オブジェクト指向による暗号化ライブラリの部品化と CRYPTO98 への実装

6 G − 9

山賀 陽† 紙谷 剛司‡ 井上 幸美†

†立命館大学理工学部情報学科 ‡日本電子計算（株）

1 はじめに

暗号ライブラリ PowerMISTY[1]を用い，用途によりライブラリ群を組み合わせて暗号化を行う暗号システム CRYPTO98 を開発した．その際，鍵情報やその他変数の取り扱いの煩雑さを避け，オブジェクト指向によりライブラリを操作するソースをすべてクラス化して実装した．本稿では，開発したシステムの基本構造とその評価について述べる．

2 暗号ライブラリのクラス設計

2.1 外部との入出力に関するクラス

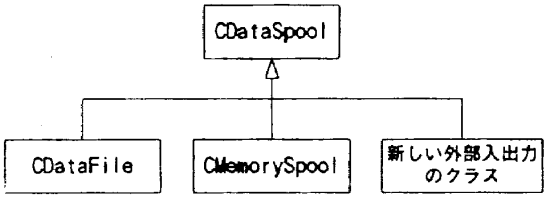

図１：外部入出力に関するクラスの継承関係

さまざまな入出力の媒体に対応できるようにするため，入出力に関するクラス（CDataSpool クラス）を作成した（図１）．新たな入出力に対応するクラスを CDataSpool クラスから派生させ，この純粋仮想関数[4]を具体的に定義することで，メッセージ処理を行うクラスに対応することができる．

これによって，暗号に関する既存のクラスには変更を加えずに外部との入出力に関するクラスを作成することで，既存のクラスを対応させることができる．

本稿では，ファイルに対して入出力を行う CDataFile クラスと，メモリ領域に対して入出力を行う CMemorySpool クラスを作成した．いずれも，CDataSpool クラスから派生したクラスである．

2.2 暗号に関するクラス

作成した暗号に関するクラスの機能について説明する（図２）．

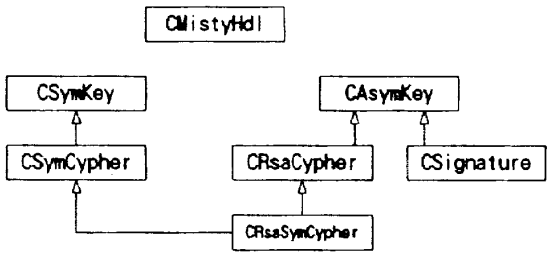

図２：暗号に関するクラス群の継承関係

- アルゴリズムハンドルに関するクラス

暗号ライブラリの窓口となるアルゴリズムハンドル[1]はメッセージ処理には必要だが，ユーザに触れさせる必要はない．したがって，暗号に関するクラスからコンポジションを用いて利用する．

- 鍵に関するクラス

対称鍵に関するクラス（CKey クラス）と非対称鍵に関するクラス（CAsymKey クラス）を作成した．非対称鍵に関するクラスは，公開鍵・秘密鍵として CKey クラスを属性として保持する．

これらのクラスは，鍵の生成条件の設定，鍵の生成してアルゴリズムハンドルからオブジェクトへの鍵の取得，オブジェクトから外部への書き込みと外部からオブジェクトへの読み込みに関する初期化，

Composition of Encryption Library by Object-Oriented Programming for "CRYPTO98"

† Akira Yamaga and Yukiyoshi Inoue, Department of Computer Science, Ritsumeikan University

‡ Takeshi Kamitani, Japan Information Processing Service Co., Ltd.

外部から取り込んだ鍵をアルゴリズムハンドルへの設定といった操作を持つ.

- 暗号化に関するクラス

対称暗号に関するクラス（CSymCypher クラス）と非対称暗号に関するクラス（CRsaCypher クラス）を作成した.それぞれ,CKey クラス,CAsymKey クラスを継承している．メッセージの暗号化，復号化といった操作を持つ.

- 署名に関するクラス

署名に関するクラスは，メッセージ縮約と署名をまとめて1つのクラス（CSignature クラス）で作成した．このクラスの機能は，メッセージ縮約のための MD5[2]と SHA[2]，ディジタル署名のための MD5+RSA[2]，SHA+RSA，DSA[2]がある．これらは，メッセージ縮約または署名の作成・検証ともに，鍵をアルゴリズムハンドルに設定する以外は同じ処理手順で行う．ゆえに，1つのクラスでまとめることができる.

このクラスは,非対称鍵クラスである CAsymKey クラスを継承している.このクラスの操作は,署名・縮約の作成，署名・縮約データのオブジェクトへのセット，署名・縮約の検証，署名・縮約データの外部への書き出しと外部からの読み込みを操作として持つ.

3 部品化した暗号ライブラリの実装

暗号アプリケーション CRYPTO98 へ今回作成した部品を実装した.

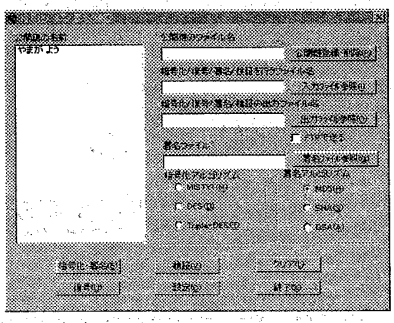

図3：CRYPTO98

CRYPTO98 は，平文ファイルを対称暗号で暗号化し，共通鍵をあらかじめ登録した公開鍵で暗号化する．そして，署名ファイルを添付する．さらに，ファイルの圧縮を行い，FTP でファイルを転送する．図3にアルゴリズム選択のダイアログを示す.

4 評価

部品化を行ったクラス群を使用した場合と部品化を行わなかった場合の暗号化にかかる処理時間を図4に示す．処理に使用したデータはテキストファイルである．使用環境は，CPU：Pentium MMX 200MHz，OS：Windows NT4.0 Workstation (Microsoft 社)とする.

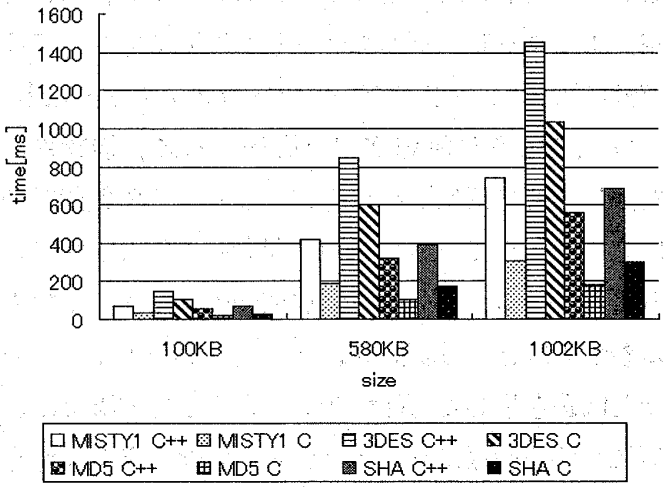

図4：評価グラフ

5 終わりに

本稿で作成したクラス群は，暗号ライブラリの煩雑な処理手順を隠蔽し，シンプルな関数インターフェースを提供することができた．さらに，各暗号アルゴリズムをクラス化しているので，それらを部品として組み合わせることが容易になった.

これらは，暗号アプリケーション開発を容易にし，開発者を強力にサポートするものと考える.

参考文献

[1] 三菱暗号ライブラリ PowerMISTY for Windows 取扱説明書，三菱電機株式会社情報システム製作所，(1996)

[2] 岡本 栄司：暗号基礎理論，共立出版，(1993)

[3] 磯田 定宏：オブジェクト指向モデリング，コロナ社(1998)

[4] 柴田 望洋，プログラミング講義 C++，ソフトバンク(1996)