(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3816337号
(P3816337)
(45)発行日　平成18年8月30日(2006.8.30)　(24)登録日　平成18年6月16日(2006.6.16)

(51)Int.Cl.　F I
H04L 9/16 (2006.01)　H04L 9/00 643
H04Q 7/38 (2006.01)　H04B 7/26 109R

請求項の数 18　(全 10 頁)

(21)出願番号　特願2000-512309(P2000-512309)
(86)(22)出願日　平成10年9月15日(1998.9.15)
(65)公表番号　特表2001-517020(P2001-517020A)
(43)公表日　平成13年10月2日(2001.10.2)
(86)国際出願番号　PCT/FI1998/000721
(87)国際公開番号　WO1999/014888
(87)国際公開日　平成11年3月25日(1999.3.25)
審査請求日　平成14年2月7日(2002.2.7)
(31)優先権主張番号　973694
(32)優先日　平成9年9月15日(1997.9.15)
(33)優先権主張国　フィンランド(FI)

前置審査

(73)特許権者　398012616
ノキア　コーポレイション
フィンランド　エフイーエンー０２１５０
エスプー　ケイララーデンティエ　４
(74)代理人　100059959
弁理士　中村　稔
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100065189
弁理士　宍戸　嘉一
(74)代理人　100074228
弁理士　今城　俊夫

最終頁に続く

(54)【発明の名称】テレコミュニケーションネットワークの送信に対するセキュリティ方法

(57)【特許請求の範囲】
【請求項１】
テレコミュニケーションネットワークにおける通信当事者端末間の送信に対する接続セキュリティを与える方法において、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータを交換し、
メッセージにシーケンス番号で番号付けし、
通信当事者端末間でメッセージを送信し、
メッセージと共に各シーケンス番号を送信し、
通信当事者間でメッセージの暗号化のためのセキュリティパラメータを再計算するための間隔を決定するためのメッセージの数につき通信当事者端末間でネゴシエーションし合意に達し、
通信当事者端末によりメッセージの暗号化のためのセキュリティパラメータの再計算の間隔を監視し、
合意された数のメッセージが送信された後に通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータを再計算し、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータの再計算のための入力として最新のシーケンス番号を使用し、
通信当事者端末間でメッセージの暗号化のための最新の再計算されたセキュリティパラメータに基づきメッセージに対する接続セキュリティを与える、
という段階を含むことを特徴とする方法。

【請求項２】
最新の再計算されたセキュリティパラメータに基づきメッセージに対する接続セキュリティを与える上記段階は、最新の再計算されたセキュリティパラメータに基づいてメッセージを暗号化することを含む請求項１に記載の方法。
【請求項３】
最新の再計算されたセキュリティパラメータに基づきメッセージに対する接続セキュリティを与える上記段階は、最新の再計算されたセキュリティパラメータに基づいてメッセージを認証しそしてメッセージの完全性を与えることを含む請求項１又は２に記載の方法。
【請求項４】
メッセージを認証しそしてメッセージの完全性を与える上記段階は、メッセージ認証コードＭＡＣで行なう請求項３に記載の方法。
【請求項５】
上記方法は、更に、セキュリティパラメータを再計算するための間隔についてハンドシェーキング中に通信当事者端末間で合意に達するという段階を含む請求項１から４のうちのいずれか１項に記載の方法。
【請求項６】
テレコミュニケーションネットワークにおける通信当事者端末間の送信に対する接続セキュリティを与えるシステムにおいて、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータを交換するための手段と、
メッセージにシーケンス番号で番号付けするための手段と、
通信当事者端末間でメッセージを送信し且つメッセージと共に各シーケンス番号を送信するための手段と、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータを再計算するための間隔を決定するためのメッセージの数につき通信当事者端末間でネゴシエーションし合意に達するための手段と、
通信当事者端末により通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータパラメータの再計算の間隔を監視するための手段と、
合意された数のメッセージが送信された後に通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータを再計算するための手段と、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータの再計算のための入力として最新のシーケンス番号を使用するための手段と、
通信当事者端末間でメッセージの暗号化のための最新の再計算されたセキュリティパラメータに基づきメッセージに対する接続セキュリティを与えるための手段と、
を備えることを特徴とするシステム。
【請求項７】
移動ステーションにおいて、
少なくとも１つの通信当事者端末と通信当事者端末間でのメッセージの暗号化のためのセキュリティパラメータを交換するための手段と、
メッセージにシーケンス番号で番号付けするための手段と、
メッセージを送信し且つメッセージと共に各シーケンス番号を送信するための手段と、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータを再計算するための間隔を決定するためのメッセージの数につき上記少なくとも１つの通信当事者端末とネゴシエーションし合意に達するための手段と、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータの再計算の間隔を監視するための手段と、
合意された数のメッセージが送信された後に通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータを再計算するための手段と、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータの再計算のた

めの入力として最新のシーケンス番号を使用するための手段と、
通信当事者端末間でメッセージの暗号化のための最新の再計算されたセキュリティパラメータに基づきメッセージに対する接続セキュリティを与えるための手段と、
を備えることを特徴とする移動ステーション。
【請求項８】
最新の再計算されたセキュリティパラメータに基づいてメッセージを暗号化するための手段を更に備える請求項７に記載の移動ステーション。
【請求項９】
最新の再計算されたセキュリティパラメータに基づいてメッセージを認証しそしてメッセージの完全性を与えるための手段を更に備える請求項７又は８に記載の移動ステーション。
【請求項１０】
メッセージが認証され、そしてメッセージの完全性には、メッセージ認証コードが与えられる請求項９に記載の移動ステーション。
【請求項１１】
セキュリティパラメータを再計算するための間隔についてハンドシェーキング中に上記少なくとも１つの通信当事者端末とネゴシエーションし合意に達するための手段を更に備える請求項７から１０のうちのいずれか１項に記載の移動ステーション。
【請求項１２】
サーバにおいて、
少なくとも１つの通信当事者端末と通信当事者端末間でのメッセージの暗号化のためのセキュリティパラメータを交換するための手段と、
メッセージにシーケンス番号で番号付けするための手段と、
メッセージを送信し且つメッセージと共に各シーケンス番号を送信するための手段と、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータを再計算するための間隔を決定するためのメッセージの数につき上記少なくとも１つの通信当事者端末とネゴシエーションし合意に達するための手段と、
通信当事者端末間でメッセージの暗号化のための再計算の間隔を監視するための手段と、
合意された数のメッセージが送信された後に通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータを再計算するための手段と、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータの再計算のための入力として最新のシーケンス番号を使用するための手段と、
通信当事者端末間でメッセージの暗号化のための最新の再計算されたセキュリティパラメータに基づきメッセージに対する接続セキュリティを与えるための手段と、
を備えることを特徴とするサーバ。
【請求項１３】
最新の再計算されたセキュリティパラメータに基づいてメッセージを暗号化するための手段を更に備える請求項１２に記載のサーバ。
【請求項１４】
最新の再計算されたセキュリティパラメータに基づいてメッセージを認証しそしてメッセージの完全性を与えるための手段を更に備える請求項１２又は１３に記載のサーバ。
【請求項１５】
メッセージが認証され、そしてメッセージの完全性には、メッセージ認証コードが与えられる請求項１４に記載のサーバ。
【請求項１６】
セキュリティパラメータを再計算するための間隔についてハンドシェーキング中に上記少なくとも１つの通信当事者端末とネゴシエーションし合意に達するための手段を更に備える請求項１２から１５のうちのいずれか１項に記載のサーバ。
【請求項１７】

移動ステーションを動作させる方法において、
少なくとも１つの通信当事者端末と通信当事者端末間でのメッセージの暗号化のためのセキュリティパラメータを交換し、
メッセージにシーケンス番号で番号付けし、
メッセージを送信し、
メッセージと共に各シーケンス番号を送信し、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータを再計算するための間隔を決定するためのメッセージの数につき上記少なくとも１つの通信当事者端末とでネゴシエーションし合意に達し、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータの再計算の間隔を監視し、
合意された数のメッセージが送信された後に通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータを再計算し、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータの再計算のための入力として最新のシーケンス番号を使用し、
通信当事者端末間でメッセージの暗号化のための最新の再計算されたセキュリティパラメータに基づきメッセージに対する接続セキュリティを与える、
という段階を含むことを特徴とする方法。
【請求項１８】
サーバを動作させる方法において、
少なくとも１つの通信当事者端末と通信当事者端末間でのメッセージの暗号化のためのセキュリティパラメータを交換し、
メッセージにシーケンス番号で番号付けし、
メッセージを送信し、
メッセージと共に各シーケンス番号を送信し、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータを再計算するための間隔を決定するためのメッセージの数につき上記少なくとも１つの通信当事者端末とでネゴシエーションし合意に達し、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータの再計算の間隔を監視し、
合意された数のメッセージが送信された後に通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータを再計算し、
通信当事者端末間でメッセージの暗号化のためのセキュリティパラメータの再計算のための入力として最新のシーケンス番号を使用し、
通信当事者端末間でメッセージの暗号化のためのえ最新の再計算されたセキュリティパラメータに基づきメッセージに対する接続セキュリティを与える、
という段階を含むことを特徴とする方法。
【発明の詳細な説明】
【０００１】
【技術分野】
本発明は、テレコミュニケーションネットワークにおける通信当事者間、すなわち、通信当事者端末間の送信に対する接続セキュリティを与える方法に係る。
【０００２】
【背景技術】
通信の始めに、通常、ハンドシェークがテレコミュニケーションネットワークのアプリケーション間で実行され、その間に、関連する当事者は、通常、互いに認証を行い、そしてキー情報を交換し、例えば、通信に使用すべき暗号化アルゴリズム及び暗号キーをネゴシエーションする。ハンドシェークの後にのみ、実際のデータが送信される。送信の機密は、例えば、暗号化により確保される。添付図面の図１ａ及び１ｂは、送信を保護するために使用できる２つの既知の暗号化アルゴリズム、即ち対称的アルゴリズム及び公開キーア

ルゴリズムのブロック図である。

【０００３】

図１ａは、参加者間に共有されるシークレットキーをベースとする対称的アルゴリズムを示す。当事者Ａの端末において、当事者Ｂへ送信されるべきメッセージＭは、図１ａのボックスＥ内で、共有シークレットキーＫで暗号化される。このメッセージは、暗号化された暗号テキストＣとして送信ルートを経て送信され、当事者Ｂは、図１ａに示すボックスＤにおいて同じシークレットキーＫでこれを暗号解読することができる。この暗号解読により、当事者Ｂは、元のメッセージＭを得る。送信を傍受する侵入者は、送信された暗号テキストＣを読み取って理解できるためには、シークレットキーＫを知る必要がある。対称的アルゴリズムの暗号化及び暗号解読は、次の式で表すことができる。

$C = E_K(M)$

$M = D_K(C)$

但し、Ｃは暗号テキストであり、Ｍは平易テキストのメッセージであり、E_KはキーＫでの暗号化であり、そしてD_KはキーＫでの暗号解読である。

【０００４】

図１ｂは、非対称的な解決策である公開キーアルゴリズムを示す。このアルゴリズムは、２つのキー、即ち公開キー及び専用キーをベースとする。これら２つのキーは、公開キーK_+で暗号化されたメッセージを、それに対応する専用キーK_-でしか暗号解読できず、そしてその逆もまた真であるように関連される。図１ｂでは、メッセージＭが当事者Ａの端末のボックスＥにおいて意図された受信者即ち当事者Ｂの公開キーK_+で暗号化される。暗号化された暗号テキストＣは、送信ラインを経て当事者Ｂの端末へ送信され、そこで、暗号テキストＣは、ボックスＤにおいて対応する当事者Ｂの専用キーＫで暗号解読され、そして元のメッセージＭが検索される。この非対称的アルゴリズムの暗号化及び暗号解読も、次の式で表すことができる。

$C = E_B^+(M)$

$M = D_B^-(C)$

但し、Ｃは暗号テキストであり、Ｍは平易テキストのメッセージであり、E_B^+は、受信者の公開キーK_B^+での暗号化であり、そしてD_B^-は、受信者の専用キーK_B^-での暗号解読である。

【０００５】

公開キーアルゴリズムでは、メッセージ送信者の専用キーＫでのメッセージの暗号化が符牒として働く。というのは、誰でも、送信者の既知の公開キーK_+でメッセージを暗号解読できるからである。非対称的キーは、通常、対称的キーより相当に長いので、非対称的アルゴリズムは、相当の処理パワーを必要とする。従って、非対称的アルゴリズムは、多量のデータの暗号化には適していない。

混成型暗号化は、上記の２つのアルゴリズムを一緒に使用するものである。例えば、公開キーアルゴリズムを使用してセッションキーのみが交換され、そして残りの通信が対称的方法により暗号化される。

【０００６】

接続におけるメッセージの完全性及び認証を与えるために、メッセージ認証コードＭＡＣが計算されそして送信メッセージに添付される。例えば、ＭＡＣは、一方向ハッシュアルゴリズムで次のように計算することができる。

$h = H(K、M、K)$

但し、Ｋはキーであり、Ｍはメッセージであり、そしてＨはハッシュコードである。出力から入力を推定することはできない。ＭＡＣがメッセージに添付されたときには、メッセージを不正使用したり模擬したりすることができない。受信者は、受信したメッセージと、送信者と同じハッシュ関数及びキーとを使用して、ＭＡＣを計算し、そしてその計算されたＭＡＣを、メッセージに添付されたＭＡＣと比較し、メッセージを照合する。

【０００７】

図２は、通信接続の例を示す。ＧＳＭネットワーク（移動通信用のグローバルシステム）

において動作する移動ステーションＭＳは、ＧＳＭネットワークから銀行への接続を直接形成することができる。図２に示す他の考えられる接続は、ＧＳＭネットワークからゲートウェイＧＷ及びインターネットを経て異なるサービスへ至る接続である。ＧＳＭのような移動通信ネットワークでは、移動ステーションＭＳからＧＳＭネットワークへのエアインターフェイスは、悪用に対して良好に保護されるが、残りの送信ルートは、接続セキュリティを与える手段が設けられていなければ、他の公衆電話ネットワークと同様にその影響を受け易い。

【０００８】

接続セキュリティの付与に関する１つの問題は、関連する当事者間で多数のメッセージを送信しなければならないので、ハンドシェークに相当の処理時間を要することである。移動ステーションは、処理パワーが低くそして帯域巾が狭いために、移動通信ネットワークにおいてハンドシェークは特に厄介なものとなる。又、ハンドシェークは、例えば、銀行のサーバのように多数の同時トランザクションを有するアプリケーションにとっても厄介である。それ故、ハンドシェークの数及び時間を最小にすることが所望される。これは、２つのハンドシェーク間に同じ暗号キーが使用されるので、侵入者が暗号分析に長い時間をかけられるという問題を招く。侵入者は、暗号分析に成功すると、２つのハンドシェーク間に送信される全ての資料にアクセスできることになる。

【０００９】

【発明の開示】

本発明の目的は、特に狭帯域接続を経て通信アプリケーション間に送信される情報を、通信当事者に不必要な負荷をかけずに、確実に保護するための方法を提供することである。これは、独立請求項１に記載した本発明の方法を使用することにより達成される。本発明の特定の実施形態は、従属請求項に記載する。

【００１０】

本発明は、通信当事者が、合意した間隔で互いに同時に通信セッションを行いそして連続的な通信を行う間にセキュリティパラメータを再計算し、そしてその新たなパラメータでメッセージに対する接続セキュリティを与えるという考え方をベースとする。通信当事者は、再計算のための時間を監視し、合意した間隔で再計算を行い、従って、ハンドシェークを行なわずにセキュリティパラメータを変更する。本発明の主たる実施形態では、メッセージが番号付けされ、そしてその合意された番号の間隔で再計算をトリガーする。

【００１１】

本発明による方法の効果は、セッション中にハンドシェークを伴わずにセキュリティパラメータを変更できることである。これは、ハンドシェークの必要性を減少する。

本発明による方法の別の効果は、送信のセキュリティが改善され、即ち侵入をより困難にし且つ利益を得られなくすることである。

【００１２】

【発明を実施するための最良の形態】

以下、添付図面を参照して、本発明の好ましい実施形態を詳細に説明する。

本発明は、いかなるテレコミュニケーションネットワークに適用することもできる。以下、本発明は、デジタルＧＳＭ移動通信システムにおいて動作してＧＳＭネットワークの内部又は外部に配置されたアプリケーションと通信する移動ステーションを一例として使用して詳細に説明する。

図２、３及び４を参照して、本発明の主たる実施形態を以下に詳細に述べる。

【００１３】

図２は、上述した接続の例を示す。銀行のサービスと連絡する移動ステーションＭＳは、先ず、公知技術に基づくハンドシェークを実行し、その間にＭＳ及び銀行の両方は、互いに他を認証し、そして必要なセッションキー情報を交換する。本発明によれば、例えば、ハンドシェーク中に、移動ステーション及び銀行のアプリケーションは、通信中にプライバシー、データ完全性及び認証を与えるために使用されるべきセキュリティパラメータを再計算するのに適した間隔をネゴシエーションしそして合意する。例えば、ネゴシエーシ

ョンは、通信の当事者、即ち図２の例では移動ステーションＭＳ及び銀行のアプリケーションの各々が、再計算に適した間隔を提案し、そしてその提案された間隔の一方、例えば、より頻度の高い方が選択され合意される。間隔を決定するのに適したパラメータは、例えば、４番目ごとのメッセージといったメッセージシーケンス番号、又は適当な時間周期である。ハンドシェークが必要とされず、従って、通信の始めに実行されなくても、本発明では、通信の当事者が再計算間隔について合意する必要がある。

【００１４】

再計算の間隔を合意した後に、両当事者は、その合意した間隔を監視する。４つのメッセージ後の間隔で合意した場合には、両当事者は、送信されるメッセージの数を監視する（これは、メッセージが失われることのない確実な送信媒体を必要とする）か、又は全ての送信メッセージに番号を付けそしてそれらのシーケンス番号をメッセージと共に送信する。シーケンス番号又はタイムスタンプをメッセージと共に送信する効果は、たとえあるメッセージが経路に沿って失われたり又は受信したメッセージが正しい順序でなくても、再計算が両端において同期されることである。上記例において第４のメッセージが送信されそして受信された場合には、両通信当事者がセキュリティパラメータを再計算し、そしてその新たなパラメータを使用して、次の４つのメッセージに対する接続セキュリティを与える。パラメータの再計算中又はその後に、ハンドシェーク又は他のセッションキー交換が行われることはない。再計算は、例えば、共有のシークレット情報及び最新のシーケンス番号をベースとすることができる。又、セキュリティパラメータを使用して、暗号化のためのセッションキーＫｎ及びメッセージ認証コードＭＡＣを例えば次のように計算することができる。

Ｋｎ＝Ｈ(Ｓ、Ｎ)

ＭＡＣ＝Ｈ(Ｍ、Ｓ、Ｎ)

但し、Ｈは、所定のハッシュアルゴリズムであり、Ｓは、共有シークレット情報であり、Ｎは、最新のシーケンス番号であり、そしてＭは、平易テキストで送信されるべきメッセージである。

【００１５】

図３は、本発明によるセッションキーの交換例を示す。図３において、ＭＳから送信されるメッセージは、シーケンス番号０ないし３と番号付けされる。図３の例では、再計算のための間隔は、２つのメッセージを送信した後と合意される。シーケンス番号０のメッセージは、セッションキーＫ１で暗号化されて銀行へ送信される。銀行のアプリケーションは、対称的アルゴリズムが暗号化に適用されたときには、メッセージ０を同じセッションキーＫ１で暗号解読する。シーケンス番号１のメッセージも、セッションキーＫ１で暗号化されて送信される。これで移動ステーションＭＳは２つのメッセージを送信したので、ＭＳ及び銀行のアプリケーションの両方は、共有シークレット情報及び最新のシーケンス番号即ち１を用いて、セキュリティパラメータ、例えば、セッションキーＫ２を再計算する。再計算の後に、ＭＳは、次のメッセージＫ２をセッションキーＫ２で暗号化して銀行へ送信する。銀行のアプリケーションは、同じ再計算されたセッションキーＫ２でメッセージ２を暗号解読する。又、メッセージ３も、送信前にセッションキーＫ２で暗号化される。その後、ＭＳ及び銀行のアプリケーションは、合意された間隔に達したことに再び気付き、そして両当事者は、共有シークレット情報及び最新のシーケンス番号３を使用して、セキュリティパラメータ、例えば、セッションキーＫ３を再計算する。

【００１６】

図４は、本発明の主たる実施形態を示すフローチャートである。段階４１において、通信の始めに、通信に関連する当事者、図２の例ではＭＳ及び銀行のアプリケーションは、セキュリティパラメータを再計算するための間隔をネゴシエーションしそして合意する。上述した例と同様に、この間隔は、２つのメッセージを送信した後であると合意されるものとする。両通信当事者は、例えば、各端のカウンタで送信メッセージの数を追跡する。段階４２において、通信当事者の一方、例えば、ＭＳは、ハンドシェーク中に交換されるか又は他のやり方で関連当事者と共有した共有シークレット情報から得られたセッションキ

ーＫ１で送信されるべき第１メッセージを暗号化する。暗号化されたメッセージが送信され、そして受信者は、対応するセッションキーＫ１でメッセージを暗号解読する（段階４３）。このときカウンタが１にセットされる。段階４４において、両当事者、この例では、ＭＳ及び銀行のアプリケーションは、例えば、カウンタの値が合意した間隔の値に等しいかどうかをチェックすることにより、合意した間隔に達したかどうかチェックする。送信されたメッセージは、第１メッセージだけであるから、再計算は行なわれず、そして次のメッセージが同じセッションキーＫ１で暗号化されそして暗号解読される。２つのメッセージが送信され、そして合意した間隔の値に対応する値２をカウンタが指示するときには、段階４４が「真」となり、両通信当事者は、所定のやり方でセキュリティパラメータを再計算し、そして新たなセッションキーＫ２を得る（段階４５）。段階４６において、間隔の監視がリセットされ、即ちカウンタを０にセットすることによりメッセージカウントが再開される。段階４７では、送信されるべきメッセージがまだあるかに関してチェックが行なわれ、もしそうであれば、段階４２において最新のセッションキーＫ２を使用して第１メッセージを暗号化するようにしてメッセージの暗号化が続けられ、その後、メッセージが送信されそしてカウンタが値１にセットされる。このプロセスは、送信されるべき全てのメッセージが送られるまで同様に続けられる。

【００１７】

本発明の別の実施形態では、暗号化に代わって、ＭＡＣを使用してメッセージ送信に対する接続セキュリティが与えられる。本発明によれば、ＭＡＣは、例えば、セキュリティパラメータの再計算を最後にトリガーしたシーケンス番号から計算される。図３の例では、ＭＡＣは、Ｋ２で暗号化されて示されたメッセージに対するシーケンス番号１、及びＫ３で暗号化されるべきメッセージに対するシーケンス番号３で計算される。その他の点では、本発明のこの実施形態は、上述した第１の実施形態と同様に実施される。

本発明の更に別の実施形態は、暗号化及びＭＡＣを使用して、メッセージに対する接続セキュリティを与える。これは、上述した実施形態を組み合わせることにより実施される。

【００１８】

セキュリティパラメータの再計算は、使用すべき暗号化アルゴリズムを次のメッセージの暗号化において変更する可能性も含む。

添付図面及びそれを参照した以上の説明は、本発明の原理を例示するものに過ぎない。本発明による方法の細部は、請求の範囲内で変更し得る。本発明は、主として、移動ステーション及びサービスアプリケーション通信に関連して説明したが、互いに通信する２つ以上のアプリケーション間や、スピーチ、データ及びショートメッセージ送信における移動ステーション対移動ステーションの接続においてメッセージに対する接続セキュリティを与えるのにも使用できる。又、本発明は、セッションキー及びＭＡＣ以外のセキュリティパラメータを再計算するのにも適している。又、本発明は、上述した暗号化アルゴリズムに関連した使用に限定されるものではなく、いかなる暗号化アルゴリズムと共に使用することもできる。

【図面の簡単な説明】

【図１ａ】　対称的暗号化アルゴリズムを示すブロック図である。

【図１ｂ】　非対称的暗号化アルゴリズムを示すブロック図である。

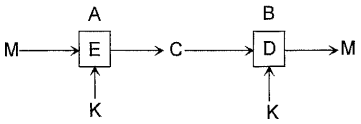
【図２】　移動通信ネットワークからあるアプリケーションへ至る幾つかの接続例を示す図である。

【図３】　本発明の主たる実施形態に基づき送信メッセージに対して接続セキュリティを与えるセッションキーを示す図である。

【図４】　本発明の主たる実施形態を示すフローチャートである。

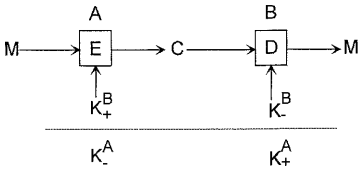
【図１ａ】

Fig. 1a



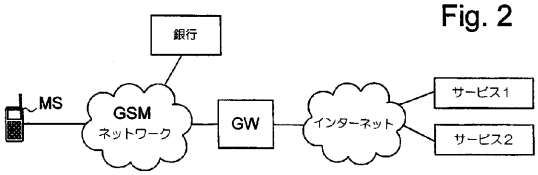
【図１ｂ】

Fig. 1b



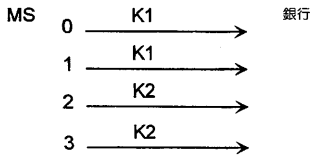
【図２】

Fig. 2



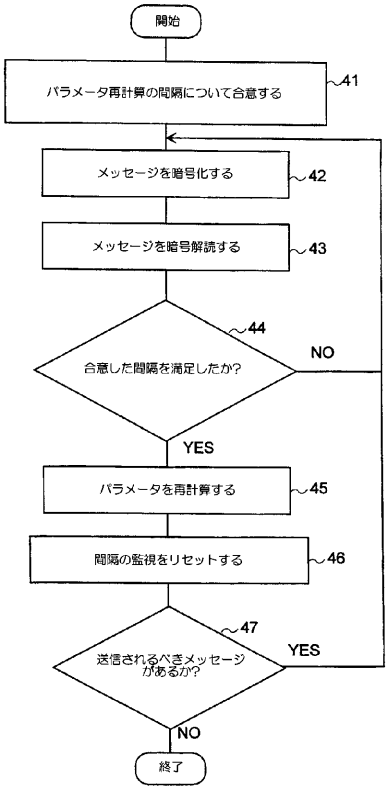
【図３】

Fig. 3



【図４】

Fig. 4



フロントページの続き

(74)代理人 100084009
弁理士 小川 信夫
(74)代理人 100086771
弁理士 西島 孝喜
(74)代理人 100084663
弁理士 箱田 篤
(72)発明者 ライヴィスト トミー
フィンランド エフイーエン－００７１０ ヘルシンキ リウスケティエ １６イー５４

審査官 中里 裕正

(56)参考文献 特開平１－２８８１３１（ＪＰ，Ａ）
特表平８－５０３１１３（ＪＰ，Ａ）
特開平６－６６１５（ＪＰ，Ａ）
特開平９－１４８９９３（ＪＰ，Ａ）
ネットワーク・セキュリティ，日経マグロウヒル社，１９８５年１２月 ５日，p.126-128

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/16
H04Q 7/38