(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5106124号
(P5106124)
(45)発行日　平成24年12月26日(2012.12.26)　(24)登録日　平成24年10月12日(2012.10.12)

(51)Int.Cl.　F I
G09C 1/00 (2006.01)　G09C 1/00 610A

請求項の数 35 (全 20 頁)

(21)出願番号　特願2007-557086(P2007-557086)
(86)(22)出願日　平成18年2月21日(2006.2.21)
(65)公表番号　特表2008-532075(P2008-532075A)
(43)公表日　平成20年8月14日(2008.8.14)
(86)国際出願番号　PCT/US2006/005942
(87)国際公開番号　WO2006/091528
(87)国際公開日　平成18年8月31日(2006.8.31)
審査請求日　平成21年2月17日(2009.2.17)
(31)優先権主張番号　11/064,912
(32)優先日　平成17年2月24日(2005.2.24)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　302070822
アクセス　ビジネス　グループ　インターナショナル　リミテッド　ライアビリティ　カンパニー
アメリカ合衆国，ミシガン　４９３５５，エイダ，フルトン　ストリート　イースト　７５７５
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100086771
弁理士　西島　孝喜
(74)代理人　100109070
弁理士　須田　洋之

最終頁に続く

(54)【発明の名称】三段階のデータ暗号化システム及び方法

(57)【特許請求の範囲】
【請求項１】
メモリに記憶された暗号化プログラムを実行する暗号化プロセッサを備えた暗号化装置で実施されるメッセージの暗号化方法であって、
前記暗号化プロセッサは、
前記メモリに記憶された既知の暗号キーＥと、第１の非公開素数Ｐと、第２の非公開素数Ｑとを読出し、当該既知の暗号キーＥ、第１の非公開素数Ｐ、第２の非公開素数Ｑを用いた関数に基づき、前記暗号化プロセッサに入力されたメッセージ内容を第１の形式Ｍから第２の形式Ｍ´に変換し、
前記メッセージ内容を前記第２の形式Ｍ´に変換した後、前記メッセージ内容を更に暗号化するために、前記メモリに記憶された第３の非公開素数Ｒを読出し、少なくとも前記第３の非公開素数Ｒを用いた関数により算出したスペースパターン(spacing pattern)に従って前記変換されたメッセージ内容にスペース又は対応する値を挿入して前記メッセージ内容を複数のメッセージ部分に分解し、
前記メッセージ内容を前記第２の形式Ｍ´に変換した後、前記メッセージ内容を更に暗号化するために、前記メモリに記憶された第４の非公開素数Ｓを読出し、少なくとも前記第４の非公開素数Ｓを用いた関数により算出したスクランブルパターン(scrambling pattern)に従って前記変換されたメッセージ内容の値を反転したり、一定値を加算したり、任意の関数式に基づく値に変換することを含むスクランブル処理、
を実行する前記メッセージの暗号化方法。

【請求項２】
前記暗号化プロセッサは、前記メッセージ内容をアルファベット構文から数値表現に変換することを更に実行する、請求項１に記載の方法。
【請求項３】
前記メッセージ内容は、前記暗号化プロセッサにより前記メモリから読出されたハッシュ関数を用いてアルファベット構文から数値表現に変換される、請求項２に記載の方法。
【請求項４】
前記メモリに記憶された前記既知の暗号キーは、前記第１の非公開素数及び前記第２の非公開素数に互いに素である、請求項１に記載の方法。
【請求項５】
前記暗号化プロセッサは、前記メッセージ内容を、以下の関数式

$$M' = M^{E} \bmod (P * Q)$$

に従い、第１の形式Ｍから第２の形式Ｍ´に変換する、請求項４に記載の方法。
【請求項６】
前記メッセージ内容を分解するためのスペースパターンは、第３の非公開素数Ｒと係数Ｋとの関数である以下の関数の式

$$F(R) = R * \bmod (K)$$

に従い算出される、請求項１に記載の方法。
【請求項７】
スペースパターン(spacing pattern)に従い前記メッセージ内容を分解する処理は、前記メッセージ内容を複数の個々のパケットにパルス化する(pulsing)ことを含む、請求項６に記載の方法。
【請求項８】
前記暗号化プロセッサは、スペースパターンに従い前記メッセージ内容を分解する処理において、前記メッセージ内容を複数のグルーピングに割り振るために、余分な文字を前記メッセージ内容に挿入することを含む、請求項６に記載の方法。
【請求項９】
前記余分な文字は、空白文字(space)である、請求項８に記載の方法。
【請求項１０】
前記スクランブルパターンは、秘密係数Ｊと第４の非公開素数Ｓとの関数である以下の関数式

$$G(S) = S * \bmod (J)$$

に従い算出される、請求項１に記載の方法。
【請求項１１】
前記暗号化プロセッサは、前記メッセージ内容を変換後、前記メッセージ内容を分解し、前記メッセージ内容をスクランブルして生成した暗号化メッセージを通信ネットワークを介して受信装置に送信する、請求項１に記載の方法。
【請求項１２】
第１のメモリに記憶された暗号化プログラムを実行する暗号化プロセッサを備えた暗号化装置と、第２のメモリに記憶された復号化プログラムを実行する復号化プロセッサを備えた復号化装置で実施されるメッセージの暗号及び復号化方法であって、
前記暗号化プロセッサは、
前記メモリに記憶された既知の暗号キーＥと、第１の非公開素数Ｐと、第２の非公開素数Ｑとを読出し、当該既知の暗号キーＥ、第１の非公開素数Ｐ、第２の非公開素数Ｑを用いた関数に基づき、前記暗号化プロセッサに入力されたメッセージ内容を第１形式Ｍから第２形式Ｍ´に変換し、
前記メッセージ内容を前記第２の形式Ｍ´に変換した後、前記メッセージ内容を更に暗

号化するために、前記メモリに記憶された第３の非公開素数Ｒと、既知である第２の暗号キーＫとを読出し、前記第３の非公開素数Ｒ及び前記第２の暗号キーＫを用いた関数により算出したスペースパターン(spacing pattern)に従って前記変換されたメッセージ内容にスペース又は対応する値を挿入して前記メッセージ内容を複数のメッセージ部分に分解し、

前記メッセージ内容を前記第２の形式Ｍ´に変換した後、前記メッセージ内容を更に暗号化するために、前記メモリに記憶された第４の非公開素数Ｓと、秘密係数Ｊとを読出し、前記第４の非公開素数Ｓ及び前記秘密係数Ｊを用いた関数により算出したスクランブルパターン(scrambling pattern)に従って前記変換されたメッセージ内容の一定値を加算したり、任意の関数式に基づく値に変換することを含むスクランブル処理を行い、

暗号化された前記メッセージ内容を前記復号化装置に送信する、

ことを実行し、

前記復号化装置内の復号化プロセッサは、

前記メモリに記憶された第４の非公開素数Ｓを読出し、少なくとも当該第４の非公開素数Ｓを用いた関数により前記スクランブルパターンを算出し、算出した当該スクランブルパターンを用いて受信した前記暗号化されたメッセージ内容をスクランブル処理する前のメッセージ内容に戻し、

前記メモリに記憶された第３の非公開素数Ｒを読出し、少なくとも当該第３の非公開素数Ｒを用いた関数により算出した前記スペースパターンに基づき、前記スクランブル処理する前に戻されたメッセージ内容に挿入されていたスペース又は対応する値を除去して単一メッセージに再構築し、

前記メモリに記憶された復号化キーＤと、前記第１の非公開素数Ｐと、前記第２の非公開素数Ｑとを読出し、当該復号化キーＤ、第１の非公開素数Ｐ、及び第２の非公開素数Ｑを用いた関数に基づき、前記単一メッセージを前記第２の形式Ｍ´から前記第１の形式Ｍに変換すること、

を実行する前記暗号及び復号化方法。

【請求項１３】

前記第１の非公開素数Ｐ及び前記第２の非公開素数Ｑの積は、前記第１形式Ｍのメッセージ内容の数値よりも大きい、請求項１２に記載の方法。

【請求項１４】

前記メモリに記憶された前記既知の暗号キーＥは、前記第１の非公開素数Ｐ及び前記第２の非公開素数Ｑに互いに素である、請求項１３に記載の方法。

【請求項１５】

前記暗号化プロセッサは、前記メッセージ内容を、以下の関数式

$$M' = M^{E} \bmod (P * Q)$$

に従い、前記第１の形式Ｍから前記第２の形式Ｍ´に変換する、請求項１４に記載の方法。

【請求項１６】

前記暗号化プロセッサ及び復号化プロセッサは、前記スペースパターン(spacing pattern)を、以下の関数式

$$F(R) = R * \bmod (K)$$

に従って算出する、請求項１２に記載の方法。

【請求項１７】

前記暗号化プロセッサ及び復号化プロセッサは、前記スクランブルパターン(scrambling pattern)を、以下の関数式

$$G(S) = S * \bmod (J)$$

に従って算出する、請求項１２に記載の方法。

【請求項１８】
前記復号化プロセッサは、前記復号化キーを、以下の関数式
$$D*E=1*\mathrm{mod}((P-1)*(Q-1))$$
に従って算出する、請求項１２に記載の方法。
【請求項１９】
前記復号化プロセッサは、前記メッセージ内容を、以下の関数式
$$M=(M')^{D}*\mathrm{mod}(P*Q)$$
に従い、前記第２の形式Ｍ´から前記第１の形式Ｍに変換する、請求項１８に記載の方法。
【請求項２０】
第１のプロセッサ(706)と、当該第１のプロセッサ(706)と結合する第１のメモリ(708)と、通信ネットワーク(712)、前記第１のプロセッサ(706)及び前記第１のメモリ(708)と接続する第１のネットワークインタフェース(710)とを含む暗号モジュール(702)を備えたメッセージの暗号化システムであって、
前記第１のプロセッサ(706)は、
既知の暗号キーＥと、第１の非公開素数Ｐと、第２の非公開素数Ｑとを用いた関数に基づき、第１の形式Ｍから第２の形式Ｍ´にメッセージ内容を変換するための変換ロジックを前記第１のメモリ(708)から読出して実行し、
前記メッセージ内容を前記第２の形式Ｍ´に変換した後、前記メッセージ内容を更に暗号化するために、スペースパターン(spacing pattern)に従って前記メッセージ内容にスペース又は対応する値を挿入して前記メッセージ内容を複数のメッセージ部分に分解するための分解ロジックを前記第１のメモリ(708)から読出して実行し、
前記メッセージ内容を前記第２の形式Ｍ´に変換した後、前記メッセージ内容を更に暗号化するために、スクランブルパターン(scrambling pattern)に従って前記メッセージ内容の値を反転したり、一定値を加算したり、任意の関数式に基づく値に変換することを含むスクランブル処理するためのスクランブルロジックを前記第１のメモリ(708)から読出して実行し、
第１のネットワークインタフェース(710)を介して前記通信ネットワーク(712)上に暗号化されたメッセージ内容を送信するための通信ロジックを前記第１のメモリ(708)から読出して実行する前記メッセージの暗号化システム。
【請求項２１】
前記第１のプロセッサは、前記メッセージ内容を、以下の関数式
$$M'=M^{E}\,\mathrm{mod}(P*Q)$$
に従い、前記第１の形式Ｍから前記第２の形式Ｍ´に変換する、請求項２０に記載のシステム。
【請求項２２】
前記メッセージ内容を分解するためのスペースパターンは、第３の非公開素数Ｒと係数Ｋとの関数である以下の関数式
$$F(R)=R*\mathrm{mod}(K)$$
に従い算出される、請求項２０に記載のシステム。
【請求項２３】
スペースパターン(spacing pattern)に従い前記メッセージ内容を分解する処理は、前記メッセージ内容を複数の個々のパケットにパルス化(pulsing)することを含む、請求項２２に記載のシステム。
【請求項２４】
スペースパターン(spacing pattern)に従い前記メッセージ内容を分解する処理は、前

記メッセージ内容を複数のグルーピングに割り振るために、余分な文字を前記メッセージ内容に挿入することを含む、請求項２２に記載のシステム。

【請求項２５】

前記スクランブルパターンは、秘密係数Ｊと第４の非公開素数Ｓとの関数である以下の関数式

$$G(S) = S * \mathrm{mod}(J)$$

に従う、請求項２０に記載のシステム。

【請求項２６】

既知の暗号キーＥと、第１の非公開素数Ｐと、第２の非公開素数Ｑとを用いた関数に基づき、第１の形式Ｍから第２の形式Ｍ´にメッセージ内容を変換するための変換手段と、

第３の非公開素数Ｒと、既知の第２の暗号キーＫとを用いた関数であらわされるスペースパターン(spacing pattern)に従い、前記メッセージ内容にスペース又は対応する値を挿入して前記メッセージ内容を複数のメッセージ部分に分解する分解手段と、

第４の非公開素数Ｓと、秘密係数Ｊとを用いた関数であらわされるスクランブルパターン(scrambling pattern)に従い、前記メッセージ内容を前記第２の形式Ｍ´に変換した後、前記メッセージ内容を更に暗号化するために、前記メッセージ内容の値を反転したり、一定値を加算したり、任意の関数式に基づく値に変換することを含むスクランブル処理を行うスクランブル手段と、

前記スクランブルパターンを反転させる(reversing)ため、前記スクランブルパターンを用いて、前記スクランブル手段によりスクランブル処理された前記メッセージ内容を、スクランブル処理する前のメッセージ内容に戻すデスクランブル（スクランブルを解く）手段と、

前記スペースパターンに基づき、前記スクランブル処理する前に戻されたメッセージ内容に挿入されていたスペース又は対応する値を除去して前記メッセージ内容を単一メッセージに再構築する単一化手段と、

前記メモリに記憶された復号化キーＤを読出し、当該復号化キーＤと、前記第１の非公開素数Ｐと、前記第２の非公開素数Ｑとを用いた関数に基づき、前記単一メッセージを前記第２の形式Ｍ´から前記第１の形式Ｍに変換する第２の変換手段とを備えた暗号及び復号化システム。

【請求項２７】

前記第２の変換手段は、前記既知の暗号キーＥと、前記第１の非公開素数Ｐと、前記第２の非公開素数Ｑとを用いた以下の関数式

$$D * E = 1 * \mathrm{mod}((P-1)*(Q-1))$$

に従い、秘密復号化キーＤを算出し、

前記算出された秘密復号化キーＤを用いて、以下の関数式

$$M = (M')^{D} * \mathrm{mod}(P * Q)$$

に従い、前記メッセージ内容を前記第２の形式Ｍ´から前記第１の形式Ｍに戻す変換をする、請求項２６に記載のシステム。

【請求項２８】

メモリに記憶された復号処理プログラムを実行する復号化プロセッサを備えた復号化装置で実施されるメッセージ復号化方法であって、

前記復号化プロセッサは、

前記メモリに記憶された既知の暗号キーＥと、第１の非公開素数Ｐと、第２の非公開素数Ｑとに基づき、第１の形式Ｍのメッセージを第２の形式Ｍ´に暗号化する第１の暗号化処理、スクランブルパターン(scrambling pattern)に基づく第２の暗号化処理、スペースパターン(spacing pattern)に基づく第３の暗号化処理が行なわれた暗号メッセージを受信し、

前記メモリに記憶された第４の非公開素数Ｓを読出し、少なくとも前記第４の非公開素数Ｓを用いた関数により前記スクランブルパターンを算出し、算出した前記スクランブルパターンに基づき暗号化された前記暗号メッセージの内容をスクランブル処理する前のメッセージ内容に戻すデスクランブル（スクランブルを解く）処理を行い、
前記メモリに記憶された第３の非公開素数Ｒを読出し、少なくとも前記第３の非公開素数Ｒを用いた関数に基づき算出した前記スペースパターンを用いて、前記スクランブル処理する前に戻されたメッセージ内容に挿入されていたスペース又は対応する値を除去して単一メッセージに再構築し、
前記暗号メッセージ内容をデスクランブル処理し、且つ前記暗号メッセージを前記単一メッセージに再構築した後、前記メモリに記憶された前記既知の暗号キーＥと、前記第１の非公開素数Ｐと、前記第２の非公開素数Ｑを用いた関数に基づき、前記単一メッセージの暗号メッセージ内容を第２の形式Ｍ´から第１の形式Ｍに戻すよう変換する、
を実行する前記メッセージ復号化方法。
【請求項２９】
前記メッセージ内容をデスクランブルする処理において、前記復号化プロセッサは、
前記メモリに記憶された秘密係数Ｊを読出し、前記第４の非公開素数Ｓ及び前記秘密係数Ｊを用いた関数により前記メッセージ内容のスクランブルパターンを算出すること、及び
前記暗号メッセージを構文解析して、前記スクランブルパターンをスクランブル処理する前のメッセージ内容に戻し、
前記スクランブルパターンを、

$$G(S) = S * \mathrm{mod}(J)$$

に従い算出することを特徴とする請求項２８に記載の方法。
【請求項３０】
前記メッセージの内容を単一メッセージに再構築する処理において、前記復号化プロセッサは、
前記メモリに記憶された第３の非公開素数Ｒと既知の第２の暗号キーＫを読出し、当該第３の非公開素数Ｒと既知の第２の暗号キーＫとを用いた関数により前記メッセージ内容のスペースパターンを算出すること、
前記スクランブル処理する前に戻されたメッセージ内容に挿入されていたスペース又は対応する値を除去して単一メッセージを再構築するため、前記スクランブル処理されたメッセージの構文解析を実行し、
前記スペースパターンを、以下の関数式

$$F(R) = R * \mathrm{mod}(K)$$

に従い算出することを特徴とする請求項２８に記載の方法。
【請求項３１】
前記メッセージ内容を前記第２の形式Ｍ´から前記第１の形式Ｍに変換する処理において、前記復号化プロセッサは、
前記メモリに記憶された前記既知の暗号キーＥと、前記第１の非公開素数Ｐと、前記第２の非公開素数Ｑとを読出し、当該既知の暗号キーＥ、第１の非公開素数Ｐ、及び第２の非公開素数Ｑを用いた以下の関数式

$$D * E = 1 * \mathrm{mod}((P-1)*(Q-1))$$

に従い、秘密復号化キーＤを算出し、そして、
前記算出された秘密復号化キーＤを用いて、以下の関数式

$$M = (M')^{D} * \mathrm{mod}(P * Q)$$

に従い、前記メッセージ内容を前記第２の形式Ｍ´から前記第１の形式Ｍに戻す変換をす

る、請求項２８に記載の方法。
【請求項３２】
プロセッサ(714)と、当該プロセッサ(714)と結合するメモリ(716)と、通信ネットワーク(712)、前記プロセッサ(714)及び前記メモリ(716)と接続するネットワークインタフェース(718)とを含む復号化モジュール(704)を備えたメッセージの復号化システムであって、
前記メモリに記憶された既知の暗号キーＥと、第１の非公開素数Ｐと、第２の非公開素数Ｑとに基づき、第１の形式Ｍのメッセージを第２の形式Ｍ´に暗号化する第１の暗号化処理、スクランブルパターン(scrambling pattern)に基づく第２の暗号化処理、スペースパターン(spacing pattern)に基づく第３の暗号化処理が行なわれた暗号メッセージに対し、
前記プロセッサ(714)は、
前記ネットワークインタフェース(718)を介して前記通信ネットワーク(712)上の前記暗号メッセージを受信するための通信ロジックを前記メモリ(718)から読出して実行し、
前記メモリに記憶された第４の非公開素数Ｓを読出し、少なくとも前記第４の非公開素数Ｓを用いた関数により前記スクランブルパターンを算出し、算出した前記スクランブルパターンに基づき暗号化された前記暗号メッセージの内容をスクランブル処理する前のメッセージ内容に戻すデスクランブル処理のためにデスクランブルロジックを前記メモリ(716)から読出して実行し、
前記メモリに記憶された第３の非公開素数Ｒを読出し、少なくとも前記第３の非公開素数Ｒを用いた関数に基づき算出した前記スペースパターンを用いて、前記スクランブル処理する前に戻されたメッセージ内容に挿入されていたスペース又は対応する値を除去して単一メッセージに再構築するための単一ロジックを前記メモリ(716)から読出して実行し、
前記暗号メッセージの内容をデスクランブル処理するとともに単一メッセージに再構築した後、前記メモリに記憶された既知の暗号キーＥと、第１の非公開素数Ｐと、第２の非公開素数Ｑとを用いた関数に基づき、前記単一メッセージのメッセージ内容を第２の形式Ｍ´から第１の形式Ｍに戻す変換をするための変換ロジックを前記メモリ(716)から読出して実行する前記メッセージ復号化システム。
【請求項３３】
前記プロセッサ(714)は、前記デスクランブルロジックにおいて、
前記メモリに記憶された秘密係数Ｊを読出し、前記第４の非公開素数Ｓ及び前記秘密係数Ｊを用いた関数により前記暗号メッセージ内容のスクランブルパターンを算出し、
前記暗号メッセージを構文解析して、前記スクランブルパターンをスクランブル処理する前のメッセージ内容に戻すこと実行し、
前記スクランブルパターンを、

$$G(S) = S^* \bmod(J)$$

に従い算出することを特徴とする請求項３２に記載のシステム。
【請求項３４】
前記プロセッサ(714)は、前記単一ロジックにおいて、
前記メモリに記憶された第３の非公開素数Ｒと既知の第２の暗号キーＫを読出し、当該第３の非公開素数Ｒと既知の第２の暗号キーＫとを用いた関数により前記暗号メッセージ内容のスペースパターンを算出し、
前記スクランブル処理する前に戻されたメッセージ内容に挿入されていたスペース又は対応する値を除去して単一メッセージを再構築するため、前記スクランブル処理されたメッセージの構文解析を実行し、
前記スペースパターンを、以下の関数式

$$F(R) = R^* \bmod(K)$$

に従い算出することを特徴とする請求項３２に記載のシステム。
【請求項３５】
前記プロセッサ(714)は、前記変換ロジックにおいて、
前記メモリに記憶された前記既知の暗号キーＥと、前記第１の非公開素数Ｐと、前記第２の非公開素数Ｑとを読出し、当該既知の暗号キーＥ、第１の非公開素数Ｐ、及び第２の非公開素数Ｑを用いた以下の関数式

$$D * E = 1 * \mathrm{mod}((P-1)*(Q-1))$$

に従い、秘密復号化キーＤを算出し、そして、
前記算出された秘密復号化キーＤを用いて、以下の関数式

$$M = (M')^{D} * \mathrm{mod}(P * Q)$$

に従い、前記メッセージ内容を前記第２の形式Ｍ´から前記第１の形式Ｍに戻す変換をすること実行する、請求項３２に記載のシステム。
【発明の詳細な説明】
【背景技術】
【０００１】
通信ネットワーク、特に無線メディアを介して全体もしくは一部で実行される通信ネットワークの拡大とともに、データセキュリティはますます重要になってきている。無線ネットワーク技術は、有線ネットワーク技術と比べて比較的新しい。そうであるから、無線ネットワークを保護する最新技術が、有線ネットワークで用いられ且つ開発されてきた技術から派生してきている。例えば、有線、無線にかかわらず、ネットワークを保護する一技術に、通信の暗号化がある。これは、未認可の機関によるネットワークのセキュリティ侵害から通信が理解されてしまうことを防止する。最新の暗号化技術は、無線部分をまったく含まない直接的な有線ネットワークパスには満足いくものである。暗号化通信をセキュリティ侵害するにあたり、ハッカー（attacker）は暗号アルゴリズムを破壊するために複数のトランザクションに耳を傾ける必要がある。例えば、外部の第三者が直接ケーブル接続されたトランザクションにアクセスするためには、そのケーブル又はそれに接続されたサーバーにアクセスし、一つのトランザクションがサーバーによって受信されるかあるいは送信されると外部の第三者が特定できるまでデータの流れを注意深くモニターしているかもしれない。あるいはまた、その外部の第三者は、例えば安全なデータベースが記憶されているサーバー上のデータにアクセスしようとするかもしれない。
【０００２】
ひとたびアクセスされ、充分な量のデータが集められると、ハッカーはデータを解読することができる。サーバーに記憶されたデータを保護するための知られた技術、及び有線メディア(wired media)へは相対的にアクセス困難であるため、有線通信のアクセス及び傍受は本質的に困難である。しかしながら、通信が無線で行われるときは、通信を伝搬する無線信号はしばしば全方向に送信する。これにより、聴きたいと思う範囲内にいる誰に対しても無線信号をアクセス可能にさせる。従って、サーバーでのトランザクション、あるいは通信メディアを介してのトランザクションを攻撃から防ぐために行われる技術では、少なくとも一部でも無線ネットワーク上で行き来するトランザクションをほとんど保護することができない。サーバーによりデータを守ることができず、無線信号を安全に閉じ込めておくことができない。トランザクションが少なくとも部分的にでも無線ネットワーク上を行き来するとき、誰かがデータストリームを傍受すること試みるかもしれない。これは、所与の暗号化アルゴリズムがハッカーによってセキュリティ侵害される可能性を増加するものである。
【０００３】
無線ネットワークを用いた如何なるトランザクションにおいても、主な懸念の一つは、トランザクションを傍受して、そのトランザクションを復号する外部の第三者の能力である。そこでは、クレジットカードの番号、銀行口座番号、及び社会保障番号などの個人情

報及び／又は安全情報を取得するために、防御のため暗号が行われてきた。それゆえ、無線トランザクションを保護し、外部の第三者がトランザクションを傍受して復号化することを阻止することが望まれている。

【発明の開示】

【課題を解決するための手段】

【０００４】

図１は、三段階の暗号技術の一実施例及び復号化技術の一実施例を表したフローチャート１００である。任意の単一デバイスが、三段階の暗号技術、三段階の復号化技術、及びその組み合わせを実行できることを理解されたい。

【０００５】

一般的に、開示された三段階の暗号及び復号化技術は、無線ネットワークを少なくともその一部に利用する通信を保護するために用いられる。しかしながら、当業者であれば、この開示された三段階の暗号及び復号化技術が、配線で接続された媒体(hardwired medium)又は他のタイプの通信媒体上での通信のために用い得ることを理解できるであろう。

【０００６】

三段階の暗号化技術は、メッセージを受信装置に送信する前にメッセージを暗号化する送信装置によって広く用いられる。外部の第三者が通信媒体を介して受信装置に伝わるメッセージを容易に傍受し、クレジットカードの番号、銀行口座番号、及び社会保障番号などの個人情報及び／又は安全情報へのアクセスを得ることを防止するために、送信装置はメッセージを暗号化する。

【０００７】

三段階の復号化技術は、送信装置からのメッセージを受信した後、そのメッセージを復号化する受信装置によって広く用いられる。受信装置は、三段階の暗号化技術が保護するクレジットカードの番号、銀行口座番号、及び社会保障番号などの個人情報及び／又は安全情報へのアクセスを得るためにメッセージを復号化する。

【０００８】

一実施例において、暗号化能力を有する送信装置は、開示された三段階の暗号化技術１０２を用いてメッセージを暗号化し、そのメッセージを受信装置に送信する１１０。このような通信は双方向であり、且つ様々なデバイスが送受信の両方を行い得ることを理解されたい。従って、ここで用いられる送信装置あるいは受信装置は前後関係から指定可能であり、ある通信における送信装置は他の通信において受信装置になり得る。送信装置は次の機器類を含む。即ち、パソコン、パーソナルデジタル機器、サーバー、ワークステーション、例えば洗濯機／乾燥機、冷蔵庫、水処理システム、ストーブなどのコンピュータ化されてネットワークにデータを送受信する電化製品、あるいは当技術分野で周知であるいかなる種類のネットワークを可能にする装置、あるいはこれらの組み合わせ、及び非ネットワーク機器であっても、改良または変更することでネットワーク可能になる装置。受信装置はメッセージ１１１を受信し、開示された三段階の復号化技術１１２を用いて暗号化されているメッセージを解読する。送信装置と同様、受信装置も、パソコン、パーソナルデジタル機器、サーバー、ワークステーション、例えば洗濯機／乾燥機、冷蔵庫、水処理システム、ストーブなどのコンピュータ化されてネットワークにデータを送受信する電化製品、あるいは当技術分野で周知であるいかなる種類のネットワークを可能にする装置、あるいはこれらの組み合わせ、及び非ネットワーク機器であっても、改良または変更することでネットワーク可能になる装置等を含んでいる。

【０００９】

暗号化されたメッセージを暗号化装置から受信装置に送信する１１０無線プロトコールには、IEEE802.11規格（802.11(a)、802.11(b)、802.11(g)等）に準拠したワイヤレス・フィディリティー（wireless fidelity：Wi-Fi）、ジェネラル・パケット・ラジオ・サービス（general packet radio service：GPRS）、ブルートゥース（Bluetooth）周辺機器や携帯電話の交信、ウルトラ・ワイドバンド（ultra wideband）、ワイマックス（WiMax）、あるいは無線周波数（RF）を使用するいかなる種類の無線プロトコール、光や他の

伝送媒体などが含まれる。さらには、ネットワークの様々な部分に係わる種々の無線技術の組み合わせが含まれる。

【００１０】

三段階の暗号化技術（１０２）をネットワーク上に送信されるメッセージに作用させる場合、典型的には素因数分解を用い、送信中のオリジナルのメッセージ内容を隠すために、メッセージの中身が第一の形Ｍから第二の形Ｍ’に変換される（１０４）。

【００１１】

次に、典型的には多数の別個のパケットあるいは多数のグルーピングにメッセージの中身が分解される（１０６）。以下に詳細を述べると、メッセージの中身を送信するスペースを非均一化することにより、第三者による送信信号の盗聴及びメッセージ内容の解読を困難にする。

【００１２】

一実施例において、メッセージ内容を分解するにあたり、送信時の時間量によって分解される複数の個々のパケット全体にメッセージ内容の部分が拡散するようメッセージ内容を細分化する。別の実施例の場合、メッセージ内容を分解するにあたり、複数のグルーピング分けに割り振るために、空白文字（スペース）などの余分な文字をメッセージ内容の全体に挿入する。

【００１３】

そして、メッセージ内容を含む複数の各パケット又は複数のグルーピングを、ユーザ定義のパターンに従ってスクランブルする（１０８）。なお、その一例を以下に詳述する。

【００１４】

上述した三段階の暗号化技術（１０２）を用いて暗号化したメッセージを復号化するには、この三段階の暗号化技術を単純に逆操作させる（１１２）。典型的には、安全性を高くする目的から、受信装置は、開示した三段階の暗号化技術１０２を用いて暗号化したメッセージを復号化するのに必要なアルゴリズム及び変数を知らされている。しかしながら、他の実施例の場合では、メッセージを復号化するのに必要なアルゴリズム及び変数は、安全性の低下を犠牲にして、受信装置に渡すようにしてもよい。

【００１５】

まず、ユーザ定義のパターンを反転することによって、複数の各パルス又は複数のグルーピング分けの中にあるメッセージ内容のスクランブルを解く（１１４）。次に、元のメッセージを細分化するのに用いた方法に応じて、メッセージ内容を含む複数のパケットを単一メッセージに再結成したり、複数のグルーピング分けの間にある余分な文字を取り除く（１１６）。通常、メッセージの冒頭に１又は２のデジタル番号の形式で、元のメッセージを細分化するのに用いた方法が示される。そして、最終的には、メッセージ内容は第２の形式Ｍ´から第１の形式Ｍへ変換される（１１８）。

【００１６】

図２は、三段階のデータ暗号化技術の変換フェーズ（２００）の一実施例を示したフローチャートである。通常、メッセージ内容を暗号化する前に、メッセージ内容のアルファベット構文が数値表現に変換される（２０２）。例えば、文字“ａ”が数字の“０１”として、文字“ｂ”が数字の“０２”として表されるように変換されるなどである。このアルファベット変換は、情報交換用米国標準コード（“ＡＳＣＩＩ”）又は拡張２進化１０進コード（“ＥＢＣＤＩＣ”）基準、或いは任意の変換に準拠している。アルファベット構文を数値表現に変換するための関数はよく知られており、殆どのプログラム言語はこのタイプの操作を実行する標準関数を備えている。

【００１７】

メッセージ内容を第１の形式Ｍから第２の形式Ｍ´に変換するにあたり、送信装置及び/又は受信装置の暗号化構成要素及び復号化構成要素は、第１の非公開素数Ｐと、第２の非公開素数Ｑと、既知の暗号キーＥと、非公開の暗号キーＤとを使ってプログラムされる。さらに、第１及び第２の非公開素数の積はＮであるよう定義される。

【００１８】

安全性を高める目的からすると、前記既知の暗号キーは、第１及び第２の非公開素数に対して互いに素であるべきである。すなわち、

$$GCD(E,(P-1)*(Q-1))=1$$

ここで、ＧＣＤは最大公約数である。よく知られているように、２以上の整数が１以外の正の公約数を共有しないときは互いに素であると定義される。

【００１９】

非公開の復号化キーＤは公開して知らされていないのが普通である。非公開の復号化キーＤは、受信装置で受信された任意のメッセージを復号化（デコード）するのに使用される。第１の非公開素数Ｐ、第２の非公開素数Ｑ、そして既知の暗号キーＥを選択した後、次の式を用いて非公開暗号キーＤを算出することができる。

$$D*E=1*\mathrm{mod}((P-1)*(Q-1))$$

【００２０】

第１の非公開素数Ｐと第２の非公開素数Ｑの積Ｎ、及び既知の暗号キーＥを用いて、メッセージ内容が次の式に従い第１の形式Ｍから第２の形式Ｍ´に変換される（２０８）。

$$M'=M^{E}\bmod N$$

第１の形式Ｍから第２の形式Ｍ´への変換２０８を正確に行うためには、数値Ｎは、第１の形式Ｍのメッセージ内容の数値より大きくなければならないことに留意されたい。

【００２１】

図３ａ及び図４ａは、三段階の暗号化技術の分解フェーズに関するフローチャートである。通常、メッセージ内容は変換フェーズの後に分解されるが、ある実施例の場合、変換フェーズの前にメッセージ内容を分解することも可能である。

【００２２】

図３ａに示す実施例の場合、メッセージ内容を分解するにあたり、メッセージ内容を複数の各パケット全体にわたりひろげるためにメッセージ内容を細分化する（３００）。通常、複数の各パケット用のスペースパターンを定義するにあたり、第３の非公開素数Ｒと既知の第２の暗号キーＫを選ぶ。既知の公開暗号キーＫの値は、１０などの任意の係数、秘密暗号キーＤ、又は他の任意の推奨値とすることができる。

【００２３】

一実施例では、スペースパターンは、暗号化装置が複数の各パケットの間で待つ文字数である。しかしながら、他の実施例では、ユーザは、複数の各パケット間の空白（スペース）に関して他の意味に対応するスペースパターンの値を有するよう選ぶこともできる。スペースパターンは、次の式に従い算出されるのが典型的である（３０２）。

$$F(R)=R*\mathrm{mod}(K)$$

実施例の中には、このスペースパターンは、“Ｒ ｍｏｄ Ｋ”、“Ｋ－Ｒ ｍｏｄ Ｋ”、又はユーザにより選ばれる他の任意の式で代替するようにしてもよい。

【００２４】

図４ａに示消す別の実施例の場合、メッセージ内容を分解するにあたり（４００）、余分な文字をメッセージ内容全体にわたり挿入して、メッセージ内容を複数のグルーピングに割り振るためにメッセージ内容に間隔をあける。余分な文字は、空白文字（スペース）であったり、ユーザが望む他の任意のタイプの文字であってよい。上述した同様の処理に従い、図３ａの実施例におけるスペースパターンを定義するために、余分な文字の数に関するスペースパターンを決定する。典型的には、第３の非公開素数Ｒと、既知の第２の暗号キーＫが選ばれる。既知の第２の暗号キーＫの値は、１０などの任意の係数、秘密暗号キーＤ、又は他の任意の推奨値とすることができる。スペースパターンは、次の式に従い算出されるのが典型的である（４０２）。

$$F(R) = R * \mathrm{mod}(K)$$

実施例の中には、このスペースパターンは、“Ｒ ｍｏｄ Ｋ”、“Ｋ－Ｒ ｍｏｄ Ｋ”、又はユーザにより選ばれる他の任意の式で代替するようにしてもよい。

【００２５】

通常は、間隔をあけるフェーズ（３００，４００）の後で、残りのメッセージ内容のセクションをスクランブルさせる（３０６，４０６）。しかしながら、他の実施例では、この三段階のデータ暗号化技術の順序を変えて、間隔をあけるフェーズ（３００，４００）又は変換フェーズ（２００）の前にメッセージ内容をスクランブルさせる（３０６，４０６）ようにしてもよい。

【００２６】

図３ｂは、図３ａの実施例における三段階のデータ暗号化方法のスクランブルフェーズ（３０６）に関するフローチャートである。通常は、第４の素数Ｓと非公開係数Ｊを選ぶ。非公開係数Ｊの値は、１０などの任意の整数、秘密暗号キー、又は非公開な数全体の集合とすることができる。第４の素数Ｓと非公開係数Ｊは、次の式に従いスクランブル化パターンを算出する（３０８）ために用いられる。

$$G(S) = S * \mathrm{mod}(J)$$

【００２７】

一実施例において、スクランブル化パターンは、所定の方法に従い複数の各パケットがスクランブルされるようにあらわされる。例えば、スクランブル化パターンがナンバー２に等しければ、これは、他のあらゆる各パケットでスクランブルの作用が発生することをあらわすだろう。スクランブル作用は、２つの数字を反転させたり、数のメッセージ値に一定値を加算したり、或いはユーザが望む他の任意の関数を含むことができる（３１０）。

【００２８】

図４ｂは、図４ａの実施例におけるスクランブルフェーズ（４０６）に関するフローチャートである。図３ａ及び図３ｂの実施例について上述したように、第４の素数Ｓと非公開係数Ｊを選ぶ。素数Ｓと非公開係数Ｊは、次の式に従いスクランブル化パターンを算出する（４０８）ために用いられる。

$$G(S) = S * \mathrm{mod}(J)$$

【００２９】

図５は、図３ａ及び図３ｂの実施例に従って生成された暗号メッセージを復号化（解読）する（５００）フローチャートである。暗号化装置が三段階のデータ暗号化技術でメッセージを処理した後、その暗号化されたメッセージが受信装置（５０２）に送信される。ひとたび受信されると、受信装置は前記データ暗号化技術を逆操作させて、暗号メッセージを解読する。

【００３０】

通常は、上述した図３ｂの処理を単純に逆操作させることにより、複数の各パケット内のメッセージ内容のスクランブルが解かれる（５０４）。通常は、受信装置には秘密係数Ｊと第４の素数Ｓが知らされており、スクランブルパターンを算出して暗号化されたメッセージ内容を構文解析し、スクランブルを反転することができる（５０４）。

【００３１】

スクランブルフェーズ（５０４）の後、メッセージを含む複数の各パケットが単一メッセージに戻って再結成される。通常、受信装置は、第３の非公開素数Ｒと既知の第２の暗号キーを知らされているので、受信装置はスペースパターンを算出し、メッセージを構文解析して、上述した図３ａの処理を逆操作することができる（５０６）。

【００３２】

複数の各パケットが単一メッセージに再結成された後で、メッセージ内容が第２の形式

Ｍ´から第１の形式Ｍへ変換される（５１０）。通常は、受信装置は公開して知られている暗号キーＥと、第１及び第２の非公開素数Ｐ，Ｑを知っているだろう。Ｅ，Ｐ、Ｑを用いて、受信装置は、以下の式を使って秘密復号化キーＤを算出する。

$$D*E=1*\mathrm{mod}((P-1)*(Q-1))$$

次に、受信装置は、以下の式に従い、第２の形式Ｍ´から第１の形式Ｍへメッセージ内容を変換する（５１０）。

$$M=(M')^{D}*\mathrm{mod}(P*Q)$$

【００３３】

図６は、図４ａ及び図４ｂの実施例に従い、暗号化装置６０２から受信した暗号メッセージを復号化（解読）する（６００）フローチャートである。通常、余分な文字で割り振られたメッセージ内容は、上述した図４ｂの処理を単純に逆操作することによってスクランブルを解く（６０４）。通常、受信装置は、秘密係数Ｊ及び第４の素数Ｓを知らされており、スクランブルパターンを算出し、メッセージを構文解析して、スクランブル処理を反転することができる。

【００３４】

スクランブルを解くフェーズ（６０４）の後、メッセージを含む複数の各パケットは、単一メッセージに再構成される（６０６）。通常、受信装置は、素数Ｒと既知の第２の暗号キーＫとを知らされているので、スペースパターンを算出することができ、そしてメッセージを構文解析して、上述した図４ａに示す分解処理を逆操作する。

【００３５】

複数の各パケットを単一メッセージに再構成した後（６０６）、メッセージ内容が第２の形式Ｍ´から第１の形式Ｍへ変換される（６１０）。通常は、受信装置は既知の暗号キーＥと、第１及び第２の非公開素数Ｐ，Ｑを知っているだろう。Ｅ，Ｐ、Ｑを用いて、受信装置は、以下の式を使って復号化キーＤを算出する。

$$D*E=1*\mathrm{mod}((P-1)*(Q-1))$$

次に、受信装置は、以下の式に従い、第２の形式Ｍ´から第１の形式Ｍへメッセージ内容を変換する（６１０）。

$$M=(M')^{D}*\mathrm{mod}(P*Q)$$

暗号処理におけるフェーズと同様、復号化処理でのフェーズの順を他の実施例において逆にすることができる。

【００３６】

図７は、三段階の暗号化技術を用いたメッセージ暗号のための暗号化モジュール７０２の一実施例、及び三段階の復号化技術を用いたメッセージ解読のための復号化モジュール７０４の一実施例を示したブロック図である。暗号化モジュール７０２及び復号化モジュール７０４は、三段階の暗号及び復号化技術を実行することのできる任意のタイプのハードウェア又はソフトウェアである。一つの装置で双方向通信ができるために、暗号化モジュール７０２及び復号化モジュール７０４をその一つの装置が備えるようにしてもよい。また、一つの装置が片方向の通信ができるために、暗号化モジュール７０２あるいは復号化モジュール７０４の何れか一方を含む構成であってもよい。

【００３７】

暗号化モジュール７０２は、典型的には、暗号プロセッサ７０６、暗号プロセッサ７０６に接続した暗号メモリ７０８、そして暗号プロセッサ７０６と暗号メモリ７０８と通信ネットワーク７１２とに接続した暗号ネットワークインタフェース７１０を含む。ここで、“～と接続した”という語は、直接的に接続されたことを意味する他に、１以上の介在する構成要素を介して間接的に接続されることを意味するように定義されている。そのような介在する構成要素は、ハードウェア及びソフトウェアベースの構成要素の両方を含む

。

【００３８】

暗号プロセッサ７０６は、標準ペンティアム（Ｒ）プロセッサ、インテルの埋め込み型プロセッサ、カスタムプロセッサ、又は他の任意のタイプのハードウェアに組み込まれたプロセッサであって、ソフトウェアプログラムを走らすことができ、第１の形式Ｍのメッセージ内容を第２の形式Ｍ´へ変換し、スペースパターンに従いメッセージ内容を分解し、そしてスクランブルパターンに従いメッセージ内容をスクランブルする上述した機能を実行する。典型的には、これらの機能は、暗号メモリ７０８に記憶され、暗号プロセッサ７０６によって実行可能なソフトウェアプログラムにおけるロジックとして実施されるであろう。

【００３９】

暗号メモリ７０８は、ＲＯＭ又はフラッシュメモリなどの任意のタイプのメモリであってもよく、また任意のタイプの固定的或いは取り外し可能なディスク又はドライブとすることもできる。暗号ネットワークインタフェース７１０は、無線ネットワーク、配線で接続された通信ネットワーク、又は他の任意のタイプの通信媒体を介して通信可能な任意のネットワークインタフェースとすることができる。

【００４０】

同様に、復号化モジュール７０４は、典型的には、復号化プロセッサ７１４、復号化プロセッサ７１４に接続した復号化メモリ７１６、そして復号化プロセッサ７１４と復号化メモリ７１６と通信ネットワーク７１２とに接続した復号化ネットワークインタフェース７１８を含む。

【００４１】

復号化プロセッサ７１４は、標準ペンティアム（Ｒ）プロセッサ、インテルの埋め込み型プロセッサ、カスタムプロセッサ、又は他の任意のタイプのハードウェアに組み込まれたプロセッサであって、ソフトウェアプログラムを走らすことができ、スクランブルパターンに従いメッセージ内容のスクランブルを解き、スペースパターンに従い分解されたメッセージ内容を単一化し、そして第２の形式Ｍ´のメッセージ内容を第１の形式Ｍへ変換する上述した機能を実行する。典型的には、これらの機能は、復号化メモリ７１６に記憶され、復号化プロセッサ７１４によって実行可能なソフトウェアプログラムにおけるロジックとして実施されるであろう。復号化メモリ７１６は、ＲＯＭ又はフラッシュメモリなどの任意のタイプのメモリであってもよく、また任意のタイプの固定的或いは取り外し可能なディスク又はドライブとすることもできる。

【００４２】

復号化メモリ７１６は、ＲＯＭ又はフラッシュメモリなどの任意のタイプのメモリであってもよく、また任意のタイプの固定的或いは取り外し可能なディスク又はドライブとすることもできる。復号ネットワークインタフェース７１８は、無線ネットワーク、配線で接続された通信ネットワーク、又は他の任意のタイプの通信媒体を介して通信可能な任意のネットワークインタフェースとすることができる。

【００４３】

図８ａ及び図８ｂは、三段階の暗号化技術を用いて暗号化され（図８ａ）、そして次に復号化された（図８ｂ）メッセージの一実施例を示したフローチャートである。図８ａに見られるように、第１の形式Ｍのメッセージは、値２３を有するように定義されている（８０２）。また、第１の非公開素数は値５を、第２の非公開素数は値７を、そして既知の暗号キーＥは値２９を有するように定義されている。上記で説明したように、第１及び第２の非公開素数の値は素数であり、既知の暗号キーはこの第１及び第２の非公開素数に対して互いに素である。さらに、第１及び第２の素数の積は、第１の形式Ｍのメッセージの値よりも大きいという条件に適合する３５となるよう計算される。

【００４４】

上述したように、このメッセージは、次の式に従い、第１の形式Ｍから第２の形式Ｍ´に変換される（８０４）。

$$M' = M^{E} \text{ *mod}(P * Q)$$
$$M' = (23)^{29} \text{ *mod}(35)$$

この変換フェーズ（８０４）が実行されるとき、第１の形式Ｍのメッセージの値２３は、第２の形式Ｍ´の値１８をもつよう計算される。

【００４５】

変換フェーズ（８０４）の後、間隔をあけるフェーズ（８０６）が実行される。本例では、第３の非公開素数が３１として、既知の第２の暗号キーが１０として定義される。スペースパターンは、上述したように次の式に従い計算され、値１を得る。

$$F(R) = R \text{ *mod}(K)$$
$$F(31) = 31 * \text{mod}(10)$$

本例では、値１は一つの空白文字（スペース）の“００”として定義する。

【００４６】

メッセージが各パケットに分解される実施例の場合（８０８）、値１は分解されるメッセージを生じさせ、“１８”が、各パケット間に１つのスペースを有する“１＿＿８”となる。或いはまた、メッセージを分解するために複数のグルーピング間に余分なスペースが配置される実施例の場合（８１０）、メッセージは“１８”から“１００８”というような、複数のグルーピング間で空白文字として定義される２つの余分な文字を有するように分解される。

【００４７】

間隔をあけるフェーズ（８０６）の後、スクランブルパターンが計算される（８１２）。本例では、第４の素数が１７として、そして秘密係数が１５として定義される。スクランブルパターンは、次の式に従い計算され、値２を得る。

$$G(S) = S \text{ *mod}(J)$$
$$G(17) = 17 \text{ *mod}(15)$$

本例では、値２は、他のあらゆるパケット又はグルーピングをスクランブルすることを意味するように定義する。

【００４８】

本例の場合、グルーピング又はパケットがスクランブルされるときは、数値に定数１０が加算され、且つ２つの数字を反転させることを意味するように定義する。メッセージが各パケットに分解される実施例の場合（８０８）、“１＿＿８”のメッセージは、まず“１＿＿１８”に変換され、次に“１＿＿８１”となる。それゆえ、このメッセージの値２３は“１＿＿８１”という暗号化された値を有する。

【００４９】

メッセージを分解するためにグルーピング間に余分な文字を配置する実施例の場合（８１０）、“１００８”のメッセージは、まず“１００１８”に変換され、次に“１００８１”となる。それゆえ、このメッセージの値２３は“１００８１”という暗号化された値を有する。

【００５０】

次に、暗号化装置はこの暗号化された値の１００８１を受信装置に送信する（８１４）。図８ｂに戻ると、受信装置はこの暗号メッセージを受信し（８１８）、そしてまずメッセージ内容のスクランブルを解く（８２０）。受信装置はスクランブルされた各グルーピング又はパケットが反転された２つの数字を有し、そして元々のメッセージに対して値１０を加算されていることを知っていなければならない。加えて、受信装置は、上述したようにスクランブルパターンの値が２であることを正確に計算できるようにするため、第４の素数が１７として定義され、秘密係数が１５として定義されていることを知っていなければならない。

【００５１】

メッセージが各パケットに分解される実施例の場合（８２２）、“１＿＿８１”のメッセージは、まず“１＿＿１８”に変換され、次に“１＿＿８”となる（８２０）。メッセージを分解するために複数のグルーピング間に余分な文字を配置する実施例の場合（８２４）、“１００８１”のメッセージは、まず“１００１８”に変換され、次に“１００８”となる（８２０）。

【００５２】

スクランブルを解くフェーズ（８２０）の後、受信装置はメッセージを単一メッセージに戻してセットする（８２６）。受信装置は、スペースパターンが１であることを計算し、メッセージ内容のグルーピング又はパケット間に挿入されているのが１つのスペース、即ち“００”であることを知ることができるため、第３の非公開素数が３１として定義され、公開して知られている係数が１０として定義されていることを知っていなければならない。

【００５３】

メッセージが各パケットに分解される実施例の場合（８２２）、“１＿＿８”のメッセージは“１８”に変換される。さらに、メッセージを分解するために複数のグルーピング間に余分な空白文字（スペース）を配置する実施例の場合（８２４）、“１００８”のメッセージは“１８”に変換される。

【００５４】

最後に、受信装置は、変換フェーズ（８３０）を実行し、第２の形式Ｍ´のメッセージ内容を第１の形式Ｍへ変換する。受信装置は、第１の非公開素数が値５を有し、第２の非公開素数が値７を有し、そして既知の暗号キーＥが値２９を有するよう定義されていることを知ってなければならない。これらの値を用いて、受信装置は次の式に従い、上述したように秘密復号化キーＤを計算し（８２８）、値５を得る。

$$D*E=1*\mathrm{mod}((P-1)*(Q-1))$$

$$D*29=1*\mathrm{mod}(4*6)$$

秘密復号化キーＤを用いて、受信装置は、次の式に従い、第２の形式Ｍ´のメッセージ内容を第１の形式Ｍへ変換する（８３０）。

$$M=(M')^{D}*\mathrm{mod}(P*Q)$$

$$M=(18)^{5}*\mathrm{mod}(7*5)$$

上述した式は、第１の形式Ｍのメッセージの値２３となる。これは、三段階の暗号化処理が行われる前の第１の形式におけるメッセージの値と同じである。

【００５５】

三段階の暗号化技術又は三段階の復号化技術を実行する装置は、この三段階の暗号化技術又は三段階の復号化技術に付加的なフェーズを結合させることもできる。図９に見られる例について、一実施例では、図８ａの三段階の暗号化技術を実行する装置は、複数のパケット又は複数のグルーピングの順をスクランブルする第４のフェーズ（９１６）を実行してもよい。その結果、任意の付加的なフェーズがデータを正しく反転せず誤って伝えない限りは、そのような新たなフェーズが三段階の暗号化技術又は三段階の復号化技術に加えられる。

【００５６】

したがって、上述した詳細な記載は制限的に解釈されるのではなく例示として意図されるのであって、特許請求の範囲には本発明の精神及びそれが及ぶ範囲を意図するすべての均等を含んでいることを理解されたい。

【図面の簡単な説明】

【００５７】

【図１】本発明の一実施例に従った三段階の暗号及び復号化技術のフローチャートである。

【図２】三段階暗号技術の変換フェーズの一実施例に関するフローチャートである。

【図３ａ】三段階暗号技術の分解フェーズの一実施例に関するフローチャートである。
【図３ｂ】図３ａに示す三段階暗号技術の実施例に関するスクランブル・フェーズのフローチャートである。
【図４ａ】三段階暗号技術の分解フェーズの別の実施例に関するフローチャートである。
【図４ｂ】図４ａに示す三段階暗号技術の実施例に関するスクランブル・フェーズのフローチャートである。
【図５】図３ａ及び３ｂに示す三段階暗号技術の実施例に関する三段階復号化技術のフローチャートである。
【図６】図４ａ及び４ｂに示す三段階暗号技術の実施例に関する三段階復号化技術のフローチャートである。
【図７】暗号モジュールの一実施例及び復号化モジュールの一実施例のブロック図である。
【図８ａ】三段階暗号技術の一実施例の例示に関するフローチャートである。
【図８ｂ】図８ａに示す実施例の三段階復号化技術の例示に関するフローチャートである。
【図９】付加的な第４のフェーズを有する三段階暗号技術の一実施例の例示に関するフローチャートである。

【図１】

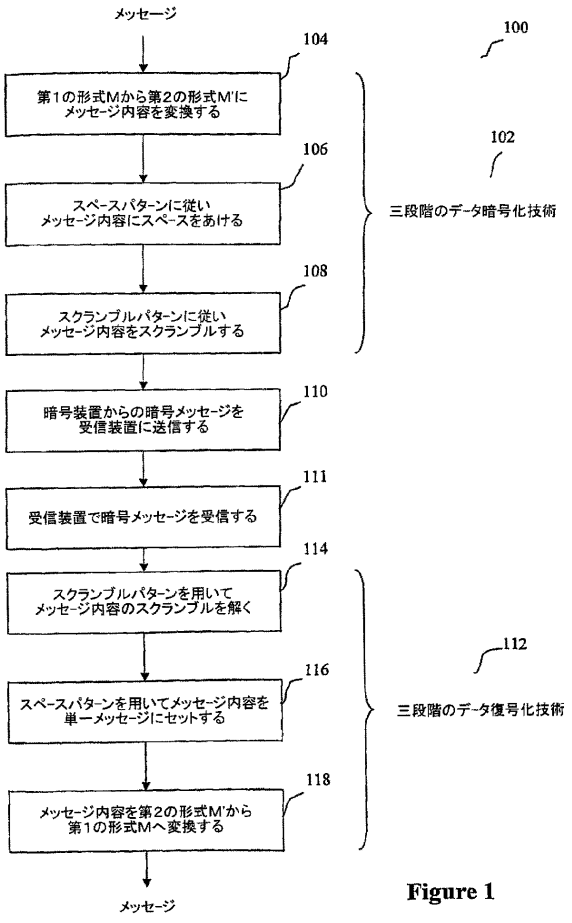

Figure 1

【図２】

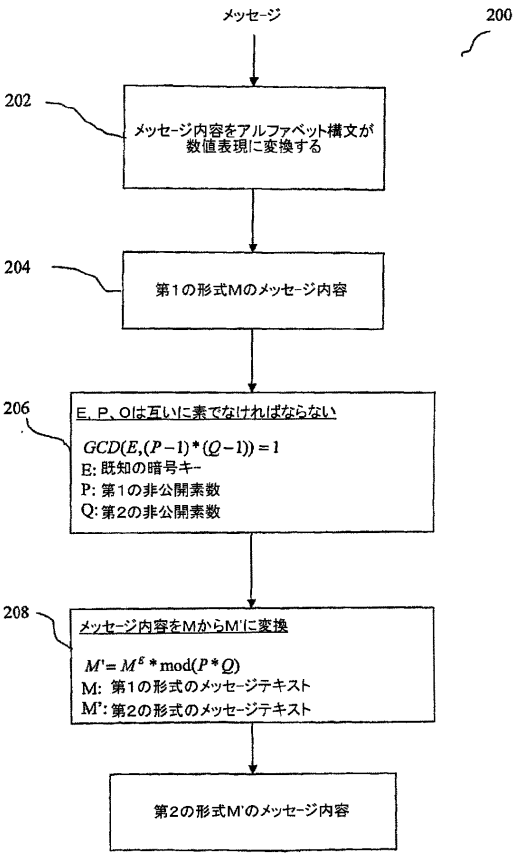

Figure 2

【図３ａ】

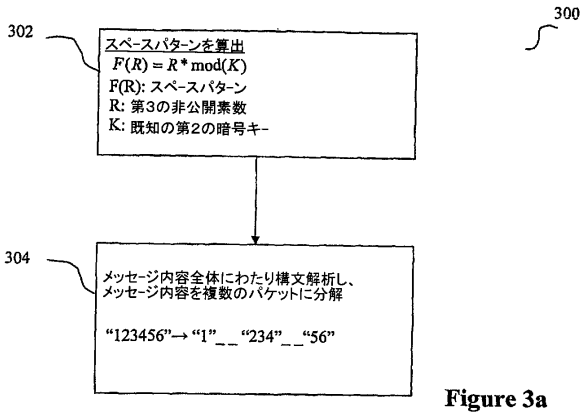

Figure 3a

【図４ａ】

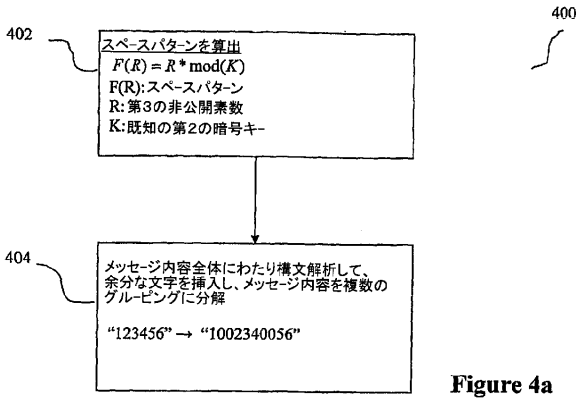

Figure 4a

【図３ｂ】

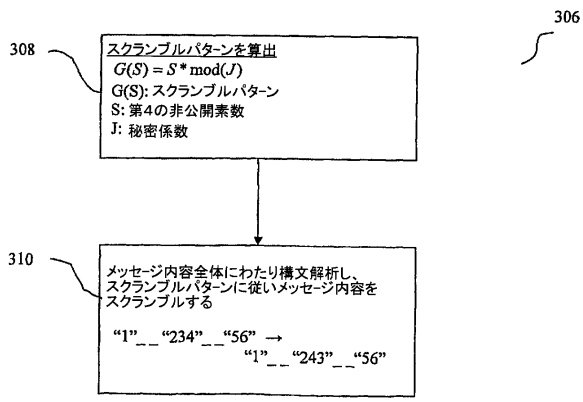

Figure 3b

【図４ｂ】

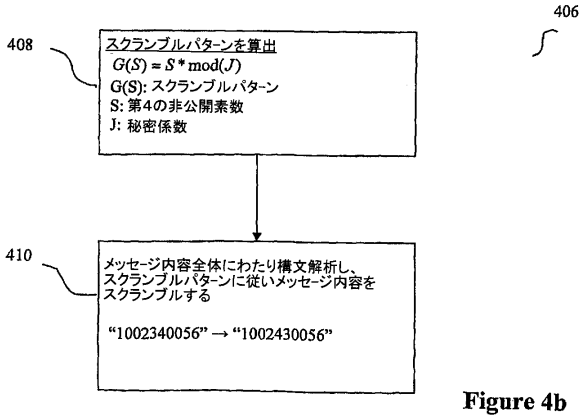

Figure 4b

【図５】

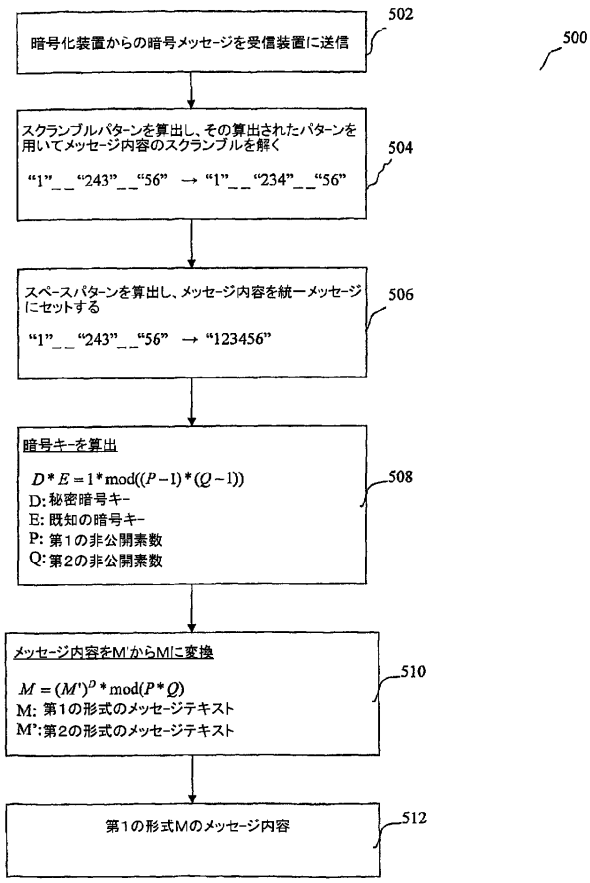

Figure 5

【図６】

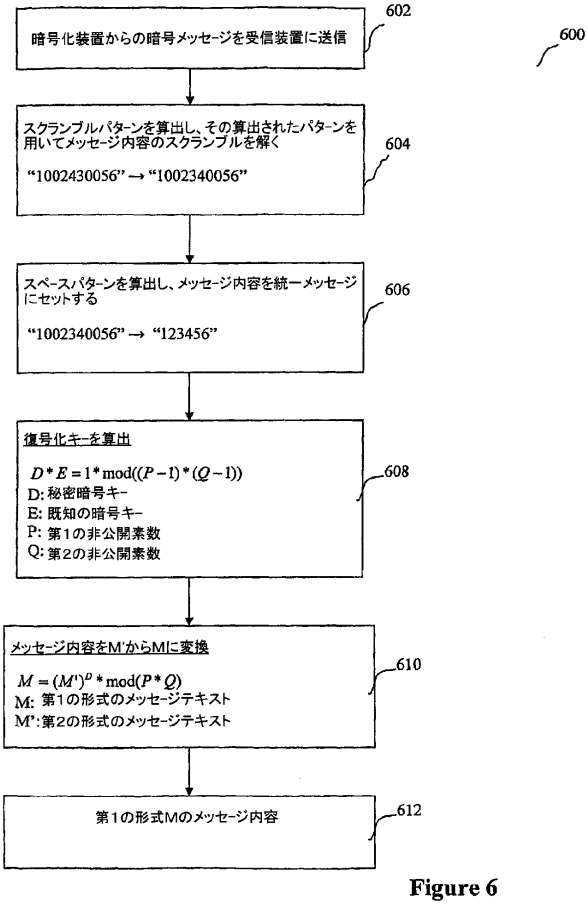

Figure 6

【図７】

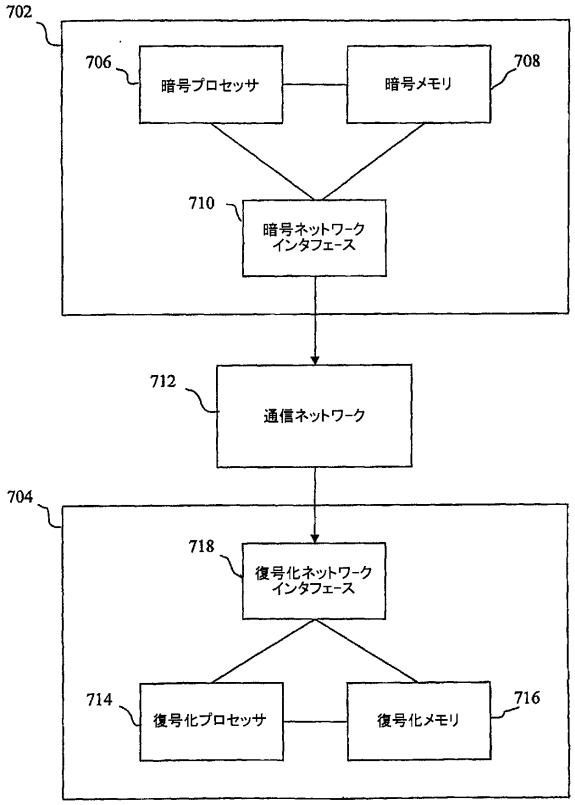

Figure 7

【図８ａ】

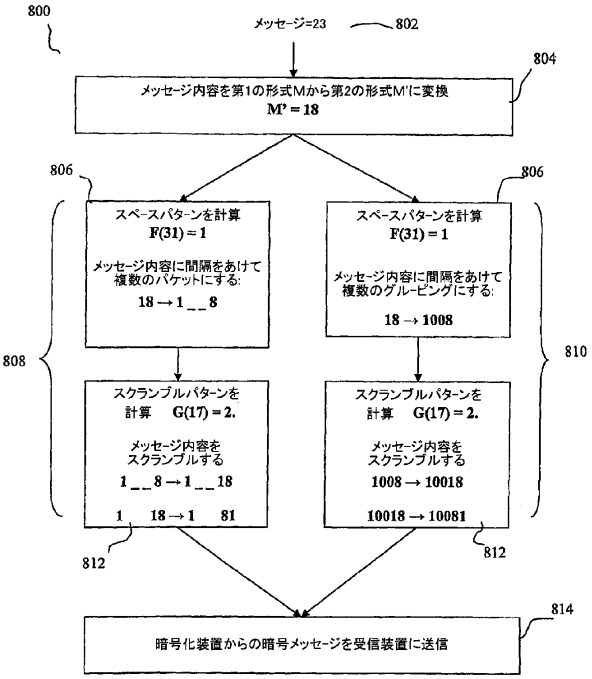

Figure 8a

【図８ｂ】

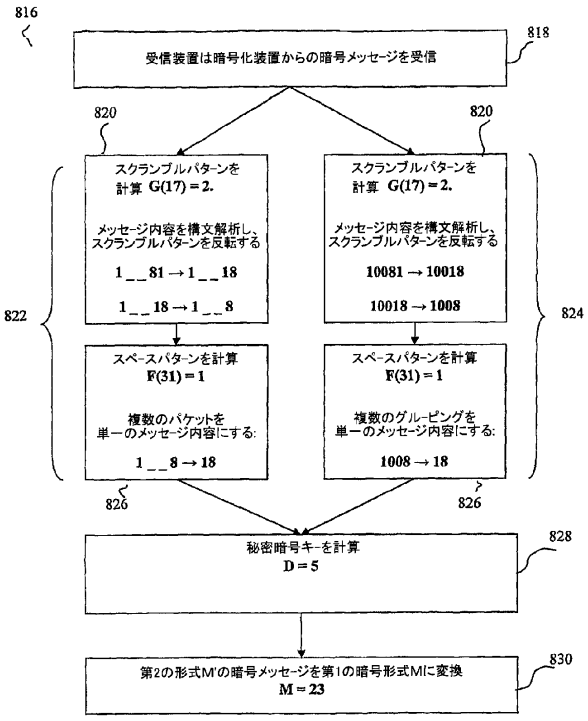

Figure 8b

【図９】

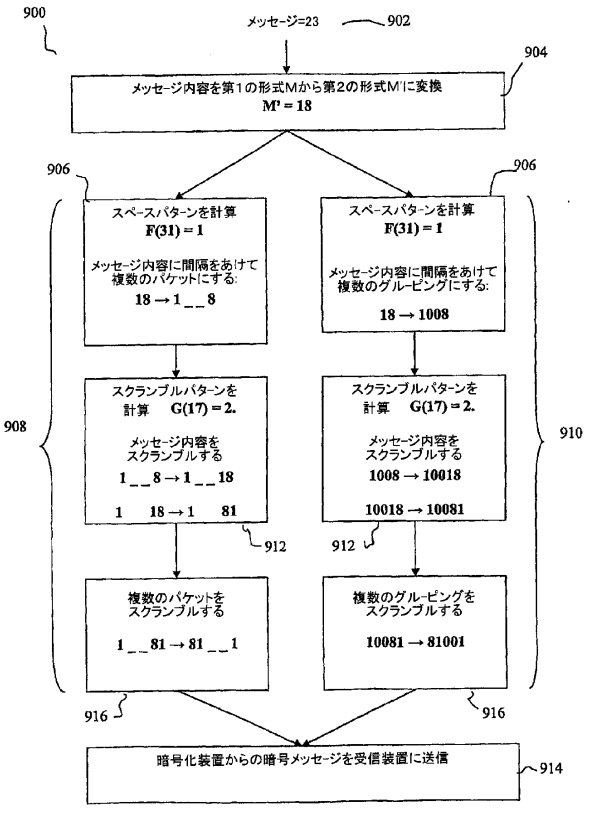

Figure 9

フロントページの続き

(74)代理人 100109335
弁理士 上杉 浩
(74)代理人 100122563
弁理士 越柴 絵里
(72)発明者 ヴェイセー ニマ
アメリカ合衆国 ミシガン州 ４９４１７ グランド ヘヴン レッドバード レーン １３５６８
(72)発明者 バーマン ディヴィッド ダブリュー
アメリカ合衆国 ミシガン州 ４９４０８ フェンヴィル ワンハンドレッドアンドトゥウェンティーセヴンス アベニュー ６４１４
(72)発明者 レピン トーマス ジェイ
アメリカ合衆国 ミシガン州 ４９４１７ グランド ヘヴン ジュニパー ヒルズ コート １１８６１

審査官 青木 重徳

(56)参考文献 特開平０１－１２２２２７（ＪＰ，Ａ）
特開平０５－０９１１０１（ＪＰ，Ａ）
特開平０４－０８８７３６（ＪＰ，Ａ）
特開２００３－１５７００３（ＪＰ，Ａ）
特開平１１－０５５２４７（ＪＰ，Ａ）
特開平１０－０９３５４８（ＪＰ，Ａ）
池野信一，小山謙二，“現代暗号理論”，日本，社団法人電子情報通信学会，１９９７年１１月１５日，初版第６刷，ｐ．１０５－１０９

(58)調査した分野(Int.Cl.，ＤＢ名)
G09C 1/00