【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6月16日(2005.6.16)

【公開番号】特開2002-261751(P2002-261751A)
【公開日】平成14年9月13日(2002.9.13)
【出願番号】特願2001-58087(P2001-58087)
【国際特許分類第７版】
　Ｈ０４Ｌ　 9/10
　Ｇ０６Ｋ　19/07
　Ｇ０９Ｃ　 1/00
【ＦＩ】
　Ｈ０４Ｌ　 9/00　　６２１Ａ
　Ｇ０９Ｃ　 1/00　　６１０Ｚ
　Ｇ０９Ｃ　 1/00　　６２０Ｚ
　Ｇ０９Ｃ　 1/00　　６６０Ａ
　Ｇ０６Ｋ　19/00　　Ｎ

【手続補正書】
【提出日】平成16年9月13日(2004.9.13)
【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】
　情報処理装置を利用して対称鍵暗号化処理を行なう方法であって、
（１）入力される平文Ｍに秘密鍵Ｋを適用する暗号化処理Ｚ＝Ｅ（Ｍ，Ｋ）を行なってその結果Ｚをメモリに格納し、
（２）前記メモリ上の結果Ｚに対して復号化処理Ｗ＝Ｄ（Ｚ，Ｋ）を行なってその結果Ｗをメモリ上に格納し、
（３）前記の処理結果Ｗと平文Ｍとが一致している場合には、処理結果Ｚを出力し、
（４）前記の処理結果Ｗと平文Ｍとが不一致の場合には、処理結果の出力を抑止することを特徴とする暗号処理方法。
【請求項２】
　前記暗号化処理及び復号化処理をＤＥＳ(Data Encryption Standard)に従って実行することを特徴とする請求項１記載の暗号処理方法。
【請求項３】
　前記処理結果の出力を抑止する方法として、前記情報処理装置をリセットすることを特徴とする請求項１記載の暗号処理方法。
【請求項４】
　前記情報処理装置及び前記メモリは、ＩＣカード上に搭載されるそれぞれ演算装置及び記憶装置であることを特徴とする請求項１記載の暗号処理方法。
【請求項５】
　情報処理装置を利用して対称鍵復号化処理を行なう方法であって、
（１）入力される暗号文Ｃに秘密鍵Ｋを適用する復号化処理Ｚ＝Ｄ（Ｃ，Ｋ）を行なってその結果Ｚをメモリに格納し、
（２）前記メモリ上の結果Ｚに対して暗号化処理Ｗ＝Ｅ（Ｚ，Ｋ）を行なってその結果Ｗをメモリ上に格納し、

（３）前記の処理結果Ｗと暗号文Ｃとが一致している場合には、処理結果Ｚを出力し、
（４）前記の処理結果Ｗと暗号文Ｃとが不一致の場合には、処理結果の出力を抑止することを特徴とする暗号処理方法。
【請求項６】
前記暗号化処理及び復号化処理をＤＥＳ(Data Encryption Standard)に従って実行することを特徴とする請求項５記載の暗号処理方法。
【請求項７】
前記処理結果の出力を抑止する方法として、前記情報処理装置をリセットすることを特徴とする請求項５記載の暗号処理方法。
【請求項８】
前記情報処理装置及び前記メモリは、ＩＣカード上に搭載されるそれぞれ演算装置及び記憶装置であることを特徴とする請求項５記載の暗号処理方法。
【請求項９】
情報処理装置を利用して非対称鍵復号化処理を行なう方法であって、
（１）入力される暗号文Ｃに秘密鍵Ｘを適用する復号化処理Ｚ＝Ｄ（Ｃ，Ｘ）を行なってその結果Ｚをメモリに格納し、
（２）前記メモリ上の結果Ｚに公開鍵Ｊを適用する暗号化処理Ｗ＝Ｅ（Ｚ，Ｊ）を行なってその結果Ｗをメモリ上に格納し、
（３）前記の処理結果Ｗと暗号文Ｃとが一致している場合には、処理結果Ｚを出力し、
（４）前記の処理結果Ｗと暗号文Ｃとが不一致の場合には、処理結果の出力を抑止することを特徴とする暗号処理方法。
【請求項１０】
前記暗号化処理及び復号化処理をＲＳＡ暗号化方式に従って実行することを特徴とする請求項９記載の暗号処理方法。
【請求項１１】
前記処理結果の出力を抑止する方法として、前記情報処理装置をリセットすることを特徴とする請求項９記載の暗号処理方法。
【請求項１２】
前記情報処理装置及び前記メモリは、ＩＣカード上に搭載されるそれぞれ演算装置及び記憶装置であることを特徴とする請求項９記載の暗号処理方法。