【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19年10月11日(2007.10.11)

【公開番号】特開2006-94241(P2006-94241A)
【公開日】平成18年4月6日(2006.4.6)
【年通号数】公開・登録公報2006-014
【出願番号】特願2004-278540(P2004-278540)
【国際特許分類】
Ｈ０４Ｌ　9/14　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６４１

【手続補正書】
【提出日】平成19年8月26日(2007.8.26)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
暗号化すべき情報の価値を表す価値情報を取得する価値情報取得手段と、
　前記情報の暗号化を行う際の暗号化強度を表す強度パラメータを前記価値情報に基づいて演算する強度パラメータ演算手段とを有することを特徴とする暗号化装置。
【請求項２】
前記強度パラメータ演算手段は、前記情報の暗号化に用いられるべき鍵の長さを前記強度パラメータとして演算する鍵長演算手段を有することを特徴とする請求項１記載の暗号化装置。
【請求項３】
前記鍵長演算手段は、暗号化された情報の解読処理に見込まれる費用が前記価値情報にて表される価値と同等またはそれ以上となる条件を満足する鍵の長さを前記情報の暗号化に用いられるべき鍵の長さとして演算することを特徴とする請求項１または２記載の暗号化装置。
【請求項４】
前記鍵長演算手段は、前記条件を満足し得る鍵の長さの最小値を前記情報の暗号化に用いられるべき鍵の長さとして演算することを特徴とする請求項３記載の暗号化装置。
【請求項５】
前記鍵長演算手段は、暗号化された情報の解読処理を行い得る処理装置の価格と処理能力とに基づいて決まる所定単価当たりの計算量能力に基づいて所定期間になされ得る前記所定単価当たりの計算量の推定値となる単価対応推定計算量を演算する手段と、
　前記単価対応推定計算量と、前記価値情報にて表される価値と、暗号化された情報の解読処理に必要な計算量の推定値を演算するための所定の推定演算式とに基づいて、前記条件を満足する鍵の長さを演算する手段とを有することを特徴とする請求項３または４記載の暗号化装置。
【請求項６】
前記単価対応推定計算量を演算する際に用いられる前記所定期間は、前記暗号化される情報の保護期間に設定されることを特徴とする請求項５記載の暗号化装置。
【請求項７】
前記単価対応推定計算量をムーアの法則に基づいた手法に従って演算することを特徴とす

る請求項５または６に記載の暗号化装置。
【請求項８】
前記単価対応推定計算量 f(Y) を
f(Y) = F・(2^(Y/1.5))
F：所定単価当たりの計算量能力
Y：所定期間
に従って演算することを特徴とする請求項７記載の暗号化装置。
【請求項９】
前記推定演算式として、素因数分解される整数をｎとした場合におけるその素因数分解に必要な計算量C(n)を与える
C(n) = v log v, v=min{w|Ψ(x,y)>=xy/log y, x=2d(n^(2/d))(w^((d+1)/2), y>0 }
Ψ(x,y)：x以下の正の整数で、その素因数がyを超えない数の個数
d：正の奇数
を用いたことを特徴とする請求項５乃至８のいずれかに記載の暗号化装置。
【請求項１０】
前記鍵の長さKを
K = lg{min{n|C(n)>=T・f(Y)}}
f(Y)：単価対応推定計算量
T：価値情報
lg：２を底とした対数を表す
に従って演算することを特徴とする請求項９記載の暗号化装置。
【請求項１１】
前記暗号化すべき情報は、一または複数のデータユニットからなるファイルであって、
前記価値情報取得手段は、前記ファイルに含まれるデータユニットの推定単価と、前記ファイルに含まれるデータユニットの個数とに基づいてファイルの推定価格を演算するファイル価格演算手段を有し、当該暗号化すべきファイルの推定価格を前記価値情報として得ることを特徴とする請求項１乃至１０のいずれかに記載の暗号化装置。
【請求項１２】
前記価値情報取得手段は、前記ファイル推定価格に所定の補正価格を加えた価格を前記価値情報として得ることを特徴とする請求項１１記載の暗号化装置。
【請求項１３】
暗号化すべき情報の価値を表す価値情報を取得する価値情報取得ステップと、
前記情報の暗号化を行う際の暗号化強度を表す強度パラメータを前記価値情報に基づいて演算する強度パラメータ演算ステップとをコンピュータに実行させるためのプログラム。
【請求項１４】
前記強度パラメータ演算ステップは、前記情報の暗号化に用いられるべき鍵の長さを前記強度パラメータとして演算する鍵長演算ステップを有することを特徴とする請求項１３記載のプログラム。
【請求項１５】
前記鍵長演算ステップは、暗号化された情報の解読処理に見込まれる費用が前記価値情報にて表される価値と同等またはそれ以上となる条件を満足する鍵の長さを前記情報の暗号化に用いられるべき鍵の長さとして演算することを特徴とする請求項１３または１４記載のプログラム。
【請求項１６】
前記鍵長演算ステップは、前記条件を満足し得る鍵の長さの最小値を前記情報の暗号化に用いられるべき鍵の長さとして演算することを特徴とする請求項１４記載のプログラム。
【請求項１７】
前記鍵長演算ステップは、暗号化された情報の解読処理を行い得る処理装置の価格と処理能力とに基づいて決まる所定単価当たりの計算量能力に基づいて所定期間になされ得る前

記所定単価当たりの計算量の推定値となる単価対応推定計算量を演算するステップと、
前記単価対応推定計算量と、前記価値情報にて表される価値と、暗号化された情報の解読処理に必要な計算量の推定値を演算するための所定の推定演算式とに基づいて、前記条件を満足する鍵の長さを演算するステップとを有することを特徴とする請求項１５または１６記載のプログラム。
【請求項１８】
前記単価対応推定計算量を演算する際に考慮される前記所定期間は、前記暗号化される情報の保護期間に設定されることを特徴とする請求項１７記載のプログラム。
【請求項１９】
請求項１乃至１２のいずれかに記載の暗号化装置と、
前記暗号化装置にて得られた強化パラメータにて表される暗号化強度にて前記情報の暗号化処理を行う暗号化処理手段を有する情報保護システム。
【請求項２０】
前記暗号化処理手段は、前記暗号化された情報を利用する機器固有の情報と、前記暗号化装置にて暗号化強度を表す強度パラメータとして決定された長さの鍵とを用いて前記情報の暗号化処理を行うことを特徴とする請求項１９記載の情報保護システム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００３６
【補正方法】削除
【補正の内容】
【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】削除
【補正の内容】
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００３８
【補正方法】削除
【補正の内容】
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００３９
【補正方法】削除
【補正の内容】
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００４０
【補正方法】削除
【補正の内容】
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００４１
【補正方法】削除
【補正の内容】
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００４２
【補正方法】削除

【補正の内容】
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００５４
【補正方法】削除
【補正の内容】
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正の内容】
【発明の名称】暗号化装置及びプログラム、並びに該暗号化装置を用いた情報保護システム
【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】０００７
【補正方法】変更
【補正の内容】
【０００７】
そこで、本発明は、このような点に鑑みてなされたもので、情報を暗号化する際の暗号化強度を合理的に決めることができる暗号化装置及びプログラム、並びに該暗号化装置を用いた情報保護システムを提供することを目的とする。
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００５５
【補正方法】変更
【補正の内容】
【００５５】
本発明に係る暗号化装置及びプログラム、並びに該暗号化装置を用いた情報保護システムによれば、情報の価値が高ければ高いほど暗号化強度を高くするような強度パラメータを決定することが可能となるので、情報を暗号化する際の暗号化強度をその情報の価値に応じて合理的に決めることができるようになる。