

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4679903号
(P4679903)

(45) 発行日 平成23年5月11日 (2011.5.11)

(24) 登録日 平成23年2月10日 (2011.2.10)

(51) Int.Cl.

F I

G 0 6 F 21/22 (2006.01)
H 0 4 N 7/167 (2011.01)G 0 6 F 9/06 6 6 0 J
H 0 4 N 7/167 Z

請求項の数 17 (全 19 頁)

(21) 出願番号	特願2004-568138 (P2004-568138)	(73) 特許権者	505272124
(86) (22) 出願日	平成15年12月3日 (2003.12.3)		ロジウェイズ・フランス
(65) 公表番号	特表2006-513511 (P2006-513511A)		フランス国エフー１９１００ プリヴ・ラ
(43) 公表日	平成18年4月20日 (2006.4.20)		・ガイヤール, リュ・ダニエル・ドゥ・コ
(86) 国際出願番号	PCT/FR2003/003578		スナック １５
(87) 国際公開番号	W02004/073307	(74) 代理人	100089705
(87) 国際公開日	平成16年8月26日 (2004.8.26)		弁理士 社本 一夫
審査請求日	平成18年11月27日 (2006.11.27)	(74) 代理人	100076691
(31) 優先権主張番号	03/00525		弁理士 増井 忠武
(32) 優先日	平成15年1月17日 (2003.1.17)	(74) 代理人	100075270
(33) 優先権主張国	フランス (FR)		弁理士 小林 泰
		(74) 代理人	100080137
			弁理士 千葉 昭男
		(74) 代理人	100096013
			弁理士 富田 博行

最終頁に続く

(54) 【発明の名称】 暗号化／暗号解読モジュールへ送信された少なくとも１つのソフトウェア・プログラムのインテグリティを保証する方法及びシステム、及び該方法を実行するための記録媒体

(57) 【特許請求の範囲】

【請求項 1】

少なくとも１つの暗号化／暗号解読モジュールにより実行されることができるとも１つのコンピュータ・ソフトウェア・プログラムのインテグリティを保証する方法であって、前記少なくとも１つのコンピュータ・ソフトウェア・プログラムは、情報信号を不正に暗号解読しようとする不正なプログラムが動作することを妨げることを意図したものであり、前記少なくとも１つのコンピュータ・ソフトウェア・プログラムが、前記少なくとも１つの暗号化／暗号解読モジュールを装備したデコーダへ、送信機により長距離情報伝送ネットワークを介して送信されるものであり、

前記送信機が、

a) 制御ワードを用いて情報信号を暗号化し、前記情報信号を前記デコーダへ送信するステップ（４０）と、

b) 前記デコーダの前記少なくとも１つの暗号化／暗号解読モジュールへ、前記ステップ a) で送信される前記情報信号を前記デコーダが暗号解読するために必要とされる前記制御ワードを含むメッセージを、送信するステップ（５０）と、

c) 前記少なくとも１つのコンピュータ・ソフトウェア・プログラムを、前記デコーダの前記少なくとも１つの暗号化／暗号解読モジュールへ送信するステップ（４２、１００）と、

を実行し、

前記デコーダが、

10

20

d) 前記ステップ b) において送信されたメッセージの中に暗号解読の目的のために備えられた前記制御ワードを用いて、前記ステップ a) において前記送信機により送信された前記情報信号を暗号解読するステップ (74)

を実行するものであり、

前記送信機が、

e) 前記ステップ c) において送信される前記コンピュータ・ソフトウェア・プログラムの第 1 の識別子を構築するステップ (44、122) であって、送信された前記コンピュータ・ソフトウェア・プログラムのチェックサムを計算し、前記チェックサムにより前記第 1 の識別子が形成されるものである、構築するステップと、

f) 前記識別子を、前記ステップ b) において送信される前記メッセージに挿入するステップ (52、124) と、

を実行し、

前記少なくとも 1 つの暗号化／暗号解読モジュールが、

g) 前記コンピュータ・ソフトウェア・プログラムの前記識別子を、受信された前記コンピュータ・ソフトウェア・プログラムに基づいて再構築するステップ (62、110) であって、この再構築は、前記ステップ e) における前記識別子の構築と同様の様式で実現されるものであり、受信された前記コンピュータ・ソフトウェア・プログラムのチェックサムを計算し、前記チェックサムにより前記識別子が形成されるものである、再構築するステップと、

h) 前記ステップ g) で再構築された前記識別子と、前記ステップ f) において前記送信機により挿入された前記識別子と比較するステップ (66、112) と、

i) 前記ステップ g) で再構築された前記識別子が、前記ステップ b) で送信されたメッセージの中に前記ステップ f) で挿入された前記識別子と対応しない場合、前記ステップ d) を阻止するステップ (68、108) と、

j) 前記ステップ g) で再構築された前記識別子が、前記ステップ b) において送信されたメッセージの中に前記ステップ f) で挿入された前記識別子と対応する場合、前記コンピュータ・ソフトウェア・プログラムのインテグリティを有効と認めるステップ (66、112) と

を実行する、

ことを特徴とする方法。

【請求項 2】

請求項 1 に記載の方法であって、前記送信機が、前記ステップ b) で前記メッセージが送信される前に前記メッセージを暗号化する (50 において) ことと、前記少なくとも 1 つの暗号化／暗号解読モジュールが、前記ステップ d) を実行することを可能にするために前記ステップ b) において送信された前記メッセージを暗号解読することと、を特徴とする方法。

【請求項 3】

それぞれが前記少なくとも 1 つの暗号化／暗号解読モジュールにより実行されることができ複数のコンピュータ・ソフトウェア・プログラムのインテグリティを保証するための請求項 1 または 2 に記載の方法であって、

前記ステップ e) が、前記ステップ c) において送信される全ての前記コンピュータ・ソフトウェア・プログラムに基づいて一意の識別子を構築するための動作 (44) であって、送信されたそれぞれの前記コンピュータ・ソフトウェアのチェックサムを計算し、全ての前記チェックサムを、前記チェックサムの間で排他的論理和の演算を行うことにより組み合わせることにより、前記一意の識別子を構築するための動作を備え、

前記ステップ g) が、一意の識別子を再構築するために、前記ステップ e) において実行される動作と同様の動作を実行するステップからなるものであって、前記デコーダにより受信されたそれぞれの前記コンピュータ・ソフトウェアのチェックサムを計算し、全ての前記チェックサムを、前記チェックサムの間で排他的論理和の演算を行うことにより組み合わせることにより、前記一意の識別子を再構築するものであり、再構築された前記一

10

20

30

40

50

意の識別子は、前記デコーダにより受信された前記コンピュータ・ソフトウェア・プログラムが、前記送信機により送信された前記コンピュータ・ソフトウェア・プログラムと同じである場合に、前記ステップ e) において構築された一意の識別子に対応するものである、

ことを特徴とする方法。

【請求項 4】

請求項 3 に記載の方法であって、前記ステップ d)、g)、h)、i) 及び j) が同じ暗号化／暗号解読モジュールにより実行されることを特徴とする方法。

【請求項 5】

請求項 3 に記載の方法であって、第 1 の自律型の暗号化／暗号解読モジュールが、前記ステップ d)、h)、i) 及び j) のみを実行し、

前記第 1 の自律型の暗号化／暗号解読モジュールから独立しており且つ前記デコーダに固定して連結される第 2 の自律型の暗号化／暗号解読モジュールが、少なくとも前記ステップ g) を実行する

ことを特徴とする方法。

【請求項 6】

請求項 5 に記載の方法であって、前記送信機が更に、

k) 前記ステップ c) において送信される前記コンピュータ・ソフトウェア・プログラムの第 2 の識別子を構築する第 2 のステップ (120) であって、送信された前記コンピュータ・ソフトウェア・プログラムのチェックサムを計算し、前記チェックサムにより前記第 2 の識別子が形成されるものである、第 2 のステップを備え、前記第 2 の識別子が前記ステップ c) において対応する前記ソフトウェア・プログラムと一緒に送信されるものであり、

前記第 2 の暗号化／暗号解読モジュールにより実行される前記ステップ g) が、

前記ソフトウェア・プログラムと一緒に送信される前記第 2 の識別子を再構築するための動作 (102) であって、受信された前記コンピュータ・ソフトウェア・プログラムのチェックサムを計算し、前記チェックサムにより前記第 2 の識別子が形成されるものである、再構築するための動作と、

再構築された前記第 2 の識別子が、前記ステップ c) において前記ソフトウェア・プログラムと一緒に送信された前記第 2 の識別子に対応する場合のみ、前記ステップ b) において送信される前記メッセージに挿入された前記第 1 の識別子を再構築し (110)、再構築された前記第 1 の識別子を前記第 1 の暗号化／暗号解読モジュールへ送信して、前記第 1 の暗号化／暗号解読モジュールが前記ステップ h) を実行できるようにするための動作と

を備え、

前記第 1 の識別子を再構築することは、前記ステップ k) における前記識別子の構築と同様の様式で実現される、

ことを特徴とする方法。

【請求項 7】

請求項 6 に記載の方法であって、前記第 1 の識別子及び前記第 2 の識別子は、それぞれに異なる第 1 の暗号化キー及び第 2 の暗号化キーを用いて前記コンピュータ・ソフトウェア・プログラムの同じ識別子を暗号化することにより、該同じ識別子から得られる、ことを特徴とする方法。

【請求項 8】

請求項 1 ないし 7 の何れかに記載の方法であって、前記少なくとも 1 つの暗号化／暗号解読モジュールが、前記ステップ j) において、前記少なくとも 1 つのコンピュータ・ソフトウェア・プログラムのインテグリティが確認される度に、当該少なくとも 1 つのコンピュータ・ソフトウェア・プログラムを実行する、ことを特徴とする方法。

【請求項 9】

少なくとも 1 つのコンピュータ・ソフトウェア・プログラムを長距離情報伝送ネットワ

10

20

30

40

50

ークを介して送信するための請求項 1 に記載された送信機に次の各処理を実行させるプログラムを記録した情報記録媒体（12）であって、前記処理は、

制御ワードを用いて情報信号を暗号化する処理、

前記情報信号を送信する処理、

前記制御ワードを含むメッセージを送信する処理、

前記少なくとも 1 つのコンピュータ・ソフトウェア・プログラムを送信する処理、

前記コンピュータ・ソフトウェア・プログラムの第 1 の識別子を構築する処理であって、送信された前記コンピュータ・ソフトウェア・プログラムのチェックサムを計算し、前記チェックサムにより前記第 1 の識別子を形成するものである、構築する処理、および

前記識別子を、送信される前記メッセージに挿入する処理を含む、

情報記録媒体。

【請求項 10】

請求項 1 に記載された少なくとも 1 つの暗号化／暗号解読モジュールにより次の各処理を実行させるプログラムを記録した情報記録媒体（22、88）であって、前記処理は、

送信機により送信されたメッセージにおいて提供される暗号解読のための制御ワードを用いて、前記送信機により送信された情報信号を暗号解読する処理、

受信したコンピュータ・ソフトウェア・プログラムの識別子を再構築する処理であって、受信された前記コンピュータ・ソフトウェア・プログラムのチェックサムを計算し、前記チェックサムにより前記識別子が形成されるものである、再構築する処理、

再構築された前記識別子と、前記送信機により前記メッセージに挿入された識別子と比較する処理、

再構築された前記識別子が、前記メッセージへ挿入された前記識別子と対応しない場合、送信された前記情報信号の暗号解読を阻止する処理、および

再構築された前記識別子が、前記メッセージへ挿入された前記識別子と対応する場合、前記コンピュータ・ソフトウェア・プログラムのインテグリティを有効と認める処理を含む、

情報記録媒体。

【請求項 11】

少なくとも 1 つの暗号化／暗号解読モジュールにより実行されることができるとも 1 つのコンピュータ・ソフトウェア・プログラムのインテグリティを保証するシステムであって、前記少なくとも 1 つのコンピュータ・ソフトウェア・プログラムは、情報信号を不正に暗号解読しようとする不正なプログラムが動作することを妨げることを意図したものであり、前記少なくとも 1 つのコンピュータ・ソフトウェア・プログラムを長距離情報伝送ネットワーク（8）を介して送信する送信機（4）と、前記少なくとも 1 つの暗号化／暗号解読モジュール（16、84）を装備するデコーダ（6、82）とを備え、

前記送信機（4）が、

前記デコーダへ送信される情報信号を、制御ワードを用いて暗号化すること、

前記デコーダの前記少なくとも 1 つの暗号化／暗号解読モジュールへ、前記デコーダが送信された前記情報信号を暗号解読するため必要とする制御ワードを含むメッセージを送信すること、および

前記少なくとも 1 つのコンピュータ・ソフトウェア・プログラムを前記デコーダの前記少なくとも 1 つの暗号化／暗号解読モジュールへ送信することが可能であり、

前記デコーダ（6、82）が、暗号解読の目的のために与えられ且つ前記送信機により送信された前記メッセージに含まれている前記制御ワードを用いて、前記送信機により送信された前記情報信号を暗号解読することが可能であり、

前記送信機は、前記コンピュータ・ソフトウェア・プログラムの第 1 の識別子を構築するものであって、送信された前記コンピュータ・ソフトウェア・プログラムのチェックサムを計算し、前記チェックサムにより前記第 1 の識別子を形成するものであり、

10

20

30

40

50

前記送信機は、前記識別子を前記メッセージに挿入するものであり、

前記少なくとも1つの暗号化／暗号解読モジュールは、前記コンピュータ・ソフトウェア・プログラムの前記識別子を、受信された前記コンピュータ・ソフトウェア・プログラムに基づいて再構築するものであり、この再構築は、前記メッセージに挿入された前記識別子の構築と同様の様式で実現されるものであって、受信された前記コンピュータ・ソフトウェア・プログラムのチェックサムを計算し、前記チェックサムにより前記識別子が形成されるものであり、

前記少なくとも1つの暗号化／暗号解読モジュールは、再構築された前記識別子と、前記送信機により前記メッセージへ挿入された前記識別子とを比較し、

再構築された前記識別子が、送信された前記メッセージへ挿入された前記識別子と対応しない場合、前記少なくとも1つの暗号化／暗号解読モジュールは、送信された前記情報信号の暗号解読を阻止し、

再構築された前記識別子が、送信された前記メッセージへ挿入された前記識別子と対応する場合、前記少なくとも1つの暗号化／暗号解読モジュールは、前記コンピュータ・ソフトウェア・プログラムのインテグリティを有効と認める、

ことを特徴とするシステム。

【請求項12】

請求項11に記載のシステムであって、前記デコーダ(6)が1つの取り外し可能な暗号化／暗号解読モジュールを装備していることを特徴とするシステム。

【請求項13】

請求項11に記載のシステムであって、前記デコーダ(82)が、互いに独立した少なくとも2つの自律型の暗号化／暗号解読モジュールを装備しており、これらの自律型の暗号化／暗号解読モジュールのうちの少なくとも1つが、前記デコーダの本体に固定して連結されることを特徴とするシステム。

【請求項14】

請求項1ないし8の何れかに記載の方法を実行するのに適した送信機(4)であって、前記デコーダへ送信される情報信号を暗号化すること、

前記デコーダの前記少なくとも1つの暗号化／暗号解読モジュールへ、前記デコーダが送信された前記情報信号を暗号解読するために必要とされる前記制御ワードを含むメッセージを送信すること、および

前記少なくとも1つのコンピュータ・ソフトウェア・プログラムを前記デコーダの前記少なくとも1つの暗号化／暗号解読モジュールへ送信することが可能であり、

前記送信機は、前記コンピュータ・ソフトウェア・プログラムの第1の識別子を構築するものであって、送信された前記コンピュータ・ソフトウェア・プログラムのチェックサムを計算し、前記チェックサムにより前記第1の識別子が形成されるものであり、前記識別子は、前記少なくとも1つの暗号化／暗号解読モジュール(16、84)が前記コンピュータ・ソフトウェア・プログラムを受信したことを、前記少なくとも1つの暗号化／暗号解読モジュール(16、84)が確認することを可能にするものであり、

前記送信機は、前記識別子を前記メッセージに挿入することが可能である、
ことを特徴とする送信機。

【請求項15】

請求項1ないし8の何れかに記載の方法を実行するのに適したデコーダ(6、82)であって、暗号解読の目的のため与えられ且つ前記送信機により送信される前記メッセージに含まれている前記制御ワードを用いて、前記送信機により送信された前記情報信号を暗号解読することが可能であり、且つ前記少なくとも1つの暗号化／暗号解読モジュール(16、84)を装備しており、

前記少なくとも1つの暗号化／暗号解読モジュールは、前記コンピュータ・ソフトウェア・プログラムの前記識別子を、受信された前記コンピュータ・ソフトウェア・プログラムに基づいて再構築し

10

20

30

40

50

前記少なくとも1つの暗号化／暗号解読モジュールは、再構築された前記識別子と、前記送信機により前記メッセージへ挿入された前記識別子とを比較し、

再構築された前記識別子が、送信された前記メッセージへ挿入された前記識別子と対応しない場合、前記少なくとも1つの暗号化／暗号解読モジュールは、送信された前記情報信号の暗号解読を阻止し、

再構築された前記識別子が、送信された前記メッセージへ挿入された前記識別子と対応する場合、前記少なくとも1つの暗号化／暗号解読モジュールは、前記コンピュータ・ソフトウェア・プログラムのインテグリティを有効と認める、

ことを特徴とするデコーダ。

【請求項16】

10

請求項15に記載のデコーダであって、1つの取り外し可能な暗号化／暗号解読モジュールを装備していることを特徴とする、デコーダ。

【請求項17】

請求項15に記載のデコーダであって、互いに独立した少なくとも2つの自律型の暗号化／暗号解読モジュールを装備しており、該自律型の暗号化／暗号解読モジュールのうちの少なくとも1つが前記デコーダの本体に固定して結合されていることを特徴とするデコーダ。

【発明の詳細な説明】

【技術分野】

【0001】

20

本発明は、少なくとも1つの暗号化／暗号解読モジュールが実行することができる少なくとも1つのコンピュータ・ソフトウェア・プログラムであって、送信機により長距離情報伝送ネットワークを介して、少なくとも1つの暗号化／暗号解読モジュールを装備したデコーダへ送信される上記少なくとも1つのソフトウェア・プログラムのインテグリティを、保証する方法及びシステムに関する。

【0002】

より正確には、本発明は、

送信機が、

a) デコーダへ送信される情報信号を暗号化するステップと、

b) デコーダがステップa) で送信された情報信号を暗号解読するために必要とされる情報を含むメッセージを、デコーダの少なくとも1つの暗号化／暗号解読モジュールへ送信するステップと、

30

c) 少なくとも1つのコンピュータ・ソフトウェア・プログラムを、デコーダの少なくとも1つの暗号化／暗号解読モジュールへ送信するステップと
を実行し、

デコーダが、

d) ステップb) の間に送信されたメッセージの中に暗号解読の目的で備えられた情報を用いて、ステップa) の間に送信機により送信された情報信号を暗号解読するステップ
を実行する、

方法に関する。

40

【0003】

このタイプの方法は、例えば、テレビジョン・チャネルをブロードキャスト（放送）する支払いベース（payment-based）のシステムで必要とされる。これらのシステムにおいては、デコーダを更新するために、送信機は、デコーダの機能を更新するために、各デコーダにより実行されることを意図している補正ソフトウェア・プログラム（corrective software programs）を、頻繁にブロードキャストする。補正ソフトウェア・プログラムは、電子コンピュータにより実行されることができる小さいプログラムであって、そのコンピュータが実行することができる大きいプログラムの特定のパラメータ又はパーツ（部品）を変更することを意図している小さいプログラムである。これらの補正ソフトウェア・プログラムはまた、英語では「patch（

50

パッチ)」として知られている。

【背景技術】

【0004】

従来の様式では、各デコーダは、送信されたテレビジョン・チャンネルを暗号解読するために、送信機により送信された信号を暗号化及び／又は暗号解読することができる暗号化／暗号解読モジュールを装備している。このモジュールは、送信機とデコーダとの間の情報交換をセキュアに行うように働くので、通常、セキュリティ・モジュールと呼ばれる。この暗号化／暗号解読モジュールはまた、それが受信する補正ソフトウェア・プログラムを実行することができる。

【0005】

暗号化／暗号解読モジュールは、自律型モジュールの形式である。例えば、この暗号化／暗号解読モジュールは、今日では、デコーダが正しく機能するようにデコーダへ挿入されねばならないチップ・カードに集積化されている。

【0006】

今日、支払いベースのテレビジョン・チャンネルを、支払いを行わずに受信するため不正に構築された多数のデコーダが存在する。これらのデコーダは海賊デコーダと呼ばれている。受信された信号の暗号化／暗号解読部分は最も複雑なので、これらの海賊デコーダは、多くの場合、真性の(a u t h e n t i c)暗号化／暗号解読モジュールを組み込み、このモジュールを制御するためにこのモジュールに不正の装置が関連付けられる。不正の制御装置は、真性の暗号化／暗号解読モジュールが支払いベースのテレビジョン・チャンネルを暗号解読するため必要とする情報を、たとえその情報が不正に獲得されたものであっても、当該真性の暗号化／暗号解読モジュールへ送信する。

【0007】

このタイプの海賊デコーダと戦うための解決策は、以前は、アンチパイレート（海賊防止）プログラムと呼ばれる特別の補正ソフトウェア・プログラムを、送信機を介してブロードキャストすることであった。これらのアンチパイレート補正ソフトウェア・プログラムは、真性の暗号化／暗号解読モジュールの動作を変更して、海賊デコーダを全体として使用不能にすることを意図している。アンチパイレート補正ソフトウェア・プログラムは、それが真性の暗号化／暗号解読モジュールにより実行された後に、例えば、真性の暗号化／暗号解読モジュールにより暗号解読された情報が格納されるメモリ・ゾーンの位置を変更したり、また、別のメモリ位置においてテレビジョン・チャンネルを暗号解読するため必要とされる情報を探そうにできる。

【0008】

しかしながら、最近の海賊デコーダは、今では、アンチパイレート補正ソフトウェア・プログラムが真性の暗号化／暗号解読モジュールにより受信される前に取り除くことができる。その場合、アンチパイレート補正ソフトウェア・プログラムは、真性の暗号化／暗号解読モジュールにより実行されない。

【発明の開示】

【発明が解決しようとする課題】

【0009】

本発明の目的は、デコーダへ送信されたソフトウェア・プログラムを取り除くことをより難しくする方法を提供することにより、上記の欠点を克服することにある。

【課題を解決するための手段】

【0010】

従って、本発明の主題は、前述した方法であって、

－送信機が、ステップc)で送信されたコンピュータ・ソフトウェア・プログラムを少なくとも1つの暗号化／暗号解読モジュールが有効に受信したことを少なくとも1つの暗号化／暗号解読モジュールが検証することを可能にする追加の情報項目を、ステップb)の間に送信されるメッセージに挿入すること、

－少なくとも1つの暗号化／暗号解読モジュールが、ステップb)の間に送信されたメ

10

20

30

40

50

ッセージの中へ前記送信機により挿入された追加の情報に基づいて、ステップc)の間に送信されたソフトウェア・プログラムを有効に受信したかどうかを検証すること、およびソフトウェア・プログラムが受信されていなかった場合、少なくとも1つの暗号化／暗号解読モジュールがステップd)を阻止すること
を特徴とする方法である。

【0011】

上記の方法においては、デコーダに装備された真性の暗号化／暗号解読モジュールは、送信機により送信された暗号化された情報信号を暗号解読するために必要とされる情報を含むメッセージを受信する。このメッセージは更に、送信機により送信された全ての補正ソフトウェア・プログラムが真性の暗号化／暗号解読モジュールへ通信されたことを当該真性の暗号化／暗号解読モジュールが検証することを可能にする情報を含む。

10

【0012】

従って、真性の暗号化／暗号解読モジュールが、ステップb)で送信されたメッセージに挿入された追加の情報から、補正ソフトウェア・プログラムが失われていることを検出した場合、この真性の暗号化／暗号解読モジュールは、ステップa)の間に送信された情報を暗号解読することを阻止するように動作する。

【0013】

この方法は、ステップc)の間に送信される補正ソフトウェア・プログラムを取り除くことを一層困難にする。

海賊デコーダが、追加の情報を含むメッセージを通じて、送信された全ての補正ソフトウェア・プログラムの存在を検証することを可能にする場合、その情報は、真性の暗号化／暗号解読モジュールにより受信される。

20

【0014】

従って、暗号化／暗号解読モジュールは、補正ソフトウェア・プログラムの除去を検出することが可能であり、そして、それに応答して、ステップa)の間に送信された情報信号、例えば、テレビジョン・チャンネルの暗号解読を、阻止する。

【0015】

従って、海賊デコーダが、追加の情報を許可する場合、ステップc)の間に送信される全ての補正ソフトウェア・プログラムを許可しなければならない。

更に、海賊デコーダはまた、ステップb)の間に送信された追加情報を含むメッセージを取り除くために簡単に変更されることができない。このメッセージはまた、ステップa)の間に送信された信号を暗号解読するため必要とされる情報を含む。従って、このメッセージが取り除かれるならば、ステップa)の間に送信された情報信号を暗号解読することが不可能である。

30

【0016】

従って、このタイプの方法により、海賊デコーダは、受信された特定の情報メッセージや補正ソフトウェア・プログラムを簡単に取り除くにはもはや十分なものではなく、また、海賊デコーダは、ステップb)の間に送信されたメッセージのコンテンツ(内容)へのアクセスを行う必要があり、それは、受信された特定のメッセージを純粹に且つ単純に取り除くことよりも極めて複雑なことである。

40

【0017】

本発明による方法の他の特徴によると、

—送信機が、ステップb)で送信されるメッセージを暗号化し、少なくとも1つの暗号化／暗号解読モジュールが、ステップb)の間に送信されたメッセージを暗号解読して、ステップd)を実行することを可能にし、

—送信機が、

e)ステップc)の間に送信されるコンピュータ・ソフトウェア・プログラムの第1の識別子を構築するステップと、

f)この識別子をステップb)の間に送信されるメッセージに挿入するステップと
を実行し、

50

少なくとも1つの暗号化／暗号解読モジュールが、

g) コンピュータ・ソフトウェア・プログラムの識別子を、受信されたコンピュータ・ソフトウェア・プログラムに基づいて再構築するステップと、

h) ステップg) で再構築された識別子と、ステップf) の間に送信機により挿入された識別子とを比較するステップと、

i) ステップg) で再構築された識別子が、ステップb) で送信されたメッセージの中にステップf) で挿入された識別子に対応しない場合、ステップd) を阻止するステップと、

j) ステップg) で再構築された識別子が、ステップb) の間に送信されたメッセージの中にステップf) で挿入された識別子に対応する場合、コンピュータ・ソフトウェア・プログラムのインテグリティを有効とするステップと、
を実行する。

10

【0018】

－それぞれが少なくとも1つの暗号化／暗号解読モジュールにより実行されることができ、幾つかのコンピュータ・ソフトウェア・プログラムのグループのインテグリティを保証するために、ステップe) は、ステップc) の間に送信される幾つかのコンピュータ・ソフトウェア・プログラムのグループのための単一の識別子を、そのグループの各ソフトウェア・プログラムに関連する情報に基づいて構築するための動作を含み、そして、ステップg) は、デコーダにより受信されたグループが、送信機により送信されたグループと同じである場合に、ステップe) の間に構築された識別子に対応する一意の識別子を再構築するために、ステップe) の間に実行される動作と同じ動作を実行することを含む。

20

【0019】

－ステップd)、g)、h)、i) 及びj) は、同じ暗号化／暗号解読モジュールにより実行される。

－第1の自律型暗号化／暗号解読モジュールが、ステップd)、h)、i) 及びj) のみを実行し、第1の自律型暗号化／暗号解読モジュールから独立しており且つデコーダに固定的に連結される第2の自律型暗号化／暗号解読モジュールが、少なくともステップg) を実行する。

【0020】

－送信機が更に、

30

k) ステップc) の間に送信される前記コンピュータ・ソフトウェア・プログラムの第2の識別子を構築する第2のステップを実行するものであり、この第2の識別子は、ステップc) の間に、対応するソフトウェア・プログラムと共に送信されるものであり、

－第2の暗号化／暗号解読モジュールにより実行されるステップg) が、

－ソフトウェア・プログラムと共に送信される第2の識別子を再構築するための動作と

、
－再構築された第2の識別子が、ステップc) の間にソフトウェア・プログラムと共に送信された第2の識別子に対応する場合のみ、ステップb) の間に送信されるメッセージに挿入された前記第1の識別子を再構築し、且つこの再構築された第1の識別子を第1の暗号化／暗号解読モジュールへ送信するための動作とを備え、それにより第1の暗号化／暗号解読モジュールがステップh) を実行できるようにする。

40

【0021】

－第1及び第2の識別子は、コンピュータ・ソフトウェア・プログラムの同じ識別子から、異なる第1及び第2の暗号化キーをそれぞれ用いてその同じ識別子を暗号化することにより、得られる。

【0022】

－少なくとも1つの暗号化／暗号解読モジュールが、ステップj) の間に、少なくとも1つのコンピュータ・ソフトウェア・プログラムのインテグリティが確認される度に、前記コンピュータ・ソフトウェア・プログラムを実行する。

【0023】

50

本発明はまた、本発明に従った方法を実行するための命令を備える情報記録媒体であって、その命令が送信機により実行される、情報記録媒体に関する。

本発明はまた、本発明に従った方法を実行するための命令を備える情報記録媒体であって、その命令が少なくとも1つの暗号化／暗号解読モジュールにより実行される、情報記録媒体に関する。

【0024】

本発明はまた、少なくとも1つの暗号化／暗号解読モジュールにより実行されることが
できる少なくとも1つのコンピュータ・ソフトウェア・プログラムのインテグリティを保
証するシステムであって、このシステムは、少なくとも1つのコンピュータ・ソフトウ
ェア・プログラムを長距離情報伝送ネットワークを介して送信する送信機と、少なく
とも1つの暗号化／暗号解読モジュールを装備するデコーダとを備え、

10

送信機は、

ー前記デコーダへ送信される情報信号を暗号化することと、

ー送信された情報信号をデコーダが暗号解読するために必要とされる情報を含むメ
ッセージを、デコーダの前記少なくとも1つの暗号化／暗号解読モジュールへ送信すること
と、

ー少なくとも1つのコンピュータ・ソフトウェア・プログラムを、デコーダの少なく
とも1つの暗号化／暗号解読モジュールへ送信することと
が可能であり、

ーデコーダは、暗号解読の目的のために備えられるものであり且つ送信機により送信
されたメッセージに含まれるものである情報を用いて、送信機により送信された情報信号
を暗号解読することが可能であり、

20

ー送信機が、送信されたコンピュータ・ソフトウェア・プログラムを少なくとも1つの
暗号化／暗号解読モジュールが受信したことを該暗号化／暗号解読モジュールが検証す
ることを可能にする追加の情報項目を、メッセージに挿入することが可能であり、

ー少なくとも1つの暗号化／暗号解読モジュールが、送信機によりメッセージへ挿入
された追加の情報に基づいて、送信機により送信されたソフトウェア・プログラムをその
暗号化／暗号解読モジュールが有効に受信したかどうかを検証することが可能であり、

ーソフトウェア・プログラムが受信されていなかった場合、少なくとも1つの暗号化／
暗号解読モジュールが、送信された情報信号の暗号解読を阻止することが可能である、
ことを特徴とする。

30

【0025】

本発明によるシステムの他の特徴によると、

ーデコーダが、一つの取り外し可能な暗号化／暗号解読モジュールを装備しており、

ーデコーダが、互いに独立した少なくとも2つの自律型暗号化／暗号解読モジュールを
装備しており、これらの暗号化／暗号解読モジュールの少なくとも1つがデコーダの本体
に固定的に連結される。

【0026】

本発明は、純粋に例として示された以下の記載を図面を参照して読めば、一層良く理解
されるであろう。

40

【発明を実施するための最良の形態】

【0027】

図1は、テレビジョン・チャンネルを送信するための支払いベースのシステムを示す。こ
のシステムを全体的に参照番号2で示す。テレビジョン・チャンネルを送信するための支
払いベースのシステムは知られている。従って、ここでは、本発明の理解に必要な特徴のみ
を詳細に説明する。

【0028】

システム2は、暗号化されたテレビジョン・チャンネルのための送信機4と、これらのテ
レビジョン・チャンネルを暗号解読することができるデコーダ6と、送信機4をデコーダ6
に接続する長距離情報伝送ネットワーク8とを備える。このネットワーク8は、典型的に

50

は無線ネットワークである。

【0029】

送信機4は、暗号化された情報信号と、情報信号を暗号解読するために必要とされる情報を含むコード化されたメッセージと、暗号化されていない補正ソフトウェア・プログラムとを、ネットワーク8を介して、システム2の全てのデコーダ6へブロードキャストすることができる。暗号化された情報信号は、この場合、制御ワードを用いてスクランブルされているテレビジョン・チャンネルに対応するものであり、この制御ワードは、これらのテレビジョン・チャンネルを暗号解読又はアンスクランブル(unscramble)するために必要とされる情報を形成する。このために、送信機4は、ブロードキャスト・テレビジョン・チャンネルをスクランブルする動作と、そのテレビジョン・チャンネルをスクランブルするために用いられる制御ワードを含むメッセージを符号化する動作とを実行することが可能であるユニット10を備える。

10

【0030】

この例では、ユニット10は、この例ではメモリ12である情報記録媒体に記録されている命令を実行することが可能である従来のプログラム可能なコンピュータに基づいて、作成される。

【0031】

メモリ12は、図2の方法を実行するための命令を備え、それらの命令はユニット10により実行される。更に、このメモリ12は、図2の方法を実行するために必要とされる暗号化キー及び制御ワード(1または複数)を備える。

20

【0032】

デコーダ6は、すべて、送信機4により送信されたテレビジョン信号を、その送信機4により送信されたメッセージに含まれた情報を用いて、暗号解読又はアンスクランブルすることができる。

【0033】

即ち、これら全てのデコーダ6が類似の機能を実行するので、説明を単純にするために、これらのデコーダ6のうちの1つのみが図1に詳細に示されている。

デコーダ6は暗号化／暗号解読モジュール16を備え、この暗号化／暗号解読モジュール16は、送信機4により送信されたコード化されたメッセージを復号して、それから制御ワードを抽出し、それを、スクランブルされたテレビジョン・チャンネルをアンスクランブルするモジュール18へ送信することができる。

30

【0034】

暗号化／暗号解読モジュール16は、通常のプロプログラム可能コンピュータ20と、この例ではメモリ22で形成される記録媒体とを備える。コンピュータ20は、メモリ22に記録されている命令を実行することができる。この例では、メモリ22は、図2の方法を実行するための命令を備え、その命令はコンピュータ20により実行される。暗号化／暗号解読モジュール16は、取り外し可能である。このモジュールは、例えば、通常のチップ・カードに基づいて作成される。

【0035】

デコーダ6は、このデコーダ6によりアンスクランブルされたテレビジョン・チャンネルを表示することができるテレビジョン・セット26と関連している。

40

ここで、システム2の動作を、図2の方法を参照して説明する。

【0036】

送信機4は、情報を暗号化してシステム2の全てのデコーダへネットワーク8を介して送信するステップ36を実行する。送信機4によりデコーダ6へ送信される情報は、スクランブルされたテレビジョン・チャンネルと、デコーダがテレビジョン・チャンネルをアンスクランブルするために必要な情報と、場合によっては、デコーダ6を更新することを意図する補正ソフトウェア・プログラムとを備える。このようにして、ステップ36の間において、送信機4は、そのサブステップ40の間に、メモリ12に格納されている制御ワードを用いて、ブロードキャストされたテレビジョン・チャンネルをスクランブルする。

50

【0037】

同時に、送信機4は、サブステップ42の間に、コード化されていない、即ち、暗号化されていない補正ソフトウェア・プログラムを、デコーダ6へ送信する。これらの補正ソフトウェア・プログラムは、それぞれ、識別子CSと従来通りに関連付けられており、識別子CSは、それらを受信するデコーダが受信したそれぞれのソフトウェア・プログラムのインテグリティを検証することを可能にする。識別子CSは、例えば、この場合は「チェックサム」である。

【0038】

サブステップ42の間に、送信機4はまた、1つの送信機4により送信された複数の補正ソフトウェア・プログラムのうちの受信された1つの補正ソフトウェア・プログラムの存在しないこと又は変更のあることを、各デコーダ6が検出することを可能にする一意の識別子を構築する動作44を実行する。このために、例えば、送信機4は、それぞれの補正ソフトウェア・プログラムの全チェックサムを、排他的論理和（EXCLUSIVE OR）演算をそれぞれのチェックサムの間で実行することにより、組み合わせる。

【0039】

次いで、送信機4は、動作46の間に、例えばメモリ12に含まれている暗号化キー K_{CS} を用いて、動作44の間に構築された一意の識別子をコード化する。この一意の識別子のコード化は、ネットワーク8を介したその一意の識別子の送信をセキュアにすることを可能にする。なぜなら、暗号化キー K_{CS} に対応する暗号化キーを備えるデコーダのみが、この一意の識別子を復号することができるからである。

【0040】

この場合、それは、補正ソフトウェア・プログラム自体ではなく補正ソフトウェア・プログラムの伝送をセキュアにするためにコード化される一意の識別子である。なぜなら、この方が本方法をより高速化するからである。一意の識別子は、送信される補正ソフトウェア・プログラムのグループよりもサイズが小さいので、一意の識別子のコード化は極めて速く行われる。

【0041】

ステップ36の間に、送信機4はまた、暗号化キー K_{ECM} を用いてコード化された、アクセス権を制御するメッセージを送信するサブステップ50を実行する。このメッセージはまた、ECMメッセージ（Entitled Control Message（権利を与えられた制御メッセージ））と呼ばれる。ECMメッセージは、通常、サブステップ40の間に、送信されたテレビジョン信号をアンスクランブルするため必要とされる制御ワードを備える。

【0042】

この場合、サブステップ50の間に、送信機4は、動作46中にコード化された一意の識別子を動作52の間に挿入する。

ステップ60で、各デコーダは、送信機4によりネットワーク8を介して送信された情報を受信する。受信された全ての情報は暗号化／暗号解読モジュール16へ送信される。

【0043】

暗号化／暗号解読モジュール16は、動作62の間に、一意の識別子を、受信された全ての補正ソフトウェア・プログラムに基づいて再構築することにより、開始する。この動作62は、例えば、動作44と同じであり、従って、暗号化／暗号解読モジュール16により再構築された一意の識別子は、受信された全ての補正ソフトウェア・プログラムがサブステップ42の間に送信された補正ソフトウェア・プログラムと同じである場合、動作44の間に構築された一意の識別子と同じである。

【0044】

次いで、暗号化／暗号解読モジュール16は、送信機4により用いられる暗号化キーに対応する暗号化キー K_{ECM} を用いて、受信されたECMメッセージを復号する。

ひとたびECMメッセージが復号されると、暗号化／暗号解読モジュール16は、動作64の間にECMメッセージに含まれる一意の識別子を復号する。

【0045】

動作66の間に、暗号化／暗号解読モジュール16は、動作62の間に再構築された一意の識別子を、動作64の間に復号された一意の識別子と比較する。比較されたこれらの一意の識別子が、送信機4が様々な補正ソフトウェア・プログラムを送信することを何回か試みたにも拘わらず、同じでないとした場合には、暗号化／暗号解読モジュール16は、テレビジョン・チャンネルをアンスクランブルすることを阻止するステップ68を実行する。このために、例えば、暗号化／暗号解読モジュール16は、アンスクランブル・モジュール18へ、受信したECMメッセージに含まれる制御ワードを送信しないか、又は誤った制御ワードを送信する。

【0046】

さもなければ、即ち、比較された2つの識別子が一致する場合、暗号化／暗号解読モジュール16は、動作70の間に、受信された補正ソフトウェア・プログラムを実行し、動作72の間に、ECMメッセージに含まれる制御ワードをアンスクランブル・モジュール18へ送信し、アンスクランブル・モジュール18は動作74の間にテレビジョン・チャンネルをアンスクランブルする。

【0047】

このようにして、暗号化／暗号解読モジュール16が海賊デコーダに用いられ、海賊デコーダが、暗号化／暗号解読モジュール16へアンチパイレート補正ソフトウェア・プログラムが送信される前にそれを取り除く又は変更するものである場合、暗号化／暗号解読モジュール16は動作68を実行し、受信されたテレビジョン・チャンネルは正しくアンスクランブルされなくなる。

【0048】

図2の方法はまた、ネットワーク8に接続されている自身の送信機を持つ無節操な個人により、送信機4により送信された補正ソフトウェア・プログラムへ追加の補正ソフトウェア・プログラムを追加することを防止することに、注目すべきである。無節操な個人により追加されるこのタイプの追加の補正ソフトウェア・プログラムは、多くの場合、暗号化／暗号解読モジュール16を破壊すること又は動作不能にさせることを意図している。無節操な個人により追加されるこれらの補正ソフトウェア・プログラムは、コンピュータ・ウィルスの形であり得る。

【0049】

図2の方法において、補正ソフトウェア・プログラムの追加は、動作66の間の補正ソフトウェア・プログラムの除去又は変更と同じ要領で検出され、この追加された補正ソフトウェア・プログラムは実行されない。

【0050】

それ自体真性であるデコーダの真性の暗号化／暗号解読モジュール16と交換することが可能である変造されたチップ・カードが現在存在することが、注目されている。

変造されたチップ・カードを装着されているこのタイプの真性のデコーダは、たとえ図2に従った方法を実行することによっても、使用不能にすることができない。なぜなら、変造されたチップ・カードは動作62かないし68を実行しないからである。図3を参照して説明される第2の実施形態は、この欠点を克服することを意図して図1のシステムを改善したものである。

【0051】

この第2の実施形態において、送信機は、図1の送信機4とは、メモリ12が図4の方法を実行するための命令を備える点が異なり、それらの命令は、この送信機の暗号化／暗号解読モジュールにより実行され、デコーダ6はデコーダ82により置換されている。

【0052】

デコーダ82は、第2の暗号化／暗号解読モジュール84を備えることを除いて、デコーダ6と構造的に同じである。

暗号化／暗号解読モジュール84は暗号化／暗号解読モジュール16と類似であり、メモリ88と関連するコンピュータ86を備える。

10

20

30

40

50

【0053】

しかしながら、暗号化／暗号解読モジュール16とは対照的に、暗号化／暗号解読モジュール84は、デコーダの本体に固定的に連結され、この暗号化／暗号解読モジュール84をデコーダ82から取り外そうとすると、デコーダ82が破壊される。

【0054】

このために、例えば、暗号化／暗号解読モジュール84は、デコーダ82の動作に必要とされる電子部品の内部に統合される。

メモリ88及び22は図4の方法を実行するための命令を備え、それらの命令は、それぞれ、コンピュータ86及び20により実行される。

【0055】

他の構成要素は図1のものと同一であり、同じ参照番号を有する。

ここで、この第2の実施形態の動作を、図4の方法を参照して説明する。

図4の方法は、図2の方法とは、サブステップ42及び動作62がサブステップ100及び動作102ないし114によりそれぞれ置換される点で、実質的に異なる。

【0056】

送信機4は、サブステップ100の間に1又はそれより多くの補正ソフトウェア・プログラムをデコーダ82へ送信する。

送信される又は送信されるべきそれぞれの補正ソフトウェア・プログラムについて、送信機4は、動作120の間に送信される補正ソフトウェア・プログラムの第1の識別子を構築し、動作122の間にこの同じ補正ソフトウェア・プログラムに対して第2の識別子を構築する。この場合、動作120の間に、送信機4は、通常的要領で、送信される補正ソフトウェア・プログラムの電子署名を計算し、次いで暗号化キー K_{MS} を用いてこの電子署名をコード化する。

【0057】

サブステップ42を参照して説明した要領と類似の要領で、この署名は、送信された補正ソフトウェア・プログラムを識別することを可能にし、そしてコード化は、補正ソフトウェア・プログラムの送信をセキュアにする。

【0058】

動作122の間に、送信機は、送信されるべき補正ソフトウェア・プログラムの第2の識別子を構築するが、この構築は、電子署名が暗号化キー K_{MS} を用いてコード化される前に暗号化キー K_{CS} を用いて動作120の間に計算された当該電子署名をコード化することによりなされる。

【0059】

動作120の間に計算された電子署名が随伴するそれぞれの補正ソフトウェア・プログラムは、サブステップ100の終わりにデコーダ82へ送信される。

この場合、送信されるECMメッセージへ一意の識別子を挿入する動作52が、動作122の間にそれぞれの補正ソフトウェア・プログラムに対して計算された第2の識別子をこのECMメッセージに挿入する動作124に置換される。

【0060】

従って、この第2の実施形態においては、ECMメッセージは1個の一意の識別子を備えずに、代わりに、送信される補正ソフトウェア・プログラムの数と同じ数の第2の識別子を備える。

【0061】

送信機4により送信される情報がデコーダ82により受信されたとき、暗号化／暗号解読モジュール84は、動作102の間に、受信されたそれぞれの補正ソフトウェア・プログラムに対する第1の識別子を再構築する。このために、デコーダ82は、動作120の間に用いたアルゴリズムと同じものを用いて、受信された補正ソフトウェア・プログラムの電子署名を計算する。

【0062】

従って、受信された補正ソフトウェア・プログラムが、送信機4により送信されたもの

10

20

30

40

50

と同じである場合、再構築された署名は、動作 1 2 0 の間に暗号化キー K_{MS} を用いてコード化されたものと同じである。

【0063】

次いで、暗号化／暗号解読モジュール 8 4 は、受信される補正ソフトウェア・プログラムと一緒にサブステップ 1 0 0 の間に送信される電子署名を、動作 1 0 4 の間に暗号解読する。

【0064】

次いで、暗号化／暗号解読モジュール 8 4 は、動作 1 0 6 の間に、動作 1 0 2 の間に再構築された電子署名を、動作 1 0 4 の間に復号された電子署名と比較する。再構築された電子署名と復号された電子署名とが一致しない場合、暗号化／暗号解読モジュール 8 4 は、動作 1 0 8 の間に、この補正ソフトウェア・プログラムの処理を中断する。

10

【0065】

さもなければ、即ち、これら電子署名が一致する場合、暗号化／暗号解読モジュール 8 4 は、動作 1 1 0 の間に、受信されたこの補正ソフトウェア・プログラムの第 2 の識別子を再構築する。典型的には、この動作 1 1 0 は、動作 1 0 2 の間又は動作 1 0 4 の間に得られた電子署名に適応される動作 1 2 2 と同じである。

【0066】

その後、暗号化／暗号解読モジュール 8 4 は、ECM メッセージを復号して、それから、受信された補正ソフトウェア・プログラムに対応する第 2 の識別子を抽出する。次いで、暗号化／暗号解読モジュール 8 4 は、動作 1 1 2 の間に、ECM メッセージから抽出された第 2 の識別子を、動作 1 1 0 の間に再構築された第 2 の識別子と比較する。これらの第 2 の識別子が同じでない場合、暗号化／暗号解読モジュール 8 4 は直ちに動作 1 0 8 を実行する。

20

【0067】

さもなければ、即ち、再構築された第 2 の識別子が、ECM メッセージを介して受信された第 2 の識別子と一致する場合、暗号化／暗号解読モジュール 8 4 は、補正ソフトウェア・プログラムが当該暗号化／暗号解読モジュール 8 4 用である場合には、その補正ソフトウェア・プログラムを実行する。

【0068】

最後に、暗号化／暗号解読モジュール 8 4 は、動作 1 1 4 の間に、動作 1 1 0 の間に再構築された第 2 の識別子を暗号化／暗号解読モジュール 1 6 へ送信する。

30

動作 1 1 2 は、この場合、いずれの補正ソフトウェア・プログラムも取り外されていないことを保証する。

【0069】

次いで、暗号化／暗号解読モジュール 1 6 は直ちに動作 6 6 を実行し、その動作 6 6 の間に、暗号化／暗号解読モジュール 1 6 は、暗号化／暗号解読モジュール 8 4 により送信された第 2 の識別子を、ECM メッセージに含まれる第 2 の識別子と比較する。暗号化／暗号解読モジュール 1 6 により実行される動作の残りの部分は、図 2 を参照して説明したものと同じである。

【0070】

40

図 4 の方法において、補正ソフトウェア・プログラムの不存在は、暗号化／暗号解読モジュール 8 4 とコンピュータ 2 0 との両方により検出されることができる。補正ソフトウェア・プログラムの不存在が暗号化／暗号解読モジュール 8 4 により検出された場合、暗号化／暗号解読モジュール 8 4 は直ちにその補正ソフトウェア・プログラムの処理を中断し、従って、再構築された第 2 の識別子を暗号化／暗号解読モジュール 1 6 へ送信しない。暗号化／暗号解読モジュール 1 6 が第 2 の識別子を受信しない場合、暗号化／暗号解読モジュール 1 6 は動作 6 8 を自動的に実行して、テレビジョン・チャンネルをアンスクランブルするのを防止する。

【0071】

即ち、第 1 の実施形態におけるように、サブステップ 1 0 0 の間に送信された補正ソフ

50

トウェア・プログラムに関しての補正ソフトウェア・プログラムの不存在、追加、又は変更は、テレビジョン・チャンネルのアンスクランブルを停止させる。

【0072】

しかしながら、第1の実施形態とは対照的に、たとえ暗号化／暗号解読モジュール16が、ECMメッセージを暗号解読するため設けられた変造されたモジュールであるとしても、また、たとえ補正ソフトウェア・プログラムが変更されるか、追加されるか、又は不存在であるとしても、デコーダ82を動作不能にするためにこのデコーダ82を操作することが依然として可能である。例えば、このために、補正ソフトウェア・プログラムは暗号化／暗号解読モジュール84へ送信され、暗号化／暗号解読モジュール84は、その補正ソフトウェア・プログラムを実行した後に、デコーダを操作して動作不能にする。例えば、暗号化／暗号解読モジュール84は、アンスクランブル・モジュール18を直接に操作する。従って、海賊デコーダの製造者は、この第2の実施形態においては、暗号化／暗号解読モジュール16を変造するのみではなく、暗号化／暗号解読モジュール84も変造しなければならない。暗号化／暗号解読モジュール84はデコーダ82の本体に固定的に連結されて取り外しできないので、海賊デコーダの製造者はまた、デコーダ全体を変造しなければならない。従って、図4の方法は、海賊デコーダにおいて真性のパーツや暗号化／暗号解読モジュールを用いることを非常に難しくする。

10

【0073】

最後に、図2又は図4の方法に直面する海賊デコーダの製造者、及び海賊デコーダに真性の暗号化／暗号解読モジュールを用いることを欲する海賊デコーダの製造者は、自身の海賊デコーダが損傷を受けやしくならないように、ステップ52又は124の間にECMメッセージに挿入された追加の情報を除去又は変更しなければならない。このために、その製造者は、ECMメッセージを復号できねばならない、即ち、その製造者は、いずれにせよ、変造された暗号化／暗号解読モジュールを自身の海賊デコーダに組み込まなければならない。これらの条件の下では、海賊デコーダで真性の暗号化／暗号解読モジュールを使用することに利点はない。

20

【0074】

この実施形態で説明したシステム及び方法は、テレビジョン・チャンネルをブロードキャストするための支払いベースの送信システムの特定のケースについて説明された。しかしながら、説明した方法は、デコーダを形成する受信機に1又はそれより多くの暗号化／暗号解読モジュールが装備された、暗号化された情報を伝送するための何れのシステムにも適用できる。暗号化／暗号解読モジュールを装備しているデコーダを形成するこのタイプの受信機は、例えば、SIMカード（加入者識別モジュール（Subscriber Identity Module））を装着しているモバイル電話器や、コード化されたソフトウェア・プログラムを受信することができるコンピュータがある。

30

【0075】

特に、テレビジョン・チャンネルをブロードキャストする送信システム以外のそのようなシステムにおいては、情報信号は必ずしもスクランブルされるとは限らないで、コード化されることもできる。

【0076】

40

チェックサムは、一つの変形形態では、電子署名により置き換えられる。

この実施形態で説明したシステム及び方法は、特定のケースについて説明され、その特定のケースにおいて、用いられた様々な暗号化／暗号解読の動作は、非対称の暗号化アルゴリズムを用いて実行され、それにより、暗号化のためのキーは暗号解読のためのキーと同じである。このタイプの非対称の暗号化アルゴリズムは、例えば、DESアルゴリズムである。一つの変形形態において、これらの暗号化／暗号解読の動作の一部又は全部が、例えば、RSAアルゴリズムのような非対称の暗号化／暗号解読アルゴリズムを用いて実行される。この変形形態においては、送信機及びデコーダのメモリは、適切な暗号化／暗号解読キーを備えるように適合されねばならない。特に、また、好ましくは、動作120と動作122とで用いられる暗号化アルゴリズムは異なるアルゴリズムであり、それによ

50

り、本方法のセキュリティが増大される。従って、動作 1 2 0 及び 1 2 2 に対応する暗号解読動作も異なる暗号解読アルゴリズムを用いることになる。

【図面の簡単な説明】

【0077】

【図 1】 図 1 は、本発明に従ったシステムの第 1 の実施形態のアーキテクチャの概略図である。

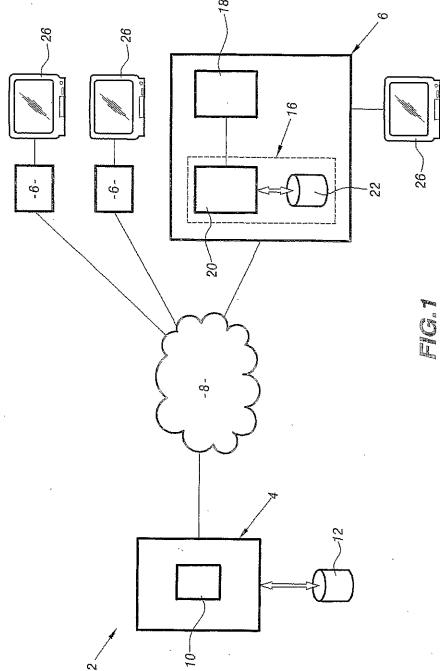
【図 2】 図 2 は、図 1 のシステムで実行される本発明に従った方法のフロー・チャートである。

【図 3】 図 3 は、本発明に従ったシステムの第 2 の実施形態の概略図である。

【図 4】 図 4 は、図 3 のシステムで実行される本発明に従った方法のフロー・チャートである。

10

【図 1】



【図 2】

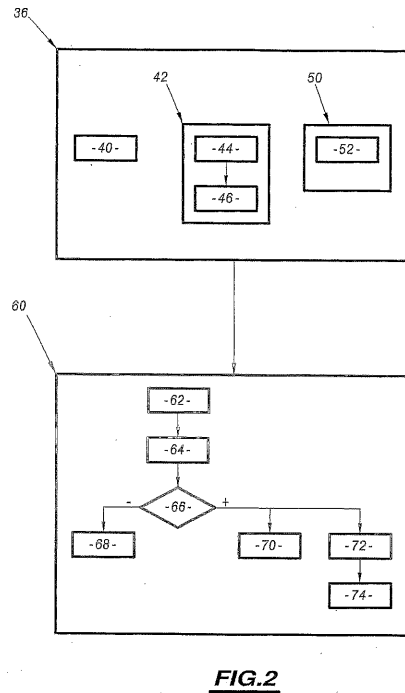


FIG. 2

【図 3】

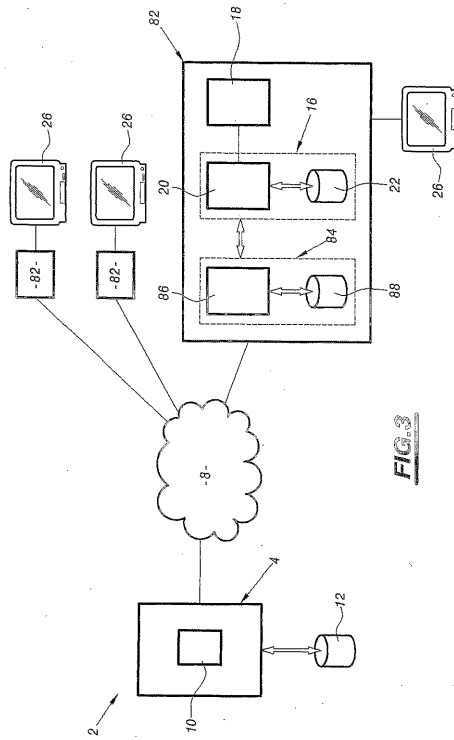


FIG. 3

【図 4】

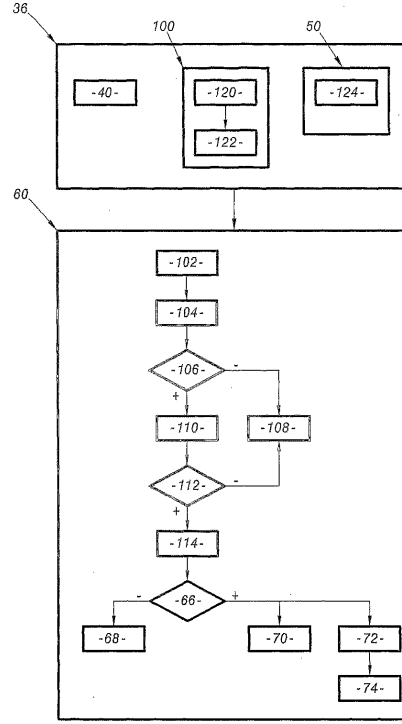


FIG. 4

フロントページの続き

(74)代理人 100084283

弁理士 秋元 芳雄

(72)発明者 ベナレドー, クリスティヤン

フランス国エフ-77600 ブズィーサン-ジョルジュ, アレ・デ・ピュイザティエ 13

審査官 後藤 彰

(56)参考文献 特開2002-251326 (JP, A)

特開2000-347846 (JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/22

H04N 7/167