

【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18年4月27日(2006.4.27)

【公開番号】特開2001-144748(P2001-144748A)

【公開日】平成13年5月25日(2001.5.25)

【出願番号】特願平11-320895

【国際特許分類】

H 04 L 9/32 (2006.01)

【F I】

H 04 L 9/00 6 7 3 D

H 04 L 9/00 6 7 3 A

【手続補正書】

【提出日】平成18年3月13日(2006.3.13)

【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】

生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、

パスワードを入力するパスワード入力手段と、

前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに基づいて中間コードを生成する中間コード生成手段と、

前記中間コードに基づいて、暗号化処理または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、

を有することを特徴とする暗号鍵生成装置。

【請求項2】

前記生体情報読み取り手段の読み取る生体情報は、指紋、眼底像、声紋、DNAパターンのいずれか、または指紋、眼底像、声紋、DNAパターンの2以上の生体情報の組み合せであることを特徴とする請求項1に記載の暗号鍵生成装置。

【請求項3】

前記生体情報読み取り手段の読み取る生体情報は指紋情報であり、

前記生体情報読み取り手段は、指紋画像を分割した複数領域において指紋の凹凸パターンの形成する隆線方向を識別し、該隆線方向に応じたコードを前記複数領域毎に対応付けることにより生体コードを生成して出力する構成であることを特徴とする請求項1に記載の暗号鍵生成装置。

【請求項4】

前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードとのいずれか一方を上位ビットとし、他方を下位ビットとする生体コードおよびパスワードのデータ連接処理を実行して中間コードを生成する構成であることを特徴とする請求項1に記載の暗号鍵生成装置。

【請求項5】

前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに対して関数を適用して新たな中間コードを生成する構成であることを特徴とする請求項1に記載の暗号鍵生成装置。

【請求項6】

前記暗号鍵生成手段の生成する暗号鍵は、共通鍵暗号化方式における共通鍵、公開鍵暗号化方式における公開鍵、秘密鍵のいずれかであることを特徴とする請求項1に記載の暗号鍵生成装置。

【請求項7】

生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、

パスワードを入力するパスワード入力手段と、

前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに基づいて中間コードを生成する中間コード生成手段と、

前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、

暗号化すべきデータを入力するデータ入力手段と、

前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力手段から入力したデータの暗号化処理を実行する暗号化手段と、

前記暗号化手段において暗号化したデータを出力する出力手段と、

を有することを特徴とする暗号化装置。

【請求項8】

生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、

パスワードを入力するパスワード入力手段と、

前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに基づいて中間コードを生成する中間コード生成手段と、

前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、

復号化すべきデータを入力するデータ入力手段と、前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力手段から入力したデータの復号化処理を実行する復号化手段と、

前記復号化手段において復号化したデータを出力する出力手段と、

を有することを特徴とする復号化装置。

【請求項9】

暗号化処理または復号化処理に使用する暗号鍵を生成する暗号鍵生成方法において、

生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、

パスワードを入力するパスワード入力ステップと、

前記生体情報読み取りステップにおいて読み取られた生体コードと上記パスワード入力ステップにおいて入力されたパスワードに基づいて中間コードを生成する中間コード生成ステップと、

前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、

を有することを特徴とする暗号鍵生成方法。

【請求項10】

生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、

パスワードを入力するパスワード入力ステップと、

前記生体情報読み取りステップで読み取られた生体コードと上記パスワード入力ステップにおいて入力されたパスワードに基づいて中間コードを生成する中間コード生成ステップと、

前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、

暗号化すべきデータを入力するデータ入力ステップと、

前記暗号鍵生成ステップにおいて生成した暗号鍵に基づいて前記データ入力ステップにおいて入力したデータの暗号化処理を実行する暗号化ステップと、

前記暗号化ステップにおいて暗号化したデータを出力する出力ステップと、
を有することを特徴とする暗号化方法。

【請求項 1 1】

生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、

パスワードを入力するパスワード入力ステップと、

前記生体情報読み取りステップで読み取られた生体コードと上記パスワード入力ステップで入力されたパスワードに基づいて中間コードを生成する中間コード生成ステップと、

前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、

復号化すべきデータを入力するデータ入力ステップと、

前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力ステップにおいて入力したデータの復号化処理を実行する復号化ステップと、

前記復号化ステップにおいて復号化したデータを出力する出力ステップと、
を有することを特徴とする復号化方法。

【請求項 1 2】

暗号鍵生成処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを有形的に提供するプログラム提供媒体であって、

前記コンピュータ・プログラムは、

生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、

パスワードを入力するパスワード入力ステップと、

前記生体情報読み取りステップにおいて読み取られた生体コードと上記パスワード入力ステップにおいて入力されたパスワードに基づいて中間コードを生成する中間コード生成ステップと、

前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、

を有することを特徴とするプログラム提供媒体。