

(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2005-202048

(P2005-202048A)

(43) 公開日 平成17年7月28日(2005.7.28)

(51) Int.Cl.⁷

G09C 1/00
H04K 1/02
H04L 9/16

F I

G09C 1/00 610A
H04K 1/02
H04L 9/00 643

テーマコード (参考)

5J104

審査請求 未請求 請求項の数 24 O L (全 34 頁)

(21) 出願番号 特願2004-6920 (P2004-6920)
(22) 出願日 平成16年1月14日 (2004.1.14)

(71) 出願人 000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(74) 代理人 100064746
弁理士 深見 久郎
(74) 代理人 100085132
弁理士 森田 俊雄
(74) 代理人 100083703
弁理士 仲村 義平
(74) 代理人 100096781
弁理士 堀井 豊
(74) 代理人 100098316
弁理士 野田 久登
(74) 代理人 100109162
弁理士 酒井 将行

最終頁に続く

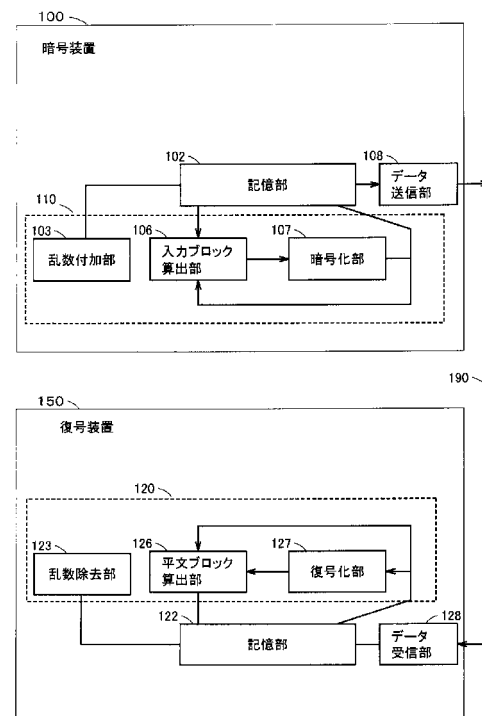
(54) 【発明の名称】 暗号通信システム、そのシステムに使用される暗号装置および復号装置、暗号化方法および復号化方法、暗号化プログラムおよび復号化プログラム、ならびに記録媒体

(57) 【要約】

【課題】 暗号通信するデータに付加するデータ数の増加を抑制する。

【解決手段】 暗号通信システムは、暗号装置100と、通信回線190に接続された復号装置150とを含む。暗号装置100は、データを記憶する記憶部102と、所定のデータに乱数を付加する乱数付加部103と、入力ブロックを算出する入力ブロック算出部106と、データを暗号化する暗号化部107と、データを送信するデータ送信部108とを含む。復号装置150は、データを記憶する記憶部122と、所定のデータから乱数を除去する乱数除去部123と、平文ブロックを算出する平文ブロック算出部126と、暗号化されたデータを復号化する復号化部127と、データを受信するデータ受信部128とを含む。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

暗号通信システムであって、

前記暗号通信システムは、複数のブロックに分割された暗号化データを生成して送信する暗号装置を備え、

前記暗号装置は、

平文データに対応する第 1 のデータの先頭から予め定められた範囲内に、前記第 1 のデータの暗号通信のための第 2 のデータを追加するための追加手段と、

前記第 1 のデータの先頭から前記第 2 のデータの先頭までのデータのサイズを少なくとも上回るデータサイズによって、前記第 2 のデータの追加によって生成される通信データを分割して、暗号化処理が行なわれる前のデータである複数の平文ブロックを生成するための通信データ分割手段と、

前記第 1 のデータの先頭が含まれる平文ブロックから、入力ブロックを生成するための第 1 の入力ブロック生成手段と、

前記第 1 のデータの先頭が含まれる平文ブロックの後に生成される少なくとも 1 つ以上の後続の平文ブロックの各々に対して、前記後続の平文ブロックを、前記後続の平文ブロックの直前の平文ブロックに対応する前記暗号化データに基づいて変換し、前記後続の平文ブロックに対応する入力ブロックを生成するための第 2 の入力ブロック生成手段と、

生成された複数の前記入力ブロックの各々に対して暗号化処理を実行して、複数の前記入力ブロックの各々に対応する前記暗号化データを生成するための暗号化手段と、

生成された複数の前記暗号化データを送信するための送信手段とを含み、

前記暗号通信システムは、複数のブロックに分割された暗号化データを受信して復号する復号装置をさらに備え、

前記復号装置は、

複数の前記暗号化データを受信するための受信手段と、

複数の前記暗号化データの各々に対して復号化処理を実行して、出力ブロックを生成するための出力ブロック生成手段と、

最初に生成される出力ブロックから、第 1 の平文ブロックを生成するための第 1 の平文ブロック生成手段と、

前記最初に生成される出力ブロックの後に生成される少なくとも 1 つ以上の後続の出力ブロックの各々に対して、前記後続の出力ブロックを、前記後続の出力ブロックの直前の出力ブロックに対応する前記暗号化データに基づいて変換し、前記後続の出力ブロックに対応する平文ブロックを生成するための第 2 の平文ブロック生成手段と、

生成された複数の前記平文ブロックを結合することにより、平文データに対応する第 1 のデータと、前記第 1 のデータの先頭から予め定められた範囲内に追加された第 2 のデータとを有する通信データを復元するための通信データ復元手段と、

前記通信データから前記第 2 のデータを除去するための除去手段とを含む、暗号通信システム。

【請求項 2】

複数のブロックに分割された暗号化データを生成して送信する暗号装置であって、

平文データに対応する第 1 のデータの先頭から予め定められた範囲内に、前記第 1 のデータの暗号通信のための第 2 のデータを追加するための追加手段と、

前記第 1 のデータの先頭から前記第 2 のデータの先頭までのデータのサイズを少なくとも上回るデータサイズによって、前記第 2 のデータの追加によって生成される通信データを分割して、暗号化処理が行なわれる前のデータである複数の平文ブロックを生成するための通信データ分割手段と、

前記第 1 のデータの先頭が含まれる平文ブロックから、入力ブロックを生成するための第 1 の入力ブロック生成手段と、

前記第 1 のデータの先頭が含まれる平文ブロックの後に生成される少なくとも 1 つ以上の後続の平文ブロックの各々に対して、前記後続の平文ブロックを、前記後続の平文ブ

10

20

30

40

50

ックの直前の平文ブロックに対応する前記暗号化データに基づいて変換し、前記後続の平文ブロックに対応する入力ブロックを生成するための第2の入力ブロック生成手段と、

生成された複数の前記入力ブロックの各々に対して暗号化処理を実行して、複数の前記入力ブロックの各々に対応する前記暗号化データを生成するための暗号化手段と、

生成された複数の前記暗号化データを送信するための送信手段とを含む、暗号装置。

【請求項3】

前記第2の入力ブロック生成手段は、

前記後続の平文ブロックと、前記直前の平文ブロックに対応する暗号化データとを記憶するための記憶手段と、

前記後続の平文ブロックと、前記直前の平文ブロックに対応する暗号化データとを予め定められた規則に基づいて演算することにより、前記後続の平文ブロックに対応する入力ブロックを生成するための入力ブロック演算手段とを含む、請求項2に記載の暗号装置。 10

【請求項4】

前記入力ブロック演算手段は、予め定められた、逆関数を有する関数を用いて演算することにより、前記後続の平文ブロックと前記直前の平文ブロックに対応する暗号化データから、前記後続の平文ブロックに対応する入力ブロックを生成する、請求項3に記載の暗号装置。

【請求項5】

前記第2の入力ブロック生成手段は、予め定められた演算処理を実行することにより、前記平文ブロックのサイズと同じサイズを有する前記入力ブロックを生成する、請求項2に記載の暗号装置。 20

【請求項6】

前記追加手段は、前記予め定められた範囲内に前記第2のデータを挿入する、請求項2に記載の暗号装置。

【請求項7】

前記暗号装置はさらに、前記暗号化処理に使用する鍵を更新するための更新手段を含む、請求項2～6のいずれかに記載の暗号装置。

【請求項8】

前記更新手段は、

前記暗号化処理の対象となる平文ブロックの前の平文ブロックから生成された前記暗号化データと、前記前の平文ブロックの入力ブロックと、前記平文ブロックと、前記前の平文ブロックの暗号化処理に使用された鍵との少なくとも1つのデータを記憶するための記憶手段と、 30

前記少なくとも1つのデータに基づいて、新たな鍵を生成するための鍵生成手段と、

前記新たな鍵を前記暗号化処理に使用する鍵として設定するための設定手段とを含む、請求項7に記載の暗号装置。

【請求項9】

前記暗号装置はさらに、乱数を有するデータを前記第2のデータとして生成するための付加データ生成手段を含む、請求項2～8のいずれかに記載の暗号装置。

【請求項10】 40

前記付加データ生成手段は、

乱数を生成するための乱数生成手段と、

生成された前記乱数を記憶するための乱数記憶手段と、

前記第2のデータのサイズと前記乱数のサイズとの差を有するデータを、前記乱数に追加することにより、前記第2のデータを生成するための手段を含む、請求項9に記載の暗号装置。

【請求項11】

前記暗号装置はさらに、

前記第1のデータの送信先を識別する識別データを生成するための識別データ生成手段と、

前記識別データを有するデータを前記第 2 のデータとして生成するための手段とを含む、請求項 2 ～ 10 のいずれかに記載の暗号装置。

【請求項 12】

前記暗号装置はさらに、

予め定められた処理に基づいて、前記第 1 のデータと前記第 2 のデータとを有する通信データを圧縮することにより、前記通信データに復元不可能なハッシュ値を生成するためのハッシュ値生成手段と、

前記ハッシュ値を有する第 2 のデータを生成するための手段とを含む、請求項 2 ～ 10 のいずれかに記載の暗号装置。

【請求項 13】

複数のブロックに分割された暗号化データを受信して復号する復号装置であって、

複数の前記暗号化データを受信するための受信手段と、

複数の前記暗号化データの各々に対して復号化処理を実行して、出力ブロックを生成するための出力ブロック生成手段と、

最初に生成される出力ブロックから、第 1 の平文ブロックを生成するための第 1 の平文ブロック生成手段と、

前記最初に生成される出力ブロックの後に生成される少なくとも 1 つ以上の後続の出力ブロックの各々に対して、前記後続の出力ブロックを、前記後続の出力ブロックの直前の出力ブロックに対応する前記暗号化データに基づいて変換し、前記後続の出力ブロックに対応する平文ブロックを生成するための第 2 の平文ブロック生成手段と、

生成された複数の前記平文ブロックを結合することにより、平文データに対応する第 1 のデータと、前記第 1 のデータの先頭から予め定められた範囲内に追加された第 2 のデータとを有する通信データを復元するための通信データ復元手段と、

前記通信データから前記第 2 のデータを除去するための除去手段とを含む、復号装置。

【請求項 14】

前記第 2 の平文ブロック生成手段は、

前記先頭の出力ブロックの後に生成される前記後続の出力ブロックと、前記直前の出力ブロックに対応する暗号化データとを記憶するための記憶手段と、

前記後続の出力ブロックと、前記直前の出力ブロックに対応する暗号化データとを予め定められた規則に基づいて演算することにより、前記後続の出力ブロックに対応する平文ブロックを生成するための平文ブロック演算手段とを含む、請求項 13 に記載の復号装置。

【請求項 15】

前記平文ブロック演算手段は、予め定められた、逆関数を有する関数を用いて、前記後続の出力ブロックと、前記直前の出力ブロックに対応する暗号化データとから、前記後続の出力ブロックに対応する平文ブロックを生成する、請求項 14 に記載の復号装置。

【請求項 16】

前記復号装置はさらに、前記復号化処理に使用する鍵を更新するための更新手段を含む、請求項 13 ～ 15 のいずれかに記載の復号装置。

【請求項 17】

前記更新手段は、

前記復号化処理の対象となる暗号化データの直前の暗号化データと、前記直前の暗号化データから生成された出力ブロックと、前記出力ブロックから生成された平文ブロックと、前記直前の暗号化データの復号化処理に使用された鍵との少なくとも 1 つのデータを記憶するための記憶手段と、

前記少なくとも 1 つのデータに基づいて、新たな鍵を生成するための鍵生成手段と、

前記新たな鍵を前記復号化処理に使用する鍵として設定するための手段とを含む、請求項 16 に記載の復号装置。

【請求項 18】

前記第 2 のデータは、前記暗号化データの送信元を識別するための識別データを含み、

10

20

30

40

50

前記復号装置はさらに、
予め定められたデータを記憶するための記憶手段と、
前記第2のデータから、前記識別データを取得するための識別データ取得手段と、
前記識別データと、前記予め定められたデータとが一致するか否かを確認するための識別データ確認手段とを含む、請求項13～15のいずれかに記載の復号装置。

【請求項19】

前記第2のデータは、予め定められた規則により算出されたハッシュ値を含み、
前記復号装置はさらに、
前記第2のデータから前記ハッシュ値を取得するための取得手段と、
復号化された第1のデータにハッシュ演算を実行することにより、ハッシュ値を算出するためのハッシュ値算出手段と、
前記取得手段により取得されたハッシュ値と、前記ハッシュ値算出手段により算出されたハッシュ値とが一致するか否かを確認するためのハッシュ値確認手段とを含む、請求項13～15のいずれかに記載の復号装置。 10

【請求項20】

複数のブロックに分割された暗号化データを生成して送信する暗号化方法であって、
データが格納された記憶手段から、平文データに対応する第1のデータと、前記第1のデータの暗号通信のための第2のデータとを読み出すステップと、
前記第1のデータの先頭から予め定められた範囲内に、前記第2のデータを追加する追加ステップと、
前記第1のデータの先頭から前記第2のデータの先頭までのデータのサイズを少なくとも上回るデータサイズによって、前記第2のデータの追加によって生成される通信データを分割して、暗号化処理が行なわれる前のデータである複数の平文ブロックを生成する通信データ分割ステップと、
前記第1のデータの先頭が含まれる平文ブロックから、入力ブロックを生成する第1の平文ブロック生成ステップと、
前記第1のデータの先頭が含まれる平文ブロックの後に生成される少なくとも1つ以上の後続の平文ブロックの各々に対して、前記後続の平文ブロックを、前記後続の平文ブロックの直前の平文ブロックに対応する前記暗号化データに基づいて変換し、前記後続の平文ブロックに対応する入力ブロックを生成する第2の平文ブロック生成ステップと、
生成された複数の前記入力ブロックの各々に対して暗号化処理を実行して、複数の前記入力ブロックの各々に対応する前記暗号化データを生成する暗号化ステップと、
生成された複数の前記暗号化データを送信する送信ステップとを含む、暗号化方法。 20

【請求項21】

複数のブロックに分割された暗号化データを受信して復号する復号化方法であって、
複数の前記暗号化データを受信するステップと、
受信した複数の前記暗号化データを電子データとして記憶手段に格納するステップと、
前記記憶手段から、複数の前記暗号化データを読み出すステップと、
複数の前記暗号化データの各々に対して復号化処理を実行して、出力ブロックを生成する出力ブロック生成ステップと、
最初に生成される出力ブロックから、平文ブロックを生成する第1の平文ブロック生成ステップと、
前記最初に生成される出力ブロックの後に生成される少なくとも1つ以上の後続の出力ブロックに対して、前記後続の出力ブロックを、前記後続の出力ブロックの直前の出力ブロックに対応する前記暗号化データに基づいて変換し、前記後続の出力ブロックに対応する平文ブロックを生成する第2の平文ブロック生成ステップと、
生成された複数の前記平文ブロックを結合することにより、平文データに対応する第1のデータと、前記第1のデータの先頭から予め定められた範囲内に追加された第2のデータとを有する通信データを復元する通信データ復元ステップと、
前記通信データから前記第2のデータを除去する除去ステップとを含む、復号化方法。 30 40 50

【請求項 2 2】

複数のブロックに分割された暗号化データを生成して送信する暗号装置として、コンピュータを機能させるための暗号化プログラムであって、前記暗号化プログラムは前記コンピュータに、

データが格納された記憶手段から、平文データに対応する第 1 のデータと、前記第 1 のデータの暗号通信のための第 2 のデータとを読み出す準備ステップと、

前記第 1 のデータの先頭から予め定められた範囲内に、前記第 2 のデータを追加する追加ステップと、

前記第 1 のデータの先頭から前記第 2 のデータの先頭までのデータのサイズを少なくとも上回るデータサイズによって、前記第 2 のデータの追加によって生成される通信データを分割して、暗号化処理が行なわれる前のデータである複数の平文ブロックを生成する通信データ分割ステップと、

前記第 1 のデータの先頭が含まれる平文ブロックから、入力ブロックを生成する第 1 の入力ブロック生成ステップと、

前記第 1 のデータの先頭が含まれる平文ブロックの後に生成される少なくとも 1 つ以上の後続の平文ブロックの各々に対して、前記後続の平文ブロックを、前記後続の平文ブロックの直前の平文ブロックに対応する前記暗号化データに基づいて、前記後続の平文ブロックに対応する入力ブロックを生成する第 2 の入力ブロック生成ステップと、

生成された複数の前記入力ブロックの各々に対して暗号化処理を実行して、複数の前記入力ブロックの各々に対応する前記暗号化データを生成する暗号化ステップと、

生成された複数の前記暗号化データを送信する送信ステップとを実行させる、暗号化プログラム。

【請求項 2 3】

複数のブロックに分割された暗号化データを受信して復号する復号装置としてコンピュータを機能させるための復号化プログラムであって、前記復号化プログラムは前記コンピュータに、

複数の前記暗号化データを受信するステップと、

受信した複数の前記暗号化データを電子データとして記憶手段に格納するステップと、

前記記憶手段から、複数の前記暗号化データを読み出すステップと、

複数の前記暗号化データの各々に対して復号化処理を実行して、出力ブロックを生成する出力ブロック生成ステップと、

最初に生成される出力ブロックから、平文ブロックを生成する第 1 の平文ブロック生成ステップと、

前記最初に生成される出力ブロックの後に生成される少なくとも 1 つ以上の後続の出力ブロックの各々に対して、前記後続の出力ブロックを、前記後続の出力ブロックの直前の出力ブロックに対応する前記暗号化データに基づいて変換し、前記後続の出力ブロックに対応する平文ブロックを生成する第 2 の平文ブロック生成ステップと、

生成された複数の前記平文ブロックを結合することにより、平文データに対応する第 1 のデータと、前記第 1 のデータの先頭から予め定められた範囲内に追加された第 2 のデータとを有する通信データを復元する通信データ復元ステップと、

前記通信データから前記第 2 のデータを除去する除去ステップとを実行させる、復号化プログラム。

【請求項 2 4】

請求項 2 2 に記載の暗号化プログラムまたは請求項 2 3 に記載の復号化プログラムを記録した、記録媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は暗号化したデータを通信する技術に関し、特に、ダミーデータが付加された平文データを暗号化し、暗号化されたデータを復号化する技術に関する。

10

20

30

40

50

【背景技術】

【0002】

一般に、ソフトウェア、音楽データその他のデジタルデータとして配信可能なデジタルコンテンツは、特別の処理が施されていない限り、そのコンテンツのデータをコピーすることにより、コンテンツの正規の購入者以外の者が、そのコンテンツを使用（たとえば、表示、再生等）することができるという問題がある。そのような問題の発生を防ぐための方法として、デジタルコンテンツを予め暗号化しておき、正規の購入者のみが暗号化されたデジタルコンテンツを表示あるいは再生することができるようにする方法がある。

【0003】

そのデジタルコンテンツの暗号化において、データサイズが大きいデジタルコンテンツを暗号化する場合には、処理時間が短い共通鍵暗号方式が用いられることが多い。この共通鍵暗号方式では、データを暗号化する時と暗号化されたデータを復号化する時に、同じ鍵が用いられる。この共通鍵暗号方式の一般的なものとして、たとえば、DES（Data Encryption Standard）などのブロック暗号がある。ブロック暗号は、暗号化するデータを64ビットなど一定の長さのブロックに区切り、ブロック単位で暗号化あるいは復号を行なうというものである。 10

【0004】

このような共通鍵暗号方式では、暗号化処理を行なう際に用いる鍵と、復号化処理を行なう際に用いる鍵とが同一であるので、データの配信側と受信側とは、同じ鍵を共有しなければならない。そのため、たとえば、デジタルコンテンツを暗号化する度に鍵を変更した場合には、配信側から受信側に正しい鍵を配送しなければならないため、どのようにしてその鍵を安全に配送するかが問題となる。その一方、鍵を変更することなく、暗号化の処理ごとに同じ鍵を用いた場合には、同一のデジタルコンテンツからは、同一の暗号データが作成されることになるため、暗号通信の強度面における信頼性が低くなるという問題もある。 20

【0005】

そこで、このような問題を解決するために、たとえば特開平10-161535号公報（特許文献1）は、通信データに対して解読されにくい暗号化処理を実行する暗号通信装置を開示する。この暗号通信装置は、入力データ列に乱数データを挿入する挿入部と、挿入部から出力されるデータ列を所定のデータサイズごとにパケット化し、各パケットごとに暗号化する暗号化部と、暗号化したパケットを送信する送信部と、暗号化されたパケットを受信する受信部と、受信したパケットを復号化する復号化部と、復号化したパケットのデータから乱数データを除去する除去部とを含む。 30

【0006】

特許文献1に開示された暗号通信装置によると、データ通信時において、パケットを暗号化する際、乱数がデータの特定の場所に予め埋め込まれて、暗号化される。これにより、暗号通信装置は、暗号化処理のために同じ鍵を使用しても、異なる暗号化データを出力することができる。

【特許文献1】特開平10-161535号公報

【発明の開示】

【発明が解決しようとする課題】

【0007】

しかしながら、特許文献1に開示された暗号通信装置によると、パケットごとに乱数データが必要なデータに付加されるため、送信データのサイズが大きくなるという問題があった。

【0008】

本発明は、上述の問題点を解決するためになされたものであって、その目的は、送信データのサイズの増加を抑制しつつ、同一の平文データを、複数の異なるデータに暗号化することにより、データ通信を行なうことができる暗号通信システムを提供することである。

【0009】

本発明の他の目的は、送信データのサイズの増加を抑制しつつ、同一の平文データを複数の異なるデータに暗号化することができる暗号装置を提供することである。

【0010】

本発明の他の目的は、送信データのサイズの増加を抑制しつつ、同一の平文データを複数の異なるデータに暗号化されたデータを復号化することができる復号装置を提供することである。

【0011】

本発明の他の目的は、送信データのサイズの増加を抑制しつつ、同一の平文データを複数の異なるデータに暗号化することができる暗号化方法を提供することである。

10

【0012】

本発明の他の目的は、送信データのサイズの増加を抑制しつつ、同一の平文データを複数の異なるデータに暗号化されたデータを復号化することができる復号化方法を提供することである。

【0013】

本発明の他の目的は、送信データのサイズの増加を抑制しつつ、同一の平文データを複数の異なるデータに暗号化することができる暗号化方法をコンピュータに実現させることができるプログラムを提供することである。

【0014】

本発明の他の目的は、送信データのサイズの増加を抑制しつつ、同一の平文データを複数の異なるデータに暗号化されたデータを復号化することができる復号化方法をコンピュータに実現させることができるプログラムを提供することである。

20

【0015】

本発明の他の目的は、送信データのサイズの増加を抑制しつつ、同一の平文データを複数の異なるデータに暗号化することができる暗号化方法をコンピュータに実現させることができるプログラムを記録した記録媒体を提供することである。

【0016】

本発明のさらに他の目的は、送信データのサイズの増加を抑制しつつ、同一の平文データを複数の異なるデータに暗号化されたデータを復号化することができる復号化方法をコンピュータに実現させることができるプログラムを記録した記録媒体を提供することである。

30

【課題を解決するための手段】

【0017】

上記の課題を解決するために、この発明のある局面に従うと、暗号通信システムは、複数のブロックに分割された暗号化データを生成して送信する暗号装置を備える。暗号装置は、平文データに対応する第1のデータの先頭から予め定められた範囲内に、第1のデータの暗号通信のための第2のデータを追加するための追加手段と、第1のデータの先頭から第2のデータの先頭までのデータのサイズを少なくとも上回るデータサイズによって、第2のデータの追加によって生成される通信データを分割して、暗号化処理が行なわれる前のデータである複数の平文ブロックを生成するための通信データ分割手段と、第1のデータの先頭が含まれる平文ブロックから、入力ブロックを生成するための第1の入力ブロック生成手段と、第1のデータの先頭が含まれる平文ブロックの後に生成される少なくとも1つ以上の後続の平文ブロックの各々に対して、後続の平文ブロックを、後続の平文ブロックの直前の平文ブロックに対応する暗号化データに基づいて変換し、後続の平文ブロックに対応する入力ブロックを生成するための第2の入力ブロック生成手段と、生成された複数の入力ブロックの各々に対して暗号化処理を実行して、複数の入力ブロックの各々に対応する暗号化データを生成するための暗号化手段と、生成された複数の暗号化データを送信するための送信手段とを含む。暗号通信システムは、複数のブロックに分割された暗号化データを受信して復号する復号装置をさらに備える。復号装置は、複数の暗号化データを受信するための受信手段と、複数の暗号化データの各々に対して復号化処理を実行

40

50

して、出力ブロックを生成するための出力ブロック生成手段と、最初に生成される出力ブロックから、第1の平文ブロックを生成するための第1の平文ブロック生成手段と、最初に生成される出力ブロックの後に生成される少なくとも1つ以上の後続の出力ブロックの各々に対して、後続の出力ブロックを、後続の出力ブロックの直前の出力ブロックに対応する暗号化データに基づいて変換し、後続の出力ブロックに対応する平文ブロックを生成するための第2の平文ブロック生成手段と、生成された複数の平文ブロックを結合することにより、平文データに対応する第1のデータと、第1のデータの先頭から予め定められた範囲内に追加された第2のデータとを有する通信データを復元するための通信データ復元手段と、通信データから第2のデータを除去するための除去手段とを含む。

【0018】

上記の暗号通信システムによると、暗号装置において、追加手段は、第1のデータ（たとえば、送信しようとする通信データ、特に暗号化される前の平文データ）の先頭から予め定められた範囲内に、第2のデータ（たとえば、乱数データ、通信装置を識別するデータ、データ処理日時等）を追加する。この追加には、第1のデータの先頭などに第2のデータを追加する場合、あるいは、第1のデータの途中に第2のデータを挿入する場合が含まれる。通信データ分割手段は、その第2のデータが追加された第1のデータを分割することにより、暗号化処理の対象となるブロックデータ（平文ブロック）を生成する。第1の入力ブロック生成手段および第2の入力ブロック生成手段が、各平文ブロックから入力ブロックを生成すると、暗号化手段は、暗号化処理（たとえば共通鍵暗号方式）により、その入力ブロックを暗号化する。このとき、入力ブロックの先頭には、第2のデータが少なくとも含まれているため、生成される暗号化データにも、その第2のデータに対応する暗号化データが含まれる。その後の入力ブロックの生成には、各平文ブロックと、既に生成された暗号化データとが使用されるため、先頭の平文ブロックに含まれる第2のデータは、その後の平文ブロックの各暗号化処理において、逐次反映される。このようにして生成された暗号化データは、暗号装置から復号装置に送信される。この送信は、たとえば、通信回線を介した送信、暗号化データをCD-ROM（Compact Disc - Read Only Memory）その他の情報記録媒体に格納して、相手先に配布すること等を含む。復号装置において、受信手段が暗号化データを受信すると、各暗号化データの受信順に、出力ブロックが生成される。この受信手段は、たとえば通信回線に接続されたデータ受信IF（Interface）、情報記録媒体からデータを読み出すための駆動装置等を含む。平文ブロックがその出力ブロックから生成されると、生成された各平文ブロックは結合されて、第1のデータと第2のデータとを有する通信データが復元される。除去手段が通信データから第2のデータを除去すると、第1のデータが抽出される。このように、暗号通信に使用する第2のデータを少なくとも最初のブロックに含まれるように埋め込み、そのブロックから暗号化データが生成された後、その他のブロックの暗号化処理は、この暗号化データを使用する。このようにすると、第2のデータを最初のブロックに挿入することにより、その他のブロックに挿入するためのデータが不要となる。したがって、データ量の増加を抑制しつつ、データ通信を行なうことができる暗号通信システムを提供することができる。

【0019】

この発明の他の局面に従うと、暗号装置は、複数のブロックに分割された暗号化データを生成して送信する。この暗号装置は、平文データに対応する第1のデータの先頭から予め定められた範囲内に、第1のデータの暗号通信のための第2のデータを追加するための追加手段と、第1のデータの先頭から第2のデータの先頭までのデータのサイズを少なくとも上回るデータサイズによって、第2のデータの追加によって生成される通信データを分割して、暗号化処理が行なわれる前のデータである複数の平文ブロックを生成するための通信データ分割手段と、第1のデータの先頭が含まれる平文ブロックから、入力ブロックを生成するための第1の入力ブロック生成手段と、第1のデータの先頭が含まれる平文ブロックの後に生成される少なくとも1つ以上の後続の平文ブロックの各々に対して、後続の平文ブロックを、後続の平文ブロックの直前の平文ブロックに対応する暗号化データに基づいて変換し、後続の平文ブロックに対応する入力ブロックを生成するための第2の

10

20

30

40

50

入力ブロック生成手段と、生成された複数の入力ブロックの各々に対して暗号化処理を実行して、複数の入力ブロックの各々に対応する暗号化データを生成するための暗号化手段と、生成された複数の暗号化データを送信するための送信手段とを含む。

【0020】

上記の暗号装置によると、追加手段は、第1のデータの先頭から予め定められた範囲内に、第2のデータを追加する。通信データ分割手段は、その第2のデータが追加された第1のデータを分割することにより、暗号化処理の対象となるブロックデータ（平文ブロック）を生成する。入力ブロック生成手段が、各平文ブロックから入力ブロックを生成すると、暗号化手段は、その入力ブロックを暗号化する。このとき、ブロックの先頭には、第2のデータが少なくとも含まれるため、暗号化データは、その第2のデータに応じて生成される。その後の入力ブロックの生成には、各平文ブロックと、既に生成された暗号化データとが使用されるため、先頭の平文ブロックに含まれる第2のデータは、その後の平文ブロックの各暗号化処理において、逐次反映される。このようにすると、1つの第2のデータを追加することにより複数の暗号化データを生成することができる。また、その第2のデータを変更することにより、同一の第1のデータと同一の鍵とから、異なる暗号データを生成することができる。これにより、第1のデータに追加するデータ量を増加させることなく、暗号化データを生成することができる暗号装置を提供することができる。

10

【0021】

好ましくは、第2の入力ブロック生成手段は、後続の平文ブロックと、直前の平文ブロックに対応する暗号化データとを記憶するための記憶手段と、後続の平文ブロックと、直前の平文ブロックに対応する暗号化データとを予め定められた規則に基づいて演算することにより、後続の平文ブロックに対応する入力ブロックを生成するための入力ブロック演算手段とを含む。

20

【0022】

上記の暗号装置によると、先頭の平文ブロックに続く平文ブロックに対応する入力ブロックは、平文ブロックと、直前の平文ブロックに対応する暗号化データとを予め定められた規則（たとえば、所定の関数、特に逆関数を有する関数）から生成される。このようにすると、先頭の平文ブロックに第2のデータを埋め込むことにより、すべての入力ブロックについて、第2のデータが反映された暗号化データが出力される。したがって、入力ブロックごとに第2のデータを追加する必要がないため、第1のデータの暗号化に不要なデータの増加を抑制することができる。

30

【0023】

好ましくは、入力ブロック演算手段は、予め定められた、逆関数を有する関数を用いて演算することにより、後続の平文ブロックと直前の平文ブロックに対応する暗号化データから、後続の平文ブロックに対応する入力ブロックを生成する。

【0024】

上記の暗号装置によると、逆関数を有する関数を予め設定しておくことにより、平文ブロックに対応する入力ブロックが生成される。その逆関数を有する復号装置に、暗号化データを送信した場合には、その復号装置における復号化処理が可能になる。

【0025】

好ましくは、第2の入力ブロック生成手段は、予め定められた演算処理を実行することにより、平文ブロックのサイズと同じサイズを有する入力ブロックを生成する。

40

【0026】

上記の暗号装置によると、第2のデータを追加して生成された入力ブロックのサイズは、平文ブロックのサイズと同じであるため、送信対象となるデータのサイズの増加を抑制することができる。したがって、暗号化データの送信速度の遅延を防止することができる。

【0027】

好ましくは、追加手段は、予め定められた範囲内に第2のデータを挿入する。

【0028】

50

上記の暗号装置によると、第2のデータを第1のデータの先頭のブロックの所定の位置に挿入することにより、その第2のデータに応じた暗号化データを生成することができる。

【0029】

好ましくは、暗号装置はさらに、暗号化処理に使用する鍵を更新するための更新手段を含む。

【0030】

上記の暗号装置によると、暗号化処理に使用する鍵を適宜変更することができるため、暗号通信のセキュリティを向上させることができる。

【0031】

好ましくは、更新手段は、暗号化処理の対象となる平文ブロックの前の平文ブロックから生成された暗号化データと、前の平文ブロックの入力ブロックと、平文ブロックと、前の平文ブロックの暗号化処理に使用された鍵との少なくとも1つのデータを記憶するための記憶手段と、少なくとも1つのデータに基づいて、新たな鍵を生成するための鍵生成手段と、新たな鍵を暗号化処理に使用する鍵として設定するための設定手段とを含む。

【0032】

上記の暗号装置によると、同一の第1のデータから生成される各暗号化データは、異なる鍵によって暗号化処理されたものになるため、通信される暗号化データごとのセキュリティを向上させることができる。

【0033】

好ましくは、暗号装置はさらに、乱数を有するデータを第2のデータとして生成するための付加データ生成手段を含む。

【0034】

上記の暗号装置によると、その乱数が暗号化データに反映されるため、暗号化データの通信時における不正（漏洩、改ざん等）を検出し易くすることができる。

【0035】

好ましくは、付加データ生成手段は、乱数を生成するための乱数生成手段と、生成された乱数を記憶するための乱数記憶手段と、第2のデータのサイズと乱数のサイズとの差を有するデータを、乱数に追加することにより、第2のデータを生成するための手段を含む。

【0036】

上記の暗号装置によると、乱数生成手段が乱数を生成すると、その乱数を含む第2のデータが生成される。これにより、乱数を含む暗号化データを生成することができるため、暗号化データの通信時における不正（漏洩、改ざん等）を検出し易くすることができる。

【0037】

好ましくは、暗号装置はさらに、第1のデータの送信先を識別する識別データを生成するための識別データ生成手段と、識別データを有するデータを第2のデータとして生成するための手段とを含む。

【0038】

上記の暗号装置によると、識別データが暗号化データに反映されるため、暗号化データの通信時における不正（漏洩、改ざん等）を検出し易くすることができる。

【0039】

好ましくは、暗号装置はさらに、予め定められた処理に基づいて、第1のデータと第2のデータとを有する通信データを圧縮することにより、通信データに復元不可能なハッシュ値を生成するためのハッシュ値生成手段と、ハッシュ値を有する第2のデータを生成するための手段とを含む。

【0040】

上記の暗号装置によると、第1のデータと第2のデータから生成されるハッシュ値が、暗号化データに反映されるため、暗号化データの通信時における不正（漏洩、改ざん等）を検出し易くすることができる。

10

20

30

40

50

【0041】

この発明の他の局面に従うと、復号装置は、複数のブロックに分割された暗号化データを受信して復号する。この復号装置は、複数の暗号化データを受信するための受信手段と、複数の暗号化データの各々に対して復号化処理を実行して、出力ブロックを生成するための出力ブロック生成手段と、最初に生成される出力ブロックから、第1の平文ブロックを生成するための第1の平文ブロック生成手段と、最初に生成される出力ブロックの後に生成される少なくとも1つ以上の後続の出力ブロックの各々に対して、後続の出力ブロックを、後続の出力ブロックの直前の出力ブロックに対応する暗号化データに基づいて変換し、後続の出力ブロックに対応する平文ブロックを生成するための第2の平文ブロック生成手段と、生成された複数の平文ブロックを結合することにより、平文データに対応する第1のデータと、第1のデータの先頭から予め定められた範囲内に追加された第2のデータとを有する通信データを復元するための通信データ復元手段と、通信データから第2のデータを除去するための除去手段とを含む。

10

【0042】

上記の復号装置によると、暗号化データが受信されると、第1の出力ブロック生成手段および第2の出力ブロック生成手段は、復号化処理を実行して、それぞれ出力ブロックを生成する。平文ブロックがその出力ブロックから生成されると、生成された各平文ブロックは結合されて、第1のデータと第2のデータとを有する通信データが復元される。除去手段が通信データから第2のデータを除去すると、第1のデータが抽出される。これにより、暗号通信に使用する第2のデータが最初のブロックに含まれている場合には、復号装置は、最初のブロックから復号化することにより、第1のデータを再現することができる。その結果、データ量の増加を抑制しつつ、データ通信を行なうことができる復号装置を提供することができる。

20

【0043】

好ましくは、第2の平文ブロック生成手段は、先頭の出力ブロックの後に生成される後続の出力ブロックと、直前の出力ブロックに対応する暗号化データとを記憶するための記憶手段と、後続の出力ブロックと、直前の出力ブロックに対応する暗号化データとを予め定められた規則に基づいて演算することにより、後続の出力ブロックに対応する平文ブロックを生成するための平文ブロック演算手段とを含む。

【0044】

上記の復号装置によると、平文ブロック演算手段は、所定の規則に基づいて（たとえば、予め定められた演算式、関数処理を実行することにより）、平文ブロックを算出することができる。このようにすると、平文データは暗号化データから逐次算出されるため、先頭の出力ブロックに対応する暗号化データに第2のデータが含まれている場合には、各暗号化データの受信順に復号化することにより、第1のデータを取得することができる。

30

【0045】

好ましくは、平文ブロック演算手段は、予め定められた、逆関数を有する関数を用いて、後続の出力ブロックと、直前の出力ブロックに対応する暗号化データとから、後続の出力ブロックに対応する平文ブロックを生成する。

【0046】

上記の復号装置によると、平文ブロックを生成する関数が予め定められており、その関数は逆関数を有する。したがって、その逆関数によって暗号化データが生成されている場合には、その関数によって復号化することができる。このようにすると、先頭の出力ブロックに対応する暗号化データに第2のデータが含まれている場合に、各暗号化データの受信順に復号化することにより、第1のデータを取得することができる。

40

【0047】

好ましくは、復号装置はさらに、復号化処理に使用する鍵を更新するための更新手段を含む。

【0048】

上記の復号装置によると、暗号化データの生成に使用する鍵が変更されても、その変更

50

に応じて、復号化処理に使用する鍵も変更することができるため、暗号化データを確実に復号化することができる。

【0049】

好ましくは、更新手段は、復号化処理の対象となる暗号化データの直前の暗号化データと、直前の暗号化データから生成された出力ブロックと、出力ブロックから生成された平文ブロックと、直前の暗号化データの復号化処理に使用された鍵との少なくとも1つのデータを記憶するための記憶手段と、少なくとも1つのデータに基づいて、新たな鍵を生成するための鍵生成手段と、新たな鍵を復号化処理に使用する鍵として設定するための手段とを含む。

【0050】

上記の復号装置によると、復号化処理に使用する鍵を適宜変更することができるため、暗号通信のセキュリティを向上させることができる。

【0051】

好ましくは、第2のデータは、暗号化データの送信元を識別するための識別データを含む。復号装置はさらに、予め定められたデータを記憶するための記憶手段と、第2のデータから、識別データを取得するための識別データ取得手段と、識別データと、予め定められたデータとが一致するか否かを確認するための識別データ確認手段とを含む。

【0052】

上記の復号装置によると、暗号化データに、送信元を識別するための識別データが含まれている場合には、その識別データを取得した後に、予め準備されているデータと比較することにより、その暗号化データが正当に送信されたものであるか否かを判断することができる。このようにすると、暗号化データの通信のセキュリティを向上させることができる。

【0053】

好ましくは、第2のデータは、予め定められた規則により算出されたハッシュ値を含む。復号装置はさらに、第2のデータからハッシュ値を取得するための取得手段と、復号化された第1のデータにハッシュ演算を実行することにより、ハッシュ値を算出するためのハッシュ値算出手段と、取得手段により取得されたハッシュ値と、ハッシュ値算出手段により算出されたハッシュ値とが一致するか否かを確認するためのハッシュ値確認手段とを含む。

【0054】

上記の復号装置によると、暗号化データに、暗号装置等の送信元において生成されたハッシュ値が含まれている場合には、取得したそのハッシュ値と、復元された第1のデータから生成されるハッシュ値とを比較することにより、その暗号化データが正当に送信されたものであるか否かを判断することができる。このようにすると、暗号化データの通信のセキュリティを向上させることができる。

【0055】

この発明の他の局面に従うと、暗号化方法は、複数のブロックに分割された暗号化データを生成して送信する方法である。この暗号化方法は、データが格納された記憶手段から、平文データに対応する第1のデータと、第1のデータの暗号通信のための第2のデータとを読み出すステップと、第1のデータの先頭から予め定められた範囲内に、第2のデータを追加する追加ステップと、第1のデータの先頭から第2のデータの先頭までのデータのサイズを少なくとも上回るデータサイズによって、第2のデータの追加によって生成される通信データを分割して、暗号化処理が行なわれる前のデータである複数の平文ブロックを生成する通信データ分割ステップと、第1のデータの先頭が含まれる平文ブロックから、入力ブロックを生成する第1の平文ブロック生成ステップと、第1のデータの先頭が含まれる平文ブロックの後に生成される少なくとも1つ以上の後続の平文ブロックの各々に対して、後続の平文ブロックを、後続の平文ブロックの直前の平文ブロックに対応する暗号化データに基づいて変換し、後続の平文ブロックに対応する入力ブロックを生成する第2の平文ブロック生成ステップと、生成された複数の入力ブロックの各々に対して暗号

10

20

30

40

50

化処理を実行して、複数の入力ブロックの各々に対応する暗号化データを生成する暗号化ステップと、生成された複数の暗号化データを送信する送信ステップとを含む。

【0056】

上記の暗号化方法によると、追加ステップにて、第1のデータの先頭から予め定められた範囲内に、第2のデータが追加される。通信データ分割ステップにて、その第2のデータが追加された第1のデータが分割され、暗号化処理の対象となるブロックデータ（平文ブロック）が生成される。第1の入力ブロック生成ステップおよび第2の入力ブロック生成ステップにて、各平文ブロックから入力ブロックが生成されると、暗号化ステップにて、各入力ブロックが暗号化される。このとき、入力ブロックの先頭には、第2のデータが少なくとも含まれるため、生成される暗号化データにも、その第2のデータに対応する暗号化データが含まれる。その後の入力ブロックの生成には、各平文ブロックと、既に生成された暗号化データとが使用されるため、先頭の平文ブロックに含まれる第2のデータは、その後の平文ブロックの各暗号化処理において、逐次反映される。このようにすると、1つの第2のデータを追加することにより複数の暗号化データを生成することができる。また、その第2のデータを変更することにより、同一の第1のデータと同一の鍵とを使用して、異なる暗号化データを生成することができる。これにより、第1のデータに追加するデータ量を増加させることなく、暗号化データを生成する暗号化方法を提供することができる。

10

【0057】

この発明の他の局面に従うと、復号化方法は、複数のブロックに分割された暗号化データを受信して復号する方法である。この復号化方法は、複数の暗号化データを受信するステップと、受信した複数の暗号化データを電子データとして記憶手段に格納するステップと、記憶手段から、複数の暗号化データを読み出すステップと、複数の暗号化データの各々に対して復号化処理を実行して、出力ブロックを生成する出力ブロック生成ステップと、最初に生成される出力ブロックから、平文ブロックを生成する第1の平文ブロック生成ステップと、最初に生成される出力ブロックの後に生成される少なくとも1つ以上の後続の出力ブロックに対して、後続の出力ブロックを、後続の出力ブロックの直前の出力ブロックに対応する暗号化データに基づいて変換し、後続の出力ブロックに対応する平文ブロックを生成する第2の平文ブロック生成ステップと、生成された複数の平文ブロックを結合することにより、平文データに対応する第1のデータと、第1のデータの先頭から予め定められた範囲内に追加された第2のデータとを有する通信データを復元する通信データ復元ステップと、通信データから第2のデータを除去する除去ステップとを含む。

20

30

【0058】

上記の復号化方法によると、分割された複数の暗号化データを受信されると、各暗号化データに応じた出力ブロックが生成される。平文ブロックがその出力ブロックから生成されると、生成された各平文ブロックは結合されて、第1のデータと第2のデータとを有する通信データが復元される。除去ステップにて、通信データから第2のデータが除去されると、第1のデータが抽出される。このようにすると、暗号通信に使用する第2のデータが最初のブロックに含まれている場合には、各暗号化データについて最初のブロックから復号化することにより、第1のデータを再現することができる。その結果、データ量の増加を抑制しつつ、データ通信を行なうことができる復号化方法を提供することができる。

40

【0059】

この発明の他の局面に従うと、暗号化プログラムは、複数のブロックに分割された暗号化データを生成して送信する暗号装置として、コンピュータを機能させる。この暗号化プログラムはコンピュータに、データが格納された記憶手段から、平文データに対応する第1のデータと、第1のデータの暗号通信のための第2のデータとを読み出す準備ステップと、第1のデータの先頭から予め定められた範囲内に、第2のデータを追加する追加ステップと、第1のデータの先頭から第2のデータの先頭までのデータのサイズを少なくとも上回るデータサイズによって、第2のデータの追加によって生成される通信データを分割して、暗号化処理が行なわれる前のデータである複数の平文ブロックを生成する通信デー

50

タ分割ステップと、第1のデータの先頭が含まれる平文ブロックから、入力ブロックを生成する第1の入力ブロック生成ステップと、第1のデータの先頭が含まれる平文ブロックの後に生成される少なくとも1つ以上の後続の平文ブロックの各々に対して、後続の平文ブロックを、後続の平文ブロックの直前の平文ブロックに対応する暗号化データに基づいて、後続の平文ブロックに対応する入力ブロックを生成する第2の入力ブロック生成ステップと、生成された複数の入力ブロックの各々に対して暗号化処理を実行して、複数の入力ブロックの各々に対応する暗号化データを生成する暗号化ステップと、生成された複数の暗号化データを送信する送信ステップとを実行させる。

【0060】

上記のプログラムがコンピュータにおいて実行されると、準備ステップにて、第1のデータと第2のデータとが、記憶手段（たとえば、固定ディスク装置等）から読み出される。追加ステップにて、第1のデータの先頭から予め定められた範囲内に、第2のデータが追加される。通信データ分割ステップにて、その第2のデータが追加された第1のデータが分割され、暗号化処理の対象となるブロックデータ（平文ブロック）が生成される。第1の入力ブロック生成ステップおよび第2の入力ブロック生成ステップにて、各平文ブロックに応じた入力ブロックが生成されると、暗号化ステップにて、各入力ブロックが暗号化される。このとき、ブロックの先頭には、第2のデータが少なくとも含まれるため、生成される暗号化データにも、その第2のデータに対応する暗号化データが含まれる。その結果、その後の入力ブロックの生成には、各平文ブロックと、既に生成された暗号化データとが使用されるため、先頭の平文ブロックに含まれる第2のデータは、その後の平文ブロックの各暗号化処理において、逐次反映される。このようにすると、1つの第2のデータを追加することにより複数の暗号化データを生成することができる。また、その第2のデータを変更することにより、同一の第1のデータと同一の鍵とから、異なる暗号データを生成することができる。これにより、第1のデータに追加するデータ量を増加させることなく、暗号化データを生成する暗号装置として、コンピュータを機能させることができるプログラムを提供することができる。

【0061】

この発明の他の局面に従うと、復号化プログラムは、複数のブロックに分割された暗号化データを受信して復号する復号装置としてコンピュータを機能させる。この復号化プログラムはコンピュータに、複数の暗号化データを受信するステップと、受信した複数の暗号化データを電子データとして記憶手段に格納するステップと、記憶手段から、複数の暗号化データを読み出すステップと、複数の暗号化データの各々に対して復号化処理を実行して、出力ブロックを生成する出力ブロック生成ステップと、最初に生成される出力ブロックから、平文ブロックを生成する第1の平文ブロック生成ステップと、最初に生成される出力ブロックの後に生成される少なくとも1つ以上の後続の出力ブロックの各々に対して、後続の出力ブロックを、後続の出力ブロックの直前の出力ブロックに対応する暗号化データに基づいて変換し、後続の出力ブロックに対応する平文ブロックを生成する第2の平文ブロック生成ステップと、生成された複数の平文ブロックを結合することにより、平文データに対応する第1のデータと、第1のデータの先頭から予め定められた範囲内に追加された第2のデータとを有する通信データを復元する通信データ復元ステップと、通信データから第2のデータを除去する除去ステップとを実行させる。

【0062】

上記のプログラムがコンピュータにおいて実行されると、コンピュータは、受信した暗号化データを記憶手段に電子データとして格納する。コンピュータは、各暗号化データについて復号化処理を実行して、出力ブロックを生成する。平文ブロックがその出力ブロックから生成されると、生成された各平文ブロックは結合されて、第1のデータと第2のデータとを有する通信データが復元される。除去ステップにて、通信データから第2のデータが除去されると、第1のデータが抽出される。これにより、暗号通信に使用する第2のデータが最初のブロックに含まれている場合には、各暗号化データについて最初のブロックから復号化することにより、第1のデータを再現することができる。その結果、データ

量の増加を抑制しつつ、データ通信を行なうことができる復号装置として、コンピュータを機能させることができるプログラムを提供することができる。

【0063】

この発明のさらに他の局面に従うと、記録媒体は、上記の暗号化プログラムまたは上記の復号化プログラムを記録した媒体である。暗号化プログラムは、複数のブロックに分割された暗号化データを生成して送信する暗号装置として、コンピュータを機能させる。復号化プログラムは、複数のブロックに分割された暗号化データを受信して復号する復号装置としてコンピュータを機能させる。

【0064】

上記の記録媒体がコンピュータに装着されると、コンピュータを暗号装置として機能させるプログラムが実行された場合には、そのコンピュータは、第1のデータに追加するデータ量を増加させることなく、暗号化データを生成する暗号装置として機能することができる。また、コンピュータを復号装置として機能させるプログラムが実行された場合には、そのコンピュータは、第1のデータに追加するデータ量を増加させることなく生成された暗号化データを復号する復号装置として機能することができる。

10

【発明の効果】

【0065】

本発明に係る暗号通信システムによると、暗号通信に必要な第2のデータを第1のデータの少なくとも先頭のブロックに含まれるように付加して、順次暗号化された各ブロックが暗号装置から復号装置に送信される。このようにすると、すべてのブロックに第2のデータのようなデータを付加する必要がなくなるため、第1のデータに付加されるデータ（たとえば、ダミーデータ、識別データ等）を増加させることなく暗号化処理および復号化処理を実行することができる。

20

【0066】

本発明に係る暗号装置によると、暗号通信に必要な第2のデータを第1のデータの少なくとも先頭のブロックに含まれるように付加して、各ブロックを順次暗号化する。このようにすると、すべてのブロックに第2のデータのようなデータを付加する必要がなくなるため、第1のデータに付加されるデータを増加させることなく暗号化処理を実行することができる。

【0067】

本発明に係る復号装置によると、暗号通信に必要な第2のデータを含む先頭の暗号化データから復号化して、その復号化されたデータを使用してさらに暗号化データが復号化される。このようにすると、すべてのブロックに第2のデータのようなデータを付加する必要がなくなるため、第1のデータに付加されるデータを増加させることなく生成された暗号化データを復号化することができる。

30

【0068】

本発明に係る暗号化方法によると、暗号通信に必要な第2のデータは、第1のデータの少なくとも先頭のブロックに含まれるように付加される。各ブロックは、順次暗号化される。このようにすると、すべてのブロックに第2のデータのようなデータを付加する必要がなくなるため、第1のデータに付加されるデータを増加させることなく暗号化処理を実行することができる。

40

【0069】

本発明に係る復号化方法によると、暗号通信に必要な第2のデータを含む先頭の暗号化データから復号化される。その復号化されたデータを使用して、後に続く暗号化データが、さらに復号化される。このようにすると、すべてのブロックに第2のデータのようなデータを付加する必要がなくなるため、第1のデータに付加されるデータを増加させることなく生成された暗号化データを復号化することができる。

【0070】

本発明に係る暗号化プログラムによると、コンピュータは、すべてのブロックに第2のデータのようなデータを付加する必要がなくなるため、第1のデータに付加されるデータ

50

を増加させることなく暗号化処理を実行することができる。その結果、処理の遅延を防止したり、第２のデータの生成処理を少なくすることができる。

【００７１】

本発明に係る復号化プログラムによると、コンピュータは、すべてのブロックに第２のデータのようなデータが付加されていない暗号化データを、順次復号化することができる。

【００７２】

本発明に係る記録媒体によると、コンピュータは、第１のデータに付加されるデータの増加を抑制しつつ、第１のデータの暗号化処理、あるいは、暗号化データの復号化処理を実行することができる。したがって、これらの処理の遅延を防止することができる。

10

【発明を実施するための最良の形態】

【００７３】

以下、図面を参照しつつ、本発明の実施の形態について説明する。以下の説明では、同一の部品には同一の符号を付してある。それらの名称および機能も同じである。したがって、それらについての詳細な説明は繰り返さない。

【００７４】

＜第１の実施の形態＞

図１を参照して、本発明の第１の実施の形態に係る暗号通信システムについて説明する。図１は、本実施の形態に係る暗号通信システムを構成する暗号装置１００と、通信回線１９０に接続された復号装置１５０との概念的な構成を表わす機能ブロック図である。

20

【００７５】

この暗号装置１００は、データを記憶するための記憶部１０２と、予め定められた基準に基づいて所定のデータに乱数を付加するための乱数付加部１０３と、予め定められた基準に基づいて入力ブロックを算出するための入力ブロック算出部１０６と、予め定められた処理に基づいてデータを暗号化するための暗号化部１０７と、データを送信するためのデータ送信部１０８とを含む。

【００７６】

なお、ここでは、「乱数」とは、データ列にどのような規則性も存在しない、ランダムなデータ列をいう。この乱数は、ある種となるデータから予測することが難しい規則に基づいて生成されるデータ列である「擬似乱数」も含む。たとえば、現在時刻を種として擬似乱数列を生成させ、その一部のデータ列を乱数としてもよい。

30

【００７７】

この暗号装置１００において、乱数付加部１０３と、入力ブロック算出部１０６と、暗号化部１０７との機能は、後に詳述するように、たとえばＣＰＵ（Central Processing Unit）１１０が所定のプログラムを実行することによって実現される。

【００７８】

図１を再び参照して、復号装置１５０は、記憶部１２２と、予め定められた基準に基づいて所定のデータから乱数を除去するための乱数除去部１２３と、予め定められた基準に基づいて平文ブロックを算出するための平文ブロック算出部１２６と、暗号化されたデータを所定の処理に基づいて復号化するための復号化部１２７と、外部からデータを受信するためのデータ受信部１２８とを含む。

40

【００７９】

この復号装置１５０において、乱数除去部１２３と、平文ブロック算出部１２６と、復号化部１２７との機能は、後述するように、たとえばＣＰＵ１２０が所定のプログラムを実行することによって実現される。

【００８０】

このような構成を有する暗号通信システムにおいて、暗号装置１００は、記憶部１０２に保存されているコンテンツ（平文データ）に対して暗号化処理を実行し、暗号化したデータを通信回線１９０を介して復号装置１５０に送信する。復号装置１５０は、受信した暗号データを所定の復号化処理を実行して復号化する。これらの処理については、後述す

50

る。

【0081】

ここで、「コンテンツ」とは、あらゆる種類のデータを対象とすることができる。対象となる主なデータとしては、不正利用を防ぎたいデータ、たとえば、著作権などがあるデータ、課金情報その他のデータである。より具体的には、たとえば、音楽や画像、動画、電子書籍などのデータ、あるいは、携帯電話、P C (Personal Computer) 等のコンテンツを利用することができる装置内で実行可能なプログラムなどである。以下では、このようなコンテンツが利用されるデータそのままの状態を「平文データ」と呼び、コンテンツが変換されて、暗号化されたものを「暗号化データ」と呼ぶ。

【0082】

また、「送信」とは、データを他の機器に送ることであり、その手段は問わない。たとえば、通信回線190その他の通信ネットワークを介して、データを受信装置へ送ってもよい。あるいは、C D - R O M (Compact Disc - Read Only Memory) や D V D (Digital Versatile Disc) その他の情報記録媒体にデータを格納し、その媒体を別の装置の駆動装置に装着してもよい。

【0083】

「受信」とは、データを他の機器から受け取ることをいい、上述の送信方法に応じて受信手段が決まる。この受信手段には、通信回線に接続可能なインターフェースであってもよいし、上述の情報記録媒体に格納されたデータを読み出すことができる駆動装置であってもよい。

【0084】

「暗号」とは、暗号化されていない通常のデータ（平文データ）を何らかの規則にしたがって変換し、そのままでは第3者にとって何を意味しているかわからないデータ（暗号化データ）に変換する処理をいう。この場合、何らかの規則（最初の規則と同一でなくてもよい）によって、暗号文を元の平文に復元できる復号処理が存在する。変換時に「鍵」を用いて暗号処理を行なうのが一般的である。このような処理には、復号処理に同じ「鍵」を用いて復号できる共通鍵暗号や、決められたペアの2つの鍵によって暗号処理、復号処理が可能である公開鍵暗号などがある。共通暗号方式としては、D E S 方式、A E S (Advance Encryption Standard) 方式その他の方法がある。公開鍵暗号方式では、R S A 暗号 (Rivest - Shamir - Adleman Scheme)、E l g a m a l 暗号などがある。以下の説明では、ブロック単位で処理を行なう共通鍵暗号について説明する。

【0085】

「鍵」は、暗号方式で利用可能な任意のデータであり、暗号化を行なうごとに1つ割り当てられる。たとえば、64ビット鍵のD E S 方式であれば、64ビット長のデータとなる。

【0086】

なお、「鍵」は、ある決められた変換処理によって、暗号方式で利用される鍵を算出できるようなデータであってもよい。コンテンツこのコンテンツ鍵を用いて暗号化コンテンツ305を生成する。この暗号化コンテンツ305は、コンテンツ全体が必ずしも暗号化されていなくてもよく、「鍵」なしで復号装置においてコンテンツが復号されることがなければよいとする。「暗号化」は、暗号化チップなどのハードウェアを使って暗号化してもよいし、ソフトウェアで暗号化してもよい。

【0087】

図2を参照して、本実施の形態に係る暗号装置100あるいは復号装置150を実現する一例であるコンピュータ200について説明する。図2は、コンピュータ200のハードウェア構成を表わすブロック図である。

【0088】

図2に示すように、このコンピュータ200は、バスによって相互に接続された、C P U 210と、モニタ220と、マウス230と、キーボード240と、メモリ250と、固定ディスク260と、F D (Flexible Disc) 駆動装置270と、C D - R O M (Compa

10

20

30

40

50

ct Disc - Read Only Memory) 駆動装置 280 と、通信 I F (Interface) 290 とを含む。F D 駆動装置 270 には、F D 272 が装着される。C D - R O M 駆動装置 280 には、C D - R O M 282 が装着される。

【0089】

モニタ 220 は、通常、グラフィックチップや V R A M (Video Random Access Memory) などと組み合わされて実現される。C P U 210 は、V R A M 上のデータを表示信号に変換して、液晶ディスプレイその他のモニタ 220 に送信する。モニタ 220 は、表示信号を画像として表示する。

【0090】

ユーザの指示を入力する手段としては、キーボード 240、マウス 230、ボタン (図示しない) 等がある。ユーザの指示は、バスを介してコンピュータ 200 の C P U 210 に入力される。この他にも各種操作機器、マイクによる音声入力など、様々な入力手段を使用することができる。

【0091】

キーボード 240 は、押下されたキーを検出する機械的もしくは電子的なスイッチなどを含む。マウス 230 は、マウスボタンの押下状態を検出するメカニカルもしくは電子的なスイッチなどと、マウスの縦と横の相対移動距離を検出するメカニカルもしくは電子的なセンサを含む。

【0092】

メモリ 250 は、たとえば、D R A M (Dynamic Random Access Memory) やフラッシュメモリなどのメモリデバイスを含む。なお、メモリ 250 は、これらに限られず、たとえば、C P U 210 内部に含まれるメモリやレジスタなどであってもよい。

【0093】

通信 I F 290 は、たとえば、ネットワークインターフェースカードなどを含む。コンピュータ 200 は、この通信 I F 290 を介して、無線や有線などにより接続された他の通信装置とデータ通信を行なうことができる。

【0094】

なお、このような構成に加えて、コンピュータ 200 は、音声を出力するための音声出力部 (たとえばサウンドカード等) を含んでもよい。この場合、コンピュータ 200 にスピーカ (図示しない) を接続することにより、そのスピーカは、音声信号を音声に変換して出力することができる。出力される音声は、単波長の単純な音の場合もあるし、音楽や人間の音声など複雑な場合もある。出力する音声は予め決まっている場合、送られて来るデータは音声信号ではなく、単なるオン、オフの動作制御信号だけという場合もある。

【0095】

このような構成を有するコンピュータが、図 1 に示した暗号装置 100 として使用された場合には、C P U 210 は、乱数付加部 103 として、メモリ 250、固定ディスク 260 等の記憶装置に格納されているデータを読み出して所定の乱数をそのデータに付加する。

【0096】

また、C P U 210 は、入力ブロック算出部 106 として、メモリ 250、固定ディスク 260 等の記憶装置 (以下、「記憶装置」と称す) に格納されているデータを読み出し、所定の処理を実行することにより、そのデータを複数のブロックに分割する。

【0097】

さらに、C P U 210 は、暗号化部 107 として、分割されたブロックを所定の暗号化方法に基づいてそれぞれ暗号化する。この暗号化されたデータは、記憶装置に再び格納される。

【0098】

一方、図 2 に示したコンピュータ 200 が図 1 における復号装置 150 として使用される場合には、C P U 210 は、復号化部 127 として、記憶装置に格納されている暗号化データを読み出して復号化する。

【0099】

また、CPU 210は、平文ブロック算出部126として、復号化された各ブロックと予め記憶されている復号化キーとを使用して平文ブロックを算出する。この算出されたデータは、記憶装置に格納される。

【0100】

さらに、CPU 210は、乱数除去部123として、そのようにして復号化された平文ブロックを記憶装置から読み出して、そのブロックに付加された乱数を除去する。乱数が除去されたデータは、記憶装置に再び格納される。

【0101】

このように、上述した各部における処理は、その処理を実行するソフトウェアをCPU 210に実行させることによって、実現することができる。このようなソフトウェアは、固定ディスク260その他のハードウェアに予め記憶されている場合もあれば、CD-ROM 282その他の記録媒体に格納されて流通し、CD-ROM駆動装置280その他の装置によって、その記録媒体から読み取られてソフトウェアを格納する固定ディスク260に一旦格納される場合もある。そのソフトウェアは、固定ディスク260からメモリ250に読み出されて、CPU 210により実行される。図2に示したコンピュータ200のハードウェア構成は、一般的なものである。したがって、本発明の最も本質的な部分は、固定ディスク260、CD-ROM 282その他の記録媒体に格納されたソフトウェアであるとも言える。

【0102】

なお、図2に示したコンピュータ200自体の動作は周知であるので、その詳細な説明は、繰り返さない。

【0103】

図3を参照して、本実施の形態に係る暗号装置100の記憶部102に格納されるデータについて説明する。図3(A)は、暗号化して通信するための平文データPに乱数Rが付加されたブロックB300を表わす図である。図3(B)は、暗号装置100において平文データPが暗号化処理された後に、記憶部102に格納される暗号化ブロックを表わす図である。

【0104】

図3(A)に示すように、平文データPを暗号化する場合には、暗号化処理の前にそのデータPに乱数Rが付加されて一時的に格納される。このとき、付加される位置は、ブロックB300が所定のデータサイズを有するブロックに分割されたとき、先頭のブロックに乱数Rの先頭が少なくとも含まれる位置であればよい。

【0105】

その後、図3(B)に示すように、暗号装置100が所定の暗号化処理に基づいて、そのブロックB300を暗号化すると、ブロック「C0」、「C1」、「C2」等が生成され、記憶部102に再び格納される。

【0106】

図4を参照して、本実施の形態に係る復号装置150の記憶部122に格納されるデータについて説明する。図4(A)は、復号装置150がデータ受信部128を介して受信した暗号化データの格納の一態様を表わす図である。図4(B)は、その暗号化データを所定の条件に基づいて復号化することにより生成されたブロックB300の格納の一態様を表わす図である。

【0107】

図4(A)に示すように、復号装置150が暗号装置100から暗号化データを受信すると、受信データは記憶部122に順次格納される。このように格納されるデータ（すなわち、ブロック「C0」、「C1」、「C2」）は、図3(B)に示したデータと同じデータである。

【0108】

図4(B)に示すように、所定の復号化処理に基づいて暗号化データを復元すると、乱

数 R と平文データ P とを含むブロック B 3 0 0 が生成され、記憶部 1 2 2 に格納される。このようにして、復号装置 1 5 0 において生成されるブロック B 3 0 0 は、暗号装置 1 0 0 において生成されるブロック B 3 0 0 (図 3 (A)) と同じ内容を含む。

【0109】

ここで、図 5 を参照して、本実施の形態に係る暗号装置 1 0 0 における暗号化処理の概念について説明する。以下では、通信データとして平文データ P を暗号化して送信する場合について、図 1 を参照しつつ説明する。

【0110】

暗号装置 1 0 0 の記憶部 1 0 2 に格納されているデータ P を暗号化して送信する場合、暗号装置 1 0 0 は、予め定められた処理条件に基づいて、その平文データ P に乱数 R を付加する。乱数 R のサイズは任意の予め定められた値である。この乱数 R が付加される位置は、たとえば平文データ P の前方部であるが、これに限られない。この位置は、付加の前に予め定められている。ただし、この乱数が付加される位置は、通信データが複数のブロックに分割される際、先頭のブロックに存在する位置であればよい。

【0111】

たとえば、1 つのブロックのサイズが X ビットである場合、乱数 R は先頭から X ビットまでの位置に埋め込まれる。この場合、たとえば、先頭 1 ブロック目全体が乱数列となっても、すなわち、乱数 R のサイズが X ビットであってもよい。あるいは、乱数 R のサイズが X ビットより大きく、乱数 R の一部が 2 番目のブロックにまたがっていてもよい。

【0112】

このようにして、乱数 R が付加された平文データ P を含む平文ブロックは、予め定められたサイズに分割され、複数のブロックが生成される。

【0113】

このブロックの中の最初のブロックは、入力ブロック「Q 1」として、暗号化部 1 0 7 に入力される。暗号化部 1 0 7 は、入力ブロック「Q 1」に対して、暗号化鍵 K と暗号化処理関数 F とに基づいて暗号化処理を実行する。その結果、入力ブロック「Q 1」に対応する暗号化データ「C 0」が生成される。

【0114】

この暗号化データ「C 0」は、記憶部 1 0 2 の所定のデータ領域に格納される一方、次の暗号化データ（すなわち「C 1」）を生成するための入力データとして、入力ブロック算出部 1 0 6 に入力される。入力ブロック算出部 1 0 6 は、入力された暗号化データ「C 0」と、暗号化処理の実行前に生成された平文ブロック「P 1」とに基づいて、所定の演算処理を実行することにより入力ブロック「Q 1」を生成する。この演算は、入力ブロック算出関数 F a の実行により行なわれる。

【0115】

ここで、入力ブロック算出関数 F a について説明する。この関数 F a は、入力ブロック「Q 1」と暗号化データ「C 0」と平文ブロック「P 1」との関係を、たとえば $Q(1) = Fa(C0, P1)$ と表わす。

【0116】

このような関数 F a は、入力ブロック「Q 1」と暗号化データ「C 0」と平文ブロック「P 1」との関係を、 $P(1) = Ga(C0, Q1)$ と表わす逆関数 G a が存在する関数であればよい。このような関数には、たとえば、関数 F a およびその逆関数 G a とともに、排他的論理和の演算を実行することができる関数が含まれる。

【0117】

図 5 を再び参照して、入力ブロック「Q 1」は入力ブロック算出部から暗号化部 1 0 7 へ出力され、暗号化処理関数 F b の実行により、暗号化データ「C 1」が生成される。

【0118】

このようにして生成された暗号化データ「C 1」は、記憶部 1 0 2 に格納されている暗号化データ「C 0」に続けて記憶されるとともに、その次の暗号化データ（すなわち「C 2」）を生成するために入力ブロック算出部 1 0 6 に入力される。

【0119】

入力ブロック算出部106は、暗号化データ「C1」と、暗号化処理の実行前に生成された平文ブロック「P2」とに対して、第1の関数F_aを実行することにより、入力ブロック「Q2」を生成する。

【0120】

入力ブロック算出部106から出力される入力ブロック「Q2」は、暗号化部107に入力される。暗号化部107は、暗号鍵Kと暗号化処理関数F_bとに基づいて所定の暗号化処理を実行することにより、入力ブロック「Q2」の暗号化データ「C2」を生成する。このようにして生成された暗号化データ「C2」は、記憶部102に格納される。このときの格納の態様は特に限られず、既に格納されている他の暗号化データ「C1」に続けて保存されてもよい。この暗号化データ「C2」はさらに、後続のブロックを暗号化するために、入力ブロック算出部106に入力される。

10

【0121】

ここで、暗号化処理関数F_bについて説明する。この関数F_bによると、Xビット長の入力ブロックと鍵Kとから、Xビット長の暗号化データが出力される。本実施の形態では、毎回同じ鍵Kを用いて暗号化処理が行なわれる。たとえば、n番目の入力ブロック「Q_n」と、暗号化データ「C_n」と、鍵Kとの関係は、 $C_n = F_b(Q_n, K)$ 、ここで、 $n = 0, 1, 2, 3 \dots$ 、と表わされる。

【0122】

このように、図5を参照して詳述したように、最初のブロックの平文データ「P0」が同一であっても、暗号通信ごとに、異なる乱数Rが平文データに付加されるため、暗号化データ「C0」は、暗号化処理ごとに異なる値が出力される。

20

【0123】

次のブロックを暗号するとき、暗号装置100は、平文ブロック「P1」と先に生成された暗号化データ「C0」とを関数F_aにより演算して、入力ブロック「Q1」を生成し、暗号化する。このブロック「Q1」の算出には、暗号化処理ごとに異なる結果となる暗号化データ「C0」が用いられる。したがって、平文ブロック「P1」が同じであっても、生成される暗号化データ「C1」は、暗号化処理ごとに異なる。以下の平文ブロックも同様に暗号化処理を実行することができる。このようにすると、暗号装置100は、暗号化処理のために同一の鍵を使用しても、暗号化処理ごとに、内容の異なる暗号化データを生成することができる。

30

【0124】

次に、図6を参照して、本実施の形態に係る復号装置150における暗号化データの復号化処理について説明する。

【0125】

暗号装置100その他の暗号装置によって暗号化されたデータが通信回線を介して送信されると、そのデータを受信した復号装置150は、受信データを記憶部122に記憶する。このデータは、たとえば図4(A)に示したように、暗号化データ「C0」, 「C1」, 「C2」などである。

【0126】

このようにして格納されているデータのうち、先頭のデータである暗号化データ「C0」は、復号化部127によって最初に読み出される。このデータは、暗号鍵Kと復号化処理関数G_bとに基づいて復号化される。その結果、出力ブロック「Q0」が生成される。このデータは、最初の平文ブロック「P0」として、記憶部122に格納される。

40

【0127】

ここで、復号化処理関数G_bについて説明する。この復号化処理関数G_bは、図5において示した暗号化処理関数F_bの逆関数である。本実施の形態における暗号化方式が共通鍵暗号方式であるため、復号装置150が使用する鍵は、暗号装置100が使用する鍵Kと同一である。したがって、出力ブロック「Q_n」と、暗号化データ「C_n」と、鍵Kとの関係は、 $Q_n = G_b(C_n, K)$ 、ただし、 $n = 0, 1, 2, \dots$ 、と表わされる。

50

【0128】

図6を再び参照して、暗号化データ「C1」が、記憶部122から復号化部127によって読み出される。復号化部127は、暗号化データ「C1」に対して、暗号鍵Kと復号化処理関数Gbとを使用して、所定の復号化処理を実行する。その結果、出力ブロック「Q1」が生成される。

【0129】

復号化部127から出力される出力ブロック「Q1」は、平文ブロック算出部126に入力される。平文ブロック算出部126は、記憶部122に格納されている暗号化データ「C0」と平文ブロック算出関数Gaとを使用して、出力ブロック「Q1」に対して所定の処理を実行する。その結果、平文ブロック「P1」が生成される。

10

【0130】

ここで、平文ブロック算出関数Gaについて説明する。このGaは、図5において示した入力ブロック算出関数Faの逆関数である。したがって、たとえば、平文ブロック「P1」と、暗号化データ「C0」と、出力ブロック「Q1」との関係は、 $P1 = Ga(C0, Q1)$ と表わされる。

【0131】

図6を再び参照して、復号化部127は、記憶部122から暗号化データ「C2」を読み出す。復号化部127は、暗号鍵Kと復号化処理関数Gbとを使用して、暗号化データ「C2」に対して所定の復号化処理を実行する。その結果、出力ブロック「Q2」が生成される。

20

【0132】

復号化部127から出力される出力ブロック「Q2」は、平文ブロック算出部126に入力される。平文ブロック算出部126は、その出力ブロック「Q2」と、記憶部122から読み出した暗号化データ「C1」とを使用して、所定の平文ブロック算出関数Gaを実行する。その結果、平文ブロック「P2」が生成される。平文ブロック算出部126は、生成した平文ブロック「P2」を記憶部122に格納する。なお、このときの格納の様子は特に限られず、たとえば、既に格納されている他の暗号化データ「C1」に続けて格納されてもよいし、別の領域に格納されてもよい。

【0133】

図7を参照して、本実施の形態に係る暗号装置100の制御構造について説明する。図7は、暗号装置100を実現するCPUが実行する処理の手順を表わすフローチャートである。

30

【0134】

ステップS702にて、暗号装置100のCPU110は、乱数付加部103として、所定の乱数を発生させ、その乱数を平文データの予め定められた位置に付加する。

【0135】

ステップS704にて、CPU110の入力ブロック算出部106は、先頭の1ブロック目のデータから入力ブロックを作成する。

【0136】

ステップS706にて、CPU110の暗号化部107は、作成された入力ブロックを所定の条件に基づいて暗号化する。

40

【0137】

ステップS708にて、CPU110は、すべての平文データを暗号化したか否かを判断する。この判断は、たとえば生成された入力ブロックの数に対して、暗号化処理を実行した回数を比較することにより行なわれる。したがって、たとえば、暗号化処理の回数が、生成された入力ブロックの数よりも少ない場合には、すべての平文データは暗号化されていないと判断されることになる。すべての平文データを暗号化したと判断すると（ステップS708にてYES）、処理は、ステップS712に移される。そうでない場合には（ステップS708にてNO）、処理は、ステップS710に移される。

【0138】

50

ステップS710にて、CPU110の入力ブロック算出部106は、平文データと、暗号化データと、次のブロックとを使用して、予め定められた処理を実行して、次の入力ブロックを作成する。

【0139】

ステップS712にて、CPU110は、暗号化したデータを記憶部102に記憶する。

【0140】

図8を参照して、本実施の形態に係る復号装置の制御構造について説明する。図8は、復号装置150を実現するCPU120が実行する処理の手順を表わすフローチャートである。

【0141】

ステップS802にて、復号装置150のCPU120は、通信回線を介して受信した暗号化データを記憶部122に保存する。

【0142】

ステップS804にて、CPU210の復号化部127は、先頭の1ブロック目の暗号化データを復号化する。その結果、出力ブロックが生成される。

【0143】

ステップS806にて、CPU210の平文ブロック算出部126は、生成された出力ブロックから平文ブロックを生成する。

【0144】

ステップS808にて、CPU210は、すべての暗号化データを復号化したか否かを判断する。この判断は、たとえば記憶部122に格納されている暗号化データの数と、復号化処理を実行した回数とを比較することにより行なわれる。したがって、たとえば、復号化処理の回数が、記憶されている暗号化データの数よりも少ない場合には、すべての暗号化データは復号化されていないと判断されることになる。すべての暗号化データを復号化したと判断すると（ステップS808にてYES）、処理は、ステップS812に移される。そうでない場合には（ステップS808にてNO）、処理は、ステップS810に移される。

【0145】

ステップS810にて、CPU210の復号化部127は、暗号鍵と、暗号化データと、次のブロックのデータに基づいて、未処理の暗号化データを復号化する。

【0146】

ステップS812にて、CPU210は、復号化して生成された平文データを記憶部122の所定のデータ領域に格納する。

【0147】

以上のような構造およびフローチャートに基づく、本実施の形態に係る暗号装置100および復号装置150を有する暗号通信システムの動作について、暗号化処理と復号化処理とに分けて説明する。以下では、利用者Aが暗号装置100を使用して、復号装置150を使用する利用者Bに通信データを送信する場合について説明する。

【0148】

〔暗号化処理〕

利用者Aが暗号送信したい通信データを暗号装置100に保存して、予め定められた手続を実行して（たとえば、送信プログラムの実行等）、所定の暗号送信の指令を入力する。暗号装置100は、その指令に応答して、所定の暗号化処理プログラムを実行し、乱数を発生し、通信データにその乱数を付加する（ステップS702）。

【0149】

暗号装置100は、そのデータを所定のサイズのブロックに分割し、入力ブロックを生成する（ステップS704）。暗号装置100は、各ブロックごとに暗号化処理を実行し（ステップS706）、利用者が送信を希望する通信データのすべてのデータを暗号化すると（ステップS708にてYES）、そのデータを記憶部102に保存する（ステップ

10

20

30

40

50

S 7 1 2)。暗号装置 1 0 0 は、予め定められた通信プロトコルに基づいて暗号データを出力する。

【0 1 5 0】

〔復号化処理〕

利用者 B が復号装置 1 5 0 が暗号装置 1 0 0 が送信した暗号化データを受信すると、各暗号化データは、復号装置 1 5 0 の記憶部 1 2 2 に格納される（ステップ S 8 0 2）。

【0 1 5 1】

復号装置 1 5 0 は、暗号化データの先頭ブロックから 1 ブロックずつ復号化して、出力ブロックを生成する（ステップ S 8 0 4）。復号装置 1 5 0 はさらに、出力ブロックから平文ブロックを生成する（ステップ S 8 0 6）。すべての暗号化データの復号化処理が完了すると（ステップ S 8 0 8 にて Y E S）、復号装置 1 5 0 はすべての平文ブロックを結合して、乱数を除去する。その結果、通信データが復元されるため、利用者 B は、その通信データを認識することができる。

10

【0 1 5 2】

以上のようにして、本発明の第 1 の実施の形態に係る暗号装置 1 0 0 は、通信データの分割後に先頭のブロックに少なくとも乱数の一部が含まれるように、その乱数を付加して、データをブロックに分割する。暗号装置 1 0 0 は、その先頭のブロックから、所定の暗号化処理を実行し、以降のブロックの暗号化処理では、先頭のブロックの暗号化処理の結果を使用する。したがって、すべてのブロックに乱数データを付加することなく、セキュリティレベルの高い暗号送信を実行することができる。

20

【0 1 5 3】

また、本実施の形態に係る復号装置 1 5 0 は、ブロックに分割された暗号化データを受信すると、先頭のブロックから、所定の復号化処理を実行する。この場合、各暗号化データは、以降のブロックにおける平文ブロックの生成処理に使用されるため、暗号装置 1 0 0 による暗号化処理によって生成されたデータを復元することができる。

【0 1 5 4】

このようにして、通信データに付加するデータサイズを増加することなく、データ通信を行なうことができる暗号装置および復号装置を実現することができる。

【0 1 5 5】

＜第 1 の実施の形態 変形例＞

30

以下、本発明の第 1 の実施の形態の変形例について説明する。

【0 1 5 6】

本変形例に係る暗号装置の入力ブロック算出部は、平文ブロックと暗号化データと先に生成された入力ブロックとに基づいて、入力ブロックを算出することができる点で、前述の暗号装置 1 0 0 と異なる。なお、本変形例に係る暗号装置の構成は、図 1 に示した暗号装置 1 0 0 の構成と同じであるため、その説明は、繰り返さない。

【0 1 5 7】

図 9 を参照して、本変形例に係る暗号装置における暗号化処理の方法について説明する。

【0 1 5 8】

40

図 9 に示すように、平文データ P に対して所定の乱数 R が付加されて所定のデータサイズ（X ビット）に分割されると、平文ブロック「P 0」, 「P 1」, 「P 2」が生成される。

【0 1 5 9】

先頭の平文ブロック「P 0」は、入力ブロック「Q 0」として暗号化部 1 0 7 に入力される。暗号化部 1 0 7 は、その入力ブロック「Q 0」と暗号鍵 K とを使用して、予め定められた暗号化処理関数 F b による暗号化処理を実行する。その結果、暗号化データ「C 0」が生成される。このデータ「C 0」は、記憶部 1 0 2 に記憶されるとともに、次の入力ブロック（すなわち「Q 1」）を生成するために、使用される。

【0 1 6 0】

50

次に、第2の平文ブロック「P1」は、入力ブロック算出部106に入力される。入力ブロック算出部106は、平文ブロック「P1」と、既に生成された暗号化データ「C0」とを使用して、入力ブロック算出関数Fcに基づく所定の演算処理を実行する。その結果、入力ブロック「Q1」が生成される。

【0161】

ここで、入力ブロック算出関数Fcについて説明する。この関数Fcは、第n番目の入力ブロック「Qn」と、第(n-1)番目の平文ブロック「Pn-1」と、第(n-1)番目の暗号化データと、第n番目の平文ブロック「Pn」との関係を、 $Q_n = F_c(P_{n-1}, C_{n-1}, P_n)$ 、ただし、 $n = 1, 2, 3, n \cdots$ 、と表わす。なお、このような関数Fcは、その逆関数Gcを有する。この場合、上記の各データの関係は、 $P_n = G_c(P_{n-1}, C_{n-1}, Q_n)$ 、と表わされる。 10

【0162】

図9を再び参照して、入力ブロック算出部106から出力される入力ブロック「Q1」は、暗号化部107に入力される。暗号化部107は、この入力ブロック「Q1」と暗号鍵Kとを使用して所定の暗号化処理を実行する。その結果、暗号化データ「C1」が生成される。

【0163】

暗号化部107から出力される暗号化データ「C1」は、記憶部102に格納されるとともに、次の暗号化データ「C2」を生成するために入力ブロック算出部106に入力される。 20

【0164】

入力ブロック算出部106は、第3の平文ブロック「P2」と既に生成された入力ブロック「Q1」と、事前に生成された暗号化データ「C1」とを使用して、所定の処理を実行する。その結果、入力ブロック「Q2」が生成される。

【0165】

入力ブロック算出部106から出力される入力ブロック「Q2」は、暗号化部107に入力される。暗号化部107は、この入力ブロック「Q2」と暗号鍵Kとを使用して所定の暗号化処理を実行する。その結果、暗号化データ「C2」が生成される。

【0166】

暗号化部107から出力される暗号化データ「C2」は、記憶部102に格納される。 30
次の暗号化データを生成する必要がある場合には、暗号化データ「C2」は、入力ブロック算出部106に入力される。

【0167】

上記の「Pn」($n = 1, 2, 3 \cdots$)を算出する処理は、すなわち、関数Fc(P_{n-1}, C_{n-1}, P_n)に基づいて行なわれる。この場合、関数Fcは逆変換を行なう関数Gcを有する。この関数Gcは、たとえば $G_c(P_{n-1}, C_{n-1}, P_n)$ と表わされる。このようにしても、同様の効果を得ることができる。

【0168】

<第2の実施の形態>

以下、本発明の第2の実施の形態について説明する。本実施の形態に係る暗号通信システムは、暗号化処理あるいは復号化処理をするための暗号鍵を算出する機能を有する点で、前述の第1の実施の形態に係るシステムと異なる。 40

【0169】

図10を参照して、本実施の形態に係る暗号通信システムの構成について説明する。このシステムは、暗号装置900と復号装置950とを含む。暗号装置900と復号装置950とは、一般の通信回線190によって接続される。

【0170】

この暗号装置900は、前述の第1の実施の形態に係る暗号装置100の構成に加えて、さらに鍵算出部910を含む。この鍵算出部910は、予め定められた暗号鍵の算出処理を実行する。 50

【0171】

なお、暗号装置900において、第1の実施の形態に係る暗号装置100が有する構成と同じ構成には、同一の番号を付してある。それらの機能も同じである。したがって、それらについての説明は、繰り返さない。

【0172】

図10を再び参照して、復号装置950は、第1の実施の形態に係る復号装置150の構成に加えて、暗号化データを復号化するための暗号鍵を算出する鍵算出部960を含む。鍵算出部960は、復号化処理において生成されたデータを使用して、復号化処理に使用する新たな暗号化鍵を逐次生成する。なお、この復号装置950において、図1に示した復号装置150の構成と同一の構成には同一の番号を付してある。それらの機能も同じである。したがって、それらについての説明は、繰り返さない。 10

【0173】

なお、本実施の形態に係る暗号装置あるいは復号装置は、図2に示したような構成を有するコンピュータによって実現することもできる。このようなコンピュータの構成は、周知であるため、ここでは、その説明は繰り返さない。

【0174】

図11を参照して、本実施の形態に係る暗号装置900における暗号化処理の方法について説明する。

【0175】

図11に示すように、平文データPに対して所定の乱数Rが付加されて所定のデータサイズ(Xビット)に分割されると、平文ブロック「P0」, 「P1」, 「P2」が生成される。 20

【0176】

先頭の平文ブロック「P0」は、入力ブロック「Q0」として暗号化部107に入力される。暗号化部107は、その入力ブロック「Q0」と暗号鍵Kとを使用して、予め定められた暗号化処理関数Fbによる暗号化処理を実行する。その結果、暗号化データ「C0」が生成される。この暗号化データ「C0」は、記憶部102に記憶される。

【0177】

暗号化部107から出力される暗号化データ「C0」は、鍵生成関数Fdを実行する鍵算出部910に入力される。鍵算出部910は、暗号化データと、事前に使用された暗号鍵(K)とを使用して、新たな暗号鍵を生成する。 30

【0178】

ここで、鍵生成関数Fdについて説明する。この関数は、第n番目の鍵Knと、第(n-1)番目の鍵「Kn-1」と、暗号化データ「Cn-1」との関係を、たとえば、 $Kn = F4(Kn-1, Cn-1)$ 、ただし、 $n = 1, 2, 3 \dots$ 、と表わす。これにより、各ブロックにおいて異なる暗号鍵を暗号化処理に使用することができるため、平文ブロックが同一であっても、異なる暗号化データが生成される。

【0179】

図11を再び参照して、第2の平文ブロック「P1」は、入力ブロック「Q1」として暗号化部107に入力される。鍵算出部910により新たに生成された暗号鍵も、暗号化部107に入力される。暗号化部107は、この入力ブロック「Q1」と暗号鍵とを使用して、所定の暗号化処理を実行する。その結果、暗号化データ「C1」が生成される。この暗号化データ「C1」は、記憶部102に格納される。 40

【0180】

暗号化部107から出力される暗号化データ「C1」は、鍵生成関数Fdを実行する鍵算出部910に入力される。鍵算出部910は、暗号化データと、事前に使用された暗号鍵とを使用して、新たな暗号鍵を生成する。

【0181】

次に、第3の平文ブロック「P2」は、入力ブロック「Q2」として暗号化部107に入力される。鍵算出部910により新たに生成された暗号鍵も、暗号化部107に入力さ 50

れる。暗号化部 107 は、この入力ブロック「Q2」と暗号鍵とを使用して、所定の暗号化処理を実行する。その結果、暗号化データ「C2」が生成される。この暗号化データ「C2」は、記憶部 102 に格納される。次の暗号化データを生成する必要がある場合には、暗号化データ「C2」は、同様に鍵算出部 910 に入力される。

【0182】

なお、本実施の形態に係る復号装置 950 における復号処理の概念も、図 11 に示した暗号装置 900 における暗号処理の概念に適用される。すなわち、暗号鍵の生成は、鍵生成関数 Fd により行なわれる。したがって、ここでは、それらについての説明は繰り返さない。

【0183】

図 12 を参照して、本実施の形態に係る暗号装置 900 を実現する CPU の制御構造について説明する。図 12 は、暗号装置 900 の CPU が実行する暗号化処理の手順を表わすフローチャートである。

【0184】

なお、前述の第 1 の実施の形態に係る暗号装置 100 における処理と同一の処理には同一のステップ番号を付し、それらについての説明は繰り返さない。

【0185】

ステップ S708 にて、暗号装置 900 の CPU110 は、すべての平文データを暗号化したか否かを判断する。すべての平文データを暗号化したと判断すると（ステップ S708 にて YES）、処理はステップ S712 に移される。そうでない場合には（ステップ S708 にて NO）、処理はステップ S1210 に移される。

【0186】

ステップ S1210 にて、CPU110 の鍵算出部 910 は、暗号化データと暗号鍵とに基づいて、次の暗号鍵を作成する。

【0187】

図 13 を参照して、本実施の形態に係る復号装置 950 を実現する CPU120 の制御構造について説明する。図 13 は、暗号装置 950 の CPU120 が実行する復号化処理の手順を表わすフローチャートである。

【0188】

なお、前述の第 1 の実施の形態に係る復号装置 150 における処理と同一の処理には同一のステップ番号を付し、それらについての説明は繰り返さない。

【0189】

ステップ S808 にて、CPU210 は、すべての暗号化データを復号化したか否かを判断する。この判断は、たとえば記憶部 122 に格納されている暗号化データの数と、復号化処理を実行した回数とを比較することにより行なわれる。したがって、たとえば、復号化処理の回数が、記憶されている暗号化データの数よりも少ない場合には、すべての暗号化データは復号化されていないと判断されることになる。すべての暗号化データを復号化したと判断すると（ステップ S808 にて YES）、処理は、ステップ S812 に移される。そうでない場合には（ステップ S808 にて NO）、処理は、ステップ S1310 に移される。

【0190】

ステップ S1310 にて、CPU210 の鍵算出部 960 は、暗号化データと暗号鍵とに基づいて、次の暗号鍵を生成する。

【0191】

以上のような構造およびフローチャートに基づく、本発明の第 2 の実施の形態に係る暗号通信システムの動作について説明する。なお、前述の第 1 の実施の形態における動作と同じ動作の説明は、ここでは繰り返さない。

【0192】

〔暗号化処理〕

暗号装置 900 において、すべての平文データの暗号化が完了していない場合には（ス

10

20

30

40

50

テップ S 7 0 8 にて N O)、暗号装置 9 0 0 は、生成した暗号データと鍵とに基づいて、新たな暗号鍵を生成する (ステップ S 1 2 1 0)。その暗号鍵により次の入力ブロックを暗号化することにより暗号化データを生成する (ステップ S 7 0 6)。

【0193】

〔復号化処理〕

復号装置 9 5 0 が暗号装置 9 0 0 により生成された暗号データを受信すると、所定の復号化処理を実行する (ステップ S 8 0 2 ~ ステップ S 8 0 6)。すべての暗号化データの復号化処理が完了していない場合には (ステップ S 8 0 8 にて N O)、復号装置 9 5 0 は、暗号鍵と暗号化データとに基づいて、新たな暗号鍵を生成する (ステップ S 1 2 1 0)。復号装置 9 5 0 は、新たに生成した暗号鍵を使用して、その後の暗号化データの復号化処理を継続する (ステップ S 8 1 0, S 8 0 6)。

【0194】

以上のようにして、本実施の形態に係る暗号装置 9 0 0 は、暗号化データを生成するごとに、次の暗号鍵を生成して、次の入力ブロックを暗号化する。このようにすると、各ブロックは、それぞれに応じて生成される暗号鍵によって暗号化されるため、暗号化データのセキュリティレベルを向上させることができる。

【0195】

また、復号装置 9 5 0 は、同様にして、暗号化データごとに生成した暗号鍵を使用して復号化処理を実行するため、暗号化データを確実に抽出することができる。

【0196】

このようにして、通信データに付加するデータのサイズを増加させることなく、セキュリティレベルが向上する暗号通信システムを実現することができる。

【0197】

なお、上述の第 1 および第 2 の実施の形態においては、通信データである平文データの先頭ブロック内に乱数が付加されているが、付加されるデータは、乱数に限られない。たとえば、暗号装置において、暗号化処理を実行するごとに、値が 1 ずつ増加する値を付加してもよいし、通信データの送信先を識別するためのデータを付加してもよい。これにより、デジタルコンテンツの所有者情報を暗号化データに埋め込むことができるため、暗号化処理において不正があった場合等に、そのデータの所有者を特定することができる。

【0198】

なお、上述したように平文データに乱数を付加する方法に加えて、平文データのハッシュ値を付加するようにしてもよい。ハッシュ値とは、ハッシュ関数によって生成される値をいう。ハッシュ関数は、データを一定長のデータに要約するための関数をいう。ハッシュ関数を通じて出力される値から、元のデータを容易に推定することはできない。ハッシュ関数には、たとえば、S H A - 1 や M D 5 と呼ばれる関数が含まれる。

【0199】

このハッシュ値を平文データに付加することにより、復号装置は、暗号化データの復号化処理を実行した後、暗号装置が使用する関数と同じハッシュ関数を用いてハッシュ値を算出する。復号装置は、その値と復号化処理から得られる値とを比較することにより、復号結果が正しいことを確認することができる。このようにすると、たとえば、データの通信途中で、平文データが改竄されたり、正当な鍵とは異なる鍵によって復号化処理が行なわれたことを検出することができる。

【0200】

この方法では、同じコンテンツの場合、同一のハッシュ値が生成されるので、同じコンテンツを暗号化する場合、たとえば、ハッシュ値と乱数を組み合わせて用いることで、異なる暗号結果とすることができる。

【0201】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図され

10

20

30

40

50

る。

【図面の簡単な説明】

【0202】

【図1】本発明の第1の実施の形態に係る暗号装置および復号装置を含む暗号通信システムの構成を概念的に表わす図である。

【図2】本発明の第1の実施の形態に係る暗号装置および復号装置を実現するコンピュータの構成を表わすブロック図である。

【図3】本発明の第1の実施の形態に係る暗号装置に格納されるデータを説明するための図である。

【図4】本発明の第1の実施の形態に係る復号装置に格納されるデータを説明するための図である。 10

【図5】本発明の第1の実施の形態に係る暗号装置による暗号化処理を説明するための図である。

【図6】本発明の第1の実施の形態に係る暗号装置による暗号化処理を説明するための図である。

【図7】本発明の第1の実施の形態に係る暗号装置が実行する処理の手順を表わすフローチャートである。

【図8】本発明の第1の実施の形態に係る復号装置が実行する処理の手順を表わすフローチャートである。

【図9】本発明の第1の実施の形態の変形例に係る暗号装置による暗号化処理を説明するための図である。 20

【図10】本発明の第2の実施の形態に係る暗号装置および復号装置を含む暗号通信システムの構成を概念的に表わす図である。

【図11】本発明の第2の実施の形態に係る暗号装置による暗号化処理を説明するための図である。

【図12】本発明の第2の実施の形態に係る暗号装置が実行する処理の手順を表わすフローチャートである。

【図13】本発明の第2の実施の形態に係る復号装置が実行する処理の手順を表わすフローチャートである。

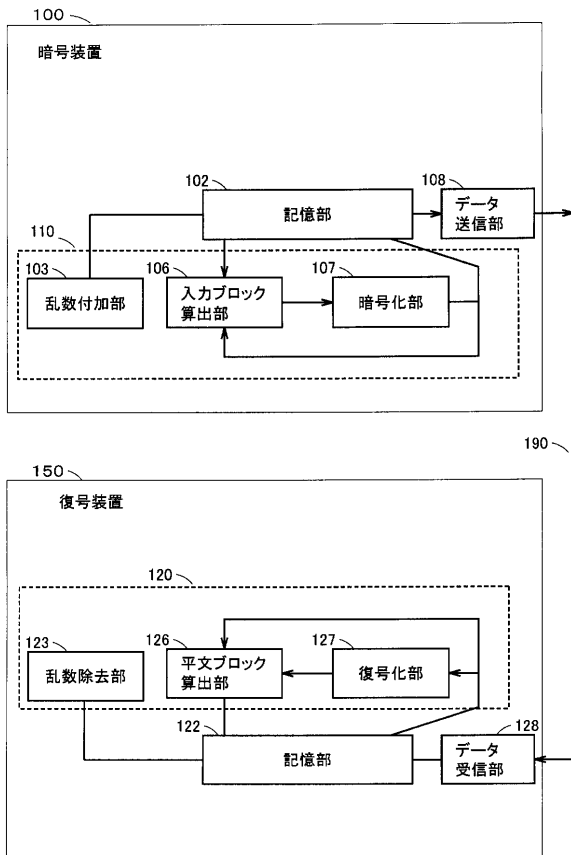
【符号の説明】

30

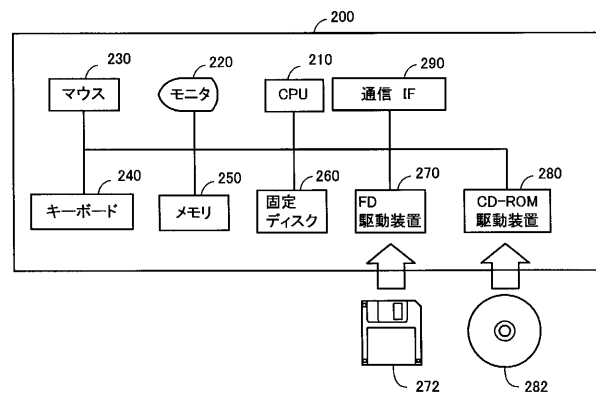
【0203】

100, 900 暗号装置、150, 950 復号装置、102, 122 記憶部、103 乱数付加部、106 入力ブロック算出部、107 暗号化部、108 データ送信部、110, 120, 210 CPU、123 乱数除去部、126 平文ブロック算出部、127 復号化部、128 データ受信部、190 通信回線、200 コンピュータ、220 モニタ、230 マウス、240 キーボード、250 メモリ、260 固定ディスク、270 FD駆動装置、272 FD、280 CD-ROM駆動装置、282 CD-ROM、910, 960 鍵算出部。

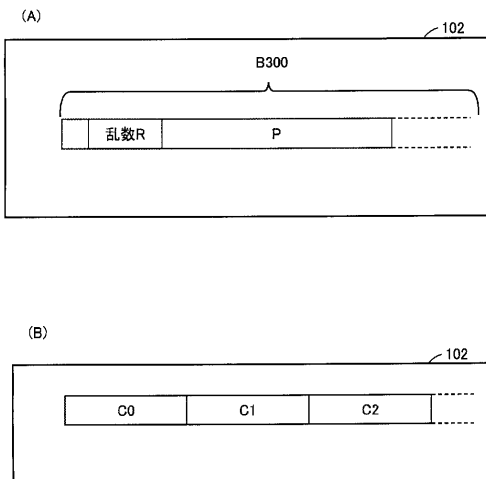
【図 1】



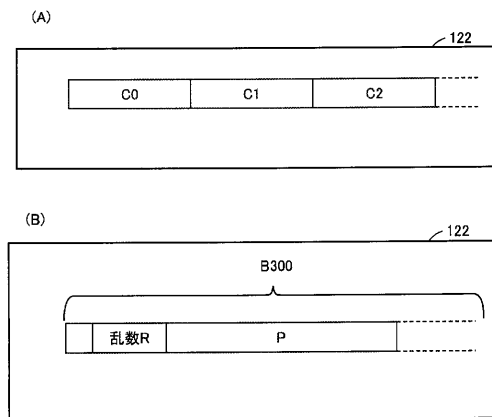
【図 2】



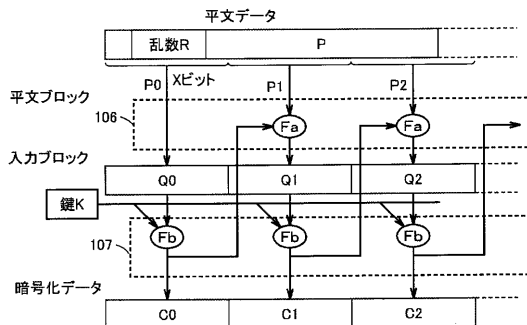
【図 3】



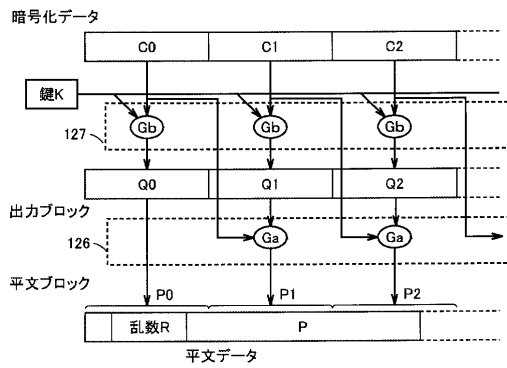
【図 4】



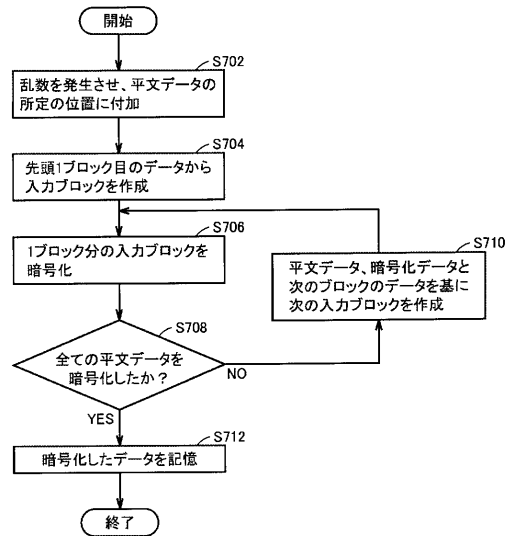
【図 5】



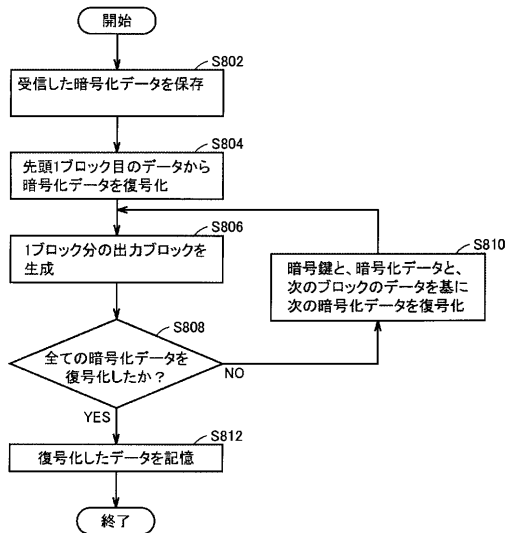
【図 6】



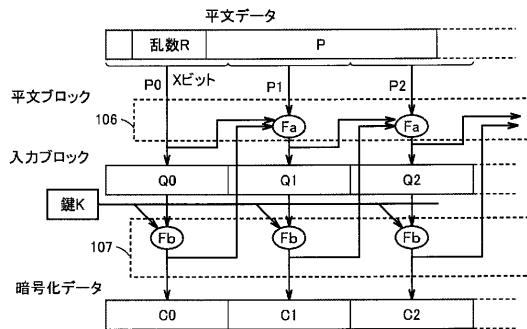
【図 7】



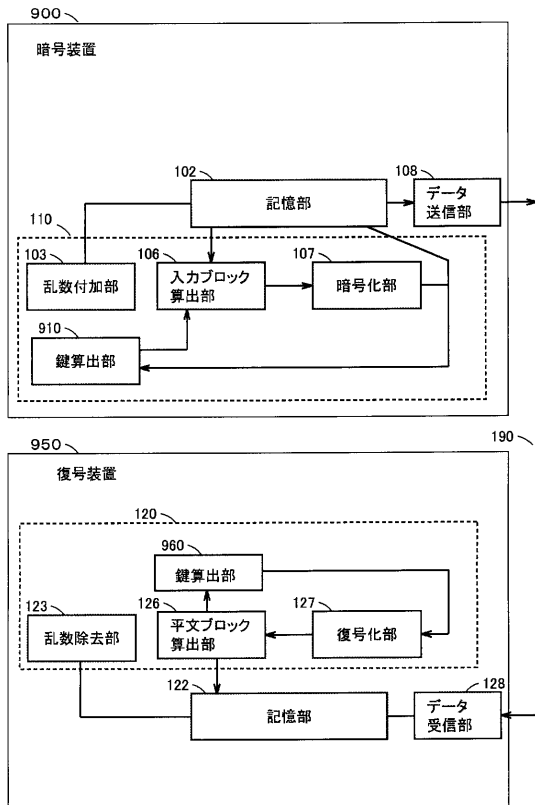
【図 8】



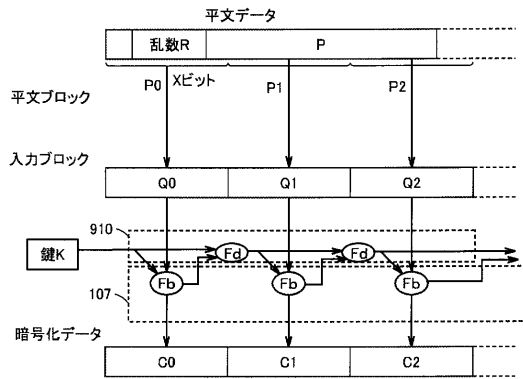
【図 9】



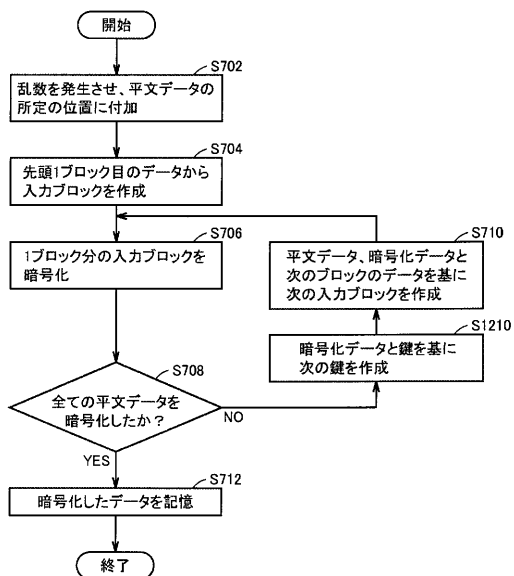
【図 10】



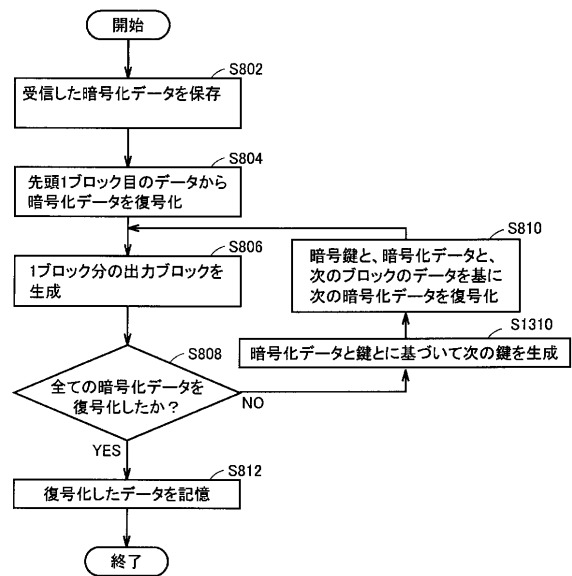
【図 11】



【図 12】



【図 13】



フロントページの続き

(72)発明者 佐藤 克彦

大阪府大阪市阿倍野区長池町2-2番2-2号 シャープ株式会社内

(72)発明者 名古 和行

大阪府大阪市阿倍野区長池町2-2番2-2号 シャープ株式会社内

Fターム(参考) 5J104 AA01 AA12 AA16 AA18 AA34 EA04 EA18 JA03 NA02 NA07
NA27 PA14