(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2015-45674
(P2015-45674A)
(43)公開日　平成27年3月12日(2015.3.12)

(51)Int.Cl.		F I			テーマコード（参考）
G09C 1/00 (2006.01)		G09C	1/00	610A	5J104

審査請求 未請求　請求項の数 6　ＯＬ　（全 12 頁）

(21)出願番号　特願2013-175191 (P2013-175191)
(22)出願日　平成25年8月27日 (2013.8.27)

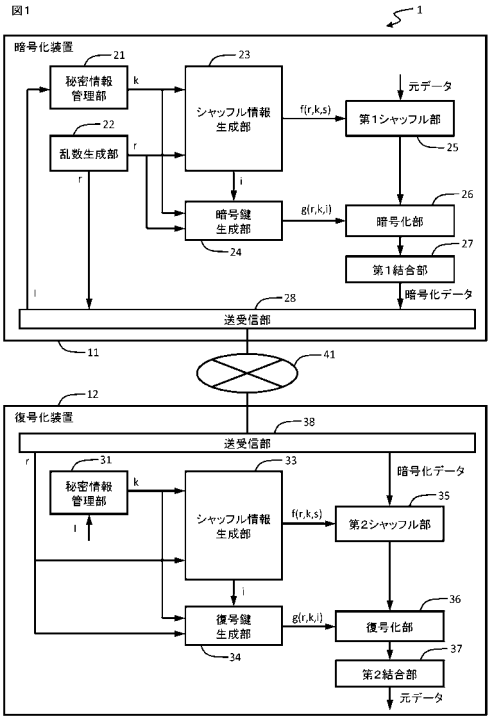
(71)出願人　000153443
株式会社　日立産業制御ソリューションズ
茨城県日立市大みか町五丁目１番２６号
(74)代理人　110000279
特許業務法人ウィルフォート国際特許事務所
(72)発明者　渡邊　健治
茨城県日立市大みか町五丁目２番１号　株式会社日立情報制御ソリューションズ内
(72)発明者　小室　和彦
茨城県日立市大みか町五丁目２番１号　株式会社日立情報制御ソリューションズ内
(72)発明者　山口　博史
茨城県日立市大みか町五丁目２番１号　株式会社日立情報制御ソリューションズ内

Ｆターム(参考)　5J104 AA43　FA06　JA03　NA02　PA07

(54)【発明の名称】暗号化システム、暗号化方法及びコンピュータプログラム

(57)【要約】
【課題】データの盗聴に対する安全性を高める。
【解決手段】暗号化装置は、元データに対するブロック番号とブロック長とシャッフル番号と鍵情報とを含むブロック情報を生成し、元データを、ブロック番号の順番にそのブロック番号に対応するブロック長で分割し、各ブロックを暗号化し、シャッフル番号の順番に並び替えて結合し、暗号化データを生成する。復号化装置は、暗号化装置と同一のブロック情報を生成し、暗号化データを、シャッフル番号の順番にそのシャッフル番号に対応するブロック長で分割し、各ブロックを復号化し、ブロック番号の順番に並び替えて結合し、元データを復元する。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
暗号化装置と復号化装置とを備える暗号化システムであって、
暗号化装置は、
元データを複数のブロックに分割した際の各々のブロックを示すブロック番号と、前記ブロック番号に対応するブロック長と、前記ブロック番号に対応するシャッフル番号と、前記ブロック番号に対応する鍵情報と、を含むブロック情報を生成するブロック情報生成部と、
前記元データを、ブロック番号の順番に、そのブロック番号に対応するブロック長で分割し、複数のブロックを生成する第１分割部と、
前記複数のブロックの各々を、そのブロック番号に対応する鍵情報を用いて暗号化し、複数の暗号化ブロックを生成する暗号化部と、
前記複数の暗号化ブロックを、シャッフル番号の順番に並び替えて結合し、暗号化データを生成する第１結合部と、を有し、
復号化装置は、
前記暗号化装置と同一のブロック情報を生成するブロック情報生成部と、
前記暗号化装置で生成された暗号化データを、シャッフル番号の順番に、そのシャッフル番号に対応するブロック長で分割し、複数の暗号化ブロックを生成する第２分割部と、
複数の暗号化ブロックの各々を、そのシャッフル番号に対応する鍵情報を用いて復号化し、複数の復号化ブロックを生成する復号化部と、
前記複数の復号化ブロックを、ブロック番号の順番に並び替えて結合し、前記元データを復元する第２結合部と、を有する
暗号化システム。

【請求項２】
前記元データの分割数と、前記ブロック番号に対応する前記ブロック長と、前記ブロック番号に対応する前記シャッフル番号とは、所定の秘密情報と、前記元データに対応する乱数と、前記元データのデータ長とに基づいて一意に決定される
請求項１に記載の暗号化システム。

【請求項３】
前記暗号化装置は、前記元データに対応する乱数を、前記復号化装置へ送信し、
前記復号化装置における前記ブロック情報生成部は、前記暗号化装置から受信した前記元データに対応する乱数を用いて、前記元データに対応するブロック情報を生成する
請求項２に記載の暗号化システム。

【請求項４】
前記暗号化装置は、前記元データに対応する乱数と、前記第１結合部において生成された前記暗号化データとを、外部記憶媒体へ書き込み、
前記復号化装置における前記ブロック情報生成部は、前記外部記憶媒体から読み出した前記元データに対応する乱数を用いて、前記元データに対応するブロック情報を生成する
請求項２に記載の暗号化システム。

【請求項５】
データの暗号化方法であって、
暗号化装置において、
元データを複数のブロックに分割した際の各々のブロックを示すブロック番号と、前記ブロック番号に対応するブロック長と、前記ブロック番号に対応するシャッフル番号と、前記ブロック番号に対応する鍵情報と、を含むブロック情報を生成し、

前記元データを、ブロック番号の順番に、そのブロック番号に対応するブロック長で分割し、複数のブロックを生成し、
前記複数のブロックの各々を、そのブロック番号に対応する鍵情報を用いて暗号化し、複数の暗号化ブロックを生成し、
前記複数の暗号化ブロックを、シャッフル番号の順番に並び替えて結合し、暗号化データを生成し、
復号化装置において、
前記暗号化装置と同一のブロック情報を生成し、
前記暗号化装置で生成された暗号化データを、シャッフル番号の順番に、そのシャッフル番号に対応するブロック長で分割し、複数の暗号化ブロックを生成し、
複数の暗号化ブロックの各々を、そのシャッフル番号に対応する鍵情報を用いて復号化し、複数の復号化ブロックを生成し、
前記複数の復号化ブロックを、ブロック番号の順番に並び替えて結合し、前記元データを復元する
データの暗号化方法。

【請求項６】
データの暗号化に係るコンピュータプログラムであって、
暗号化装置において実行されると、
元データを複数のブロックに分割した際の各々のブロックを示すブロック番号と、前記ブロック番号に対応するブロック長と、前記ブロック番号に対応するシャッフル番号と、前記ブロック番号に対応する鍵情報と、を含むブロック情報を生成し、
前記元データを、ブロック番号の示す順番に、そのブロック番号に対応するブロック長で分割し、複数のブロックを生成し、
前記複数のブロックの各々を、そのブロック番号に対応する鍵情報を用いて暗号化し、複数の暗号化ブロックを生成し、
前記複数の暗号化ブロックの各々を、シャッフル番号の順番に並び替えて結合し、暗号化データを生成し、
復号化装置において実行されると、
前記暗号化装置と同一のブロック情報を生成し、
前記暗号化装置で生成された暗号化データを、シャッフル番号の順番に、そのシャッフル番号に対応するブロック長で分割し、複数の暗号化ブロックを生成し、
複数の暗号化ブロックの各々を、そのシャッフル番号に対応する鍵情報を用いて復号化し、複数の復号化ブロックを生成し、
前記複数の復号化ブロックを、ブロック番号の順番に並び替えて結合し、前記元データを復元する
コンピュータプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データの暗号化および復号化の技術に関する。
【背景技術】
【０００２】
送信データを複数のブロックに分割し、各ブロックをそれぞれ異なる暗号鍵で暗号化し、その暗号化ブロックを送信する暗号化通信方法は知られている（特許文献１）。
【先行技術文献】
【特許文献】

【０００３】
【特許文献１】特開平１０－３１３３０６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
特許文献１の暗号化通信方法において、通信の途中で暗号化ブロックが盗聴された場合、その盗聴者は、その暗号化ブロックのデータサイズを知ることができる。暗号化ブロックのデータサイズは、その暗号化ブロックの解読のヒントの一つとなりえる。
【０００５】
そこで、本発明の目的は、暗号化ブロックのデータサイズを隠蔽し、送信データの盗聴に対する安全性を高めることができるようにした暗号化システム、暗号化方法及びコンピュータプログラムを提供することにある。
【課題を解決するための手段】
【０００６】
本発明の一実施例に係る暗号化システムは、暗号化装置と復号化装置とを備える。
暗号化装置は、
元データを複数のブロックに分割した際の各々のブロックを示すブロック番号と、ブロック番号に対応するブロック長と、ブロック番号に対応するシャッフル番号と、ブロック番号に対応する鍵情報と、を含むブロック情報を生成するブロック情報生成部と、
元データを、ブロック番号の順番に、そのブロック番号に対応するブロック長で分割し、複数のブロックを生成する第１分割部と、
複数のブロックの各々を、そのブロック番号に対応する鍵情報を用いて暗号化し、複数の暗号化ブロックを生成する暗号化部と、
複数の暗号化ブロックの各々を、シャッフル番号の順番に並び替えて結合し、暗号化データを生成する第１結合部と、を有する。
復号化装置は、
暗号化装置と同一のブロック情報を生成するブロック情報生成部と、
暗号化装置で生成された暗号化データを、シャッフル番号の順番に、そのシャッフル番号に対応するブロック長で分割し、複数の暗号化ブロックを生成する第２分割部と、
複数の暗号化ブロックの各々を、そのシャッフル番号に対応する鍵情報を用いて復号化し、複数の復号化ブロックを生成する復号化部と、
複数の復号化ブロックを、ブロック番号の順番に並び替えて結合し、元データを復元する第２結合部と、を有する。
【発明の効果】
【０００７】
本発明によれば、暗号化ブロックのデータサイズを隠蔽し、送信データの盗聴に対する安全性を高めることができる。
【図面の簡単な説明】
【０００８】
【図１】暗号化システムの備える暗号化装置および復号化装置の機能構成の一例を示す。
【図２】シャッフル情報に含まれる情報の一例を示す。
【図３】暗号化装置が元データから暗号化データを生成する過程の一例を示す。
【図４】復号化装置が暗号化データから元データを生成する過程の一例を示す。
【図５】暗号化装置および復号化装置の処理の一例を示すフローチャートである。
【発明を実施するための形態】
【０００９】
以下、暗号化装置と復号化装置との間で盗聴に対して安全にデータをやりとりすることのできる暗号化システム実施例について、図面を参照しながら説明する。
【実施例１】
【００１０】

図１は、暗号化システム１の備える暗号化装置１１および復号化装置１２の機能構成の一例を示す。

【００１１】

暗号化システム１は、暗号化装置１１と、復号化装置１２とを備える。暗号化装置１１と復号化装置１２とは、通信ネットワーク４１を介して、データを送受信する。

【００１２】

暗号化装置１１および復号化装置１２はそれぞれ、ＣＰＵ、メモリ、記憶媒体および通信デバイス（何れも不図示）などを備える計算機装置であり、所定のコンピュータプログラムをＣＰＵ等で実行することにより、図１に示す各種機能を実現する。

【００１３】

メモリは、例えば、ＤＲＡＭ（Ｄｙｎａｍｉｃ　Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）などによって構成される。記憶媒体は、例えば、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）またはフラッシュメモリなどによって構成される。通信デバイスは、例えば、Ｅｔｈｅｒｎｅｔ（登録商標）、無線ＬＡＮ（ＩＥＥＥ８０２．１１）または３Ｇ／ＬＴＥ（Ｌｏｎｇ　Ｔｅｒｍ　Ｅｖｏｌｕｔｉｏｎ）などに対応するデバイスによって構成される。通信ネットワークは、例えば、有線／無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）又はインターネット網、もしくはこれらの組み合わせによって構成される。

【００１４】

＜暗号化装置＞

暗号化装置１１は、機能として、送受信部２８と、秘密情報管理部２１と、乱数生成部２２と、シャッフル情報生成部２３と、暗号鍵生成部２４と、第１シャッフル部２５と、暗号化部２６と、第１結合部２７とを有する。

【００１５】

秘密情報管理部２１は、ユーザ情報Ｉおよび秘密情報ｋを保持すると共に、ユーザ情報Ｉと秘密情報ｋとの対応関係を管理する。ユーザ情報Ｉは、ユーザ又は装置を一意に識別し得る情報である。秘密情報ｋは、後述するシャッフル情報１００と、暗号／復号用の鍵とを生成するための情報である。秘密情報ｋは、ユーザ情報Ｉと一意の対応関係を有する。秘密情報ｋは、例えば、耐タンパ性を有する不揮発性メモリなどに格納され、外部に漏洩しないように保護される。秘密情報管理部２１は、ユーザ情報Ｉが入力されると、そのユーザ情報Ｉに対応する秘密情報ｋを、シャッフル情報生成部２３および暗号鍵生成部２４に提供する。

【００１６】

乱数生成部２２は、乱数ｒを生成する。乱数生成部２２は、生成した乱数ｒを、シャッフル情報生成部２３および暗号鍵生成部２４に提供する。また、乱数生成部２２は、その生成した乱数ｒを、復号化装置１２に送信する。乱数生成部２２は、復号化装置１２からのデータ要求を受信したことをトリガーとして、乱数ｒを生成してもよい。もしくは、乱数生成部２２は、シャッフル情報生成部２３からの乱数の要求をトリガーとして、乱数ｒを生成してもよい。

【００１７】

シャッフル情報生成部２３は、シャッフル情報１００を生成する。シャッフル情報生成部２３は、乱数生成部２２から提供された乱数ｒと、秘密情報管理部２１から提供された秘密情報ｋと、復号化装置１２へ送信する元データのデータ長ｓと、を所定の関数ｆ（ｒ，ｋ，ｓ）に代入して、シャッフル情報１００を生成する。関数ｆは、例えば、ｒ，ｋ，ｓからｆ（ｒ，ｋ，ｓ）の算出は容易であるが、ｆ（ｒ，ｋ，ｓ）からｒ，ｋ，ｓを推測することは極めて困難な一方向性関数である。秘密情報ｋと、乱数ｒと、データ長ｓとが全て同一の場合は、同一のシャッフル情報１００が生成される。シャッフル情報１００も、例えば、耐タンパ性を有する不揮発性メモリなどに格納される。

【００１８】

図２は、シャッフル情報１００に含まれる情報の一例を示す。なお、図２は、説明の便

宜上、シャッフル情報１００をテーブル形式で表記しているが、暗号化装置１１の内部において、シャッフル情報１００がこのように管理されていることを示すものではない。

【００１９】

シャッフル情報１００には、ブロックの数と、ブロック番号１０１と、オフセット１０２と、ブロック長１０３と、シャッフル番号１０４との対応関係を示す情報が含まれる。

【００２０】

ブロックの数は、元データをいくつのブロックに分割するかを示す。元データをいくつのブロックに分割するかは、ｆ（ｒ，ｋ，ｓ）によって決定される。図２に示すシャッフル情報１００おいては、ブロック番号１０１の最大数がブロックの数に対応する。

【００２１】

ブロック番号１０１は、元データを複数のブロックに分割したときに、先頭のブロックから順番に割り当てられる番号である。つまり、分割された複数のブロックを、ブロック番号の順番に結合すると、元データが復元される。

【００２２】

オフセット１０２は、ブロック番号１０１の示すブロックの元データにおける開始位置を示す。ブロック長１０３は、ブロック番号１０１の示すブロックの長さ（データサイズ）を示す。オフセット１０２およびブロック長１０３は、例えば、Ｂｙｔｅ単位で指定される。本実施例において、ブロック長１０３は、ブロック毎に異なり得る。しかし、全てのブロックが同じブロック長１０３であってもよい。各ブロックをどのくらいの長さにするかも、ｆ（ｒ，ｋ，ｓ）によって決定される。

【００２３】

シャッフル番号１０４は、複数のブロックのシャッフル後の順番を示す。後述する第１結合部２７は、このシャッフル番号１０４の順番にブロックを並び替えて結合する。各ブロックがどのシャッフル番号となるかも、ｆ（ｒ，ｋ，ｓ）によって決定される。

【００２４】

例えば、図２の行１１０は、ブロック番号１０１が「３」のブロックは、元データの先頭から「２５０ｂｙｔｅ（オフセット）」を開始位置として「２００ｂｙｔｅ（ブロック長）」分を抽出したデータであり、シャッフル後の順番は「１番目（シャッフル番号）」であることを示す。以下、図１の説明に戻る。

【００２５】

暗号鍵生成部２４は、暗号鍵を生成する。暗号鍵生成部２４は、ブロック毎に異なる暗号鍵を生成する。暗号鍵生成部２４は、乱数生成部２２から提供された乱数ｒと、秘密情報管理部２１から提供されたｋと、シャッフル情報生成部２３において生成されたシャッフル情報１００に含まれるブロック番号ｉと、を所定の関数ｇ（ｒ，ｋ，ｉ）に代入し、暗号鍵を生成する。関数ｇは、例えば、ｒ，ｋ，ｉからｇ（ｒ，ｋ，ｉ）の算出は容易であるが、ｇ（ｒ，ｋ，ｉ）からｒ，ｋ，ｉを推測することは極めて困難な一方向性関数である。乱数ｒと、秘密情報ｋと、ブロック番号ｉとが全て同一の場合は、同一の暗号鍵が生成される。暗号鍵生成部２４は、ブロック番号ｉに対応する暗号鍵を、暗号化部２６へ提供する。

【００２６】

第１シャッフル部２５は、元データを先頭から、シャッフル情報１００の有するブロック番号１０１の順番に、そのブロック番号１０１に対応するオフセット１０２およびブロック長１０３に従って、複数のブロックに分割する。そして、第１シャッフル部２５は、複数のブロックを、シャッフル情報１００の有するシャッフル番号１０４の順番に並び替える。

【００２７】

暗号化部２６は、第１シャッフル部２５で分割された複数のブロックの各々を、そのブロックに対応する暗号鍵で暗号化する。つまり、暗号化部２６は、ブロック番号ｉのブロックを、暗号鍵ｇ（ｒ，ｋ，ｉ）を用いて暗号化する。以下、暗号化されたブロックを「暗号化ブロック」という。

【００２８】
第１結合部２７は、第１シャッフル部２５によって分割及び並び替えられ、暗号化部２６によって暗号化された複数の暗号化ブロックを、シャッフル情報１００の有するシャッフル番号１０１の順番に結合し、暗号化データを生成する。
【００２９】
送受信部２８は、通信ネットワーク１４を通じて、復号化装置１２と様々なデータを送受信する。送受信部２８の受信したユーザ情報Ｉは、秘密情報管理部２１へ提供される。送受信部２８は、乱数ｒを復号化装置１２へ送信する。送受信部２８は、暗号化データを復号化装置１２へ送信する。
【００３０】
図３は、暗号化装置１１が元データから暗号化データを生成する過程の一例を示す。
（１）第１シャッフル部２５は、所定の記憶媒体から元データを読み出す。
（２）第１シャッフル部２５は、元データの先頭から、図２に示すシャッフル情報１００のブロック番号１０１の順番に、そのブロック番号１０１に対応するオフセット１０２およびブロック長１０３に従って、ブロック長１０３の異なる複数のブロック１、２。３、４に分割する。
（３）第１シャッフル部２５は、複数のブロック１、２、３、４を、図２に示すシャッフル情報１００のシャッフル番号１０４の順番に従って、ブロック番号３、２、４、１に並べ替える。
（４）暗号化部２６は、ブロック番号３、２、４、１のブロックをそれぞれ、暗号鍵ｇ（ｒ，ｋ，３）、ｇ（ｒ，ｋ，２）、ｇ（ｒ，ｋ，４）、ｇ（ｒ，ｋ，１）で暗号化する。
（５）第１結合部２７は、図２に示すシャッフル情報１００のシャッフル番号１０４の順番に従って、ブロック番号３、２、４、１の順番に暗号化ブロックを結合し、暗号化データを生成する。
【００３１】
なお、上記の（３）と（４）は、入れ替えられてもよい。つまり、（２）元データの分割後、（３）暗号鍵を用いてブロック１、２、３、４を暗号化し、（４）暗号化したブロック１、２、３、４を、シャッフル情報１００のシャッフル番号１０４に従ってブロック３、２、４、１の順番に並び替えてから、（５）結合してもよい。以下、図１の説明に戻る。
【００３２】
＜復号化装置＞
復号化装置１２は、機能として、送受信部３８と、秘密情報管理部３１と、シャッフル情報生成部３３と、復号鍵生成部３４と、第２シャッフル部３５と、復号化部３６と、第２結合部３７とを有する。
【００３３】
秘密情報管理部３１は、基本的に、暗号化装置１１の秘密情報管理部２１と同様の機能を有する。暗号化装置１１の秘密情報管理部２１と、復号化装置１２の秘密情報管理部３１とは、同じユーザ情報Ｉおよび秘密情報ｋを保持すると共に、同じユーザ情報Ｉと秘密情報ｋとの対応関係を管理する。
【００３４】
秘密情報ｋは、予め（例えば、製造段階で）暗号化装置１１および復号化装置１２に格納されていてもよいし、所定のサーバからセキュアな通信経路を介して取得されて暗号化装置１１および復号化装置１２に格納されてもよい。
【００３５】
シャッフル情報生成部３３は、基本的に、暗号化装置１１のシャッフル情報生成部２３と同様の機能及び関数ｆ（ｒ，ｋ，ｓ）を有する。シャッフル情報生成部３３は、乱数ｒについては、暗号化装置１１から送信されたものを使用する。シャッフル情報生成部３３は、データ長ｓについては、暗号化装置１１から送信された暗号化データのデータ長から算出する。これにより、シャッフル情報生成部３３は、関数ｆ（ｒ，ｋ，ｓ）を用いて、

暗号化装置１１と同じシャッフル情報１００を生成することができる。
【００３６】
復号鍵生成部３４は、復号鍵を生成する。暗号鍵と復号鍵とが共通鍵である場合、復号鍵生成部３４は、基本的に、暗号鍵生成部３４と同様の機能及び関数ｇ（ｒ，ｋ，ｉ）を有する。復号鍵生成部３４は、乱数ｒについては、暗号化装置１１から送信されたものを使用する。これにより復号鍵生成部３４は、関数ｇ（ｒ，ｋ，ｉ）を用いて、各暗号化ブロックの復号鍵を生成することができる。
【００３７】
第２シャッフル部３５は、暗号化データを先頭から、シャッフル情報１００の有するシャッフル番号１０４の順番に、そのシャッフル番号１０４に対応するオフセット１０１およびデータ長１０２に従って、複数の暗号化ブロックに分割する。そして、第２シャッフル部３５は、複数の暗号化ブロックを、シャッフル情報１００の有するブロック番号１０１の順番に並び替える。
【００３８】
復号化部３６は、第２シャッフル部３５で分割された複数の暗号化ブロックの各々を、そのブロックに対応する復号鍵で復号化する。つまり、復号化部３６は、ブロック番号ｉのブロックを、復号鍵ｇ（ｒ，ｋ，ｉ）を用いて復号化する。
【００３９】
第２結合部３７は、第２シャッフル部３５によって分割され、ブロック番号１０１の順番（元の順番）に並び替えられ、復号化部３６によって復号化された複数のブロックを、シャッフル情報１００の有するブロック番号１０１の順番に結合し、元データを生成する。
【００４０】
送受信部３８は、通信ネットワーク１４を通じて、暗号化装置１１と様々なデータを送受信する。送受信部３８は、ユーザ情報Ｉおよびデータ要求を暗号化装置１１へ送信する。送受信部３８の受信した暗号化データは、第２シャッフル部３５へ提供される。
【００４１】
図４は、復号化装置１２が暗号化データから元データを生成する過程の一例を示す。
（１）第２シャッフル部３５は、送受信部３９を通じて、暗号化データを受信する。
（２）第２シャッフル部３５は、暗号化データの先頭から、図２に示すシャッフル情報１００のシャッフル番号１０１の順番に、そのシャッフル番号１０１に対応するオフセット１０２およびブロック長１０３に従って、ブロック長の異なる複数の暗号化ブロック３、２、４、１に分割する。
（３）第２シャッフル部３５は、複数の暗号化ブロック３、２、４、１を、図２に示すシャッフル情報１００のブロック番号１０１の順番に従って、ブロック番号１、２、３、４に並べ替える。
（４）復号化部３６は、ブロック番号１、２、３、４の暗号化ブロックをそれぞれ、復号鍵ｇ（ｒ，ｋ，１）、ｇ（ｒ，ｋ，２）、ｇ（ｒ，ｋ，３）、ｇ（ｒ，ｋ，４）で復号化する。
（５）第２結合部３７は、図２に示すシャッフル情報１００のブロック番号１０１の順番に従って、ブロック番号１、２、３、４の順番にブロックを結合し、元データを復元する。
【００４２】
なお、上記の（３）と（４）は、入れ替えられてもよい。つまり、（２）暗号化データの分割後、（３）復号鍵を用いてブロック３、２、４、１を復号化し、（４）復号化したブロック３、２、４、１を、シャッフル情報のブロック番号に従ってブロック１、２、３、４の順番に並び替えてから、（５）結合してもよい。
【００４３】
図５は、暗号化装置１１および復号化装置１２の処理の一例を示すフローチャートである。

【００４４】
復号化装置１２は、暗号化装置１１に、データ要求およびユーザ情報Ｉを送信する（Ｓ１０）。ユーザ情報Ｉは、データ要求に含まれていてもよい。
【００４５】
データ要求を受信した暗号化装置１１は、乱数ｒを生成し、その乱数ｒを復号化装置１２へ送信する（Ｓ１１）。
【００４６】
そして、暗号化装置１１は、その生成した乱数ｒと、復号化装置１２から受信したユーザ情報Ｉに対応する秘密情報ｋと、復号化装置１２へ送信する元データのデータ長ｓとを用いて、シャッフル情報ｆ（ｒ，ｋ，ｓ）を生成する（Ｓ１２）。
【００４７】
暗号化装置１１は、その生成したシャッフル情報１００のブロック番号１０１の順番に、元データを、そのブロック番号１０１に対応するオフセット１０２およびデータ長１０３に従って分割し、複数のブロックを生成する（Ｓ１３）。
【００４８】
暗号化装置１１は、その複数のブロックをシャッフル情報１００のシャッフル番号１０４の順番に並び替える（Ｓ１４）。
【００４９】
暗号化装置１１は、ブロック番号１０１毎に異なる暗号鍵ｇ（ｒ，ｋ，ｉ）を生成する（Ｓ１５）。
暗号化装置１１は、ブロック番号１０１に対応するブロックを、そのブロック番号１０１に対応する暗号鍵ｇ（ｒ，ｋ，ｉ）を用いて暗号化する（Ｓ１６）。
【００５０】
暗号化装置１１は、複数の暗号化ブロックを、シャッフル情報１００のシャッフル番号１０１の順番に結合し、暗号化データを生成する（Ｓ１７）。
暗号化装置１１は、その暗号化データを、復号化装置１２へ送信する（Ｓ１８）。
【００５１】
暗号化データを受信した復号化装置１２は、暗号化装置１１から受信した乱数ｒと、暗号化装置１１へ送信したユーザ情報Ｉに対応する秘密情報ｋと、暗号化装置１１から受信した暗号化データのデータ長ｓとを関数ｆ（ｒ，ｋ，ｓ）へ代入し、シャッフル情報１００を生成する（Ｓ２２）。このシャッフル情報１００は、暗号化装置１１で生成されたシャッフル情報１００と同じである。
【００５２】
復号化装置１２は、その生成したシャッフル情報１００のシャッフル番号１０４の順番に、暗号化データを、そのシャッフル番号１０４に対応するオフセット１０２およびデータ長１０３に従って分割し、複数の暗号化ブロックを生成する（Ｓ２３）。
【００５３】
復号化装置１２は、その複数の暗号化ブロックをシャッフル情報１００のブロック番号１０１の順番（元の順番）に並び替える（Ｓ２４）。
【００５４】
復号化装置１２は、ブロック番号１０１毎に異なる復号鍵ｇ（ｒ，ｋ，ｉ）を生成する（Ｓ２５）。暗号鍵と復号鍵とが共通鍵である場合、この復号鍵は、暗号化装置１１で生成された暗号鍵と同じである。
【００５５】
復号化装置１２は、ブロック番号１０１に対応するブロックを、そのブロック番号１０１に対応する復号鍵ｇ（ｒ，ｋ，ｉ）を用いて復号化する（Ｓ２６）。
【００５６】
復号化装置１２は、複数の複合化されたブロックを、シャッフル情報１００のブロック番号１０１の順番に結合し、元データを生成する（Ｓ２７）
【００５７】

以上の処理により、暗号化装置１１は、復号化装置１２に元データをセキュアに送信することができる。そして、上述の構成によれば、第三者（盗聴者）に暗号化データが解読される虞をさらに小さくすることができる。なぜなら、暗号化データは、異なるブロック長の暗号化ブロックが結合されて構成されているため、第三者は、暗号化データを解読しようとしても、その暗号化データの分割位置を推測することができないからである。さらに、それぞれのブロック長が異なり、ブロックの順番も並び替えられており、各ブロックが異なる暗号鍵で暗号化されていることもまた、第三者の暗号化データの解読を困難にする。また、ブロック内にブロック番号に関する情報も含まれていないため、第三者の暗号化データの解読をさらに困難にする。

【００５８】

＜変形例＞

上述の実施例は、以下のように変形されてもよい。

【００５９】

（１）上述において、暗号化装置１１と復号化装置１２は、それぞれ独自にシャッフル情報１００を生成している。しかし、暗号化装置１１は、生成したシャッフル情報１００を暗号化し、暗号化データと一緒に復号化装置１２へ送信してもよい。そして、復号化装置１２は、その暗号化装置１１から送信されたシャッフル情報１００を用いて、暗号化データを元データに変換してもよい。これにより、復号化装置１２は、自分でシャッフル情報１００を生成する必要がなくなる。つまり、復号化装置１２の処理負荷が軽減される。

【００６０】

（２）暗号化装置１１は、暗号化データを外部記憶媒体（ＵＳＢメモリ又はＳＤカード等）に出力する機能を有し、復号化装置１２は、その外部記憶媒体から暗号化データを読み出して、元データを生成する機能を有してもよい。この場合、例えば、暗号化装置１１は、自己のユーザ情報Ｉと生成した乱数ｒとを暗号化データと合わせて外部記憶媒体に出力する。そして、復号化装置１２は、外部記憶媒体に格納されているユーザ情報Ｉと乱数ｒとを用いて、暗号化データを元データに変換する。

【００６１】

（３）上記（２）の構成において、暗号化装置１１は、生成したシャッフル情報１００を暗号化して、暗号化データと共に外部記憶媒体へ出力してもよい。そして、復号化装置１２は、その外部記憶媒体から読み出したシャッフル情報１００を用いて、暗号化データを元データに変換してもよい。

【００６２】

（４）上記（２）又は（３）の構成において、暗号化装置１１は、１つの乱数ｒを用いて複数の暗号化データを生成した場合、その１つの乱数ｒと複数の暗号化データとをまとめて外部記憶媒体へ出力してもよい。そして、復号化装置１２は、その外部記憶媒体から読み出した１つの乱数ｒを用いて、複数の暗号化データをそれぞれ元データに変換してもよい。

【００６３】

（５）暗号鍵および復号鍵として用いられる共通鍵は、例えば、ＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）、Ｔｒｉｐｌｅ ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）、ＲＣ４等の暗号アルゴリズムを用いて生成されてよい。

【００６４】

（６）暗号鍵と復号鍵は、共通鍵でなく、何れか一方が「秘密鍵」で他方が「公開鍵」であってもよい。

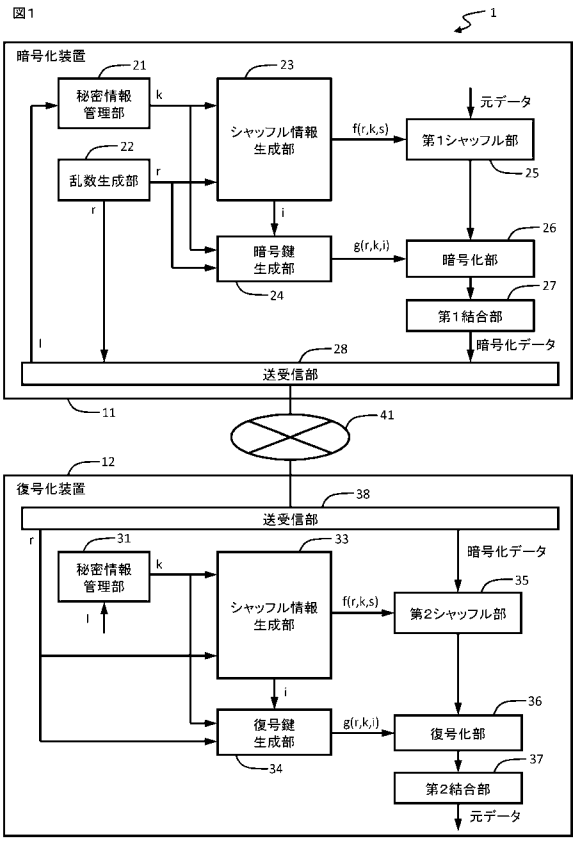
【００６５】

上述した本発明の実施例は、本発明の説明のための例示であり、本発明の範囲をそれらの実施例にのみ限定する趣旨ではない。当業者は、本発明の要旨を逸脱することなしに、他の様々な態様で本発明を実施することができる。

【符号の説明】

【００６６】
１…暗号化システム　１１…暗号化装置　１２…復号化装置

【図１】
図1



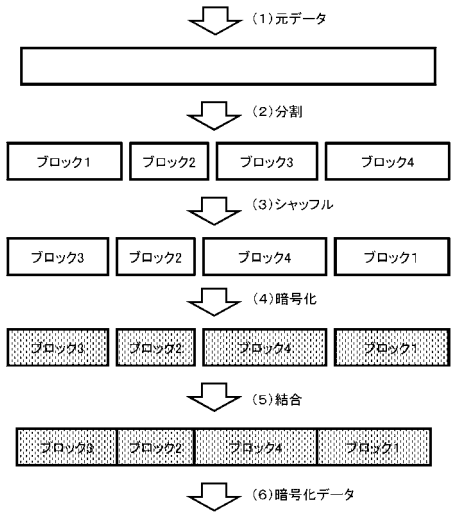
【図２】
図2

100
シャッフル情報

101 ブロック番号	102 オフセット (Byte)	103 ブロック長 (byte)	104 シャッフル番号
1	0	150	4
2	150	100	2
3	250	200	1
4	450	180	3

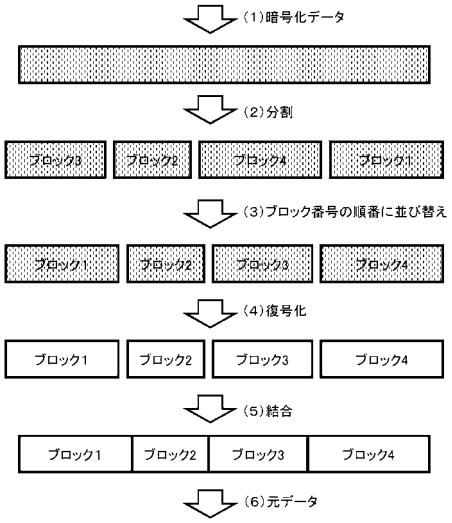
110

【図３】
図3



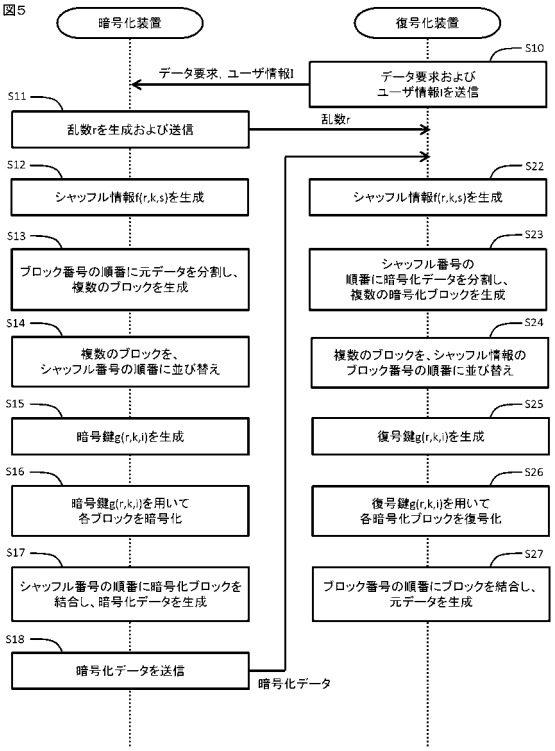
【図４】

図4


(1)暗号化データ
(2)分割
ブロック3
ブロック2
ブロック4
ブロック1
(3)ブロック番号の順番に並び替え
ブロック1
ブロック2
ブロック3
ブロック4
(4)復号化
ブロック1
ブロック2
ブロック3
ブロック4
(5)結合
ブロック1
ブロック2
ブロック3
ブロック4
(6)元データ

【図５】

図5


暗号化装置
復号化装置
S10
データ要求、ユーザ情報I
データ要求およびユーザ情報Iを送信
S11
乱数rを生成および送信
乱数r
S12
シャッフル情報f(r,k,s)を生成
S22
シャッフル情報f(r,k,s)を生成
S13
ブロック番号の順番に元データを分割し、複数のブロックを生成
S23
シャッフル番号の順番に暗号化データを分割し、複数の暗号化ブロックを生成
S14
複数のブロックを、シャッフル番号の順番に並び替え
S24
複数のブロックを、シャッフル情報のブロック番号の順番に並び替え
S15
暗号鍵g(r,k,i)を生成
S25
復号鍵g(r,k,i)を生成
S16
暗号鍵g(r,k,i)を用いて各ブロックを暗号化
S26
復号鍵g(r,k,i)を用いて各暗号化ブロックを復号化
S17
シャッフル番号の順番に暗号化ブロックを結合し、暗号化データを生成
S27
ブロック番号の順番にブロックを結合し、元データを生成
S18
暗号化データを送信
暗号化データ