日立暗号ライブラリ
Keymate/Crypto （キーメイト/クリプト）

HITACHI
Inspire the Next

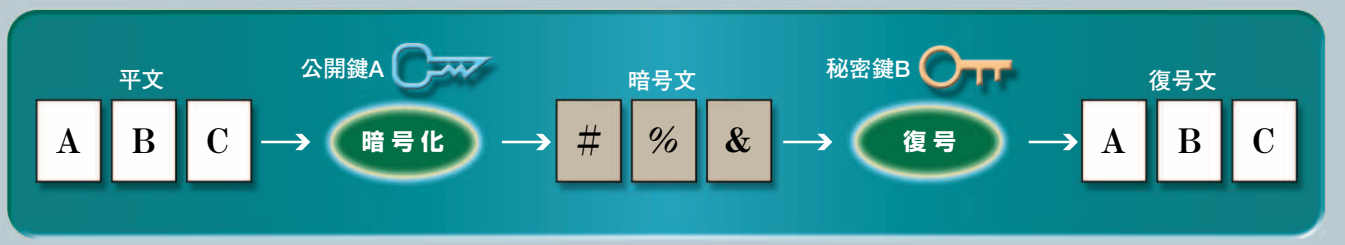
日立の高信頼な暗号技術に JCMVP®認証のさらなる安心を。

Keymate/Crypto

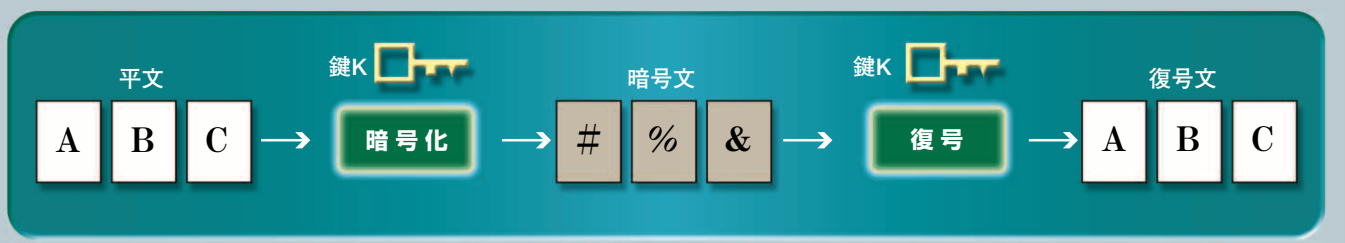
Keymate/Crypto Version 4 は、
JCMVPにおける「承認されたセキュリティ機能」や
国際標準に準拠した暗号アルゴリズムを実装したライブラリです。
公開鍵、共通鍵暗号、ハッシュ関数など、
豊富な暗号機能をご利用いただけます。

公開鍵暗号方式と共通鍵暗号方式。
「Keymate/Crypto」は、両方の暗号技術をサポートしています。

■公開鍵暗号方式
データの暗号化と復号に対となる鍵を使用する暗号方式です。



■共通鍵暗号方式
データの暗号化と復号に同一の鍵を使用する暗号方式です。



uVALUE

JCMVP認証を取得したJCMVPライブラリと Cryptoライブラリを提供

■JCMVPライブラリ

暗号アルゴリズムはCryptoライブラリのサブセットとし、JCMVPに要求される機能を拡張しています。提供する暗号アルゴリズムは「承認されたセキュリティ機能」*から選択しています。

*IPA「承認されたセキュリティ機能に関する仕様」

JCMVPはIPAが運用する暗号モジュール試験及び認証制度です。本製品のJCMVPライブラリはJIS X 19790「セキュリティ技術-暗号モジュールのセキュリティ要求事項」(2007)に基づくJCMVP認証取得製品です。

特 長

パワーアップテストとしてライブラリローディング時に、暗号ライブラリ自身の改ざん検知(完全性テスト)、正しい暗号動作の確認(暗号アルゴリズムテスト)、健全な乱数エントロピーの確認(RBGエントロピーテスト)を行います。暗号ライブラリ自身が健全であることをライブラリローディングのたびに確認します。また暗号処理時に条件自己テストを行います。JCMVPライブラリは、暗号モジュール試験の一部としての暗号アルゴリズム実装試験に合格しています。この試験に合格した製品同士において、承認された同じ暗号アルゴリズムを同一使用法で用いると、暗号データの互換性が確保できます。

■Cryptoライブラリ

従来のKeymate/Cryptoの機能を継承しています。古い暗号アルゴリズムから最新のものまで豊富な暗号アルゴリズムをサポートします。

製 品 構 成

●開発キット(Development Kit)
アプリケーションを開発するために必要な環境、および開発したアプリケーションを実行するために必要な環境を提供します。

●ランタイム(Run Time)
開発したアプリケーションを実行するために必要な環境のみを提供します。開発キットで開発アプリケーションを動作させる装置にインストールします。

●開発キットプログラムインタフェース
開発キットはC言語のプログラムインタフェースを提供するライブラリです。

■JCMVP ライブラリ機能一覧

機 能	アルゴリズム
公開鍵暗号	署名:ECDSA、RSASSA-PKCS1-v1_5、RSASSA-PSS 守秘:RSA-OAEP
共通鍵暗号	128ビットブロック暗号:AES
ハッシュ関数ほか	SHA-256、SHA-384、SHA-512 HMAC(SHA-256、SHA-384、SHA-512)
乱数	NIST SP800-90のHash_DRBG(SHA-512)
自己テスト機能	パワーアップテスト(完全性、暗号アルゴリズム、RBGエントロピー)、条件自己テスト(鍵ペア整合性など)

■Crypto ライブラリ機能一覧

機 能	アルゴリズム
公開鍵暗号	署名:DSA、ECDSA、RSASSA-PKCS1-v1_5、RSASSA-PSS 守秘:RSA-OAEP、RSAES-PKCS1-v1_5、ECIES-AES、ELCURVE 鍵共有:DH、ECDH
共通鍵暗号	128ビットブロック暗号:AES 64ビットブロック暗号:DES、Triple DES(2-key、3-key) ストリーム暗号:MULTI-S01
ハッシュ関数ほか	SHA-1、SHA-256、SHA-384、SHA-512 HMAC(SHA-1、SHA-256、SHA-384、SHA-512) パスワードから共通鍵導出(PKCS#5、PKCS#12)

■標準価格例

製品	価格
Keymate/Crypto Development Kit Version 4 Linux(AMD/Intel 64)版 適用OS:Red Hat Enterprise Linux 5、Red Hat Enterprise Linux 5 Advanced Platform	媒体、マニュアル、1CPUライセンス **315,000円**(税抜き300,000円)
Keymate/Crypto Run Time Version 4 Linux(AMD/Intel 64)版 適用OS:Red Hat Enterprise Linux 5、Red Hat Enterprise Linux 5 Advanced Platform	媒体、1CPUライセンス **144,900円**(税抜き138,000円)

本製品は、独立行政法人 情報処理推進機構(IPA)が推進する創造的ソフトウェア育成事業の一環として技術開発された内容を含みます。

- 製品仕様は、改良のため変更することがあります。
- 本製品を輸出される場合には、外国為替及び外国貿易法並びに米国の輸出管理関連法規などの規制をご確認のうえ、必要な手続きをお取りください。
  なお、ご不明な場合は、弊社担当営業にお問い合わせください。
- 本カタログに掲載されている価格は、2008年4月現在のものです。

製品に関する詳細・お問い合わせは下記へ

■ 製品情報サイト
http://www.hitachi.co.jp/soft/keymate/

■ インターネットでのお問い合わせは
http://www.hitachi.co.jp/soft/ask

■ 電話でのお問い合わせは**HMCC**(日立オープンミドルウェア 問い合わせセンター)へ
0120-55-0504 利用時間 9:00~12:00、13:00~17:00(土・日・祝日・弊社休日を除く)

株式会社 日立製作所 情報・通信グループ ソフトウェア事業部

CA-681 2008.4
Printed in Japan(H)