(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2010-152012
(P2010-152012A)
(43)公開日　平成22年7月8日(2010.7.8)

(51)Int.Cl.		F I			テーマコード（参考）
G09C 1/00 (2006.01)		G09C	1/00	620A	5J104

審査請求 未請求　請求項の数 19　ＯＬ　（全 34 頁）

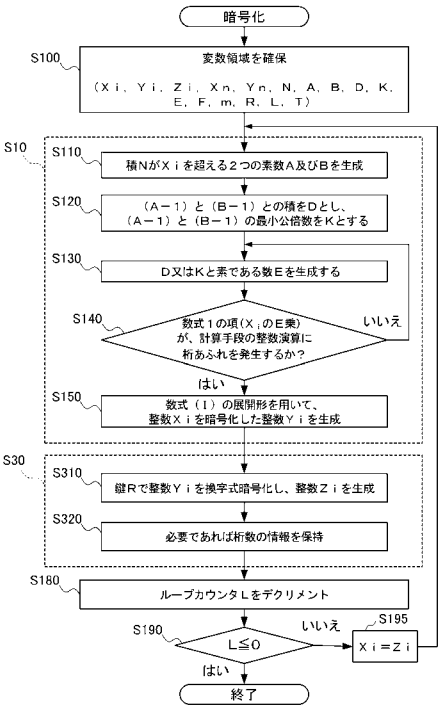
(21)出願番号　特願2008-328768 (P2008-328768)
(22)出願日　平成20年12月24日 (2008.12.24)

(71)出願人　000211307
中国電力株式会社
広島県広島市中区小町４番３３号
(74)代理人　100106002
弁理士　正林　真之
(74)代理人　100120891
弁理士　林　一好
(72)発明者　芳野　達哉
広島県広島市中区小町４番３３号　中国電力株式会社内

Ｆターム(参考)　5J104 AA21　JA21　JA23　NA02　NA10　NA17

(54)【発明の名称】整数の暗号化及び復号化方法

(57)【要約】
【課題】整数の暗号化及び復号化方法を提供する。
【解決手段】守秘情報を参照する識別子情報等に係る整数Ｘｉを入力として受け付け、積Ｎが入力整数Ｘｉを超える２つの素数Ａ及びＢを生成し、（Ａ－１）と（Ｂ－１）との積をＤとし、（Ａ－１）と（Ｂ－１）の最小公倍数をＫとし、Ｄ又はＫと素である数をＥとして、べき乗（ＸｉのＥ乗）が計算機の整数演算に桁あふれを発生する条件で剰余計算により整数を変換する。さらに、換字式暗号化を重畳した後、剰余計算及び換字式暗号化を繰り返しすことにより暗号化する。暗号化した整数は、暗号化の逆順で換字式復号化及びべき剰余を用いる復号化を繰り返して復号化し、元のＸｉが得られる。べき剰余を用いる復号化においては、ｍを任意の整数としてＥ×Ｆ＝ｍ×Ｋ＋１を成立するＦを用意し、べき乗（ＹｉのＦ乗）の剰余計算を実施する。
【選択図】図１



【特許請求の範囲】
【請求項１】
整数Ｘｉを暗号化し復号化する方法であって、
換字式暗号化を用いて整数を換字暗号した整数に変換するステップと、
換字式復号化を用いて前記換字暗号した整数を復号化するステップと、
積ＮがＸｉを超える２つの素数Ａ及びＢを生成するステップと、
（Ａ－１）と（Ｂ－１）との積をＤとし、（Ａ－１）と（Ｂ－１）の最小公倍数をＫとし、Ｄ又はＫと素である数をＥとして、次式において項ＸｉのＥ乗が計算手段の整数演算に桁あふれを発生する条件で、次式の展開形を用いて前記整数Ｘｉを変換した整数Ｙｉを生成するステップと、
【数１】

$$Y_i \equiv X_i^{E} \pmod{N}$$

ｍを任意の整数として次式を成立するＦを用意するステップと、
【数２】

$$E \times F = m \times K + 1$$

次式を用いて前記変換した整数Ｙｉを整数Ｘｎに復号化するステップと、
【数３】

$$X_n \equiv Y_i^{F} \pmod{N}$$

を含む、整数を暗号化し復号化する方法。
【請求項２】
前記展開形を用いて前記整数Ｘｉを前記整数Ｙｉに変換した後に、前記換字式暗号化を用いて前記整数Ｙｉを整数Ｚｉに変換する、べき剰余と換字とを連続する暗号化ステップと、
前記換字式復号化を用いて前記整数Ｚｉを前記整数Ｙｉに復号化した後に、前記整数ＹｉをＸｎに復号化する、換字とべき剰余とを連続する復号化ステップと、
を含む、請求項１に記載の整数を暗号化し復号化する方法。
【請求項３】
前記べき剰余と換字とを連続する暗号化ステップ、及び前記換字とべき剰余とを連続する復号化ステップは、少なくとも２以上の同一の回数実施される、請求項２に記載の整数を暗号化し復号化する方法。
【請求項４】
前記整数Ｘｉは前記換字式暗号化を用いて変換された整数である、換字とべき剰余とを連続する暗号化ステップと、
前記整数Ｙｉから復号化された前記整数Ｘｎに対して前記換字式復号化を用いて復号化する、べき剰余と換字を連続する復号化ステップと、
を含む、請求項１に記載の整数を暗号化し復号化する方法。
【請求項５】
前記換字とべき剰余とを連続する暗号化ステップ、及び前記べき剰余と換字を連続する復号化ステップは、少なくとも２以上の同一の回数実施される、請求項４に記載の整数を暗号化し復号化する方法。
【請求項６】
前記少なくとも２以上の同一の回数は、所定の正の整数、前記所定の正の整数を暗号化した正の整数、及びランダムに発生した正の整数からなる群から選ばれる、請求項３又は５に記載の整数を暗号化し復号化する方法。
【請求項７】

前記換字式暗号化は、単表式暗号化、多表式暗号化及び自動鍵暗号化からなる群から選ばれ、
前記換字式復号化は、前記換字式暗号化に対応して単表式復号化、多表式復号化及び自動鍵復号化からなる群から選ばれる、
請求項１に記載の整数を暗号化し復号化する方法。
【請求項８】
前記換字式暗号化及び前記換字式復号化の鍵は、ランダムに発生した整数に基づいて選択される、請求項１に記載の整数を暗号化し復号化する方法。
【請求項９】
さらに、前記整数Ｘｉを変換した整数Ｙｉを生成する前に、前記整数Ｘｉから前記整数Ｘｉ以下の整数Ｔを加算して前記整数Ｘｉと置き換えるステップと、
前記変換した整数Ｙｉを整数Ｘｎに復号化した後に、前記整数Ｘｎに前記整数Ｔを減算して前記整数Ｘｎと置き換えるステップと、
を含む、請求項１に記載の整数を暗号化し復号化する方法。
【請求項１０】
前記整数Ｔはランダムに発生した整数である、請求項９に記載の整数を暗号化し復号化する方法。
【請求項１１】
前記展開形はＸｉの桁を２つに分割し、前記分割した桁の上位の桁により表される整数Ｘｕ及び前記分割した下位の桁により表される整数Ｘｄを生成し、次式を用いてＸｉを置き換えることであり、
【数４】

$$Xi \equiv X_u \times M^{Cd} + X_d$$

式中、Ｍは記数法の底であり、Ｃｄは前記下位の桁の数であり、Ｃｄは少なくとも１であり、前記置き換えたＸｕ又はＸｄを用いて剰余計算を実施する、請求項１に記載の整数を暗号化し復号化する方法。
【請求項１２】
前記整数Ｘｉは、識別子に含まれる文字又は数字の一部又は全体から、可逆的に変換された整数である、請求項１に記載の整数を暗号化し復号化する方法。
【請求項１３】
前記整数Ｘｉは、１次元画像又は２次元画像から可逆的に変換された１次元画像の一部又は全体から、可逆的に変換された整数である、請求項１に記載の整数を暗号化し復号化する方法。
【請求項１４】
さらに、暗号化に先立って、少なくとも一つの桁を元の整数に対して追加することにより桁を増した整数に置き換えるステップを含む、請求項１に記載の整数を暗号化し復号化する方法。
【請求項１５】
さらに、復号化の後に復号化した整数から前記追加した少なくとも一つの桁を除去するステップを含む、請求項１４に記載の整数を暗号化し復号化する方法。
【請求項１６】
請求項１から１５のいずれかに記載の方法の各ステップをコンピュータを用いて実行するための、コンピュータ・プログラム。
【請求項１７】
請求項１から１６のいずれかに記載の方法の各ステップを用いてエンコードした数値を含むコンピュータ可読媒体。
【請求項１８】
整数Ｘｉを暗号化し復号化する装置であって、

換字式暗号化を用いて整数を換字暗号した整数に変換する換字式暗号化実行部と、
換字式復号化を用いて前記換字暗号した整数を復号化する換字式復号化実行部と、
積ＮがＸｉを超える２つの素数Ａ及びＢを生成する素数生成部と、
（Ａ－１）と（Ｂ－１）との積をＤとし、（Ａ－１）と（Ｂ－１）の最小公倍数をＫとし、Ｄ又はＫと素である数をＥとして、次式において項ＸｉのＥ乗が計算手段の整数演算に桁あふれを発生する条件で、次式の展開形を用いて整数Ｘｉを変換した整数Ｙｉを生成する剰余暗号化実行部と、
【数５】

$$Y_i \equiv X_i^{E} \pmod{N}$$

ｍを任意の整数として次式を成立するＦを用意する秘密鍵生成部と、
【数６】

$$E \times F = m \times K + 1$$

次式を用いて前記変換したＹｉをＸｎに復号化する剰余復号化実行部と、
【数７】

$$X_n \equiv Y_i^{F} \pmod{N}$$

を含む、整数を暗号化し復号化する装置。
【請求項１９】
整数Ｘｉを暗号化し復号化するシステムであって、
換字式暗号化を用いて整数を換字暗号した整数に変換する換字式暗号化手段と、
換字式復号化を用いて前記換字暗号した整数を復号化する換字式復号化手段と、
積ＮがＸｉを超える２つの素数Ａ及びＢを生成する素数生成手段と、
（Ａ－１）と（Ｂ－１）との積をＤとし、（Ａ－１）と（Ｂ－１）の最小公倍数をＫとし、Ｄ又はＫと素である数をＥとして、次式において項ＸｉのＥ乗が計算手段の整数演算に桁あふれを発生する条件で、次式の展開形を用いて整数Ｘｉを変換した整数Ｙｉを生成する剰余暗号化手段と、
【数８】

$$Y_i \equiv X_i^{E} \pmod{N}$$

ｍを任意の整数として次式を成立するＦを用意する秘密鍵生成手段と、
【数９】

$$E \times F = m \times K + 1$$

次式を用いて前記変換したＹｉをＸｎに復号化する剰余復号化手段と、
【数１０】

$$X_n \equiv Y_i^{F} \pmod{N}$$

を含む、整数を暗号化し復号化するシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、整数の暗号化及び復号化の方法に関する、特に、本発明は、守秘情報を参照するための識別情報等を高い秘匿性で暗号化し復号化する方法に関する。
【背景技術】

【０００２】
従来より、法人組織等において構成員を識別するためにユニークな整数等を含む識別子を用いることが知られ、例えば国民健康保険制度等において加入者を識別するために８桁程度の数字が用いられ、又は銀行口座を識別するために銀行の支店及び口座のそれぞれに３桁から１０桁程度の数字等が用いられ、あるいはクレジット会員を識別するために１２桁程度の数字が用いられ、適当な区切り記号、文字列又は他の情報等を併用して、識別される本人が覚えやすい形式が適宜用いられている。
また、暗号及びデジタル署名を実現しうる方式として、桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号であるＲＳＡ暗号が知られている（特許文献１及び非特許文献１）。ＲＳＡ暗号は、暗号化の段階においては適当な正数によるべき乗と素数２個の積を法数とする剰余演算とを用い、復号化においては当該積の素因数を要するべき乗根を用いることにより、素因数を知らなければ復号化が困難になることによって暗号の安全性を確保している。
さらに、コンピュータ・ネットワークを介する情報の送受信においてセキュリティを確保するために、暗号化、認証、改ざん検出の機能を有するＳＳＬプロトコル等が知られている（非特許文献２）。ＳＳＬプロトコルに含まれる公開鍵証明書に基づく認証は、ＲＳＡ暗号を用いうることが知られている。
【特許文献１】米国特許第４４０５８２９号
【非特許文献１】「ＲＳＡ暗号」［ｏｎｌｉｎｅ］、平成２０年６月１２日、［平成２０年７月３０日検索］、インターネット、＜ＵＲＬ：ｈｔｔｐ：／／ｊａ．ｗｉｋｉｐｅｄｉａ．ｏｒｇ／ｗｉｋｉ／ＲＳＡ％Ｅ６％９Ａ％９７％Ｅ５％８Ｆ％Ｂ７＞
【非特許文献２】「Ｓｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ」［ｏｎｌｉｎｅ］、平成２０年７月２９日、［平成２０年７月３０日検索］、インターネット、＜ＵＲＬ：ｈｔｔｐ：／／ｊａ．ｗｉｋｉｐｅｄｉａ．ｏｒｇ／ｗｉｋｉ／Ｓｅｃｕｒｅ＿Ｓｏｃｋｅｔｓ＿Ｌａｙｅｒ＞
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかし、従来技術又は従来技術の組み合わせにおいては、暗号化前の数字又は文字と、復号化後の数字又は文字の形式との組み合わせ等を手がかりとして、公開鍵と対をなす秘密鍵が解読されると、同じ公開鍵及び秘密鍵の組み合わせを用いる暗号は全て解読可能になるという弱点があった。ＲＳＡ暗号においては素因数を特定するまでの所用時間の長さを暗号の安全性の根拠としていることから、解読に用いるコンピュータ機器等を高性能化することにより、一定の解読手法であってもより短時間で解読されて秘匿情報が漏洩する可能性が高まるという問題があった。
また、ＲＳＡ暗号化等の公開鍵暗号化方式においては、元の数字が０又は１の場合、又は数字の並びのうちで最後の数字が変換されないために、暗号化した情報が単純さを含む場合があった。
さらに、音声による通話又は印刷物等の文書を介する情報の漏洩においては、コンピュータ・ネットワークを用いて伝達される情報に対するＳＳＬプロトコル等のセキュリティ技術では対応できないため、音声又は文書等を含む多様な形態で個人情報を隠蔽しうる方法が必要であった。
【０００４】
本発明は、暗号化及び復号化の諸段階の実施に要する処理時間は従来技術とほぼ同等のまま、解読装置の高性能化をもってしても鍵の解読の所要時間が非現実的な長期間となる暗号化及び復号化の手順を用い、解読を飛躍的に困難にする方法を提供することを目的とする。本発明は、公開鍵暗号方式だけでは暗号化が不十分な数字に対しても、単純さを残すことなく情報の変換を実施できることを目的とする。これらによって、本発明は、コンピュータ・ネットワークを含む情報通信を介して送受信される個人情報等のセキュリティを確保することを目的とする。また、本発明は、コンピュータ・ネットワーク、音声、又

は文書等の多様な形態で送受信しうる暗号化された情報を、同一の識別番号等から生成することを目的とする。

【課題を解決するための手段】

【０００５】

本発明者は、計算過程において計算機が桁あふれを生じるような大きな数を意図的に発生する計算手順を用い、所定の手順で桁あふれを回避して暗号化及び復号化を実施することにより、個人情報を秘匿する方法を見出した（特願２００８－２４４７６１）。さらに、本発明者は、生成した整数に対して、この方法とは異なる暗号化の方法である換字式暗号化を重畳することにより秘匿性を飛躍的に向上しうることを見出し、本発明を完成するに至った。

本発明では、以下のような解決手段を提供する。

【０００６】

（１）　整数Ｘｉを暗号化し復号化する方法であって、換字式暗号化を用いて整数を換字暗号した整数に変換するステップと、換字式復号化を用いて換字暗号した整数を復号化するステップと、積ＮがＸｉを超える２つの素数Ａ及びＢを生成するステップと、（Ａ－１）と（Ｂ－１）との積をＤとし、（Ａ－１）と（Ｂ－１）の最小公倍数をＫとし、Ｄ又はＫと素である数をＥとして、次式において項ＸｉのＥ乗が計算手段の整数演算に桁あふれを発生する条件で、次式の展開形を用いて整数Ｘｉを変換した整数Ｙｉを生成するステップと、

【数１１】

$$Y_i \equiv X_i^{E} \pmod{N} \qquad \cdots(\mathrm{I})$$

ｍを任意の整数として次式を成立するＦを用意するステップと、

【数１２】

$$E \times F = m \times K + 1 \qquad \cdots(\mathrm{II})$$

次式を用いて変換した整数Ｙｉを整数Ｘｎに復号化するステップと、

【数１３】

$$X_n \equiv Y_i^{F} \pmod{N} \qquad \cdots(\mathrm{III})$$

を含む、整数を暗号化し復号化する方法。

【０００７】

本発明の暗号化及び復号化方法においては、整数演算を実施可能なコンピュータ装置等を用い、整数を入力して暗号化した整数を生成し、当該生成した暗号化した整数を復号化することにより、入力した整数を復元しうる。

入力に用いる整数は、コンピュータ処理可能な整数であればよく、文字又は画像等から可逆的に変換された整数でもよい。例えば、コンピュータ処理可能な文字のそれぞれに割り当てられた文字コード等を１桁、２桁又は４桁等の１６進数の整数として扱ってもよい。また、例えば、英字アルファベットに含まれる２６個の文字を、２６進数を表す１桁の整数として扱ってもよい。また、例えば、コンピュータ処理可能な画像に含まれる個々の画素を、ＲＧＢ各８ビットの整数の一組とする２４ビットの２進数の整数として扱ってもよい。

一実施形態において、構成員の識別番号等の個人情報は、コンピュータ処理可能な整数に可逆的に変換され、本発明の整数を暗号化し復号化する方法の入力に用いられる。

【０００８】

本発明の暗号化及び復号化方法に係る計算手段は、コンピュータに整数演算を実施させるプログラム等であり、アセンブラ又はコンパイラ等により生成された、インタープリタ等により変換された、あるいはスクリプト又はスプレッドシート等が内蔵する計算ルーチ

ンにより呼び出される機械語プログラム等でありうる。
一実施形態において、桁あふれは、コンピュータが備える中央演算ユニット（ＣＰＵ）の演算レジスタに発生しうる。従って、特定のＣＰＵが有する演算レジスタの桁数に従って、有効な桁数の整数演算が実施されうる。例えば、レジスタ長が１６ビットのＣＰＵの場合、整数演算に用いうる整数は、例えば符号なし１６ビット整数として、１０進数の０～６５５３５の範囲である。レジスタ長が３２ビットのＣＰＵの場合は、同様に符号なし３２ビット整数として、１０進数の０～４２９４９６７２９５の範囲である。
別の実施形態において、桁あふれは、インタープリタ、スクリプト又はスプレッドシート等が整数演算のために用意する内部関数において発生しうる。従って、特定のインタープリタ、スクリプト又はスプレッドシート等が有する内部関数が表現可能な整数の桁数に従って、有効な桁数の整数演算が実施されうる。例えば、特定のコンパイラ等において符号なし１６ビット整数の型が定義された変数が表しうる整数は、１０進数の０～６５５３５の範囲である。

【０００９】
また、本発明の方法に係る、換字式暗号化を用いて整数を換字暗号した整数に変換するステップにおいては、入力の整数の数値又は記数法における桁の数字に対して換字暗号が実施される。好適な換字式暗号化はシーザー暗号化であるが、これに限定しない。例えば、整数Ｙｉを換字暗号して整数Ｚｉに換字式暗号化することにおいて、次式のような変換を用いうる。

【数１４】

$$Z_i = Rot(Y_i, R) \qquad \cdots (\mathrm{IV})$$

式中、Ｒは換字式暗号化の鍵として用いる整数であり、Ｒｏｔ（）は鍵Ｒを用いて整数Ｙｉを換字式暗号化する関数である。Ｒｏｔ（）は、十進法等の記数法を用いて整数Ｙｉを記述して得られる数字の並びを文字列として扱う、公知のシーザー暗号化を用いることができる。例えば、シーザー暗号化における鍵Ｒを整数３として、十進数の数字１文字からなる集合｛０，１，２，３，４，５，６，７，８，９｝の各要素に鍵Ｒを加算し、集合｛３，４，５，６，７，８，９，０，１，２｝の各要素を同一の順番で対応させて換字することが可能である。あるいは、シーザー暗号化とは異なって、鍵Ｒはランダムな順序を用いる情報又は所定の数字の並び方の情報等と関連付け、対応させる集合はランダムな順序又は所定の数字の並び方でもよい。またあるいは、元の集合の一部の要素に対して鍵Ｒを用いる換字式暗号化を実施してもよく、当該一部の要素の選択には乱数を用いてもよく、当該一部の要素以外の残りの要素に対して公開鍵暗号化を含む任意の暗号化を実施してもよい。これらに限定せず、記数法の桁の数字を予め用意した規則に従って、可逆的かつ一対一に対応するように換字し、整数Ｙｉを整数Ｚｉに変換してもよい。これらの換字式暗号化は、ループカウンタＬに依存せずに毎回実施してもよく、ループカウンタＬに依存して、初回のみ又は偶数回のみ等、Ｌの所定の値に基づいて実施してもよく、適宜設計しうる。

【００１０】
さらに、本発明の方法に係る、換字式復号化を用いて換字暗号した整数を復号化するステップにおいては、前述の換字式暗号化を用いて変換された整数から、変換前の整数が復号化される。例えば、変換された整数Ｚｉから元の整数Ｙｉを復号化する場合に、次式に示す換字式復号化を用いうる。

【数１５】

$$Y_i = Rot^{-1}(Z_i, R) \qquad \cdots (\mathrm{V})$$

式中、Ｒｏｔ$^{-1}$（）は、換字式暗号化により生成した整数Ｚｉに対して、暗号化の鍵Ｒを用いて元の整数Ｙｉに復号化する関数である。

【００１１】
本発明の方法は、暗号化において上述のべき剰余を用いる暗号化及び換字式暗号化の両者を用い、復号化においてこれらの両者を逆順で用いる。それぞれの暗号化の順序は何でもよく、暗号化において先に換字式暗号化を実施した後にべき剰余を用いる暗号化を実施してもよく、これらを入れ替えて暗号化してもよい。復号化は、対応する暗号化に含まれる換字式又はべき剰余による暗号化の手順を逆順で実施すればよい。
【００１２】
本発明の方法においては、数式（Ｉ）で表されるべき乗の計算において、上述の桁あふれを含む任意の桁あふれを発生するよう、整数Ｅを選択する。桁あふれは、例えばＣＰＵ内部における整数演算中の桁あふれの発生の検出、又はコンパイラ等が適宜備える整数演算ライブラリに含まれる桁あふれに対するエラー処理ルーチン等の、当技術分野に公知の手法を用いて検出しうる。
【００１３】
本発明に係る暗号化及び復号化の方法に用いる展開形は、上述のように桁あふれを発生する条件を満たす整数のべき乗を代替する計算法を含む。具体的には、直接に数式（Ｉ）を用いる代わりに、数式（Ｉ）の項ＸｉのＥ乗における桁あふれを回避するために、当該項を複数の整数の積で表す公知の手法を用いうるが、これに限定しない。
【数１６】

$$Y_i \equiv (X_i^{E-s} \pmod N) \cdot (X_i^{s} \pmod N) \pmod N \quad \cdots (\mathrm{VI})$$

式中、ｓは０＜ｓ＜Ｅを満たす整数である。展開した右辺のいずれかの項が桁あふれを発生する場合は適宜さらにその項を展開してもよい。数式（ＩＶ）のような展開形は整数ｓの選択に計算回数が依存しうる。このように得られたＹｉは、元のＸｉを暗号化した整数でありうる。
【００１４】
また、本発明に係る整数を暗号化し復号化する方法において、数式（ＩＩ）で表される整数Ｆは、任意のｍを含んで選択された素数Ａ及びＢに基づいて生成しうる右辺の式（ｍ×Ｋ＋１）の因数であれば何でもよい。整数Ｅ及びＦの対は、当業に公知の公開鍵暗号化技術における公開鍵及び秘密鍵の対として扱ってもよい。
【００１５】
本発明に係る整数を暗号化し復号化する方法においては、桁あふれを発生する条件で数式（Ｉ）のＥを選択するため、本発明の方法を用いないコンピュータ装置等においては暗号化した整数Ｙｉを正確に得ることができず、情報秘匿性の高い暗号化を実施することが可能になる。また、同じ方法を用いて暗号化を繰り返すことは、他の鍵による１回の暗号化と等価でありうるが、本発明においてはべき剰余と異なる方法である換字式暗号化を含み、これらを重畳することで互いに独立した暗号化を多重に用いることになり、元の情報を飛躍的に解読困難とすることができる。すなわち、Ｆが第三者に知られにくいこと、換字式暗号化及びべき剰余を用いる暗号化が独立して繰り返し用いられうることによる解読の困難さに基づいて、本発明においては高いセキュリティを確保しうる。重畳及び繰り返しの詳細は後述する。
【００１６】
さらに、本発明に係る整数を暗号化し復号化する方法においては、べき剰余による暗号化において特異点である０、１及びＮに対しても、これらの整数を換字式暗号化によって他の整数に変換することにより、べき剰余の特異点ではない整数に暗号化することが可能になる。すなわち、本発明に係る方法においては、従来技術における特異点を元の整数に含んでもよく、第三者による解読の手がかりとなりうる特異点がないことから、より高い秘匿性を提供することが可能になる。
【００１７】
（２）　展開形を用いて整数Ｘｉを整数Ｙｉに変換した後に、換字式暗号化を用いて整数

Ｙｉを整数Ｚｉに変換する、べき剰余と換字とを連続する暗号化ステップと、換字式復号化を用いて整数Ｚｉを整数Ｙｉに復号化した後に、整数ＹｉをＸｎに復号化する、換字とべき剰余とを連続する復号化ステップと、を含む、（１）に記載の整数を暗号化し復号化する方法。

【００１８】

このようにすることで、本発明に係る整数を暗号化する方法においては、異なる暗号化の方法を連続することにより、同じ暗号化の方法の繰り返しからは得られない、より秘匿性の高い暗号化が可能になる。本発明に係る整数を復号化する方法においても、対応する暗号化の手順を知らなければ正確な復号化ができないため、第三者による解読にはより多くの手間を必要とする。従って、本発明に係る整数を暗号化し復号化する方法においては、元の整数に対して極めて高い秘匿性を与えることが可能になる。

【００１９】

（３）　べき剰余と換字とを連続する暗号化ステップ、及び換字とべき剰余とを連続する復号化ステップは、少なくとも２以上の同一の回数実施される、（２）に記載の整数を暗号化し復号化する方法。

【００２０】

このようにすることで、暗号化ステップにおいては、べき剰余と換字とが交互に繰り返される。隣接する暗号化の方法は互いに異なるので、それぞれの暗号化は互いに独立して実施される。すなわち、隣接する二つの暗号化は、等価な一つのべき剰余又は換字式暗号化と置き換えることはできないので、本発明に係る連続する暗号化ステップを用いて暗号化した整数は、第三者による解読により多くの手間を必要とする。同様に、連続する復号化ステップにおける隣接する二つの復号化は、等価な一つのべき剰余又は換字式暗号化と置き換えることはできないため、本発明に係る整数を暗号化し復号化する方法においては、元の整数に対して極めて高い秘匿性を与えることが可能になる。

【００２１】

（４）　整数Ｘｉは換字式暗号化を用いて変換された整数である、換字とべき剰余とを連続する暗号化ステップと、整数Ｙｉから復号化された整数Ｘｎに対して換字式復号化を用いて復号化する、べき剰余と換字を連続する復号化ステップと、を含む、（１）に記載の整数を暗号化し復号化する方法。

【００２２】

本発明に係る整数を暗号化し復号化する方法においては、連続する暗号化ステップとして換字式暗号化とべき剰余を用いる暗号化とが交互に実施され、連続する復号化ステップとしてべき剰余を用いる復号化と換字式復号化とが、暗号化と対応して逆順で交互に実施されればよい。前述の（２）に示したように、暗号化においてべき剰余を用いる暗号化を先に実施する場合は、復号化において換字式復号化を先に実施すればよく、（４）に示すように暗号化において換字式暗号化を先に実施する場合は、復号化においてべき剰余を用いる復号化を先に実施すればよい。これらの連続する手順が実施可能であることは、本発明に係る方法を用いて暗号化したときの正確な情報に基づいてのみ、暗号化された整数が正しく復号化され、当該正確な情報に基づかない解読の試行では、復号化に膨大な手間を必要とすることを意味している。従って、本発明に係る整数を暗号化し復号化する方法においては、元の整数に対して極めて高い秘匿性を与えることが可能になる。

【００２３】

（５）　換字とべき剰余とを連続する暗号化ステップ、及びべき剰余と換字を連続する復号化ステップは、少なくとも２以上の同一の回数実施される、（４）に記載の整数を暗号化し復号化する方法。

【００２４】

前述の（３）に示した暗号化ステップと同様に、本発明においては、換字とべき剰余とを交互に繰り返して暗号化してもよい。隣接する暗号化の方法は互いに異なるので、それぞれの暗号化は互いに独立して実施されうる。すなわち、隣接する二つの暗号化は、等価な一つのべき剰余又は換字式暗号化と置き換えることはできないので、本発明に係る連続

する暗号化ステップを用いて暗号化した整数は、第三者による解読により多くの手間を必要とする。同様に、連続する復号化ステップにおける隣接する二つの復号化は、等価な一つのべき剰余又は換字式復号化と置き換えることはできない。本発明においてはこれらの繰り返し手順が実施可能であり、本発明に係る方法を用いて暗号化したときの正確な情報に基づいてのみ、暗号化された整数が正しく復号化される。一方、当該正確な情報に基づかない第三者による解読の試行においては、復号化に膨大な手間を必要とする。従って、本発明に係る整数を暗号化し復号化する方法においては、元の整数に対して極めて高い秘匿性を与えることが可能になる。

【００２５】

（６）　少なくとも２以上の同一の回数は、所定の正の整数、所定の正の整数を暗号化した正の整数、及びランダムに発生した正の整数からなる群から選ばれる、（３）又は（５）に記載の整数を暗号化し復号化する方法。

【００２６】

当該回数は、コンピュータ・プログラムにおける制御のためのループカウンタ等に記憶させる数値として設定してもよい。当該回数は２回以上であればよいが、暗号化の強度を確保するために、予め下限を設定してもよい。また、暗号化及び復号化の計算処理のための時間を短縮するために、予め上限を設定してもよい。従って、本発明に係る整数を暗号化し復号化する方法における当該回数の値は、予め設定された下限及び／又は上限の範囲に従って、所定の正の整数、所定の正の整数を暗号化した正の整数、及びランダムに発生した正の整数からなる群から選ばれうる。当該回数を暗号化する方法は何でもよい。

このように、べき剰余を用いる暗号化及び換字式暗号化のいずれとも独立した変数でありうる当該回数を秘密とすることで、当該回数は第三者に不明となる。すなわち、第三者の解読の手間はさらに膨大となりうる。従って、本発明に係る整数を暗号化し復号化する方法においては、元の整数に対して極めて高い秘匿性を与えることが可能になる。

【００２７】

（７）　換字式暗号化は、単表式暗号化、多表式暗号化及び自動鍵暗号化からなる群から選ばれ、換字式復号化は、換字式暗号化に対応して単表式復号化、多表式復号化及び自動鍵復号化からなる群から選ばれる、（１）に記載の整数を暗号化し復号化する方法。

【００２８】

本発明に係る換字式暗号化は、前述のシーザー暗号化以外にも、当業に公知の換字式暗号化を用いることが可能である。単表式暗号化は、単一換字式暗号化、単文字換字暗号化、単純換字暗号化を含む公知の暗号化でもよく、多表式暗号化は、ヴィジュネル暗号化、進行鍵暗号化、正方換字表を用いる暗号化を含む公知の暗号化でもよく、自動鍵暗号化は暗号化の鍵が元の整数又は暗号文、又はその両方に基づいて自動的に変更あるいは更新される暗号化でもよい。本発明に係る復号化においても、暗号化と同様に換字式復号化を用いることが可能であり、暗号化として列挙した種々の方法に対応する復号化の手順を用いることが可能である。

【００２９】

（８）　換字式暗号化及び換字式復号化の鍵は、ランダムに発生した整数に基づいて選択される、（１）に記載の整数を暗号化し復号化する方法。

【００３０】

換字式暗号化及び換字式復号化の鍵には、換字式暗号化及び換字式復号化の鍵Ｒ、べき剰余を用いる暗号化及び復号化における公開鍵として用いうる変数Ｅ及び秘密鍵として用いうる変数Ｆ、素数Ａ、素数Ｂ、素数の積Ｎ、任意の整数ｍが含まれる。これらは、第三者による暗号の解読に用いられる可能性又は危険性が伴う情報であり、いずれかの情報から他を推測されないことが望ましい。そこで、本発明に係る整数を暗号化し復号化する方法においては、これらの情報のいずれか又は全体を、ランダムに発生した整数に基づいて選択することにより、第三者による暗号の解読を困難としうる。

【００３１】

一実施形態において、素数Ａ及び素数Ｂは、予め素数の集合等を用意し、この集合の要

素を順番付けし、最大の順番の数字以下の整数の乱数を発生させ、発生した乱数を順番として有する要素として選択することができる。別の実施形態において、素数Ａ及び素数Ｂは、積Ｎ以下の整数の乱数を発生させ、発生した乱数との差が最も小さい素数から選択することができる。他の変数の値を選択することについても同様である。またこれらの選択の手順に限らず、発生した乱数との関連付けが可能な選択の手順により、上記の変数の値を選択してもよい。このようにすることで、本発明に係る整数を暗号化し復号化する方法においては、第三者による暗号の解読をさらに困難としうる。

【００３２】

（９）　さらに、整数Ｘｉを変換した整数Ｙｉを生成する前に、整数Ｘｉから整数Ｘｉ以下の整数Ｔを加算して整数Ｘｉと置き換えるステップと、変換した整数Ｙｉを整数Ｘｎに復号化した後に、整数Ｘｎに整数Ｔを減算して整数Ｘｎと置き換えるステップと、を含む、（１）に記載の整数を暗号化し復号化する方法。

【００３３】

整数Ｔは、いわゆるオフセットであり、本発明に係る暗号化及び復号化においては、前述の換字式暗号化及び復号化に加えて、数値の加算によるオフセットの適用及び当該数値の減算によるオフセットの消去を用いて、情報の秘匿化を行いうる。

特に、べき剰余を用いる暗号化及び復号化においては、従来の公開鍵暗号化技術等では０、１、及び元の整数自身が変換されずに特異点となりうるが、本発明においてはオフセットを用いて従来法における特異点の数値を変更することが可能である。従って、本発明においては、従来法の特異点に係る問題を避けて暗号化及び復号化を実施することが可能になる。ここで、オフセットＴの加算により得られる整数（Ｘｉ＋Ｔ）が、上述の素数Ａ及びＢの積Ｎを超える場合は、入力として受け付ける整数Ｘｉの範囲を（Ｎ－Ｔ）未満としてもよく、積Ｎが整数（Ｘｉ＋Ｔ）を超えるように素数Ａ及びＢを改めて選択してもよく、適宜設計しうる。

【００３４】

（１０）　整数Ｔはランダムに発生した整数である、（９）に記載の整数を暗号化し復号化する方法。

【００３５】

前述の変数Ｅ、変数Ｆ、素数Ａ、素数Ｂ、素数の積Ｎ、任意の整数ｍ等と同様に、整数Ｔも、第三者による暗号の解読に用いられる可能性又は危険性が伴う情報でありうる。本発明に係る整数を暗号化し復号化する方法においては、整数Ｔをランダムに発生した整数とすることにより、第三者による暗号の解読を困難としうる。

【００３６】

（１１）　展開形はＸｉの桁を２つに分割し、分割した桁の上位の桁により表される整数Ｘｕ及び分割した下位の桁により表される整数Ｘｄを生成し、次式を用いてＸｉを置き換えることであり、

【数１７】

$$Xi \equiv X_u \times M^{Cd} + X_d \qquad \cdots（ＶＩＩ）$$

式中、Ｍは記数法の底であり、Ｃｄは下位の桁の数であり、Ｃｄは少なくとも１であり、置き換えたＸｕ又はＸｄを用いて剰余計算を実施する、（１）に記載の整数を暗号化し復号化する方法。

【００３７】

このようにすることで、本発明に係る整数を暗号化し復号化する方法においては、桁あふれを発生する条件で前述の数式（Ｉ）のＥを選択した後に、数式（ＶＩＩ）を用いてＸｉを展開し、桁あふれを避けて、暗号化した整数であるＹｉを正確に得ることができる。

従って、前述の数式（Ｉ）として表されるＸｉのべき乗の計算において、数式（ＶＩＩ）を用いて適宜元の整数Ｘｉを上位の桁と下位の桁とに分割することにより、べき乗の計算過程での桁あふれを避けることが可能になる。

【００３８】
（１２）　整数Ｘｉは、識別子に含まれる文字又は数字の一部又は全体から、可逆的に変換された整数である、（１）に記載の整数を暗号化し復号化する方法。
【００３９】
本発明に係る識別子は、典型的にはコンピュータ処理可能な文字（文字としての数字を含む）又は数値であり、文字は文字コード等の公知技法を用いることによりユニークな整数に変換されうる。従って、本発明に係る整数の暗号化及び復号化の方法においては、ユニークな整数との関連付けが可能な文字又は数値を元の整数として暗号化し、復号化することができる。
【００４０】
（１３）　整数Ｘｉは、１次元画像又は２次元画像から可逆的に変換された１次元画像の一部又は全体から、可逆的に変換された整数である、（１）に記載の整数を暗号化し復号化する方法。
【００４１】
本発明に係る画像は、典型的にはコンピュータ処理可能な画像データであり、例えば一つの画素は、Ｒ（赤）Ｇ（緑）Ｂ（青）の各色ごとに８ビットの階調の値を含む符号なしの２４ビットの整数でありうる。２次元画像は、所定の手順に従って画素を並び替えることにより１次元画像に変換してもよい。このようにして、画素からなる画像は整数として扱うことができ、特定の画像はユニークな整数と関連付けられる。暗号化される元の整数に含まれる画素数は適宜設計しうる。従って、本発明に係る整数の暗号化及び復号化の方法においては、ユニークな整数との関連付けが可能な１次元又は２次元画像を元の整数として暗号化し、復号化することができる。
【００４２】
（１４）　さらに、暗号化に先立って、少なくとも一つの桁を元の整数に対して追加することにより桁を増した整数に置き換えるステップを含む、（１）に記載の整数を暗号化し復号化する方法。
【００４３】
このようにすることで、暗号化される整数Ｘｉに対して、任意に選択される桁数を追加した整数を生成して暗号化の入力に用いうる。桁数を増した整数Ｗｉは、元の整数Ｘｉが同一であっても、増した桁数及び当該桁数の整数に含まれる各桁の数字に依存して変化しうる。従って、同一のＸｉ及び任意に選択される桁数の整数に基づいて、互いに異なる整数Ｗｉを生成して暗号化に用いうる。
一実施形態において、暗号化される整数Ｘｉは生年月日の日付の情報を含む文字列に基づいて生成される４桁、６桁、又は８桁等の整数であり、任意に選択される桁数は例えば２桁の整数でありうる。本発明に係る整数を暗号化し復号化する方法のユーザ等は、自己の生年月日に基づく同一の整数及び任意に選択される２桁の整数から生成される、桁数を増した整数Ｗｉを暗号化の入力とし、当該２桁の整数を使い分けることにより、複数の暗号化した整数を生成して利用しうる。暗号化される整数は例えば１０桁等であっても、ユーザは全ての桁の数字を使用目的ごとに記憶する必要はなく、当該２桁の整数を使い分ければよい。
従って、本発明に係る整数を暗号化し復号化する方法においては、生年月日の日付等の個人情報を含む文字列と関連付けられる整数であっても、任意に選択される桁数を増して暗号化することにより、複数の暗号化した整数を生成して使い分けることが可能になる。
【００４４】
（１５）　さらに、復号化の後に復号化した整数から前記追加した少なくとも一つの桁を除去するステップを含む、（１４）に記載の整数を暗号化し復号化する方法。
【００４５】
このようにすることで、本発明に係る整数を暗号化し復号化する方法においては、復号化の後に、桁を増した整数Ｗｉから元の整数Ｘｉを完全に復号化することが可能になる。
【００４６】

（１６）　（１）から（１５）のいずれかに記載の方法の各ステップをコンピュータを用いて実行するための、コンピュータ・プログラム。

【００４７】

これにより、本発明に係る整数を暗号化し復号化する方法の各ステップをコンピュータに実行させうる。従って、暗号化及び復号化に係る各ステップはコンピュータを用いて自動的に処理されうる。

【００４８】

（１７）　（１）から（１６）のいずれかに記載の方法の各ステップを用いてエンコードした数値を含むコンピュータ可読媒体。

【００４９】

これにより、本発明に係る整数を暗号化し復号化する方法を用いて、記憶媒体に記録する任意のデータ、及び／又は記憶媒体の特定の記憶領域を参照するためのファイル割り当てテーブル等に含まれる数値を暗号化及び復号化しうる。当該データ又は当該数値は整数と見なしうるものであれば何でもよい。すなわち、本発明により、第三者に対して隠蔽したコンピュータ可読媒体を提供しうる。具体的には、コンピュータ可読媒体はフラッシュメモリ等の電気的記憶媒体、ＣＤ－ＲＯＭ等の光学読み取り可能媒体、ハードディスク等の磁気記憶媒体等の任意の形態を含む。本発明に係る整数を暗号化し復号化する方法を用いて提供しうるコンピュータ可読媒体は、暗号化又は復号化の諸段階においてコンピュータ・ネットワーク等を介する必要はなく、ネットワーク等から切り離されたオフライン状態でも本発明に係る暗号化及び復号化の方法を用いてエンコードした情報を記憶しうる。従って、本発明においては、通信技術と連携して動作するセキュリティ技術等とは独立して、単独で暗号化及び復号化の方法を用いるコンピュータ可読媒体を提供しうる。

【００５０】

（１８）　整数Ｘｉを暗号化し復号化する装置であって、換字式暗号化を用いて整数を換字暗号した整数に変換する換字式暗号化実行部と、換字式復号化を用いて換字暗号した整数を復号化する換字式復号化実行部と、積ＮがＸｉを超える２つの素数Ａ及びＢを生成する素数生成部と、（Ａ－１）と（Ｂ－１）との積をＤとし、（Ａ－１）と（Ｂ－１）の最小公倍数をＫとし、Ｄ又はＫと素である数をＥとして、次式において項ＸｉのＥ乗が計算手段の整数演算に桁あふれを発生する条件で、次式の展開形を用いて整数Ｘｉを変換した整数Ｙｉを生成する剰余暗号化実行部と、

【数１８】

$$Y_i \equiv X_i^{E} \pmod{N}$$

ｍを任意の整数として次式を成立するＦを用意する秘密鍵生成部と、

【数１９】

$$E \times F = m \times K + 1$$

次式を用いて変換したＹｉをＸｎに復号化する剰余復号化実行部と、

【数２０】

$$X_n \equiv Y_i^{F} \pmod{N}$$

を含む、整数を暗号化し復号化する装置。

【００５１】

本発明に係る整数の暗号化及び復号化装置においては、ＣＰＵ内部における整数演算中の桁あふれの検出又はプログラム実行中の整数演算の桁あふれ発生の検出を実施可能であればよい。

また、本発明に係る整数の暗号化及び復号化装置においては、桁あふれを発生する条件で前述の数式（Ｉ）のＥを選択した後に、例えば前述の数式（ＶＩＩ）を用いてＸｉを展

開し、桁あふれを避けて、暗号化した整数であるＹｉを正確に得ることができる。
さらに、本発明に係る整数の暗号化及び復号化装置においては、換字式暗号化実行部及び換字式復号化実行部を、べき剰余暗号化及び復号化に重畳して用いることにより、単独の方法の繰り返しでは得られない、秘匿性の高い暗号化を実施し、この暗号化により変換された整数を正しく復号化するための情報を生成することが可能である。
【００５２】
従って、本発明に係る整数を暗号化及び復号化する装置においては、個人情報等と関連付けられた整数に対して高いセキュリティを確保した暗号化した整数を生成でき、この暗号化した整数を正しく復号化して元の整数を得られる。
【００５３】
（１９）　整数Ｘｉを暗号化し復号化するシステムであって、換字式暗号化を用いて整数を換字暗号した整数に変換する換字式暗号化手段と、換字式復号化を用いて換字暗号した整数を復号化する換字式復号化手段と、積ＮがＸｉを超える２つの素数Ａ及びＢを生成する素数生成手段と、（Ａ－１）と（Ｂ－１）との積をＤとし、（Ａ－１）と（Ｂ－１）の最小公倍数をＫとし、Ｄ又はＫと素である数をＥとして、次式において項ＸｉのＥ乗が計算手段の整数演算に桁あふれを発生する条件で、次式の展開形を用いて整数Ｘｉを変換した整数Ｙｉを生成する剰余暗号化手段と、
【数２１】

$$Y_i \equiv X_i^{E} \pmod{N}$$

ｍを任意の整数として次式を成立するＦを用意する秘密鍵生成手段と、
【数２２】

$$E \times F = m \times K + 1$$

次式を用いて変換したＹｉをＸｎに復号化する剰余復号化手段と、
【数２３】

$$X_n \equiv Y_i^{F} \pmod{N}$$

を含む、整数を暗号化し復号化するシステム。
【００５４】
本発明に係る情報を暗号化及び復号化するシステムにおいては、ＣＰＵ内部における整数演算中の桁あふれの検出又はプログラム実行中の整数演算の桁あふれ発生の検出を実施可能であればよく、これを用いて数式（ＩＸ）で表されるべき乗計算に含まれる整数Ｅを選択してもよい。
さらに、本発明に係る整数を暗号化及び復号化するシステムにおいては、桁あふれを発生する条件で前述の数式（ＩＸ）のＥを選択した後に、例えば前述の数式（ＶＩ）を用いてＸｉを展開し、桁あふれを避けて、暗号化した整数であるＹｉを正確に得ることができる。
さらに、本発明に係る整数の暗号化及び復号化するシステムにおいては、換字式暗号化手段及び換字式復号化手段による処理を、べき剰余暗号化及び復号化に重畳するにより、単独の方法の繰り返しでは得られない、秘匿性の高い暗号化を実施し、この暗号化により変換された整数を正しく復号化するための情報を生成することが可能である。
【００５５】
従って、本発明に係る整数を暗号化及び復号化するシステムにおいては、個人情報等と関連付けられた整数に対して高いセキュリティを確保した暗号化した整数を生成でき、この暗号化した整数を正しく復号化して元の整数を得られる。
【００５６】
本発明に係る整数を暗号化及び復号化する方法、装置、システム等は、コンピュータ・

ネットワーク技術等の、既存の情報伝達技術等と組み合わせることができ、そのように組み合わせた技術もまた、本発明の技術範囲に含まれる。同様に、本発明の技法を含む情報記録システム、情報管理システム、情報処理システム等も、本発明の技術範囲に含まれる。さらに、本発明の技法は、暗号化及び復号化の諸段階を、ＦＰＧＡ（現場でプログラム可能なゲートアレイ）、ＡＳＩＣ（特定用途向け集積回路）、これらと同等のハードウェア・ロジック素子、プログラム可能な集積回路、又はこれらの組み合わせが記憶し得るプログラムの形態、すなわちプログラム製品として提供し得る。具体的には、入出力、データバス、メモリバス、システムバス等を備えるカスタムＬＳＩ（大規模集積回路）の形態として、本発明に係る暗号化及び復号化装置等を提供でき、そのように集積回路に記憶されたプログラム製品の形態も、本発明の技術範囲に含まれる。

【発明の効果】

【００５７】

本発明によれば、暗号化及び復号化の諸段階の実施に要する処理時間は従来技術とほぼ同等のまま、解読装置の高性能化をもってしても鍵の解読の所要時間が非現実的な長期間となる暗号化及び復号化の手順を提供し、解読を飛躍的に困難にする暗号化及び復号化の方法を提供することが可能になる。本発明を用いて個人を特定するための識別番号等を、計算機が桁あふれを発生する条件で暗号化した整数を生成することにより、第三者に対して当該整数から当該識別番号の推定を極めて困難として、当該識別番号を秘匿しうるという効果がある。また、本発明によれば、当該識別番号と関連付けられた特定の個人情報が漏洩する状況においても、同一の識別番号と関連付けられた他の複数の個人情報に対する第三者からの推定を極めて困難にしうるという効果がある。また、本発明によれば、生年月日等の同一の個人情報を含む文字列を表す整数及び任意に選択される整数を用いて、桁数を増した整数を暗号化することにより、同一の個人情報等から複数の異なる暗号化した整数を生成して使い分けることが可能になる。さらに、本発明によれば、音声による通話又は印刷物等の文書等を含む多様な形態で個人情報を隠蔽することが可能になる。

【発明を実施するための最良の形態】

【００５８】

以下、本発明の実施形態について、図面を併用して説明する。

【００５９】

［暗号化及び復号化のフロー図］

図１及び図２に、本発明の一実施形態に係る、整数を暗号化し復号化する方法のフロー図を示す。図１は本発明に係る整数を暗号化する方法のフロー図の例であり、図２は当該暗号化した整数を復号化する方法のフロー図の例である。

【００６０】

［暗号化の諸段階］

まず、図１を参照し、暗号化の諸段階を説明する。本発明に係る整数を暗号化する方法は、図１のステップＳ１００において、変数領域を確保する。具体的には、次の表１に列挙する変数を用いる計算のためにコンピュータ装置等のメモリ領域が適宜確保される。

【表１】

表１　変数名及び変数の内容

変数名	変数の内容
Ｘｉ	元の整数
Ｙｉ	暗号化した整数
Ｚｉ	暗号化した整数
Ｘｎ	復号化した整数
Ｙｎ	復号化した整数
Ｎ	Ａ及びＢの積
Ａ	任意の素数
Ｂ	任意の素数
Ｄ	（Ａ－１）及び（Ｂ－１）の積
Ｋ	（Ａ－１）及び（Ｂ－１）の最小公倍数
Ｅ	Ｄ又はＫと素である任意の整数
Ｆ	数式（ＩＩ）を満たす任意の整数
ｍ	任意の整数
Ｒ	換字式暗号化の鍵
Ｌ	ループカウンタ
Ｔ	オフセット

【００６１】

このとき、ループカウンタＬ等の初期設定を適宜実施してもよい。

例えば、べき剰余を用いる暗号化及び換字式暗号化の組み合わせを全体として３回繰り返す場合に、ステップＳ１００においてループカウンタＬに整数３を設定してもよい。これに限定せず、ループカウンタＬは、所定の正の整数、前記所定の正の整数を暗号化した正の整数、及びランダムに発生した正の整数からなる群から選択してもよい。

ループカウンタＬは、べき剰余を用いる暗号化及び換字式暗号化のいずれとも独立した変数であり、暗号化による秘匿性の強度に影響し、暗号化及び復号化のために計算時間に影響しうる。

ループカウンタＬに対して、秘匿性の強度を確保するために、予め下限を設定してもよい。さらに、暗号化及び復号化の計算処理のための時間を短縮するために、予め上限を設定してもよい。従って、本発明に係る整数を暗号化し復号化する方法におけるループカウンタＬの値は、予め設定された下限及び／又は上限の範囲に従って、所定の正の整数、前記所定の正の整数を暗号化した正の整数、及びランダムに発生した正の整数からなる群から選ばれうる。ループカウンタＬを第三者に秘密とすることで、それぞれの暗号化の方法における秘匿性に加えて、第三者の解読の手間はさらに膨大となりうる。従って、本発明に係る整数を暗号化し復号化する方法においては、元の整数に対して極めて高い秘匿性を与えることが可能になる。

【００６２】

他の、べき剰余を用いる暗号化に含まれる変数であるオフセットＴ及び任意の整数ｍ、並びに換字式暗号化に含まれる変数である鍵Ｒも同様に、第三者に秘密となるように選択してもよい。

【００６３】

暗号化する整数としては、識別子等に含まれうる符号なしの整数が挙げられるが、これに限定せず、任意の形式の整数を本発明に係る方法に用いうる。好適には、暗号化する整数は０以上の任意の整数でありうる。

一実施形態において、計算に用いるコンピュータ装置等における整数Ｘｉ、Ｙｉ、Ｚｉ、Ｘｎ及びＹｎのワード長は、当該コンピュータ装置等が備えるＣＰＵの内部命令において一つの整数を表すために用いうるレジスタのビット幅の最大以内でありうる。例えば、１６ビットレジスタを用いて内部命令に含まれる整数演算を実施可能なＣＰＵを備えるコンピュータ装置においては、整数Ｘｉ、Ｙｉ、Ｚｉ、Ｘｎ及びＹｎのワード長は１６ビッ

ト以下であり、これらの整数の変数は１０進数の記法における０以上６５５３５以下でありうる。

【００６４】

変数領域を確保した後、本発明に係る整数を暗号化する方法は、ステップＳ１０に含まれるべき剰余を用いて暗号化する諸段階、及びステップＳ３０に含まれる換字式暗号化の諸段階を、順次実施する。

【００６５】

ステップＳ１０は、Ｓ１１０からＳ１５０の各ステップを含む。まず、本発明に係る整数を暗号化する方法は、ステップＳ１１０において、積ＮがＸｉを超える２つの素数Ａ及びＢを生成する。素数Ａ及びＢは、予め素数の集合等を用意して適宜選択してもよい。

次いで、本発明に係る整数を暗号化する方法は、ステップＳ１２０において、（Ａ－１）と（Ｂ－１）との積をＤに代入し、（Ａ－１）と（Ｂ－１）の最小公倍数をＫに代入する。

次いで、本発明に係る整数を暗号化する方法は、ステップＳ１３０において、Ｄ又はＫと素である整数Ｅを生成する。

次いで、本発明に係る整数を暗号化する方法は、ステップＳ１４０において、次の数式（ＶＩＩＩ）の右辺の項（ＸｉのＥ乗）が、計算手段の整数演算に桁あふれを発生するか否かを判定する。判定の結果が真であればステップＳ１５０に進み、偽であればステップＳ１３０に戻る。

【数２４】

$$Y_i \equiv X_i^{E} \pmod{N} \qquad \cdots(\mathrm{VIII})$$

【００６６】

桁あふれの検出は、計算手段が備えるＣＰＵの内部動作の状況を記憶するための、ＣＰＵの特定のレジスタに含まれるフラグ（例えばステータス・レジスタ又はコンディション・レジスタ等に含まれるオーバーフロー・フラグ等）の値を参照してもよく、コンパイラ言語等により予めオペレーティング・システムに例外処理等を登録して当該例外処理の動作を参照してもよく、スクリプト言語又はコンパイラ言語等に付属するライブラリ等が備えるオーバーフロー・エラー処理を参照してもよく、適宜設計しうる。

【００６７】

次いで、本発明に係る整数を暗号化する方法は、ステップＳ１５０において、数式（ＶＩＩＩ）の展開形を用いて、整数Ｘｉを暗号化した整数Ｙｉを生成しうる。数式（ＶＩＩＩ）の展開形には、例えば次の式を用いうる。

【数２５】

$$Xi = X_u \times M^{Cd} + X_d \qquad \cdots(\mathrm{IX})$$

式中、Ｍは記数法の底であり、Ｃｄは前記下位の桁の数であり、Ｃｄは少なくとも１でありうる。すなわち、このようにして置き換えたＸｕ又はＸｄを用いて、数式（ＶＩＩＩ）の剰余計算を実施しうる。

このようにすることで、本発明に係る整数を暗号化し復号化する方法においては、桁あふれを発生する条件で前述の数式（ＶＩＩＩ）のＥを選択した後に、数式（ＩＸ）を用いてＸｉを展開し、桁あふれを避けて、暗号化した整数であるＹｉを正確に得ることができる。

【００６８】

一実施形態において、記数法の底であるＭを１０とし、Ｘｉの桁数を１０桁、下位の桁数Ｃｔを５桁とする場合、数式（ＩＸ）は次式のように表される。

【数２６】

$$Xi = X_u \times 10^5 + X_d \qquad \cdots(\mathrm{X})$$

別の実施形態において、記数法の底であるＭを２とし、Ｘｉの桁数を１６桁、下位の桁数Ｃｔを８桁とする場合、数式（ＩＸ）は次式のように表される。

【数２７】

$$Xi = X_u \times 2^8 + X_d \qquad \cdots(\mathrm{XI})$$

【００６９】

例えば、本発明に係る整数を暗号化し復号化する方法の実施手段等が１６ビット幅のレジスタを有するＣＰＵを備えるコンピュータ装置等である場合に、元の整数Ｘｉの値が１０進数の６５５３２等であると、Ｘｉのべき乗の計算において、最も小さい整数のべき数でありうる２を用いた時点で、当該ＣＰＵが備える１６ビット幅のレジスタを用いて表しうる整数の上限値６５５３５を超えてしまう。すなわち、単に元の整数をそのままべき乗する通常の計算方法に従って数式（ＶＩＩＩ）の右辺に含まれるＸｉのＥ乗の計算を実施すると、正確なべき乗の値が得られない場合がある。

本発明に係る方法においては、数式（ＩＸ）又はその具体例である数式（Ｘ）又は数式（ＸＩ）等を用いて上位の桁と下位の桁を分離しうる。例えば前述の元の整数Ｘｉの値である６５５３２を、２進数の１１１１１１１１１１１１１１００（２）として表し、上位８桁と下位８桁等に分割し、上位８桁に含まれる整数１１１１１１１１（２）（１０進数の２５５）及び下位８桁に含まれる整数１１１１１１００（２）（１０進数の２５２）を用い、２５５の２乗、２５５と２５２の積、２５２の２乗をそれぞれ計算すると、これらの整数の積はいずれも当該ＣＰＵが備える１６ビット幅のレジスタを用いて表しうる整数の範囲内にあることは明白である。３２ビット幅のレジスタ、６４ビット幅のレジスタ等についても同様である。

従って、前述の数式（ＶＩＩＩ）として表されるＸｉのべき乗の計算において、最も少ない回数であるＸｉの２乗の場合に、数式（ＸＩ）の右辺の２乗からは、Ｘｕの２乗、Ｘｕ・Ｘｄ、及びＸｄの２乗が生成され、これらはいずれも元のＸｉの桁数以下の整数でありうるため、桁あふれを避けられる。すなわち、Ｘｉの任意のべき乗において、数式（ＸＩ）の手順を繰り返すことにより、べき乗の計算過程での桁あふれを避けることが可能になる。

分割する桁数は、計算手段等が備えるＣＰＵの整数演算のためのレジスタのビット幅等に基づいて適宜設定しうる。好適には、符号なし整数演算のためのレジスタのビット幅を等分した上位の桁数及び下位の桁数を、分割した桁数として用いうる。

【００７０】

以上の諸段階により、元の整数Ｘｉから、べき剰余を用いて暗号化した整数であるＹｉを得られる。整数Ｙｉを表すために必要なワード長は、元の整数Ｘｉを表すためのワード長と同じでありうるが、これに限定せず、暗号化した整数Ｙｉの用途等に応じて、又は他のセキュリティ手段又は方法等を組み合わせて、桁数を増す数字等を追加してもよく、あるいは整数Ｙｉを文字に変換して適宜記号等を含む文字を任意に追加してもよい。

【００７１】

さらに、本発明に係る整数を暗号化する方法は、ステップＳ３０に含まれる換字式暗号化の諸段階を、順次実施する。ステップＳ３０は、次のＳ３１０及びＳ３２０の各ステップを含む。まず、本発明に係る整数を暗号化する方法は、ステップＳ３１０において、鍵Ｒで整数Ｙｉを換字式暗号化し、整数Ｚｉを生成する。例えば、整数Ｚｉは、次式で表される。

【数２８】

$$Z_i = Rot(Y_i, R) \quad \cdots（ＸＩＩ）$$

式中、Ｒは換字式暗号化の鍵として用いる整数であり、Ｒｏｔ（）は鍵Ｒを用いて整数Ｙｉを換字式暗号化する関数である。具体的には、Ｒｏｔ（）は、十進法等の記数法を用いて整数Ｙｉを記述して得られる数字の並びを文字列として扱う、公知のシーザー暗号化を用いることができる。例えば、シーザー暗号化における鍵Ｒを整数３として、十進数の数字１文字からなる集合｛０，１，２，３，４，５，６，７，８，９｝の各要素に鍵Ｒを加算し、集合｛３，４，５，６，７，８，９，０，１，２｝の各要素を同一の順番で対応させて換字することが可能である。あるいは、シーザー暗号化とは異なって、鍵Ｒはランダムな順序を用いる情報又は所定の数字の並び方の情報等と関連付け、対応させる集合はランダムな順序又は所定の数字の並び方でもよい。またあるいは、元の集合の一部の要素に対して鍵Ｒを用いる換字式暗号化を実施してもよく、当該一部の要素の選択には乱数を用いてもよく、当該一部の要素以外の残りの要素に対して公開鍵暗号化を含む任意の暗号化を実施してもよい。これらに限定せず、記数法の桁の数字を予め用意した規則に従って、可逆的かつ一対一に対応するように換字し、整数Ｙｉを整数Ｚｉに変換してもよい。これらの換字式暗号化は、ループカウンタＬに依存せずに毎回実施してもよく、ループカウンタＬに依存して、初回のみ又は偶数回のみ等、Ｌの所定の値に基づいて実施してもよく、適宜設計しうる。

例えば、英字アルファベットを２６進数の１桁の数字として扱い、ｕｎｉｘ（登録商標）オペレーティング・システムが備える文字列をシーザー暗号化するためのｒｏｔ１３関数等を利用してもよい。また例えば、このｒｏｔ１３関数が有する鍵である、整数の１３に換えて任意の１桁の整数を鍵に用い、同様の関数を１０進数の整数に対するシーザー暗号化の関数として定義して用いてもよい。

【００７２】

次いで、本発明に係る整数を暗号化する方法は、ステップＳ３２０において、必要であれば桁数の情報を保持する。例えば、換字式暗号化により生成した整数Ｚｉの最上位がゼロである場合に、この情報を変換前の整数Ｙｉの桁数として保持してもよい。当該保持した桁数の情報は、後述する復号化の諸段階において生成する整数の確認のために用いられてもよい。

【００７３】

ステップＳ１０及びステップＳ３０を続けて実施した後に、本発明に係る整数を暗号化する方法は、ステップＳ１８０において、ループカウンタＬをデクリメントする。さらに、ステップＳ１９０において、ループカウンタＬが０以下であるかを判定する。判定の結果が真であれば終了し、偽であればステップＳ１９５に進み、上述の式（ＸＩＩ）から生成した整数ＺｉをＸｉとして、ステップＳ１０の諸段階を繰り返す。

なお、繰り返しにおいて、変数Ａ、Ｂ、Ｄ、Ｋは同じ値を再利用してもよい。変数Ｅ及びＦの対も同じ値を再利用してもよいが、より好適には、ループカウンタＬの値に依存して変数Ｅ及びＦの対を変化することにより、第三者による解読をさらに困難にすることが可能になる。

このようにして、ステップＳ１９０の判定が真になるまで上述の諸段階を繰り返し、暗号化した整数Ｚｉが得られる。例えば、ループカウンタＬを３とした場合には、上述のステップＳ１０及びステップＳ３０からなる諸段階が３回繰り返される。

【００７４】

従って、本発明に係る整数を暗号化する方法においては、ループカウンタＬが０以下となるまで、ステップＳ１０に含まれるべき剰余を用いる暗号化の諸段階、及びステップＳ３０に含まれる換字式暗号化の諸段階が、続けて繰り返して実行される。べき剰余を用いる暗号化の諸段階と換字式暗号化の諸段階とは、全体を入れ替えてもよい。すなわち、ステップＳ１００の変数初期化の後にステップＳ３０に含まれる換字式暗号化の諸段階を実施し、その後にステップＳ１０に含まれるべき剰余を用いる暗号化の諸段階を実施し、ス

テップＳ１８０及びステップＳ１９０、適宜ステップＳ１９５を実施してもよい。

【００７５】

このように、本発明に係る整数を暗号化する方法においては、べき剰余を用いる暗号化の諸段階と換字式暗号化の諸段階とを重畳して用いることにより、いずれかの暗号化のみを用いる場合と比較して、極めて高い秘匿性を確保することが可能になる。

【００７６】

［復号化の諸段階］

次に、復号化の諸段階を説明する。本発明に係る整数を暗号化する方法は、図２のステップＳ２００において、変数領域を確保し、ループカウンタＬを初期化する。この変数領域の確保は、前述の暗号化の諸段階におけるステップＳ１００と同様でもよく、暗号化及び復号化の諸段階を一つのコンピュータ装置等に内蔵し、共通の変数領域を暗号化及び復号化の両方の諸段階に用いてもよい。ループカウンタＬの初期化は、復号化と対応する暗号化におけるループカウンタＬの値を繰り返し用いうる。例えば、暗号化においてループカウンタＬを３とした場合には、復号化においても同様にループカウンタＬを３とする。

次いで、本発明に係る暗号化した整数を復号化する方法は、ステップＳ４０に含まれる換字式暗号を復号化する諸段階、及びステップＳ２０に含まれるべき剰余を用いる復号化の諸段階を実施する。ここで、復号化の対象になる数は、図１を用いて前述した暗号化した整数Ｚｉである。

【００７７】

ステップＳ４０は、Ｓ４１０及びＳ４２０の各ステップを含む。ステップＳ４１０では、必要であれば整数Ｚｉの桁数の情報が復元される。これは、単に暗号化の過程において保持した情報との照合のために行われてもよい。ステップＳ４２０においては、換字式暗号の復号化が実施され、暗号化した整数Ｚｉから整数Ｙｉを生成する。例えば、整数Ｙｉは次式により復号化される。

【数２９】

$$Y_i = Rot^{-1}(Z_i, R) \qquad \cdots(\mathrm{XIII})$$

式中、Ｒｏｔ$^{-1}$（）は、換字式暗号化により生成した整数Ｚｉを、鍵Ｒを用いて元の整数Ｙｉに復号化する関数である。

【００７８】

次いで、本発明に係る整数を暗号化する方法においては、ステップＳ２０に含まれるべき剰余を用いる復号化の諸段階を実施する。ステップＳ２０は、Ｓ２１０及びＳ２２０の各ステップを含む。まず、本発明に係る整数を暗号化する方法は、ステップＳ２１０において、ｍを任意の整数として次の数式（ＸＶＩ）を成立するＦを生成する。

【数３０】

$$E \times F = m \times K + 1 \qquad \cdots(\mathrm{XIV})$$

数式（ＸＶＩ）において、整数Ｆは、任意のｍを含んで選択された素数Ａ及びＢに基づいて生成しうる右辺の式（ｍ×Ｋ＋１）の因数であれば何でもよい。

次いで、本発明に係る暗号化した整数を復号化する方法は、ステップＳ２２０において、次の数式（ＸＶＩＩ）を用いて前記暗号化したＹｉをＸｎに復号化する。

【数３１】

$$X_n \equiv Y_i^F \pmod{N} \qquad \cdots(\mathrm{XV})$$

【００７９】

このようにすることで、本発明に係る整数を暗号化し復号化する方法においては、桁あふれを発生する条件で数式（ＶＩＩＩ）のＥを選択するため、本発明の方法を用いないコンピュータ装置等においては暗号化した整数Ｙｉを正確に得ることができず、情報秘匿性の高い暗号化を実施することが可能になる。

さらに、本発明の整数を暗号化し復号化する方法においては、暗号化の過程である数式（ＶＩＩＩ）に含まれず、復号化の過程である数式（ＸＶＩ）及び数式（ＸＶＩＩ）に含まれる整数Ｆが第三者に知られにくい又は推定されにくいことに基づいて高いセキュリティを確保しうる。

なお、式（ＸＩＶ）の左辺に含まれるＥ及びＦを、当業に公知の公開鍵暗号に係る公開鍵及び秘密鍵の対として用いうること、鍵の保管又は認証に第三者機関等を用いうること等、公開鍵暗号技術に関連する方法は周知であり、本発明に適宜取り入れて用いることができる。

【００８０】

ステップＳ４０及びステップＳ２０を続けて実施した後に、本発明に係る整数を暗号化する方法は、ステップＳ２８０において、ループカウンタＬをデクリメントする。さらに、ステップＳ２９０において、ループカウンタＬが０以下であるかを判定する。判定の結果が真であれば終了し、偽であればステップＳ２９５に進み、上述の式（ＸＶ）から生成した整数ＸｎをＺｉとして、ステップＳ４０の諸段階を繰り返す。このようにして、ステップＳ２９０の判定が真になるまで上述の諸段階を繰り返し、復号化した整数Ｘｎが得られる。例えば、ループカウンタＬを３とした場合には、上述のステップＳ４０及びＳ２０からなる諸段階が３回繰り返される。

【００８１】

従って、本発明に係る整数を暗号化する方法においては、ループカウンタＬが０以下となるまで、ステップＳ４０に含まれる換字式暗号を復号化する諸段階、及びステップＳ２０に含まれるべき剰余を用いる復号化の諸段階が、続けて繰り返して実行される。換字式暗号を復号化する諸段階とべき剰余を用いる復号化の諸段階とは、暗号化の諸段階の逆順であればよく、全体を入れ替えてもよい。すなわち、ステップＳ２００の変数初期化の後にステップＳ２０に含まれるべき剰余を用いる復号化の諸段階を実施し、その後にステップＳ４０に含まれる換字式暗号を復号化する諸段階を実施し、ステップＳ２８０及びステップＳ２９０、適宜ステップＳ２９５を実施してもよい。

【００８２】

このように、本発明に係る整数を暗号化する方法においては、換字式暗号を復号化する諸段階とべき剰余を用いる復号化の諸段階とを重畳して用い、対応する暗号化の諸段階により暗号化された整数Ｚｉから、元の整数Ｘｉと等しい整数Ｘｎに復号化することが可能になる。

【００８３】

図１に示した本発明に係る整数を暗号化する方法、及び図２に示した整数を復号化する方法においては、個人を識別するための識別子等を整数型の識別子として受け付けて暗号化しうる。これに限らず、本発明に係る整数を暗号化し復号化する方法においては、整数のべき乗及び剰余計算等を実施可能なコンピュータ装置等が受け付けうる、種々のデータもまた暗号化及び復号化に用いうる。例えば、整数に変換した画像を本発明の方法を用いて暗号化及び復号化することにより、第三者に対して隠蔽した画像の伝達が可能になる。また例えば、記憶媒体の特定の記憶領域を参照するためのファイル割り当てテーブル等を本発明の方法を用いて暗号化及び復号化することにより、第三者に対して隠蔽した記憶媒体等を提供しうる。これらの、本発明に係る整数を暗号化し復号化する方法を用いて提供しうる記憶媒体等は、暗号化又は復号化の諸段階においてコンピュータ・ネットワーク等を介する必要はなく、ネットワーク等から切り離されたオフライン状態でも暗号化及び復号化を実施可能である。従って、本発明においては、通信技術と連携して動作するセキュリティ技術等とは独立して、単独で暗号化及び復号化の方法を提供しうる。

【００８４】

［個人情報隠蔽手順の形態］

図３に、本発明の一実施形態に係る、整数を暗号化する方法を用いる個人情報隠蔽手順の例を示す。

暗号化手段１００は、本発明に係る入力された整数から暗号化した整数を生成する手段

である。暗号化手段１００は、特定の個人２０が有する識別のための数字及び／又は文字を含む識別子等を、整数型の識別子３０として受け付ける。具体的には、個人２０は事業体等に所属する構成員の１人であり、整数型の識別子３０は当該事業体において複数の構成員を識別するために適宜用いられる、複数の桁の整数を含む構成員識別子等でありうる。例えば、当該構成員識別子の形態は、当該事業体等の所属が開始された年次を表す数字２桁及び同時期に所属を開始した他の構成員を含む複数の構成員のそれぞれに割り当てられた６桁の数字等からなる、全体として８桁の数字等であり、適宜設定しうる。典型的には、特定の個人２０と整数型の識別子３０とは１対１に関連付けられ、他の構成員等とは関連付けられない。また、構成員識別子等が英文字等を含む場合、整数型の識別子３０は、英文字及び数字の全体又はその一部をコンピュータ処理可能な文字コードの集まりとして扱い、個々の文字コードを１６進法の整数として、整数型の識別子３０を構成してもよい。本発明に係る整数を暗号化し復号化する方法においては、このように変換された１６進法の整数を暗号化し、当該暗号化した１６進法の整数から元のコンピュータ処理可能な文字コードの集まりを復号化しうる。構成員識別子等が画像データの場合についても、１６進法の整数の集まりとして元の画像データを扱うことにより、同様に暗号化及び復号化が可能である。

【００８５】

識別用途Ａ（１２２）、識別用途Ｂ（１２４）及び識別用途Ｃ（１２６）は、整数型の識別子３０を用いて特定の個人２０を識別することが必要な任意の用途でありうる。図１にはこれらの３つの識別用途を図示するが、これらに限定せず、識別用途の種類、個数等は適宜設定しうる具体的には、これらの用途は、特定の個人２０による電子メール送受信等を含む事業体内部のコンピュータ・ネットワーク利用又は事業体と関連付けられるオンライン銀行業務又は保険サービス等の利用、あるいは事業体による特定の個人２０の業務に係る記録行為等でありうる。それぞれの識別用途Ａ（１２２）、識別用途Ｂ（１２４）及び識別用途Ｃ（１２６）は、暗号化手段１００において互いに他を区別するための情報を含んでもよい。すなわち、識別用途Ａの固有情報（６２）、識別用途Ｂの固有情報（６４）及び識別用途Ｃの固有情報（６６）等は、互いに他と異なればよい。例えば、これらの識別用途の固有情報は特定の整数の値でもよく、前述の数式（ＶＩＩＩ）に含まれるＮ又はＥの値として、それぞれ独立して異なる値を用いてもよい。

【００８６】

暗号化手段１００は、受け付けた整数型の識別子３０に対して、識別用途Ａの固有情報（６２）、識別用途Ｂの固有情報（６４）又は識別用途Ｃの固有情報（６６）を用い、それぞれの識別用途の固有情報ごとに独立して、暗号化計算Ａ（７２）、暗号化計算Ｂ（７４）又は暗号化計算Ｃ（７６）を実施しうる。当該暗号化計算には、前述のように、整数のべき乗を含む計算のために暗号化手段１００が用いるコンピュータ装置等において桁あふれを発生する条件で、数式（ＶＩＩＩ）の展開形を用いて暗号化した整数を生成する諸段階を含む。当該暗号化計算の結果として、暗号化した整数Ａ（４２）、暗号化した整数Ｂ（４４）又は暗号化した整数Ｃ（４６）が生成される。

【００８７】

生成したそれぞれの暗号化した整数Ａ（４２）、暗号化した整数Ｂ（４４）又は暗号化した整数Ｃ（４６）のそれぞれは、独立して、対応する識別用途Ａ（１２２）、識別用途Ｂ（１２４）又は識別用途Ｃ（１２６）のために提供されうる。

例えば、識別用途Ａ（１２２）が事業体内部のコンピュータ・ネットワーク利用等である場合、本発明に係る暗号化手段１００は、特定の個人２０を識別するための整数型の識別子３０に替えて暗号化した整数Ａ（４２）を、情報伝達経路Ａ（８２）を介して当該事業体のコンピュータ・ネットワーク１３２等に提供しうる。情報伝達経路Ａ（８２）は例えば当該事業体内のローカルエリアネットワーク等でありうる。

また、例えば、識別用途Ｂ（１２４）が事業体による特定の個人２０の業務に係る記録行為等である場合、本発明に係る暗号化手段１００は、特定の個人２０を識別するための整数型の識別子３０に替えて暗号化した整数Ｂ（４４）を、情報伝達経路Ｂ（８４）を介

して当該事業体の勤務管理記憶装置１３４等に提供しうる。情報伝達経路Ｂ（８４）は例えば当該事業体の出入口等に適宜備えられた入構者記録のための端末装置及び記憶装置等でありうる。

【００８８】

これらのコンピュータ処理可能な数値データに限らず、暗号化手段１００は、特定の個人２０を識別するための整数型の識別子３０に替えて暗号化した整数Ｃ（４６）を、情報伝達経路Ｃ（８６）を介して不特定の他者１３６等に提供しうる。情報伝達経路Ｃ（８６）は、口頭又は文書等を含む任意の形式でもよい。例えば、不特定の他者１３６は当該事業体と独立して運営される団体加入保険サービス業の受け付け担当者であり、当該事業体の構成員である特定の個人２０は、情報伝達経路Ｃ（８６）として一般公衆回線の電話等を用い、当該団体保健サービスにおいて自己を特定するための情報として、暗号化した整数Ｃ（４６）を送信しうる。この送信は、通話、ファクシミリ、電子メール等の任意の形態を含む。従って、電話等の通話の音声がたまたま周囲にいる第三者に聞かれてしまう等の状況により、この送信の内容が無関係の第三者に傍受されても、本発明に係る暗号化手段１００により暗号化した整数Ｃ（４６）は、特定の個人２０を識別するための整数型の識別子３０とは異なる整数であるため、当該第三者は傍受内容から当該整数型の識別子３０を知ることができない。すなわち、本発明に係る暗号化手段１００を用いることにより、個人情報を隠蔽することが可能になる。

このようにして、本発明に係る暗号化手段１００においては、特定の個人２０に関連付けられる整数型の識別子３０から、識別用途ごとに異なる暗号化した整数を生成し、当該特定の個人２０の個人情報を隠蔽しうる。

【００８９】

さらに、本発明に係る暗号化手段１００は、特定の識別用途において複数の構成員の識別子を一括して暗号化してもよい。

図１に示し、識別用途Ａ（１２２）、識別用途Ａの固有情報（６２）、暗号化計算Ａ（７２）及び暗号化した整数Ａ（４２）を用いて上述のように、本発明に係る暗号化手段１００は特定の識別用途に対して特定の個人情報を隠蔽しうる。ここで、暗号化手段１００が受け付ける整数型の識別子３０が個々の特定の個人２０ごとに異なることにより、別個の整数型の識別子３０ごとに、暗号化した整数が生成される。従って、識別用途Ａ（１２２）、識別用途Ａの固有情報（６２）及び暗号化計算Ａ（７２）が一定であっても、異なる整数型の識別子３０を有する次行体内の複数の構成員等は、それぞれが異なる暗号化した整数Ａ（７２）を得ることができる。

例えば、事業体のネットワーク管理者等は、識別用途Ａの固有情報（６２）をネットワーク・メンテナンスの日時等の特定の条件に従って選択することにより、当該事業体の複数の構成員のネットワーク・アカウント情報のそれぞれを別個に一括して暗号化しうる。ネットワーク管理者等は識別用途Ａの固有情報（６２）を選択する条件を管理することにより、複数の構成員のアカウント情報を一括して暗号化して保持し、管理しうる。さらに数式（ＸＶＩ）及び数式（ＸＶＩＩ）に含まれる整数Ｆが第三者に知られにくい又は推定されにくいことにより、この値を知らない第三者に対して明示的なアカウント情報を隠蔽することが可能になる。

【００９０】

図３には、特定の個人２０から事業体のコンピュータ・ネットワーク１３２、事業体の勤務管理記憶装置１３４、又は不特定の他者１３６等に向けて、本発明に係る暗号化手段１００を用いて整数型の識別子３０を暗号化して送信することを示すが、送受信の主体を入れ替えても、本発明に係る暗号化手段１００を用いることができる。すなわち、事業体のコンピュータ・ネットワーク１３２に接続されたサーバ装置（図示せず）等が記憶した整数型の識別子３０を本発明に係る暗号化手段１００への入力として、上述の手順に従って暗号化した整数Ａ（４２）等を生成し、特定の個人２０に送信してもよい。このようにすることで、事業体等は、構成員の識別情報又は事業に関連する情報等を暗号化し、当該暗号化した識別子等を使用するよう従業員に促して、セキュリティを高めることが可能に

なる。

【００９１】

本発明に係る暗号化手段１００は、具体的にはパーソナル・コンピュータ等で実行可能な汎用のワークシート等のアプリケーションに内蔵された整数計算ライブラリ等を用いて実施しうる。従って、本発明に係る整数を暗号化し復号化する方法においては、特に専用の計算機等を用意することなく、既存の計算機を用いて社員番号等の暗号化及び復号化を実施することも可能である。さらに、本発明においては、本発明に係る整数を暗号化し復号化する方法によらなければ暗号化又は復号化のいずれかの諸段階における桁あふれが発生して、正確な暗号化及び／又は復号化ができないため、本発明の方法を実施しない第三者に対して構成員の識別子等の個人情報を隠蔽することが可能になる。

【００９２】

［個人情報隠蔽手順の別の形態］

図４に、本発明の一実施形態に係る、整数を暗号化する方法を用いる個人情報隠蔽手順の別の例を示す。図３と共通する箇所は説明を省略する。

【００９３】

図４においては、暗号化手段１００は特定の個人２０から受け付けた整数型の識別子３０に対して、追加の桁３７を適宜追加しうる。この追加の桁は整数型の識別子３０と同様に整数でありうる。追加の桁３７の桁数は何桁でもよく、例えば２桁、３桁、又は４桁等でもよい。追加の桁３７は、整数型の識別子３０に対して左側から追加してもよく右側から追加してもよい。あるいは、整数型の識別子３０を予め定めた桁において分割し、追加の桁３７を挿入してもよく、追加の桁３７の追加の態様は適宜設定しうる。また、追加の桁３７の値は何でもよく、本発明に係る整数の暗号化及び復号化を利用する事業体又はシステム等により任意に用意されてもよく、あるいは整数型の識別子３０から予め定めた手順により生成してもよい。例えば、整数型の識別子３０の各桁の数字の和を算出した値の下位２桁等を、追加の桁３７としてもよい。さらに、追加の桁３７は、識別用途Ａ（１２２）、識別用途Ｂ（１２４）及び識別用途Ｃ（１２６）等に依存してそれぞれの識別用途ごとに独立して用意されてもよい。

追加の桁３７を追加することにより、整数型の識別子３０及び追加の桁３７に含まれる各桁の数字を含む新たな整数である、桁増しした識別子３８が生成されうる。

【００９４】

一実施形態において、桁増しした識別子３８は、整数型の識別子３０の右に追加の桁３７を追加した整数として生成される。例えば、整数型の識別子３０が８桁の整数であり、追加の桁３７が２桁の整数である場合、桁増しした識別子３８は１０桁の整数であり、桁増しした識別子３８の値は次式で表される。

【数３２】

$$X_{38} = X_{30} \times M^2 + X_{37} \qquad \cdots (\mathrm{XVI})$$

式中、X_{38}は桁増しした識別子３８の値、X_{30}は整数型の識別子３０の値、X_{37}は追加の桁３７の値であり、Ｍは記数法の底である。例えば、これらの整数が１０進法の整数であるときには、X_{38}の値はX_{30}を１００倍してX_{37}を加えた値でありうる。記数法は１０進法に限らず、２進法、８進法又は１６進法等を任意に用いうる。桁増しする桁の数は２桁に限らず適宜設定しうる。

【００９５】

追加の桁３７を含む桁増しした識別子３８に対する暗号化の諸段階は、図１に示した一実施形態のフロー図、又は図３に示した一実施形態の識別用途に依存して実施しうる暗号化の手順等と同様である。すなわち、図４に示す形態の暗号化の諸段階により生成される暗号化した整数は、コンピュータ・ネットワーク１３２又は勤務管理記憶装置１３４等を用いてコンピュータ処理可能なデータとして生成してもよく、不特定の他者１３６が知りうる音声又は出版物等の形態で生成してもよい。

【００９６】
一実施形態において、構成員の生年月日に含まれる数字等を識別子として利用する事業体等は、本発明に係る整数を暗号化し復号化する方法を用い、当該構成員の生年月日に含まれる数字等に追加して、任意の２桁の数字を追加の桁３７として組み合わせうる。これにより、生年月日が同一の構成員が複数存在しても、任意の２桁の数字が相互に異なれば、生成する暗号化された数字は互いに異なるので、追加の桁３７を用いることにより当該事業体等は暗号化した整数を用いて構成員を識別しうる。
【００９７】
このようにして、予め定めた桁数の追加の桁３７を追加することにより、本発明に係る暗号化手段１００の暗号化の諸段階に入力される整数は、特定の個人２０等が有する識別のための情報そのものではなくなる。桁を追加して得られる整数を暗号化することにより、本発明に係る整数の暗号化においては、特定の個人２０等の個人情報をさらに隠蔽した暗号化が可能になる。
【００９８】
［個人情報隠蔽手順のさらに別の形態］
図５に、本発明の一実施形態に係る、整数を暗号化する方法を用いる個人情報隠蔽手順のさらに別の例を示す。図３と共通する箇所は説明を省略する。
【００９９】
図５に示す個人情報隠蔽手順においては、本発明に係る暗号化手段１００が、乱数発生手段３９及びオフセット情報４０を含みうることを示す。
【０１００】
一実施形態において、本発明に係る暗号化手段１００は乱数発生手段３９を用いて乱数を発生させ、当該発生した乱数に基づいて、整数型の識別子３０を暗号化しうる。具体的には、図１を用いて前述したステップＳ３０に含まれる換字式暗号化の鍵Ｒの選択に、当該発生した乱数を用いることができる。具体的には、換字式暗号化の鍵Ｒの選択は、発生した乱数に対して直近の素数を選択してもよい。すなわち、重複無く素数を含む集合から、当該発生した乱数との差が最も小さい素数を選択してもよい。あるいは、換字式暗号化の鍵Ｒの選択は、重複無く素数を含む集合からそれぞれの要素（すなわち素数）を昇順又は降順に配列した数列を用意し、乱数の上限を当該集合の要素数として、発生した乱数を項番号とする要素（すなわち素数）を当該数列から選択してもよい。これらに限らず、乱数と素数の関連付けは適宜設計しうる。
【０１０１】
別の実施形態において、本発明に係る暗号化手段１００はオフセット情報４０を用いて整数型の識別子３０をオフセットした後に、図１を用いて示した暗号化の諸段階を実施しうる。すなわち、本発明に係る暗号化手段１００は、整数型の識別子３０に整数型の所定の定数を加算又は減算しうる。この加算又は減算される所定の定数は、元の整数への復号化の段階において減算又は加算されることにより、整数型の識別子３０が正しく復元されうる。オフセット情報４０は定数に限らず、本発明に係る暗号化手段１００が一つの整数型の識別子３０を受け付けて動作するごとに、毎回異なる値を選択して用いてもよい。この異なる値の選択において、上述の乱数発生手段３９を用いてもよい。
【０１０２】
また別の実施形態において、本発明に係る暗号化手段１００は乱数発生手段３９を用いて乱数を発生させ、当該発生した乱数に基づいて、図１に示したステップＳ１９０のループカウンタＬを選択してもよい。図２に示したステップＳ２９０のループカウンタＬは、図１に示したステップＳ１９０のループカウンタＬと同一の値でありうる。すなわち、ループカウンタＬは、所定の正の整数、前記所定の正の整数を暗号化した正の整数、及びランダムに発生した正の整数からなる群から選ばれうる。
ループカウンタＬは、暗号化の強度を確保するために、予め下限を設定してもよい。また、暗号化及び復号化の計算処理のための時間を短縮するために、予め上限を設定してもよい。従って、本発明に係る整数を暗号化し復号化する方法におけるループカウンタＬの

値は、予め設定された下限及び／又は上限の範囲に従って、所定の正の整数、前記所定の正の整数を暗号化した正の整数、及びランダムに発生した正の整数からなる群から選ばれうる。このように、べき剰余を用いる暗号化及び換字式暗号化のいずれとも独立した変数でありうるループカウンタＬを秘密とすることで、第三者の解読の手間はさらに膨大となりうる。

【０１０３】

さらに別の実施形態において、本発明に係る暗号化手段１００は、公開鍵暗号化技術における公開鍵に対して、オフセット情報４０を用いてオフセットした公開鍵を生成してもよい。具体的には、式（Ｉ）に含まれる変数Ｅを決定した後に、当該変数Ｅに整数型の所定の定数を加算又は減算して公開鍵としてもよい。従って、この整数型の所定の定数が加算又は減算されていることを知らない第三者が解読のために当該公開鍵を用いることは無駄な手順となる。従って、オフセット情報４０を公開鍵に適用することにより、暗号化された整数等の情報の秘匿性はさらに高められる。

【０１０４】

また別の実施形態において、本発明に係る暗号化手段１００は、上述の乱数発生手段３９及びオフセット情報４０の両者を用いて、整数型の識別子３０を暗号化してもよい。

【０１０５】

図５においては、識別用途Ａ（１２２）、識別用途Ｂ（１２４）及び識別用途Ｃ（１２６）等のそれぞれに対して暗号化の過程を一つの矢印として表しているが、図１を用いて前述したように、本発明に係る暗号化の方法においては、それぞれの識別用途ごとに、べき剰余を用いる暗号化及び換字式暗号化が所定の繰り返し回数だけ交互に重畳されうる。それぞれの識別用途ごとに生成した、暗号化した整数Ａ（４２）、暗号化した整数Ｂ（４４）又は暗号化した整数Ｃ（４６）は、乱数発生手段３９を用いて発生した乱数の情報、べき剰余を用いる暗号化の情報、及び換字式暗号化の情報の全てを正確に用いなければ、いずれも正しく復号化することができない。従って、本発明の実施の形態における個人情報隠蔽手順においては、正確な復号化のための情報の種類をより多く必要とすることで、周知の公開鍵暗号化技術等に比較してさらに秘匿性を高めることが可能になる。

【０１０６】

［復号化の手順の例］

図６に、本発明の一実施形態に係る、暗号化した整数の復号化手順の例を示す。図６においては、説明の簡潔化のためにコンピュータ処理可能な数値に関し、図３を示して説明した暗号化手段１００が生成した暗号化した整数Ａ（４２）及び／又は暗号化した整数Ｂ（４４）に対する復号化を説明するが、通話又は文書等の形態で伝達しうる暗号化した整数の復号化についても同様である。図３又は図４と共通する箇所は説明を省略する。

【０１０７】

図６は、本発明に係る復号化手段１１０が、暗号化した整数Ａ’（５２）及び／又は暗号化した整数Ｂ’（５４）を受け付け、整数型の復号化した識別子４１を生成することを示す。ここで、暗号化した整数Ａ’（５２）は、整数型の識別子３０に対して暗号化手段１００が暗号化計算Ａ（７２）を用いて生成した暗号化した整数Ａ（４２）が、情報伝達経路Ａ（８２）を介してコンピュータ・ネットワーク１３２等に伝達された後に、さらに情報伝達経路Ａ’（１０２）を介して本発明に係る復号化手段１１０に伝達したものでありうる。従って、整数型の数値としては、暗号化した整数Ａ’（５２）は対応する暗号化した整数Ａ（４２）と同一でありうる。

同様に、暗号化した整数Ｂ’（５４）は暗号化した整数Ｂ（４４）と同一でありうる。

【０１０８】

本発明に係る復号化手段１１０は、暗号化した整数Ａ’（５２）及び暗号化した整数Ｂ’（５４）に対して、図１に示したステップＳ２００からステップＳ２２０の諸段階を実施し、整数型の復号化した識別子４１を生成しうる。

暗号化した整数Ａ’（５２）は、暗号化手段１００による暗号化計算Ａ（７２）において識別用途Ａ（１２２）の固有情報（６２）を用いて生成した暗号化した整数Ａ（４２）

でありうる。当該固有情報（６２）は、前述の数式（ＶＩＩＩ）に含まれるＮ又はＥの値、及びＫの値でありうるので、例えば、暗号化計算Ａ（７２）において用いられたＥの値及びＫの値を固有情報（９２）として復号化計算Ａ（１１２）に用いうる。

同様に、暗号化計算Ｂ（７４）において用いられたＥの値及びＫの値を固有情報（９４）として復号化計算Ｂ（１１４）に用いうる。

固有情報（９２）及び／又は固有情報（９４）は、予め復号化手段１１０が記憶してもよく、予め定められた手順に従って暗号化手段１００又は復号化手段１１０の一方又は両方が生成してもよく、適宜設定しうる。

【０１０９】

図６は、情報伝達経路Ａ（８２）、情報伝達経路Ｂ（８４）、情報伝達経路Ａ’（１０２）及び情報伝達経路Ｂ’（１０４）としてコンピュータ処理可能な数値を伝達しうるネットワーク等の情報伝達経路を示すが、これらに限らず、音声又は文書等を含む任意の伝達経路又は伝達手段を介して、暗号化した整数を暗号化手段１００から復号化手段１１０に向かって伝達しうる。

本発明に係る整数を暗号化し復号化する方法には、これらの伝達経路又は伝達手段を介して伝達される整数が暗号化されていること、桁あふれを発生する条件での暗号化に用いた特定の数値で復号化する本発明の方法によらなければ元の整数を復号化することはできないという特徴がある。従って、本発明においては、伝達経路又は伝達手段等にアクセスする可能性のある第三者に対して個人情報を隠蔽し、所定の固有情報及び所定の暗号化及び所定の復号化の方法を用いる本発明の実施手段等のみが当該個人情報を正確に復号化することが可能になる。

【０１１０】

図６には、暗号化手段１００及び復号化手段１１０のそれぞれを別個に示したが、これに限らず、暗号化手段１００及び復号化手段１１０を一体の装置としてもよい。暗号化した整数を伝達する伝達経路又は伝達手段等の形態は、コンピュータ・ネットワークでもよく、一般公衆回線の電話を含む通話、ファクシミリ、電子メール等の形態でもよく、任意に設定しうる。それぞれの伝達経路又は伝達手段に依存して、一つの整数型の識別子３０から独立して別個に暗号化した整数を生成してもよく、さらに図４に示した追加の桁３７、図５に示した乱数発生手段３９、オフセット情報４０、又はこれらの組み合わせを適宜用いて整数型の識別子３０を加工した後に暗号化してもよい。このようにして、本発明に係る整数を暗号化し復号化する方法においては、構成員識別子等の一つの識別子から、当該識別子を用いる各種の情報伝達手段ごとに、個人情報を隠蔽した整数を識別子に替えて提供しうる。暗号化又は復号化の諸段階はコンピュータ装置等を用いて自動的に実施しうるので、本発明に係る方法のユーザはこれらの手順を特に意識することなく、自己の個人情報を隠蔽した整数を自己の識別子に替えて用いうる。

【０１１１】

図６には、整数型の識別子３０が暗号化され、事業体のコンピュータ・ネットワーク１３２又は事業体の勤務管理記憶装置１３４等に向けて送信された後に、上述の用に復号化されうることを示すが、送受信の主体を入れ替えても、本発明に係る復号化手段１１０を用いることができる。すなわち、事業体のコンピュータ・ネットワーク１３２に接続されたサーバ装置（図示せず）等が記憶した整数型の識別子３０を本発明に係る暗号化手段１００で暗号化して構成員等に送信し、構成員等は上述の手順に従って、本発明に係る復号化手段１１０を用いて整数型の識別子３０を復号化してもよい。

【実施例】

【０１１２】

［実施例１：ワークシートの内部関数を用いて整数を暗号化する例］

図７に、本発明の一実施形態に係る、暗号化の諸段階をスプレッドシート形式の計算アプリケーション・パッケージを用いて実装する例を示す。スプレッドシート形式の計算アプリケーション・パッケージとしてはマイクロソフト社製エクセル２００７等を用いうるが、これに限らず、整数のべき乗及び剰余計算を実施可能なパッケージ・ソフトウェア等

を任意に用いうる。
図７に示す整数の暗号化計算ワークシート２００は、複数の行及び列の形態に配列されるセルを含む、スプレッドシート形式の計算アプリケーションのデータでありうる。整数の暗号化計算ワークシート２００に含まれる個々のセルは、１組の行番号及び列番号を用いて特定しうる。
【０１１３】
整数の暗号化計算ワークシート２００に含まれる、２行１列から１５行１列の領域、及び２行２列から１５行（２ｎ＋１）列の領域は、図１に示したステップＳ１００からステップＳ１９５における暗号化の諸段階に係る計算のために用いられうる。
具体的には、２行１列から１５行１列の領域は、図１に示したステップＳ１００における変数領域を確保するために用いられる。２行２列から１５行（２ｎ＋１）列の領域は、図１に示したステップＳ１０及びステップＳ３０の繰り返しのために用いられる。図７には、変数Ａ、Ｂ、Ｄ、Ｋはそれぞれ同じ値が繰り返して用いられ、変数Ｅ、Ｆ、Ｔはループカウンタに依存して繰り返しの各回において変化する例を示す。
【０１１４】
例示的実施形態において、２行１列のセルは暗号化の入力Ｘｉを記憶するために用いうる。１列の他のセルには、べき剰余を用いる復号化における素数Ａ及びＢ、（Ａ－１）と（Ｂ－１）との積Ｄ及び最小公倍数Ｋ、公開鍵及び秘密鍵の対でありうる整数Ｅｉ及びＦｉ、換字式暗号化鍵Ｒｉ、オフセットＴｉ、ループカウンタＬ等が適宜定義され得る。
すなわち、３行１列のセル及び４行２列のセルは、２個の素数Ａ及びＢを記憶するために用いうる。また、Ａ及びＢの積が入力Ｘｉを超えることの判定を、例えば3行２列のセルを用いて表示してもよい。このＡ及びＢの積は、前述の数式（ＶＩＩＩ）におけるＮであり、Ｎは本発明に係る整数の暗号化に含まれる剰余計算の底でありうる。
７行１列のセルは、（Ａ－１）及び（Ｂ－１）の積であるＤ値を記憶するために用いうる。８行１列のセルは、（Ａ－１）と（Ｂ－１）の最小公倍数であるＫ値を記憶するために用いうる。９行１列のセルは、Ｄ又はＫと素である整数Ｅｉを記憶するために用いうる。この整数Ｅｉは、公開鍵暗号化技術における公開鍵として用いうる。１１行１列のセルは、前述の数式（ＸＶＩ）を成立する整数Ｆを記憶するために用いうる。この整数Ｆｉは、公開鍵暗号化技術における秘密鍵として用いうる。１３行１列のセルは、換字式暗号化の鍵Ｒｉを、１４行１列のセルはオフセットＴｉを、１５行１列はループカウンタＬを記憶するために用いうる。
【０１１５】
１０行の各セルは、整数Ｅｉによるべき乗がワークシート内蔵の整数演算においてオーバーフローを発生しているか否かを表示するために用いうる。例えば、当該オーバーフローが発生することは、整数Ｅｉによるべき乗の値がスプレッドシート形式の計算アプリケーション・パッケージにおいて取り扱い可能な範囲を超えていることを表す「エラー」等の文字等により表されてもよく、又は当該エラーに対応して論理値の偽を表す数値等を表示してもよい。同様に、１２行の各セルは、整数Ｆｉによるべき乗がワークシート内蔵の整数演算においてオーバーフローを発生しているか否かを表示するために用いうる。これらの整数Ｅｉによるべき乗又は整数Ｆｉによるべき乗がオーバーフローを発生することを条件として、本発明に係るべき剰余を用いる暗号化の方法は、式（ＶＩＩ）に示した展開形を用いて変換前の整数を展開し、正確なべき剰余を得ることができる。具体的には、１行２列の元の整数Ｘｉに対して、１４行２列のオフセットＴ１を用いてオフセットした整数から、暗号化した整数として２行２列に整数Ｙ１を得ることができる。このときに、当該べき剰余を用いる暗号化から生じる公開鍵Ｅ１及び秘密鍵Ｆ１が、それぞれ９行２列、１１行２列に記憶される。
【０１１６】
なお、添え字ｉを伴う変数は配列でもよい。すなわち、１個のセルに割り当てられるＥｉ、Ｆｉ、Ｒｉ及びＴｉのそれぞれは、｛Ｅ１，Ｅ２，…，Ｅｎ｝，｛Ｆ１，Ｆ２，…，Ｆｎ｝，｛Ｒ１，Ｒ２，…，Ｒｎ｝，｛Ｔ１，Ｔ２，…，Ｔｎ｝等の配列又は配列の形式

を用いる数列（適宜、漸化式又は任意の関数により各項を定義してもよい）でもよく、行ごとにこれらの配列に含まれる個々の整数を取り出して用いてもよい。

【０１１７】

さらなる例示的実施形態において、２列は、べき剰余を用いる暗号化のために用いられる。図５においては、２行２列には、べき剰余を用いる暗号化を１回実施して得られる整数Ｙ１が記憶される。３列は、換字式暗号化のために用いられ、図５においては、２行３列には、Ｙ１から換字式暗号化により生じる、変換された整数Ｚ１が記憶される。

他の２列のセルには、暗号化の諸段階から生じる変数の値が適宜記憶される。例えば、９行２列には公開鍵Ｅ１、１１行２列には秘密鍵Ｆ１、１４行２列にはオフセットＴ１がそれぞれ記憶される。同様に、他の３列のセルに関しては、１３行３列には換字式暗号化の鍵Ｒ１、１５行３列には１回デクリメントされたループカウンタ（Ｌ－１）がそれぞれ記憶される。

このようにして、入力Ｘｉから、２列にはべき剰余を用いる暗号化における変換後の整数Ｙ１、他の変数Ｅ１、Ｆ１、及びＴ１が記憶され、３列には整数Ｙ１から変換される整数Ｚ１、他の変数Ｒ１、及びデクリメントされたループカウンタ（Ｌ－１）が記憶される。

【０１１８】

なお、一つのセルに配列等を定義して複数の定数、変数又は計算式を任意に含みうることは当技術分野において公知である。すなわち、２行１列のセルは１個の整数Ｘｉを記憶してもよく、配列の形式を用いて数列｛Ｘ１，Ｘ２，Ｘ３，…，Ｘｋ｝を記憶してもよい。ここに、Ｘｋは、べき剰余を用いる暗号化における鍵の絶対値に依存して定義される、暗号化可能な整数の個数であり、この数列に含まれる整数の個数は最小公倍数Ｋと同じ値でもよく、当該個数はＫ－１，Ｋ－２，Ｋ－３等でもよく任意に設定しうる。数列｛Ｘ１，Ｘ２，Ｘ３，…，Ｘｋ｝の初項Ｘ１は０でもよく、１でもよく、２以上の整数でもよい。例えば、初項の値を整数２として、数列に含まれる整数の個数をＫ－１個とする場合は、全体としてこの数列にはＫ－２個の整数が含まれうる。本発明に係る整数を暗号化する方法は、このようなＫ－２個の整数のそれぞれを別個に暗号化し、暗号化した数列を得ることができるが、これに限定せずに、暗号化した数列に含まれる整数の個数は適宜設計しうる。従って、本発明のユーザは、予め計算された暗号化した数列から適宜抽出して暗号化した整数を用いることも可能である。

【０１１９】

次いで、本発明に係る整数を暗号化する方法は、換字式暗号化を用いて、２行２列に記憶された整数Ｙ１を、２行３列の整数Ｚ１に変換する。この変換は、換字式暗号化の鍵として１３行３列のＲ１を用いうる。

換字式暗号化により整数Ｚ１が得られた後に、本発明に係る整数を暗号化する方法は、１５行１列のループカウンタＬをデクリメントし、１５行３列に当該デクリメントした値である（Ｌ－１）を記憶する。当該デクリメントした値がゼロ以下である場合は、暗号化の諸段階を終了させる。当該デクリメントしたループカウンタの値がゼロより大きければ、２行３列のＺ１の値を上述の２行１列のＸｉの値のように取り扱い、べき剰余を用いる暗号化の諸段階及び換字式暗号化の諸段階を繰り返し、２行５列にＺ２として暗号化した整数を得られる。

【０１２０】

このようにして、本発明に係る整数を暗号化する方法は、べき剰余を用いる暗号化及び換字式暗号化の組み合わせを繰り返し実施し、ループカウンタがゼロ以下となることを条件として、２行（２ｎ＋１）列に整数Ｚｎとして暗号化した整数が得られる。

【０１２１】

［実施例２：ワークシートの内部関数を用いて整数を復号化する例］

図８に、本発明の一実施形態に係る、復号化の諸段階をスプレッドシート形式の計算アプリケーション・パッケージを用いて実装する例を示す。図８に示す整数の復号化計算ワークシート２２０は、複数の行及び列の形態に配列されるセルを含む、スプレッドシート

形式の計算アプリケーションのデータでありうる。整数の復号化計算ワークシート２２０に含まれる個々のセルは、１組の行番号及び列番号を用いて特定しうる。

【０１２２】

整数の復号化計算ワークシート２２０に含まれる、２行１列から１５行１列の領域、及び２行２列から１５行（２ｎ＋１）列の領域は、図２に示したステップＳ２００からステップＳ２９５における暗号化の諸段階に係る計算のために用いられうる。

具体的には、２行１列から１５行１列の領域は、図１に示したステップＳ２００における変数領域の確保及びループカウンタＬの初期化のために用いられる。２行２列から１５行（２ｎ＋１）列の領域は、図２に示したステップＳ４０及びステップＳ２０の繰り返しのために用いられる。

【０１２３】

例示的実施形態において、２行１列のセルは復号化の入力Ｚｉを記憶するために用いうる。１列の他のセルには、前述の図７を用いて示したべき剰余を用いる復号化における変数と同一である。すなわち、復号化の入力Ｚｉに対応する暗号化の過程において、すでに用いられた値をそれぞれの変数Ａ，Ｂ，Ｄ，Ｋ，Ｅｉ、Ｆｉ、Ｒｉ，Ｔｉに用いることができる。従って、復号化においては、対応する暗号化の変数の値を再利用し、入力Ｚｉに対応するループカウンタＬを初期化してもよい。

【０１２４】

本発明に係る整数の復号化においては、対応する暗号化と逆の手順により、暗号化された整数から元の整数を復号化する。例えば、べき剰余及び換字式の暗号化がこの順番の組み合わせで繰り返された場合、対応する復号化は、換字式及びべき剰余の復号化をこの順番で同じ回数だけ繰り返す。

【０１２５】

まず、換字式復号化を用いて、入力Ｚｉを変換する手順を説明する。換字式復号化においては、２行１列に記憶された整数Ｚｎを、２行２列の整数Ｙｎに変換する。この変換のための換字式暗号化の鍵は１３行２列のＲｎであり、当該Ｒｎは対応する暗号化に用いられた、図７の整数の暗号化計算ワークシート２００における１３行（２ｎ＋１）列のＲｎと同一でありうる。

【０１２６】

次いで、本発明に係る整数の復号化において、２行２列のＹｎに対してべき剰余を用いる復号化を実施し、さらにオフセットを消去して、２行３列に整数Ｘｎ－１が得られる。べき剰余の指数には１１行３列のＦｎが用いられ、オフセットの値としては１４行３列のＴｎが用いられる。

べき剰余を用いる復号化により整数Ｘｎ－１が得られた後に、本発明に係る整数を復号化する方法は、１５行１列のループカウンタＬをデクリメントし、１５行３列に当該デクリメントした値である（Ｌ－１）を記憶する。当該デクリメントした値がゼロ以下である場合は、復号化の諸段階を終了させる。当該デクリメントしたループカウンタの値がゼロより大きければ、２行３列のＸｎ－１の値を上述の２行１列のＺｉの値のように取り扱い、換字式復号化の諸段階及びべき剰余を用いる復号化の諸段階を繰り返し、２行５列にＸｎ－２として復号化した整数を得られる。

【０１２７】

１０行及び１２行の各セルは、暗号化と同様に、整数Ｅｉ及び整数Ｆｉによるべき乗がワークシート内蔵の整数演算においてオーバーフローを発生しているか否かを表示するために用いうる。これらの整数Ｅｉによるべき乗又は整数Ｆｉによるべき乗がオーバーフローを発生することを条件として、本発明に係るべき剰余を用いる復号化の方法は、式（ＶＩＩ）に示した展開形を用いて変換前の整数を展開し、正確なべき剰余を得ることができる。

【０１２８】

さらなる例示的実施形態において、２列は、べき剰余を用いる暗号化のために用いられる。図５においては、２行２列には、べき剰余を用いる暗号化を１回実施して得られる整

数Ｙ１が記憶される。３列は、換字式暗号化のために用いられ、図５においては、２行３列には、Ｙ１から換字式暗号化により生じる、変換された整数Ｚ１が記憶される。
他の２列のセルには、暗号化の諸段階から生じる変数の値が適宜記憶される。例えば、９行２列には公開鍵Ｅ１、１１行２列には秘密鍵Ｆ１、１４行２列にはオフセットＴ１がそれぞれ記憶される。同様に、他の３列のセルに関しては、１３行３列には換字式暗号化の鍵Ｒ１、１５行３列には１回デクリメントされたループカウンタ（Ｌ－１）がそれぞれ記憶される。
このようにして、入力Ｘｉから、２列にはべき剰余を用いる暗号化における変換後の整数Ｙ１、他の変数Ｅ１、Ｆ１、及びＴ１が記憶され、３列には整数Ｙ１から変換される整数Ｚ１、他の変数Ｒ１、及びデクリメントされたループカウンタ（Ｌ－１）が記憶される。

【０１２９】
このようにして、本発明に係る整数を復号化する方法は、換字式復号化及びべき剰余を用いる復号化の組み合わせを繰り返し実施し、ループカウンタがゼロ以下となることを条件として、２行（２ｎ＋１）列に整数Ｘ１として復号化した整数が得られる。これらの復号化の諸段階が、対応する暗号化の諸段階の逆順で実施されることにより、図８に示す整数の復号化計算ワークシート２２０の２行（２ｎ＋１）列に得られる整数Ｘ１は、図７に示した整数の暗号化計算ワークシート２００の２行１列に入力された元の整数Ｘｉと等しくなる。

【０１３０】
本発明に係る整数の暗号化及び復号化の方法の諸段階を用いることにより、べき剰余を用いる暗号化及び復号化の諸段階のいずれにおいても、計算過程において桁あふれを発生することにより、本発明の方法を用いない計算手段等においては、正しい暗号化も復号化も実施することはできない。さらに、べき剰余に加えて換字式暗号化及び復号化を重畳することにより、本発明の方法においては情報の秘匿性を飛躍的に高めることが可能になる。これにより、本発明に係る整数の暗号化及び復号化の方法及び該方法の実施手段等は、個人情報等と関連する整数の形態の情報に対して高い秘匿性を付与することが可能になる。

【０１３１】
［解読のための所要時間］
本発明に係る整数を暗号化する方法を用いて生成した整数に対して、解読の可能性を総当たりにより探索する場合の所要時間を例示する。これは、いわゆるブルート・フォース・アタック（総当たり攻撃）を用いて秘密情報を解読するための計算時間でありうる。
コンピュータの計算能力が毎秒１ペタフロップス、すなわち１秒間に１０の１５乗命令数であると仮定すると、当該コンピュータは１年間に約１０の２２乗命令数を実行することが可能である。
本発明に係る整数を暗号化する方法において、元の整数が６桁の１０進数であり、べき剰余を用いる暗号化及び換字式暗号化が連続して実行されるとする。暗号化において、この連続して実行される暗号化が５回繰り返される場合、当該５回繰り返された暗号化に含まれる独立した五重の換字式暗号化の組み合わせの総数は１０の３０乗（すなわち、１０の６乗の５乗）であり、前述のコンピュータによる総当たり計算の所要時間は約１０の８乗年（すなわち約１億年）と算出できる。本発明に係る暗号化の方法においては、さらに五重の独立したべき剰余を用いる暗号化が実施され、これらの暗号化に用いられる鍵は乱数発生手段によりランダムに選択されうるので、総当たりによる解読の所要時間は１億年をはるかに超える天文学的数字の時間でありうる。
このように、本発明においては、べき剰余を用いる暗号化及び換字式暗号化を連続して複数回繰り返し実行することにより、元の整数から極めて秘匿性の高い暗号化した整数を生成することが可能である。本発明においては、第三者による解読の手間を膨大化することにより、守秘情報を参照するための識別情報等を高い秘匿性で暗号化し復号化することができる。

【０１３２】
以上、本発明の実施形態を用いて説明したが、本発明の技術的範囲は上記実施形態に記載の範囲には限定されない。上記実施形態に、多様な変更又は改良を加えることができる。そのような変更又は改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

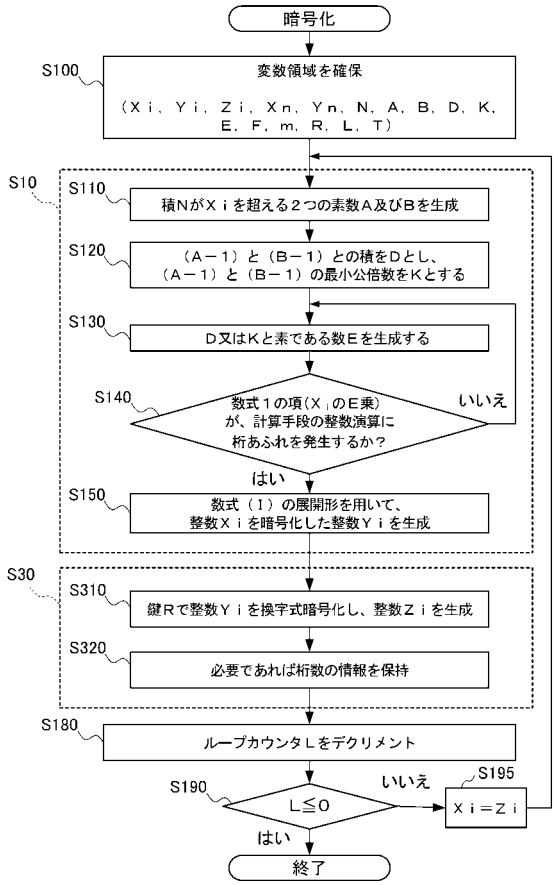
【図面の簡単な説明】

【０１３３】
【図１】本発明の一実施形態に係る、整数を暗号化する方法のフロー図である。
【図２】本発明の一実施形態に係る、暗号化した整数を復号化する方法のフロー図である。
【図３】本発明の一実施形態に係る、整数を暗号化する方法を用いる個人情報隠蔽手順の例を示す図である。
【図４】本発明の一実施形態に係る、整数を暗号化する方法を用いる個人情報隠蔽手順の別の例を示す図である。
【図５】本発明の一実施形態に係る、整数を暗号化する方法を用いる個人情報隠蔽手順のさらに別の例を示す図である。
【図６】本発明の一実施形態に係る、暗号化した整数の復号化手順の例を示す図である。
【図７】本発明の一実施形態に係る、暗号化の方法の諸段階をスプレッドシート形式の計算アプリケーション・パッケージを用いて実装する例を示す図である。
【図８】本発明の一実施形態に係る、復号化の方法の諸段階をスプレッドシート形式の計算アプリケーション・パッケージに実装して計算する実施例を示す図である。

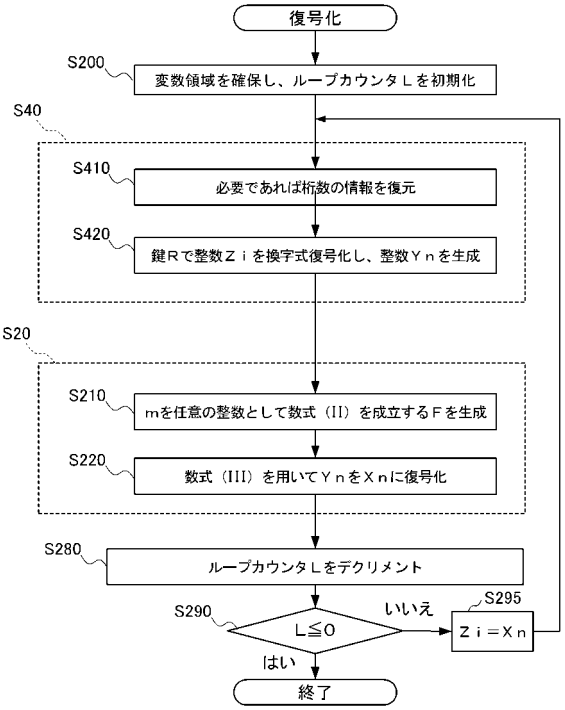
【符号の説明】

【０１３４】
２０　特定の個人
３０　整数型の識別子
３７　追加の桁
３９　乱数発生手段
４０　オフセット情報
４１　整数型の復号化した識別子
４２、４４、４６、５２、５４　暗号化した整数
６２、６４、６６、９２、９４　固有情報
７２、７４、７６　暗号化計算
８２、８４、１０２、１０４　情報伝達経路
１００　暗号化手段
１１０　復号化手段
１１２、１１４　復号化計算
１２２、１２４、１２６　識別用途

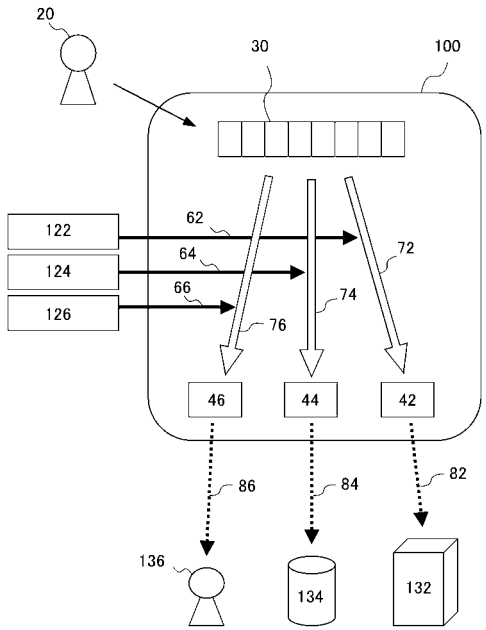
【図１】


暗号化
S100
変数領域を確保
（Ｘｉ，Ｙｉ，Ｚｉ，Ｘｎ，Ｙｎ，Ｎ，Ａ，Ｂ，Ｄ，Ｋ，Ｅ，Ｆ，ｍ，Ｒ，Ｌ，Ｔ）
S10
S110
積ＮがＸｉを超える２つの素数Ａ及びＢを生成
S120
（Ａ－１）と（Ｂ－１）との積をＤとし、（Ａ－１）と（Ｂ－１）の最小公倍数をＫとする
S130
Ｄ又はＫと素である数Ｅを生成する
S140
数式１の項（Ｘｉのｅ乗）が、計算手段の整数演算に桁あふれを発生するか？
いいえ
はい
S150
数式（Ｉ）の展開形を用いて、整数Ｘｉを暗号化した整数Ｙｉを生成
S30
S310
鍵Ｒで整数Ｙｉを換字式暗号化し、整数Ｚｉを生成
S320
必要であれば桁数の情報を保持
S180
ループカウンタＬをデクリメント
S190
Ｌ≦０
いいえ
S195
Ｘｉ＝Ｚｉ
はい
終了

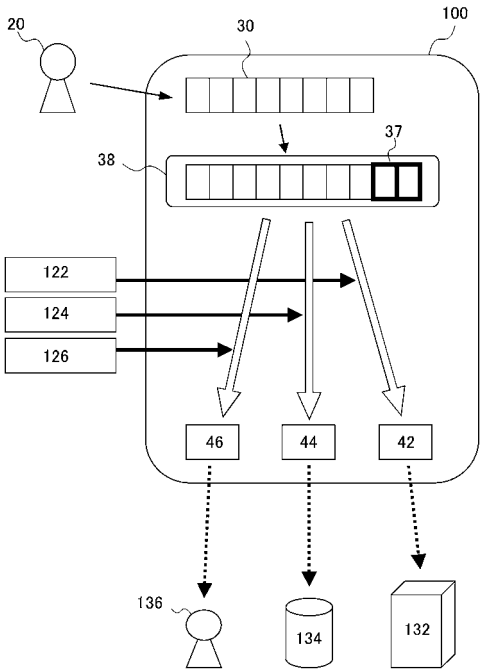
【図２】


復号化
S200
変数領域を確保し、ループカウンタＬを初期化
S40
S410
必要であれば桁数の情報を復元
S420
鍵Ｒで整数Ｚｉを換字式復号化し、整数Ｙｎを生成
S20
S210
ｍを任意の整数として数式（II）を成立するＦを生成
S220
数式（III）を用いてＹｎをＸｎに復号化
S280
ループカウンタＬをデクリメント
S290
Ｌ≦０
いいえ
S295
Ｚｉ＝Ｘｎ
はい
終了

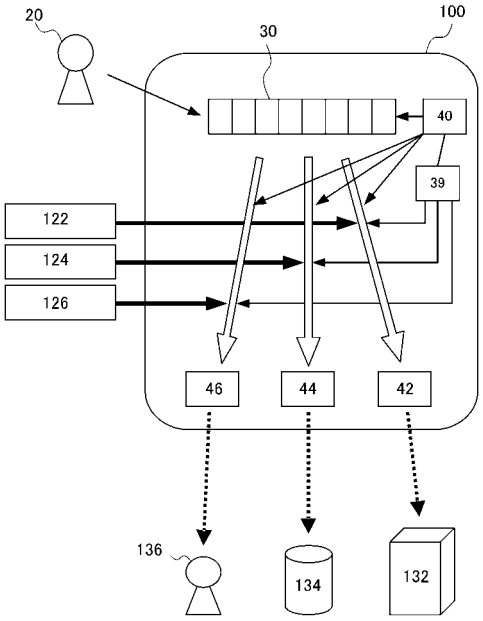
【図３】


20
30
100
122
124
126
62
64
66
72
74
76
46
44
42
86
84
82
136
134
132

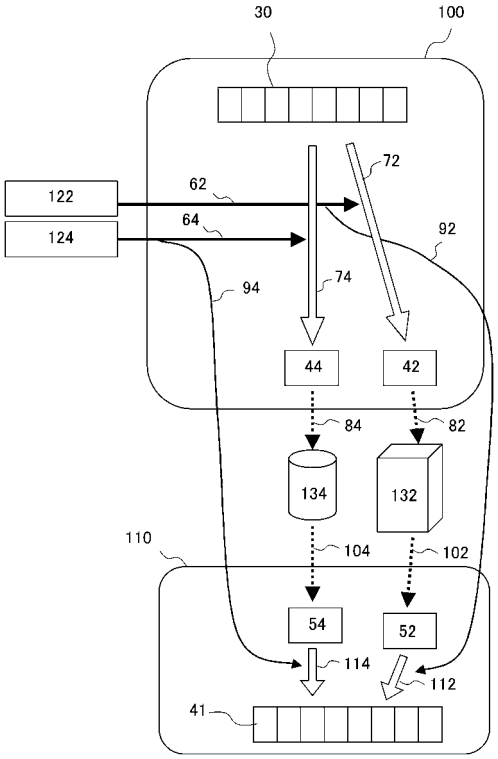
【図４】


20
30
100
37
38
122
124
126
46
44
42
136
134
132

【図５】



【図６】



【図７】

200 整数の暗号化計算ワークシート

	1列	2列	3列	4列	5列	…	2n列	(2n+1)列
1行		べき剰余 暗号化－1	換字式 暗号化－1	べき剰余 暗号化－2	換字式 暗号化－2	…	べき剰余 暗号化－n	換字式 暗号化－n
2行	入力Xi	Y_1	Z_1	Y_2	Z_2	…	Y_n	Z_n
3行	素数A					…		
4行	素数B	N				…		
5行	A－1					…		
6行	B－1					…		
7行	積D					…		
8行	最小公倍数K							
9行	公開鍵Ei	E_1		E_2		…	E_n	
10行	オーバーフロー判定(E)							
11行	秘密鍵Fi	F_1		F_2		…	F_n	
12行	オーバーフロー判定(F)							
13行	換字式暗号化鍵Ri		R_1		R_2	…		R_n
14行	オフセットTi	T_1		T_2		…	T_n	
15行	ループカウンタL		L－1		L－2			L－n

【図８】

220 整数の復号化計算ワークシート

	1列	2列	3列	4列	5列	…	2n列	(2n+1)列
1行		換字式 復号化－1	べき剰余 復号化－1	換字式 復号化－2	べき剰余 復号化－2	…	べき剰余 復号化－n	換字式 復号化－n
2行	入力Zi	Y_n	X_{n-1}	Y_{n-1}	X_{n-2}	…	Y_1	X_1
3行	素数A					…		
4行	素数B	N				…		
5行	A－1					…		
6行	B－1					…		
7行	積D					…		
8行	最小公倍数K							
9行	公開鍵Ei		E_n		E_{n-1}	…		E_1
10行	オーバーフロー判定(E)							
11行	秘密鍵Fi		F_n		F_{n-1}	…		F_1
12行	オーバーフロー判定(F)							
13行	換字式復号化鍵Ri	R_n		R_{n-1}		…	R_1	
14行	オフセットTi		T_n		T_{n-1}	…		T_1
15行	ループカウンタL		L－1		L－2			L－n