(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2007-13506
(P2007-13506A)
(43)公開日　平成19年1月18日(2007.1.18)

(51)Int.Cl.	F I		テーマコード（参考）
H04L 9/10 (2006.01)	H04L	9/00　621A	5J104

審査請求 未請求　請求項の数 57　ＯＬ　（全 56 頁）

(21)出願番号　特願2005-190803 (P2005-190803)
(22)出願日　平成17年6月29日 (2005.6.29)

(71)出願人　504148491
株式会社エヌクリプト
三重県四日市市中村町２２９３番地１
(74)代理人　100099324
弁理士　鈴木　正剛
(74)代理人　100108604
弁理士　村松　義人
(74)代理人　100111615
弁理士　佐野　良太
(72)発明者　中村　貴利
三重県四日市市中村町２２９３番地１　株式会社エヌクリプト内

Ｆターム(参考)　5J104 AA12 AA16 AA32 EA04 EA15 EA16 JA03 NA02 NA27 NA37 PA14

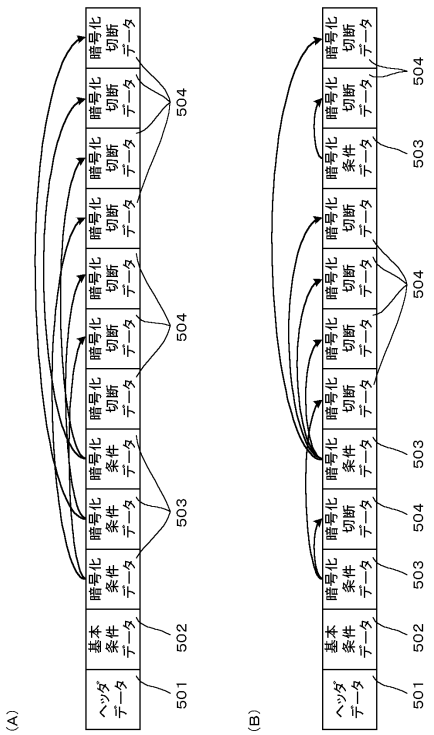
(54)【発明の名称】暗号化処理装置、暗号化方法、復号化処理装置、復号化方法、及びデータ構造

(57)【要約】

【課題】　復号化の条件を多様に設定して暗号化を行えるようにする。

【解決手段】　処理対象データを暗号化して得られる暗号化データは、ヘッダデータ５０１、基本条件データ５０２、暗号化条件データ５０３、暗号化切断データ５０４を有する。基本条件データ５０２は、暗号化条件データ５０３の復号化を許容又は禁止するための条件についてのデータを含んでいる。復号化処理装置では、基本条件データ５０２で復号化が認められた暗号化条件データのみが復号化されて条件データとされる。条件データは、暗号化切断データの復号化を許容又は禁止するための条件についてのデータを含んでいる。復号化処理装置では、条件データ５０３で復号化が認められた暗号化切断データ５０４のみが復号化される。

【選択図】　図４



【特許請求の範囲】
【請求項１】
平文である処理対象データを所定のビット数毎に切断して複数の平文切断データにする切断手段と、
複数の前記平文切断データを、所定の鍵、及び所定のアルゴリズムによって暗号化して複数の暗号化切断データとする暗号化手段と、
前記暗号化切断データのそれぞれの復号化を許容する場合の条件と、前記暗号化切断データのそれぞれの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む条件データを生成する条件データ生成手段と、
前記条件データを所定の鍵、及び所定のアルゴリズムによって暗号化して暗号化条件データとする条件データ暗号化手段と、
前記暗号化条件データの復号化を許容する場合の条件と、前記暗号化条件データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む基本条件データを生成する基本条件データ生成手段と、
複数の前記暗号化切断データと、前記暗号化条件データと、前記基本条件データとを一まとめにして、所定の復号化処理装置で復号化されることが予定された一連の暗号化データとする接続手段と、
を備えている暗号化処理装置であって、
前記接続手段は、前記暗号化切断データと、前記暗号化条件データと、前記基本条件データとを、前記暗号化条件データが、その暗号化条件データの元になった条件データに含まれた条件によりその復号化が許容又は禁止される暗号化切断データよりも前方に位置するようにしながら、且つ前記基本条件データが前記暗号化条件データよりも前方に位置するようにしながら一まとめにして一連の暗号化データとするようになっている、
暗号化処理装置。
【請求項２】
前記条件データ生成手段は、
以下の（１）～（３）の条件を充足するようにして前記条件データを複数生成するようになっているとともに、
（１）複数の前記条件データのそれぞれは、前記暗号化切断データのうちの少なくとも一つと対応付けられているとともに、その対応付けられた前記暗号化切断データの復号化を許容する場合の条件と、その対応付けられた前記暗号化切断データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む、
（２）複数の前記条件データは、前記暗号化切断データのすべてが複数の前記条件データのいずれかと対応付けられるようにされる、
（３）一つの前記暗号化切断データに複数の前記条件データが対応付けられることはない、
前記基本条件データ生成手段は、
複数の前記暗号化条件データのうちのどれの復号化を許容するのかという条件と、複数の前記暗号化条件データのうちのどれの復号化を禁止するのかという条件の少なくとも一方についてのデータを含む基本条件データを生成するようになっている、
請求項１記載の暗号化処理装置。
【請求項３】
前記条件データは、以下の（４）～（７）の少なくとも一つについてのデータを含んでいる、請求項１又は２記載の暗号化処理装置。
（４）前記暗号化切断データのうちの少なくとも一つについての復号化を行うことが許容又は禁止された復号化処理装置を特定するための情報
（５）前記暗号化切断データの少なくとも一つについての復号化を行うことが許容又は禁止されたユーザを特定するための情報
（６）前記暗号化切断データの少なくとも一つについての復号化が許容される期間に関する情報と、前記暗号化切断データの少なくとも一つについての復号化が禁止される期間に

関する情報の少なくとも一方
（７）複数の前記暗号化切断データのうちのどれの復号化を許容するかという情報、又は複数の前記暗号化切断データのうちのどれの復号化を禁止するかという情報
【請求項４】
前記暗号化手段が前記平文切断データを暗号化する際に用いられる鍵である複数の暗号化用鍵が保持された暗号化用鍵保持手段を備えており、
前記暗号化手段は、前記暗号化用鍵保持手段に保持された複数の暗号化用鍵のうちの少なくとも２つを用いて複数の前記平文切断データを、そのうちの少なくとも１つが他の前記平文切断データとは異なる暗号化用鍵で暗号化されるようにして暗号化切断データとするようになっており、
且つ、前記条件データ生成手段は、前記暗号化切断データのそれぞれが、前記暗号化用鍵保持手段に保持されている暗号化用鍵のうちのどれを用いて暗号化切断データとされたかということについてのデータを含む条件データを生成するようになっている、
請求項１記載の暗号化処理装置。
【請求項５】
前記条件データ生成手段は、前記条件データを複数生成するようになっているとともに、
前記条件データ暗号化手段が前記条件データを暗号化する際に用いられる鍵である複数の条件データ暗号化用鍵が保持された条件データ暗号化用鍵保持手段を備えており、
前記条件データ暗号化手段は、前記条件データ暗号化用鍵保持手段に保持された複数の条件データ暗号化用鍵のうちの少なくとも２つを用いて複数の前記条件データを、そのうちの少なくとも１つが他の条件データとは異なる条件データ暗号化用鍵で暗号化されるようにして暗号化条件データとするようになっており、
且つ、前記基本条件データ生成手段は、前記暗号化条件データのそれぞれが、前記条件データ鍵保持手段に保持されている条件データ暗号化用鍵のうちのどれを用いて暗号化条件データとされたかということについてのデータを含む基本条件データを生成するようになっている、
請求項１記載の暗号化処理装置。
【請求項６】
前記暗号化手段が前記平文切断データを暗号化する際に用いられる鍵である暗号化用鍵を所定のタイミングで生成する暗号化用鍵生成手段を備えており、
前記暗号化手段は、前記暗号化用鍵生成手段により生成された複数の暗号化用鍵を用いて複数の前記平文切断データを、そのうちの少なくとも１つが他の前記平文切断データとは異なる暗号化用鍵で暗号化されるようにして暗号化切断データとするようになっており、
且つ、前記条件データ生成手段は、前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータを含む条件データを生成するようになっている、
請求項１記載の暗号化処理装置。
【請求項７】
前記暗号化用鍵生成手段は、前記暗号化用鍵を、初期状態から順次前記暗号化用鍵を生成した場合に、同じ順番で生成された暗号化用鍵が常に同じものとなるようにして生成するようになっており、
且つ、前記条件データ生成手段が生成する前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータは、前記暗号化用鍵が生成された順番を示すものである、
請求項６記載の暗号化処理装置。
【請求項８】
擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用鍵用解生成手段を備えており、

前記暗号化用鍵生成手段は、前記暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記暗号化用鍵を生成するものとされており、
且つ、前記条件データ生成手段が生成する前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータは、前記暗号化用鍵が生成されたときに用いられた解を示すものである、
請求項７記載の暗号化処理装置。
【請求項９】
擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用鍵用解生成手段を備えており、
前記暗号化用鍵生成手段は、前記暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記暗号化用鍵を生成するものとされており、
且つ、前記条件データ生成手段が生成する前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータは、前記暗号化用鍵が生成されたときに用いられた解の生成された順番を示すものである、
請求項７記載の暗号化処理装置。
【請求項１０】
前記条件データ生成手段は、前記条件データを複数生成するようになっているとともに、
前記条件データ暗号化手段が前記条件データを暗号化する際に用いられる鍵である条件データ暗号化用鍵を所定のタイミングで生成する条件データ暗号化用鍵生成手段を備えており、
前記条件データ暗号化手段は、前記条件データ暗号化用鍵生成手段により生成された複数の条件データ暗号化用鍵を用いて複数の前記条件データを、そのうちの少なくとも１つが他の条件データとは異なる条件データ暗号化用鍵で暗号化されるようにして暗号化条件データとするようになっており、
且つ、前記基本条件データ生成手段は、前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータを含む基本条件データを生成するようになっている、
請求項１記載の暗号化処理装置。
【請求項１１】
前記条件データ暗号化用鍵生成手段は、前記条件データ暗号化用鍵を、初期状態から順次前記条件データ暗号化用鍵を生成した場合に、同じ順番で生成された条件データ暗号化用鍵が常に同じものとなるようにして生成するようになっており、
且つ、前記基本条件データ生成手段が生成する前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータは、前記条件データ暗号化用鍵が生成された順番を示すものである、
請求項１０記載の暗号化処理装置。
【請求項１２】
擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用鍵用解生成手段を備えており、
前記条件データ暗号化用鍵生成手段は、前記条件データ暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用鍵を生成するものとされており、
且つ、前記基本条件データ生成手段が生成する前記暗号化暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータは、前記条件データ暗号化用鍵が生成されたときに用いられた解を示すものである、
請求項１１記載の暗号化処理装置。
【請求項１３】
擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用鍵用解生成手段を備えており

、
前記条件データ暗号化用鍵生成手段は、前記条件データ暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用鍵を生成するものとされており、
且つ、前記基本条件データ生成手段が生成する前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータは、前記条件データ暗号化用鍵が生成されたときに用いられた解の生成された順番を示すものである、
請求項１１記載の暗号化処理装置。
【請求項１４】
前記暗号化手段が前記平文切断データを暗号化する際に用いられるアルゴリズムである複数の暗号化用アルゴリズムが保持された暗号化用アルゴリズム保持手段を備えており、
前記暗号化手段は、前記暗号化用アルゴリズム保持手段に保持された複数の暗号化用アルゴリズムのうちの少なくとも２つを用いて複数の前記平文切断データを、そのうちの少なくとも１つが他の前記平文切断データとは異なる暗号化用アルゴリズムで暗号化されるようにして暗号化切断データとするようになっており、
且つ、前記条件データ生成手段は、前記暗号化切断データのそれぞれが、前記暗号化用アルゴリズム保持手段に保持されている暗号化用アルゴリズムのうちのどれを用いて暗号化切断データとされたかということについてのデータを含む条件データを生成するようになっている、
請求項１記載の暗号化処理装置。
【請求項１５】
前記条件データ生成手段は、前記条件データを複数生成するようになっているとともに、
前記条件データ暗号化手段が前記条件データを暗号化する際に用いられるアルゴリズムである複数の条件データ暗号化用アルゴリズムが保持された条件データ暗号化用アルゴリズム保持手段を備えており、
前記条件データ暗号化手段は、前記条件データ暗号化用アルゴリズム保持手段に保持された複数の条件データ暗号化用アルゴリズムのうちの少なくとも２つを用いて複数の前記条件データを、そのうちの少なくとも１つが他の条件データとは異なる条件データ暗号化用アルゴリズムで暗号化されるようにして暗号化条件データとするようになっており、
且つ、前記基本条件データ生成手段は、前記暗号化条件データのそれぞれが、前記条件データ暗号化用アルゴリズム保持手段に保持されている条件データ暗号化用アルゴリズムのうちのどれを用いて暗号化条件データとされたかということについてのデータを含む条件データを生成するようになっている、
請求項１記載の暗号化処理装置。
【請求項１６】
前記暗号化手段が前記平文切断データを暗号化する際に用いられるアルゴリズムである暗号化用アルゴリズムを所定のタイミングで生成する暗号化用アルゴリズム生成手段を備えており、
前記暗号化手段は、前記暗号化用アルゴリズム生成手段により生成された複数の暗号化用アルゴリズムを用いて複数の前記平文切断データを、そのうちの少なくとも１つが他の前記平文切断データとは異なる暗号化用アルゴリズムで暗号化されるようにして暗号化切断データとするようになっており、
且つ、前記条件データ生成手段は、前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータを含む条件データを生成するようになっている、
請求項１記載の暗号化処理装置。
【請求項１７】
前記暗号化用アルゴリズム生成手段は、前記暗号化用アルゴリズムを、初期状態から順次前記暗号化用アルゴリズムを生成した場合に、同じ順番で生成された暗号化用アルゴリズムが常に同じものとなるようにして生成するようになっており、

且つ、前記条件データ生成手段が生成する前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータは、前記暗号化用アルゴリズムが生成された順番を示すものである、
請求項１６記載の暗号化処理装置。
【請求項１８】
擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用アルゴリズム用解生成手段を備えており、
前記暗号化用アルゴリズム生成手段は、前記暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記暗号化用アルゴリズムを生成するものとされており、
且つ、前記条件データ生成手段が生成する前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータは、前記暗号化用アルゴリズムが生成されたときに用いられた解を示すものである、
請求項１７記載の暗号化処理装置。
【請求項１９】
擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用アルゴリズム用解生成手段を備えており、
前記暗号化用アルゴリズム生成手段は、前記暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記暗号化用アルゴリズムを生成するものとされており、
且つ、前記条件データ生成手段が生成する前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータは、前記暗号化用アルゴリズムが生成されたときに用いられた解の生成された順番を示すものである、
請求項１７記載の暗号化処理装置。
【請求項２０】
前記条件データ生成手段は、前記条件データを複数生成するようになっているとともに、
前記条件データ暗号化手段が前記条件データを暗号化する際に用いられるアルゴリズムである条件データ暗号化用アルゴリズムを所定のタイミングで生成する条件データ暗号化用アルゴリズム生成手段を備えており、
前記条件データ暗号化手段は、前記条件データ暗号化用アルゴリズム生成手段により生成された複数の条件データ暗号化用アルゴリズムを用いて複数の前記条件データを、そのうちの少なくとも１つが他の条件データとは異なる条件データ暗号化用アルゴリズムで暗号化されるようにして暗号化条件データとするようになっており、
且つ、前記基本条件データ生成手段は、前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータを含む基本条件データを生成するようになっている、
請求項１記載の暗号化処理装置。
【請求項２１】
前記条件データ暗号化用アルゴリズム生成手段は、前記条件データ暗号化用アルゴリズムを、初期状態から順次前記条件データ暗号化用アルゴリズムを生成した場合に、同じ順番で生成された条件データ暗号化用アルゴリズムが常に同じものとなるようにして生成するようになっており、
且つ、前記基本条件データ生成手段が生成する前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータは、前記条件データ暗号化用アルゴリズムが生成された順番を示すものである、
請求項２０記載の暗号化処理装置。
【請求項２２】
擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用アルゴリズム用解生成手段を

備えており、
前記条件データ暗号化用アルゴリズム生成手段は、前記前記条件データ暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用アルゴリズムを生成するものとされており、
且つ、前記基本条件データ生成手段が生成する前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータは、前記条件データ暗号化用アルゴリズムが生成されたときに用いられた解を示すものである、
請求項２１記載の暗号化処理装置。
【請求項２３】
擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用アルゴリズム用解生成手段を備えており、
前記条件データ暗号化用アルゴリズム生成手段は、前記条件データ暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用アルゴリズムを生成するものとされており、
且つ、前記基本条件データ生成手段が生成する前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータは、前記条件データ暗号化用アルゴリズムが生成されたときに用いられた解の生成された順番を示すものである、
請求項２１記載の暗号化処理装置。
【請求項２４】
暗号化処理装置にて実行される方法であって、
当該暗号化処理装置が、
平文である処理対象データを所定のビット数毎に切断して複数の平文切断データにする過程、
複数の前記平文切断データを、所定の鍵、及び所定のアルゴリズムによって暗号化して複数の暗号化切断データとする過程、
前記暗号化切断データのそれぞれの復号化を許容する場合の条件と、前記暗号化切断データのそれぞれの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む条件データを生成する過程、
前記条件データを所定の鍵、及び所定のアルゴリズムによって暗号化して暗号化条件データとする過程、
前記暗号化条件データの復号化を許容する場合の条件と、前記暗号化条件データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む基本条件データを生成する過程、
複数の前記暗号化切断データと、前記暗号化条件データと、前記基本条件データとを一まとめにして、所定の復号化処理装置で復号化されることが予定された一連の暗号化データとする過程、
を実行し、
前記暗号化処理装置は、複数の前記暗号化切断データと、前記暗号化条件データと、前記基本条件データとを一まとめにして、所定の復号化処理装置で復号化されることが予定された一連の暗号化データとする過程では、
前記暗号化切断データと、前記暗号化条件データと、前記基本条件データとを、前記暗号化条件データが、その暗号化条件データの元になった条件データに含まれた条件によりその復号化が許容又は禁止される暗号化切断データよりも前方に位置するようにしながら、且つ前記基本条件データが前記暗号化条件データよりも前方に位置するようにしながら一まとめにして一連の暗号化データとする、
暗号化方法。
【請求項２５】
平文である処理対象データを所定のビット数毎に切断して得られた複数の平文切断デー

タを、所定の鍵、及び所定のアルゴリズムによって暗号化して得られた複数の暗号化切断データと、
前記暗号化切断データのそれぞれの復号化を許容する場合の条件と、前記暗号化切断データのそれぞれの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む条件データを所定の鍵、及び所定のアルゴリズムによって暗号化して得られた暗号化条件データと、
前記暗号化条件データの復号化を許容する場合の条件と、前記暗号化条件データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む基本条件データと、
を、一まとめにして一連とした、所定の復号化処理装置で復号化されることが予定された暗号化データのデータ構造であって、
前記暗号化切断データと、前記暗号化条件データと、前記基本条件データとは、前記暗号化条件データが、その暗号化条件データの元になった条件データに含まれた条件によりその復号化が許容又は禁止される暗号化切断データよりも前方に位置するようにしながら、且つ前記基本条件データが前記暗号化条件データよりも前方に位置するようになっている、
暗号化データのデータ構造。
【請求項２６】
前記条件データは複数であり、且つ以下の（１）～（３）の条件を充足するようになっているとともに、
（１）複数の前記条件データのそれぞれは、前記暗号化切断データのうちの少なくとも一つと対応付けられているとともに、その対応付けられた前記暗号化切断データの復号化を許容する場合の条件と、その対応付けられた前記暗号化切断データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む、
（２）複数の前記条件データは、前記暗号化切断データのすべてが複数の前記条件データのいずれかと対応付けられるようにされる、
（３）一つの前記暗号化切断データに複数の前記条件データが対応付けられることはない、
前記基本条件データは、
複数の前記暗号化条件データのうちのどれの復号化を許容するのかという条件と、複数の前記暗号化条件データのうちのどれの復号化を禁止するのかという条件の少なくとも一方についてのデータを含むようになっている、
請求項２５記載の暗号化データのデータ構造。
【請求項２７】
前記条件データは、以下の（４）～（７）の少なくとも一つについてのデータを含んでいる、請求項２５又は２６記載の暗号化データのデータ構造。
（４）前記暗号化切断データのうちの少なくとも一つについての復号化を行うことが許容又は禁止された復号化処理装置を特定するための情報
（５）前記暗号化切断データの少なくとも一つについての復号化を行うことが許容又は禁止されたユーザを特定するための情報
（６）前記暗号化切断データの少なくとも一つについての復号化が許容される期間に関する情報と、前記暗号化切断データの少なくとも一つについての復号化が禁止される期間に関する情報の少なくとも一方
（７）複数の前記暗号化切断データのうちのどれの復号化を許容するかという情報、又は複数の前記暗号化切断データのうちのどれの復号化を禁止するかという情報
【請求項２８】
前記暗号化切断データのそれぞれは、複数の暗号化用鍵の１つを用いて、且つ複数の前記平文切断データの少なくとも１つが他の平文切断データとは異なる暗号化用鍵で暗号化されるようにして暗号化されたものであり、
且つ、前記条件データは、前記暗号化切断データのそれぞれが、複数の前記暗号化用鍵のうちのどれを用いて暗号化切断データとされたかということについてのデータを含むも

のとされている、
請求項２５記載の暗号化データのデータ構造。
【請求項２９】
前記条件データは複数であり、
前記暗号化条件データのそれぞれは、複数の条件データ暗号化用鍵の１つを用いて、且つ複数の前記条件データの少なくとも１つが他の条件データとは異なる条件データ暗号化用鍵で暗号化されるようにして暗号化されたものであり、
且つ、前記基本条件データは、前記暗号化条件データのそれぞれが、複数の前記条件データ暗号化用鍵のうちのどれを用いて暗号化条件データとされたかということについてのデータを含むものとされている、
請求項２５記載の暗号化データのデータ構造。
【請求項３０】
前記暗号化データは、複数の暗号化用鍵を所定のタイミングで生成する暗号化用鍵生成手段を備える暗号化処理装置で生成されるものであり、
前記暗号化切断データのそれぞれは、前記暗号化用鍵生成手段が生成した複数の暗号化用鍵の１つを用いて、且つ複数の前記平文切断データの少なくとも１つが他の平文切断データとは異なる暗号化用鍵で暗号化されるようにして暗号化されたものであり、
且つ、前記条件データは、前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータを含むものとされている、
請求項２５記載の暗号化データのデータ構造。
【請求項３１】
前記暗号化用鍵生成手段は、前記暗号化用鍵を、初期状態から順次前記暗号化用鍵を生成した場合に、同じ順番で生成された暗号化用鍵が常に同じものとなるようにして生成するようになっており、
且つ、前記条件データに含まれる前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータは、前記暗号化用鍵が生成された順番を示すものとされている、
請求項３０記載の暗号化データのデータ構造。
【請求項３２】
前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用鍵用解生成手段を備える暗号化処理装置で生成されるものであり、
前記暗号化用鍵生成手段は、前記暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記暗号化用鍵を生成するものとされており、
且つ、前記条件データに含まれる前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータは、前記暗号化用鍵が生成されたときに用いられた解を示すものである、
請求項３１記載の暗号化データのデータ構造。
【請求項３３】
前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用鍵用解生成手段を備える暗号化処理装置で生成されるものであり、
前記暗号化用鍵生成手段は、前記暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記暗号化用鍵を生成するものとされており、
且つ、前記条件データに含まれる前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータは、前記暗号化用鍵が生成されたときに用いられた解の生成された順番を示すものである、
請求項３１記載の暗号化データのデータ構造。
【請求項３４】
前記条件データは複数であり、

前記暗号化条件データは、複数の条件データ暗号化用鍵を所定のタイミングで生成する条件データ暗号化用鍵生成手段を備える暗号化処理装置で生成されるものであり、
前記暗号化条件データのそれぞれは、前記条件データ暗号化用鍵生成手段が生成した複数の条件データ暗号化用鍵の１つを用いて、且つ複数の前記条件データの少なくとも１つが他の条件データとは異なる条件データ暗号化用鍵で暗号化されるようにして暗号化されたものであり、
且つ、前記基本条件データは、前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータを含むものとされている、
請求項２５記載の暗号化データのデータ構造。
【請求項３５】
前記条件データ暗号化用鍵生成手段は、前記条件データ暗号化用鍵を、初期状態から順次前記条件データ暗号化用鍵を生成した場合に、同じ順番で生成された条件データ暗号化用鍵が常に同じものとなるようにして生成するようになっており、
且つ、前記基本条件データに含まれる前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータは、前記条件データ暗号化用鍵が生成された順番を示すものとされている、
請求項３４記載の暗号化データのデータ構造。
【請求項３６】
前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用鍵用解生成手段を備える暗号化処理装置で生成されるものであり、
前記条件データ暗号化用鍵生成手段は、前記条件データ暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用鍵を生成するものとされており、
且つ、前記基本条件データに含まれる前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータは、前記条件データ暗号化用鍵生成されたときに用いられた解を示すものである、
請求項３５記載の暗号化データのデータ構造。
【請求項３７】
前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用鍵用解生成手段を備える暗号化処理装置で生成されるものであり、
前記条件データ暗号化用鍵生成手段は、前記条件データ暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用鍵を生成するものとされており、
且つ、前記基本条件データに含まれる前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータは、前記条件データ暗号化用鍵が生成されたときに用いられた解の生成された順番を示すものである、
請求項３６記載の暗号化データのデータ構造。
【請求項３８】
前記暗号化切断データのそれぞれは、複数の暗号化用アルゴリズムの１つを用いて、且つ複数の前記平文切断データの少なくとも１つが他の平文切断データとは異なる暗号化用アルゴリズムで暗号化されるようにして暗号化されたものであり、
且つ、前記条件データは、前記暗号化切断データのそれぞれが、複数の前記暗号化用アルゴリズムのうちのどれを用いて暗号化切断データとされたかということについてのデータを含むものとされている、
請求項２５記載の暗号化データのデータ構造。
【請求項３９】
前記条件データは複数であり、
前記暗号化条件データのそれぞれは、複数の条件データ暗号化用アルゴリズムの１つを用いて、且つ複数の前記条件データの少なくとも１つが他の条件データとは異なる条件データ暗号化用アルゴリズムで暗号化されるようにして暗号化されたものであり、

且つ、前記基本条件データは、前記暗号化条件データのそれぞれが、複数の前記条件データ暗号化用アルゴリズムのうちのどれを用いて暗号化条件データとされたかということについてのデータを含むものとされている、
請求項２５記載の暗号化データのデータ構造。
【請求項４０】
前記暗号化データは、前記暗号化データは、複数の暗号化用アルゴリズムを所定のタイミングで生成する暗号化用アルゴリズム生成手段を備える暗号化処理装置で生成されるものであり、
前記暗号化切断データのそれぞれは、前記暗号化用アルゴリズム生成手段が生成した複数の暗号化用アルゴリズムの１つを用いて、且つ複数の前記平文切断データの少なくとも１つが他の平文切断データとは異なる暗号化用アルゴリズムで暗号化されるようにして暗号化されたものであり、
且つ、前記条件データは、前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータを含むものとされている、
請求項２５記載の暗号化データのデータ構造。
【請求項４１】
前記暗号化用アルゴリズム生成手段は、前記暗号化用アルゴリズムを、初期状態から順次前記暗号化用アルゴリズムを生成した場合に、同じ順番で生成された暗号化用アルゴリズムが常に同じものとなるようにして生成するようになっており、
且つ、前記条件データに含まれる前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータは、前記暗号化用アルゴリズムが生成された順番を示すものとされている、
請求項４０記載の暗号化データのデータ構造。
【請求項４２】
前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用アルゴリズム用解生成手段を備える暗号化処理装置で生成されるものであり、
前記暗号化用アルゴリズム生成手段は、前記暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記暗号化用アルゴリズムを生成するものとされており、
且つ、前記条件データに含まれる前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータは、前記暗号化用アルゴリズムが生成されたときに用いられた解を示すものである、
請求項４１記載の暗号化データのデータ構造。
【請求項４３】
前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用アルゴリズム用解生成手段を備える暗号化処理装置で生成されるものであり、
前記暗号化用アルゴリズム生成手段は、前記暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記暗号化用アルゴリズムを生成するものとされており、
且つ、前記条件データに含まれる前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータは、前記暗号化用アルゴリズムが生成されたときに用いられた解の生成された順番を示すものである、
請求項４１記載の暗号化データのデータ構造。
【請求項４４】
前記条件データは複数であり、
前記暗号化条件データは、複数の条件データ暗号化用アルゴリズムを所定のタイミングで生成する条件データ暗号化用アルゴリズム生成手段を備える暗号化処理装置で生成されるものであり、
前記暗号化条件データのそれぞれは、前記条件データ暗号化用アルゴリズム生成手段が生成した複数の条件データ暗号化用アルゴリズムの１つを用いて、且つ複数の前記条件デ

ータの少なくとも１つが他の条件データとは異なる条件データ暗号化用アルゴリズムで暗号化されるようにして暗号化されたものであり、
　且つ、前記基本条件データは、前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータを含むものとされている、
　請求項２５記載の暗号化データのデータ構造。
【請求項４５】
　前記条件データ暗号化用アルゴリズム生成手段は、前記条件データ暗号化用アルゴリズムを、初期状態から順次前記条件データ暗号化用アルゴリズムを生成した場合に、同じ順番で生成された条件データ暗号化用アルゴリズムが常に同じものとなるようにして生成するようになっており、
　且つ、前記基本条件データに含まれる前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータは、前記条件データ暗号化用アルゴリズムが生成された順番を示すものとされている、
　請求項４４記載の暗号化データのデータ構造。
【請求項４６】
　前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用アルゴリズム用解生成手段を備える暗号化処理装置で生成されるものであり、
　前記条件データ暗号化用アルゴリズム生成手段は、前記条件データ暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用アルゴリズムを生成するものとされており、
　且つ、前記基本条件データに含まれる前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータは、前記条件データ暗号化用アルゴリズムが生成されたときに用いられた解を示すものである、
　請求項４５記載の暗号化データのデータ構造。
【請求項４７】
　前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用アルゴリズム用解生成手段を備える暗号化処理装置で生成されるものであり、
　前記条件データ暗号化用アルゴリズム生成手段は、前記条件データ暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用アルゴリズムを生成するものとされており、
　且つ、前記基本条件データに含まれる前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータは、前記条件データ暗号化用アルゴリズムが生成されたときに用いられた解の生成された順番を示すものである、
　請求項４５記載の暗号化データのデータ構造。
【請求項４８】
　請求項２５記載の暗号化データを復号化するものであり、
　前記暗号化データから基本条件データを読出す基本条件データ読出し手段、
　前記暗号化データから前記暗号化条件データを読出す暗号化条件データ読出し手段、
　前記暗号化データから前記暗号化切断データを読出す暗号化切断データ読出し手段、
　前記暗号化条件データ読出し手段によって読出した前記暗号化条件データが、前記基本条件データ読出し手段が読出した前記基本条件データに示された暗号化条件データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化条件データが復号化を禁止される場合の条件に合致しないと判断した場合に前記暗号化条件データを復号化して条件データにする暗号化条件データ復号化手段、
　前記暗号化切断データ読出し手段によって読出した暗号化切断データのそれぞれを、前記暗号化条件データ復号化手段によって復号化された条件データに示された暗号化切断デ

ータが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化切断データが復号化を禁止される場合の条件に合致しないと判断した場合にのみ復号化して平文切断データにする復号化手段、
前記復号化手段によって復号化された平文切断データを一まとめにして処理対象データとする接続手段、
を備えている、
復号化処理装置。
【請求項４９】
請求項２６記載の暗号化データを復号化するものであり、
前記暗号化データから基本条件データを読出す基本条件データ読出し手段、
前記暗号化データから前記暗号化条件データを読出す暗号化条件データ読出し手段、
前記暗号化データから前記暗号化切断データを読出す暗号化切断データ読出し手段、
前記暗号化条件データ読出し手段によって読出した前記暗号化条件データが、前記基本条件データ読出し手段が読出した前記基本条件データに示された暗号化条件データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化条件データが復号化を禁止される場合の条件に合致しないと判断した場合に前記暗号化条件データを復号化して条件データにする暗号化条件データ復号化手段、
前記暗号化切断データ読出し手段によって読出した暗号化切断データのそれぞれが、前記暗号化条件データ復号化手段によって復号化された条件データに示された暗号化切断データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化切断データが復号化を禁止される場合の条件に合致しないと判断した場合にのみ、その暗号化切断データを復号化して平文切断データにする復号化手段、
前記復号化手段によって復号化された平文切断データを一まとめにして処理対象データとする接続手段、
を備えており、
前記暗号化条件データ復号化手段は、
前記暗号化条件データ読出し手段によって読出した暗号化条件データのそれぞれが、複数の前記暗号化条件データのうちのどれの復号化を許容するのかという条件に合致すると判断した場合、又は複数の前記暗号化条件データのうちのどれの復号化を禁止するのかという条件に合致しなかった場合にのみ、その暗号化条件データを復号化して条件データにするようにされており、
前記復号化手段は、
復号化された条件データのみに基づいて、前記暗号化切断データを復号化して前記平文切断データにする処理を行う、
復号化処理装置。
【請求項５０】
請求項２５記載の暗号化データを復号化する復号化処理装置で実行される方法であって、
前記復号化処理装置が、
前記暗号化データから基本条件データを読出す過程、
前記暗号化データから前記暗号化条件データを読出す過程、
前記暗号化データから前記暗号化切断データを読出す過程、
読出した暗号化条件データが、読出した前記基本条件データに示された暗号化条件データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化条件データが復号化を禁止される場合の条件に合致しないと判断した場合に前記暗号化条件データを復号化して条件データにする過程、
読出した暗号化切断データのそれぞれを、復号化された条件データに示された暗号化切断データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化切断データが復号化を禁止される場合の条件に合致しないと判断した場合にのみ復号化して平文切断データにする過程、

前記復号化手段によって復号化された平文切断データを一まとめにして処理対象データとする過程、
を含む復号化方法。
【請求項５１】
請求項２６記載の暗号化データを復号化する復号化処理装置で実行される方法であって、
前記暗号化データから基本条件データを読出す過程、
前記暗号化データから前記暗号化条件データを読出す過程、
前記暗号化データから前記暗号化切断データを読出す過程、
読出した前記暗号化条件データが、前記基本条件データ読出し手段が読出した前記基本条件データに示された暗号化条件データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化条件データが復号化を禁止される場合の条件に合致しないと判断した場合に前記暗号化条件データを復号化して条件データにする過程、
前記暗号化切断データ読出し手段によって読出した暗号化切断データのそれぞれが、復号化された条件データに示された暗号化切断データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化切断データが復号化を禁止される場合の条件に合致しないと判断した場合にのみ、その暗号化切断データを復号化して平文切断データにする過程、
復号化された平文切断データを一まとめにして処理対象データとする過程、
を含み、
前記暗号化条件データを復号化して条件データにする前記過程では、読出した暗号化条件データのそれぞれが、複数の前記暗号化条件データのうちのどれの復号化を許容するのかという条件に合致すると判断した場合、又は複数の前記暗号化条件データのうちのどれの復号化を禁止するのかという条件に合致しなかった場合にのみ、その暗号化条件データを復号化して条件データにし、
暗号化切断データを復号化して平文切断データにする前記過程では、復号化された条件データのみに基づいて、前記暗号化切断データを復号化して前記平文切断データにする処理を行う、
復号化方法。
【請求項５２】
前記条件データ生成手段は、前記条件データを複数生成するようになっているとともに、前記条件データの少なくとも一つに、他の条件データを暗号化して生成された暗号化条件データの復号化を許容する場合の条件についてのデータを含めるようになっている、
請求項１記載の暗号化処理装置。
【請求項５３】
前記条件データ生成手段は、
前記条件データを複数生成するようになっているとともに、
複数の前記条件データのうちの少なくとも幾つかを、それら幾つかの条件データを暗号化して生成された暗号化条件データの復号化が所定の順番で行われるように関連付けられており、且つそれら幾つかの条件データには、その条件データを暗号化して生成された暗号化条件データの次に復号化される暗号化条件データを復号化するための条件についてのデータが含まれるようにして生成するようになっている、
請求項１記載の暗号化処理装置。
【請求項５４】
前記基本条件データ生成手段は、前記幾つかの条件データのうち、それらを暗号化して生成された暗号化条件データのうち最初に復号化されるものの復号化を許容する場合の条件を含んでいる、
請求項５３記載の暗号化処理装置。
【請求項５５】
前記条件データは複数であり、且つ前記条件データの少なくとも一つには、他の条件デ

ータを暗号化して生成された暗号化条件データの復号化を許容する場合の条件についてのデータが含められている、
請求項２５記載の暗号化データのデータ構造。
【請求項５６】
前記条件データは複数であり、且つ複数の前記条件データのうちの少なくとも幾つかは、それら幾つかの条件データを暗号化して生成された暗号化条件データの復号化が所定の順番で行われるように関連付けられており、且つそれら幾つかの条件データのそれぞれには、その条件データを暗号化して生成された暗号化条件データの次に復号化される暗号化条件データを復号化するための条件についてのデータが含まれている、
請求項２５記載の暗号化データのデータ構造。
【請求項５７】
前記基本条件データは、前記幾つかの条件データのうち、それらを暗号化して生成された暗号化条件データのうち最初に復号化されるものの復号化を許容する場合の条件を含んでいる、
請求項５６記載の暗号化データのデータ構造。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、平文である処理対象データを暗号化し暗号化データとする暗号化技術、及び暗号化データを復号化する復号化技術に関する。
【背景技術】
【０００２】
情報に関するセキュリティの重要性が益々高まる現在、正当と認められない第三者にその内容を知られるのが好ましくないデータ（この明細書では、これを「処理対象データ」と呼ぶ。）を暗号化して暗号化データにする暗号化技術についての様々な研究がなされている。
【０００３】
ところで、暗号化データは、復号化処理装置を兼ねるその暗号化データの暗号化を行った暗号化処理装置で復号化される場合もあるが、第三者に引渡されることが多い。その第三者は、所定の鍵とアルゴリズムを用いて受取った暗号化データを復号化して元の処理対象データに戻し、その処理対象データを適宜利用する。
【０００４】
ところで、例えば、同一の暗号化データを複数人に渡す場合に、その複数人のそれぞれに暗号化データの異なる部分の復号化を許容できれば便利である。
また、ある暗号化データの復号化を、特定の条件下、例えば期間限定で認められれば便利である。例えば、近年の個人情報保護の高まりを鑑みれば、暗号化された暗号化データだからといって、いつまでも復号化可能な状態でどこかに存在しつづけるというのは、あまり好ましいことではない。また、上述の如き期間限定での暗号化データの復号化を許容する場合、期間を複数に分け、この期間であれば暗号化データのこの部分の復号化を許容する、また、他の期間であれば暗号化データの他の部分の復号化を許容するといったきめ細かな制限をかけられれば、非常に便利である。
【０００５】
しかしながら、このようなことを可能とする、復号化の条件を多様に設定する暗号化技術は存在しない。
【発明の開示】
【発明が解決しようとする課題】
【０００６】
本発明は、処理対象データの暗号化によって生成された暗号化データの復号化の条件を多様に設定することのできる暗号化技術、その暗号化技術により暗号化された暗号化データのデータ構造、及びその暗号化データの復号化技術を提供することをその課題とする。

【課題を解決するための手段】
【０００７】
かかる課題を解決するため、本願発明者は、以下に説明する発明を提案する。
【０００８】
本願発明は、平文である処理対象データを所定のビット数毎に切断して複数の平文切断データにする切断手段と、複数の前記平文切断データを、所定の鍵、及び所定のアルゴリズムによって暗号化して複数の暗号化切断データとする暗号化手段と、前記暗号化切断データのそれぞれの復号化を許容する場合の条件と、前記暗号化切断データのそれぞれの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む条件データを生成する条件データ生成手段と、前記条件データを所定の鍵、及び所定のアルゴリズムによって暗号化して暗号化条件データとする条件データ暗号化手段と、前記暗号化条件データの復号化を許容する場合の条件と、前記暗号化条件データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む基本条件データを生成する基本条件データ生成手段と、複数の前記暗号化切断データと、前記暗号化条件データと、前記基本条件データとを一まとめにして、所定の復号化処理装置で復号化されることが予定された一連の暗号化データとする接続手段と、を備えている暗号化処理装置である。
そして、前記接続手段は、前記暗号化切断データと、前記暗号化条件データと、前記基本条件データとを、前記暗号化条件データが、その暗号化条件データの元になった条件データに含まれた条件によりその復号化が許容又は禁止される暗号化切断データよりも前方に位置するようにしながら、且つ前記基本条件データが前記暗号化条件データよりも前方に位置するようにしながら一まとめにして一連の暗号化データとするようになっている。
この暗号化処理装置は、処理対象データを切断して生成した複数の平文切断データのそれぞれを暗号化することにより複数の暗号化切断データを生成し、それを一まとめにして暗号化データとするという、一般的な暗号化処理装置をその基本としている。そして、この暗号化処理装置は、暗号化切断データのそれぞれの復号化を許容する場合の条件と、暗号化切断データのそれぞれの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む条件データを生成する条件データ生成手段を備えており、その条件データをも暗号化して暗号化条件データとし、それを暗号化データの一部に加えるものとしている。したがって、この暗号化処理装置で生成された暗号化データは、上述の条件データにより、暗号化データの少なくとも一部（少なくとも複数の暗号化切断データのうちの一部）を他の部分とは異なる条件で復号化できるな条件設定を行えるようになる。これにより、この暗号化処理装置は、処理対象データの暗号化によって生成された暗号化データの復号化の条件を多様に設定することのできるものとなる。
なお、上述したように、この暗号化処理装置は、条件データも暗号化して暗号化条件データとすることとしている。したがって、どのような条件で暗号化切断データのそれぞれを復号化できるのかということは、予定された者以外は知ることができない。したがって、この暗号化処理装置によって作られた暗号化データは、安全性が高い。
この暗号化処理装置は、暗号化条件データの復号化を許容する場合の条件と、暗号化条件データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む基本条件データを生成する基本条件データ生成手段を備えており、基本条件データ生成手段が生成した基本条件データを暗号化データに含めることとしている。暗号化データの復号化を行う者は、この基本条件データにより、上述の暗号化条件データの復号化が行えることになる。
なお、この暗号化処理装置は、前記暗号化切断データと、前記暗号化条件データと、前記基本条件データとを、前記暗号化条件データが、その暗号化条件データの元になった条件データに含まれた条件によりその復号化が許容又は禁止される暗号化切断データよりも前方に位置するようにしながら、且つ前記基本条件データが前記暗号化条件データよりも前方に位置するようにしながら一まとめにして一連の暗号化データとするようになっている。暗号化条件データが、その暗号化条件データの元になった条件データに含まれた条件によりその復号化が許容又は禁止される暗号化切断データよりも前方に位置するようにす

るのは、復号化処理装置で暗号化データが復号化される際に、暗号化データは先頭から読込まれるのであるが、暗号化データを復号化するには条件データが必要となるので、その条件データを生成するための暗号化条件データを先に読込む必要があるからである。基本条件データが暗号化条件データよりも前方に位置するようにするのも同様の理由からである。

【０００９】

この暗号化処理装置が有する作用効果と同様の作用効果を、例えば以下の方法によっても得ることができる。

暗号化処理装置にて実行される方法であって、当該暗号化処理装置が、平文である処理対象データを所定のビット数毎に切断して複数の平文切断データにする過程、複数の前記平文切断データを、所定の鍵、及び所定のアルゴリズムによって暗号化して複数の暗号化切断データとする過程、前記暗号化切断データのそれぞれの復号化を許容する場合の条件と、前記暗号化切断データのそれぞれの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む条件データを生成する過程、前記条件データを所定の鍵、及び所定のアルゴリズムによって暗号化して暗号化条件データとする過程、前記暗号化条件データの復号化を許容する場合の条件と、前記暗号化条件データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む基本条件データを生成する過程、複数の前記暗号化切断データと、前記暗号化条件データと、前記基本条件データとを一まとめにして、所定の復号化処理装置で復号化されることが予定された一連の暗号化データとする過程、を実行し、前記暗号化処理装置は、複数の前記暗号化切断データと、前記暗号化条件データと、前記基本条件データとを一まとめにして、所定の復号化処理装置で復号化されることが予定された一連の暗号化データとする過程では、前記暗号化切断データと、前記暗号化条件データと、前記基本条件データとを、前記暗号化条件データが、その暗号化条件データの元になった条件データに含まれた条件によりその復号化が許容又は禁止される暗号化切断データよりも前方に位置するようにしながら、且つ前記基本条件データが前記暗号化条件データよりも前方に位置するようにしながら一まとめにして一連の暗号化データとする、暗号化方法である。

【００１０】

前記条件データ生成手段は、条件データを一つだけ生成してもよいし、複数生成してもよい。前者の場合、暗号化条件データは一つとなり、後者の場合、暗号化条件データは複数となる。

前記条件データ生成手段は、例えば、以下の（１）～（３）の条件を充足するようにして前記条件データを複数生成するようになっていてもよい。

（１）複数の前記条件データのそれぞれは、前記暗号化切断データのうちの少なくとも一つと対応付けられているとともに、その対応付けられた前記暗号化切断データの復号化を許容する場合の条件と、その対応付けられた前記暗号化切断データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む、

（２）複数の前記条件データは、前記暗号化切断データのすべてが複数の前記条件データのいずれかと対応付けられるようにされる、

（３）一つの前記暗号化切断データに複数の前記条件データが対応付けられることはない。

この場合、基本条件データ生成手段は、複数の前記暗号化条件データのうちのどれの復号化を許容するのかという条件と、複数の前記暗号化条件データのうちのどれの復号化を禁止するのかという条件の少なくとも一方についてのデータを含む基本条件データを生成するようになっている。

このようにすることで、暗号化切断データのどれの復号化を許容するのかということの前提となる条件データの元となる暗号化条件データの復号化についての設定をきめ細かく行えるようになる。

この場合、各暗号化条件データは、各暗号化条件データの元となった条件データと対応付けられた平文切断データを暗号化して作られた暗号化切断データよりも前方に位置する

ようにされる。なお、暗号化条件データは、場合によっては、暗号化切断データよりも後方に位置する場合がある。

【００１１】

上述したように、条件データ生成手段は、前記条件データを複数生成するようになっている場合がある。この場合、前記条件データ生成手段は、前記条件データの少なくとも一つに、他の条件データを暗号化して生成された暗号化条件データの復号化を許容する場合の条件についてのデータを含めるようになっていてもよい。

条件データ生成手段がこのような条件データを生成する場合、ある暗号化条件データを復号化することによって生成された条件データは、次の暗号化条件データ（次の暗号化条件データは、一つとは限らない。）を復号化するための前提条件となりうる。

つまり、ある暗号化条件データを復号化することにより得られた条件データから、次の暗号化条件データの復号化を許容する場合の条件についてのデータを取り出せたとしても、次の暗号化条件データの復号化を許容する場合の条件が充足されない場合には、次の暗号化条件データの復号化を行うことができない。また、ある暗号化条件データを復号化する際に、その一つ手前で復号化されるべきであった暗号化条件データが復号化されていない場合にはその暗号化条件データの復号化はなされることがない。

前記条件データ生成手段は、前記条件データを複数生成するようになっているとともに、複数の前記条件データのうちの少なくとも幾つかを、それら幾つかの条件データを暗号化して生成された暗号化条件データの復号化が所定の順番で行われるように関連付けられており、且つそれら幾つかの条件データには、その条件データを暗号化して生成された暗号化条件データの次に復号化される暗号化条件データを復号化するための条件についてのデータが含まれるようにして生成するようになっていても構わない。

この場合、ある暗号化条件データを復号化することによって生成された条件データは、次の暗号化条件データ（次の暗号化条件データは、一つである。）を復号化するための前提条件となりうる。この場合、次に復号化される暗号化条件データを復号化するための条件が充足される限り、暗号化条件データは、所定の順番で、芋づる式に次々と復号化されることとなる。

前記基本条件データ生成手段は、前記幾つかの条件データのうち、それらを暗号化して生成された暗号化条件データのうち最初に復号化されるものの復号化を許容する場合の条件を含んでいてもよい。このようにすれば、復号化が所定の順番で行われるように関連付けられた一連の暗号化条件データの最初のものから順に、復号化を行えるようになる。

【００１２】

前記条件データにより特定される暗号化切断データの復号化を許容又は禁止するための条件は、上述のようなものであれば特にその制限はない。前記条件データは、例えば、以下の（４）～（７）の少なくとも一つについてのデータを含んでいる。

（４）前記暗号化切断データのうちの少なくとも一つについての復号化を行うことが許容又は禁止された復号化処理装置を特定するための情報、

（５）前記暗号化切断データの少なくとも一つについての復号化を行うことが許容又は禁止されたユーザを特定するための情報、

（６）前記暗号化切断データの少なくとも一つについての復号化が許容される期間に関する情報と、前記暗号化切断データの少なくとも一つについての復号化が禁止される期間に関する情報の少なくとも一方、

（７）複数の前記暗号化切断データのうちのどれの復号化を許容するかという情報、又は複数の前記暗号化切断データのうちのどれの復号化を禁止するかという情報。

【００１３】

暗号化処理装置は、前記暗号化手段が前記平文切断データを暗号化する際に用いられる鍵である複数の暗号化用鍵が保持された暗号化用鍵保持手段を備えていてもよい。

そして、前記暗号化手段は、前記暗号化用鍵保持手段に保持された複数の暗号化用鍵のうちの少なくとも２つを用いて複数の前記平文切断データを、そのうちの少なくとも１つが他の前記平文切断データとは異なる暗号化用鍵で暗号化されるようにして暗号化切断デ

ータとするようになっており、且つ、前記条件データ生成手段は、前記暗号化切断データのそれぞれが、前記暗号化用鍵保持手段に保持されている暗号化用鍵のうちのどれを用いて暗号化切断データとされたかということについてのデータを含む条件データを生成するようになっていてもよい。

この暗号化処理装置は、複数の暗号化用鍵を用いて平文切断データを暗号化切断データにするとともに、その暗号化切断データを暗号化するための暗号化用鍵を特定するためのデータを条件データに含めることで、暗号化データを復号化する者がその復号化を行えるようにしている。なお、この暗号化処理装置で作られた暗号化データを復号化する復号化処理装置は、この暗号化処理装置が備えるのと同様の鍵保持手段を備えていることが必要となる。

この暗号化処理装置は、複数の暗号化用鍵を用いて平文切断データの暗号化を行うことで暗号化データの安全性を高くできる。

【００１４】

上述の発明では、複数の暗号化用鍵を鍵保持手段によって予め保持しておくことで、平文切断データの暗号化にあたり複数の鍵を用いることができるようにしている。

これに対して、複数の暗号化用鍵を順次生成することで、平文切断データの暗号化にあたり複数の鍵を用いることができるようにすることも可能である。

そのような暗号化処理装置は、例えば、前記暗号化手段が前記平文切断データを暗号化する際に用いられる鍵である暗号化用鍵を所定のタイミングで生成する暗号化用鍵生成手段を備えている。そして、前記暗号化手段は、前記暗号化用鍵生成手段により生成された複数の暗号化用鍵を用いて複数の前記平文切断データを、そのうちの少なくとも１つが他の前記平文切断データとは異なる暗号化用鍵で暗号化されるようにして暗号化切断データとするようになっており、且つ、前記条件データ生成手段は、前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータを含む条件データを生成するようになっている。

このような暗号化処理装置は、平文切断データを暗号化するために用いる暗号化用鍵を保持しておらず、その代わりにそれを連続的に発生させるようになっているので、暗号化用鍵を盗まれることがない。したがって、このような暗号化処理装置で暗号化された暗号化データは、その安全性が高い。

前記暗号化用鍵生成手段は、前記暗号化用鍵を、初期状態から順次前記暗号化用鍵を生成した場合に、同じ順番で生成された暗号化用鍵が常に同じものとなるようにして生成するようになっていてもよい。この場合、前記条件データ生成手段が生成する前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータは、前記暗号化用鍵が生成された順番を示すものとすることができる。暗号化用鍵生成手段が生成する鍵が、同じ順番で生成されたものが常に同じものとなるようになっているのであれば、その暗号化用鍵を特定するためのデータは、暗号化用鍵が生成された順番を示すものとするのが簡単である。

なお、この暗号化処理装置で作られた暗号化データを復号化する復号化処理装置は、この暗号化処理装置が備えるのと同様の鍵生成手段を備えていることが必要となる。

【００１５】

前記暗号化用鍵生成手段を備える暗号化処理装置は、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用鍵用解生成手段を備えていてもよい。この場合、前記暗号化用鍵生成手段は、前記暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記暗号化用鍵を生成する。また、この場合、前記条件データ生成手段が生成する前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータは、前記暗号化用鍵が生成されたときに用いられた解を示すものとすることができる。

この暗号化処理装置における暗号化用鍵生成手段は、順次生成される擬似乱数である解に基づいて暗号化用鍵を生成する。したがって、この暗号化処理装置によって生成された暗号化データを復号化する復号化処理装置は、その解を特定するためのデータが条件デー

タに含まれていれば、その解に基づいて暗号化用鍵を生成し、また、その暗号化用鍵によって暗号化切断データを復号化することが可能である。

上述したように、前記暗号化用鍵生成手段を備える暗号化処理装置は、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用鍵用解生成手段を備えている場合がある。

この場合、前記暗号化用鍵生成手段は、前記暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記暗号化用鍵を生成するものとされており、且つ、前記条件データ生成手段が生成する前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータは、前記暗号化用鍵が生成されたときに用いられた解の生成された順番を示すものとすることができる。

この暗号化処理装置における暗号化用鍵生成手段は、順次生成される擬似乱数である解に基づいて暗号化用鍵を生成するが、その解は、同じ順番で生成させられた解が常に同じものとなるようになっている。したがって、この暗号化処理装置によって生成された暗号化データを復号化する復号化処理装置は、その解の生成された順番がわかればその解を特定でき、またその解が特定されればそれに基づいて暗号化用鍵を生成し、また、その暗号化用鍵によって暗号化切断データを復号化することが可能である。

ただし、以上２つの暗号化処理装置で作られた暗号化データを復号化する復号化処理装置は、この暗号化処理装置が備えるのと同様の鍵生成手段と暗号化用鍵用解生成手段を備えていることが必要となる。

【００１６】

上述したように、前記条件データ生成手段は、前記条件データを複数生成するようになっている場合がある。

この場合、暗号化処理装置は、前記条件データ暗号化手段が前記条件データを暗号化する際に用いられる鍵である複数の条件データ暗号化用鍵が保持された条件データ暗号化用鍵保持手段を備えていてもよい。

そして、前記条件データ暗号化手段は、前記条件データ暗号化用鍵保持手段に保持された複数の条件データ暗号化用鍵のうちの少なくとも２つを用いて複数の前記条件データを、そのうちの少なくとも１つが他の条件データとは異なる条件データ暗号化用鍵で暗号化されるようにして暗号化条件データとするようになっており、且つ、前記基本条件データ生成手段は、前記暗号化条件データのそれぞれが、前記条件データ鍵保持手段に保持されている条件データ暗号化用鍵のうちのどれを用いて暗号化条件データとされたかということについてのデータを含む基本条件データを生成するようになっていてもよい。

この暗号化処理装置は、複数の暗号化用鍵を予め準備しておくことで、平文切断データの暗号化にあたり複数の鍵を用いることができるようにした上述の場合と同様に、複数の条件データ暗号化用鍵を予め準備しておくことで、条件データの暗号化にあたり複数の鍵を用いることができるようにしたものである。

なお、この暗号化処理装置で作られた暗号化データを復号化する復号化処理装置は、この暗号化処理装置が備えるのと同様の条件データ暗号化用鍵保持手段を備えていることが必要となる。

この暗号化処理装置は、複数の条件データ暗号化用鍵を用いて条件データの暗号化を行うことで暗号化データの安全性を高くできる。

【００１７】

本願の暗号化処理装置が備える前記条件データ生成手段は、前記条件データを複数生成するようになっていてもよいが、この場合、前記条件データ暗号化手段が前記条件データを暗号化する際に用いられる鍵である条件データ暗号化用鍵を所定のタイミングで生成する条件データ暗号化用鍵生成手段を備えており、前記条件データ暗号化手段は、前記条件データ暗号化用鍵生成手段により生成された複数の条件データ暗号化用鍵を用いて複数の前記条件データを、そのうちの少なくとも１つが他の条件データとは異なる条件データ暗号化用鍵で暗号化されるようにして暗号化条件データとするようになっており、且つ、前記基本条件データ生成手段は、前記暗号化条件データのそれぞれが暗号化された際に使用

された条件データ暗号化用鍵を特定するためのデータを含む基本条件データを生成するようになっていてもよい。

これは、複数の暗号化用鍵を順次生成することで、平文切断データの暗号化にあたり複数の鍵を用いることができるようにした上述の場合と同様に、複数の条件データ暗号化用鍵を順次生成することで、条件データの暗号化にあたり複数の鍵を用いることができるようにしたものである。

以下の発明も、複数の暗号化用鍵を生成する上述の発明と類似するものである。

この暗号化処理装置によっても、暗号化データの安全性を高められるという効果を得られる。

前記条件データ暗号化用鍵生成手段は、前記条件データ暗号化用鍵を、初期状態から順次前記条件データ暗号化用鍵を生成した場合に、同じ順番で生成された条件データ暗号化用鍵が常に同じものとなるようにして生成するようになっており、且つ、前記基本条件データ生成手段が生成する前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータは、前記条件データ暗号化用鍵が生成された順番を示すものとすることができる。

この暗号化処理装置は、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用鍵用解生成手段を備えており、前記条件データ暗号化用鍵生成手段は、前記条件データ暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用鍵を生成するものとされており、且つ、前記基本条件データ生成手段が生成する前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータは、前記条件データ暗号化用鍵が生成されたときに用いられた解を示すものとすることができる。

また、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用鍵用解生成手段を備えており、前記条件データ暗号化用鍵生成手段は、前記条件データ暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用鍵を生成するものとされており、且つ、前記基本条件データ生成手段が生成する前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータは、前記条件データ暗号化用鍵が生成されたときに用いられた解の生成された順番を示すものとすることができる。

ただし、以上２つの暗号化処理装置で作られた暗号化データを復号化する復号化処理装置は、この暗号化処理装置が備えるのと同様の条件データ暗号化用鍵生成手段と条件データ暗号化用鍵用解生成手段を備えていることが必要となる。

【００１８】

本発明の暗号化処理装置は、上述のように、暗号化用鍵を複数用いるものとすることができる。これに代えて、複数の暗号化用アルゴリズムを用いるようにすることもできる。

例えば、暗号化処理装置は、前記暗号化手段が前記平文切断データを暗号化する際に用いられるアルゴリズムである複数の暗号化用アルゴリズムが保持された暗号化用アルゴリズム保持手段を備えていてもよい。この場合、前記暗号化手段は、前記暗号化用アルゴリズム保持手段に保持された複数の暗号化用アルゴリズムのうちの少なくとも２つを用いて複数の前記平文切断データを、そのうちの少なくとも１つが他の前記平文切断データとは異なる暗号化用アルゴリズムで暗号化されるようにして暗号化切断データとするようになっており、且つ、前記条件データ生成手段は、前記暗号化切断データのそれぞれが、前記暗号化用アルゴリズム保持手段に保持されている暗号化用アルゴリズムのうちのどれを用いて暗号化切断データとされたかということについてのデータを含む条件データを生成するようになっている。

これによっても、暗号化処理装置で生成された暗号化データの安全性を高められる。

なお、この暗号化処理装置で作られた暗号化データを復号化する復号化処理装置は、この暗号化処理装置が備えるのと同様の暗号化用アルゴリズム保持手段を備えていることが

必要となる。

【００１９】

複数の暗号化用鍵を連続して生成する暗号化処理装置について上述したが、本願の暗号化処理装置は、複数の暗号化用鍵を連続して生成するのに代えて複数の暗号化用アルゴリズムを連続して生成するものとすることもできる。

その暗号化処理装置は、前記暗号化手段が前記平文切断データを暗号化する際に用いられるアルゴリズムである暗号化用アルゴリズムを所定のタイミングで生成する暗号化用アルゴリズム生成手段を備えており、前記暗号化手段は、前記暗号化用アルゴリズム生成手段により生成された複数の暗号化用アルゴリズムを用いて複数の前記平文切断データを、そのうちの少なくとも１つが他の前記平文切断データとは異なる暗号化用アルゴリズムで暗号化されるようにして暗号化切断データとするようになっており、且つ、前記条件データ生成手段は、前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータを含む条件データを生成するようになっている。

この場合、前記暗号化用アルゴリズム生成手段は、前記暗号化用アルゴリズムを、初期状態から順次前記暗号化用アルゴリズムを生成した場合に、同じ順番で生成された暗号化用アルゴリズムが常に同じものとなるようにして生成するようになっており、且つ、前記条件データ生成手段が生成する前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータは、前記暗号化用アルゴリズムが生成された順番を示すものとすることができる。

同じ順番で生成された暗号化用アルゴリズムが常に同じものとなるようにして暗号化用アルゴリズムを生成する暗号化用アルゴリズム生成手段を備える暗号化処理装置は、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用アルゴリズム用解生成手段を備えており、前記暗号化用アルゴリズム生成手段は、前記暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記暗号化用アルゴリズムを生成するものとされており、且つ、前記条件データ生成手段が生成する前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータは、前記暗号化用アルゴリズムが生成されたときに用いられた解を示すもとすることができる。

或いは、暗号化処理装置は、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用アルゴリズム用解生成手段を備えており、前記暗号化用アルゴリズム生成手段は、前記暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記暗号化用アルゴリズムを生成するものとされており、且つ、前記条件データ生成手段が生成する前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータは、前記暗号化用アルゴリズムが生成されたときに用いられた解の生成された順番を示すものとすることができる。

【００２０】

上述したように条件データ生成手段は、条件データを複数生成するようになっている場合がある。そして、生成した複数の条件データの少なくとも一つを他とは異なる条件データ暗号化用鍵で暗号化する暗号化処理装置について既に説明した。これに代えて、生成した複数の条件データの少なくとも一つを他とは異なる条件データ暗号化用アルゴリズムで暗号化することができる。

それは例えば、以下の暗号化処理装置により可能となる。

即ち、前記条件データ生成手段は、前記条件データを複数生成するようになっており、前記条件データ暗号化手段が前記条件データを暗号化する際に用いられるアルゴリズムである複数の条件データ暗号化用アルゴリズムが保持された条件データ暗号化用アルゴリズム保持手段を備えており、前記条件データ暗号化手段は、前記条件データ暗号化用アルゴリズム保持手段に保持された複数の条件データ暗号化用アルゴリズムのうちの少なくとも２つを用いて複数の前記条件データを、そのうちの少なくとも１つが他の条件データとは異なる条件データ暗号化用アルゴリズムで暗号化されるようにして暗号化条件データとす

るようになっており、且つ、前記基本条件データ生成手段は、前記暗号化条件データのそれぞれが、前記条件データ暗号化用アルゴリズム保持手段に保持されている条件データ暗号化用アルゴリズムのうちのどれを用いて暗号化条件データとされたかということについてのデータを含む条件データを生成するようになっている暗号化処理装置である。

【００２１】

暗号化処理装置の条件データ生成手段が条件データを複数生成するようになっている場合、条件データ暗号化用アルゴリズムを連続的に生成することによっても、生成した複数の条件データの少なくとも一つを他とは異なる条件データ暗号化用アルゴリズムで暗号化することができる。

例えば、前記条件データ生成手段は、前記条件データを複数生成するようになっているとともに、前記条件データ暗号化手段が前記条件データを暗号化する際に用いられるアルゴリズムである条件データ暗号化用アルゴリズムを所定のタイミングで生成する条件データ暗号化用アルゴリズム生成手段を備えており、前記条件データ暗号化手段は、前記条件データ暗号化用アルゴリズム生成手段により生成された複数の条件データ暗号化用アルゴリズムを用いて複数の前記条件データを、そのうちの少なくとも１つが他の条件データとは異なる条件データ暗号化用アルゴリズムで暗号化されるようにして暗号化条件データとするようになっており、且つ、前記基本条件データ生成手段は、前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータを含む基本条件データを生成するようになっている、暗号化処理装置である。

この暗号化処理装置における前記条件データ暗号化用アルゴリズム生成手段は、前記条件データ暗号化用アルゴリズムを、初期状態から順次前記条件データ暗号化用アルゴリズムを生成した場合に、同じ順番で生成された条件データ暗号化用アルゴリズムが常に同じものとなるようにして生成するようになっており、且つ、前記基本条件データ生成手段が生成する前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータは、前記条件データ暗号化用アルゴリズムが生成された順番を示すものとすることができる。

同じ順番で生成された条件データ暗号化用アルゴリズムが常に同じものとなるようにして条件データ暗号化用アルゴリズムを生成する条件データ暗号化用アルゴリズム生成手段を備える暗号化処理装置は、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用アルゴリズム用解生成手段を備えており、前記条件データ暗号化用アルゴリズム生成手段は、前記条件データ暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用アルゴリズムを生成するものとされており、且つ前記基本条件データ生成手段が生成する前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータは、前記条件データ暗号化用アルゴリズムが生成されたときに用いられた解を示すものとすることができる。

また、条件データ暗号化用アルゴリズム生成手段を備える暗号化処理装置は、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用アルゴリズム用解生成手段を備えており、前記条件データ暗号化用アルゴリズム生成手段は、前記条件データ暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用アルゴリズムを生成するものとされており、且つ前記基本条件データ生成手段が生成する前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータは、前記条件データ暗号化用アルゴリズムが生成されたときに用いられた解の生成された順番を示すものとすることができる。

【００２２】

本発明の暗号化処理装置が生成する暗号化データのデータ構造は、以下に述べるようなものであり、いずれもその安全性が高い。

即ち、平文である処理対象データを所定のビット数毎に切断して得られた複数の平文切断データを、所定の鍵、及び所定のアルゴリズムによって暗号化して得られた複数の暗号

化切断データと、前記暗号化切断データのそれぞれの復号化を許容する場合の条件と、前記暗号化切断データのそれぞれの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む条件データを所定の鍵、及び所定のアルゴリズムによって暗号化して得られた暗号化条件データと、前記暗号化条件データの復号化を許容する場合の条件と、前記暗号化条件データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む基本条件データと、を、一まとめにして一連とした、所定の復号化処理装置で復号化されることが予定された暗号化データのデータ構造であって、前記暗号化切断データと、前記暗号化条件データと、前記基本条件データとは、前記暗号化条件データが、その暗号化条件データの元になった条件データに含まれた条件によりその復号化が許容又は禁止される暗号化切断データよりも前方に位置するようにしながら、且つ前記基本条件データが前記暗号化条件データよりも前方に位置するようになっている、暗号化データのデータ構造である。

このデータ構造において、前記条件データは複数とすることができ、且つ以下の（１）～（３）の条件を充足するようになっているようにすることができる。

（１）複数の前記条件データのそれぞれは、前記暗号化切断データのうちの少なくとも一つと対応付けられているとともに、その対応付けられた前記暗号化切断データの復号化を許容する場合の条件と、その対応付けられた前記暗号化切断データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含む、

（２）複数の前記条件データは、前記暗号化切断データのすべてが複数の前記条件データのいずれかと対応付けられるようにされる、

（３）一つの前記暗号化切断データに複数の前記条件データが対応付けられることはない。

この場合、前記基本条件データは、複数の前記暗号化条件データのうちのどれの復号化を許容するのかという条件と、複数の前記暗号化条件データのうちのどれの復号化を禁止するのかという条件の少なくとも一方についてのデータを含むようになっているものとすることができる。

前記条件データは複数であり、且つ前記条件データの少なくとも一つには、他の条件データを暗号化して生成された暗号化条件データの復号化を許容する場合の条件についてのデータが含められていてもよい。

前記条件データは複数であり、且つ複数の前記条件データのうちの少なくとも幾つかは、それら幾つかの条件データを暗号化して生成された暗号化条件データの復号化が所定の順番で行われるように関連付けられており、且つそれら幾つかの条件データのそれぞれには、その条件データを暗号化して生成された暗号化条件データの次に復号化される暗号化条件データを復号化するための条件についてのデータが含まれていてもよい。この場合、前記基本条件データは、前記幾つかの条件データのうち、それらを暗号化して生成された暗号化条件データのうち最初に復号化されるものの復号化を許容する場合の条件を含んでいても構わない。

上述のデータ構造に含まれる前記条件データは、以下の（４）～（７）の少なくとも一つについてのデータを含んでいてもよい。

（４）前記暗号化切断データのうちの少なくとも一つについての復号化を行うことが許容又は禁止された復号化処理装置を特定するための情報、

（５）前記暗号化切断データの少なくとも一つについての復号化を行うことが許容又は禁止されたユーザを特定するための情報、

（６）前記暗号化切断データの少なくとも一つについての復号化が許容される期間に関する情報と、前記暗号化切断データの少なくとも一つについての復号化が禁止される期間に関する情報の少なくとも一方、

（７）複数の前記暗号化切断データのうちのどれの復号化を許容するかという情報、又は複数の前記暗号化切断データのうちのどれの復号化を禁止するかという情報。

【００２３】

本発明のデータ構造における前記暗号化切断データのそれぞれは、複数の暗号化用鍵の

１つを用いて、且つ複数の前記平文切断データの少なくとも１つが他の平文切断データとは異なる暗号化用鍵で暗号化されるようにして暗号化されたものであり、且つ、前記条件データは、前記暗号化切断データのそれぞれが、複数の前記暗号化用鍵のうちのどれを用いて暗号化切断データとされたかということについてのデータを含むものとされていてもよい。

【００２４】

本発明のデータ構造における前記暗号化データは、複数の暗号化用鍵を所定のタイミングで生成する暗号化用鍵生成手段を備える暗号化処理装置で生成されるものであり、前記暗号化切断データのそれぞれは、前記暗号化用鍵生成手段が生成した複数の暗号化用鍵の１つを用いて、且つ複数の前記平文切断データの少なくとも１つが他の平文切断データとは異なる暗号化用鍵で暗号化されるようにして暗号化されたものであり、且つ、前記条件データは、前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータを含むものとされていてもよい。

本発明のデータ構造は、それが複数の前記暗号化用鍵を所定のタイミングで生成する暗号化用鍵生成手段を備える暗号化処理装置で生成される場合には次のようなものとできる。

即ち、前記暗号化用鍵生成手段は、前記暗号化用鍵を、初期状態から順次前記暗号化用鍵を生成した場合に、同じ順番で生成された暗号化用鍵が常に同じものとなるようにして生成するようになっており、且つ、前記条件データに含まれる前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータは、前記暗号化用鍵が生成された順番を示すものとすることができる。

暗号化用鍵生成手段を有する暗号化処理装置で生成される暗号化データは、次のようなものとすることができる。

即ち、前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用鍵用解生成手段を備える暗号化処理装置で生成されるものであり、前記暗号化用鍵生成手段は、前記暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記暗号化用鍵を生成するものとされており、且つ、前記条件データに含まれる前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータは、前記暗号化用鍵が生成されたときに用いられた解を示すものとされていてもよい。

或いは、前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用鍵用解生成手段を備える暗号化処理装置で生成されるものであり、前記暗号化用鍵生成手段は、前記暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記暗号化用鍵を生成するものとされており、且つ、前記条件データに含まれる前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用鍵を特定するためのデータは、前記暗号化用鍵が生成されたときに用いられた解の生成された順番を示すものとされていてもよい。

【００２５】

本発明の暗号化データのデータ構造において、前記条件データは複数である場合がある。この場合、前記暗号化条件データのそれぞれは、複数の条件データ暗号化用鍵の１つを用いて、且つ複数の前記条件データの少なくとも１つが他の条件データとは異なる条件データ暗号化用鍵で暗号化されるようにして暗号化されたものであり、且つ、前記基本条件データは、前記暗号化条件データのそれぞれが、複数の前記条件データ暗号化用鍵のうちのどれを用いて暗号化条件データとされたかということについてのデータを含むものとされていてもよい。

【００２６】

本発明の暗号化データのデータ構造において、前記条件データは複数である場合がある。この場合、前記暗号化条件データは、複数の前記条件データ暗号化用鍵を所定のタイミングで生成する条件データ暗号化用鍵生成手段を備える暗号化処理装置で生成されるものであり、前記暗号化条件データのそれぞれは、前記条件データ暗号化用鍵生成手段が生成

した複数の条件データ暗号化用鍵の１つを用いて、且つ複数の前記条件データの少なくとも１つが他の条件データとは異なる条件データ暗号化用鍵で暗号化されるようにして暗号化されたものであり、且つ前記基本条件データは、前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータを含むものとされていてもよい。

本発明のデータ構造は、それが複数の前記条件データ暗号化用鍵を所定のタイミングで生成する条件データ暗号化用鍵生成手段を備える暗号化処理装置で生成される場合には次のようなものとできる。

即ち、前記条件データ暗号化用鍵生成手段は、前記条件データ暗号化用鍵を、初期状態から順次前記条件データ暗号化用鍵を生成した場合に、同じ順番で生成された条件データ暗号化用鍵が常に同じものとなるようにして生成するようになっており、且つ、前記基本条件データに含まれる前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータは、前記条件データ暗号化用鍵が生成された順番を示すものとされていてもよい。

条件データ暗号化用鍵生成手段を有する暗号化処理装置で生成される暗号化データは、次のようなものとすることができる。

即ち、前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用鍵用解生成手段を備える暗号化処理装置で生成されるものであり、前記条件データ暗号化用鍵生成手段は、前記条件データ暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用鍵を生成するものとされており、且つ、前記基本条件データに含まれる前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータは、前記条件データ暗号化用鍵生成されたときに用いられた解を示すものとすることができる。

或いは、前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用鍵用解生成手段を備える暗号化処理装置で生成されるものであり、前記条件データ暗号化用鍵生成手段は、前記条件データ暗号化用鍵用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用鍵を生成するものとされており、且つ、前記基本条件データに含まれる前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用鍵を特定するためのデータは、前記条件データ暗号化用鍵が生成されたときに用いられた解の生成された順番を示すものとすることができる。

【００２７】

本発明のデータ構造における前記暗号化切断データのそれぞれは、複数の暗号化用アルゴリズムの１つを用いて、且つ複数の前記平文切断データの少なくとも１つが他の平文切断データとは異なる暗号化用アルゴリズムで暗号化されるようにして暗号化されたものであり、且つ、前記条件データは、前記暗号化切断データのそれぞれが、複数の前記暗号化用アルゴリズムのうちのどれを用いて暗号化切断データとされたかということについてのデータを含むものとされていてもよい。

【００２８】

本発明のデータ構造における前記暗号化データは、前記暗号化データは、複数の暗号化用アルゴリズムを所定のタイミングで生成する暗号化用アルゴリズム生成手段を備える暗号化処理装置で生成されるものであり、前記暗号化切断データのそれぞれは、前記暗号化用アルゴリズム生成手段が生成した複数の暗号化用アルゴリズムの１つを用いて、且つ複数の前記平文切断データの少なくとも１つが他の平文切断データとは異なる暗号化用アルゴリズムで暗号化されるようにして暗号化されたものであり、且つ前記条件データは、前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータを含むものとされていてもよい。

本発明のデータ構造は、それが複数の前記暗号化用アルゴリズムを所定のタイミングで生成する暗号化用アルゴリズム生成手段を備える暗号化処理装置で生成される場合には次

のようなものとできる。

即ち、前記暗号化用アルゴリズム生成手段は、前記暗号化用アルゴリズムを、初期状態から順次前記暗号化用アルゴリズムを生成した場合に、同じ順番で生成された暗号化用アルゴリズムが常に同じものとなるようにして生成するようになっており、且つ、前記条件データに含まれる前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータは、前記暗号化用アルゴリズムが生成された順番を示すものとすることができる。

暗号化用アルゴリズム生成手段を有する暗号化処理装置で生成される暗号化データは、次のようなものとすることができる。

即ち、前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用アルゴリズム用解生成手段を備える暗号化処理装置で生成されるものであり、前記暗号化用アルゴリズム生成手段は、前記暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記暗号化用アルゴリズムを生成するものとされており、且つ、前記条件データに含まれる前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータは、前記暗号化用アルゴリズムが生成されたときに用いられた解を示すものとされていてもよい。

或いは、前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる暗号化用アルゴリズム用解生成手段を備える暗号化処理装置で生成されるものであり、前記暗号化用アルゴリズム生成手段は、前記暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記暗号化用アルゴリズムを生成するものとされており、且つ、前記条件データに含まれる前記暗号化切断データのそれぞれが暗号化された際に使用された暗号化用アルゴリズムを特定するためのデータは、前記暗号化用アルゴリズムが生成されたときに用いられた解の生成された順番を示すものとされていてもよい。

【００２９】

本発明の暗号化データのデータ構造において、前記条件データは複数である場合がある。この場合、前記暗号化条件データのそれぞれは、複数の条件データ暗号化用アルゴリズムの１つを用いて、且つ複数の前記条件データの少なくとも１つが他の条件データとは異なる条件データ暗号化用アルゴリズムで暗号化されるようにして暗号化されたものであり、且つ、前記基本条件データは、前記暗号化条件データのそれぞれが、複数の前記条件データ暗号化用アルゴリズムのうちのどれを用いて暗号化条件データとされたかということについてのデータを含むものとされていてもよい。

【００３０】

本発明の暗号化データのデータ構造において、前記条件データは複数である場合がある。この場合、前記暗号化条件データは、複数の条件データ暗号化用アルゴリズムを所定のタイミングで生成する条件データ暗号化用アルゴリズム生成手段を備える暗号化処理装置で生成されるものであり、前記暗号化条件データのそれぞれは、条件データ暗号化用アルゴリズム生成手段が生成した複数の条件データ暗号化用アルゴリズムの１つを用いて、且つ複数の前記条件データの少なくとも１つが他の条件データとは異なる条件データ暗号化用アルゴリズムで暗号化されるようにして暗号化されたものであり、且つ前記基本条件データは、前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータを含むものとされていてもよい。

本発明のデータ構造は、それが複数の前記条件データ暗号化用アルゴリズムを所定のタイミングで生成する条件データ暗号化用アルゴリズム生成手段を備える暗号化処理装置で生成される場合には次のようなものとできる。

即ち、前記条件データ暗号化用アルゴリズム生成手段は、前記条件データ暗号化用アルゴリズムを、初期状態から順次前記条件データ暗号化用アルゴリズムを生成した場合に、同じ順番で生成された条件データ暗号化用アルゴリズムが常に同じものとなるようにして生成するようになっており、且つ前記基本条件データに含まれる前記暗号化条件データの

それぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータは、前記条件データ暗号化用アルゴリズムが生成された順番を示すものとされていてもよい。

条件データ暗号化用アルゴリズム生成手段を有する暗号化処理装置で生成される暗号化データは、次のようなものとすることができる。

即ち、前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用アルゴリズム用解生成手段を備える暗号化処理装置で生成されるものであり、前記条件データ暗号化用アルゴリズム生成手段は、前記条件データ暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用アルゴリズムを生成するものとされており、且つ前記基本条件データに含まれる前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータは、前記条件データ暗号化用アルゴリズムが生成されたときに用いられた解を示すものとすることができる。

或いは、前記暗号化データは、擬似乱数である解を、初期状態から同じ順番で生成させられた解が常に同じものとなるようにして順次生成させることのできる条件データ暗号化用アルゴリズム用解生成手段を備える暗号化処理装置で生成されるものであり、前記条件データ暗号化用アルゴリズム生成手段は、前記条件データ暗号化用アルゴリズム用解生成手段から受付けた前記解に基づいて、前記条件データ暗号化用アルゴリズムを生成するものとされており、且つ前記基本条件データに含まれる前記暗号化条件データのそれぞれが暗号化された際に使用された条件データ暗号化用アルゴリズムを特定するためのデータは、前記条件データ暗号化用アルゴリズムが生成されたときに用いられた解の生成された順番を示すものとすることができる。

【００３１】

本発明の暗号化処理装置によって生成された暗号化データは、例えば次の復号化処理装置によって復号化することができる。

即ち、前記暗号化データから基本条件データを読出す基本条件データ読出し手段、前記暗号化データから前記暗号化条件データを読出す暗号化条件データ読出し手段、前記暗号化データから前記暗号化切断データを読出す暗号化切断データ読出し手段、前記暗号化条件データ読出し手段によって読出した前記暗号化条件データが、前記基本条件データ読出し手段が読出した前記基本条件データに示された暗号化条件データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化条件データが復号化を禁止される場合の条件に合致しないと判断した場合に前記暗号化条件データを復号化して条件データにする暗号化条件データ復号化手段、前記暗号化切断データ読出し手段によって読出した暗号化切断データのそれぞれを、前記暗号化条件データ復号化手段によって復号化された条件データに示された暗号化切断データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化切断データが復号化を禁止される場合の条件に合致しないと判断した場合にのみ復号化して平文切断データにする復号化手段、前記復号化手段によって復号化された平文切断データを一まとめにして処理対象データとする接続手段、を備えている復号化処理装置である。

或いは、前記暗号化データから基本条件データを読出す基本条件データ読出し手段、前記暗号化データから前記暗号化条件データを読出す暗号化条件データ読出し手段、前記暗号化データから前記暗号化切断データを読出す暗号化切断データ読出し手段、前記暗号化条件データ読出し手段によって読出した前記暗号化条件データが、前記基本条件データ読出し手段が読出した前記基本条件データに示された暗号化条件データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化条件データが復号化を禁止される場合の条件に合致しないと判断した場合に前記暗号化条件データを復号化して条件データにする暗号化条件データ復号化手段、前記暗号化切断データ読出し手段によって読出した暗号化切断データのそれぞれが、前記暗号化条件データ復号化手段によって復号化された条件データに示された暗号化切断データが復号化を許容される場合の条件に合致すると判断

した場合、又は暗号化切断データが復号化を禁止される場合の条件に合致しないと判断した場合にのみ、その暗号化切断データを復号化して平文切断データにする復号化手段、前記復号化手段によって復号化された平文切断データを一まとめにして処理対象データとする接続手段、を備えており、前記暗号化条件データ復号化手段は、前記暗号化条件データ読出し手段によって読出した暗号化条件データのそれぞれが、複数の前記暗号化条件データのうちのどれの復号化を許容するのかという条件に合致すると判断した場合、又は複数の前記暗号化条件データのうちのどれの復号化を禁止するのかという条件に合致しなかった場合にのみ、その暗号化条件データを復号化して条件データにするようにされており、前記復号化手段は、復号化された条件データのみに基づいて、前記暗号化切断データを復号化して前記平文切断データにする処理を行う、復号化処理装置である。

【００３２】

復号化処理装置では、例えば以下の方法が実行される。

復号化処理装置で実行される方法であって、前記復号化処理装置が、前記暗号化データから基本条件データを読出す過程、前記暗号化データから前記暗号化条件データを読出す過程、前記暗号化データから前記暗号化切断データを読出す過程、読出した暗号化条件データが、読出した前記基本条件データに示された暗号化条件データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化条件データが復号化を禁止される場合の条件に合致しないと判断した場合に前記暗号化条件データを復号化して条件データにする過程、読出した暗号化切断データのそれぞれを、復号化された条件データに示された暗号化切断データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化切断データが復号化を禁止される場合の条件に合致しないと判断した場合にのみ復号化して平文切断データにする過程、前記復号化手段によって復号化された平文切断データを一まとめにして処理対象データとする過程、を含む復号化方法である。

或いは、復号化処理装置で実行される方法であって、前記暗号化データから基本条件データを読出す過程、前記暗号化データから前記暗号化条件データを読出す過程、前記暗号化データから前記暗号化切断データを読出す過程、読出した前記暗号化条件データが、読出した前記基本条件データに示された暗号化条件データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化条件データが復号化を禁止される場合の条件に合致しないと判断した場合に前記暗号化条件データを復号化して条件データにする過程、前記暗号化切断データ読出し手段によって読出した暗号化切断データのそれぞれが、前記暗号化条件データ復号化手段によって復号化された条件データに示された暗号化切断データが復号化を許容される場合の条件に合致すると判断した場合、又は暗号化切断データが復号化を禁止される場合の条件に合致しないと判断した場合にのみ、その暗号化切断データを復号化して平文切断データにする過程、復号化された平文切断データを一まとめにして処理対象データとする過程、を含み、前記暗号化条件データを復号化して条件データにする前記過程では、暗号化条件データのそれぞれが、複数の前記暗号化条件データのうちのどれの復号化を許容するのかという条件に合致すると判断した場合、又は複数の前記暗号化条件データのうちのどれの復号化を禁止するのかという条件に合致しなかった場合にのみ、その暗号化条件データを復号化して条件データにし、暗号化切断データを復号化して平文切断データにする前記過程では、復号化された条件データのみに基づいて、前記暗号化切断データを復号化して前記平文切断データにする前記過程を行う、復号化方法である。

【発明を実施するための最良の形態】

【００３３】

以下、本発明の第１、及び第２実施形態について説明する。

各実施形態の説明では、同一の対象には同一の符号を付すものとし、また、重複する説明は場合により省略するものとする。

【００３４】

≪第１実施形態≫

この実施形態では、暗号化処理装置１と、複数の復号化処理装置２を含む図１に示した

如き暗号化システムを、本発明の一実施形態として挙げる。
暗号化処理装置１と、復号化処理装置２は、ＬＡＮ（Local Area Network）その他のネットワークＮによって接続されており、暗号化処理装置１が後述するようにして生成した暗号化データを、復号化処理装置２のそれぞれに送ることができるようにされている。
もっとも、暗号化処理装置１と復号化処理装置２がネットワークＮで接続されている必要は必ずしも無い。ただし、復号化処理装置２は、暗号化処理装置１が生成した暗号化データを、例えばＣＤ－ＲＯＭなどの記録媒体を介して暗号化処理装置１から受取れるようにする必要がある。そのために必要な、記録媒体に暗号化データの記録を行うデータライタや、記録媒体から暗号化データを読出すデータリーダについては、それらが汎用的な技術なのでその説明を省略する。
なお、復号化処理装置２は少なくとも一つあれば足り、また、暗号化処理装置１が復号化処理装置２を兼ねる場合もある。
【００３５】
暗号化処理装置１、復号化処理装置２の構成を説明する。まず、暗号化処理装置１の構成を説明することにする。
【００３６】
暗号化処理装置１のハードウエア構成を図２に示す。
暗号化処理装置１は、この実施形態では、ＣＰＵ（central processing unit）２１、ＲＯＭ（read only memory）２２、ＨＤＤ（hard disk drive）２３、ＲＡＭ（random access memory）２４、入力装置２５、表示装置２６、暗号化装置２７、通信装置２８、バス２９を含む構成とされている。ＣＰＵ２１、ＲＯＭ２２、ＨＤＤ２３、ＲＡＭ２４、入力装置２５、表示装置２６、暗号化装置２７、通信装置２８は、バス２９を介してデータの交換が可能とされている。
ＲＯＭ２２、あるいはＨＤＤ２３には、所定のプログラム、及び所定のデータ（これには、処理対象データとなるものが含まれる場合があり、本実施形態ではそのようにされている。また、所定のデータには、上記プログラムを実行するために必要なデータが含まれる。）が記録されている。ＣＰＵ２１は、暗号化処理装置１全体の制御を行うものであり、ＲＯＭ２２、あるいはＨＤＤ２３に記憶されたプログラムやデータに基づいて、後述する処理を実行するものである。ＲＡＭ２４は、ＣＰＵ２１で処理を行う際の作業用記憶領域として用いられる。
入力装置２５は、キーボード、マウスなどから構成されており、コマンドやデータの入力に用いられる。表示装置２６は、ＬＣＤ（liquid crystal display）、ＣＲＴ（cathode ray tube）などから構成されており、コマンドや入力されたデータや、後述する処理の状況などを表示するために用いられる。
暗号化装置２７は、後述する、処理対象データの暗号化、及び暗号化データの復号化を行うものである。
通信装置２８は、ネットワークＮを介しての復号化処理装置２との通信を実行するものである。通信装置２８は、後述する暗号化データの後述するヘッダに含まれるＭＡＣアドレスなどで指定される宛先に、暗号化データを送信するようになっている。
【００３７】
次に、暗号化装置２７の構成について説明する。図３に、暗号化装置２７のブロック構成図を示す。
暗号化装置２７は、インタフェイス部２７１、前処理部２７２、暗号化部２７３、解生成部２７４、アルゴリズム生成部２７５、鍵生成部２７６、条件データ生成部２７７、基本条件データ生成部２７８、ヘッダ生成部２７９、及び接続部２８０から構成される。
【００３８】
インタフェイス部２７１は、バス２９と通信装置２８との間におけるデータのやりとりを行うものである。
インタフェイス部２７１は、バス２９を介して、ＨＤＤＨＨ２３から処理対象データを受取るようになっており、受取った処理対象データを前処理部２７２に送るようになって

いる。また、インタフェイス部２７１は処理対象データ又は暗号化データを受取った場合、その旨を示すデータを解生成部２７４に送るようになっている。

他方、インタフェイス部２７１は、後述するように、接続部２８０から暗号化データを受取るようになっており、受取った暗号化データをバス２９に送るようになっている。この暗号化データは、通信装置２８介して、ネットワークＮ経由で復号化処理装置２へ送られる。

【００３９】

前処理部２７２は、インタフェイス部２７１を介してバス２９から受取った処理対象データを、所定のビット数毎に切断して、平文切断データを生成し、これを暗号化部２７３に送る機能を有している。処理対象データをどのように切断するかについては後述する。なお、前処理部２７２は、この実施形態では、処理対象データに後述するような方法で、処理対象データとは関係のないデータであるダミーデータを含める機能を有している。

【００４０】

暗号化部２７３は、平文切断データを前処理部２７２から受取り、それを暗号化する機能を有している。また、暗号化部２７３は、後述する条件データを条件データ生成部２７７から受取り、これも暗号化する機能を有している。なお、条件データ生成部２７７は、生成した条件データを後述する基準ビット数に予め切断してから暗号化部２７３に送るようにされている。

なお、この実施形態における暗号化部２７３は、暗号化を行う場合の処理単位である基準ビット数が固定されている。この実施形態における基準ビット数は、これには限られないが８ビットとなっている。暗号化の処理の詳細については後で述べる。

【００４１】

解生成部２７４は、解を順次生成するものである。暗号化処理装置１の解生成部２７４が生成する解は、同じ順番で生成された解が同じものになるようにされている。なお、後述する復号化処理装置２における復号化装置も解生成部を備えており、この解生成部は暗号化処理装置１が備える解生成部２７４と同じにされている。つまり、同じ順番で生成された解を比較すれば、暗号化処理装置１が備える解生成部２７４が生成する解と、復号化処理装置２が備える解生成部が生成する解は同じになるようにされている。この実施形態における解は、擬似乱数である。生成された解は、前処理部２７２と、アルゴリズム生成部２７５と、鍵生成部２７６とに送られる。また、その解が何番目に生成された解なのかという情報が、解生成部２７４から、条件データ生成部２７７と、基本条件データ生成部２７８とに送られる。

【００４２】

アルゴリズム生成部２７５は、解生成部２７４から受付けた解に基づいてアルゴリズムを生成するものである。このアルゴリズムは、暗号化部２７３で、暗号化処理を行うときに使用されるものである。

【００４３】

鍵生成部２７６は、解生成部２７４から受付けた解に基づいて鍵を生成するものである。鍵は、暗号化部２７３で、暗号化処理を行うときに使用されるものである。

【００４４】

条件データ生成部２７７は、例えばユーザが操作した入力装置から、インタフェイス部２７１を介して受付けたデータに基づいて、条件データを生成するものである。

条件データは、復号化処理装置２で、上述の暗号化切断データのそれぞれの復号化を許容する場合の条件と、暗号化切断データのそれぞれの復号化を禁止する場合の条件の少なくとも一方についてのデータを含んでいる。

この実施形態の条件データは、複数である。

条件データのそれぞれは、複数ある暗号化切断データの少なくとも一つと対応付けられている。ただし、一つの暗号化切断データに複数の条件データが対応付けられていることはない。また、暗号化切断データのすべてが、複数の条件データのいずれかと対応付けられている。

条件データは、その対応付けられた暗号化切断データの復号化を許容する場合の条件と、その対応付けられた暗号化切断データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含んでいる。また、条件データは、解生成部２７４から受付けたその解が何番目に生成された解であるのかという上述の情報（なお、この情報は、その条件データが対応付けられた暗号化切断データのそれぞれが、何番目の解に基づいて生成された鍵とアルゴリズムで暗号化されたのかということを示すものである）を含んでいる場合がある。ただし、条件データに含まれるその解が何番目に生成された解であるかという情報は、すべての解について含まれている必要はない。復号化処理装置２で復号化が許容される暗号化切断データを暗号化する際に使用された解のそれぞれが何番目に生成された解であるかという情報が含まれていれば足りる。

条件データが含んでいる対応付けられた暗号化切断データの復号化を許容する場合の条件と、その対応付けられた暗号化切断データの復号化を禁止する場合の条件は、この実施形態では、以下の（Ａ）～（Ｄ）のいずれか、またはそれらの組合わせである。

（Ａ）暗号化切断データの復号化を行うことが許容又は禁止された復号化処理装置を特定するための情報

（Ｂ）暗号化切断データの少なくとも一つについての復号化を行うことが許容又は禁止されたユーザを特定するための情報

（Ｃ）暗号化切断データの復号化が許容される時期に関する情報と、暗号化切断データの少なくとも一つについての復号化が禁止される時期に関する情報の少なくとも一方

（Ｄ）複数の暗号化切断データのうちのどれの復号化を許容するかという情報、又は複数の暗号化切断データのうちのどれの復号化を禁止するかという情報

生成された条件データは、暗号化部２７３に送られ、そこで暗号化されて暗号化条件データにされるようになっている。

【００４５】

基本条件データ生成部２７８は、例えばユーザが操作した入力装置から、インタフェイス部２７１を介して受付けたデータに基づいて、基本条件データを生成するものである。

基本条件データは、復号化処理装置２で、暗号化条件データの復号化を許容する場合の条件と、暗号化条件データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含んでいる。この実施形態における暗号化条件データは複数であるので、この実施形態における基本条件データは、復号化処理装置２で、複数の暗号化条件データのうちのどれの復号化を許容するのかという条件と、複数の暗号化条件データのどれの復号化を禁止するのかという条件の少なくとも一方についてのデータを含む基本条件データを生成するようになっている。

より具体的には、基本条件データは、解生成部２７４から受付けたその解が何番目に生成された解であるのかという上述の情報（なお、この情報は、復号化処理装置２で復号が許される暗号化条件データがのそれぞれが、何番目の解に基づいて生成された鍵とアルゴリズムで暗号化されたのかということを示すものである。）を含んでいる場合がある。ただし、この実施形態では、基本条件データに含まれる解が生成された順番を示す情報は、復号化処理装置２で復号が許される暗号化条件データを暗号化したときに使用された解が生成された順番を示す情報のみである。

基本条件データ生成部２７８は、生成した基本条件データを、接続部２８０に送るようになっている。

【００４６】

ヘッダ生成部２７９は、例えばユーザが操作した入力装置から、インタフェイス部２７１を介して受付けたデータに基づいて、暗号化データのヘッダとなるヘッダデータを生成するものである。

ヘッダデータには、暗号化データの送信元となる暗号化処理装置１のアドレス、暗号化データの送信先となる復号化処理装置２のアドレスなどが記載されている。

ヘッダ生成部２７９は、生成したヘッダデータを、接続部２８０に送るようになっている。

【００４７】
接続部２８０は、暗号化部２７３で平文切断データを暗号化することによって生成された暗号化切断データを接続して一まとめの暗号化データとする機能を有している。この実施形態の接続部２８０は、暗号化部２７３から受付けた暗号化切断データの他に、暗号化部２７３から受付けた暗号化条件データ、基本条件データ生成部２７８が生成した基本条件データ、ヘッダ生成部２７９が生成したヘッダデータを接続することで、一まとめの暗号化データとするようになっている。
暗号化データのデータ構造は、図４に例示したようにされる。なお、暗号化切断データ５０４の数は、実際はずっと多数であるが、図示の都合上、図４ではその数をかなり少なく書いている。
暗号化データは、図４（Ａ）、（Ｂ）に示したように、その先頭（図４においては左側が暗号化データの先頭にあたる。）に、上述のヘッダデータ５０１が置かれている。
ヘッダデータ５０１の直後には上述の基本条件データ５０２が配されている。なお、基本条件データ５０２は、後述する暗号化条件データ５０３のうちの最も前方に位置するものよりも前方に置かれている必要がある。それ故、図４（Ａ）、（Ｂ）に示した暗号化データでは、ヘッダデータ５０１の直後に基本条件データ５０２が置かれている。もっとも、ヘッダデータ５０１内に基本条件データ５０２を置くようにしても構わない。
図４（Ａ）、（Ｂ）に示した暗号化データとも、基本条件データ５０２の後に暗号化条件データ５０３と、暗号化切断データ５０４が続いている。
図４（Ａ）の暗号化データでは、基本条件データ５０２の後に複数の暗号化条件データ５０３が続いており、更にその後に複数の暗号化切断データ５０４が配されている。
図４（Ｂ）の暗号化データでは、基本条件データ５０２の後に、暗号化条件データ５０３と暗号化切断データ５０４が入り組んで配されている。ただし、暗号化条件データ５０３は、その元となった条件データが対応付けられていた平文切断データを暗号化して生成された暗号化切断データ５０４よりも前方に位置するようにされている。
なお、図４（Ａ）、（Ｂ）において暗号化条件データ５０３から暗号化切断データ５０４に向けて引いてある矢印は、矢印の基端に位置する暗号化条件データ５０３の元となった条件データが、矢印の先端に位置する暗号化切断データ５０４の元となった平文切断データと対応付けられているということを示している。
接続部２８０で生成された暗号化データは、インタフェイス部２７１に送られ、そこから、バス２９を介して通信装置２８に送られ、更にネットワークＮ経由で復号化処理装置２に送られるようになっている。
【００４８】
次に、復号化処理装置２の構成について説明する。
復号化処理装置２のハードウエア構成は、図５に示したとおりになっている。
復号化処理装置２は、ＣＰＵ３１、ＲＯＭ３２、ＨＤＤ３３、ＲＡＭ３４、入力装置３５、表示装置３６、復号化装置３７、通信装置３８、及びバス３９を備えている。復号化処理装置２におけるＣＰＵ３１、ＲＯＭ３２、ＨＤＤ３３、ＲＡＭ３４、入力装置３５、表示装置３６、及びバス３９のそれぞれは、暗号化処理装置１におけるＣＰＵ２１、ＲＯＭ２２、ＨＤＤ２３、ＲＡＭ２４、入力装置２５、表示装置２６、及びバス２９とそれぞれ同一に構成され、同様の機能を有するようにされている。復号化処理装置２のＨＤＤ３３には、復号化処理装置２のＭＡＣアドレスが保持されている。
なお、復号化処理装置２の通信装置３８は、暗号化処理装置１から送信された暗号化データを、ネットワークＮを介して受付けることができるようになっている。
【００４９】
復号化装置３７は、暗号化処理装置１から受取った暗号化データを復号化するものであり、図６に示されたように構成されている。
復号化装置３７は、インタフェイス部３７１、前処理部３７２、復号化部３７３、解生成部３７４、アルゴリズム生成部３７５、鍵生成部３７６、条件データ解析部３７７、基本条件データ解析部３７８、接続部３７９、及びタイマー３８０から構成される。

【００５０】
インタフェイス部３７１は、バス３９を介して、通信装置３８から暗号化データを受取るようになっており、受取った暗号化データを前処理部３７２に送るようになっている。
他方、インタフェイス部３７１は、後述するように、接続部３７９から処理対象データを受取るようになっており、受取った処理対象データをバス３９に送るようになっている。
前処理部３７２は、インタフェイス部３７１を介してバス３９から受取った暗号化データからヘッダデータを取除くとともに、基本条件データを取り出し、取り出した基本条件データを基本条件データ解析部３７８に送るようになっている。
また、前処理部３７２は、後述するような条件下で暗号化データから暗号化条件データを取り出し、それを復号化部３７３に送るようになっている。
また、前処理部３７２は、後述するような条件下で暗号化切断データを取り出し、それを復号化部３７３に送るようになっている。
前処理部３７２は、暗号化条件データと暗号化切断データを、暗号化処理装置１における基準ビット数と同じビット数に切断して、それを復号化部３７３に送るようになっている。
【００５１】
復号化部３７３は、前処理部３７２から受付けた暗号化条件データと暗号化切断データを復号化する機能を有している。なお、この実施形態における復号化部３７３は、復号化の処理を行う場合の処理単位である基準ビット数が、暗号化処理装置１と同じになるようにして固定されている。この実施形態における基準ビット数は、これには限られないが８ビットとなっている。復号化の処理の詳細については後で述べる。
【００５２】
解生成部３７４は、解を順次生成するものである。この解生成部３７４が生成する解は、上述したように、同じ順番で生成された解同士を比較すれば、暗号化処理装置１の解生成部３７４が生成した解と同じになるっている。生成された解は、前処理部３７２と、アルゴリズム生成部３７５と、鍵生成部３７６とに送られる。
アルゴリズム生成部３７５は、解生成部３７４から受付けた解に基づいてアルゴリズムを生成するものである。このアルゴリズムは、復号化部３７３で、復号化処理を行うときに使用されるものである。復号化処理装置２におけるアルゴリズム生成部３７５が生成するアルゴリズムは、暗号化処理装置１におけるアルゴリズム生成部２７５で同じ順番で生成されたアルゴリズムと同じものとなるようにされている。
鍵生成部３７６は、解生成部３７４から受付けた解に基づいて鍵を生成するものである。鍵は、復号化部３７３で、復号化処理を行うときに使用されるものである。復号化処理装置２における鍵生成部３７６が生成する鍵は、暗号化処理装置１における鍵生成部２７６で同じ順番で生成された鍵と同じものとなるようにされている。
【００５３】
条件データ解析部３７７は、復号化部３７３から送られた条件データを受付け、その条件データに示された内容を解析するものである。
条件データ解析部３７７が解析した条件データの内容についての情報は、解生成部３７４、又は復号化部３７３に送られるようになっている。
【００５４】
基本条件データ解析部３７８は、前処理部３７２から送られた基本条件データを受付け、その基本条件データに示された内容を解析するものである。
基本条件データ解析部３７８が解析した基本条件データの内容についての情報は、解生成部３７４、又は復号化部３７３に送られるようになっている。
【００５５】
復号化処理装置２における接続部３７９の機能は、暗号化処理装置１のそれと略同様である。接続部３７９は、復号化部３７３が暗号化切断データを復号化することによって生成した平文切断データを一まとめにして処理対象データを生成する。この処理対象データ

は、暗号化処理装置１で暗号化された元の処理対象データと同じか、その一部になっている。この処理対象データは、バス３９を介してＨＤＤ３３に送られるようになっている。

【００５６】

タイマー３８０は、現在の時刻を計測する時計である。タイマー３８０は、必要に応じて、条件データ解析部３７７、基本条件データ解析部３７８にその時点の時刻についての時刻データを送る。

【００５７】

次に、この暗号化システムで行われる処理の流れについて説明する。

図７を用いて概略で説明すると、このデータ処理システムで行われる処理の流れは以下のとおりである。

まず、暗号化処理装置１が処理対象データを暗号化して暗号化データを生成する（Ｓ１１０）。

次いで、その暗号化処理装置１がその暗号化データを復号化処理装置２に送る（Ｓ１２０）。

次いで、暗号化データを受取った復号化処理装置２が、その暗号化データを復号化して処理対象データにする（Ｓ１３０）。

【００５８】

まず、暗号化処理装置１が処理対象データを暗号化して暗号化データを生成する上述のＳ１１０の過程について、図８を参照しながら詳しく説明する。

【００５９】

まず、処理対象データの読み出しが行われる（Ｓ１１０１）。処理対象データは暗号化処理装置１から復号化処理装置２に送信する必要のあるデータであればどのようなものでもよい。この実施形態では、処理対象データはＨＤＤ２３に記録されているものとする。外部記録媒体などの他の記録媒体から暗号化処理装置１に読み込ませた何らかのデータを処理対象データとしてもよい。

処理対象データを復号化処理装置２へ送れという内容のコマンドが例えば入力装置２５から入力された場合、ＣＰＵ２１は、処理対象データをＨＤＤ２３から読み出し、バス２９を経て、暗号化装置２７に送る。この処理対象データは、より詳細には、バス２９から、暗号化装置２７内のインタフェイス部２７１に送られ、そこから前処理部２７２に送られることになる。

処理対象データの読出しと前後して、その処理対象データを暗号化して得られる暗号化データをどの復号化処理装置２へ送るのかという宛先情報と、条件データを生成するための情報と、基本条件データを生成するための情報が入力装置２５から入力される（Ｓ１１０２）。これら宛先情報と、条件データを生成するための情報と、基本条件データを生成するための情報は、ＣＰＵ２１によって、バス２９を経て暗号化装置２７に送られる。より詳細には、宛先情報はインタフェイス部３７１を経てヘッダ生成部２７９へ、条件データを生成するための情報はインタフェイス部３７１を経て条件データ生成部２７７へ、基本条件データを生成するための情報はインタフェイス部３７１を経て基本条件データ生成部２７８へ、それぞれ送られる。

【００６０】

宛先情報を受付けたヘッダ生成部２７９は、ヘッダデータを生成し、条件データを生成するための情報を受付けた条件データ生成部２７７は条件データを生成し、基本条件データを生成するための情報を受付けた基本条件データ生成部２７８は基本条件データを生成する（Ｓ１１０３）。

ヘッダデータ、条件データ、基本条件データは、上述したような内容である。

ただし、条件データ又は基本条件データが、解が何番目に生成されたのかという情報を含むものである場合には、条件データ生成部２７７と、基本条件データ生成部２７８は、解生成部２７４からその解が何番目に作られたものであるかという情報を受付けてから、条件データと基本条件データの生成を行う。なお、同一の処理対象データに対して、複数回暗号化を行い、それにより生成された複数の暗号化データを異なる複数の復号化処理装

置２に送る場合、それぞれの暗号化データに暗号化してから暗号化条件データとして含めることになる条件データは、互いに異なるものとすることができる。基本条件データも同様である。

この実施形態では、各条件データには、

（Ａ）暗号化切断データの復号化を行うことが許容又は禁止された復号化処理装置を特定するための情報

（Ｂ）暗号化切断データの復号化を行うことが許容又は禁止されたユーザを特定するための情報

（Ｃ）暗号化切断データの少なくとも一つについての復号化が許容される時期に関する情報と、暗号化切断データの少なくとも一つについての復号化が禁止される時期に関する情報の少なくとも一方

（Ｄ）複数の暗号化切断データのうちのどれの復号化を許容するかという情報、又は複数の暗号化切断データのうちのどれの復号化を禁止するかという情報

のうちの一つと、その条件データと対応付けられた平文切断データを暗号化したときに用いられた鍵、及びアルゴリズムを生成したときに用いた解が何番目に生成されたものかという情報が含まれているものとする。なお、平文切断データを暗号化したときに用いられた鍵、及びアルゴリズムを生成したときに用いた解が何番目に生成されたものかという情報に代えて、その条件データと対応付けられた平文切断データを生成したときに用いられた鍵、及びアルゴリズムを生成したときに用いた解そのもの、或いは、その条件データと対応付けられた平文切断データを暗号化したときに用いられた鍵、及びアルゴリズムそのものを条件データに含めることも可能である。

また、この実施形態における基本条件データには、復号化処理装置２で、各暗号化条件データの復号化が許容されるための条件と、暗号化条件データの復号化が禁止されるための条件の少なくとも一方についてのデータ（これらは、上記（Ａ）から（Ｄ）と同等のものとすることができる。）と、各暗号化条件データを暗号化したときに用いられた鍵、及びアルゴリズムを生成したときに用いた解が何番目に生成されたものかという情報が含まれているものとする。なお、各暗号化条件データを暗号化したときに用いられた鍵、及びアルゴリズムを生成したときに用いた解が何番目に生成されたものかという情報に代えて、各暗号化条件データを暗号化したときに用いられた鍵、及びアルゴリズムを生成したときに用いた解そのもの、或いは、各暗号化条件デーを暗号化したときに用いられた鍵、及びアルゴリズムそのものを基本条件データに含めることも可能である。

ヘッダデータはヘッダ生成部２７９から、基本条件データは基本条件データ生成部２７８から、接続部２８０へ送られる。また、条件データは条件データ生成部２７７から、暗号化部２７３へ送られる。

【００６１】

前処理部２７２で、処理対象データは、所定のビット数毎に切断され、平文切断データにされる（Ｓ１１０４）。前処理部２７２は、必要に応じて、平文切断データにダミーデータを含める。

処理対象データから平文切断データを生成する方法は一通りであってもよいが、この実施形態では、以下の３通りの方法のいずれかで、処理対象データから平文切断データを生成するようになっている。

Ｘ）処理対象データを基準ビット数よりも短い一定のビット数に切断して平文切断データにするとともに、そのすべてが基準ビット数よりもビット数が短くされている平文切断データのそれぞれの一定の位置にダミーデータを含める場合

Ｙ）処理対象データを基準ビット数よりも短いビット数の一定のビット数に切断して平文切断データにするとともに、そのすべてが基準ビット数よりもビット数が短くされている平文切断データのそれぞれの異なる位置にダミーデータを含める場合

Ｚ）処理対象データを基準ビット数と同じかそれよりも短いビット数に切断して平文切断データにするとともに、基準ビット数よりもビット数の短い平文切断データのそれぞれにダミーデータを含める場合

【００６２】
上述した３通りの方法のどれで、処理対象データから平文切断データを生成するかは、解生成部２７４が生成した解によって決定されるようになっている。
【００６３】
そこで、解生成部２７４がどのように解を生成するかについて先に説明することにする。
解生成部２７４は、インタフェイス部２７１がバス２９から処理対象データを受付けた場合、その情報をインタフェイス部２７１から受付ける。
これを契機に解生成部２７４は、解の生成を開始する。この実施形態では、解生成部２７４は、処理対象データがインタフェイス部２７１で受付けられるたびに、解を生成するようになっている。なお、これには限られないが、この実施形態における解は８行８列の行列（Ｘ）である。
【００６４】
解生成部２７４は、必ずしもそうなっている必要はないが、この実施形態では、解を、非線形遷移するようなものとして連続して発生させる。この解は、結果として擬似乱数となる。
非線形遷移するように解を連続して発生させるには、例えば、（１）解の生成の過程に、過去の解のべき乗の演算を含む、（２）解の生成の過程に、過去の２つ以上の解の掛け合わせを含む、或いは、（１）と（２）を組み合わせるなどの手法が考えられる。
【００６５】
この実施形態では、解生成部２７４は、初期行列として、第０１解（X_{01}）と第０２解（X_{02}）を予め定められたものとして持っている（例えば、第０１解と第０２解は、ＨＤＤ２３やＲＯＭ２２などの所定のメモリに記録されている）。なお、暗号化処理装置１が有する初期行列は、後述するように、復号化処理装置２が有する初期行列と同じである。
【００６６】
解生成部２７４は、この初期行列を、解生成部２７４が保持している解生成用アルゴリズムに代入して、第１解（X_1）を以下のように生成する。
第１解（X_1）＝$X_{02}\,X_{01}$＋α（α＝８行８列の行列）
これが最初に生成される解である。
次にインタフェイス部２７１がバス２９から処理対象データを受付けた場合、解生成部２７４は、第２解（X_2）を以下のように生成する。
第２解（X_2）＝$X_1\,X_{02}$＋α
同様に、インタフェイス部２７１がバス２９から処理対象データを受付けるたびに、解生成部２７４は、第３解、第４解、……第Ｎ解を、以下のように生成する。
第３解（X_3）＝$X_2\,X_1$＋α
第４解（X_4）＝$X_3\,X_2$＋α
：
第Ｎ解（X_N）＝$X_{N-1}\,X_{N-2}$＋α
このようにして生成された解は、前処理部２７２、アルゴリズム生成部２７５、及び鍵生成部２７６に送られるとともに、解生成部２７４で保持されることになる。この実施形態では、第Ｎ解（X_N）を生成するために、第Ｎ－１解（X_{N-1}）と第Ｎ－２解（X_{N-2}）を、要するに、その直前に生成された２つの解を用いる。したがって、解生成部２７４は、新しい解を生成するにあたって、過去に生成された直近２つの解を保持していなければならない（又は、解生成部２７４ではない他の何者かがこれら２つの解を保持していなければならない）。逆に過去に生成された直近２つの解よりも古い解は、新しい解を生成するために今後使用されることのないものである。そこで、この実施形態では、常に過去２つの解を解生成部２７４で保持することとするが、新しい解が生成されることで直近３つ目の解となったそれまで直近２つ目の解であった解を、その解が記録されていた所定のメモリなどから消去することとしている。ただし、初期行列だけは消去しないで保持

しておく。
なお、このように生成される解は、非線形遷移するカオス的なものとなり、擬似乱数となる。
【００６７】
非線形遷移を起こさせるには、第Ｎ解を求める際に、上述した
第Ｎ解（X_N）＝X_{N-1} X_{N-2}＋α
という式を用いる他に、以下のような式を用いることが考えられる。
例えば、
（ａ）第Ｎ解（X_N）＝（X_{N-1}）^{P}
（ｂ）第Ｎ解（X_N）＝（X_{N-1}）^{P}（X_{N-2}）^{Q}（X_{N-3}）^{R}（X_{N-4}）^{S}
（ｃ）　第Ｎ解（X_N）＝（X_{N-1}）^{P}＋（X_{N-2}）^{Q}
などである。
なお、Ｐ、Ｑ、Ｒ、Ｓはそれぞれ所定の定数である。また、数式（ａ）又は（ｃ）を用いる場合には、２つ、数式（ｂ）を用いる場合には４つの初期行列を、解生成部２７４は有している。
また、上述したαは定数であったが、これを、特定の変化する環境情報とすることもできる。この環境情報は、時間の経過にしたがって次々と自然発生する情報であって離れた場所でも共通して取得できる情報であり例えば、特定地方の天気に基づいて定められる情報、特定の時間に放送されるあるテレビ局のテレビジョン放送の内容に基づいて定められる情報、特定のスポーツの結果によって定められる情報などである。
このような環境情報から、上述のαを次々に作成し共通情報を生成することにすれば、通信の秘匿性をより高められる。
上述した、数式（ａ）～（ｃ）の右辺に、α（これは環境情報から生成されたものでもよい。）を加えることももちろん可能である。
【００６８】
上述したように生成された解（即ち、上述の解）を受付けた前処理部２７２は、それにしたがって、上述のＸ）、Ｙ）、Ｚ）のいずれの方法で平文切断データを生成するかを決定する。この実施形態では、これには限られないが、解である８行８列の行列を構成する数字を足し合わせた和を３で割り、その余りが０のときはＸ）の方法で、その余りが１のときはＹ）の方法で、その余りが２のときはＺ）の方法で、それぞれ平文切断データを生成することとしている。
Ｘ）の方法で平文切断データを生成する場合には、前処理部２７２は、インタフェイス部２７１から受付けた処理対象データを先頭から順に、基準ビット数よりも短い一定のビット数（この実施形態では、７ビット）で切断することで、平文切断データを生成していく。また、前処理部２７２は、平文切断データの一定の位置に、ダミーデータを埋め込んでいく。なお、ダミーデータを埋め込む平文切断データにおける位置は、変化してもよいし、固定されていてもよい。後者の場合、ダミーデータが埋め込まれる位置は、例えば、平文切断データの先頭や末尾、或いは２ビット目や３ビット目などの所定の中間の位置とすることができる。このダミーデータは、処理対象データとは無関係のデータであればどのようなものでも構わない。例えば、常に０というデータを埋め込んでいく、又は１というデータを埋め込んでいく、或いは１と０というデータを交互に埋め込んでいくなどの処理が考えられる。更に他の例として、上述の解に基づいて、どのようなダミーデータを埋め込んでいくかを決定することもできる。例えば、解である８行８列の行列を構成する数字を足し合わせた和を９で割り、その余りが０のときは０、０、０、０…と０を連続し、その余りが１のときは、０、１、０、１…と１つおきに１を挟み込み、その余りが２のときは、０、０、１、０、０、１…と２つおきに１を挟み込み、同様に、余りが３のときは３つおきに、余りが４のときは４つおきに、……余りが９のときは９つおきに１を挟み込むようなものとすることができる。
Ｙ）の方法で平文切断データを生成する場合には、前処理部２７２は、処理対象データを基準ビット数よりも短いビット数の一定のビット数（例えば、７ビット）に切断して平

文切断データにするとともに、そのすべてが基準ビット数よりもビット数が短くされている平文切断データにダミーデータを含める。この場合、ダミーデータの埋め込まれる位置は、固定でもよいし、平文切断データのそれぞれについて、１ビット目、２ビット目、３ビット目…８ビット目、１ビット目、２ビット目…８ビット目、と順に移動していくような、規則的に変化するものでも、或いは、ランダムに変化するようなものであってもよい。ダミーデータの埋め込まれる位置がランダムに変化する場合には、例えば、ダミーデータの埋め込まれる位置が、解に基づいて決定されるようになっていてもよい。

解によって、ダミーデータの埋め込まれる位置を決定する方法としては、例えば、解である８行８列の行列を構成する数字を足し合わせた和を８で割り、その余りが０のときは、平文切断データ１つおきに、先頭と末尾に交互にダミーデータを埋め込む、余りが１のときは先頭にダミーデータが埋め込まれた平文切断データと、末尾にダミーデータが埋め込まれた平文切断データが２つおきになるようにする、余りが２のときは先頭にダミーデータが埋め込まれた平文切断データと、末尾にダミーデータが埋め込まれた平文切断データが３つおきになるようにする、……余りが７のときは先頭にダミーデータが埋め込まれた平文切断データと、末尾にダミーデータが埋め込まれた平文切断データが８つおきになるようにする、という処理を行うようにすることができる。先頭と末尾のように、ダミーデータを埋め込む位置を固定せずに、その位置を更に動かすようにすることもできる。

Ｚ）の方法により平文切断データを生成する場合には、処理対象データを基準ビット数と同じかそれよりも短いビット数に切断する。この切断は、処理対象データを、８ビットよりも短いランダムな長さに切断することにより行うことができ、例えば、解である８行８列の行列を構成する数字を足し合わせた和を８で割り、その余りが０のときは処理対象データのその時点における先頭部分を８ビットで切断し、その余りが１のときは処理対象データのその時点における先頭部分を１ビットで切断し、その余りが２のときは処理対象データのその時点における先頭部分を２ビットで切断し、…その余りが７のときは処理対象データのその時点における先頭部分を７ビットで切断するようにすることができる。また、前処理部２７２は、これにより生成された平文切断データのうち、基準ビット数よりもビット数の短い平文切断データのそれぞれに、ダミーデータを埋め込む。この場合のダミーデータの埋め込み位置は先頭、末尾などの特定の位置であってもよいし、例えば解によって特定される変化する所定の位置であってもよい。

いずれにせよ、このようにして生成された平文切断データは、生成された順番で、暗号化部２７３に送られる。

【００６９】

平文切断データの生成と並行して、アルゴリズム生成部２７５が、平文切断データを暗号化する際に用いられるアルゴリズムを生成する。

この実施形態におけるアルゴリズム生成部２７５は、アルゴリズムを、解に基づいて生成する。

この実施形態においては、アルゴリズム生成部２７５は、アルゴリズムを以下のようなものとして生成する。

この実施形態におけるアルゴリズムは、『８ビットのデータである平文切断データを１行８列の行列Ｙとした場合に、解である８行８列の行列Ｘをａ乗してから、時計周りにｎ×９０°だけ回転させた行列に、Ｙを掛け合わせて求められるもの』と定義される。

ここで、ａは所定の定数とされる場合もあるが、この実施形態では、解に基づいて変化する数字である。つまり、この実施形態におけるアルゴリズムは、解に基づいて変化する。例えばａは、８行８列の行列である解に含まれている行列の要素である数すべてを足し合わせて得られる数を５で割った場合の余り（ただし、余りが０の場合はａ＝１とする）のように定めることができる。

また、上述のｎは、鍵によって定められる所定の数である。鍵が一定の数であればｎは固定であるが、以下に説明するように、鍵は解に基づいて変化する。つまり、この実施形態では、このｎも解に基づいて変化するようになっている。

もっとも、アルゴリズムを他のものとして決定することもできる。

この実施形態では、アルゴリズム生成部２７５は、解生成部２７４から解を受取るたびにアルゴリズムを生成し、それを暗号化部２７３に送る。

【００７０】

平文切断データの生成と並行して、鍵生成部２７６が、平文切断データを暗号化する際に用いられる鍵を生成する。

鍵生成部２７６は、鍵を解に基づいて生成する。

この実施形態においては、鍵生成部２７６は、鍵を以下のようなものとして生成する。

この実施形態における鍵は、８行８列の行列である解に含まれている行列の要素である数すべてを足し合わせて得られる数とされる。したがって、鍵は、この実施形態では、解に基づいて変化する。

なお、鍵を他のものとして決定することもできる。

この実施形態では、鍵生成部２７６は、解生成部２７４から解を受取るたびに鍵を生成し、それを暗号化部２７３に送る。

【００７１】

暗号化部２７３は、アルゴリズム生成部２７５から受付けたアルゴリズムと、鍵生成部２７６から受付けた鍵に基づいて、条件データ生成部２７７から受付けた条件データと、前処理部２７２から受付けた平文切断データを暗号化する（Ｓ１１０５）。

この実施形態では、条件データを先に暗号化し、続けて平文切断データを暗号化することとしている。

アルゴリズムは、上述したように、『８ビットのデータである平文切断データを１行８列の行列Ｙとした場合に、解である８行８列の行列Ｘをａ乗してから、時計周りにｎ×９０°だけ回転させた行列に、Ｙを掛け合わせて求められるもの』という決まりであり、鍵であるｎは、上述したような数である。

例えば、ａが３、ｎが６である場合には、Ｘを３乗して得られる８行８列の行列を、６×９０°＝５４０°だけ時計回りに回転させることによって得られた８行８列の行列に、条件データ、又は平文切断データを掛け合わせて暗号化が行われる。

これにより生成されたデータが、暗号化条件データと、暗号化切断データである。

【００７２】

暗号化条件データと、暗号化切断データは、接続部２８０に送られる。接続部２８０は、これらとヘッダデータと、基本条件データを、図４に示したような構造で一まとめに接続し、暗号化データを生成する（Ｓ１１０６）。このときの暗号化切断データの並び順は、元の平文切断データの並び順に対応したものとされる。

【００７３】

以上のようにして、まず、暗号化処理装置１が処理対象データを暗号化して暗号化データを生成するＳ１１０の過程が終了する。

【００７４】

このようにして生成された暗号化データは、バス２９を介して暗号化処理装置１内の通信装置２８に送られる。

通信装置２８は、その暗号化データを、暗号化データのヘッダデータに含まれているＭＡＣアドレスで指定された復号化処理装置２へネットワークＮを介して送る。

これにより、上述したＳ１２０の過程が実行される。

【００７５】

この暗号化データを受取った復号化処理装置２にて、暗号化データを復号化して処理対象データに戻すＳ１３０の過程が実行される。

以下、この復号化の過程について図９を参照しながら詳述する。

【００７６】

復号化処理装置２に送られた暗号化データは、復号化処理装置２の通信装置３８が受付ける（Ｓ１３０１）。

通信装置３８は、この暗号化データを復号化装置３７に送る。

【００７７】

復号化装置３７内の前処理部３７２が、インタフェイス部３７１を介してこの暗号化データを受取る。

前処理部３７２は、受付けた暗号化データから基本条件データを取出して（Ｓ１３０２）、それを基本条件データ解析部３７８に送る。前処理部３７２は、暗号化条件データを、復号化部３７３に送る。

【００７８】

基本条件データ解析部３７８は、基本条件データの示す内容を解析する（Ｓ１３０３）。基本条件データ解析部３７８は、この情報から判断されるどの暗号化条件データを復号化するのかという情報を、復号化部３７３に送る。

また、上述したように、基本条件データには、各暗号化条件データを暗号化したときに用いられた鍵、及びアルゴリズムを生成したときに用いた解が何番目に生成されたものかという情報が含まれている。基本条件データ解析部３７８は、基本条件データに含まれていた各暗号化条件データを暗号化したときに用いられた鍵、及びアルゴリズムを生成したときに用いた解が何番目に生成されたものかという情報を解生成部３７４に送る。ただし、解生成部３７４に送られるのは、基本条件データに含まれた条件により復号化が許容されている、或いは復号化が禁止されていない暗号化条件データを暗号化したときに用いられた鍵、及びアルゴリズムを生成したときに用いた解が何番目に生成されたものかという情報のみである。

【００７９】

解生成部３７４は、この情報に基づいて、暗号化条件データを復号化するための解を生成する（Ｓ１３０４）。

復号化処理装置２の復号化装置３７内にある解生成部３７４で行われる解の生成は、暗号化処理装置１の解生成部２７４で行われたのと同じ過程を経て行われる。

なお、この解生成部３７４は、上述したように、その解生成部３７４を含む復号化装置３７と対応付けられた暗号化処理装置１の解生成部２７４が持っていたのと同様の初期行列と、解生成用アルゴリズムを持っている。したがって、復号化処理装置２の復号化装置３７内で生成される解は、生成された順番が同じもの同士を比較すれば、暗号化処理装置１の暗号化装置２７内で生成される解と同じになっている。

生成された解は、解生成部３７４から、アルゴリズム生成部３７５と、鍵生成部３７６とに送られる。

アルゴリズム生成部３７５と、鍵生成部３７６は暗号化条件データを復号化するためのアルゴリズムと鍵を生成する（Ｓ１３０５）。

アルゴリズム生成部３７５は、受付けた情報に基づいてアルゴリズムを生成する。復号化処理装置２のアルゴリズム生成部３７５がアルゴリズムを生成する過程は、暗号化処理装置１のアルゴリズム生成部２７５がアルゴリズムを生成する過程と同じである。同じ解に基づいて生成されたアルゴリズムは、暗号化処理装置１のアルゴリズム生成部２７５で生成されたものと常に同じになるようになっている。

他方、鍵生成部３７６は、受付けた情報に基づいて鍵を生成する。復号化処理装置２の鍵生成部３７６が鍵を生成する過程は、暗号化処理装置１の鍵生成部２７６が鍵を生成する過程と同じである。同じ解に基づいて生成された鍵は、暗号化処理装置１の鍵生成部２７６で生成されたものと常に同じになるようになっている。

ところで、復号化処理装置２では、暗号化処理装置１で条件データを暗号化したときに使用された解が何番目に生成されたものかという情報に基づいて暗号化処理装置１で生成されたのと同じ解を生成し、それに基づいてアルゴリズムと鍵を生成することとしている。したがって、復号化処理装置２は、暗号化処理装置１で条件データを暗号化したときに使用されたアルゴリズムと鍵と同じものを生成することができるのである。

生成されたアルゴリズムは、アルゴリズム生成部３７５から復号化部３７３へ送られる。また、生成された鍵は、鍵生成部３７６から復号化部３７３へ送られる。

【００８０】

なお、基本条件データに、各条件データを暗号化したときに用いられた鍵、及びアルゴ

リズムを生成したときに用いた解そのものが含まれている場合には、このデータをアルゴリズム生成部３７５と、鍵生成部２７６に送ればよい。この場合、アルゴリズム生成部３７５と、鍵生成部３７６で生成されたアルゴリズムは、アルゴリズム生成部３７５から復号化部３７３へ送られる。また、生成された鍵は、鍵生成部３７６から復号化部３７３へ送られる。

また、基本条件データに、各条件デーを暗号化したときに用いられた鍵、及びアルゴリズムそのものを条件データに含めた場合には、それらを復号化部３７３へ送るようにする。

【００８１】

次いで、アルゴリズム生成部３７５と鍵生成部３７６から受付けたアルゴリズムと鍵を用いて、復号化部３７３で、暗号化条件データの復号化が行われる（Ｓ１３０６）。

より詳細には、復号化部３７３は、アルゴリズム生成部３７５から受付けたアルゴリズム（『８ビットのデータである条件データを１行８列の行列Ｙとした場合に、解である８行８列の行列Ｘをａ乗してから、時計周りにｎ×９０°だけ回転させた行列に、Ｙを掛け合わせて求められるものが暗号化条件データである』という定義）に基づいて、復号化処理を行うためのアルゴリズム（『暗号化条件データを１行８列の行列Ｚと見た場合に、解である８行８列の行列Ｘをａ乗してから、時計周りにｎ×９０°だけ回転させた行列の逆行列に、Ｙを掛け合わせて求められるものが条件データである』という定義）を生成し、鍵を用いて上述の定義にしたがった演算を行うことで、復号化の処理を行う。

こうして、復号化部３７３では、前処理部３７２から送られた暗号化条件データを復号化し、条件データを生成する。なお、ここで復号化される暗号化条件データは、基本条件データに含まれた条件により復号化が許容されている、或いは復号化が禁止されていない暗号化条件データのみである。

【００８２】

次いで、復号化された条件データは、条件データ解析部３７７に送られる。

条件データ解析部３７７は、条件データの示す内容を解析する（Ｓ１３０７）。上述したように、条件データには、下記（Ａ）～（Ｄ）の少なくとも一つと、各暗号化切断データを暗号化したときに用いられた鍵、及びアルゴリズムを生成したときに用いた解が何番目に生成されたものかという情報が含まれている。

条件データ解析部３７７は、まず、各暗号化切断データが、下記（Ａ）～（Ｄ）の条件に合致するか否かを判断する。

（Ａ）暗号化切断データの復号化を行うことが許容又は禁止された復号化処理装置を特定するための情報

（Ｂ）暗号化切断データの復号化を行うことが許容又は禁止されたユーザを特定するための情報

（Ｃ）暗号化切断データの少なくとも一つについての復号化が許容される時期に関する情報と、暗号化切断データの少なくとも一つについての復号化が禁止される時期に関する情報の少なくとも一方

（Ｄ）複数の暗号化切断データのうちのどれの復号化を許容するかという情報、又は複数の暗号化切断データのうちのどれの復号化を禁止するかという情報

例えば、（Ａ）の条件に合致するか否かを判断するにあたっては、条件データ解析部３７７は、その復号化処理装置２のＭＡＣアドレスをＨＤＤ３３からバス３９経由で読出し、その復号化処理装置２のＭＡＣアドレスと条件データに含まれていた暗号化切断データの復号化を行うことが許容又は禁止された復号化処理装置２のＭＡＣアドレスの情報とを対比する。

また、（Ｂ）の条件に合致するか否かを判断するにあたっては、例えば、各ユーザ毎に割振られたユニークなＩＤやパスワードをユーザに入力装置３５から入力させてからバス３９経由で受取り、そのＩＤやパスワードを、その復号化処理装置２の条件データに含まれていた、暗号化切断データの復号化を行うことが許容又は禁止されたユーザのＩＤやパスワードと対比する。

また、（Ｃ）の条件に合致するか否かを判断するにあたっては、例えば、タイマー３８０から時刻データを受付け、それによって示される現在時刻と、暗号化切断データの復号化を行うことが許容又は禁止された時期に関する情報とを対比する。

また、（Ｄ）の条件に合致するか否かを判断するにあたっては、各暗号化切断データが、条件データに含まれている、復号化を許容する暗号化切断データに該当するか、或いは復号化が禁止される暗号化切断データに該当するかという点を個別に判断する。

なお、説明を省略したが、以上の判断手法は、基本条件データに（Ａ）～（Ｄ）の条件が含まれている場合においては、基本条件データ解析部３７８でも同様に行われる。

結果的に、復号化が許容される条件に一つでも該当しなかった暗号化切断データ、及び復号化が禁止される条件に一つでも該当した暗号化切断データは、その復号化が許されないものと判断される。それ以外の暗号化切断データは、復号化が許容されたものと判断される。

条件データ解析部３７７は、この情報を復号化部３７３に送る。

また、条件データ解析部３７７は、条件データに含まれていた、アルゴリズム及び鍵が何番目に生成されたものかということについての情報を、解生成部３７４に送る。ただし、解生成部３７４に送られるのは、基本条件データに含まれた条件により復号化が許容されている、或いは復号化が禁止されていない暗号化条件データを暗号化したときに用いられた鍵、及びアルゴリズムを生成したときに用いた解が何番目に生成されたものかという情報のみである。

【００８３】

解生成部３７４は、受付けた情報に基づいて、暗号化切断データを復号化するための解を生成する（Ｓ１３０８）。

復号化処理装置２の復号化装置３７内にある解生成部３７４で行われる解の生成は、暗号化処理装置１の解生成部２７４で行われたのと同じ過程を経て行われる。

生成された解は、解生成部３７４から、前処理部３７２と、アルゴリズム生成部３７５と、鍵生成部３７６とに送られる。

【００８４】

アルゴリズム生成部３７５と、鍵生成部３７６は、暗号化切断データを復号化するためのアルゴリズムと鍵を生成する（Ｓ１３０９）。

アルゴリズム生成部３７５は、受付けた情報に基づいて、アルゴリズムを生成する。復号化処理装置２のアルゴリズム生成部３７５がアルゴリズムを生成する過程は、暗号化処理装置１のアルゴリズム生成部２７５がアルゴリズムを生成する過程と同じである。

他方、鍵生成部３７６は、受付けた情報に基づいて、鍵を生成する。復号化処理装置２の鍵生成部３７６が鍵を生成する過程は、暗号化処理装置１の鍵生成部２７６が鍵を生成する過程と同じである。

暗号化条件データを復号化するときに発生させた鍵とアルゴリズムと同じ理由で、暗号化切断データを復号化するときに復号化処理装置２で発生させる鍵とアルゴリズムは、暗号化処理装置１で発生させた鍵とアルゴリズムと同一のものとなる。

生成されたアルゴリズムは、アルゴリズム生成部３７５から復号化部３７３へ送られる。また、生成された鍵は、鍵生成部３７６から復号化部３７３へ送られる。

【００８５】

なお、条件データに、各条件データを暗号化したときに用いられた鍵を生成したとき、及びアルゴリズムを生成したときに用いられた解そのものが含まれている場合には、このデータをアルゴリズム生成部３７５と、鍵生成部３７６に送る。この場合、アルゴリズム生成部３７５で生成されたアルゴリズムと、鍵生成部３７６で生成された鍵は、アルゴリズム生成部３７５、鍵生成部３７６のそれぞれから、復号化部３７３へ送られる。

また、基本条件データに、各条件データを暗号化したときに用いられた鍵、及びアルゴリズムそのものが含められている場合には、それらを復号化部３７３へ送るようにする。

【００８６】

次いで、アルゴリズム生成部３７５と鍵生成部３７６から受付けたアルゴリズムと鍵を

用いて、復号化部３７３で、暗号化条件データの復号化が行われる（Ｓ１３１０）。その際に、必要な場合には、ダミーデータの除去が行われる。

暗号化切断データの復号化による平文切断データの生成は、暗号化条件データを復号化して条件データを生成する上述の過程と同様にして行われる。

ダミーデータの除去は、以下のように行われる。

上述したように、解生成部３７４で生成された解は前処理部３７２に送られている。この解は、暗号化処理装置１の前処理部２７２でどのようにしてダミーデータを平文切断データに埋め込んだのかを決定するときに使用されたものである。つまり、復号化装置３７の前処理部３７２がその時点で持っている解は、復号化処理装置２の復号化部３７３が復号化を終えた（或いは復号化を行っている、もしくは今から復号化をしようとしている）暗号化切断データ（より正確には、その暗号化切断データが暗号化される前の平文切断データ）にどのようにしてダミーデータを埋め込んだかを示すものである。

前処理部３７２は、復号化部３７３で復号化された平文切断データのどこにダミーデータが埋め込まれているかということについての情報を、復号化部３７３に送る。これを用いて、復号化部３７３は、ダミーデータを平文切断データの中から除く。

なお、ダミーデータの除去は、暗号化切断データを復号化して生成された平文切断データからではなく、暗号化切断データから除いても構わない。

なお、ここで復号化される暗号化切断データは、条件データに含まれた条件により復号化が許容されている、或いは復号化が禁止されていない暗号化切断データのみである。

【００８７】

次いで、復号化された平文切断データは、接続部３７９に送られる。接続部３７９は、受付けた平文切断データを接続して一まとめにすることで、処理対象データを生成する（Ｓ１３１１）。

このようにして、復号化処理装置２が暗号化データを復号化して処理対象データに戻すＳ１３０の過程が終了する。

【００８８】

生成された処理対象データは、接続部３７９からインタフェイス部３７１に送られ、バス３９を介して、例えばＨＤＤ３３に送られる。この処理対象データは、復号化処理装置２で適宜利用される。

【００８９】

＜変形例１＞

第１実施形態における暗号化システムの第１の変形例である変形例１について説明する。

この変形例１に係る暗号化システムは、基本的に、上述した暗号化システムと同一であるが、暗号化処理装置１における暗号化装置２７と、復号化処理装置２における復号化装置３７の一部の構成が、上述した暗号化システムに含まれていたものとは異なっている。

【００９０】

変形例１に係る暗号化処理装置１における暗号化装置２７は、図１０に示したように構成されている。

この暗号化装置２７が、第１実施形態の場合と異なるのは、第１実施形態におけるアルゴリズム生成部２７５が、第１アルゴリズム生成部２７５Ａと第２アルゴリズム生成部２７５Ｂに、第１実施形態における鍵生成部２７６が、第１鍵生成部２７６Ａと第２鍵生成部２７６Ｂに、それぞれ置き換えられているという点である。

第１アルゴリズム生成部２７５Ａと第２アルゴリズム生成部２７５Ｂはともに、アルゴリズム生成部２７５と同様にアルゴリズムを生成するものであるが、第１アルゴリズム生成部２７５Ａが平文切断データを暗号化するためのアルゴリズムを生成するものであるのに対して、第２アルゴリズム生成部２７５Ｂが条件データを暗号化するためのアルゴリズムを生成するためのものである点で異なっている。

第１鍵生成部２７６Ａと第２鍵生成部２７６Ｂはともに、鍵生成部２７６と同様に鍵を生成するものであるが、第１鍵生成部２７６Ａが平文切断データを暗号化するための鍵を

生成するものであるのに対して、第２鍵生成部２７６Ｂが条件データを暗号化するための鍵を生成するためのものである点で異なっている。

この変形例１では、平文切断データを暗号化する場合には、解生成部２７４から第１アルゴリズム生成部２７５Ａへ解が送られ、そこで平文切断データを暗号化するためのアルゴリズムが生成される。また、条件データを暗号化する場合には、解生成部２７４から第２アルゴリズム生成部２７５Ｂへ解が送られ、そこで条件データを暗号化するためのアルゴリズムが生成される。

また、この変形例１では、平文切断データを暗号化する場合には、解生成部２７４から第１鍵生成部２７６Ａへ解が送られ、そこで平文切断データを暗号化するための鍵が生成される。また、条件データを暗号化する場合には、解生成部２７４から第２鍵生成部２７６Ｂへ解が送られ、そこで条件データを暗号化するための鍵が生成される。

【００９１】

変形例１に係る復号化処理装置２における復号化装置３７は、図１１に示したように構成されている。

この復号化装置３７が、第１実施形態の場合と異なるのは、第１実施形態におけるアルゴリズム生成部３７５が、第１アルゴリズム生成部３７５Ａと第２アルゴリズム生成部３７５Ｂに、第１実施形態における鍵生成部３７６が、第１鍵生成部３７６Ａと第２鍵生成部３７６Ｂに、それぞれ置き換えられているという点である。

第１アルゴリズム生成部３７５Ａと第２アルゴリズム生成部３７５Ｂはともに、アルゴリズム生成部３７５と同様にアルゴリズムを生成するものであるが、第１アルゴリズム生成部３７５Ａが暗号化切断データを暗号化するためのアルゴリズムを生成するものであるのに対して、第２アルゴリズム生成部３７５Ｂが暗号化条件データを暗号化するためのアルゴリズムを復号化するためのものである点で異なっている。

第１鍵生成部３７６Ａと第２鍵生成部３７６Ｂはともに、鍵生成部３７６と同様に鍵を生成するものであるが、第１鍵生成部３７６Ａが暗号化データを暗号化するための鍵を生成するものであるのに対して、第２鍵生成部３７６Ｂが暗号化条件データを復号化するための鍵を生成するためのものである点で異なっている。

この変形例１では、暗号化切断データを復号化する場合には、解生成部３７４から第１アルゴリズム生成部３７５Ａへ解が送られ、そこで暗号化切断データを復号化するためのアルゴリズムが生成される。また、暗号化条件データを復号化する場合には、解生成部３７４から第２アルゴリズム生成部３７５Ｂへ解が送られ、そこで暗号化条件データを復号化するためのアルゴリズムが生成される。

また、この変形例１では、暗号化切断データを復号化する場合には、解生成部３７４から第１鍵生成部３７６Ａへ解が送られ、そこで暗号化切断データを復号化するための鍵が生成される。また、暗号化条件データを復号化する場合には、解生成部３７４から第２鍵生成部３７６Ｂへ解が送られ、そこで暗号化条件データを復号化するための鍵が生成される。

この変形例１では、以上のように、暗号化又は復号化する対象が平文切断データ又は暗号化切断データであるか、それとも条件データ又は暗号化条件データであるかにより、アルゴリズムと鍵を生成する手段を分けている。

【００９２】

なお、アルゴリズム生成部２７５と鍵生成部２７６のみならず、解生成部２７４をも分けることができる。

例えば、第１実施形態の暗号化処理装置１の場合であれば、一つの解生成部２７４から、アルゴリズム生成部２７５と鍵生成部２７６へと解を送ることにしていたが、上記解生成部２７４を例えば第１解生成部２７４Ａと第２解生成部２７４Ｂのように２つに分けて、前者が生成した解をアルゴリズム生成部２７５へ、後者が生成した解を鍵生成部２７６へ送るようにすることができる。

この場合、復号化処理装置２の解生成部３７４は、暗号化処理装置１に対応させて、第１解生成部３７４Ａと第２解生成部３７４Ｂに分ける必要がある。この場合、前者が生成

した解はアルゴリズム生成部３７５へ、後者が生成した解は鍵生成部３７６へそれぞれ送られる。

変形例１のように、暗号化処理装置１において、第１実施形態におけるアルゴリズム生成部２７５を、第１アルゴリズム生成部２７５Ａと、第２アルゴリズム生成部２７５Ｂに、第１実施形態における鍵生成部２７６を、第１鍵生成部２７６Ａと、第２鍵生成部２７６Ｂにそれぞれ置き換えるとともに、復号化処理装置２において、第１実施形態におけるアルゴリズム生成部３７５を、第１アルゴリズム生成部３７５Ａと、第２アルゴリズム生成部３７５Ｂに、第１実施形態における鍵生成部３７６を、第１鍵生成部３７６Ａと、第２鍵生成部３７６Ｂにそれぞれ置き換えた場合には、解生成部２７４、３７４を以下のようにすることができる。即ち、暗号化処理装置１における解生成部２７４を、第１～第４解生成部２７４Ａ～Ｄに置き換えて、第１解生成部２７４Ａが生成した解を第１アルゴリズム生成部２７５Ａに、第２解生成部２７４Ｂが生成した解を第２アルゴリズム生成部２７５Ｂに、第３解生成部２７４Ｃが生成した解を第１鍵生成部２７６Ａに、第４解生成部２７４Ｄが生成した解を第２鍵生成部２７６Ｂにそれぞれ送るようにするとともに、復号化処理装置２における解生成部３７４を、第１～第４解生成部３７４Ａ～Ｄに置き換えて、第１解生成部３７４Ａが生成した解を第１アルゴリズム生成部３７５Ａに、第２解生成部３７４Ｂが生成した解を第２アルゴリズム生成部３７５Ｂに、第３解生成部３７４Ｃが生成した解を第１鍵生成部３７６Ａに、第４解生成部３７４Ｄが生成した解を第２鍵生成部３７６Ｂにそれぞれ送るようにすることができる。

【００９３】

＜変形例２＞

次いで、変形例２について説明する。

変形例２における暗号化システムは、基本的に、上述した第１実施形態による暗号化システムと同一であり、それに含まれる暗号化処理装置１と復号化処理装置２の構成も、第１実施形態の場合と同様である。ただし、この変形例２に含まれる暗号化処理装置１における暗号化装置２７と、復号化処理装置２における復号化装置３７の一部の機能が、上述した暗号化システムに含まれていたものとは異なっている。

【００９４】

上述したように、変形例２における暗号化装置２７の構成は第１実施形態におけるそれの構成と同様であり、図３に示したようなものとなっている。

変形例２と第１実施形態で異なっているのは、条件データ生成部２７７の機能である。もっとも、変形例２における条件データ生成部２７７は、第１実施形態における条件データ生成部２７７と同様に、複数の条件データを生成するものであるので、その基本的機能に関していえば、第１実施形態の条件データ生成部２７７と変わらない。

第１実施形態の条件データ生成部２７７が生成する条件データは、その条件データと対応付けられた暗号化切断データの復号化を許容する場合の条件と、その対応付けられた暗号化切断データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含むものとされていたが、変形例２の条件データ生成部２７７が生成する条件データには、上述のデータに加えて、条件データの少なくとも一つに、他の条件データを暗号化して生成された暗号化条件データの復号化を許容する場合の条件についてのデータが含まれるようになっている。つまり、変形例２の条件データ生成部２７７は、第１実施形態のそれと比べて、機能が追加されている。

より詳細には、変形例２の条件データ生成部２７７は、条件データを複数生成するようになっているとともに、複数の条件データのうちの少なくとも幾つかを、それら幾つかの条件データを暗号化して生成された暗号化条件データの復号化が所定の順番で行われるように関連付けた状態で生成するようになっている。また、条件データ生成部２７７は、その幾つかの条件データを、ある条件データを暗号化して生成された暗号化条件データの次に復号化される暗号化条件データを復号化するための条件についてのデータが含まれるようにして生成するようになっている。この場合における条件データに含まれる、ある条件データを暗号化して生成された暗号化条件データの次に復号化される暗号化条件データを

復号化するための条件は、どのようなものでも構わない。例えば、以下の（Ａ）～（Ｃ）のようなものとすることができる。
（Ａ）暗号化条件データの復号化を行うことが許容された復号化処理装置を特定するための情報
（Ｂ）暗号化条件データの復号化を行うことが許容されたユーザを特定するための情報
（Ｃ）暗号化条件データの復号化が許容される時期に関する情報
なお、上述したように、変形例２の条件データ生成部２７７は、複数の条件データのうちの少なくとも幾つかを、それら幾つかの条件データを暗号化して生成された暗号化条件データの復号化が所定の順番で行われるように関連付けた状態で生成するようになっているが、上述の幾つかの条件データは、複数の条件データのすべてであっても構わない。

【００９５】
また、変形例２の基本条件データ生成部２７８の機能も、第１実施形態の基本条件データ生成部２７８の機能とは異なっている。
変形例２では、上述のように、複数の条件データのうちの少なくとも幾つかを、それら幾つかの条件データを暗号化して生成された暗号化条件データの復号化が所定の順番で行われるように関連付けた状態で生成されるが、変形例２における基本条件データ生成部２７８は、これら幾つかの条件データのうち、それを暗号化して得られた暗号化条件データが最初に復号化されるものの復号化を許容するための条件についてのデータを含めて基本条件データを生成する。この条件は、上述した、ある条件データを暗号化して生成された暗号化条件データの次に復号化される暗号化条件データを復号化するための条件に準じたものとすることができる。
なお、基本条件データ生成部２７８は、それら条件データを暗号化して生成された暗号化条件データの復号化が所定の順番で行われるように関連付けた状態で生成された上述の幾つかの条件データが、複数の条件データのすべてではない場合には、上記幾つかの条件データ以外の条件データの復号化を許容又は禁止するための条件の少なくとも一方を含んでいる。

【００９６】
変形例２でも、上述した如き条件データは暗号化されて、暗号化条件データとなる。
基本条件データと、暗号化条件データは、変形例２の場合でも、接続部２８０で、ヘッダデータ及び暗号化切断データとともに一まとめにされて、暗号化データとされる。
なお、この場合、暗号化条件データのうち、復号化が所定の順番で行われるように関連付けた幾つかのものは、先に復号化されるものが前方に位置するようにされる。

【００９７】
次に、変形例２における復号化装置３７について説明する。変形例２の復号化装置３７の機能の一部が、上述したように、第１実施形態の場合と多少異なる。もっとも、この機能の相違は、第１実施形態の場合と変形例２の場合とで、暗号化データに含まれている暗号化条件データ及び基本条件データに含まれているデータが異なることに起因するものであり、本質的な相違はない。
変形例２と第１実施形態で異なっているのは、基本条件データ解析部３７８、条件データ解析部３７７の機能である。
変形例２における基本条件データ解析部３７８は、第１実施形態の場合と同様に、前処理部３７２から送られた基本条件データを受付け、その基本条件データに示された内容を解析する。
上述したように、変形例２における基本条件データには、復号化が所定の順番で行われるように関連付けられた幾つかの暗号化条件データのうち、最初に復号化されるものの復号化を許容するための条件についてのデータが含まれている。基本条件データ解析部３７８は、それを読出して、復号化部３７３に送るようになっている。
また、変形例２における基本条件データには、復号化が所定の順番で行われるように関連付けられた幾つかの暗号化条件データ以外の暗号化条件データが含まれる場合がある。この場合には、復号化が所定の順番で行われるように関連付けられた幾つかの暗号化条件

データ以外の暗号化条件データのそれぞれの復号化を許容又は禁止する条件を、基本条件データから読出す。基本条件データ解析部３７８は、そのようなデータを読出した場合には、それを、復号化部３７３と解生成部３７４に送るようになっている。

【００９８】

変形例２の復号化部３７３は、第１実施形態の場合と同様に、前処理部３７２から受付けた暗号化切断データと暗号化条件データを復号化する機能を有する。

前者の復号化は、第１実施形態の場合と同様である。したがって、後者について説明する。

暗号化条件データの復号化は、基本的には、第１実施形態の場合と同様である。特に、復号化が所定の順番で行われるように関連付けられた幾つかの暗号化条件データ以外の暗号化条件データについては、第１実施形態の場合と同一である。

復号化が所定の順番で行われるように関連付けられた幾つかの暗号化条件データの復号化は、以下のようにしてなされる。まず、基本条件データから読出された、復号化が所定の順番で行われるように関連付けられた幾つかの暗号化条件データのうち、最初に復号化されるものの復号化を許容するための条件に基づいて、前処理部３７２から送られた、復号化が所定の順番で行われるように関連付けられた幾つかの暗号化条件データのうち最初に復号化されるものの復号化が試みられる。復号化部３７３が、復号化が所定の順番で行われるように関連付けられた幾つかの暗号化条件データのうち、最初に復号化されるものの復号化を許容するための条件が充足されていると判断した場合、その暗号化条件データは復号化されて条件データに戻される。

復号化されて得られたその条件データは、条件データ解析部３７７に送られる。条件データ解析部３７７は、その条件データから、その次に復号化されるべき暗号化条件データの復号化を許容するための条件を読出す。その条件についてのデータは、復号化部３７３に送られる。

復号化部３７３は、復号化が所定の順番で行われるように関連付けられた幾つかの暗号化条件データのうち２番目に復号化されるものの復号化を試みる。復号化が所定の順番で行われるように関連付けられた幾つかの暗号化条件データのうち、２番目に復号化されるものの復号化を許容するための条件が充足されていると判断した場合、復号化部３７３は、その暗号化条件データを復号化して条件データにする。

このような処理を繰り返し、復号化部３７３は、復号化が所定の順番で行われるように関連付けられた上記幾つかの暗号化条件データを、芋づる式に復号化していく。

ただし、復号化部３７３は、復号化が所定の順番で行われるように関連付けられた幾つかの暗号化条件データの復号化を試みる際に、その暗号化条件データの復号化を許容する条件が満たされていないと判断した場合には、その暗号化条件データの復号化を行わない。

暗号化切断データの復号化、その後行われる接続部３７９での処理などについては、第１実施形態の場合と同様である。

【００９９】

≪第２実施形態≫

第２実施形態の暗号化システムについて説明する。

第２実施形態の暗号化システムは、概ね第１実施形態の暗号化システムと共通する。

第２実施形態の暗号化システムは、暗号化処理装置における暗号化装置２７と、復号化処理装置２における復号化装置３７の一部の構成が、第１実施形態における暗号化システムに含まれていたものとは異なっている。

【０１００】

第２実施形態の暗号化装置２７は、図１２に示されたように構成されている。

この暗号化装置２７は第１実施形態の場合と概ね同様であるが、アルゴリズム生成部２７５と鍵生成部２７６がなくなっており、その代わりにアルゴリズム保持部２８１と、鍵保持部２８２が設けられている点で第１実施形態の暗号化装置２７と異なっている。

【０１０１】

アルゴリズム保持部２８１は複数のアルゴリズムを、鍵保持部２８２は複数の鍵を保持している。アルゴリズムは、暗号化部２７３で平文切断データと条件データを暗号化するために用いられるアルゴリズムであり、鍵は、暗号化部２７３で平文切断データと条件データを暗号化するために用いられる鍵である。

第１実施形態では、アルゴリズムと鍵を、解生成部２７４が生成した解に基づいてアルゴリズム生成部２７５と鍵生成部２７６で生成することにより、平文切断データと条件データを暗号化する場合に使用されるアルゴリズムと鍵の双方を複数とできるようにしていたが、第２実施形態では、アルゴリズム保持部２８１と鍵保持部２８２にそれぞれ複数のアルゴリズム、又は複数の鍵を保持させておくことで、新たにアルゴリズムや解を生成しなくても、平文切断データと条件データを暗号化する場合に複数のアルゴリズムと複数の鍵を使用できるようになっている。

【０１０２】

第２実施形態における条件データ生成部２７７が生成する条件データは、アルゴリズム生成部２７５と鍵生成部２７６がアルゴリズム保持部２８１と、鍵保持部２８２に置き換えられたことに伴い、それが生成する条件データの内容を第１実施形態の場合と多少異にする。

第２実施形態で生成される複数の条件データは、第１実施形態の場合と同様に、復号化処理装置２で、上述の暗号化切断データのそれぞれの復号化を許容する場合の条件と、暗号化切断データのそれぞれの復号化を禁止する場合の条件の少なくとも一方についてのデータを含んでいる。条件データは、第１実施形態の場合と同様に、対応付けられた暗号化切断データの復号化を許容する場合の条件と、その対応付けられた暗号化切断データの復号化を禁止する場合の条件との少なくとも一方についてのデータを含んでいる。

ただし、第２実施形態における条件データは、第１実施形態における条件データに含まれている場合のあった、解生成部２７４から受付けたその解が何番目に生成された解であるのかという情報（なお、この情報は、その条件データが対応付けられた暗号化切断データのそれぞれが、何番目の解に基づいて生成された鍵とアルゴリズムで暗号化されたのかということを示すものである）を含んでいない。その代わり、第２実施形態における条件データは、各平文切断データを暗号化するときに使用されたアルゴリズムがアルゴリズム保持部２８１に保持されていたもののうちのどれかということを示す情報と、各平文切断データを暗号化するときに使用された鍵が鍵保持部２８２に保持されていたもののうちのどれかということを示す情報とが含まれている場合がある。この情報は、例えば、アルゴリズムと鍵に、通し番号のような識別子が振られている場合であればその識別子とすることができ、または、アルゴリズムそのもの、或いは鍵そのものとすることができる。この実施形態では、識別子を条件データに含めることとしている。

同様に、第１実施形態の基本条件データに含まれることのあったその解が何番目に生成された解であるのかという情報は、第２実施形態の基本条件データには含まれていない。その代わりに、第２実施形態における基本条件データには、各条件データを暗号化するときに使用されたアルゴリズムがアルゴリズム保持部２８１に保持されていたもののうちのどれかということを示す情報と、各条件データを暗号化するときに使用された鍵が鍵保持部２８２に保持されていたもののうちのどれかということを示す情報とが含まれている場合がある。この情報は、例えば、アルゴリズムと鍵に、通し番号のような識別子が振られている場合であればその識別子とすることができ、または、アルゴリズムそのもの、或いは鍵そのものとすることができる。この実施形態では、識別子を条件データに含めることとしている。

【０１０３】

第２実施形態の復号化装置３７は、図１３に示されたように構成されている。

この復号化装置３７は第１実施形態の場合と概ね同様であるが、アルゴリズム生成部３７５と鍵生成部３７６がなくなっており、その代わりにアルゴリズム保持部３８１と、鍵保持部３８２が設けられている点で第１実施形態の復号化装置３７と異なっている。この変更は、暗号化装置２７の上述の変更と対応したものとなっている。

【０１０４】
アルゴリズム保持部３８１及び鍵保持部３８２は、暗号化装置２７内のアルゴリズム保持部２８１及び鍵保持部２８２と同じものとされている。アルゴリズム保持部３８１は複数のアルゴリズムを、鍵保持部３８２は複数の鍵を保持している。
アルゴリズムは、復号化部３７３で暗号化切断データと暗号化条件データを復号化するために用いられるアルゴリズムであり、鍵は、復号化部３７３で暗号化切断データと暗号化条件データを復号化するために用いられる鍵である。
第１実施形態では、アルゴリズムと鍵を、解生成部３７４が生成した解に基づいてアルゴリズム生成部３７５と鍵生成部３７６で生成することにより、暗号化切断データと暗号化条件データを復号化する場合に使用されるアルゴリズムと鍵の双方を複数とできるようにしていたが、第２実施形態では、アルゴリズム保持部３８１と鍵保持部３８２にそれぞれ複数のアルゴリズム、又は複数の鍵を保持させておくことで、新たにアルゴリズムや解を生成しなくても、暗号化切断データと暗号化条件データを復号化する場合に複数のアルゴリズムと複数の鍵を使用できるようになっている。
【０１０５】
第２実施形態の復号化装置３７での条件データ解析部３７７と基本条件データ解析部３７８の機能は、第１実施形態の場合と多少異なるものとなっている。この相違は、第２実施形態における条件データ及び基本条件データが、第１実施形態における条件データ及び基本条件データと上述したように異なっていることに起因したものである。
【０１０６】
第１実施形態の基本条件データ解析部３７８は、基本条件データの示す内容を解析するＳ１３０３において、どの暗号化条件データを復号化してよいのかという情報を復号化部３７３に送るとともに、復号化をしてよい暗号化条件データのそれぞれを暗号化したときに用いられたアルゴリズム及び鍵を生成したときに用いられた解が何番目に生成されたものかという情報を解生成部３７４に送ることとしている。
第２実施形態の基本条件データ解析部３７８は、第１実施形態の場合と同様に、どの暗号化条件データを復号化してよいのかという情報を復号化部３７３に送るが、復号化をしてよい暗号化条件データのそれぞれを暗号化したときに用いられたアルゴリズム及び鍵を生成したときに用いられた解が何番目に生成されたものかという情報を解生成部３７４に送ることをしない。その代わりに、第２実施形態の基本条件データ解析部３７８は、復号化をしてよい暗号化条件データのそれぞれを暗号化するときに使用されたアルゴリズムがアルゴリズム保持部２８１に保持されていたもののうちのどれかということを示す情報（上述の識別子）と、復号化をしてよい暗号化条件データを暗号化するときに使用された鍵が鍵保持部２８２に保持されていたもののうちのどれかということを示す情報（上述の識別子）とを復号化部３７３に送ることとしている。
識別子を受付けた復号化部３７３は、アルゴリズム保持部３８１からその識別子と対応付けられたアルゴリズムを読出し、また、鍵保持部３８２からその識別子と対応付けられた鍵を読出す。
こうしてアルゴリズム保持部３８１と鍵保持部３８２から読出されたアルゴリズム及び鍵は、暗号化処理装置１で条件データを暗号化するときに使用されたアルゴリズム及び鍵と同一のものとなっている。このアルゴリズムと鍵を用いて、復号化部３７３は暗号化条件データの復号化を行う。
なお、基本条件データに含まれている暗号化条件データのそれぞれを暗号化するときに使用されたアルゴリズムがアルゴリズム保持部２８１に保持されていたもののうちのどれかということを示す情報がアルゴリズム自体である場合には、アルゴリズム保持部３８１は不要になる。この場合には、基本条件データ解析部３７８は、基本条件データに含まれていたアルゴリズム自体を、復号化部３７３に送るようになっていればよい。また、基本条件データに含まれている暗号化条件データのそれぞれを暗号化するときに使用された鍵が鍵保持部２８２に保持されていたもののうちのどれかということを示す情報が鍵自体である場合には、鍵保持部３８２は不要になる。この場合には、基本条件データ解析部３７

８は、基本条件データに含まれていた鍵自体を、復号化部３７３に送るようになっていればよい。

【０１０７】

条件データ解析部３７７もこれと同様の処理を行う。

第１実施形態の条件データ解析部３７７は、条件データの示す内容を解析するＳ１３０７において、どの暗号化切断データを復号してよいのかという情報を復号化部３７３に送るとともに、復号化をしてよい暗号化切断データのそれぞれを暗号化したときに用いられたアルゴリズム及び鍵を生成したときに用いられた解が何番目に生成されたものかという情報を解生成部３７４に送ることとしている。

第２実施形態の基本条件データ解析部３７８は、第１実施形態の場合と同様に、どの暗号化切断データを復号化してよいのかという情報を復号化部３７３に送るが、復号化をしてよい暗号化切断データのそれぞれを暗号化したときに用いられたアルゴリズム及び鍵を生成したときに用いられた解が何番目に生成されたものかという情報を解生成部３７４に送ることをしない。その代わりに、第２実施形態の条件データ解析部３７７は、復号化をしてよい暗号化切断データのそれぞれを暗号化するときに使用されたアルゴリズムがアルゴリズム保持部２８１に保持されていたもののうちのどれかということを示す情報（上述の識別子）と、復号化をしてよい暗号化切断データを暗号化するときに使用された鍵が鍵保持部２８２に保持されていたもののうちのどれかということを示す情報（上述の識別子）とを復号化部３７３に送ることとしている。

識別子を受付けた復号化部３７３は、上述の場合と同様に、アルゴリズム保持部３８１からその識別子と対応付けられたアルゴリズムを読出し、また、鍵保持部３８２からその識別子と対応付けられた鍵を読出し、それを用いて暗号化切断データの復号化を行う。

なお、条件データに含まれている暗号化切断データのそれぞれを暗号化するときに使用されたアルゴリズムがアルゴリズム保持部２８１に保持されていたもののうちのどれかということを示す情報がアルゴリズム自体である場合にアルゴリズム保持部３８１は不要になること、及び条件データに含まれている暗号化切断データのそれぞれを暗号化するときに使用された鍵が鍵保持部２８２に保持されていたもののうちのどれかということを示す情報が鍵自体である場合には、鍵保持部３８２は不要になることは、上述の場合と同様である。

【図面の簡単な説明】

【０１０８】

【図１】第１実施形態における暗号化システムの全体構成を示す図。

【図２】図１に示した暗号化システムに含まれる暗号化処理装置のハードウエア構成を示す図。

【図３】図２に示した暗号化処理装置に含まれる暗号化装置の構成を示すブロック図。

【図４】図２に示した暗号化処理装置で生成される暗号化データのデータ構造を示す図。

【図５】図１に示した暗号化システムに含まれる復号化処理装置のハードウエア構成を示す図。

【図６】図５に示した復号化処理装置に含まれる暗号化装置の構成を示すブロック図。

【図７】図１に示した暗号化システムで実行される処理の流れを示す流れ図。

【図８】図７で示したＳ１１０で実行される処理の流れを示す流れ図。

【図９】図７で示したＳ１３０で実行される処理の流れを示す流れ図。

【図１０】図３に示した暗号化装置の変形例に係る構成を示すブロック図。

【図１１】図６に示した復号化装置の変形例に係る構成を示すブロック図。

【図１２】第２実施形態における暗号化処理装置に含まれる暗号化装置の構成を示すブロック図。

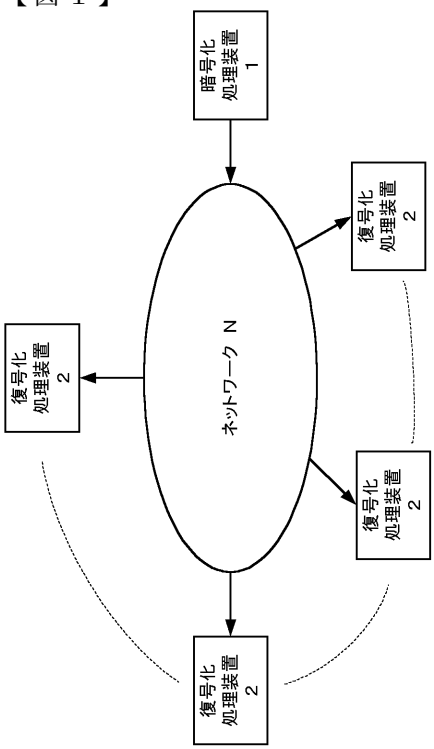
【図１３】第２実施形態における復号化処理装置に含まれる復号化装置の構成を示すブロック図。

【符号の説明】

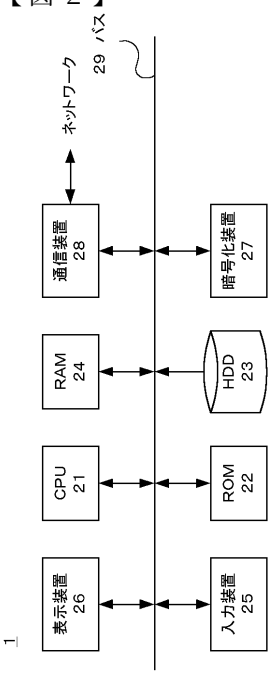
【０１０９】

１　暗号化処理装置
２　復号化処理装置
２５　入力装置
２６　表示装置
２７　暗号化装置
２８　通信装置
２９　バス
３５　入力装置
３６　表示装置
３７　復号化装置
３８　通信装置
３９　バス
２７１　インタフェイス部
２７２　前処理部
２７３　暗号化部
２７４　解生成部
２７５　アルゴリズム生成部
２７６　鍵生成部
２７７　条件データ生成部
２７８　基本条件データ生成部
２７９　ヘッダ生成部
２８０　接続部
２８１　アルゴリズム保持部
２８２　鍵保持部
３７１　インタフェイス部
３７２　前処理部
３７３　復号化部
３７４　解生成部
３７５　アルゴリズム生成部
３７６　鍵生成部
３７７　条件データ解析部
３７８　基本条件データ解析部
３７９　接続部
３８０　タイマー
３８１　アルゴリズム保持部
３８２　鍵保持部
５０１　ヘッダデータ
５０２　基本条件データ
５０３　暗号化条件データ
５０４　暗号化切断データ

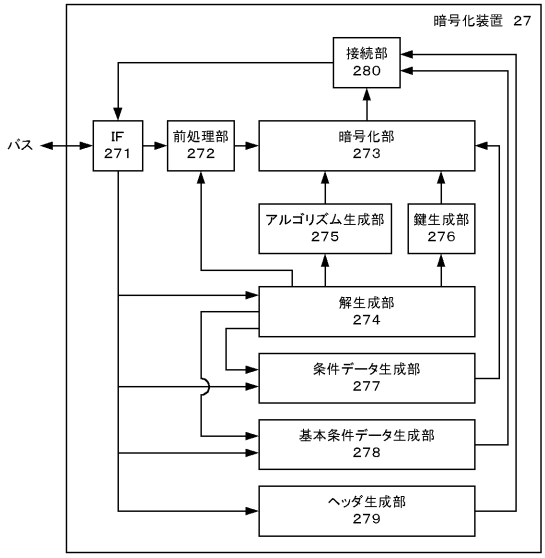
【図１】


暗号化処理装置 1
復号化処理装置 2
復号化処理装置 2
ネットワーク N
復号化処理装置 2
復号化処理装置 2

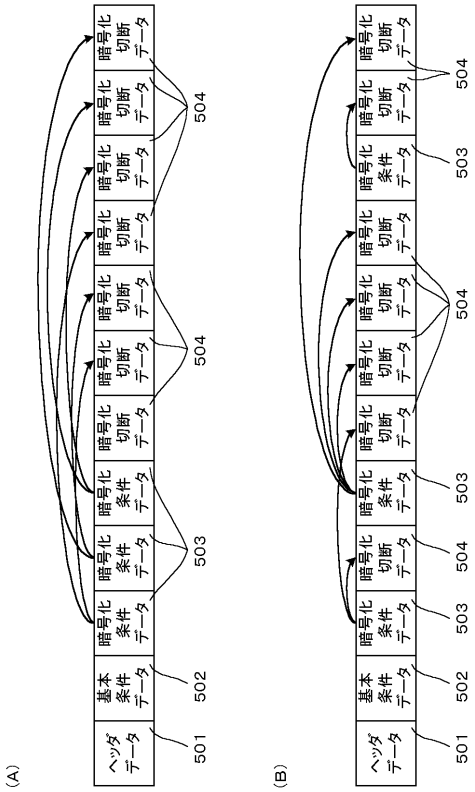
【図２】


ネットワーク
29 バス
通信装置 28
暗号化装置 27
RAM 24
HDD 23
CPU 21
ROM 22
表示装置 26
入力装置 25
1

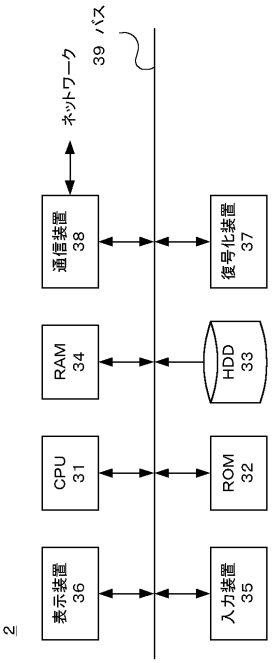
【図３】


暗号化装置 27
接続部 280
バス
IF 271
前処理部 272
暗号化部 273
アルゴリズム生成部 275
鍵生成部 276
解生成部 274
条件データ生成部 277
基本条件データ生成部 278
ヘッダ生成部 279

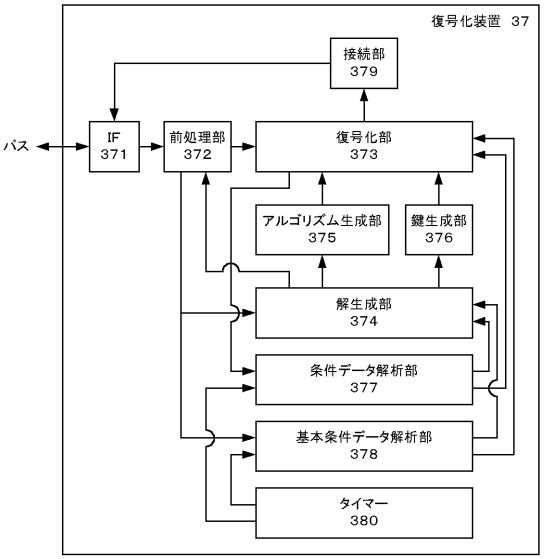
【図４】


(A)
ヘッダデータ
基本条件データ
暗号化条件データ
暗号化切断データ
501
502
503
504
(B)
ヘッダデータ
基本条件データ
暗号化条件データ
暗号化切断データ
501
502
503
504

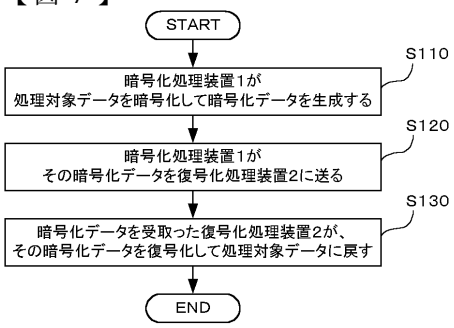
【図５】


ネットワーク
39 バス
通信装置 38
復号化装置 37
RAM 34
HDD 33
CPU 31
ROM 32
表示装置 36
入力装置 35
2

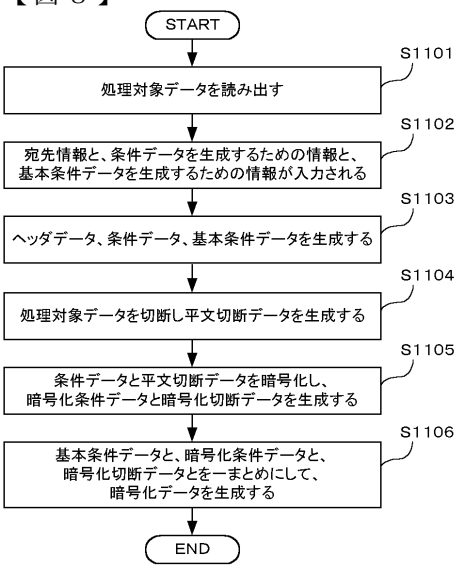
【図６】


復号化装置 37
接続部 379
バス
IF 371
前処理部 372
復号化部 373
アルゴリズム生成部 375
鍵生成部 376
解生成部 374
条件データ解析部 377
基本条件データ解析部 378
タイマー 380

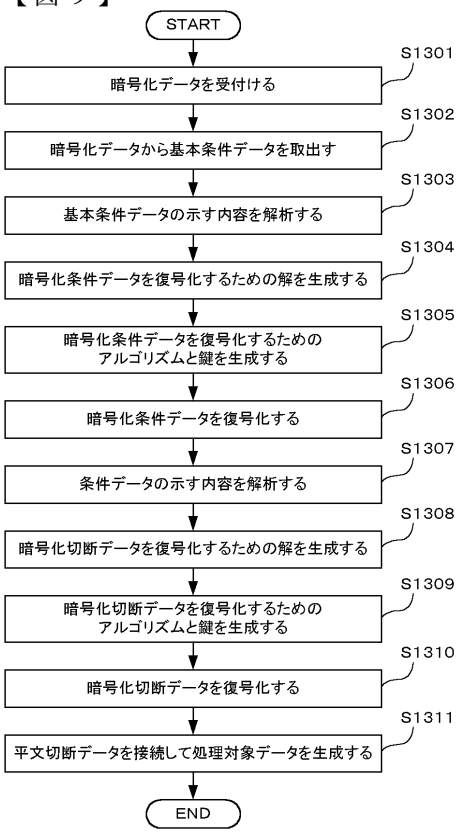
【図７】


START
暗号化処理装置1が
処理対象データを暗号化して暗号化データを生成する
S110
暗号化処理装置1が
その暗号化データを復号化処理装置2に送る
S120
暗号化データを受取った復号化処理装置2が、
その暗号化データを復号化して処理対象データに戻す
S130
END

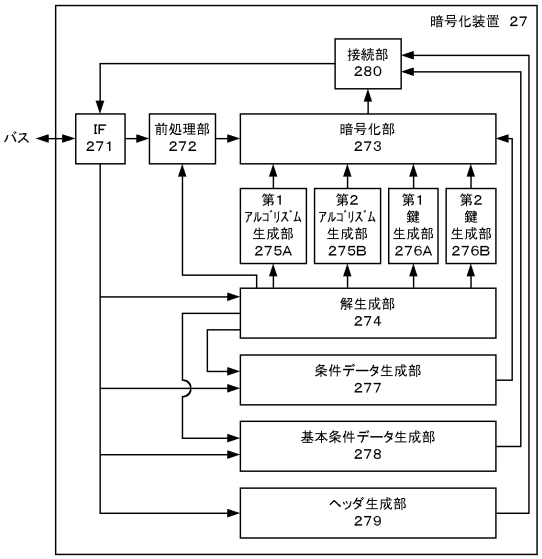
【図８】


START
処理対象データを読み出す
S1101
宛先情報と、条件データを生成するための情報と、
基本条件データを生成するための情報が入力される
S1102
ヘッダデータ、条件データ、基本条件データを生成する
S1103
処理対象データを切断し平文切断データを生成する
S1104
条件データと平文切断データを暗号化し、
暗号化条件データと暗号化切断データを生成する
S1105
基本条件データと、暗号化条件データと、
暗号化切断データとを一まとめにして、
暗号化データを生成する
S1106
END

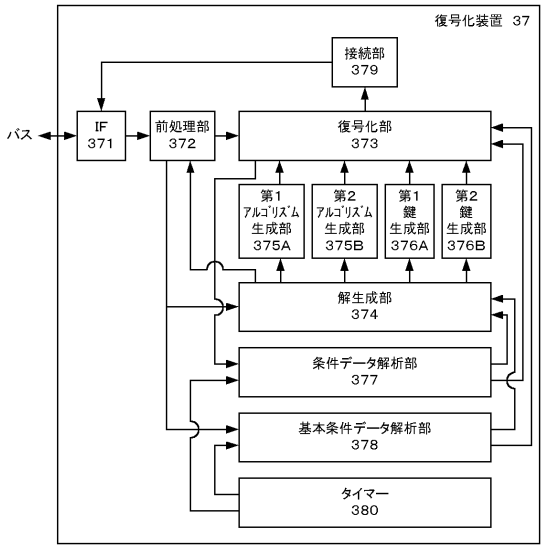
【図９】



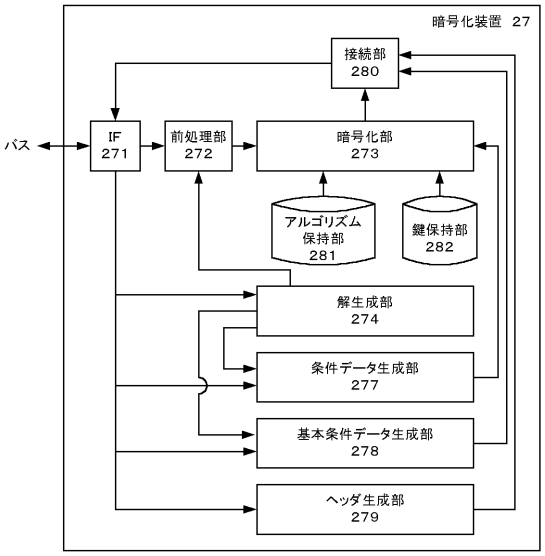
【図１０】



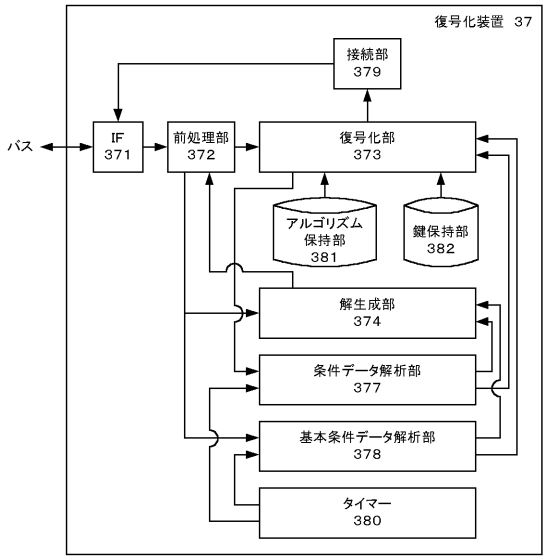
【図１１】



【図１２】



【図１３】


復号化装置 37
接続部
379
バス
IF
371
前処理部
372
復号化部
373
アルゴリズム
保持部
381
鍵保持部
382
解生成部
374
条件データ解析部
377
基本条件データ解析部
378
タイマー
380