XOR RANDOMIZER version 0.8 取り扱い説明書 2011/10/12 版

【ソフトウェア名称】
XOR RANDOMIZER

【種類】
乱数生成ソフトウェア

【取り扱い種別】
フリーソフトウェア

【動作環境】
WINDOWS 2000,XP,VISTA,7

WINDOWS 95,98,98SE,ME についても、動作するようにプログラム上は対応しておりますが、動作の保証は出来ません。

基本的に当ソフトウェアは UNICODE 環境での動作を想定して作成されました。
そのため、非 UNICODE 環境の場合 UNICODE 環境とは別のロジックで動作する箇所がありますが、その部分のテストが出来ておりません。
WINDOWS 95,98,98SE,ME での当ソフトウェアの起動は私の意図しない動作をする恐れがあるため、推奨しません。(一見正常に動作しているように見えたとしても、メモリリーク等が発生している可能性がありますので、重要な基幹システム等での起動は避けるべきです。)
仮に、WINDOWS 95,98,98SE,ME 日本語版で当ソフトウェアが正常に動作したとしても、WINDOWS 95,98,98SE,ME 英語版等の日本語版以外の環境では少なくとも文字化けする等の問題が発生すると考えられますし、最悪、システムに悪影響を与える動作をしかねませんので、WINDOWS 95,98,98SE,ME 日本語版で当ソフトウェアが正常に動作したとしても、WINDOWS 95,98,98SE,ME 英語版等の日本語版以外の環境では実行しないようにして下さい。

動作環境に挙げた WINDOWS 2000,XP,VISTA,7 のうち、テスト済みの環境は WINDOWS XP,7 のみですが、WINDOWS 2000,VISTA についても、UNICODE 対応環境であるため問題無く動作すると考えられます。
しかし、テストは未済であるため、何かしら意図しない動作が発生する可能性がある事を認識して下さい。

また、OS の問題ではなく、ハードウェア的に低速な記憶装置(例えば USB1.1 ポートに挿した USB メモリ等)では、動作が不安定になる場合がある事を確認しております。
当ソフトウェアは内蔵の HDD 上等のある程度高速な記憶装置上に格納し、使用する事を推奨します。

【開発環境】
Microsoft Visual C++ 2010 Express

当ソフトウェアは、世界で初めてチューリングマシンと等価なコンピュータ上で周期性の無い疑似乱数を生成する事を可能にした画期的なソフトウェアです。

基本的な原理は周期性を持っている疑似乱数と周期性の無いビット列の排他的論理和を取る事により実現しました。

【排他的論理和の真理値表】

P	Q	P XOR Q
0	0	0
0	1	1
1	0	1
1	1	0

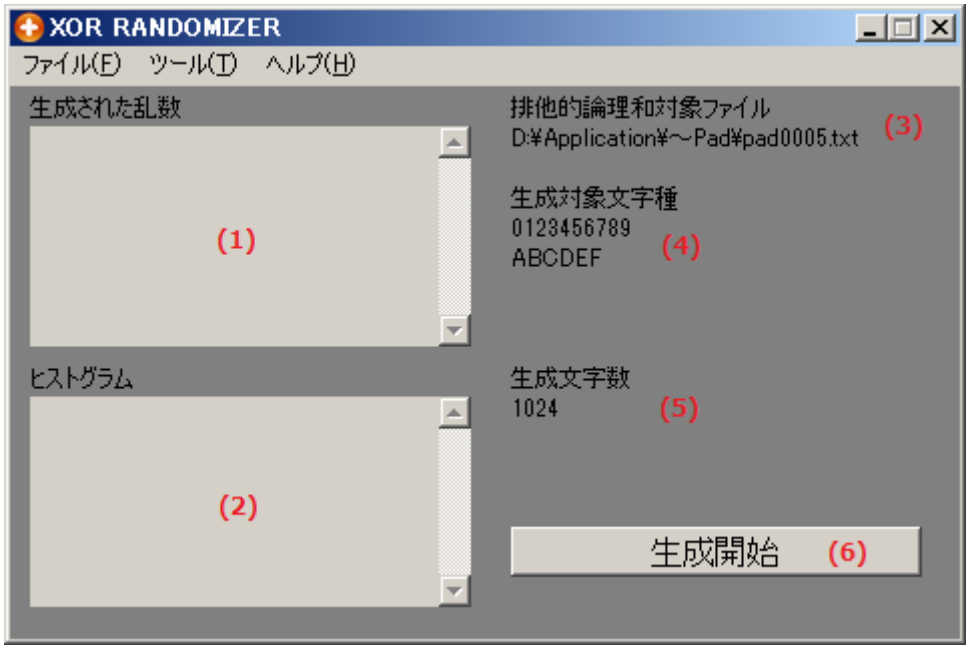
これまで、チューリングマシンと等価なコンピュータ上で周期性の無い疑似乱数を生成する事は不可能とされてきましたが、例えば上の排他的論理和の真理値表において、P を周期性のある疑似乱数に設定したとしても、Q を周期性の無い値(例えば$\pi, e, \sqrt{2}$等の無理数の各桁)を設定する事により、P XOR Q の値は周期性の無い値になり、かつ、疑似乱数のようにデタラメな値にもなります。

つまり、この方法を使う事により、周期性の無い疑似乱数をチューリングマシンと等価なコンピュータ上で生成する事が可能になるのです。

ここでは、当ソフトウェアの技術情報の詳細は割愛させて頂き、操作方法を中心に説明したいと思います。

技術的な情報を閲覧したい場合、私の Home Page であるトンデモ論文製作所
(http://tondemoronbun.web.fc2.com/index.html)までアクセスし、
”排他的論理和乱数生成器”の項目を参照して頂ければと思います。

それでは、使用方法について説明します。
XOR Randomizer.exe を起動してください。
すると以下のようなウィンドウが表示されます。
このウィンドウがメインウィンドウです。

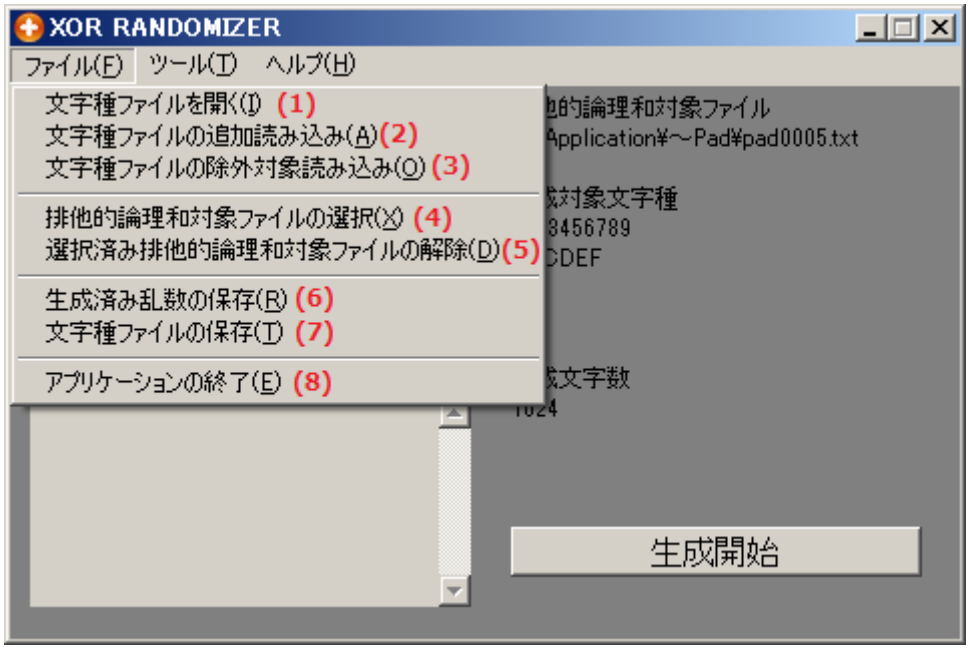


表示されている各項目は、以下のように機能しています。

(1) 生成された乱数列が表示されます。
(2) 生成された乱数列内の文字の種類毎のヒストグラムが表示されます。
(3) ソフトウェアが内部的に生成する疑似乱数と排他的論理和を取る対象データが記録されたファイルが表示されます。
(4) 生成される乱数の文字種が表示されます。
(5) 生成される乱数の桁数が表示されます。(*最大 65535 桁に制限されています)
(6) 乱数を生成する処理を開始する為のボタンです。

次に、メニュー項目について説明します。

ファイルの項目は以下のようになっています。



(1) 文字種ファイルを開く

生成対象となる文字が記されているファイルを指定する事で、生成対象文字種をそのファイル内に含まれている文字種に設定できます。

(2) 文字種ファイルの追加読み込み

現在設定されている生成対象文字種に、更に指定されたファイル内に記されている文字種を加える事が出来ます。

(3) 文字種ファイルの除外対象読み込み

現在設定されている生成対象文字種から、指定されたファイル内に記されている文字種を除外する事が出来ます。

(4) 排他的論理和対象ファイルの選択

疑似乱数生成器により生成された乱数と排他的論理和を取るデータを指定する事が出来ます。

(5) 選択済み排他的論理和対象ファイルの解除

疑似乱数生成器により生成された乱数と排他的論理和を取るデータを解除する事が出来ます。

この項目を選択した場合、疑似乱数生成器により生成された乱数とリテラルで指定された値(0x20)の排他的論理和を取った値が生成されます。

(6) 生成済み乱数の保存

生成された乱数列をファイルに保存できます。

(7) 文字種ファイルの保存

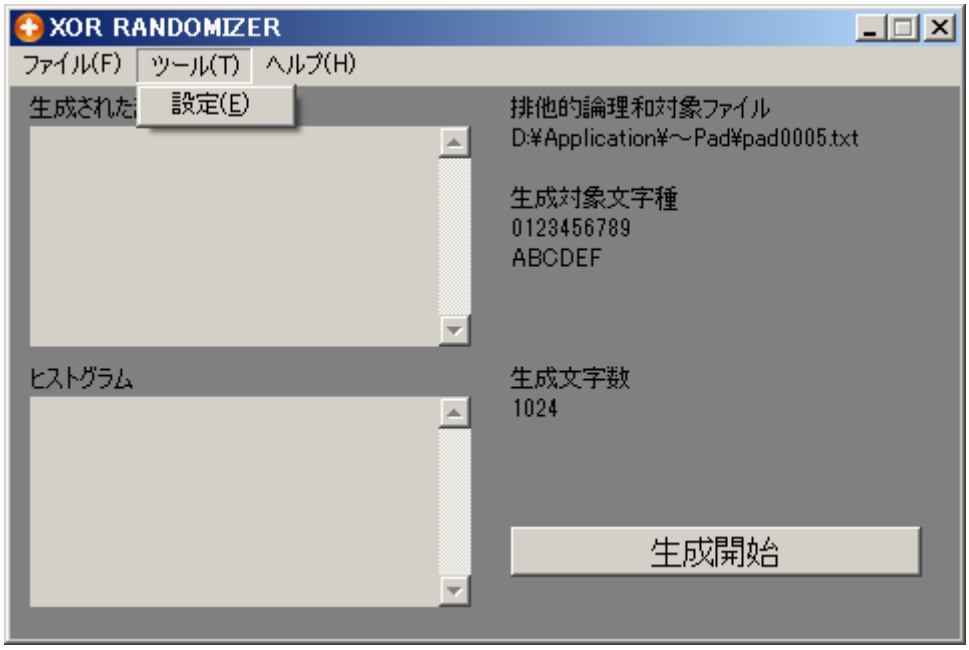
現在設定されている生成対象文字種をファイルに保存する事が出来ます。

(8) アプリケーションの終了

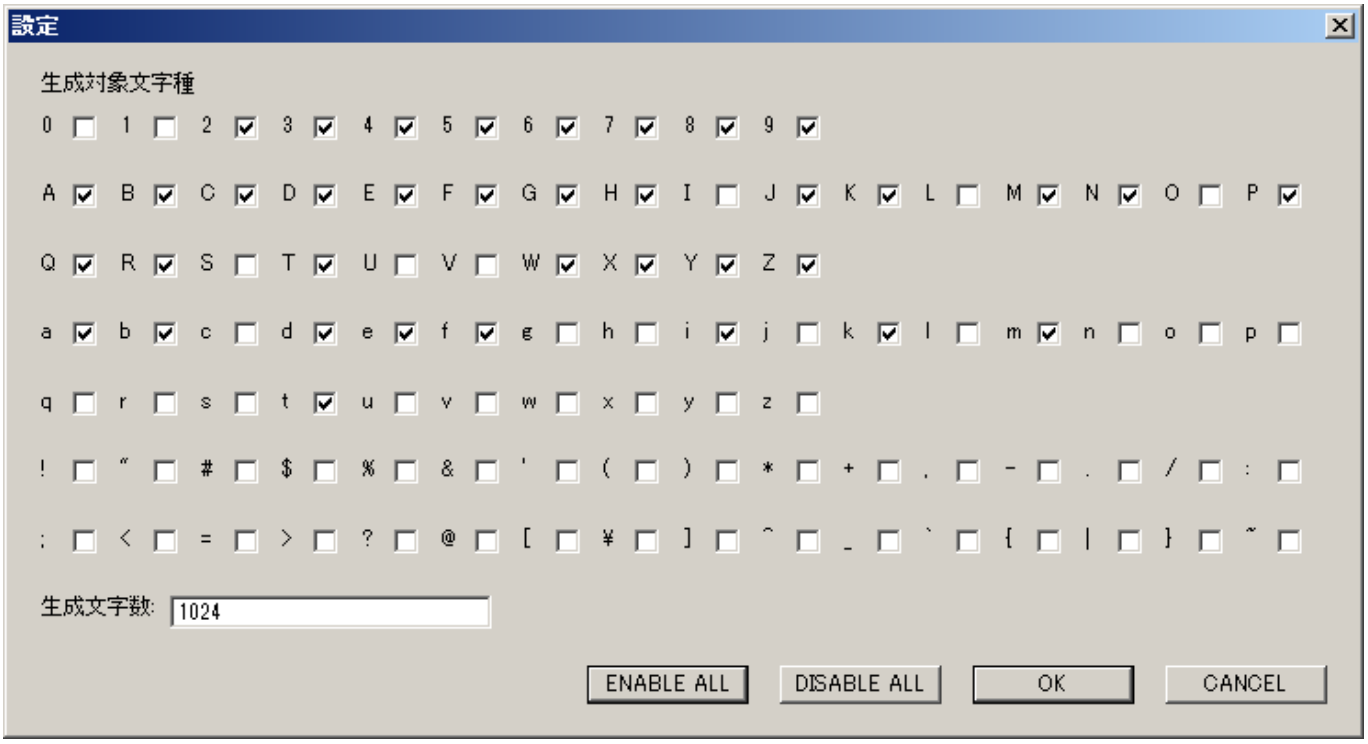
アプリケーションを終了します。

次に、ツール項目について説明します。

現在ツール項目は設定のみです。



この項目をクリックすると、以下のダイアログが表示されます。



(1) 生成対象文字種

チェックがついている文字が生成対象の文字種となります。

(2) 生成文字数

生成する文字数を 1～65535 桁までの範囲で入力します

(3) ENABLE ALL ボタン

ソフトウェアが対応している、生成可能な文字全てを生成対象とします。

(4) DISABLE ALL ボタン

生成対象となっている文字全てのチェックを解除します。

(5) OK ボタン

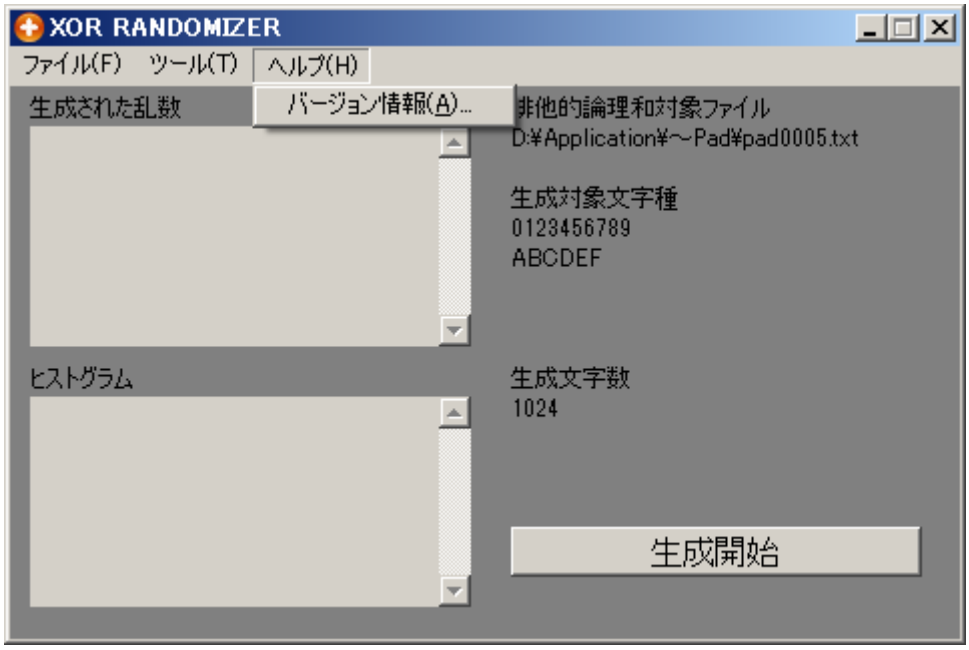
現時点で入力されている設定を確定し、ファイルに設定情報を記録します。

(6) CANCEL ボタン

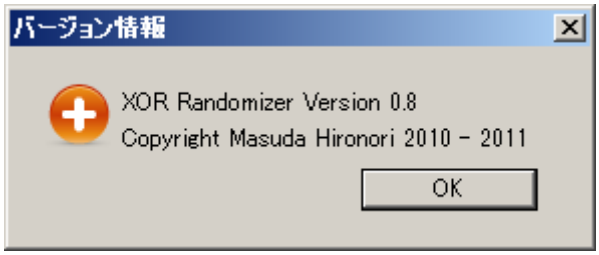
設定ファイルの内容を更新せず、ダイアログを終了します。

最後に、ヘルプ項目について説明します。

現在ツール項目はバージョン情報のみです。



この項目をクリックすると、以下のダイアログが表示されます。



当ソフトウェアと同じディレクトリに Catalog というディレクトリが同梱されていますが､その中にはよく使いそうな文字種ファイルを入れておきましたので、宜しければご使用ください。

0-9.txt:0～9 の文字のセットです。
　0123456789

LA-LZ.txt:A～Z の文字のセットです。
　ABCDEFGHIJKLMNOPQRSTUVWXYZ

SA-SZ.txt: a～z の文字のセットです。
　abcdefghijklmnopqrstuvwxyz

!-~.txt:記号全ての文字のセットです。
　!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~

LX16.txt:大文字 16 進数の文字のセットです。
　0123456789ABCDEF

SX16.txt: 小文字 16 進数の文字のセットです。
　0123456789abcdef

AVOIDANCE_CODE.txt:フォントによって見間違いやすい文字と記号を除いた文字のセットです。
　23456789ABCDEFGHJKMNPQRTWXYZabdefikmt

―周期性の無い乱数を生成するには―

当ソフトウェアの当初の目的である周期性のない乱数を生成する方法については、基本的な流れは、排他的論理和対象ファイルに周期性の無いデータを選択し、生成開始ボタンをクリックするという流れになります。

しかし、当ソフトウェアに於いては、一度に生成可能な乱数の桁数が 65535 桁までに制限されているため、排他的論理和対象ファイルの如何に関わらず、標準関数の乱数生成器でも生成可能な範囲内では周期を迎えることはないと思われます。

そのため、周期性の無い 65535 桁以上の乱数を生成したい場合は、周期性の無いデータの記されたファイルを 65535byte 毎に分割して、生成する度に排他的論理和対象ファイルを切り替えるという方法が有効です。

私の Home Page であるトンデモ論文製作所
(http://tondemoronbun.web.fc2.com/index.html)までアクセスし、
”排他的論理和乱数生成器”の項目を参照して頂ければ、より詳細な技術的情報や、様々な使用方法を閲覧する事が可能ですので、是非ご覧ください。

当ソフトウェアは排他的論理和対象ファイルに設定するデータを変更する事で、ある有限桁長の文字列が取り得る全ての文字列を包括する事が出来るので、排他的論理和対象ファイルに設定するデータを自分のオリジナルなものにする事で、同ソフトウェアを使用している他の人とは違った乱数が生成される特性があります。

ですので、周期性の無い乱数を生成するという本来の目的に関わらず、パスワード用の文字列の生成等、様々な場面で活躍できると思います。

URL: http://tondemoronbun.web.fc2.com/index.html
Mail:darmath1107@yahoo.co.jp