【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成17年7月28日(2005.7.28)

【公開番号】特開2000-151578(P2000-151578A)
【公開日】平成12年5月30日(2000.5.30)
【出願番号】特願平10-318605
【国際特許分類第７版】
　Ｈ０４Ｌ　 9/14
　Ｇ０７Ｂ　15/00
　Ｈ０４Ｑ　 7/38
【ＦＩ】
　Ｈ０４Ｌ　 9/00　　６４１
　Ｇ０７Ｂ　15/00　　Ｌ
　Ｇ０７Ｂ　15/00　　５１０
　Ｈ０４Ｂ　 7/26　　１０９Ｒ

【手続補正書】
【提出日】平成16年12月24日(2004.12.24)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、
　上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の暗号アルゴリズム識別子と鍵識別子とを格納するとともに、上記受信された暗号文を格納する第１の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第１の記憶手段に格納された暗号アルゴリズム識別子と鍵識別子と暗号文をともに上記情報処理装置へ向けて送信する手段とを具備し、上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、暗号アルゴリズム識別子、及び鍵識別子を受信する手段と、上記移動体が個々に有する暗号アルゴリズム識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する鍵識別子にそれぞれ対応した異なる複数の鍵を格納する第２の記憶手段と、上記第２の記憶手段に格納された複数のアルゴリズムから受信された暗号アルゴリズム識別子に対応するアルゴリズムを選択する手段、及び上記第２の記憶手段に記憶された複数の鍵から受信された暗号アルゴリズム識別子に対応する鍵を選択する手段を有する選択手段と、上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで受信された暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された処理情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する手段とを具備したことを特徴とする暗号通信装置。
【請求項２】
　情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、
　上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の複数の異なる暗号アルゴリズム識別子と複数の異なる鍵識別子とを格納するとともに、上記受

信された暗号文を格納する第１の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第１の記憶手段に記憶された暗号アルゴリズム識別子と鍵識別子と上記第１の記憶手段に格納された暗号文をともに上記情報処理装置へ向けて送信する手段とを具備し、上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、暗号アルゴリズム識別子、及び鍵識別子を受信する手段と、上記移動体が個々に有する暗号アルゴリズム識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する鍵識別子にそれぞれ対応した異なる複数の鍵を格納する第２の記憶手段と、上記第２の記憶手段に記憶された複数のアルゴリズムから受信された暗号アルゴリズム識別子に対応するアルゴリズムを選択する手段、及び上記記憶手段に記憶された複数の鍵から受信された暗号アルゴリズム識別子に対応する鍵を選択する手段を有する選択手段と、上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで上記受信された暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された処理情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する手段とを具備したことを特徴とする暗号通信装置。

【請求項３】

上記情報処理装置の上記選択手段は、上記受信した暗号識別子または鍵識別子を変更する手段と、上記第２の記憶手段に記憶された複数のアルゴリズムから上記受信した暗号アルゴリズム識別子あるいは上記変更された暗号アルゴリズム識別子のいずれか一方に対応するアルゴリズムを選択する手段、及び上記記憶手段に記憶された複数の鍵から上記受信した鍵識別子あるいは上記変更された鍵識別子のいずれか一方に対応する鍵とを選択する手段を備え、上記情報処理装置の送信手段は、上記暗号化手段で生成された暗号文とともに上記受信された暗号アルゴリズム識別子、及び鍵識別子を上記所定位置に有る移動体へ向けて送信する手段を備えたことを特徴とする請求項１もしくは２記載の暗号通信装置。

【請求項４】

情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、

上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の移動体識別子とを格納するとともに、上記受信された暗号文を格納する第１の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第１の記憶手段に格納された移動体識別子と暗号文をともに上記情報処理装置へ向けて送信する手段とを具備し、上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、及び移動体識別子を受信する手段と、上記移動体が個々に有する移動体識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する移動体識別子にそれぞれ対応した異なる複数の鍵を格納する第２の記憶手段と、上記第２の記憶手段に記憶された複数のアルゴリズムから受信された移動体識別子に対応するアルゴリズムを選択する手段、及び上記第２の記憶手段に記憶された複数の鍵から受信された移動体識別子に対応する鍵を選択する手段を有する選択手段と、上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで上記移動体からの暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する手段とを具備したことを特徴とする暗号通信装置。

【請求項５】

上記暗号化手段は、上記復号化された情報に基づいて利用料金を計算し、上記復号化された情報の有する所持金とこの計算された利用料金との差から新たな所持金を計算し、この計算された所持金と当該情報処理装置に固有の情報とから上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する手段を備えたことを特徴とする請求項１から４記載の暗号通信装置。

【請求項６】
移動体と双方向通信を行う暗号通信装置において、
異なる複数の暗号アルゴリズム及び当該それぞれの暗号アルゴリズムを識別する暗号アルゴリズム識別子と、異なる複数の暗号鍵及び当該それぞれの暗号鍵を識別する鍵識別子とを格納する記憶手段と、
上記移動体から受信した暗号アルゴリズム識別子及び鍵識別子に基づいて、上記記憶手段から対応する暗号アルゴリズム及び対応する暗号鍵を選択する選択手段と、
上記選択手段で選択された暗号鍵を用いて、上記選択された暗号アルゴリズムにて上記移動体から受信した暗号文を復号する復号化手段と、
を具備したことを特徴とする暗号通信装置。
【請求項７】
複数の移動体と双方向通信する暗号通信装置において、
移動体から送信された暗号文、暗号アルゴリズム識別子、及び鍵識別子を受信する手段と、
上記移動体が個々に有する暗号アルゴリズム識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する鍵識別子にそれぞれ対応した異なる複数の鍵を格納する記憶手段と、
上記第２の記憶手段に格納された複数のアルゴリズムから受信された暗号アルゴリズム識別子に対応するアルゴリズムを選択する手段、及び上記記憶手段に記憶された複数の鍵から受信された暗号アルゴリズム識別子に対応する鍵を選択する手段を有する選択手段と、
上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで受信された暗号文を復号化する復号化手段と、
上記復号化手段で復号化された情報に基づいて処理された処理情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、
上記暗号化手段で生成された暗号文を移動体へ向けて送信する手段と、
を具備したことを特徴とする暗号通信装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１９
【補正方法】変更
【補正の内容】
【００１９】
第５の発明による暗号通信装置は、第１の発明から第４の発明において、上記暗号化手段は、上記復号化された情報に基づいて利用料金を計算し、上記復号化された情報の有する所持金とこの計算された利用料金との差から新たな所持金を計算し、この計算された所持金と当該情報処理装置に固有の情報とから上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する手段を備えたものである。
また、第６の発明による暗号通信装置は、移動体と双方向通信を行う暗号通信装置において、異なる複数の暗号アルゴリズム及び当該それぞれの暗号アルゴリズムを識別する暗号アルゴリズム識別子と異なる複数の暗号鍵及び当該それぞれの暗号鍵を識別する鍵識別子とを格納する記憶手段と、上記移動体から受信した暗号アルゴリズム識別子及び鍵識別子に基づいて、上記記憶手段から対応する暗号アルゴリズム及び対応する暗号鍵を選択する選択手段と、上記選択手段で選択された暗号鍵を用いて、上記選択された暗号アルゴリズムにて上記移動体から受信した暗号文を復号する復号化手段と、を備えたものである。
また、第７の発明による暗号通信装置は、複数の移動体と双方向通信する暗号通信装置において、移動体から送信された暗号文、暗号アルゴリズム識別子、及び鍵識別子を受信する手段と、上記移動体が個々に有する暗号アルゴリズム識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する鍵識別子にそれぞれ対応した異な

る複数の鍵を格納する記憶手段と、上記第２の記憶手段に格納された複数のアルゴリズムから受信された暗号アルゴリズム識別子に対応するアルゴリズムを選択する手段、及び上記記憶手段に記憶された複数の鍵から受信された暗号アルゴリズム識別子に対応する鍵を選択する手段を有する選択手段と、上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで受信された暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された処理情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を移動体へ向けて送信する手段と、を具備したものである。

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００３７
【補正方法】変更
【補正の内容】
【００３７】
　また、第４の発明によれば、移動体が具備する移動体識別子を情報処理装置が認識することで、移動体がシステムで決められた複数の暗号アルゴリズムの何れで処理しても、かつ、移動体がシステムで決められた複数の暗号鍵／復号鍵の何れで処理しても、移動体と情報処理装置において暗号処理が可能な方式を提供することができる。
　また、第６、第７の発明によれば、複数の暗号アルゴリズム及び暗号鍵を備えることにより、暗号アルゴリズムと暗号鍵が１つに固定される場合に比べて、通信情報の秘匿性をより向上させることができる。