(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4287397号
(P4287397)
(45)発行日　平成21年7月1日(2009.7.1)　(24)登録日　平成21年4月3日(2009.4.3)

(51)Int.Cl.　　F I
G09C 1/00 (2006.01)　　G09C 1/00 610A
H04L 9/06 (2006.01)　　H04L 9/00 611Z

請求項の数 8　(全 11 頁)

(21)出願番号　特願2005-95097(P2005-95097)
(22)出願日　平成17年3月29日(2005.3.29)
(65)公開番号　特開2006-279488(P2006-279488A)
(43)公開日　平成18年10月12日(2006.10.12)
審査請求日　平成18年3月17日(2006.3.17)

（出願人による申告）平成１６年度、総務省、情報通信政策局委託研究「自由でかつ安全なコンテンツ流通を実現するためのエージェントフレームワークの研究開発」、産業活力再生特別措置法第３０条の適用を受けるもの

(73)特許権者　391016358
東芝情報システム株式会社
神奈川県川崎市川崎区日進町１番地５３
(74)代理人　100074147
弁理士　本田　崇
(72)発明者　奥富　秀俊
神奈川県川崎市川崎区日進町７番地１　東芝情報システム株式会社内
(72)発明者　金田　学
神奈川県川崎市川崎区日進町７番地１　東芝情報システム株式会社内
(72)発明者　新田　基博
神奈川県川崎市川崎区日進町７番地１　東芝情報システム株式会社内

最終頁に続く

(54)【発明の名称】暗号文生成装置、暗号文復号装置、暗号文生成プログラム及び暗号文復号プログラム

(57)【特許請求の範囲】
【請求項１】
平文を所定の長さを持つブロックに分割し、分割されたブロック単位にブロック鍵を用いて暗号文生成のための演算を行って暗号文を得る暗号化部と、
ブロック単位の暗号文生成終了毎に所定値をカウントアップまたは所定値をカウントダウンするカウンタと、
現時点において暗号文生成を行っているブロックよりも所定ブロック前に暗号化された暗号文と、前記カウンタによるカウント値と、暗号鍵データとを用いて、暗号化するブロック毎に適用するブロック鍵を作成して前記暗号化部へ与えるブロック鍵作成手段と
を具備することを特徴とする暗号文生成装置。
【請求項２】
暗号文生成の初期時と再開時に、前記カウンタの値と前記所定ブロック前の暗号文のデータとを設定する制御手段が備えられていることを特徴とする請求項１に記載の暗号文生成装置。
【請求項３】
暗号化された暗号文を所定の長さを持つブロックに分割し、分割されたブロック単位にブロック鍵を用いて復号化のための演算を行って平文を得る復号化部と、
ブロック単位の暗号文復号化終了毎に所定値をカウントアップまたは所定値をカウントダウンするカウンタと、
現時点において暗号文復号化を行っているブロックよりも所定ブロック前に復号化に用

いた復号化前の暗号文と、前記カウンタによるカウント値と、暗号鍵データとを用いて、復号化するブロック毎に適用するブロック鍵を作成して前記復号化部へ与えるブロック鍵作成手段と
を具備することを特徴とする暗号文復号装置。
【請求項４】
暗号文復号化の初期時と再開時に、前記カウンタの値と前記所定ブロック前に復号化に用いた復号化前の暗号文のデータとを設定する制御手段が備えられていることを特徴とする請求項３に記載の暗号文復号装置。
【請求項５】
平文から暗号文を得るためにコンピュータを、
平文を所定の長さを持つブロックに分割し、分割されたブロック単位にブロック鍵を用いて暗号文生成のための演算を行って暗号文を得る暗号化手段と、
ブロック単位の暗号文生成終了毎に所定値をカウントアップまたは所定値をカウントダウンするカウント手段と、
現時点において暗号文生成を行っているブロックよりも所定ブロック前に暗号化された暗号文と、前記カウントステップによって得られるカウント値と、暗号鍵データとを用いて、暗号化するブロック毎に適用するブロック鍵を作成して前記暗号化手段へ与えるブロック鍵作成手段と
して機能させるための暗号文生成プログラム。
【請求項６】
前記コンピュータを、更に、
暗号文生成の初期時と再開時に、前記カウント値と前記所定ブロック前の暗号文のデータとを設定する制御手段として機能させることを特徴とする請求項５に記載の暗号文生成プログラム。
【請求項７】
暗号文を復号化するためにコンピュータを、
暗号化された暗号文を所定の長さを持つブロックに分割し、分割されたブロック単位にブロック鍵を用いて復号化のための演算を行って平文を得る復号化手段と、
ブロック単位の暗号文復号化終了毎に所定値をカウントアップまたは所定値をカウントダウンするカウント手段と、
現時点において暗号文復号化を行っているブロックよりも所定ブロック前に復号化に用いた復号化前の暗号文と、前記カウントステップによって得られるカウント値と、暗号鍵データとを用いて、復号化するブロック毎に適用するブロック鍵を作成して前記復号化手段へ与えるブロック鍵作成手段と
して機能させるための暗号文復号プログラム。
【請求項８】
前記コンピュータを、更に、
暗号文復号化の初期時と再開時に、前記カウント値と前記所定ブロック前に復号化に用いた復号化前の暗号文のデータとを設定する制御手段として機能させることを特徴とする請求項７に記載の暗号文復号プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、平文／暗号文を所定の長さを持つブロックに区切り、ブロック単位で暗号化／復号化処理を行う場合に好適な暗号文生成装置、暗号文復号装置、暗号文生成プログラム及び暗号文復号プログラムに関するものである。
【背景技術】
【０００２】
平文の長さより短いブロック長単位に分割されたデータに対し、ブロック毎に暗号化を完結させたいような利用においてストリーム暗号の適用を考えた場合で、かつ、ブロック

毎に同一の暗号鍵を使いまわす場合では、一般的に平文に作用させる擬似乱数はブロック毎に同一パターンとなってしまうため、十分な暗号強度が保たれるとは言い難い。

【０００３】

例えば、特許文献１では、共通の鍵系列発生用基数である種とメディアアクセスユニットナンバー等とから秘密に定義した関数を生成し、これを用いて鍵を作成し、ブロック暗号化することが開示されている。

【特許文献１】特開２００３－１１５８３０号公報

【０００４】

しかしながら、上記の特許文献1においては暗号化のブロック単位に鍵変更を行うストリーム暗号方式のものではない。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

本発明の課題は、鍵変更用の擬似乱数生成アルゴリズムなどの複雑で大掛かりな構成を用いることなく、秘匿性の高い暗号化を行うことが可能な暗号文生成装置を提供することであり、この暗号文生成装置により暗号化された暗号文を復号化する暗号文復号装置を提供し、コンピュータにより上記暗号文生成装置と暗号文復号装置を実現するための暗号文生成プログラム及び暗号文復号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】

本発明に係る暗号文生成装置は、平文を所定の長さを持つブロックに分割し、分割されたブロック単位にブロック鍵を用いて暗号文生成のための演算を行って暗号文を得る暗号化部と、ブロック単位の暗号文生成終了毎に所定値をカウントアップまたは所定値をカウントダウンするカウンタと、現時点において暗号文生成を行っているブロックよりも所定ブロック前に暗号化された暗号文と、前記カウンタによるカウント値と、暗号鍵データとを用いて、暗号化するブロック毎に適用するブロック鍵を作成して前記暗号化部へ与えるブロック鍵作成手段とを具備することを特徴とする。

【０００７】

本発明に係る暗号文生成装置は、暗号文生成の初期時と再開時に、前記カウンタの値と前記所定ブロック前の暗号文のデータとを設定する制御手段が備えられていることを特徴とする。

【０００８】

本発明に係る暗号文復号装置は、暗号化された暗号文を所定の長さを持つブロックに分割し、分割されたブロック単位にブロック鍵を用いて復号化のための演算を行って平文を得る復号化部と、ブロック単位の暗号文復号化終了毎に所定値をカウントアップまたは所定値をカウントダウンするカウンタと、現時点において暗号文復号化を行っているブロックよりも所定ブロック前に復号化に用いた復号化前の暗号文と、前記カウンタによるカウント値と、暗号鍵データとを用いて、復号化するブロック毎に適用するブロック鍵を作成して前記復号化部へ与えるブロック鍵作成手段とを具備することを特徴とする。

【０００９】

本発明に係る暗号文復号装置は、暗号文復号化の初期時と再開時に、前記カウンタの値と前記所定ブロック前に復号化に用いた復号化前の暗号文のデータとを設定する制御手段が備えられていることを特徴とする。

【００１０】

発明に係る暗号文生成プログラムは、平文から暗号文を得るためにコンピュータを、平文を所定の長さを持つブロックに分割し、分割されたブロック単位にブロック鍵を用いて暗号文生成のための演算を行って暗号文を得る暗号化手段と、ブロック単位の暗号文生成終了毎に所定値をカウントアップまたは所定値をカウントダウンするカウント手段と、現時点において暗号文生成を行っているブロックよりも所定ブロック前に暗号化された暗号文と、前記カウントステップによって得られるカウント値と、暗号鍵データとを用いて、

暗号化するブロック毎に適用するブロック鍵を作成して前記暗号化手段へ与えるブロック鍵作成手段として機能させるためのものであることを特徴とする。

【００１１】

発明に係る暗号文生成プログラムは、前記コンピュータを、更に、暗号文生成の初期時と再開時に、前記カウント値と前記所定ブロック前の暗号文のデータとを設定する制御手段として機能させることを特徴とする。

【００１２】

発明に係る暗号文復号プログラムは、暗号文を復号化するためにコンピュータを、暗号化された暗号文を所定の長さを持つブロックに分割し、分割されたブロック単位にブロック鍵を用いて復号化のための演算を行って平文を得る復号化手段と、ブロック単位の暗号文復号化終了毎に所定値をカウントアップまたは所定値をカウントダウンするカウント手段と、現時点において暗号文復号化を行っているブロックよりも所定ブロック前に復号化に用いた復号化前の暗号文と、前記カウントステップによって得られるカウント値と、暗号鍵データとを用いて、復号化するブロック毎に適用するブロック鍵を作成して前記復号化手段へ与えるブロック鍵作成手段として機能させるためのものであることを特徴とする。

【００１３】

発明に係る暗号文復号プログラムは、前記コンピュータを、更に、暗号文復号化の初期時と再開時に、前記カウント値と前記所定ブロック前に復号化に用いた復号化前の暗号文のデータとを設定する制御手段として機能させることを特徴とする。

【発明の効果】

【００１４】

本発明では、所定ブロック前に暗号化された暗号文と、ブロック単位の暗号文生成終了毎にカウントしたカウント値と暗号鍵データとを用いて、暗号化するブロック毎にブロック鍵を作成するので、暗号化のブロック単位に鍵が変更されることになり、ブロック毎に異なる乱数パターンが生成可能となる。また、このような乱数パターンが生成される暗号化手法による暗号文を復号化できる効果を奏する。

【００１５】

また、暗号文生成の初期時と再開時に、前記カウント値と前記所定ブロック前の暗号文のデータとを設定し、暗号文復号化の初期時と再開時に、前記カウント値と前記所定ブロック前に復号化に用いた復号化前の暗号文のデータとを設定するので、初期状態と停止後の再開において暗号化・復号化の適切なるスタートを確保できる。

【発明を実施するための最良の形態】

【００１６】

本発明では、複雑・大掛かりな構成を用いずにブロック毎に異なる乱数パターンを生成可能とするという目的を、所定ブロック前に暗号化された暗号文と、ブロック単位の暗号文生成終了毎にカウントしたカウント値と暗号鍵データとを用いて、暗号化するブロック毎にブロック鍵を作成することにより達成したものである。

【実施例１】

【００１７】

以下添付図面を参照して本発明の実施例を説明する。図１に、暗号文生成装置のブロック図を示す。この暗号文生成装置は、装置全体を統括制御する制御部１を有し、平文格納部２、暗号化部３、ブロック鍵作成部４、暗号鍵記憶部５、ブロックカウンタ６、前暗号文供給部７、暗号文出力部８、暗号文記憶部９を備えている。

【００１８】

平文格納部２には、暗号化すべき平文（暗号化前のデータ）が制御部１の制御によって１ブロック毎（例えば、１バイト毎）に格納される。暗号化部３は、ブロック毎の平文とブロック鍵作成部４により作成されたブロック鍵とに基づいて例えばＸＯＲ（排他的論理和）演算により暗号文生成を行うものである。

【００１９】

ブロック鍵作成部４にはブロックカウンタ６の出力と、前暗号文供給部７により供給される１ステップ前に暗号化された暗号文と、暗号鍵記憶部５から暗号鍵データとが与えられる。ここでは、１ステップ前に暗号化された暗号文を与えたが、一般的には所定ステップ前に暗号化された暗号文を与えることになる。ブロック鍵作成部４は前暗号文供給部７により供給される暗号文を鍵長に揃える圧縮を行い、暗号文と暗号鍵及びブロックカウンタ６の出力をビット毎にＸＯＲ（排他的論理和）演算を行うなどしてブロック鍵を作成する。上記の圧縮の手法としては、暗号文中の所定ビット部分を抽出するなどが簡便であるが、どのような手法を用いるかについて特に制限はない。

【００２０】

ブロックカウンタ６は、暗号化部３が１ブロックの平文について暗号化を終了したときに所定値づつカウントアップまたはカウントダウンを行うものである。ブロックカウンタ６の出力ビット長は、例えば鍵長に等しいものとする。

【００２１】

暗号鍵記憶部５は、予め定められた暗号鍵を記憶しておくものである。暗号文出力部８は、暗号化部３により暗号化された暗号文を、例えば相手側へ伝送し、或いは記憶媒体へ記憶する処理部へ送出するものである。暗号文記憶部９は、暗号化された暗号文を例えば全て記憶しているものである。

【００２２】

制御部１は、装置全体の統括制御において、暗号文生成の初期時と再開時に、ブロックカウンタ６の値と前暗号文供給部７へ所定の暗号文のデータを設定し、また、暗号鍵記憶部５へ暗号鍵を記憶する。更に、制御部１は、暗号化部３が１ブロックの平文について暗号化を終了し、次の１ブロックの平文を平文格納部２から全て読み出したときに、更に新たな１ブロックの平文を平文格納部２へ格納する制御を行うものである。

【００２３】

以上の通りに各部より構成される暗号文生成装置は、実際には、パーソナルコンピュータやワークステーションなどのコンピュータにより構成されており、図２に示されるフローチャートに対応する暗号文生成プログラムを上記コンピュータが実行することにより、制御部１、暗号化部３、ブロック鍵作成部４、ブロックカウンタ６、前暗号文供給部７、暗号文出力部８の動作が実現されるので、以下において、図２に示されるフローチャートに基づき動作を説明する。

【００２４】

プログラムがスタートされると、外部からの入力に応じて、初期スタートであるか否かを検出する（Ｓ１）。例えば、再スタートの場合には、再スタートの指示と必要なデータ（カウント値等）が、初期スタートの場合には、スタートの指示のみが入力される。

【００２５】

上記ステップＳ１においてＹＥＳへ分岐すると、ブロックカウンタ６に対して、予めプログラムにセットされているスタート用のカウント値をセットし、前暗号文供給部７に対して、予めプログラムにセットされているスタート用の暗号文データ（任意のデータ）をセットする（Ｓ２：制御ステップ）。

【００２６】

一方、上記ステップＳ１においてＮＯへ分岐すると、ブロックカウンタ６に対して、外部から与えられた再スタート用のカウント値をセットし、前暗号文供給部７に対して、外部から与えられたカウント値に対応する再スタート用の暗号文データ（上記カウント値がブロックカウンタ６にセットされていたときに、前暗号文供給部７にセットされていた暗号文のデータ）を暗号文記憶部９から読み出してセットする（Ｓ３：制御ステップ）。

【００２７】

以上のステップＳ２またはステップＳ３の処理を終えると、予めプログラムにセットされている暗号鍵データを暗号鍵記憶部５へセットする（Ｓ４）。次に、ブロックカウンタ６にセットしたカウント値に応じた１ブロック分の平文データを平文格納部２へ読み出す（Ｓ５）。即ち、初期スタートの場合には、最初の１ブロック分の平文データが平文格納

部２へ格納され、再スタートの場合には、上記カウント値がブロックカウンタ６にセットされていたときに、平文格納部２にセットされていた平文データが平文格納部２へ格納される。

【００２８】

続いて、暗号鍵記憶部５にセットされている暗号鍵データと、ブロックカウンタ６にセットされているカウント値と、前暗号文供給部７にセットされている暗号文データとを用いて前述の通りにしてブロック鍵が作成され（ブロック鍵作成ステップ）、このブロック鍵に基づき平文の暗号化が行われ（暗号化ステップ）、暗号文出力部８としての出力が行われる（Ｓ６）。

【００２９】

次に、ブロックカウンタ６を更新（所定値のカウントアップもしくはカウントダウン）し（Ｓ７：カウントステップ）、前暗号文供給部７にその時点において暗号化された１ブロック分の暗号文をセットする（Ｓ８）。そこで、記憶媒体等に暗号化すべき平文データが残っているかを検出することにより全ての平文についての暗号化済みを確認する（Ｓ９）。

【００３０】

上記のステップＳ９において暗号化されずに残っている平文がある場合には、ステップＳ５へ戻って次の１ブロックの平文に対する暗号化へと進む。このようにして、ステップＳ５からステップＳ９へ進み、このステップＳ９からステップＳ５へ戻るルーチンが繰り返されて、ステップＳ９において全ての平文についての暗号化済みが確認できると、エンドとなる。

【００３１】

このようにして、実施例では、暗号鍵記憶部５にセットされている暗号鍵データと、ブロックカウンタ６にセットされているカウント値と、前暗号文供給部７にセットされている暗号文データとを用いてブロック鍵が作成され、このブロック鍵に基づき平文の暗号化が行われるので、別途に暗号鍵変更用の乱数生成アルゴリズムを用いることなく、ブロック毎に異なる乱数パターンを生成してストリーム暗号化を実行できる。しかも、暗号文記憶部９を有しており、カウント値に基づき再スタートが可能な構成を採用しているので、暗号文出力部８以降の構成（例えば伝送路）などの不具合により再度の暗号化が必要な場合にも迅速に対応することが可能である。

【００３２】

なお、再スタートの指示とカウント値を入力する例を示したが、カウント値に代えて１ブロックの暗号文を入力して再スタートを行わせるように構成しても良い。この場合には、与えられた１ブロックの暗号文が何番目か（カウント値に相当）を暗号文記憶部９に蓄積された暗号文の順から取得する処理が必要となるが、それ以外の構成は上記実施例と同様にして再スタートを行うこともできる。また、暗号文記憶部９には、暗号化した暗号文の全てを記憶する例を示したが、再スタートを保証できる範囲をＮブロック前までとし、Ｎブロック前までに暗号化した暗号文を暗号文記憶部９に記憶するようにしても良い。

【００３３】

次に、上記暗号文生成装置によって暗号化された暗号文を復号化する暗号文復号装置の実施例を説明する。図３に、暗号文復号装置のブロック図を示す。この暗号文復号装置は、装置全体を統括制御する制御部１１を有し、暗号文格納部１２、復号化部１３、ブロック鍵作成部１４、暗号鍵記憶部１５、ブロックカウンタ１６、前暗号文供給部１７、復号文出力部１８、暗号文記憶部１９を備えている。

【００３４】

暗号文格納部１２には、復号化すべき暗号文のデータが制御部１１の制御によって１ブロック毎（例えば、１バイト毎）に格納される。復号化部１３は、ブロック毎の暗号文とブロック鍵作成部１４により作成されたブロック鍵とに基づいて例えばＸＯＲ（排他的論理和）演算により暗号文の復号化を行うものである。

【００３５】

ブロック鍵作成部１４にはブロックカウンタ１６の出力と、前暗号文供給部１７により供給される１ステップ前に復号化に用いた復号化前の暗号文と、暗号鍵記憶部１５から暗号鍵データ（暗号文生成装置の暗号鍵記憶部５に記憶された暗号鍵データと同一の暗号鍵データ）とが与えられる。ここでは、１ステップ前に暗号化した暗号文を与えたが、一般的には所定ステップ前に復号化に用いた復号化前の暗号文を与えることになる。ブロック鍵作成部１４は前暗号文供給部１７により供給される暗号文を鍵長に揃える圧縮を行い、暗号文と暗号鍵及びブロックカウンタ１６の出力をビット毎にＸＯＲ（排他的論理和）演算を行うなどしてブロック鍵を作成する。上記の圧縮の手法としては、暗号文中の所定ビット部分を抽出するなどが簡便であるが、どのような手法を用いるかについて特に制限はない。

【００３６】

ブロックカウンタ１６は、復号化部１３が１ブロックの暗号文について復号化を終了したときに暗号文生成装置のブロックカウンタ１６と同じ所定値づつカウントアップまたはカウントダウンを行うものである。ブロックカウンタ１６の出力ビット長は、例えば鍵長に等しいものとする。

【００３７】

暗号鍵記憶部１５は、予め定められた暗号鍵（暗号文生成装置の暗号鍵記憶部５に記憶された暗号鍵データと同一の暗号鍵データ）を記憶しておくものである。復号文出力部１８は、復号化部１３により復号化された復号文を、例えばコンテンツを再生する端末側へ伝送し、或いは記憶媒体へ記憶する処理部へ送出するものである。暗号文記憶部１９は、復号化に用いた復号化前の暗号文を例えば全て記憶しているものである。

【００３８】

制御部１１は、装置全体の統括制御において、復号文生成の初期時と再開時に、ブロックカウンタ１６の値と前暗号文供給部１７へ所定の暗号文のデータを設定し、また、暗号鍵記憶部１５へ暗号鍵を記憶する。更に、制御部１１は、復号化部１３が１ブロックの暗号文について復号化を終了し、次の１ブロックの暗号文を暗号文格納部１２から全て読み出したときに、暗号文格納部１２の暗号文を前暗号文供給部１７へ送り出すと共に更に新たな１ブロックの暗号文を暗号文格納部１２へ格納する制御を行うものである。

【００３９】

以上の通りに各部より構成される暗号文復号装置は、実際には、パーソナルコンピュータやワークステーションなどのコンピュータにより構成されており、図４に示されるフローチャートに対応する暗号文復号プログラムを上記コンピュータが実行することにより、制御部１１、復号化部１３、ブロック鍵作成部１４、ブロックカウンタ１６、前暗号文供給部１７、復号文出力部１８の動作が実現されるので、以下において、図４に示されるフローチャートに基づき動作を説明する。

【００４０】

プログラムがスタートされると、外部からの入力に応じて、初期スタートであるか否かを検出する（Ｓ１１）。例えば、再スタートの場合には、再スタートの指示と必要なデータ（カウント値等）が、初期スタートの場合には、スタートの指示のみが入力される。

【００４１】

上記ステップＳ１１においてＹＥＳへ分岐すると、ブロックカウンタ１６に対して、予めプログラムにセットされているスタート用のカウント値（暗号生成プログラムのものと同じカウント値）をセットし、前暗号文供給部１７に対して、予めプログラムにセットされているスタート用の暗号文データ（任意のデータ：暗号生成プログラムのものと同じデータ）をセットする（Ｓ１２：制御ステップ）。

【００４２】

一方、上記ステップＳ１１においてＮＯへ分岐すると、ブロックカウンタ１６に対して、外部から与えられた再スタート用のカウント値をセットし、前暗号文供給部１７に対して、外部から与えられたカウント値に対応する再スタート用の暗号文データ（上記カウント値がブロックカウンタ１６にセットされていたときに、前暗号文供給部１７にセットさ

れていた暗号文のデータ）を暗号文記憶部１９から読み出してセットする（Ｓ１３：制御ステップ）。

【００４３】

以上のステップＳ１２またはステップＳ１３の処理を終えると、予めプログラムにセットされている暗号鍵データを暗号鍵記憶部１５へセットする（Ｓ１４）。次に、ブロックカウンタ１６にセットしたカウント値に応じた１ブロック分の暗号文データを暗号文格納部１２へ読み出す（Ｓ１５）。即ち、初期スタートの場合には、最初の１ブロック分の暗号文データが暗号文格納部１２へ格納され、再スタートの場合には、上記カウント値がブロックカウンタ１６にセットされていたときに、暗号文格納部１２にセットされていた暗号文データが暗号文格納部１２へ格納される。

【００４４】

続いて、暗号鍵記憶部１５にセットされている暗号鍵データと、ブロックカウンタ１６にセットされているカウント値と、前暗号文供給部１７にセットされている暗号文データとを用いて前述の通りにしてブロック鍵が作成され（ブロック鍵作成ステップ）、このブロック鍵に基づき暗号文の復号化（暗号化と逆の処理）が行われ（復号化ステップ）、復号文出力部１８としての出力が行われる（Ｓ１６）。

【００４５】

次に、ブロックカウンタ１６を更新（所定値のカウントアップもしくはカウントダウン）し（Ｓ１７：カウントステップ）、前暗号文供給部１７にその時点において復号化した１ブロック分の復号化前の暗号文を暗号文格納部１２から転送してセットする（Ｓ１８）。そこで、記憶媒体等に復号化すべき暗号文データが残っているかを検出することにより全ての暗号文についての復号化済みを確認する（Ｓ１９）。

【００４６】

上記のステップＳ１９において復号化されずに残っている復号文がある場合には、ステップＳ１５へ戻って次の１ブロックの暗号文に対する復号化へと進む。このようにして、ステップＳ１５からステップＳ１９へ進み、このステップＳ１９からステップＳ１５へ戻るルーチンが繰り返されて、ステップＳ１９において全ての暗号文についての復号化済みが確認できると、エンドとなる。

【００４７】

このようにして、実施例では、暗号鍵記憶部１５にセットされている暗号鍵データと、ブロックカウンタ１６にセットされているカウント値と、前暗号文供給部７にセットされている暗号文データとを用いてブロック鍵が作成され、このブロック鍵に基づき暗号文の復号化が行われるので、既に説明した暗号文生成装置または暗号文生成プログラムによって別途に暗号鍵変更用の乱数生成アルゴリズムを用いることなく、ブロック毎に異なる乱数パターンを生成してストリーム暗号化を実行した結果の暗号文について適切に復号化が可能である。しかも、暗号文記憶部１９を有しており、カウント値に基づき再スタートが可能な構成を採用しているので、暗号文生成装置から暗号文が送られてくる経路（例えば伝送路）や当該暗号文復号装置などの不具合により復号化が停止したブロックから再度の復号化が必要な場合にも迅速に対応することが可能である。

【００４８】

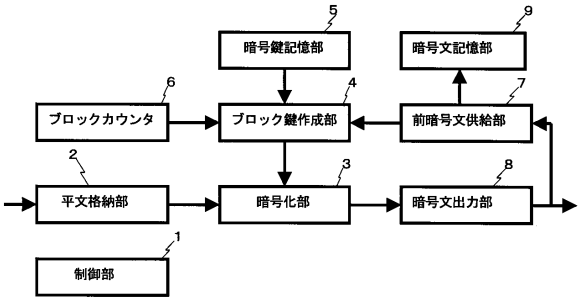
なお、再スタートの指示とカウント値を入力する例を示したが、カウント値に代えて１ブロックの暗号文を入力して再スタートを行わせるように構成しても良い。この場合には、与えられた１ブロックの暗号文が何番目か（カウント値に相当）を暗号文記憶部１９に蓄積された暗号文の順から取得する処理が必要となるが、それ以外の構成は上記実施例と同様にして再スタートを行うこともできる。また、暗号文記憶部１９には、復号化前の暗号文全てを記憶する構成を例示したが、再スタートを保証できる範囲をＮブロック前までとし、Ｎブロック前までに復号化した復号前の暗号文を暗号文記憶部１９に記憶するようにしても良い。

【図面の簡単な説明】

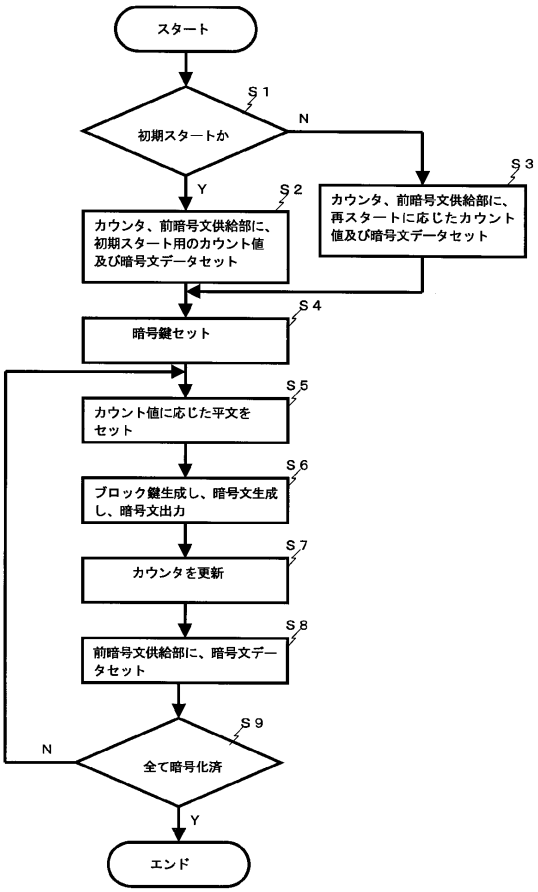
【００４９】

【図１】本発明に係る暗号文生成装置の実施例の構成を示すブロック図。
【図２】本発明に係る暗号文生成装置をコンピュータにより実現する場合の暗号文生成プログラムによる処理を示すフローチャート。
【図３】本発明に係る暗号文復号装置の実施例の構成を示すブロック図。
【図４】本発明に係る暗号文復号装置をコンピュータにより実現する場合の暗号文復号プログラムによる処理を示すフローチャート。
【符号の説明】
【００５０】
１、１１　制御部
２　平文格納部
３　暗号化部
４、１４　ブロック鍵生成部
５、１５　暗号鍵記憶部
６、１６　ブロックカウンタ
７　前暗号文供給部
８　暗号文出力部
９　暗号文記憶部
１２　暗号文格納部
１３　復号化部
１７　前暗号文供給部
１８　復号文出力部
１９　暗号文記憶部

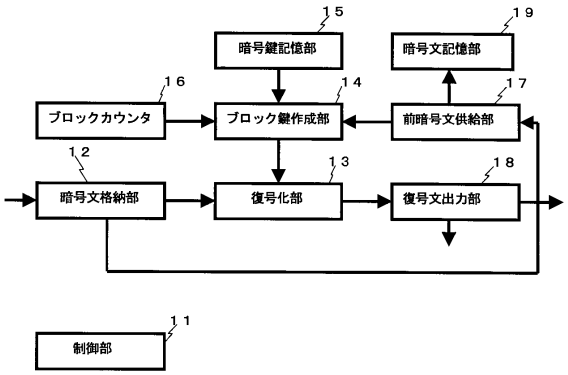
【図１】



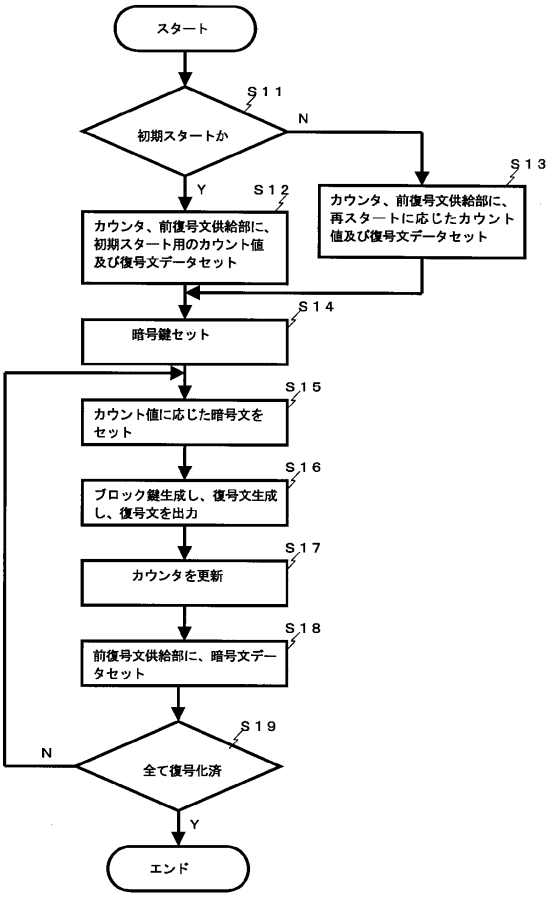
【図２】



【図３】


15
暗号鍵記憶部
19
暗号文記憶部
16
ブロックカウンタ
14
ブロック鍵作成部
17
前暗号文供給部
12
暗号文格納部
13
復号化部
18
復号文出力部
11
制御部

【図４】


スタート
S11
初期スタートか
N
Y
S12
カウンタ、前復号文供給部に、初期スタート用のカウント値及び復号文データセット
S13
カウンタ、前復号文供給部に、再スタートに応じたカウント値及び復号文データセット
S14
暗号鍵セット
S15
カウント値に応じた暗号文をセット
S16
ブロック鍵生成し、復号文生成し、復号文を出力
S17
カウンタを更新
S18
前復号文供給部に、暗号文データセット
S19
全て復号化済
N
Y
エンド

フロントページの続き

審査官　青木　重徳

(56)参考文献　国際公開第０１／０５２４７２（WO，Ａ１）
特開平１０－３１３３０６（ＪＰ，Ａ）
特開平１０－０６６１５７（ＪＰ，Ａ）
特開平０９－２３３０６６（ＪＰ，Ａ）
特開平０５－１６０８６６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／０６