(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4105339号
(P4105339)

(45)発行日　平成20年6月25日(2008.6.25)　(24)登録日　平成20年4月4日(2008.4.4)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　　H04L 9/00 601C
H04Q 7/38 (2006.01)　　H04L 9/00 601E
　　H04B 7/26 109R

請求項の数 9　(全 11 頁)

(21)出願番号　特願平11-214544
(22)出願日　平成11年7月29日(1999.7.29)
(65)公開番号　特開2000-78124(P2000-78124A)
(43)公開日　平成12年3月14日(2000.3.14)
審査請求日　平成12年10月10日(2000.10.10)
審判番号　不服2004-19956(P2004-19956/J1)
審判請求日　平成16年9月27日(2004.9.27)
(31)優先権主張番号　09/127769
(32)優先日　平成10年7月31日(1998.7.31)
(33)優先権主張国　米国(US)

(73)特許権者　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国．０７９７４－０６３６　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　６００
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100085176
弁理士　加藤　伸晃
(74)代理人　100106703
弁理士　産形　和央
(74)代理人　100096943
弁理士　臼井　伸一

最終頁に続く

(54)【発明の名称】空中通信とパスワードを用いてキーを確立するための方法およびパスワードプロトコル

(57)【特許請求の範囲】

【請求項１】

パスワードを用いて第一の装置と第二の装置との間でキーを生成するための方法であって、

（ａ）認証情報を機密通信チャネルを通じて前記第二の装置に送信するステップ；

（ａ′）前記第二の装置が前記認証情報を受理した場合、前記パスワードＰを前記第二の装置から前記機密通信チャネルを通じて前記第一の装置で受信するステップ；

（ａ″）前記第一の装置において、第一の乱数R_Mを生成するステップ；

（ｂ）ｐが素数を表し、ｇが前記素数ｐによって生成されるグループのジェネレータを表すものとして、$((g^{R_M} + P) \bmod p)$を計算することで、第一の計算結果を生成するステップ；

（ｃ）前記素数ｐ、前記ジェネレータｇ、および前記第一の計算結果を前記第二の装置に送信するステップ；

（ｄ）R_Nが第二の乱数を表すとき前記第二の装置から$((g^{R_N} + P) \bmod p)$に等しい第二の計算結果を受信するステップ；および

（ｅ）前記第二の計算結果と前記第一の乱数に基づいてキーを生成するステップを含むことを特徴とする方法。

【請求項２】

前記ステップ（ｅ）が：

（ｅ１）（Ｐ mod p）を計算するステップ；

（ｅ２）前記((g^R_N ＋ Ｐ) mod p) なる第二の計算結果から（Ｐ mod p）を減算することで、(g^R_N mod p) を得るステップ；および
（ｅ３）前記キーを、(g^R_N mod p) および前記第一の乱数に基づいて生成するステップを含むことを特徴とする請求項１の方法。
【請求項３】
前記第一の装置が無線システムの移動機であり、前記第二の装置が網であることを特徴とする請求項１の方法。
【請求項４】
前記第一の装置が無線システムの移動機であり、前記第二の装置が網であり；
前記機密通信チャネルが地上回線であることを特徴とする請求項１の方法。
【請求項５】
パスワードを用いて第一の装置と第二の装置との間でキーを確立するための方法であって、
（ａ′）認証情報を機密通信チャネルを通じて前記第一の装置で受信するステップ；
（ａ″）前記第一の装置が前記認証情報を受理した場合、前記パスワードＰを前記機密通信チャネルを通じて前記第二の装置に送信するステップ；
（ａ）前記第二の装置から素数ｐ、前記素数ｐによって生成されるグループのジェネレータｇ、および第一の計算結果であって、Ｐがパスワードを表し、R_Mが第一の乱数を表わすとき((g^R_M ＋ Ｐ) mod p)を計算することで得られるような第一の計算結果を前記第１の装置で受信するステップ；
（ｂ）第二の乱数R_Nを生成するステップ；
（ｃ）((g^R_N ＋ Ｐ) mod p)を計算することにより第二の計算結果を生成するステップ；
（ｄ）前記第二の計算結果を前記第二の装置に送信するステップ；および
（ｅ）前記第一の計算結果と前記第二の乱数に基づいてキーを生成するステップを含むことを特徴とする方法。
【請求項６】
前記ステップ（ｅ）が：
（ｅ１）（Ｐ mod p） を計算するステップ；
（ｅ２）前記((g^R_M ＋ Ｐ) mod p)なる第一の計算結果から（Ｐ mod p） を減算することで、(g^R_M mod p)を得るステップ；および
（ｅ３）前記キーを、(g^R_M mod p)および前記第二の乱数に基づいて生成するステップを含むことを特徴とする請求項５の方法。
【請求項７】
前記第一の装置が無線システムの網であり、前記第二の装置が移動機であることを特徴とする請求項５の方法。
【請求項８】
前記ステップ（ａ）の前に、さらに：
（ｆ）認証情報を前記第二の装置から機密通信チャネルを通じて受信するステップ；および
（ｇ）前記認証情報が受理できる場合は、前記パスワードを前記第二の装置に前記機密通信チャネルを通じて送信するステップを含むことを特徴とする請求項５の方法。
【請求項９】
前記第一の装置が無線システムの網であり、前記第二の装置が移動機であり；
前記機密通信チャネルが地上回線であることを特徴とする請求項８の方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、パスワードプロトコルに関し、本発明の一つの実施例は、空中通信およびこのパスワードプロトコルを用いてキーを確立するための方法に関する。

【０００２】
【従来の技術】
無線通信システムにおいては、しばしば移動機とも呼ばれる移動機ユーザによって購入されるハンドセットは、典型的には、サービスを起動するためには、網サービスプロバイダに持ち込み、長いキーおよびパラメータをそのハンドセットに入力することを必要とされる。網サービスプロバイダもその移動機に対して、長いキーおよびパラメータのコピーを維持し、これらをその移動機と関連づける。周知のように、これら長いキーおよびパラメータを用いることで、網と移動機の間で空中を通じて情報を機密に伝送することが可能となる。
【０００３】
別の方法においては、ユーザは、長いキーをサービスプロバイダから安全な（機密）通信チャネル、例えば、電話／地上回線等を通じて受信し、これらコードを手操作で移動機に入力する。
【０００４】
長いキーおよびパラメータを、空中を介してではなく、電話／地上回線を介して伝送する方法や、網サービスプロバイダに持ち込んでこれらを入力する方法は、空中アタックに対しては安全である。ただし、これらの情報を安全（機密）に伝送するための方法は、移動機ユーザになんらかの負担および制約を課す。理想的には、移動機ユーザにとっては、ハンドセットを購入したときハンドセットを物理的にプロバイダの所に持ち込んだり、あるいは、移動機に手操作にて長いキーをエラーなしに入力することなく、直ちにサービスを得られることが望ましい。移動機を遠隔的に起動および準備する能力は北米無線標準の一部であり、“over the air service provisioning、OTAP）”（空中を通じてのサービスの準備）と呼ばれる。
【０００５】
現在、北米セルラ標準IS41-CはOTASP プロトコルを指定するが、このプロトコルにおいては、周知のDiffe-Hellman （DH）キー合意を用いて２パーティ間の機密キーが確立される。図１は、IS41-Cにおいて用いられるDHキー合意を、移動機２０と網１０との間の機密キーの確立に適用した場合について示す。すなわち、図１は、DHキー合意に従う網１０と移動機２０との間の通信を簡略的に示す。ここで用いられる網なる用語は、網サービスプロバイダによって運用される認証センタ、ホーム位置レジスタ、ビジティング（訪問）位置レジスタ、移動体交換センタ、および基地局等の設備を総称的に指称する。従って、網は、装置の範疇に属する。
【０００６】
網１０は、乱数R_Nを生成し、（g^R_N mod p）を計算する。図１に示すように、網１０は、５１２ビットの素数ｐ、素数ｐによって生成されるグループ（群）のジェネレータ（生成プログラム）ｇ、および（g^R_N mod p）を移動機２０に送信する。次に、移動機２０は、乱数RMを生成し、（g^R_M mod p）を計算し、（g^R_M mod p）を網１０に送信する。
【０００７】
移動機２０は、網１０から受信された(g^R_N mod p)に乱数R_Mをべき乗することで(g^R_MR_N mod p)を得、網１０は、移動機２０から受信された(g^R_N mod p)に乱数R_Nをべき乗することで(g^R_MR_N mod p)を得る。移動機２０と網１０は両方とも同一の結果を得、この６４個の最下位ビットを用いて、Ａ－キーと呼ばれる長く生きるキーを確立する。このＡ－キーは、移動機２０と網１０との間の通信を機密化するために用いられる他のキーを生成するためのルートキーとして用いられる。
【０００８】
【発明が解決しようとする課題】
このDHキー交換と関連する一つの問題は、これが認証手続きを経ておらず、受マン－イン－ザ－ミドルアタックに弱いことである。例えば、移動機と網との２パーティ間の通信の例においては、アタッカは、最初に網１０のふりをし、次に、網１０に対して、移動機の

ふりをする。こうして、アタッカは、移動機２０と網１０との間でメッセージを中継する際に、Ａ－キーを選択し、これを知ることで、認証要件を満すことができる。加えて、DHキーの交換は、オフラインディクショナリアタックにも弱い。

【０００９】

Ａ－キー等の情報の空中伝送を保護するためのもう一つの周知の方法として、Diffe-Hellman Encrypted Key Exchange（DH-EKE）がある。DH-EKEは、情報の交換するためのパスワードベースのプロトコルであり、移動機ユーザと網サービスプロバイダの両方が、空中伝送の前に、パスワードを確立していることを想定する。図１との関連で説明したDHキー交換システムとは異なり、DH-EKEは、マン－イン－ザ－ミドルアタックおよびオフラインディクショナリアタックに対しては保護されている。

【００１０】

以下に、DH-EKEについて図２との関連で説明する。図２は、DH-EKEプロトコルによる移動機２０と網１０との間の通信を図解する。図２に示すように、最初、移動機２０が網１０に、５１２ビット素数ｐおよびジェネレータｇを、暗号化された$(g^{R_M} \bmod p)$と共に送信する。この$(g^{R_M} \bmod p)$の暗号化は、暗号化／暗号解読アルゴリズムENC に従って、移動機ユーザと網１０の両方によって暗号化キーとして知られているパスワードＰを用いて行なわれる。この計算は、$ENC_P(g^{R_M} \bmod p)$として表される。網１０は、パスワードＰを用いて$(g^{R_M} \bmod p)$を解読し、$(g^{R_M} \bmod p)^{R_N}$を計算するが、これは、$(g^{R_M R_N} \bmod p)$に等しい。網１０は、$(g^{R_M R_N} \bmod p)$、この値のハッシュ、あるいはこのある一部を、セッションキーSKとして選択する。

【００１１】

次に、網１０は、移動機２０に、ENC に従ってパスワードＰを用いて暗号化された$(g^{R_N} \bmod p)$と、ENC に従ってセッションキーSKを用いて暗号化された乱数R_N'を送信する。移動機２０は、パスワードＰを用いて$(g^{R_N} \bmod p)$を解読し、$(g^{R_N} \bmod p)^{R_M}$を計算するが、これは、$(g^{R_M R_N} \bmod p)$に等しい。次に、移動機２０は、網１０の場合と同様に、$(g^{R_M R_N} \bmod p)$、このハッシュ、あるいはこの一部を、セッションキーSKとして選択する。移動機２０は、次に、このセッションキーSKを用いてR_N'を解読する。

【００１２】

次に、移動機２０は、乱数R_M'を生成し、乱数R_M'とR_N'をENC に従ってセッションキーSKを用いて暗号化し、この暗号化された乱数R_N'とR_M'を網１０に送信する。網１０は、セッションキーSKを用いてこれら乱数R_N'とR_M'を解読し、R_N'の解読されたバージョンが最初に移動機２０に送信したバージョンと等しいか否か決定する。網１０は、R_N'の解読されたバージョンがR_N'の最初に移動機２０に送信したバージョンに等しい場合に、そのセッションキーSKを正当なものと認証する。

【００１３】

網１０は、次に、ENC に従ってセッションキーを用いて暗号化された乱数R_M'を移動機２０に送信する。移動機２０は、セッションキーSKを用いて乱数R_M'を解読し、R_M'の計算されたバージョンがR_M'の最初に網１０に送信したバージョンに等しいか否か決定する。移動機２０は、RM'の解読されたバージョンがR_M'の最初に網に送信したバージョンと等しい場合に、そのセッションキーSKを正当なものと認証する。

【００１４】

いったん、網１０と移動機２０が、セッションキーＳＫを認証すると、そのセッションキーがＡ－キーとして用いられ、移動機２０と網１０との間の通信がそのＡ－キーを用いて再構成（リコンフィギュア）される。

【００１５】

DH-EKEプロトコルは、マン－イン－ザ－ミドルアタックおよびオフラインディクショナリアタックを排斥するが、まだ情報が漏れ、アタッカがパスワードＰを回復する可能性が残される。

【００１６】

【課題を解決するための手段】

本発明によるパスワードプロトコルにおいては、通信パーティは、互いに計算結果を交換するが、これは、おのおの、キーを計算するための（べき）指数を含む。この計算結果の生成において、各パーティは、おのおのの指数にパスワードを加える。片方のパーティによって先に送信された認証情報が他方のパーティによって許容（受理）できる場合に、他方のパーティは、パスワードプロトコルに従って確立されたキーを使用する。認証情報は、機密通信チャネルを通じて送信される。各指数にパスワードを加えることで、パスワードに関する情報の漏れが少なくなり、計算はより効率的となる。

【００１７】

この機密通信チャネルが、他の幾つかの実施例においては、パーティ間に送信される少なくとも一つの計算結果に関するハッシュを検証（認証）するためにも用いられる。ただし、パスワードプロトコルの場合とは異なり、この計算結果は、パスワードを含まない。ハッシュが認証された場合に、これらパーティ間で送信された計算結果を用いてキーが確立される。この認証プロセスは、このキーを確立する前の機密手段を提供する。

【００１８】

本発明は、様々な用途を持ち、これら用途には無線産業も含まれる。この場合、これらパーティは、移動機ユーザと網である。

【００１９】

【発明の実施の形態】

以下に本発明のより完全な理解を図るために、本発明を図面を用いて詳細に説明するが、これら図面中、類似する参照符号は対応するパーツを指す。

【００２０】

以下では、空中通信を用いてキーを確立するための本発明によるシステムおよび方法を、無線システムに適用した場合について説明する。つまり、移動機２０と網１０との間で、キーを、電話／地上回線３０と、パスワードプロトコルの両方を用いて確立する本発明の一つの実施例について説明する。

【００２１】

図３は、本発明の第一の実施例による（１）集合的に網１０として示される網プロバイダ／網１０と、（２）移動機ユーザとの間で、電話／地上回線３０および移動機２０を介して遂行される通信を示す。図３に示すように、最初に、移動機ユーザが、認証情報（例えば、課金目的のクレジットカード情報）を、電話／地上回線３０を介して網１０に送信する。網１０がその認証情報を受理した場合は、網１０は、移動機ユーザに、電話／地上回線３０を通じて、４桁のパスワードＰを送信する。ただし、このパスワードＰは、４桁より大きくても、小さくても構わない。

【００２２】

次に、移動機ユーザは、この短なパスワードＰを起動プログラムの一部として移動機２０に入力する。移動機２０は、乱数発生器を用いて、乱数R_Mを生成し、事前に格納されている５１２ビットの素数ｐと素数ｐによって生成されるグループ（群）のジェネレータ（生成プログラム）ｇを用いて、$((g^{R_M} + P) \bmod p)$を計算する。

【００２３】

移動機は、次に、素数ｐとジェネレータｇを、$((g^{R_M} + P) \bmod p)$と共に網１０に送信する。$((g^{R_M} + P) \bmod p)$は、$(g^{R_M} + P)+(P \bmod p)$ に等ししく、網１０は、パスワードＰを知っているために、網１０は、$(P \bmod p)$を計算し、$((g^{R_M} + P) \bmod p)$ から$(g^{R_M} + P)$を抽出する。網１０は、乱数R_Nを生成し、次に、$(g^{R_M} \bmod P)^{R_N}$ を計算するが、これは、$(g^{R_M R_N} \bmod p)$に等しい。 網１０は、$(g^{R_M R_N} \bmod p)$ 、このハッシュ、あるいはこの一部をセッションキーSKとして選択する。例えば、IS41プロトコル内に組み込まれる場合は、$(g^{R_M R_N} \bmod p)$の６４個の最下位ビットがセッションキーSKとして選択される。

【００２４】

次に、網１０は、$((g^{R_N} + P) \bmod p)$を計算し、これを移動機２０に送信する。移動機２０は、$(g^{R_N} \bmod p)$を抽出し、次に、$(g^{R_N} \bmod p)^{R_M}$ を生成するが、これは、$(g^{R_M}R$

$_N$ mod p)に等しい。移動機２０は、網１０と同様なやり方で、(g^R_MR_N mod p)、このハッシュ、あるいはこの一部を、セッションキーSKとして選択する。例えば、IS41プロトコル内に組み込まれる場合は、(g^R_MR_N mod p)の６４個の最下位ビットがセッションキーSKとして選択される。

【００２５】

いったん網１０と移動機２０がセッションキーSKを得ると、このセッションキーSKがＡ－キーとして用いられ、移動機２０と網１０との間の通信がこのＡ－キーを用いて再構成（リコンフィギュア）される。

【００２６】

上述の本発明による空中交換は、パスワードプロトコルを用いるが（つまり、図３に示すように、((g^R_M + P) mod p)と((g^R_N + P) mod p)の伝送を行なうが）、この方式による情報の漏れは、DH-EKEプロトコルの情報の漏れと同程度である。さらに、このパスワードプロトコルは、パスワードの効果を除去しても、なにも明らかにならないために安全である。つまり、R_MとR_Nは、一様な乱数であり、これらをｇに上げ（raising）（ベキ乗し）、その後、mod pだけ減算（reducing）ても、指数mod pによって導かれる置換（permutation）のために、結果は、一様な乱数となる。また、P mod pをこの数に加えても、結果の一様性およびランダムさは変わらない。全ての数は同様に確からしく、他のパスワードの効果を除去しても、同様に確からしい数が生成され、このため、情報が漏れることはない。当業者においては理解できるように、上述のパスワードプロトコルは、上述の空中交換への適用に限定されるものではない。例えば、このパスワードプロトコルは、エンティティ認証や、セッションキー合意にも適用できる。

【００２７】

次に、本発明の第二の実施例を図４との関連で説明する。図４は、本発明の第二の実施例による網１０と、移動機ユーザの間の、電話／地上回線３０を介しての通信を図解する。図４に示すように、最初に、移動機ユーザが、認証情報を、電話／地上回線３０を介して、網１０に供給する。網１０が、その認証情報を受理した場合は、移動機２０は、次に、移動機の初期化手続きの一部として初期化リクエストを発行し、この初期化プロセスは以下のように継続される。

【００２８】

例えば、移動機２０は、乱数R_Mを生成し、(g^R_M mod p)を計算し、(g^R_M mod p)と共に初期化リクエストを網１０に送信する。

【００２９】

網１０は、乱数R_Nを生成し、(g^R_N mod p)を移動機２０に送信する。

移動機２０と網１０は、両方とも、周知のSecure Hashing Algorithm（SHA）を用いて、h((g^R_N mod p),(g^R_M mod p))を遂行するが、これは、(g^R_N mod p)と(g^R_M mod P)に関する集合的なハッシュである。ただし、任意の他のハッシングアルゴリズムを用いることもできることに注意する。移動機２０は、ハッシュの結果を表示し、移動機のユーザは、電話／地上回線３０を介して、ハッシュの数字を網１０に供給する。

【００３０】

網１０が、移動機ユーザによって供給された数字と、網１０によって遂行されたハッシュとが一致することを見つけた場合は、その通信は、検証（認証）され、(g^R_MR_N mod p)、このハッシュ、あるいはこの一部として、Ａ－キーが確立される。すなわち、移動機２０は、このようにしてＡ－キーを確立するが、ただし、網１０は、そのハッシュが正当であると検証（認証）された場合にのみ、このＡ－キーを移動機２０と関連付ける。

【００３１】

もう一つの代替、すなわち、第三の実施例においては、移動機ユーザ２０は、認証情報と共に、網１０が移動機２０と連絡し、最初の通信として(g^R_N mod p)を送信することを可能にするために十分な情報（例えば、移動機の識別番号等）を網１０に送信する。

【００３２】

この第三の実施例は、誕生日アタックを受ける；つまり、マン－イン－ザ－ミドルアタッ

カは、このプロトコルにアタックするためには、通常の半分の試みで済む。ただし、この第三の実施例の一つの代替として、ハッシュを、h(g^R_M mod p),(g^R_N mod p),(g^$R_M R_N$ mod p))に変更した場合は、アタッカは、これらハッシュと共に指数化（exponentiation）を行なう必要があるために（ハッシュの数と共にアタックの数が指数関数的に増加するために）、アタックに成功する可能性は著しく低下する。

【００３３】

第三の実施例に対するもう一つの代替として、移動機２０と網１０との間の通信の正当性を検証するために遂行されるハッシュに、移動機２０の識別番号を含めることもできる。

【００３４】

この第三の実施例のさらにもう一つの代替（つまり、本発明の第四の実施例）においては、図４においては移動機２０が最初に（g^R_M mod p）を網１０に送信したが、網１０から（g^R_N mod p）を受信した後に、これを送信する。第三の実施例においては、マンーインーザーミドルアタッカは、（g^R_M mod p）と（g^R_N mod p）の両方を知ることができ、こうして、誕生日アタックを行なうことが可能であったが、この第四の実施例では、アタッカは、移動機２０が（g^R_M mod p）にて応答する前に、（g^R_N mod p）をコミットする（解決して送信する）ことを必要とされ、このため、アタッカの自由度が１だけ低減される。

【００３５】

図５は、本発明の第五の実施例による網１０と移動機ユーザとの間の、電話／地上回線３０と移動機２０を介しての通信を図解する。図５に示すように、移動機ユーザは、最初に認証情報を電話／地上回線３０を介して網１０に供給する。上述のように、移動機２０は、この認証情報と共に、網１０が移動機２０と最初に連絡を取るのに十分な情報（例えば、移動機識別子等）を供給することもできる。網がその認証情報を受理した場合は、次に、初期化プロセスが以下のよう継続される。

【００３６】

この初期化プロセスは、移動機２０か網１０のいずれかが、初期化リクエストを他方に送信することで開始される。

【００３７】

例えば、移動機２０が初期化リクエストを送信した場合は、網は乱数R_Nを生成し、(g^R_N mod p)と(g^R_N mod p)のハッシュを計算し、h（g^R_N mod p） を移動機２０に送信する。移動機２０は、乱数R_Mを生成し、(g^$_R$M mod p)を計算し、(g^R_M mod p)を網１０に送信する。網１０は、これに応答して、(g^R_N mod p)を移動機２０に送信する。

【００３８】

次に、移動機２０は、受信された(g^R_N mod p)のハッシュを計算し、h(g^R_N mod p) のこの計算されたバージョンが、網１０から最初に受信されたバージョンと等しいか検証する。等しいことが検証された場合は、初期化プロセスは、継続される。

【００３９】

すなわち、移動機２０と網１０の両方が、h((g^R_M mod p),(g^R_N mod p))を遂行する。移動機２０は、ハッシュの結果を表示し、移動機ユーザは、電話／地上回線３０を介して、このハッシュの数字を網１０に供給する。

【００４０】

網１０が、供給されたハッシュと網１０によって遂行されたハッシュが一致することを見つけた場合は、通信は正当なものとして認証され、(g^$R_M R_N$ mod p)、このハッシュ、あるいはこの一部として、Ａ－キーが確立される。すなわち、移動機２０は、こうしてＡ－キーを確立するが、ただし、網１０は、そのハッシュが正当であるものと認証された場合にのみ、このＡ－キーを移動機２０と関連付ける。

【００４１】

上述のように、移動機２０が最初に初期化リクエストを送信する代わりに、網１０が最初に初期化リクエストを送信することもできる。網１０が最初に初期化リクエストを送信した場合は、移動機２０は、乱数R_Mを生成し、(g^R_M mod p)を計算し、(g^R_M mod p)のハッ

シュを計算し、h(g^R_M mod p)を網１０に送信する。網１０は、これに応答して、乱数R_Nを生成し、(g^R_N mod p)を計算し、(g^R_N mod p)を移動機２０に送信する。

【００４２】

次に、移動機２０が、(g^R_M mod p)を網１０に送信し、網１０は、(g^R_M mod p)のハッシュを計算する。次に、網１０は、h(g^R_M mod p) の計算されたバージョンが、移動機２０から最初に受信したバージョンと等しいか検証する。等しい場合は、初期化プロセスが以下のように継続される。

【００４３】

すなわち、移動機２０と網１０は、両方とも、h((g^R_N mod p),(g^R_M mod p))を遂行する。移動機２０が、ハッシュの結果を表示し、移動機のユーザは、電話／地上回線３０を介して、そのハッシュの数字を網１０に供給する。

【００４４】

網１０が、供給されたハッシュと網１０によって遂行されたハッシュが一致することを見つけた場合は、通信は正当なものとして認証され、(g^$R_M R_N$ mod p)、このハッシュ、あるいはこの一部としてＡ－キーが確立される。すなわち、移動機２０は、こうしてＡ－キーを確立するが、ただし、網１０は、そのハッシュが正当であるものと認証された場合にのみ、このＡ－キーを移動機２０と関連付ける。

【００４５】

さらにもう一つの代替として、移動機２０と網１０との間の通信を検証するために遂行される最後のハッシュに移動機２０の識別番号を含めることもできる。この方式では、マン－イン－ザ－ミドルアタッカは、誕生日タイプのアタックを行なうことはできない。つまり、アタッカは、網１０のふりをするときは、アタッカが使用している指数を（そのハッシュを介して）、アタッカが移動機ユーザの指数（exponential）を見つける前にコミットする（解読して送信する）ことを必要とされ、同様に、アタッカは、移動機２０のふりをするときは、そのハッシュと関連する網の指数の値を見つけだす前にその指数をコミットする（解読して送信する）ことを必要とされる。

【００４６】

本発明の幾つかの実施例においては、素数ｐと、ジェネレータｇは、固定されており、移動機２０内に事前に格納されているものと想定されが、ただし、このようにしない場合は、アタッカは、ｇとｐを、ｇ’とｐ’と取り替え、アタッカは、これにより、この離散アルゴリズムを効率的に計算することが可能となる。このため、ｇとｐも空中伝送される場合は、アタッカによってｇとｐを取り替えられることを阻止するために、これらも、ハッシュ計算、すなわち、h((g,p,(g^R_M mod p),(g^R_N mod p))の一部として用いる必要がある。

【００４７】

さらに、上述の各実施例は、電話／地上回線３０を用いるものとして説明されたが、電話／地上回線３０の代わりに、他の形式の安全な（機密）通信を用いることもできる。例えば、電話／地上回線３０の代わりに既に起動されている移動機を用いることもできる。別の方法として、電話／地上回線上のそれほど機密を要さない通信は移動機２０と網１０の間の音声チャネルを用いて遂行し、機密を要する残りの通信は、移動機２０と網１０との間の制御チャネルを用いて遂行することもできる。

【００４８】

本発明がこうして説明されたが、明らかなように、本発明は、様々な修正された形態にて実現することもでき、これらバリエーションも、本発明の精神および範囲から逸脱するものと見做されるべきではなく、これら全ての修正が特許請求の範囲に含まれるものである。

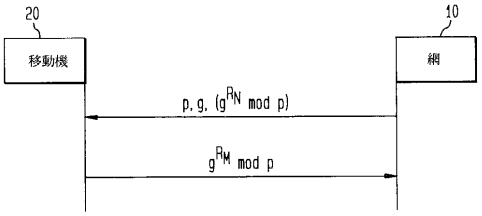
【図面の簡単な説明】

【図１】　Diffe-Hellmanキー合意による網と移動機の間の通信を示す図である。

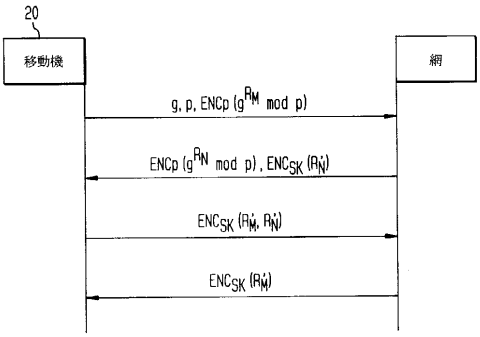
【図２】　Diffe-Hellman Encrypted Key Exchange（EKE）プロトコルによる網と移動機の間の通信を示す図である。

【図３】本発明の第一の実施例による網と移動機ユーザとの間の電話／地上回線と移動機を介しての通信を示す図である。
【図４】本発明の第二の実施例による網と移動機ユーザとの間の電話／地上回線と移動機を介しての通信を示す図である。
【図５】本発明の第二の実施例による網と移動機ユーザとの間の電話／地上回線と移動機を介しての通信を示す図である。
【符号の説明】
１０　網プロバイダ／網
２０　移動機
３０　電話／地上回線

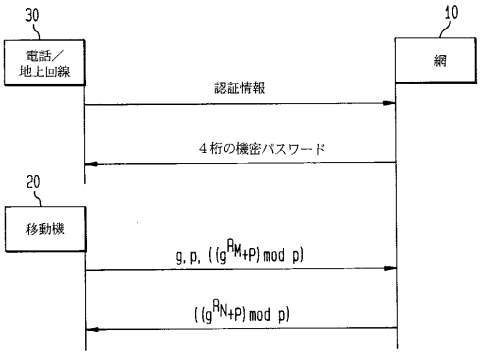
【図１】



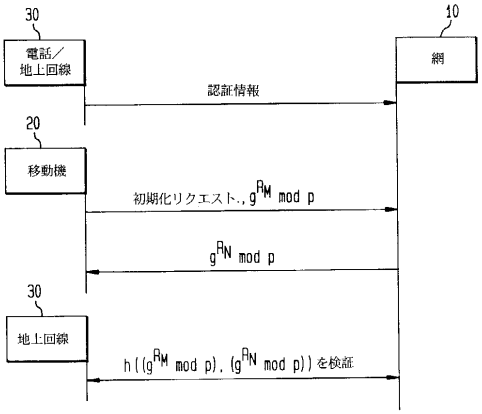
【図２】



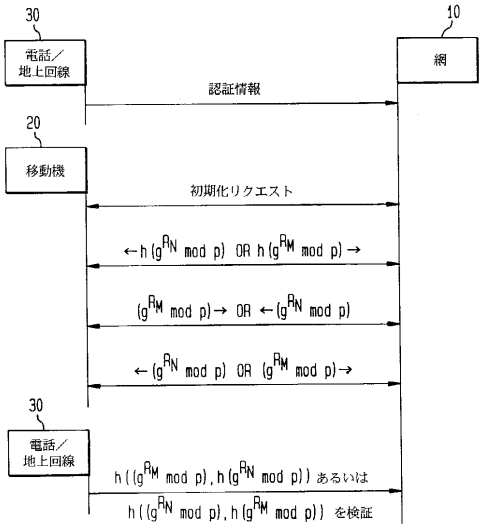
【図３】



【図４】



【図５】


30
電話／
地上回線
10
網
認証情報
20
移動機
初期化リクエスト
←h(g^RN mod p) OR h(g^RM mod p)→
(g^RM mod p)→ OR ←(g^RN mod p)
←(g^RN mod p) OR (g^RM mod p)→
30
電話／
地上回線
h{(g^RM mod p), h(g^RN mod p)} あるいは
h{(g^RN mod p), h(g^RM mod p)} を検証

フロントページの続き

(74)代理人 100101498
弁理士 越智 隆夫
(74)代理人 100096688
弁理士 本宮 照久
(74)代理人 100104352
弁理士 朝日 伸光
(72)発明者 アダム エル．ベレンズウェグ
アメリカ合衆国 １０００３ ニューヨーク，ニューヨーク，イースト ツェルヴス ストリート ７０
(72)発明者 サーヴァー パテル
アメリカ合衆国 ０７０４５ ニュージャーシィ，モンヴィル，ミラー レーン ３４

合議体
審判長 吉岡 浩
審判官 相崎 裕恒
審判官 桑江 晃

(56)参考文献 国際公開第９６／３２７９１（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/06