(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6501873号
(P6501873)
(45)発行日　平成31年4月17日(2019.4.17)　(24)登録日　平成31年3月29日(2019.3.29)

(51)Int.Cl.　　F I
H04L 9/22 (2006.01)　　H04L 9/00 655
H04L 9/08 (2006.01)　　H04L 9/00 601B
　　H04L 9/00 601E

請求項の数 8　(全 19 頁)

(21)出願番号　特願2017-513389(P2017-513389)
(86)(22)出願日　平成26年9月14日(2014.9.14)
(65)公表番号　特表2017-527225(P2017-527225A)
(43)公表日　平成29年9月14日(2017.9.14)
(86)国際出願番号　PCT/IB2014/064502
(87)国際公開番号　WO2016/038428
(87)国際公開日　平成28年3月17日(2016.3.17)
審査請求日　平成29年9月11日(2017.9.11)

(73)特許権者　517078596
デュランド　アレクサンドル
DURAND Alexandre
フランス国　ル　ベジネ　エフ－７８１１
０　リュ　ヴィルボワ　マレイユ　３３
３３ rue Villebois Mareuil F-78110 Le Vesinet France
(74)代理人　110001564
フェリシテ特許業務法人
(72)発明者　デュランド　アレクサンドル
フランス国　ル　ベジネ　エフ－７８１１
０　リュ　ヴィルボワ　マレイユ　３３

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】暗号システムの再現可能なランダムシーケンス

(57)【特許請求の範囲】
【請求項１】
１つ又はいくつかのプロセッサにより実施される暗号オペレーションでの使用のためのランダムな文字列を生成するためのコンピュータに実装された方法であって、
ランダム性生成により、１つ又はいくつかのランダム転送マップを生成する工程（ａ）であって、前記ランダム性生成は、擬似ランダム生成器によって作成されない工程（ａ）と、
ランダムシーケンスを生成することとなる前記コンピュータに対して、生成された前記ランダム転送マップを提供する工程（ｂ）と、
前記コンピュータに対して、擬似ランダムシーケンス生成器のシードを提供する工程（ｃ）と、
生成されるランダムシーケンス毎に１つのランダムマッピングオペレーションを使用して、いくつかの入力に対して、１つ又はいくつかのプロセッサを動作させることにより、ランダムな文字列を生成する工程（ｄ）であって、前記入力が、
ｉ．前記挙げられたランダム転送マップ提供工程中に提供されるランダム転送マップ、及び、
ｉｉ．前記挙げられた擬似ランダムシーケンス生成器の出力であり、
前記ランダムマッピングオペレーションのそれぞれが、
シードを用いて擬似ランダムシーケンス生成器を初期化する工程（ｉ）であって、前記シードが、

Ａ．前記コンピュータへ提供され、
Ｂ．又は、前記コンピュータへ提供される１つ又はいくつかのランダム転送マップの一部において選択される工程（ｉ）と、
混合演算を使用して、前記ランダムマッピングオペレーションの入力を混合する工程（ｉｉ）であって、前記ランダムマッピングオペレーションの入力が、
Ａ．別のランダムマッピングオペレーション由来の出力、
Ｂ．又はいくつかのその他のランダムマッピングオペレーションの出力の混合演算による組み合わせ、
Ｃ．又は前記ランダムマッピングオペレーションにより使用される、擬似ランダムシーケンス生成器由来の出力、
Ｄ．又は前記ランダムマッピングオペレーションにより使用される擬似ランダムシーケンス生成器由来の出力と、１つ又はいくつかのその他のランダムマッピングオペレーションの出力との混合演算による組み合わせ、
Ｅ．又は前記ランダムマッピングオペレーションにより使用される擬似ランダムシーケンス生成器由来の出力と、フィードバックとして使用される、前記ランダムマッピングオペレーションにより先に生成された出力との混合演算による組み合わせ、
Ｆ．又はフィードバックとして使用される、前記ランダムマッピングオペレーションにより先に生成された出力と交互に行われる、前記ランダムマッピングオペレーションにより使用される、擬似ランダムシーケンス生成器由来の出力、
Ｇ．又は前記ランダムマッピングオペレーションにより使用される擬似ランダムシーケンス生成器由来の出力と、１つ又はいくつかのその他のランダムマッピングオペレーションの出力と、フィードバックとして使用される、前記ランダムマッピングオペレーションにより先に生成された出力との混合演算による組み合わせ、
Ｈ．又は前記ランダムマッピングオペレーションにより使用される擬似ランダム生成器由来の出力と、１つ又はいくつかのその他のランダムマッピングオペレーションの出力との混合演算による組み合わせであって、この組み合わせは、フィードバックとして使用される、前記ランダムマッピングオペレーションにより先に生成された出力と交互に行われる、組み合わせである工程（ｉｉ）と、
前記工程（ｉｉ）からの結果を使用して、マップ選択プロトコルの使用により、前記ランダムマッピングオペレーションに起因する前記ランダム転送マップ由来の文字を選択する工程（ｉｉｉ）と、
前記工程（ｉｉｉ）において選択された前記文字を出力する工程（ｉｖ）と、
全てのランダムな文字列が生成されるまで、次の出力文字を生成するために、前記工程（ｉｉ）に立ち戻る工程（ｖ）とを含み、
前記ランダムマッピングオペレーションの出力を、他のランダムマッピングオペレーションの入力へ送り出し、及び、結果として前記ランダムマッピングオペレーションの出力が、前記方法を適用する前に規定されている工程（ｄ）と、
前記結果として前記生成されたランダムな文字列を出力する工程（ｅ）とを含むことを特徴とする方法。

【請求項２】
平文文字列を暗号文文字列へ変換及び逆の変換を行うための符号及び復元の対称鍵による暗号装置システムであって、
（ａ）文字列を暗号化するための手段と、
（ｂ）復号スキームが暗号スキームとは異なる場合、暗号化された文字列を復号するための手段と、
（ｃ）１つ又はいくつかのランダムシーケンスを生成するための手段とを含み、
全ての前記手段が各々暗号化構造によって構成されているか、或いは、全ての前記手段を含めて１個の暗号化構造となっており、
ランダムシーケンス生成器のそれぞれは、１つ又はいくつかのランダムシーケンスを生成するための前記手段において実装され、

前記ランダムシーケンス生成器は、前記文字列の暗号化又は復号を行う前記手段のための秘密鍵を生成し、
前記生成器は、
（ａ）１つ又はいくつかの擬似ランダムシーケンス生成モジュールと、
（ｂ）１つ又はいくつかのランダムマッピングモジュールとを備え、
前記ランダムマッピングモジュールのそれぞれは、受信シーケンス由来の文字を発信シーケンス用のランダム文字へとマッピングし、
前記受信シーケンスは、
（ａ）別のランダムマッピングモジュールの発信シーケンス、
（ｂ）いくつかのその他のランダムマッピングモジュールの発信シーケンスの混合演算による組み合わせ、
（ｃ）１つの擬似ランダムシーケンス生成モジュールの発信シーケンス、
（ｄ）１つの擬似ランダムシーケンス生成モジュールの発信シーケンスと、１つ又はいくつかのその他のランダムマッピングモジュールの発信シーケンスとの混合演算による組み合わせ、
（ｅ）１つの擬似ランダムシーケンス生成モジュールの発信シーケンスと、フィードバックランダムシーケンスとの混合演算による組み合わせであって、このフィードバックランダムシーケンスが、前記ランダムマッピングモジュールの発信シーケンスである組み合わせ、
（ｆ）前記フィードバックランダムシーケンスと交互に行われる１つの擬似ランダムシーケンス生成モジュールの発信シーケンスであって、前記フィードバックランダムシーケンスが、前記ランダムマッピングモジュールの発信シーケンスである発信シーケンス、
（ｇ）１つの擬似ランダムシーケンス生成モジュールの発信シーケンスと、１つ又はいくつかのその他のランダムマッピングモジュールの発信シーケンスと、前記フィードバックランダムシーケンスとの混合演算による組み合わせであって、前記フィードバックランダムシーケンスが、前記ランダムマッピングモジュールの発信シーケンスである発信シーケンス、又は、
（ｈ）１つの擬似ランダムシーケンス生成モジュールの発信シーケンスと、１つ又はいくつかのその他のランダムマッピングモジュールの発信シーケンスとの混合演算による組み合わせであって、前記組み合わせが、前記フィードバックランダムシーケンスと交互に行われ、前記フィードバックランダムシーケンスが、前記ランダムマッピングモジュールの発信シーケンスである組み合わせであり、
前記挙げられたランダムマッピングモジュールのそれぞれは、これらの受信シーケンスのそれぞれの文字をランダム文字へとマップして、１つの発信ランダムシーケンスを作成するために、マップ選択プロトコルにより、ランダム転送マップを使用し、
前記ランダム転送マップは、ランダム性生成により生成され、
前記ランダム性生成は、擬似ランダム生成器によっては作成されず、前記ランダムマッピングモジュールへ提供され、前記ランダムマッピングモジュール毎に１つのランダム転送マップであることを特徴とする暗号装置システム。
【請求項３】
前記ランダム転送マップを変換するための手段を更に備え、
前記ランダム転送マップを変換するための手段は、暗号化構造であり、
前記ランダム転送マップを変換するための手段からの前記ランダム転送マップ変換モジュールは、
（ａ）前記ランダム転送マップを変更すべき挙げられたランダムマッピングモジュール由来のランダム転送マップと、
（ｂ）変換ランダム文字とを入力し、
前記変換ランダム文字は、
（ａ）入力される前記ランダム転送マップの長さに到達するまで次々と繰り返されるランダム文字である、提供されるパラメータ、又は、

（ｂ）別のランダムシーケンス生成モジュールの出力であり、
前記挙げられたランダム転送マップ変換モジュールは、前記挙げられたランダム転送マップ変換モジュールへ入力された前記ランダム転送マップの代わりに、送り返す二次ランダム転送マップを生成するために、前記ランダム転送マップを変更すべき前記ランダムマッピングモジュールへの入力間の混合演算を行うことを特徴とする請求項２に記載の暗号装置システム。
【請求項４】
擬似ランダムシーケンス生成器のシードを生成するための手段を更に含み、
前記擬似ランダムシーケンス生成器のシードを生成するための手段は、暗号化構造であり、
前記シードを生成するための手段からのシード生成モジュールは、１つ又はいくつかのランダムシーケンスを生成するための前記手段の前記擬似ランダムシーケンス生成モジュールのために、シード計算アルゴリズムを使用して、提供又は選択された文字由来のシードを計算することを特徴とする請求項３に記載の暗号装置システム。
【請求項５】
前記挙げられたシード生成モジュールへ提供された前記選択した文字は、前記１つ又はいくつかのランダムシーケンスを生成するための手段により格納された１つ又はいくつかのランダム転送マップの一部において選択されることを特徴とする請求項４に記載の暗号装置システム。
【請求項６】
前記生成されたランダム転送マップを提供する工程は、暗号的に安全な通信チャネルを生成するために、暗号化スキーム及び復号スキームでの結果としてみなされた前記出力が生成したランダムな文字列使用して、
（ａ）最初は、非一時的コンピュータ可読媒体を使用して、ランダムな文字列を生成することとなる前記挙げられたコンピュータへ前記ランダム転送マップを転送する工程と、
（ｂ）以降は、前記暗号的に安全な通信チャネル生成工程により生成された暗号的に安全な通信チャネルを介して、ランダムな文字列を生成することとなる前記コンピュータへ新規のランダム転送マップを転送する工程とを使用して実施されることを特徴とする請求項１に記載の方法。
【請求項７】
非一時的コンピュータで可読な記憶媒体であって、
１つ又はいくつかのコンピュータに請求項２に記載の暗号装置システムとして機能させるためのプログラムを前記記憶媒体上に格納し、前記暗号装置システムとして機能する前記コンピュータは両方共、前記１つ又はいくつかのランダムシーケンスを生成するための手段において実装された１つ又はいくつかの挙げられたランダムシーケンス生成器の機能性を備えることを特徴とする記憶媒体。
【請求項８】
請求項２～６のいずれか一項に記載された暗号装置システムを使用する方法であって、
（ａ）最初は、非一時的コンピュータ可読媒体を使用して、前記１つ又はいくつかのランダムシーケンスを生成するための手段へ、前記暗号装置システムに必要な前記ランダム転送マップを転送する工程と、
（ｂ）以降は、前記暗号装置システムを使用して生成された暗号的に安全なチャネルを介して、前記１つ又はいくつかのランダムシーケンスを生成するための手段へ、新規のランダム転送マップを転送する工程とを含むことを特徴とする方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号プロセス及び暗号装置の分野に属する。暗号化は、データを暗号化（別名、符号化）、又は暗号化されたデータの暗号を復号（別名、復元）する技術である。当該技術は長く軍事及び外交によって使用されてきたが、昨今その使用は、世間一般及び実

業界にまで拡大してきている。商用データ及び銀行の通信を保護するために強力かつ安全な暗号システムを有することは、今日、経済的に極めて重要なことである。

【背景技術】

【０００２】

（定義）

従来技術を紹介する前に、本明細書において使用することとなるいくつかの専門用語の定義を付与することとする。これらの定義は、本明細書全体（明細書、請求の範囲、要約書）において適用するものとする。

【０００３】

単語「データ」は、全ての種類の情報、知識、テキスト、メッセージ、ドキュメント、図面、数値結果、画像、イメージ、これらの一部若しくは全ての組み合わせ、又は文字列により表現、転写若しくはモデル化可能な任意のものを意味する。

【０００４】

「文字列」とは、全ての種類のスペース、グリフ、表意文字、数字、（モールス信号、テレタイプコード、電子装置におけるデジタル２進コード等のような）いくつかの状態に準拠したコード、場合により（ＡＳＣＩＩ、ＡＮＳＩ、Ｕｎｉｃｏｄｅ、Ｂａｕｄｏｔ、又はその他のもの等の）コード体系に従う数字コード（２進法、１０進法、１６進法又は任意の基数におけるもの）、任意の同等のもの、又は、これらの一部若しくは全ての組み合わせからなる、記号（文字、数字、句読記号等）の列を意味する。したがって、「文字」は、文字列を形成する要素として定義される。

【０００５】

「ランダムシーケンス」とは、どの文字が文字列内の前の文字（及び／又は次の文字）であり、文字列内の場所毎にこれをたとえ分かっていたとしても、どの文字が文字列内の特定の場所に存在するかを予測することが不可能な文字列のことを意味する。

【０００６】

（従来の技術）

何世紀もの間、Ｖｉｇｅｎｅｒｅ暗号が最も安全な暗号システムの１つであるとして考えられてきた。Ｖｉｇｅｎｅｒｅ暗号は、メッセージの文字毎に異なるシフトで、それぞれの文字をアルファベット順にシフトしたその他の文字で置換することに基づいていた。異なるシフトのシーケンスを記憶するために、「鍵（key）」のシステムが作成された。鍵は、それぞれの文字が、「Ａ」には「０」、「Ｂ」には「１」、「Ｃ」には「２」、以下、「Ｚ」には「２５」とみなして適用するシフトを付与する単語又は文である。鍵は、暗号化するテキストの終わりまでループする。

【０００７】

この手法は、第１次世界大戦中にＧｉｌｂｅｒｔ　Ｓ．Ｖｅｒｎａｍによる「印刷電信機」（テレタイプライタ）（米国特許第１,３１０,７１９号）に採用された。このシステムにおいて、文字はＢａｕｄｏｔコードを用いて２進法でコード化されている。これは、２つの記号及び実行可能な２つのシフト、つまり、何もないか、又は「その他の記号へのシフト」のみが存在していることを意味している。また、鍵をテープに付与すると、もはや鍵を記憶する必要がなくなったため、ランダムシーケンスが使用され始めた。

【０００８】

最初に成功したＶｉｇｅｎｅｒｅ暗号に対する攻撃は、Ｆｒｉｅｄｒｉｃｈ　Ｋａｓｉｓｋｉにより実行され、また、より効果的な攻撃は、Ｗｉｌｌｉａｍ　Ｆｒｉｅｄｍａｎによって考案された。双方の手法とも、鍵が繰り返し何度も使用されるという事実に付け込んだものであった。

【０００９】

これらの手法に対抗するために、少なくとも暗号化するテキストと同じの長さの鍵を使用することが考案された。このような鍵を見出すための最良の方法は、（当然、敵には知られていない）ブックを使用することであった。しかしながら、この種の暗号は、鍵が意味を有していたため依然として解読可能であった。

【００１０】
この問題に対する解決策は、米国陸軍少佐のＪｏｓｅｐｈ　Ｏ．Ｍａｕｂｏｒｇｎｅにより見出された。彼は、Ｖｅｒｎａｍのシステム及びそのランダム鍵に関する情報を得ると、暗号化するテキストと同じ長さのランダム鍵をセットすることにより、かつ、それぞれのランダム鍵を一度だけ使用すべきであると定めることにより、上記解決策を完成させた。

【００１１】
このようなシステムは、ワンタイムパッドとして知られており、かかる暗号システムを完全に破ることは不可能であることが正式に証明されている。しかしながら、鍵を一度だけ使用するという条件を課すことは、実際、かかる完全証明された暗号システムが滅多に使用されない理由であり、膨大な数のランダム鍵を生成しなければならないという事実の他、安全なチャネルを介して受信者に鍵を送信することが大きな問題である。このことは、「鍵配送問題（ｋｅｙ　ｄｉｓｔｒｉｂｕｔｉｏｎ　ｐｒｏｂｌｅｍ）」と称されている。かかる安全なチャネルが存在すると考えられる場合、先ずランダム鍵を送信し、それから暗号化メッセージを送信するのではなく、明らかに、当該チャネルを使用して、当該チャネルを介して直接メッセージを送信するであろうと思われる。

【００１２】
この問題を解決するための１つの試みとしては、非常に短いランダム鍵を使用し、当該ランダム鍵をループする代わりに当該ランダム鍵から擬似ランダムシーケンス（全ての要素が、計算の（複数の）先行要素及び/又は（複数の）先行状態から計算されるシーケンス）を計算することである。通常、公開鍵暗号法（以下を参照のこと）を使用して、この短いランダム鍵を受信者に送信し、当該ランダム鍵から生成した擬似ランダムシーケンスを、暗号鍵として使用する。この種の暗号システムは、「ストリーム暗号」と称される。

【００１３】
ストリーム暗号は、まるでワンタイムパッドのように、テキストと同じ長さの、意味を有さない鍵を提供する。しかしながら、ワンタイムパッドとは対照的に、鍵の要素が互いに関連し合っているという事実がシステムを劇的に弱め、結果的に暗号解読者が暗号を破ることを可能とする。つまり、（可能性のある全ての鍵を順次試す）ブルートフォース攻撃の場合には、試される鍵はより少なくなり（通常の長さの鍵ではなく短い全ランダム鍵のみ）、計算された鍵の文字間の相関により、（もしあるとすれば）さほど多くの偽鍵が可能とはならない。

【００１４】
また、「短い」ランダム鍵を使用する暗号システムの別の群としては、「ブロック暗号」の群が挙げられる。ここでは、データを、固定長のブロックへと切り捨て、数回暗号化する。毎回（それを「ターン」と呼ぶ）、ターン毎に異なる鍵を用い、いくつかの手法（転置及び換字）を使用してブロックを暗号化し、規定のアルゴリズムを使用しこれら全ての鍵を短いランダム鍵から計算する。ターンの回数により、従来の手法を使用した暗号解読を防止するようになっている。しかしながら、ワンタイムパッドと比較した場合、ブルートフォース攻撃に対するストリーム暗号と同一の問題を有している。

【００１５】
公開鍵暗号法では、データを符号化するために、秘密鍵の代わりに、（例えば、膨大な数字の因数分解のような）今も解かれていないある数理問題を使用している。公開鍵を用いるこの暗号システム群の基本原理は、暗号鍵と復号鍵とを分けることであり、（メッセージの復号には使用不可能であるため）暗号鍵を公開し、潜在的な送信者へと付与し、復号鍵を秘密とし受信者側で保持することにより、一方向性の通信チャネルを構築する（したがって、２人の個人間に双方向性のチャネルを有するためには、一方が２つの一方向性チャネルを生成する必要があり、２つの公開鍵及び２つの秘密鍵を作成することとなる）。

【００１６】
このように、テキストと同じ長さの秘密鍵を送受信するための安全なチャネルをもはや

必要としないため、このスキームにより、「鍵配送問題」を解決することができる。しかしながら、これらの暗号システムは、通常、時間がかかるものであることから、実際には、（短い真ランダム鍵のような）非常に短いデータを符号化するためにのみ使用され、長いデータに対しては、（送信した短いランダム鍵を使用する）前述の暗号システムを使用して符号化する。

【００１７】

しかしながら、ワンタイムパッドとは対照的に、暗号システムのベースとなる数理問題を誰も（秘密裏に）解き明かしていないということを証明することは不可能であるため、公開鍵暗号法は無条件に安全というわけではないことを理解すべきである。

【発明の概要】

【発明が解決しようとする課題】

【００１８】

したがって、技術及び暗号解読手法の進化に対抗できる完璧に安全な暗号システムを有するために、ワンタイムパッドよりも無条件に安全で、かつ「鍵配送問題」を生じない、暗号システムが依然として求められている。

【課題を解決するための手段】

【００１９】

鍵として１つ又はいくつかのランダムシーケンス、例えば、処理するデータと少なくとも同じ長さの鍵を使用して、データを暗号化（別名、符号化）、又は暗号化データを復号（別名、復元）するための、新規の暗号スキームを（その実装及び実施形態の一部と共に）ここに開示する。本開示の暗号プロセスは、１つ又はいくつかのランダムシーケンス生成プロセスを含み、そのうち１つは暗号化プロセスであり、１つは復号化プロセスである。暗号化プロセスと復号化プロセスの双方は、ランダムシーケンス生成プロセス由来の（複数の）ランダムシーケンスを使用して、データを（それぞれ）暗号化及び復号する。

【００２０】

基本的な方法において、１つのランダムシーケンス生成プロセスは、少なくとも１つの擬似ランダム生成プロセス及び１つのランダムマッピングプロセスを含む。擬似ランダム生成プロセスは、ランダムマッピングプロセスへ擬似ランダムシーケンスを送信する。ランダムマッピングプロセスは、擬似ランダムシーケンスを使用して、ランダムシーケンスを生成し、ランダム転送マップを使用して、擬似ランダムシーケンスの要素をランダムシーケンスのランダム要素へと変換する。実際には、このランダム転送マップは、データを暗号化及び復号することを許可された人々にのみ提供される。

【００２１】

より複雑な方法において、１つのランダムシーケンス生成プロセスは、１つ又はいくつかの擬似ランダム生成プロセス、及びいくつかのランダムマッピングプロセスを含んでいてもよい。１つの擬似ランダム生成プロセスは、その出力を１つ又はいくつかのランダムマッピングプロセスへ送信することができる。１つのランダムマッピングプロセスはまた、１つ又はいくつかの他のランダムマッピングプロセスからの出力を入力として受信することも可能であり、更にプロセス自体の出力のフィードバックを受信することも可能である。同様に、ランダム転送マップは場合により、暗号化セッション毎に変換されてもよい。

【００２２】

本開示の暗号プロセスは、いわゆる「暗号化構造（ｃｒｙｐｔｏｓｔｒｕｃｔｕｒｅ）」上にいくつかの方法で具体化可能であるが、当該暗号化構造は、適切なソフトウェアを備えたコンピュータ（デスクトップ、ラップトップ、ワークステーション、又はタブレットコンピュータ及び携帯電話を含む任意のもの）のみならず、現存している若しくは今後開発されるマイクロコントローラ、埋め込み式電子装置、専用電子回路、スマートカード、又はこれらの同等物のうち任意のものもまた含む（この「暗号化構造」の定義は、請求の範囲を含む本明細書全体において適用するものとする）。

【００２３】

（優位性）
本開示の暗号プロセスは、１つ又はいくつかのランダムシーケンスを鍵として使用する。現在に至るまで、このようなランダムシーケンスは再現不可能なように生成されていたため、ワンタイムパッドシステムが直面する鍵配送問題の要因となっていた。これはランダム性に関する誤解によるものであり、人々はこの誤解により、ランダムシーケンス生成器を用いて同一の（真）ランダムシーケンスを数回再現させることができなくなっている。再現可能なかかる生成器を本明細書において開示する。

【００２４】
多くの人々にとって、ランダム性とは、あらゆる規則から完全に免れるカオス現象から生じるもので、完全に予測不可能な結果をもたらすものである。実際に、カオス現象があらゆる規則に従わないとする場合、カオス系への同期は不可能となり、実験では全く正反対の結果を示すこととなる。

【００２５】
更に、サイコロを振る場合或いは不透明なバッグからカラーボールを引く場合、その結果はランダムであるとみなされる。しかし、バッグが不透明ではないとしたら、或いは、サイコロを全く同一の方法つまり同一の力かつ同一のエネルギー量を用いて振るとしたら、プロセスの完全な制御が存在し、望み得る結果がもたらされるため、その結果は、もはやランダムであるとはみなされないだろう。

【００２６】
したがって、ランダム性を結果の予測不可能性として定義することができ、これは、実際には、暗号化に使用されるランダム性の特性そのものである。この不確実性を得るためには、この結果は、完全な制御を有しないプロセスから生じなければならない。結果として、シーケンスが生じる生成プロセスにおいて幾分の制御も欠く限りは、あらゆるシーケンスがランダムであると演繹することができる。

【００２７】
したがって、制御されたプロセスと制御されていないプロセスとの混合からランダムシーケンスを得ることが可能であり、制御されていないプロセスは、シーケンスのランダム性を保証することが可能である。本明細書において開示する暗号プロセスでは、制御されていないプロセス由来の結果として生じるデータを有する者（及び有する者のみ）が再現可能な特徴を提示するランダムシーケンスを生成するために、いくつかの制御されたプロセスと制御されていないプロセスとの組み合わせを使用する。したがって、このようなランダムシーケンスを、ワンタイムパッドと同じ強度を有する暗号システムを生成するために使用することができ、これらの「一度だけの鍵」が実際には（本明細書において、メッセージングシステムの場合に例示として使用する）通信チャネルの両側で生成されるため、膨大な量の鍵を配送する必要性はない。

【００２８】
ここでは、制御されていないプロセス由来の結果として生じるデータのみが配送される必要がある。実際のところ、この暗号プロセスを使用することにより、無条件に安全な通信チャネルを実装可能であることが、本明細書の記載により理解されるだろう。このように、これらの鍵を（一旦確立されると）このチャネルを介して送信することが可能であるため、「鍵配送問題」は解決される。したがって、我々は、（「鍵配送問題」がなくなるわけではないが、）鍵配送問題が極めて些細であり、無条件に安全であり、利用可能な最も有用な暗号システムの１つを付与する、最も強力な暗号システムの１つを有することとなる。

【図面の簡単な説明】
【００２９】
【図１】本開示における暗号プロセスの基本的なオペレーションを示すフローチャートである。
【図２】任意選択的な機構を有するランダムシーケンス生成プロセスの内部オペレーションを示すフローチャートである。任意選択的なフローを破線で表す。

【発明を実施するための形態】
【００３０】
詳しい説明をより容易に理解するために、いくつかの図面を本明細書と共に提供する。しかしながら、全てのケースを１つの図面に統合することは不可能であった。それゆえ、発明を実施するための形態は、図面に明確に記載しない変形例を提示するものとする。実際、図面は、基本原理を視覚化するための一助となる。
【００３１】
ここで、様々な実施形態を説明する。本開示の暗号プロセス及びその実施形態の特徴に傾注することとする。したがって、当業者にとって既知である、暗号プロセスの強度を向上させるための全ての手法（冗長性を最小限に抑えるためのデータ圧縮、シーケンスのランダム性を増大させるための、連続的に入力し擬似乱数的に選択するバッファテーブルの使用等）については言及せずに、本開示の暗号プロセス及びその実施形態に対する有効性について示唆する。
【００３２】
（暗号プロセス）
装置の実施形態は、（通常）データの暗号化又は暗号化データの復号を行うために、暗号システムを実装し、本明細書で開示する新規の暗号プロセスを以下で説明する。本発明の暗号プロセスは、１つ又はいくつかのランダムシーケンス生成プロセス１（図１を参照のこと）、暗号化プロセス２、及び復号化プロセス３を使用する。ランダムシーケンス生成プロセス１は、１つ又はいくつかの擬似ランダムシーケンス生成プロセス６（図２を参照のこと）、及び１つ又はいくつかのランダムマッピングプロセス７に基づいている。
【００３３】
擬似ランダムシーケンス生成プロセスは、線形合同法（Ｌｉｎｅａｒ　Ｃｏｎｇｒｕｅｎｔｉａｌ　Ｇｅｎｅｒａｔｏｒ）アルゴリズム（又は、その群の一部）、逆数合同法（Ｉｎｖｅｒｓｉｖｅ　Ｃｏｎｇｒｕｅｎｔｉａｌ　Ｇｅｎｅｒａｔｏｒ）アルゴリズム（又は、その群の一部）、線形帰還シフトレジスタ（又は、一般化帰還シフトレジスタ）アルゴリズム、Ｂｌｕｍ　Ｂｌｕｍ　Ｓｈｕｂ擬似ランダム生成器アルゴリズム、（例えば、米国特許第５,０４８,０８６号を参照されるロジスティック差分方程式のような）１つ又はいくつかのカオス方程式に基づいたアルゴリズム、（例えば、米国特許第６,０７８,６６５号を参照されるＬｏｒｅｎｔｚ系のような）１つ又はいくつかのカオス方程式系に基づいたアルゴリズム、（例えば、ジュリア集合又はマンデルブロー集合のような）フラクタル方程式に基づいたアルゴリズム、若しくは、これらのうちのいずれか、ハッシュ関数を用いて出力をハッシュするその他の擬似ランダム生成アルゴリズム、開発者により所望された任意の擬似ランダム生成アルゴリズム（後ほど説明する混合演算、又は、いくつかの出力に由来する文字に対する任意の演算等を使用する）、又は、これらのうちのいくつかの任意の組み合わせを使用することができる。
【００３４】
「ランダムマッピングプロセス」とは、マップ選択プロトコルを使用して、受信シーケンス由来のそれぞれの文字を発信シーケンスのランダム文字へとマッピングするために、「ランダム転送マップ」４と称するランダムな文字列を使用するプロセスである。「マップ選択プロトコル」とは、入力データ由来のシーケンス中の要素を選択する方法であり、その方法は、例えば、モジュロインデックス化、正規化インデックス化、ｎ次元テーブルインデックス化、微調整したｎ次元テーブルインデックス化又はシーケンス（ここでは、ランダム転送マップ）からどの文字を選択するかを決定するために、１つ又はいくつかの文字を入力として使用する任意のアルゴリズムである。
【００３５】
モジュロインデックス化プロトコルは、入力文字を数字として使用することにあり、この数字は、出力文字を選択するシーケンス中のランクを示すこととなる。入力文字が数字でない場合、（ＡＳＣＩＩ、ＡＮＳＩ又はＵｎｉｃｏｄｅのような）いくつかのコード体系内におけるコーディング数字を入力数字としてみなすことができる。入力数字が（シー

ケンスの要素数である）シーケンスのサイズよりも大きい場合、シーケンスのサイズによるランク数字のユークリッド除法の剰余を使用する（故にモジュラ算術演算であるため、「モジュロ」）。

【００３６】

正規化インデックス化プロトコルは、モジュロ演算の代わりにランクがシーケンスのサイズに正規化されることを除いて、モジュロインデックス化プロトコルと類似している。これは、ランクを出来る限り最上位ランクで除してから、その計算結果にシーケンスのサイズを乗じることを意味する。ランク番号が１から始まる場合、その計算結果を切り上げ、又は、ランク番号が０から始まる場合、その計算結果を切り下げる。

【００３７】

ｎ次元テーブルインデックス化プロトコルでは、シーケンスは、ｎ次元を有するテーブルからの一連の線分としてみなされる。これは、シーケンスのサイズが、それぞれの次元において、テーブルのサイズの積でなければならないことを意味する。このプロトコルは、テーブル内で文字座標を選択する際、数字とみなされるｎ個の受信文字を使用する。

【００３８】

微調整したｎ次元テーブルインデックス化プロトコルは、選択する文字座標の計算方法以外は、ｎ次元テーブルインデックス化プロトコルと類似している。ここでは、演算がテーブルの次元内に座標を与える限り、入力文字に対して行われる任意の演算が適合することとなる。例えば、モジュラ算術、「排他的論理和」のような論理演算、又は（ＤＥＳのＳボックスのような）数字を形成するための選択ビットの選択を挙げることができる。

【００３９】

本実施形態は、通常、いくつかのマップ選択プロトコルを提供し、使用するプロトコルをユーザに選択させる。しかしながら、マップ選択プロトコルによって文字を選択するために使用する文字インデックス法は、ランダム転送マップの生成中に使用する方法とは異なる場合があるということに留意すべきである。例えば、ＡＮＳＩのランダムな文字列を生成し、その後、マップ選択プロトコルにおいて当該ランダムシーケンスをビットのシーケンスとみなすことが可能であり、逆の場合もまた同様である。実際、これにより、ランダムマップ作成プロセスを、出力ランダムシーケンスに必要な文字型から完全に分離することが可能となる。

【００４０】

ランダムマッピングプロセス７の受信シーケンスは、擬似ランダム生成プロセス６から得られる擬似ランダムシーケンス（プロセスの出力の（以下で定義する）「混合演算」を出力として使用した、いくつかの擬似ランダムシーケンス生成プロセスの組み合わせは、実際、１つの擬似ランダムシーケンス生成プロセスとみなされることに留意すべきである）、前のランダムマッピングプロセス８から得られるランダムシーケンス、いくつかの前のランダムマッピングプロセス８から得られるいくつかのランダムシーケンスの（プロセス文字の「混合演算」を使用する）組み合わせ、又は、これらの可能性のうちの（プロセス文字の「混合演算」を使用する）いくつかの組み合わせであり得る。

【００４１】

「混合演算」とは、開発者が望む入力文字に対する「排他的論理和」、モジュラ加算、モジュラ減算、連結、Ｖｉｇｅｎｅｒｅ暗号化、Ｂｅａｕｆｏｒｔ暗号化、換字式暗号法、モジュラ線形結合法、任意の演算又は演算シーケンスのことを意味し、この計算により、結果として１つの文字又はいくつかの文字のシーケンスが与えられる。この定義は、本明細書全体（明細書、請求の範囲、要約書）に対して適用するものとする。

【００４２】

いくつかの代替的な実装において、受信シーケンスは、上記で説明した受信シーケンス及び真性ランダム（ｖｅｒｙ　ｒａｎｄｏｍ）マッピングプロセス７の発信シーケンスの両方から、フィードバックとして得られる。これらの代替的な実装のうちのいくつかにおいて、その他の受信シーケンスの次の文字が処理される前に、フィードバックは、所定の回数、（ランダムマッピングプロセス中に）ループで処理される。これらの代替的な実装

のうち他の実装では、フィードバックの文字は、「混合演算」を使用して、（複数の）その他の受信シーケンスの文字と組み合わされる。これらの他の代替的な実装のうちのいくつかにおいて、フィードバックは、所定の文字数だけ遅延する。いくつかのその他の実装において、前述し提供した構成のいくつか又は全ては、どの構成を使用するかをユーザに選択させるいくつかの実行可能な「回路」を含む。また、いくつかの実装においては、ユーザはこの回路を設計することさえできる。

【００４３】

「回路」とは、ランダムシーケンス生成プロセスの内部プロセス（擬似ランダムシーケンス生成プロセス及びランダムマッピングプロセス）の出力及び入力が、互いに接続している方法を意味する。回路はまた、どのランダムマッピングプロセスの出力をランダムシーケンス生成プロセスの出力として使用するかを特定する。

【００４４】

ランダム転送マップ４とは、「ランダム性生成」９により生成されたランダムな文字列のことであり、当該マップは、本実施形態のランダムマッピングプロセス７へと提供される。このランダム転送マップは、本発明のランダムシーケンス生成器の（当業者には「エントロピー」としても知られている）ランダム性の源である。発明者は、ランダム性が２つの事柄、つまり、予測不可能性及び制御の欠如を示唆することを理解した。予測不可能性とは、ランダム転送マップを秘密に保持し、かつ、「敵」にアクセス不能な状態にする必要があることを示唆する（また、ユーザにもアクセス不能な状態にすることが推奨される）。制御の欠如は、ランダム性生成を定義可能な条件を示唆する。

【００４５】

「ランダム性生成」とは、文字を生成するために、数学又は計算を使用せずに（又は全面的には使用せずに）、１つ又はいくつかの制御されていない現象を使用する生成のプロセスである。このプロセスの最も明白な実施形態のうちのいくつかは、ハードウェアによる「真」ランダム生成器である。このようなハードウェアは例えば、（「ランダム性抽出」として知られている）アルゴリズムによって後処理されるランダム値の源として、電子ノイズを使用する。別の例としては、放射性物質の各分解の間の時間を測定するという、より稀なハードウェアが挙げられる。

【００４６】

実施形態の別の群は、一切合理的選択をすることなく選択されるテキスト１０（又は、コンパイルされたプログラムバイナリ若しくはファイル）を、ランダム性の源として使用する。実際のところ、秘匿されたテキストにおいて、どの文字が決定された場所に存在するのかを知ることは誰にもできない。しかし、通常、テキストは、「換字演算」を用いて１回又は数回、後処理される。本実施形態は後処理するべきであるため、後処理は通常、再現可能でなければならない。たとえ換字演算ではないにしても、極めて周知の後処理は、データを複数のビットブロックに分け、それからこれらのブロックをハッシュ関数（いわゆる「一方向性関数」であり、関数を用いて特定サイズのビットの結果を容易に計算することができるが、妥当な時間内にその計算結果から関数の入力を特定することはできない）を用いて処理することである。

【００４７】

換字演算とは、特定されたプロトコル及び、通常は外部データを使用して、１つの文字を別の文字へと置換するプロセスである。外部データとしては、別のテキスト由来の文字、無作為にタイプされループで使用される文字又は任意の他のデータ源であってもよい。特定されたプロトコルは、テキストの文字と外部データとの間の１つ又はいくつかの（上で定義したような）「混合演算」、外部データを（複数の）鍵として使用した（ブロック暗号、ストリーム暗号又は任意のものによる）テキストの暗号化、若しくは、更により複雑なプロトコルであってもよく、又はこれらのうちのいくつかの組み合わせであってもよい。特定されたプロトコルが、上記に記載した再現性の条件に従っていることに留意されたい。

【００４８】

いくつかの実施形態では、ランダムシーケンス生成プロセス１は、また、ランダム転送マップ変換プロセス１１を含む。このプロセスは、提供されたパラメータ（無作為にタイプされた文字、無作為に生成した文字又は任意のデータ）及び１つ又はいくつかの混合演算を使用して、提供された（「一次ランダム転送マップ」と称することとなる）ランダム転送マップを、（「二次ランダム転送マップ」と称することとなる）別のマップへと変換する。二次ランダム転送マップが、（それぞれのパラメータの文字を有する一次ランダム転送マップのそれぞれの文字に対して、（複数の）混合演算を適用し、全ての一次ランダム転送マップが処理されるまでパラメータをループすることにより）生成され、一次ランダム転送マップの代わりにランダムマッピングプロセスにより使用されることとなる。このような機構は、通常、暗号化セッション毎に提供された異なるパラメータで使用され、通常１つのセッションのランダム転送マップ変換毎に異なるパラメータで使用される。

【００４９】

いくつかの代替の実施形態では、（ちょうど本明細書で開示するプロセス１のような）ランダムシーケンス生成プロセスは、一次ランダム転送マップを二次ランダム転送マップへ変換するために使用されるが、当該プロセスは、専用の別個のプロセスであってもよく、或いは、暗号化プロセス及び/又は復号化プロセスにより使用されるプロセスの一部（又は、全体）であってもよい。この構成では、提供されたパラメータを使用して、ランダムシーケンス生成プロセスを開始し、生成したランダムシーケンスを使用して、混合演算を使用して一次ランダム転送マップを変換する。いくつかの代替の実施形態では、一次ランダム転送マップを変換する代わりに、生成したランダム出力を直接二次ランダム転送マップとして使用する。

【００５０】

いくつかの実施形態では、ランダムシーケンス生成プロセス１は、また、擬似ランダム生成プロセス６のために、（シーケンスの計算を開始するために擬似ランダムシーケンス生成器が必要とする開始データであり、これらのデータの値は、シーケンスの文字に影響を及ぼす）シード５を計算する、シード生成プロセス１２を含む。シード生成プロセス１２は、提供又は選択された文字に対して「シード計算アルゴリズム」を使用するが、かかる選択された文字は、場合により、コンピュータメモリ又は１つ若しくはいくつかのランダム転送マップ４の一部から得られる。「シード計算アルゴリズム」とは、（複数の）シードとして使用する（複数の）ある値を出力するために、入力文字に対して、算術演算、混合演算、若しくは任意の演算等、又は、これらのうちのいくつか（又は全て）の組み合わせを使用するアルゴリズムである。

【００５１】

少なくとも暗号化プロセス２及び復号化プロセス３の両方を、同一の暗号装置或いは別々の暗号装置で実施することができる。シード計算アルゴリズムは、あらゆる暗号スキーム、つまり、Ｖｉｇｅｎｅｒｅ暗号、Ｂｅａｕｆｏｒｔ暗号、ブロック暗号、ストリーム暗号又は開発者が望む任意の暗号スキームを使用することができる。シード計算アルゴリズムは、また、ランダムシーケンス生成プロセスが必要とする任意の数の鍵を使用することができる。実際のところ、暗号化プロセス及び復号化プロセスの両方は、いくつかの鍵（通常は別々の鍵）を使用し、数回データを処理することができる。

【００５２】

（暗号装置）

実施形態の１つの群では、独立型若しくはネットワーク接続型の１つ若しくはいくつかのコンピュータ、タブレットコンピュータ又は携帯電話は、データを暗号化又は暗号化データを復号するために、ソフトウェアを使用し、上で開示した暗号プロセスの後に、暗号化プロセス２及び復号化プロセス３は、両方とも同一のコンピュータ上（以下において、単語「コンピュータ」は、また、タブレット及び携帯電話を含むこととなる）に存在するか、又は、（両方のコンピュータはランダムシーケンス生成プロセスを有する）別々のコンピュータ上に存在する。ソフトウェア内の暗号プロセスの実装は、明白である。

【００５３】

装置の実施形態の第２の群では、専用電子回路は、上で開示された暗号プロセスを実装する。このような回路は、いくつかの部分からなり、それぞれの部分は、上記の暗号プロセスの工程のうちの１つを実装する（ランダムシーケンス生成プロセス１を実装するためのランダムシーケンス生成器、データ暗号化プロセス２を実装するための暗号化部（ｃｉｐｈｅｒｅｒ）、暗号化データの復号化プロセス３を実装するための復号部（ｄｅｃｉｐｈｅｒｅｒ）、擬似ランダムシーケンス生成プロセス６を実装する１つ又はいくつかの擬似ランダム生成器からなるそれぞれのランダムシーケンス生成器及びランダムマッピングプロセス７を実装する１つ又はいくつかのランダムマッパユニット（ｍａｐｐｅｒ　ｕｎｉｔ））。

【００５４】

本開示の暗号プロセスの後、擬似ランダム生成器及びランダムマッパユニットは、回路内において共に接続される。この回路は、通常、ハードウェアであるが、論理的に又はソフトウェアで切り換える回路のいくつかの実施形態を後に参照することとする。ハードウェアのケースでは、１つ又はいくつかの回路が提案可能である。これらの回路は、切り換え可能であるか又は並行して動作可能である。

【００５５】

それぞれのランダムマッパユニットは、ランダムマッパユニット内部の（例えば、メモリ又はフラッシュカードのような）記憶ユニット内に記憶されている、（前に定義されたような）提供されたランダム転送マップ４を使用するが、このランダム転送マップは、（前に定義及び前述したような）ランダム性生成９により生成される。

【００５６】

ある代替の実施形態では、ランダムシーケンス生成器のそれぞれは、また、ランダム転送マップ変換プロセス１１を実装するランダム転送マップ変換器を備える。

【００５７】

いくつかの実施形態では、いくつかのマイクロコントローラも組み込んだ電子回路は、（他の物との間に）いくつかのプログラマブルマルチプレクサを実装可能であるが、以下のことを可能とする。それぞれのランダムシーケンス生成器１内部の回路をプログラムすること、暗号スキームを選択するために、暗号化回路を選択すること（又はその回路の計算アルゴリズムを実装すること）、復号に関する同一のこと、生成アルゴリズムを選択するために擬似ランダム生成器を選択すること（又はその生成器の計算アルゴリズムを実装すること）等。

【００５８】

いくつかの実施形態では、シード生成プロセス１２が、シード生成器により実装されている。通常はハードウェアに実装されるが、マイクロコントローラで実行させるために、ソフトウェアに（部分的又は全面的に）実装することも可能である。同様に、いくつかの実施形態では、ハードウェア内部の場合もあるが、通常、マイクロコントローラを備えたソフトウェア内部において、ランダム性生成９が実装される。

【００５９】

本明細書に記載する暗号プロセスを実装するいくつかの他の種類の装置の実施形態もまた存在する。実装する機構の量は、実施形態で使用する構造の容量及び計算能力によって決まる。

【００６０】

１つの種類の実施形態は、暗号システムがマイクロコントローラ上に実装されるものである。それは、第１の群の実施形態のある種のポケットの実装（ｐｏｃｋｅｔ　ｉｍｐｌｅｍｅｎｔａｔｉｏｎ）である。暗号プロセスは、通常、マイクロコントローラ上のソフトウェア内に実装されるが、当該マイクロコントローラは多少の電子回路と接続し、データ入力用のボタン、ジョグホイール及びその他のデバイス並びにＵＳＢデータストレージ又はインターネットアクセス用のいくつかのプラグを備える（が、Ｗｉ－Ｆｉも搭載可能である）。操作に関し、ユーザは、マイクロコントローラ上のソフトウェアと対話するためのデータ入力に、デバイスを使用する。

【００６１】
別の種類の実施形態は、スマートカードに関するものである。暗号プロセスは、（限られた容量及び計算能力を有する）チップに搭載されたソフトウェア内に実装される。開発者は、（スコープステートメントにより求められるものに応じて）どの機構をチップ上に実装するかを注意深く選択するべきである。このような実施形態は、例えば、本人確認又は銀行の取引若しくは引き出しに使用することができる。これらの実施形態は、スマートカードを使用するかのように実行される。
【００６２】
前述した種類の実施形態の両者の組み合わせは、ある種のＵＳＢキーに関するものであり、ＵＳＢキーは、フラッシュメモリの代わりに、通常、スマートカード等の小さなチップが一緒に組み込まれた一部の電子部品である。それは、実際には、暗号化用途に使用するコンピュータ用のＵＳＢプラグ及び再生デバイスである。それらの動作は、明白である。
【００６３】
特殊な種類の実施形態は、暗号システム生成器（ｃｒｙｐｔｏｓｙｓｔｅｍ　ｍａｋｅｒ）であるが、当該生成器は、コンピュータメモリ内に搭載すると、コンピュータに本開示の暗号プロセスを実行させるように構成されたコンピュータプログラムコードを格納するストレージユニットである。このようなストレージユニットは、「記憶媒体」と称されるものを使用して製造される。「記憶媒体」は、ハードドライブ、ＵＳＢキー、ＣＤ-ＲＯＭ、ＤＶＤ－ＲＯＭ、フラッシュカード又はコンピュータプログラムコードを記憶可能な任意のもの及びコンピュータシステムがこのプログラムコードをメモリへロードするためにアクセス可能な任意のものである（この「記憶媒体」の定義は、請求の範囲を含む本明細書全体において適用するものとする）。
【００６４】
（実施形態のオペレーション）
装置の実施形態の第１の群のオペレーションに関して言えば、（タブレット及び携帯電話を含む）コンピュータの設定は、当業者にとって明白であり、それは、つまり、適切なソフトウェアをコンピュータへ提供し、コンピュータは、コンピュータのメモリへソフトウェアをロードすることである。それから、このプログラムにより、本開示の暗号プロセスをコンピュータに実行させるように構成することとなる。
【００６５】
コンピュータの設定後、ランダム転送マップをランダムシーケンス生成プロセスへと提供する。これらのランダム転送マップは、データへのアクセスを許可されたユーザのコンピュータにのみ提供されるべきである。実施形態がランダム転送マップ生成プロセスを実装する場合、処理セッションのパラメータが生成プロセスへと提供され、ランダム転送マップから二次ランダム転送マップが生成され、その後、ランダムシーケンス生成プロセスにおいて、ランダム転送マップがその対応する二次ランダム転送マップと置き換わる。（他の新規セッション中、他のセッションパラメータからの）他の二次ランダム転送マップを生成するために使用可能とするために、一次ランダム転送マップは、どこに格納されていてもよい。
【００６６】
動作させたいデータをコンピュータへ提供する。データは、既にハードドライブ上（又は任意の他のドライブ上）にあってもよく、或いは、ネットワークから受信してもよいが、データは、コンピュータのメモリ内へとロードされる。（実装に応じて）１つ又はいくつかのランダムシーケンス生成プロセスは、（暗号化/復号化プロセスに必要な鍵の数に応じて）処理するデータと同一の長さの１つ又はいくつかのランダムな文字列を生成する。
【００６７】
このタスクに関して、（必要なシードの数に応じて）１つ又はいくつかのシードが擬似ランダムシーケンス生成プロセスへ提供され、それから発信擬似ランダムシーケンスが（

複数の）ランダムマッピングプロセスへと送信されるが、ランダムシーケンス生成プロセスにより最後の発信ランダムシーケンスが暗号化プロセス（又はタスクにより復号化プロセス）へと送信されるまで、（複数の）発信ランダムシーケンスは実装した「回路」に従う。

【００６８】

このプロセスでは、データをメモリから取り出し、実装したアルゴリズムを使用してデータを暗号化（それぞれ復号化）し、メモリへとデータを返送する。次に続くのは、データに対して何をしたいかによる（ハードドライブ上に若しくは任意の他のドライブ上にデータを記憶するか又はネットワークを介し離れた受信者へとデータを送信するか等）。

【００６９】

ランダム転送マップをランダムシーケンス生成器へ提供するいくつかの方法がある。すなわち、（例えば、信頼できる人物が送達又は配送する）ＵＳＢキー又はシリアルナンバーが付いたＣＤ-ＲＯＭを使用して、ランダム転送マップを暗号装置（コンピュータ等）へと物理的に転送してもよく、本開示の暗号プロセスを使用して符号化した安全なチャネルを使用して、（例えば、ネットワークを介して）データを送信してもよく、暗号装置上でデータを生成してもよい。物理的に転送したマップの場合、ランダム転送マップは、（例えば、ハードウェア上の「真」のランダム生成器を使用して）どこかに生成され、それから「権限のある」ユーザの暗号装置（例えば、ドライブ上、ＣＤ-ＲＯＭ上又はＵＳＢキー上）へと転送され、最終的に装置内へ適切な場所へ転送される。重要な用途においては、この場所を、認可管理者以外のユーザには、アクセス不能な状態にしておく方がよい。

【００７０】

このような方法及び後ほど参照するその他の設定を用いれば、符号化されたチャネルを（例えば、ネットワークを介して又はあらゆる通信手段を介して）実装することが可能となり、このことは、データが符号化された双方向性通信を意味する（用語「安全なチャネル」もまた当業者は使用する）。このようなチャネルは、（暗号文単独攻撃に対して）無条件に安全であるため、それ故に、物理的な転送の代わりに当該チャネルを使用して、必要に応じて新規のランダム転送マップを転送することが可能となる。

【００７１】

ランダム転送マップがコンピュータへ転送されない場合、ファイルを選択し、通常は搭載された換字演算を使用してファイルを変換する。データのうちのいくつかを符号化したい単一ユーザにとって、ファイルは、自身のドライブ上又はインターネット上のあらゆるファイルであってもよく、それはつまり、データの復元を可能にするために、使用したファイル及び外部データがどれであるかを記憶しておけばよいだけである。共通データを使用及び送受信する数人のユーザがいるネットワークでは、同一のランダム転送マップを生成可能とするためには、全員が同一のデータを有していなければならない。これは通常、選択する（複数の）ファイルの（複数の）アドレス（インターネットのＵＲＬ又はファイルシステムパス）を他のユーザのうちの１人又は全員に送信することで行われ、また場合により、例えば、公開鍵暗号法又は後ほど説明する無条件に安全なチャネルを使用して、外部データを残すことにより行われる。したがって、受信者のそれぞれは、自身のコンピュータに自身の適切なランダム転送マップを計算させる。

【００７２】

本実施形態において機構を実装する場合、コンピュータに搭載したランダム転送マップの生成に使用する同一の手順は、二次ランダム転送マップの生成に必要なパラメータに対して使用される。この場合、回路、ファイル又は外部データ（無作為にタイプされた文字、無作為に生成した文字、又は任意のデータ）は、（上記で参照した方法を用いて）ランダム転送マップの全てを送信する必要なしに、それぞれの暗号化セッションにおいて新規のランダム転送マップ（二次ランダム転送マップ）を生成するために、ランダム転送マップ変換プロセスにより使用される。

【００７３】

この機構の利点は、ファイル又は外部データが通常、ランダム転送マップのサイズよりもかなり小さいサイズを有しているという点であり、また１つの外部データ群を全てのランダム転送マップの変換に使用してもよく、それによりランダム転送マップの変更のための通信がより短くなる。実際のところ、既に出力したシーケンスを生成することを防止するために、擬似ランダムシーケンス生成プロセスがループバックする前に、ランダム転送マップは通常、変更される。したがって、データ処理に必要な長さが、擬似ランダムシーケンスの最大長（ランダムマッピングのフィードバックを使用する場合、実際にはランダムシーケンスの最大長）を超過していないことを確認する必要があるので、それぞれの暗号化セッションの前にランダム転送マップを変更することにより、擬似ランダムシーケンス生成の管理を簡略化することが可能となる。

【００７４】

擬似ランダムシーケンス生成プロセスに必要なシードを提供するために、いくつかの方法が可能である。例えば、データの符号化を望む単一ユーザに関して、ソフトウェアが、（ユーザは正確に記憶する必要がある）ユーザが使用したいシードの入力をユーザに求める場合もあり、或いは、最初の文字、最後の文字、又は（開発者により）事前に定義された文字がシードとして使用されるファイル（圧縮されている若しくは圧縮されていない、テキストファイル又はバイナリファイル）をユーザに要求する場合もある。しかし、別の方法としては、１つ又はいくつかのランダム転送マップの少しの部分（通常マップの終端）、つまり、ランダムマッピングプロセスによっては使用されずにシードとして使用されるデータを保存することであり、或いは、（シードの値と共にシード生成プロセスを使用して）シードを計算することである。この最後の方法の利点は、ユーザがシードについて注意を払う必要がないということである。ランダム転送マップ変換プロセスを実装した場合、ランダム転送マップの保存部分もまた換字演算により変換されるため、セッション毎にシードが変更されるということもまた理解できる。

【００７５】

複数ユーザの構成においては、上記で説明したシード生成のための、（複数の）ランダム転送マップにおける保存された部分の方法もまた実装可能である。実際のところ、ランダム転送マップ変換プロセスの実装とランダム転送マップの物理的転送とを組み合わせて、（擬似ランダムシーケンス生成プロセスへとシードを提供するための）この方法を使用することにより、（前述した通り）ネットワークに亘って無条件に安全な通信チャネルを構築することが可能となる。ランダム転送マップが無作為に生成され（故に、文字のあらゆる可能な組み合わせのうち任意であり得る）、かつ任意のサイズであってもよいので、擬似ランダムシーケンス生成アルゴリズムが多くのアルゴリズムのうちの１つであり、かつシードが未知であり得るため、或いは、ランダムシーケンス生成プロセスにより内部で使用される「回路」がかなり多くの回路のうちの１つであるため、「敵」は暗号プロセス内部で何が起こっているのかを知る手がかりを持たず、またワンタイムパッド同様、敵にとって、任意の文字の組み合わせが暗号鍵となり得る同一の確率を有する。

【００７６】

ランダム転送マップ変換プロセスのパラメータを見ることは、ランダム転送マップがランダムでありかつそのサイズが未知であるため、擬似ランダムシーケンス生成アルゴリズムが未知であるため、シードの変換が未知であるため、選択されたランダムシーケンス生成プロセスの内部回路が未知であるため、ランダム転送マップ変換プロセスが使用する（複数の）混合演算が未知であるため、使用する暗号化プロトコルが未知であるため、及びその他のいくつかのパラメータが未知であるため、敵にとっては何の助けにもならない。したがって、本発明の特定のケースでは、ランダム転送マップ変換プロセスのためのこれらのパラメータを、暗号化する必要なしにその他のユーザへ送信することが可能となる。

【００７７】

また、本発明の特定のケースでは、依然として、これらのパラメータが通信セッションの開始に必要なデータにすぎないため、システムは無条件に安全であり、例えば、新規のランダム転送マップのようなあらゆるその他の必要なデータは、安全なチャネルを介して

送信可能である。したがって、システムの設定には物理的な転送のみが必要である。例えば、ランダム転送マップ（場合によりシード）を含むシリアルナンバー付きＣＤ－ＲＯＭを使用することにより、この転送が実行可能となるため、ユーザは、符号化されたチャネルを構築するためにパラメータとしてのシリアルナンバーを送信しさえすればよい。

【００７８】

無条件に安全な通信チャネルに関するこのケース以外で、擬似ランダムシーケンス生成プロセスに必要なシードを提供するためのその他の方法は、公開鍵暗号法又は開発者が望む任意の方法であってもよい。

【００７９】

単一ユーザの構成と複数ユーザの構成の両方に対して、ランダム転送マップ変換プロセスを利用できない場合、ランダム転送マップ毎に一度だけシードが必要であること、また次回シードとして使用するために、擬似ランダムシーケンスが最大長に達するまで最後の値がレジスタ内に保存されること、に留意されたい。その後、最大長に達する前にランダムシーケンスを繰り返さないために、ランダム転送マップを変更することに留意されたい。

【００８０】

重要な用途に関して、ある興味深い構成が存在する。それはつまり、暗号装置が、中央でネットワークサーバと、（少なくとも）ネットワークサーバにのみ接続するその他のデバイスと、「スター型ネットワーク」で（場合により無線で）接続する構成である。それぞれのデバイスがサーバと通信する（ランダム転送マップ等の）データのみを有する一方で、サーバは、全てのデバイスと通信するデータを有する。１つのデバイスをその他のデバイスと安全なチャネル上で通信させたい場合は、先ずデバイスにおいてメッセージを暗号化し、その暗号化メッセージをサーバへと送信し、それからサーバにおいてそのメッセージを復号し、その復号メッセージをその他のデバイスのデータを用いて再暗号化し、その再暗号化メッセージをその他のデバイスへと送信し、最後にその再暗号化メッセージを復号してもよい。このような構成の利点としては次のことが挙げられる。（サーバを除く）デバイスが敵によって捕捉された場合であっても、敵は、捕捉したデバイスのデータを用いてその他の通信を復号することはできない。

【００８１】

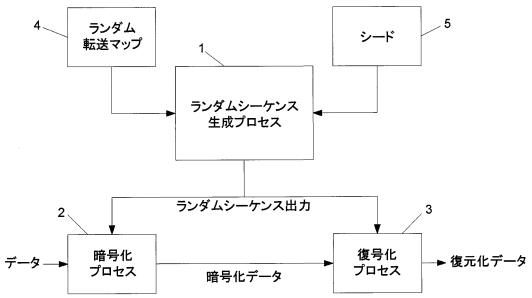
装置の実施形態の第２の群のオペレーションに関して言えば、実施形態の第１の群の場合と同様に、オペレーションは正確に動作する。一般的に、専用電子回路とは、より大きな電子機械の一部にすぎない。時に専用電子回路は、ＣＰＵの代わりに専用の計算を実行するために、コンピュータに接続する電子部品である。そのため、実施形態のこの群は通常、「マスター」回路により制御される「スレーブ」回路を含む。

【００８２】

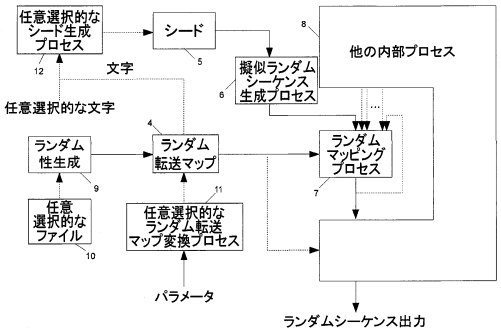
（ベストモードの問題）

本開示の暗号プロセスがいくつかの方法で実装可能であることを考慮し、異なる用途には異なるニーズが求められることを考慮すると、反対のニーズは反対の基準をもたらすことになるため、ベストモードを推定することは困難である。

【図１】


4
ランダム
転送マップ
1
ランダムシーケンス
生成プロセス
シード
5
ランダムシーケンス出力
2
暗号化
プロセス
3
復号化
プロセス
データ
暗号化データ
復元化データ

【図２】


任意選択的な
シード生成
プロセス
12
シード
5
8
他の内部プロセス
文字
擬似ランダム
シーケンス
生成プロセス
6
任意選択的な文字
4
ランダム
性生成
ランダム
転送マップ
ランダム
マッピング
プロセス
7
9
11
任意
選択的な
ファイル
10
任意選択的な
ランダム転送
マップ変換プロセス
パラメータ
ランダムシーケンス出力

フロントページの続き

(56)参考文献 特開２００７－０３４８３６（ＪＰ，Ａ）
特開２００６－２１５８２４（ＪＰ，Ａ）
特表２０１０－５１５０８３（ＪＰ，Ａ）
特表２００９－５０６４３８（ＪＰ，Ａ）
米国特許出願公開第２００５／０２２６４０８（ＵＳ，Ａ１）
米国特許出願公開第２０１０／０２１１７８７（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／２２
Ｈ０４Ｌ　　９／０８