
【００２３】
受信装置３０は、前述したように送信装置１０において所定の形式に変換されて伝送路２０を介して伝送されるデータを受信し、元の形式のデータファイルを復元して出力する。したがって、受信装置３０は、前述した送信装置１０の各構成部に対応した構成を有する。
受信装置３０のその構成について説明する。
受信装置３０は、ＩＣカード処理部３１、受信部３２、暗号復号化部３３、並び替え部３４、ダミーファイル除去部３５、ファイル統合部３６およびファイル復号化部３７を有する。
【００２４】
ＩＣカード処理部３１は、送信装置１０より受信装置３０にデータを暗号化して送信する際に用いられる公開鍵および秘密鍵などの情報を、データの伝送に先立って装着されるＩＣカード２１より読み出し、暗号復号化部３３に出力する。
【００２５】
受信部３２は、受信装置３０が接続されている伝送路２０に応じたインターフェイスおよびプロトコル制御手段などを有しており、伝送路２０を介して送信装置１０より送信される暗号化された複数のファイルを順次受信し、暗号復号化部３３に出力する。
【００２６】
暗号復号化部３３は、受信部３２で順次受信された複数のファイルに対して、暗号復号化処理を施し、暗号化が解除された複数のデータファイルを生成し、並び替え部３４に出力する。前述したように、送信装置１０の暗号化部１５においては、複数のファイルの各々に対して、同一の暗号化アルゴリズムを用いて、鍵を各ファイルごとに変えて暗号化処理を行なっている。したがって、暗号復号化部３３においても、受信部３２より入力される複数のファイルの各々に対して、同一の暗号解読アルゴリズムを用いて、鍵を各ファイルごとに変えて暗号復号化処理を行なう。なお、この時に用いる鍵の情報、たとえば、公開鍵および秘密鍵などの情報は、前述したようにＩＣカード処理部３１を介して予め入力され記憶されているものである。
【００２７】
並び替え部３４は、前述したように送信装置１０の並び替え部１４で行なわれた並び替えの処理の反対の処理を行い、暗号が復号化された複数のファイルを元の順番に並び替えて、ダミーファイル除去部３５に出力する。
【００２８】
ダミーファイル除去部３５は、並び替え部３４において並び替えられた複数のファイルより、ダミーファイルを検出してこれを除去し、残りの複数のファイルをファイル統合部３６に出力する。なお、本実施の形態においては、前述したように、送信装置１０のダミーファイル付加部１３では単にダミーファイルを実ファイルの最後尾に付加しているだけなので、ダミーファイル除去部３５においても、最後のファイルを除去することによりダミーファイルを除去し実ファイルを検出する。
【００２９】

ファイル統合部３６は、前述したように送信装置１０のファイル分割部１２で行なわれたファイル分割の処理の反対の処理を行い、複数のファイルの各データを順に再配置して、符号化処理が行なわれたのみの元の１つのファイルを生成し、ファイル統合部３６７に出力する。

【００３０】

ファイル復号化部３７は、前述したように送信装置１０のファイル符号化部１１で行なわれた符号化処理に対応した所定の復号化処理を行い、元のファイルを復元して受信装置３０より出力する。これにより、たとえば図２（Ｂ）に示したような符号化されたデータが、図２（Ａ）に示したようなテキストファイルが復元される。

【００３１】

このような構成の受信装置３０により、受信装置３０より伝送路２０を介して伝送されたファイルが受信され、元のデータが復元されて出力される。

この時の、受信装置３０の動作についてまとめて説明する。

まず、予め暗号復号化部３３における暗号復号化処理で用いる公開鍵および秘密鍵の情報が記録されたＩＣカード２１がＩＣカード処理部３１に装着され、これよりそれら鍵情報が読みだされて、暗号復号化部３３に記録される。

そしてこのような状況において、送信装置１０より伝送路２０を介して前述したような形式に変換された複数のファイルが伝送されてきたら、受信部３２においてこれを順に受信し、暗号復号化部３３で各ファイルごとに、先に記録されている鍵のいずれかを用いて暗号復号化処理を行なう。

【００３２】

次に、暗号の解読された複数のファイルを並び替え部３４で並び替えて元の順番に戻し、ダミーファイル除去部３５で最後尾に付加されているダミーファイルを除去する。

そして、ファイル統合部３６において、所定の規則に基づいて複数のファイルの各データを再配置して元の１つのファイルに統合し、そのファイルのデータに対して、ファイル復号化部３７で、送信装置１０のファイル符号化部１１で行なった処理に対応する所定の復号化処理を行い元のデータを復元し、受信装置３０より出力する。

【００３３】

このように、本実施の形態の通信システム１においては、送信対象のデータを一旦符号化してその内容を直接的に認識するのを不可能な状態にして、暗号化処理を施している。一般に、暗号化されたファイルを不正に解読する場合には、元のデータを推定してこれと暗号化されたデータとを比較することにより行なうが、本実施の形態の通信システム１においては、前述したように、暗号化処理の前後で元のファイル内容を推定することは実質的に不可能である。具体的には、たとえば、仮に、考え得る全ての暗号化アルゴリズムと鍵とを総当たり方式で適用して解読を試みたとしても、解読された結果のデータは何ら意味をなすデータではないので、解読されているのか否かを確認することができない。したがって、本実施の形態の通信システム１は、このような不正な暗号解読の攻撃に対して、非常に高いセキュリティ性を有する。

【００３４】

また、通信システム１においては、送信対象のデータを複数のファイルに分割し、この各ファイルごとに暗号化アルゴリズムおよび暗号化鍵を選択して暗号化処理を施すことができる。したがって、たとえ１つのファイルについて暗号が解読されたとしても、データ全体の解読にはつながらない。すなわち、データ全体の解読にはより一層の時間と労力が必要となり、その点からも高いセキュリティ性を有すると言うことができる。

【００３５】

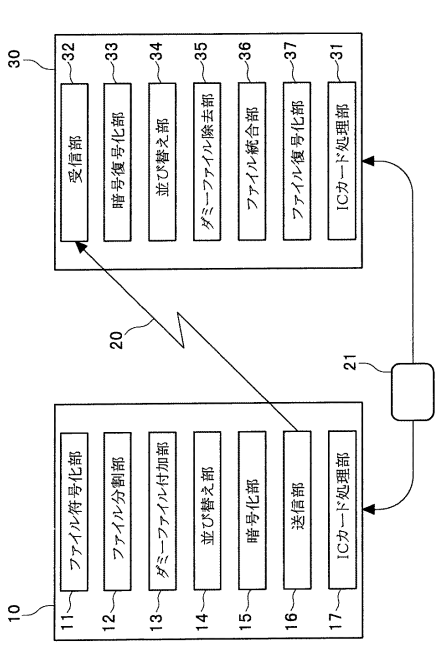
また、通信システム１において、その分割の方法は、バイト単位で細かく分割しているため、この点においても元のデータの推定を困難にして暗号解読を難しくしており、セキュリティ性が高くなっている。

また、通信システム１においては、分割したファイルの順序の並び替えを行なっており、これによってもより一層元のファイルの推定を困難にしており、セキュリテイ性を高めて

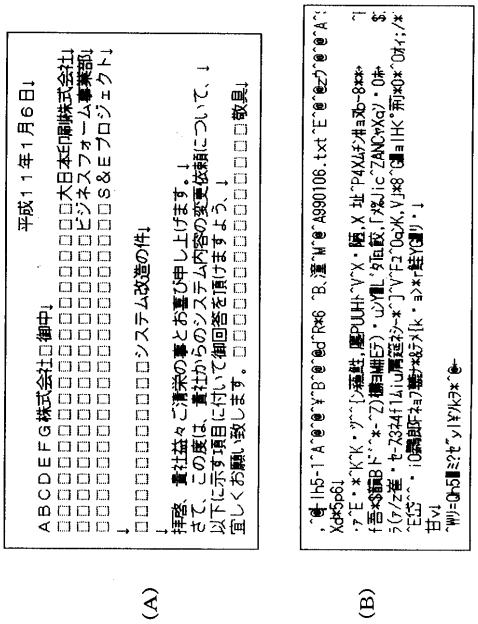
いる。
また、通信システム１においては、ダミーファイルを付加しているので、仮にこのファイルの解読を試みた場合には何ら有効なデータが得られないことになり、暗号解読の試みを困惑させることができ、なお一層セキュリティ性を高めることができる。
【００３６】
さらに、通信システム１においては、暗号化処理およびその解読処理に用いる鍵情報は、送信装置１０で直接ＩＣカード２１に記録され、これが搬送されて受信装置３０に装着され、受信装置３０に直接的に読み込まれる。すなわち、この鍵情報は、伝送路２０によって全く伝送されない。したがって、伝送路２０を伝送される信号を傍受して鍵情報を検出することによりデータを解読しようとする攻撃を完全に防ぐことができ、セキュリティ性を著しく高めることができる。
【００３７】
また、ファイル符号化部１１において行なう符号化処理においてデータサイズが少なくなる、すなわち圧縮される符号化を行なうようにすれば、伝送するデータ量を少なくすることができ、通信時間や通信コストを低減できるという効果も得られる。
【００３８】
なお、本発明は本実施の形態に限られるものではなく、種々の改変が可能である。
たとえば、前述した送信装置１０は、ダミーファイル付加部１３および並び替え部１４を有する構成としたが、本発明の主旨はファイル符号化部１１で符号化したデータをファイル分割部１２で分割し、暗号化部１５で暗号化することにある。したがって、これらダミーファイル付加部１３および並び替え部１４は設けられていなくとも、または、いずれか一方のみを有するような構成であっても、あるいは、暗号化部１５の後にダミーファイルを付加したり並べ替えを行なう手段として設けられていても、何ら差し支えなく、いずれも本発明の範囲内である。
【００３９】
また、送信装置１０のファイル符号化部１１における符号化方法は、任意の方法を用いてよい。この時、データサイズが圧縮される符号化方法であれば、前述したように通信時間や通信コストの点から有効であるが、本発明はこれに限られるものではなく、結果的にデータ量が増大するような符号化方法を用いてもよい。
【００４０】
また、送信装置１０のファイル分割部１２においては、送信対象のデータを順に１バイト、３バイトに繰り返し区切り、順次３つのファイルに再配置したが、分割の方法は、この方法に限られるものではなく、任意の方法により分割してよい。
また、分割するファイルの数も、３に限られるものではなく、任意の数に分割してよい。
もちろん、送信対象のデータは、図２に示したようなテキストファイルである必要はなく、任意の形式のデータでよい。
【００４１】
また、送信装置１０のダミーファイル付加部１３において、本実施の形態においては、後段に並び替え部１４が具備されているので、ダミーファイルをファイル分割部１２で分割された送信対象の実データの最後に付加するものとしたが、たとえば、後段に並び替え部１４が設けられてないような構成の場合には、分割された複数のファイルのいずれかのファイルの間に配置させるのが好適である。本発明は、そのような構成により実施してもよい。
【００４２】
また、送信装置１０の暗号化部１５においては、送信対象のファイル個々に異なる鍵を用いて暗号化を行なっているが、全体を同じ鍵を用いて暗号化を行なったり、反対にファイル個々に異なる暗号化アルゴリズムを用いて暗号化するようにしてもよい。
【００４３】
その他、暗号化部１５における暗号化方式、暗号化アルゴリズム、鍵の生成方法、送信部１６の構成、使用する通信路の形態、ＩＣカード処理部１７の構成および適用するＩＣカ

ード２１の形態なども、任意の構成、形態でよい。
また、受信装置３０の構成およびその変形例なども、前述した送信装置１０に対応する形態で、任意に変更してよい。
【００４４】
【発明の効果】
以上説明したように、本発明によれば、より秘匿性が高く所望のデータを暗号化することができる、通信に適用して好適な暗号化装置および暗号化方法を提供することができる。また、そのような暗号化装置および暗号化方法により暗号化されたデータを適切に復号化することができる、通信に適用して好適な暗号復号化装置および暗号復号化方法を提供することができる。
さらに、所望のデータを、より高い秘匿性で伝送することができる通信システムを提供することができる。
【図面の簡単な説明】
【図１】図１は、本発明の一実施の形態の通信システムの構成を示すブロック図である。
【図２】図２は、図１に示した通信システムの送信装置のファイル符号化部の処理を説明するための図である。
【図３】図３は、図１に示した通信システムの送信装置のファイル分割部の処理を説明するための図である。
【符号の説明】
１…通信システム
１０…送信装置
１１…ファイル符号化部
１２…ファイル分割部
１３…ダミーファイル付加部
１４…並び替え部
１５…暗号化部
１６…送信部
１７…ＩＣカード処理部
２０…伝送路
２１…ＩＣカード
３０…受信装置
３１…ＩＣカード処理部
３２…受信部
３３…暗号復号化部
３４…並び替え部
３５…ダミーファイル除去部
３６…ファイル統合部
３７…ファイル復号化部

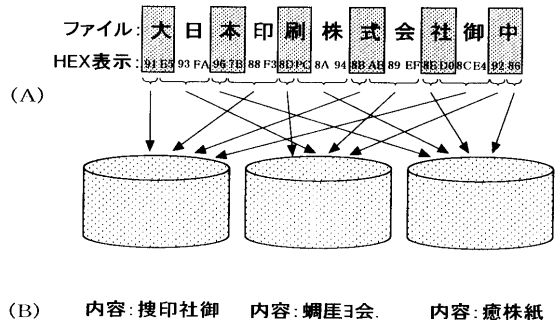
【図１】


30
32 受信部
33 暗号復号化部
34 並び替え部
35 ダミーファイル除去部
36 ファイル統合部
37 ファイル復号化部
31 ICカード処理部
20
21
10
11 ファイル符号化部
12 ファイル分割部
13 ダミーファイル付加部
14 並び替え部
15 暗号化部
16 送信部
17 ICカード処理部

【図２】


平成１１年１月６日
ＡＢＣＤＥＦＧ株式会社□御中
□□□□□□□□□□□□□□□□□□□□□□大日本印刷株式会社
□□□□□□□□□□□□□□□□□□□□□□ビジネスフォーム事業部
□□□□□□□□□□□□□□□□□□□□□□ＳＳ＆Ｅプロジェクト
□□□□□□□□□□□□システム改造の件
拝啓、貴社益々ご清栄のお慶び申し上げます。
さて、この度は、貴社からのシステム内容の変更依頼について、
以下に示す項目に付いて御回答を頂けますよう、
宜しくお願い致します。□□□□□□□□□□□□□□敬具
(A)
(B)

【図３】


ファイル：大 日 本 印 刷 株 式 会 社 御 中
HEX表示：91 E5 93 FA 96 7B 88 F3 8D FC 8A 94 8B AE 89 EF 8E D0 8C E4 92 86
(A)
(B) 内容：捜印社御 内容：蜩匪ヨ会. 内容：癒株紙

フロントページの続き

(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

審査官　金沢　史明

(56)参考文献　特開平７－１４０８９６（ＪＰ，Ａ）
特開平１０－３０３８６４（ＪＰ，Ａ）
特開平８－５６３５６（ＪＰ，Ａ）
特開平７－２８４０７（ＪＰ，Ａ）
国際公開第９６／００２９９２（WO，Ａ１）
特開平１０－１７３６４６（ＪＰ，Ａ）
特開昭６１－１６６２４０（ＪＰ，Ａ）
特許第４３９２８０８（ＪＰ，Ｂ２）
特開平７－２７１２９７（ＪＰ，Ａ）
特開平７－２８１５９６（ＪＰ，Ａ）
特開平１０－３２２５６０（ＪＰ，Ａ）
特開平１１－５５２４１（ＪＰ，Ａ）
特開平１１－６５４３９（ＪＰ，Ａ）
特開２０００－５９３５５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/00- 9/32
G09C　1/00