

# Zoocrypt – 暗号 & ハッシュ

16 進文字列の暗号・ハッシュ演算を行います。

もともとデバッグツールとして作成したのですが、他にもさまざまな使い方があり、かも？

## 重要な注意事項

Zoocrypt は暗号鍵を保護していませんので、暗号通信やデータ秘匿の用途には使えません。

## 動作環境

Zoocrypt は、Microsoft Windows 上で動作するアプリケーションソフトウェアです。

動作環境は下表をご覧ください。

Zoocrypt の動作環境

ハードウェア	<ul style="list-style-type: none"><li>◆ x86 系プロセッサ</li><li>◆ ストレージデバイスの 8.5 メガバイト以上の空き領域</li></ul>
OS	<ul style="list-style-type: none"><li>◆ Microsoft Windows 2000 または後方互換性を有する上位バージョン</li></ul>
入出力機器	<ul style="list-style-type: none"><li>◆ 文字入力デバイス(キーボードなど)</li><li>◆ 800×600 ピクセル、256 色以上の表示モードをサポートする表示デバイス</li><li>◆ ポインティングデバイス(マウスなど)の使用を推奨</li></ul>

## 改版履歴

Zoocrypt の最新バージョンは 2.3.4 です。

機能の追加・変更点は下表をご覧ください。

Zoocrypt の改版履歴

バージョン	リリース日	機能の追加・変更点
バージョン 1 は、共通鍵暗号アルゴリズムとして DES と AES に、NIST SP 800-38A で規定された各種処理モード、およびハッシュアルゴリズムとして MD 系と SHA 系各種の搭載を構想。		
0.1	2004 年 10 月 30 日	<p>頻繁に使用するもののみを搭載した暫定版(正式版は作らず仕舞い)。</p> <ul style="list-style-type: none"><li>◆ 共通鍵暗号アルゴリズム: DES、TDEA(通称 Triple DES)</li><li>◆ 共通鍵暗号の処理モード:</li></ul>

バージョン	リリース日	機能の追加・変更点
		ECB、CBC ◆ ハッシュアルゴリズム： MD5、SHA-1
バージョン 2 は、公開鍵暗号アルゴリズムとして RSA を追加。		
2.0	2005 年 12 月 18 日	◆ 共通鍵暗号アルゴリズム(追加分)： AES ◆ 共通鍵暗号の処理モード(追加分)： CFB、OFB ◆ 公開鍵暗号アルゴリズム： RSA(512～8192 ビット non-CRT および CRT 鍵) ◆ RSA 暗号の処理スキーム： 無形式、PKCS#1 v1.5 ◆ ハッシュアルゴリズム(追加分)： MD2、SHA-224、SHA-256、SHA-384、SHA-512
2.0.1	2006 年 2 月 12 日	◆ RSA 暗号演算の所要時間を、バージョン 2.0 比で約 63%に短縮 ◆ RSA 鍵ペア生成の所要時間を、バージョン 2.0 比で約 14%に短縮 ◆ RSA 鍵ペア生成で鍵長が 323 ビット以下の場合の公開指数[e]を 3 から 17 に変更 ◆ RSA 暗号文の値によって稀に正しく復号されない不具合を修正 ◆ RSA 鍵ペア生成中にキャンセルボタンをクリックすると異常終了することがある不具合を修正 ◆ RSA 鍵ペア生成中にキャンセルボタンをクリックするとウィンドウを閉じた後もしばらく生成処理が継続する不具合を修正
2.1	2007 年 2 月 7 日	◆ ハッシュアルゴリズム(追加分)： RIPEMD-128、RIPEMD-160、RIPEMD-256、RIPEMD-320 ◆ 16 進文字列入力欄のうち、平文と暗号文の右ポップアップメニューから、クリップボード形式を選択して貼り付けられるよう改良 ◆ RSA 鍵ペア生成の所要時間を、バージョン 2.0.1 比で約 48%に短縮 ◆ コンパイラソフトをバージョンアップしたら、Zoocrypt の実行時にコマンドウィンドウが開くようになった。な

バージョン	リリース日	機能の追加・変更点
		ぜだろう？
2.1.1	2007 年 4 月 6 日	<ul style="list-style-type: none"> <li>◆ クリップボードへコピーした鍵を、DER エンコードした 16 進文字列として他のソフトウェア(テキストエディタなど)へ貼り付けられるよう改良</li> <li>◆ RSA 署名生成・検証(PKCS#1 v1.5)で、オブジェクト識別子が定義されていないハッシュアルゴリズム RIPEMD-320 を選択できないよう修正</li> <li>◆ DER エンコードした 16 進文字列の鍵をクリップボードから貼り付けられない不具合を修正</li> <li>◆ RSA 鍵長が 751 ビット以下の場合に、ハッシュアルゴリズムとして SHA-1 を選択すると、RSA 署名生成ボタン・検証ボタンが淡色表示される不具合を修正</li> <li>◆ RSA 署名生成・検証(PKCS#1 v1.5)で、ハッシュアルゴリズムとして SHA-224、SHA-256、SHA-384、SHA-512 を選択すると DigestInfo 構造体が正しく構成されず誤った署名値となる不具合を修正</li> </ul>
2.2	2007 年 9 月 1 日	<ul style="list-style-type: none"> <li>◆ RSA 暗号の処理スキーム(追加分): PKCS#1 v2.1</li> <li>◆ ハッシュ応用アルゴリズム: HMAC(任意長の鍵を許容)</li> <li>◆ RSA 暗号演算の所要時間を、バージョン 2.1.1 比で約 83%(1024 ビット non-CRT 秘密鍵の場合)～約 46%(8192 ビット non-CRT 秘密鍵の場合)に短縮</li> </ul>
2.2.1	2008 年 2 月 9 日	<ul style="list-style-type: none"> <li>◆ Zoocrypt の起動時にコマンドウィンドウが開かないよう修正</li> </ul>
2.3	2011 年 4 月 4 日	<ul style="list-style-type: none"> <li>◆ 共通鍵暗号の処理モード(追加分): CTR、CMAC</li> <li>◆ RSA 鍵長の最大値を 16384 ビットに変更</li> <li>◆ 16 進文字列のアルファベット表記を、小文字固定から、小文字・大文字の選択ができるよう変更</li> <li>◆ 16 進文字列入力の各欄で、右ポップアップメニューの項目「貼り付け」「バイト列と見なして貼り付け」を、文字列全体の置換えから、カーソル位置への挿入に変更</li> <li>◆ 共通鍵暗号の CFB モードで、ビット幅が 2 ビット、4 ビットの場合に正しく暗号化されず、また 16 ビット以上の場合に復号できない不具合を修正</li> </ul>

バージョン	リリース日	機能の追加・変更点
		<ul style="list-style-type: none"> <li>◆ RSA 鍵ペア生成の経過時間表示が、24 時間経つと 00:00:00 に戻る不具合を修正</li> <li>◆ 16 進文字列入力の各欄で、改行キーを押すと 1 文字消える不具合を修正</li> </ul>
2.3.1	2011 年 4 月 17 日	<ul style="list-style-type: none"> <li>◆ RSA 鍵種別が CRT 鍵の場合に、non-CRT 秘密指数[d]欄が空でないと公開鍵を保存できない不具合を修正</li> </ul>
2.3.2	2011 年 9 月 12 日	<ul style="list-style-type: none"> <li>◆ 16 進文字列入力の各欄(鍵を除く)で、ファイルに保存できない不具合を修正</li> <li>◆ 16 進文字列入力の各欄で、日本語の文字を含む名前のファイルを開く・保存ができない不具合を修正</li> </ul>
2.3.3	2012 年 3 月 17 日	<ul style="list-style-type: none"> <li>◆ 右ポップアップメニューに「値を 16 進書式付きでコピー」を追加</li> </ul>
2.3.4	2012 年 5 月 30 日	<ul style="list-style-type: none"> <li>◆ 右ポップアップメニューに「値を文字列としてコピー」を追加</li> <li>◆ 右ポップアップメニューの「バイト列と見なして貼り付け」で、クリップボード上のデータオブジェクト長がゼロの場合には項目を淡色表示するよう変更</li> </ul>

---

## Zoocrypt という名称について

さまざまな暗号アルゴリズムの振る舞いを、16 進文字列の形で「見る」ことができる様子を動物園に例えて、Zoocrypt という名称にしました。

Zoocrypt にはどうやら、未確認動物やその追っかけといった意味があるようですが(cryptozoology の変形か?)、気にしない気にしない。というか、未確認動物は嫌いじゃないですよ。クッシーの模型を見に行ったら、つちのこフェスタも見物したし。

---

## 商標の表示

この文書中にある企業名・製品名は、各社の登録商標または商標です。

(以下余白)