

PWGen *for Windows*



Generator of cryptographically strong passwords

USER MANUAL

Version 2.2.1

Licensing Information

By using, copying, distributing or modifying PWGen or a portion thereof you accept all terms and conditions contained in the file *license.txt* included in the package of this program.

Copyright Information

This software as a whole:

Copyright © 2002-2013 by Christian Thöing <c.thoeing@web.de>.

Portions of this software:

Copyright © 2006-2010 by Brainspark B.V.

*(implementations of AES and SHA-256 algorithms, base64 encoding;
part of the "PolarSSL" library)*

Copyright © 1996-2011 by Markus F.X.J. Oberhumer

("minilzo" compression library)

Copyright © 2000 by Arnold G. Reinhold

("diceware8k" word list)

Copyright © 2005-2010 by Aha-Soft

(toolbar icons)

World Wide Web

PWGen is hosted at sourceforge.net.

Homepage: <http://pwgen-win.sourceforge.net/>

Project page/downloads: <http://sourceforge.net/projects/pwgen-win/>

Contents

Introduction	3
Program Features	4
Step-by-Step Tutorial	5
Include Characters	5
Include Words	6
Format Password	7
Advanced Password Options	12
Generate Multiple Passwords	15
Generate Single Passwords	16
Random Pool	17
Main Menu	19
File	19
Tools	20
Options	21
Help	22
Additional Menus	24
System Tray Menu	24
Password List Menu	24
Command Line Options	25
Questions & Answers	26
Which security level is appropriate for my password?	26
Which security measures should I take when generating a strong password?	28
Is it possible to memorize those random passwords?	28
What about pronounceable passwords?	28
Can I use PWGen as a password safe?	29
Which kind of word lists does PWGen accept?	29
How shall I interpret the information about the random pool?	30
Technical Details	31
Random Pool	31
Text Encryption	33
High-Resolution Timer	35
Contact	37
Translations	37
Word Lists	37
Please Donate!	37
Acknowledgement	37

Introduction

The usage of a *password* is still the simplest way to control the access to specific resources. Although many other authentication factors have been developed—examples include identification cards, fingerprint or retinal patterns, voice recognition and other biometric identifiers—, password authentication systems are easier to implement for most applications, are relatively hard to break (note the term “*relatively*”!) and can thus provide accurate security, if used carefully. However, it is essential for the security that the password is *strictly kept secret*, and that it is chosen in a way that makes it hard for an attacker to guess it or to find it by try-and-error (that is, “brute force”). Both conditions are closely connected, but in a rather fatal way: Passwords which are easy to memorize for humans are for the most part *disastrous* in terms of security! Among these bad examples we find personal data (names of family members, pets, meaningful places, etc.), names and characters from favourite books, films or video games, simple words or character sequences (such as the famous “qwerty”), and so on. These passwords are for sure easy to memorize—but can often be guessed without much effort. How can we solve this dilemma?

There are many ways to choose good (that is, *secure*) passwords—but the best way is to let a random generator choose a password. If these passwords are long enough, it will take years, if not centuries, to find them by “brute force”. Computer programs like PWGen can assist you in generating random passwords, as humans are not very good at making up random numbers themselves. Unfortunately, random character sequences like `zi05FcV7J` are fairly hard to memorize (although this is possible and probably not as difficult as you might imagine), so you may want to try *passphrases* composed of words from a word list instead: Five words from a word list with 8000 words or more are sufficient in most cases to create a high-quality passphrase; the security can easily be increased by adding some random characters.

[Here is an interesting article](#) about problems regarding passwords chosen by humans.

The need for secure passwords has grown since the advent of the Internet and its many websites where the access to a certain resource (message board, user account, and so on) is controlled by a user name/password pair. Fortunately, since the invention of so-called *password safes*, you don't have to remember all these passwords any more—you just store them in the password safe which is protected by a “master password” (that must be memorized carefully, of course). As this master password is used to protect highly sensitive data, it should conform to the highest security level possible. The security level, which grows with increasing password length, is only limited by the user's ability to memorize random characters or words. With some effort, most people are certainly able to memorize a 90-bit password.

PWGen is capable of generating cryptographically secure random passwords and passphrases conforming to highest security levels. It can be used to generate master passwords, account passwords and generally all sorts of random sequences. It also offers the option to create many passwords at once. Just give it a try!

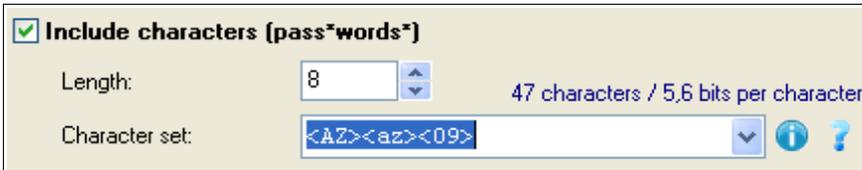
Program Features

- Password generation based on a **cryptographically secure pseudo-random number generator** (combination of SHA-256 and AES)
- **Entropy gathering** by measuring time intervals between keystrokes, mouse movements and mouse clicks; additionally, entropy from volatile system-specific parameters is collected in regular time intervals
- **Secure memory management:** memory reserved by the program is filled with binary zeros before release
- Generation of **passphrases** composed of words from a word list
- **Pattern-based password generation** (formatted passwords) provides nearly endless possibilities to customize passwords to the user's needs
- Numerous **password options** for various purposes
- Generation of **large amounts of passwords** at once
- Secure **text encryption** (AES with 256-bit key)
- **Multilingual support**
- Runs on all 32-bit & 64-bit Windows versions (beginning with *Windows 95 OEM Service Release 2*)

Step-by-Step Tutorial

In this section I want to elaborate on each step in creating a password. The main functions of the program are accessible in PWGen’s main window, where you can adjust the parameters for password generation. Here we go:

Include Characters



- Check “**Include characters**” if you want to include characters in your password. Enter the desired length of the character string in the “**Length**” field (maximum 20,000).
- Enter the desired character set (that is, all the characters that may occur in your password) in the field below or choose one from the drop-down list. Note that each character must only occur once—otherwise, it will not be accepted. As a non-unicode application, PWGen can “only” accept 226 ANSI characters (#30 to #255). You may use the following placeholders to abbreviate the sequence:

Placeholder	Meaning	Character set
<AZ>	upper-case letters	ABCDEFGHIJKLMNOPQRSTUVWXYZ
<az>	lower-case letters	abcdefghijklmnopqrstuvwxyz
<09>	digits	0123456789
<Hex>	upper-case hexadecimal symbols	0123456789ABCDEF
<hex>	lower-case hexadecimal symbols	0123456789abcdef
<base64>	base64 symbols	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789+/ /
<easytoread>	like <AZ><az><09>, but without similar-looking (“ambiguous”) characters (B8G6I1l 00QDS5Z2 by default). See “Advanced Password Options” for more options.	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789 <i>without ambiguous characters</i>
<symbols>	additional symbols accessible via the keyboard	!"#\$%&'()*+,-./:;<=>? @[\\]^_`{ }~
<brackets>	brackets	()[]{}<>
<punct>	punctuation marks	,. ; :

<high>	higher ANSI characters (symbols #127 to #255)	<i>(characters depend on the current ANSI code page)</i>
---------------------	---	--

- You may provide a **comment** included in square brackets [...] at the beginning of the entry. All characters in this comment will be ignored by PWGen. For example, entering [This is a comment.]<AZ> will add only upper-case letters to the character set. Note that the comment must be placed right at the beginning; otherwise, it will be treated as a normal sequence of characters!
- The character set will be updated as soon as you leave the input field, e.g., by clicking on another interaction element. The number of bits per character is displayed on top of the “Character set” field; it is calculated as $\log_2 N$, where N is the number of characters and \log_2 is the logarithm base 2. Due to the limitation of 226 ANSI characters the number of bits per character is limited to 7.8.
- Clicking on the **symbol**  opens a quick help box containing the most important information.
- Clicking on the **symbol**  opens a message box where each character of the currently loaded set is displayed.
- **Errors** occur when the set contains less than two unique characters. Keep that in mind if you want to generally exclude ambiguous characters (see below).

Include Words

Include words (pass*phrases*)
 Number: 8192 words / 13,0 bits per word
 Word list file:  
 Combine words with characters

- Check “**Include words**” if you want to include words from a word list in your password. Enter the desired number of words into the “**Number**” field (maximum 200).
- By default, PWGen uses an internal English word list containing 8192 (2^{13}) words. If you enter <default> into the “**Word list file**” field or if you simply leave this field blank, PWGen will use its internal list. However, you may enter the name of your own word list file into this field; alternatively, you can click on the **symbol**  to browse through your folders and select a file.
- The word list will be loaded as soon as you leave the input field, e.g., by clicking on another interaction element.
- To reload a word list from an already loaded file, load the default list, then load the

previous file again by selecting it from the drop-down list.

- By default, PWGen accepts words that are not longer than 30 characters; however, you can reduce this number in the “*Advanced Password Options*” dialog (see below). The number of bits per word is calculated as $\log_2 N$ (with N being the number of words) and will be displayed on top of the “*Word list file*” field. The size of word lists is limited to 1,048,576 (2^{20}) words.
- Clicking on the **symbol**  will show some information about the currently loaded word list.
- **Errors** occur when the word list cannot be opened (for whatever reason), or when it contains less than two valid words.
- Check “**Combine words with characters**” to generate passwords as a combination of words with characters. This means that each word will be combined with one or more characters, depending on the number of words and the number of characters, respectively. Example of 3 words combined with 8 characters by a “-” symbol: `putty-fuV umbra-Sxq faint-fT`.

Format Password



- Check “**Format Password**” to format your password or passphrase generated via *Include characters* or *Include words*, respectively (see above). Additionally (or alternatively), you can use format specifiers and placeholders to introduce random characters from various character sets, and random words from the word list.
- Format strings can contain two types of characters, **format specifiers** and **literal characters**. Literal characters are copied verbatim to the resulting password. Format specifiers begin with a “%” character and can be used to insert random characters/words or manipulate the input sequence (e.g., by randomly permuting a character sequence). A literal percent sign can be inserted into the resulting password by the sequence `%%`.
- Format specifiers have the following form: `%{number}{specifier}`. All format specifiers begin with a “%” character. The optional *number* argument indicates how many times the format command is to be repeated; it can be a decimal number in the range from 1 to (theoretically) 99,999. If *number* is not specified, “1” is assumed by default. The *specifier* argument is the actual format specifier or placeholder for a character from a certain character set (see below for a list of format specifiers). For example, `%20a` means “insert 20 alphanumeric characters into the formatted password”, whereas `%a` means “insert 1 alphanumeric character”. Note that not all

format specifiers recognize the *number* argument.

- The **length of the formatted password** is currently limited to 32,767 bytes.
- Some format specifiers have **special functions** (“{N}” means that the *number* argument may be specified optionally):
 - **%P**: Insert the password generated via *Include characters* and/or *Include words*. The password can be inserted only once! A “warning” message will be displayed on top of the input field, if ...
 - “*Include characters*” or “*Include words*” is checked, but **%P** is not specified in the format string (“%P is not specified.”);
 - **%P** is specified, but neither “*Include characters*” nor “*Include words*” is checked (“%P: password not available.”);
 - the password is too long to insert it, that is, inserting the full password exceeds the size limitation of the formatted password (“%P: password too long.”).

Example: Entering `This is your password: "%P"` may result in a password like this: `This is your password: "Zq3wu9gL"`.

- **%{N}w** or **%{N}W**: Insert random word(s) from the currently loaded word list (see above). In case of multiple words ($N > 1$), the words are separated by a space if the specifier is **w** (lower-case), or they are not separated at all if the specifier is **W** (upper-case). Note that *Include words* doesn't have to be checked in order to use the word list for formatted passwords

Example: `%5w` → `dod zion belt xylem avery`

- **%{N}[...%]**: Repeat the sequence included in the brackets **%[** and **]% N** times. Repeat sequences may be nested up to 4 times (e.g., `%5[...%4[...%3[...%2[...%] %] %] %]`).

Example: `%5[%a%d%]` → `u9o2p9r2a8`

- **%{...%}**: Randomly permute the sequence included in the brackets **%{** and **%}**. Nesting is not possible (because it doesn't make any sense). Please note that, when PWGen calculates the quality/security of the resulting password, it does *not* take into account the security gain caused by the random permutation, which is very likely unless the permuted sequence consists of characters from only one character set (in the latter case, there wouldn't be any increase in security). Calculating this security gain is actually not that trivial, so I haven't

implemented this feature yet. However, you can try to calculate the gained security bits by this formula:

$\log_2(N! / (n_1! n_2! \dots n_i!))$, where N is the total number of characters in the permuted sequence, and n_i are the numbers of characters from a specific character set.

Examples: (1) `%{hello world!%}` → `ldloor w!lhe`; (2) `%{%9l%d%}` → `euvk8bfifg`

- `%{N}<...%>`: Treat the sequence included in the brackets `%<` and `%>` as a character set, and choose N random characters from this set. Note that within this sequence, format specifiers don't have any effect (except for `%>` which ends the sequence); each character will be used "as-is". Note that it is possible to use abbreviation codes, that is, placeholders for character sets (see "Include words" above), such as `<AZ>`, `<09>`, and so on.

Example: `%10<<az>0123%+/%>` → `r0/bpya%0y`

- **Comments** included in square brackets `[...]` may be provided at the beginning of the sequence (and only there!).
- Here is a complete list with the format specifiers which are currently supported by PWGen (the placeholders for the character sets are identical to those defined by the built-in password generator of [KeePass](#)):

Format specifier/ placeholder	Meaning	Character set
1) Placeholders for random characters from various character sets (number argument may be specified optionally in all cases)		
<code>%x</code>	insert random character(s) from the user-defined character set (as given in the input field below "Include characters")	(user-defined)
<code>%a</code>	lower-case alphanumeric	abcdefghijklmnopqrstuvwxyz0123456789
<code>%A</code>	mixed-case alphanumeric	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789
<code>%U</code>	upper-case alphanumeric	ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789

%E	mixed-case alphanumeric, but without ambiguous characters	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789 <i>without ambiguous characters</i>
%d	digit	0123456789
%h	lower-case hexadecimal	0123456789abcdef
%H	upper-case hexadecimal	0123456789ABCDEF
%l	lower-case letter	abcdefghijklmnopqrstuvwxyz
%L	mixed-case letter	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
%u	upper-case letter	ABCDEFGHIJKLMNOPQRSTUVWXYZ
%v	lower-case vowel	aeiou
%V	mixed-case vowel	AEIOUaeiou
%Z	upper-case vowel	AEIOU
%c	lower-case consonant	bcd fgh jkl mnp qrst vwxyz
%C	mixed-case consonant	BCDFGHJKLMNPQRSTUVWXYZbcd fgh jkl mnp qrst vwxyz
%z	upper-case consonant	BCDFGHJKLMNPQRSTUVWXYZ
%p	punctuation marks	, . ; :
%b	brackets	() [] {} <>
%s	special symbols (may be user-defined)	! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~ (or user-defined)
%S	mixed-case alphanumeric and special symbols	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~ (special symbols may be user-defined)
%y	higher ANSI characters (symbols #127 to #255)	(characters depend on the current ANSI code page)
2) Special format specifiers (possible usage of number argument is indicated by {N})		
%P	insert password generated via <i>Include characters</i> and/or <i>Include words</i> ; password may be inserted only once	
%{N}w	word from word list; multiple words are separated by a space	
%{N}W	word from word list; multiple words are concatenated without any separators	
%{N}[repeat input sequence included in the brackets <i>N</i> times; maximum nesting depth is 4	
%]		

<code>%{N}{</code>	randomly permute formatted sequence included in the brackets
<code>%}</code>	
<code>%{N}<</code>	treat the character sequence included in the brackets as a character set and insert <i>N</i> characters from this set
<code>%></code>	

- With the format option at hand, you can easily define your own **rules for creating passwords for specific purposes**. Some examples are given in the following table.

Rule	Format sequence
4 upper-case letters, 4 lower-case letters, 2 digits, 1 special symbol <i>in random order</i>	<code>%{4u%4l%2d%s%}</code>
8 alphanumeric characters, of which at least 1 is a letter and at least 1 is a digit	<code>%{6A%L%d%}</code>
4 artificial words, where each word consists of 6 letters and is composed of alternating consonants and vocals	<code>%4[%3[%c%v%] %]</code>
5 words from the currently loaded word list, each combined with 2 digits	<code>%5[%w-%2d %]</code>
random permutation of upper-case letters	<code>%{ABCDEFGHJKLMN OPQRSTUVWXYZ%}</code>
10 alphanumeric characters, first character must not be a lower-case letter	<code>%U%9A</code>
random product ID	<code>%5d-0EM-%7d-%5d</code>
hexadecimal 128-bit key (e.g., WEP key)	<code>%32h</code>
random MAC address (48-bit)	<code>%5[%2h-%]%2h</code>
12 random base64 symbols	<code>%12<<base64>>%></code>
128-bit key in binary notation	<code>%128<01%></code>
8 random characters from the German alphabet	<code>%8<<AZ><az>ÄÖÜäöüß%></code>
3 artificial <i>German</i> words, where each word consists of 6 letters and is composed of alternating consonants (including <i>ß</i>) and vocals (including <i>ä, ö</i> and <i>ü</i>)	<code>%3[%3[%<bcdfghjklmn pqrstvwxyzß%>%<aeiouäöü %>%] %]</code>

Advanced Password Options

Advanced

- Clicking on this button opens a dialog where you can activate or deactivate some “advanced” password options:
 - **Exclude ambiguous characters:** Excludes those characters from character sets that might be confused with other similar-looking characters (that is, by default, `B8G6I1l | 00QDS5Z2`). As this option reduces the size of the character set, the password security will be reduced accordingly. This option also applies to formatted passwords and affects all character sets encoded by the placeholders `%a`, `%A`, `%U`, etc.
 - **First character must not be a lower-case letter:** Activate this option if you don't want the first password character to be a lower-case letter (a-z). This might be useful when copying passwords to certain word processors or e-mail programs that automatically convert the first character to upper-case in case it's a lower-case letter, thereby manipulating the original password. If the first character belongs to a word, it will simply be converted to upper-case. If it is, however, a random character, PWGen will choose a character that is *not* a lower-case letter (for example, if the character set consists of lower-case letters and numbers, the first character will be a number). If the character set does not contain any non-lower-case letters, the first character will be an upper-case letter. Note that activating this option (slightly) reduces the password security.
 - **Don't separate words by a space:** By default, PWGen inserts spaces to separate words in passphrases. Select this option to deactivate this behaviour.
 - **Don't separate words and characters by a '-' character:** By default, PWGen inserts a minus sign (“-”) between a word and a character (when the option “Combine words with characters” is selected). Select this option to deactivate this behaviour.
 - **Reverse default order of character/word combinations:** When you generate passwords/passphrases consisting of both characters and words, PWGen by default puts the characters at the beginning and appends the words. If “Combine words with characters” is activated, a subset of the character sequence is appended to each word (e.g., `word1-3wp word2-k8#`). If you activate this option, however, the order is reversed in each case: If “Combine...” is activated, each word is appended to a subset of characters (e.g., `3wp-word1 k8#-word2`); otherwise, the words are put first, and the characters are appended.

- **Include at least ...:** Activate these options in order to force the program to include at least one character from the given character sets (upper-case letters [A-Z], lower-case letters [a-z], digits [0-9], and special symbols [!"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~], or user-defined symbols, see below]). If the user-specified character set does not contain any characters from a pre-defined set, the resulting passwords will contain exactly one character from this pre-defined set. Otherwise, they will contain *at least* one character from this set. For example, if you specify a “<az>” character set and activate all of the aforementioned options, PWGen will generate passwords like this one: `t]cXy7cu`. (If the desired password length is less than 4, not all characters can be included, of course.) Depending on the user-specified character set, selecting these options can—rather slightly—reduce (but in some cases also *increase*) the password security. Note that these options do not affect the generation of *passphrases* or formatted passwords.
- **Exclude repeating consecutive characters:** Choose this option if you want to avoid repeating sequences of the same character, as in `r3aa5ZiK` or `E0u555Wp`, for example. If this option is activated, each character in the sequence will be different from the previous one. This option certainly reduces the security of the passwords, but the extent of this reduction strongly depends on the size of the user-defined character set: For large character sets, this effect becomes almost negligible. For example, if your set contains 64 characters (6 bits per character) and the password length is 16, the loss of entropy is only 0.34 bits of 96 bits (0.35%). The effect is more pronounced for small character sets: If your set contains only 4 characters (2 bits per character) and the password length is 48, the loss of entropy is 19.5 bits of 96 bits (20.3%). This option also applies to formatted passwords.
- **Exclude duplicate entries in password lists:** Select this option if you want to generate “unique” password lists where each entry occurs only once. Generating unique lists may take considerably longer than usual because PWGen has to search through the entire list before adding a new password. Note that, in certain cases, it might not be possible to generate a complete password list using the parameters given by the user; for example, if the user chooses “0123456789” as the character set (= 10 possibilities) and “3” as the password length, it’s not possible to generate a list of more than 1,000 (= 10^3) unique entries, since the total number of possible password permutations is limited to this exact number. As a consequence, the security of the entire password list is decreased, because the number of possibilities decreases from top to bottom in the list. However, when a single password independent from the rest of the list is considered, it retains its designated security. Note that you can cancel the generation process any time.

- **Convert all words in word lists to lower-case:** When loading word lists, each word in the list must occur only once, and the words are compared in a case-sensitive manner. So if you don't want the list to contain both upper-case and lower-case words, you can activate this option and thus force PWGen to convert each letter in a word to lower-case.
- **Redefine ambiguous characters:** The set of ambiguous characters is defined as `B8G6I1l | 00QDS5Z2` by default. Redefining this set also affects the other pre-defined character sets (i.e., `<AZ>`, `<az>`, `<09>`, etc., as well as all the character sets accessible via the “*Format Password*” option). You can also supply this character set in *groups* of similar-looking characters, separated by a space. Then, each group of this set is only excluded from the user-defined character sets if they contain *two or more* characters from this group; if only one character is used, the group will *not* be excluded. Please note that
 - a group must consist of at least two characters;
 - each character must only occur once in the whole sequence, that is, it cannot be part of more than one group;
 - you can still exclude the space character itself by supplying it at position 1 or 2 in the sequence (e.g., `1 00QD` is not a valid definition of groups, so the sequence will be treated as a “normal” set of ambiguous characters, including the space character);
 - group definitions exclusively apply to user-defined character sets (i.e., via option “*Include Characters*” and via format specifier `%< . . . %>`). For all pre-defined character sets, *all ambiguous characters* present in the sequence will be excluded, independent from any group definitions!

Example: Enter `B8 G6 I1l | 00QD S5 Z2` to define *six groups* of similar-looking characters. If your character set is defined as `<az><09>` (that is, lower-case letters and digits), only the characters `1` and `l` from group 3 will be excluded, whereas all the characters from the other groups remain unaffected, because your character set doesn't contain any other characters from these groups which might be confused with the characters in the set. All groups will be excluded, however, if you add upper-case letters to the set.

- **Redefine special symbols:** The set of special symbols is defined as `!"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~` by default. Redefining this character set affects the `<symbols>` character set, the option “*Include at least one special symbol*” and the corresponding placeholder character sets in the “*Format Password*” option (see above).

- The field **Maximum length of words in word lists** should be self-explanatory. When you load a word list, only those words the lengths of which do not exceed this value will be added to the list. The maximum word length can range between 1 and 30 (default). Changing this value is particularly useful to filter out very long words. It may also be helpful in reducing the word list size in case of very long lists. Note that this option does not apply to the default word list but only to lists from an external source.
- Most of these options can potentially—but not necessarily!—reduce the security of the resulting passwords. See the corresponding notes for the options above for more details.

Generate Multiple Passwords



- If you want to create more than one password and display the list in a separate window, enter the exact number into this field (maximum 2,000,000,000) and click on “**Generate**”. The program will open a window showing the password list.

Note: PWGen is a 32-bit application and thus cannot handle more than 2 gigabytes (2,147,483,647 bytes) of RAM. Considering a safety factor of ~4 for various buffering operations, PWGen limits the size of memory buffers for password lists to 500,000,000 bytes. For example, if you want to generate 10 million 8-character passwords, a memory buffer of $10,000,000 \times (8 + 2)$ bytes = 100,000,000 bytes \approx 100 megabytes is required (8 + 2 to account for line break characters); however, the actual memory requirement may be much larger (up to 600 megabytes) when the memory buffer has to be enlarged, or when the list is copied to the window control that displays it on the screen. Thus, generating very large lists may exceed the available memory (of your system or of the program, respectively) and cause an “out of memory” error.

- If you want the list to be directly written to a data storage device (hard disk, USB stick, etc.) instead of being displayed in a window, click on the button  and specify a file where the list is to be stored. PWGen will write each password directly to this file without any limitations regarding RAM requirements. Instead, this process only requires negligible 64 kilobytes of memory, and the amount of data that can be generated is only limited by the free disk space on the device. Thus, you can theoretically generate several gigabytes of data (and more ... but note that I have not tested this myself!).

Note that if the option “*Exclude duplicate entries*” is activated, the computational effort is much greater compared to the generation in memory because for each

newly generated password, the entire file contents that have been written so far have to be read into memory again.

- If you generate a larger amount of passwords (more than, say, 1,000 passwords), PWGen shows a progress window with a “*Cancel*” button. Click on “*Cancel*” to stop the process and show a list of the passwords which have been generated so far.

Generate Single Passwords



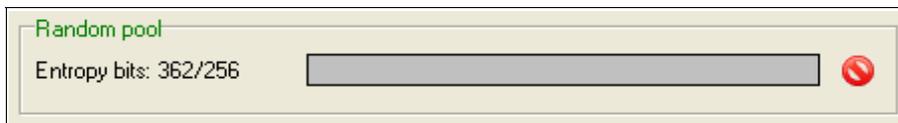
- If you want to create one single password, click on “**Generate**”. PWGen will display the password in the box.
- The estimated security of the password is indicated by the coloured “**security bar**” below the password box. The colour of this bar ranges from red-orange to light green, that is, from “*low security*” to “*high security*”, where the limit for “*highest security*” has been—more or less arbitrarily—set to 128 bits (which is just some kind of a “magic number” for cryptographers). Always stay on the green side when generating “serious” passwords!
- Note that the **security of a single password is limited to 256 bits**, since the “random pool” which is used to generate passwords has an effective size of 256 bits (which corresponds to the message-digest length and the key length of SHA-256 and AES, respectively). However, if the random pool hasn’t been filled with enough entropy before password generation, the actual security is lower than the value shown in this field—to be more precise here, the pool must have been filled with *at least* N bits with N being the password security. For more information about how to interpret these values, see *Questions & Answers*.
- If—for whatever reason (severe paranoia?)—you want to create a password with a security of more than 256 bits, you may concatenate two or more 256-bit passwords to a 512-bit (or more) password. This is done as follows: First, collect entropy for a 256-bit password, generate it and store it somewhere; then collect entropy for a second password and concatenate that with the first one. Note, however, that there are *absolutely no concerns* that it will ever be possible to break 256-bit keys.
- PWGen also offers you the possibility to test your own password creations. Right-click in the password box and activate the option “**Enable Password Testing**”. Now you can type into the box, and PWGen *estimates*(!) the security/quality (in bits) of

the entered sequence. The colour of the label (“*xx bits / xx characters*”) will change from blue to teal, indicating that the displayed value in bits are estimated and therefore not exact. Note that the underlying algorithm is quite simple and does not make use of any sophisticated statistical tests for randomness (e.g., autocorrelation, runs test, entropy estimation, etc.), as passwords—even though they may be chosen randomly—are typically much too short for these kinds of tests to be applicable. As a consequence, the algorithm tends to *underrate* passwords (consisting of random characters) and to *overrate* passphrases (consisting of random words from a word list). Furthermore, please note that PWGen does *not* test for popular (= bad) passwords like “qwerty”, “1234”, and so on. So please apply some common sense when judging passwords!

If you deactivate this option, the contents of the password box is read-only and thus cannot be modified by the user.

- Clicking on the **symbol**  hides the password characters behind asterisks (***).
- You can change the font which is used to display the password by right-clicking in the box and selecting the entry “**Change Font**” from the context menu.

Random Pool

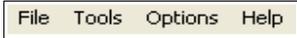


- This progress bar informs you about the current state of the random pool, that is, the amount of entropy bits the pool can currently provide. Whenever you generate one or more passwords, $N \cdot p$ bits will be “consumed” from the pool (N = number of passwords, p = amount of entropy present in every password).
- You can provide entropy by moving your mouse, by clicking with your mouse and by typing on your keyboard. Furthermore, the program regularly collects entropy from various system parameters.
- As stated above, the random pool can yield a maximum Shannon entropy of 256 bits. However, PWGen also shows the non-limited entropy amount (possibly *exceeding* 256 bits), which might be of your interest if you don’t trust PWGen’s estimations regarding the entropy content of the different sources. So the message “*Entropy Bits: 416/256*” means that you have provided 416 entropy bits so far, and that the random pool has reached maximum entropy *according to PWGen’s estimations*. The non-limited entropy counter is increased (up to 9,999 maximum) as long as you don’t generate any passwords. Whenever you “consume” entropy from the pool, the “total entropy” counter will assume a value less than 256 bits, of

course. Additionally, there is a *total entropy counter* which counts the amount of entropy gathered by the program during its runtime (up to 999,999,999 maximum), and which is *not* decreased after consuming entropy from the pool. The value of this counter is displayed in the context menu of the progress bar (right-click). You can reset the counters by selecting “*Reset Counters*” from the menu (this won’t affect the actual contents of the random pool in any way).

- If the blinking of the progress bar irritates you, click on the **symbol**  in order to hide the entropy progress.

Main Menu

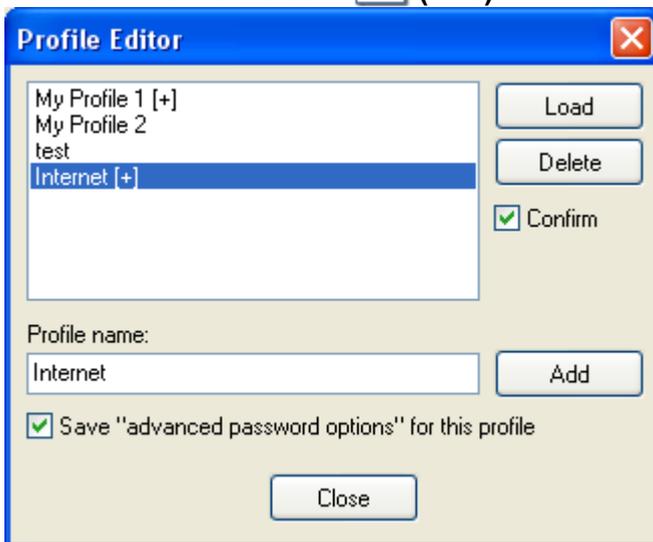


Note that some of the following functions can also be accessed via the toolbar buttons right below the main menu.

File

- **Profile:** Shows a submenu containing all password generation profiles. To load a profile, select the respective menu item or press the designated key combination (Shift+Ctrl+0, 1, 2, ..., A, B, C ...). All settings for generating passwords (including advanced password options, if saved additionally) will be restored according to the selected profile.

- **Profile / Profile Editor**  (F10):



In this dialog, you can manage your profiles, that is, add/overwrite, load and delete profiles. Note that the number of profiles is limited to 36, and that profiles which contain additional advanced password options are marked with the sequence “[+]”.

- **Add/overwrite profiles:** Enter the name of the profile into the “**Profile name**” box and click on “**Add**”. Activate “**Save 'advanced password options' for this profile**” if you want to explicitly store the advanced options with this profile; if you leave this option deactivated instead, the current advanced options will never be modified when loading this profile. If a profile with an identical name already exists and “**Confirm**” is activated, you will be asked to confirm the overwriting.
- **Load a profile:** Select the profile of your choice and click on “**Load**”, or double-click on the entry.
- **Delete profiles:** Select the profile(s) you want to delete and click on “**Delete**”. If “**Confirm**” is activated, you will be asked to confirm the deletion.

Note that there are no “OK” and “Cancel” buttons in this dialog; all changes to the profiles are made active instantaneously, and there is no possibility to undo an accidental deletion within a PWGen session. To restore the profile settings to the “start-up state” (initial settings loaded from the INI file on start-up), close the window, make sure that the *Options / Save Settings on Exit* menu item is deactivated, and restart the program.

- **Exit** : Exits the program.

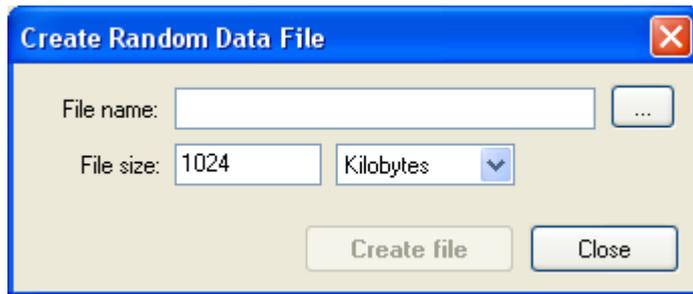
Tools

- **Clear Clipboard**  (F2): Securely clears the text contents of the clipboard. The text buffer is overwritten with binary zeros before deallocation. An error message is shown when the clipboard could not be opened (but no message is shown in case of success).
- **Encrypt/Decrypt Clipboard**  (F3/F4): Encrypts or decrypts the clipboard text and stores the result in the clipboard. At first you have to enter a password which can be of any length. The clipboard text (if there’s any) will then be en-/decrypted using a secure 256-bit key derived from this password. The encryption algorithm is AES with a key length of 256 bits. Note that the text is compressed before encryption. (For more information about the exact encryption procedure, see *Technical Details* below.) The ciphertext will be converted to the base64 format consisting of letters (A-Z, a-z), numbers (0-9) and the symbols “+”, “/” and possibly “=”. In the resulting text, lines are automatically wrapped after 76 characters. It is, of course, strongly recommended to check the encryption before discarding the plaintext. If decryption fails, you probably entered a wrong password. Another possibility is that the text is corrupted, that is, it has been modified in some (bad) way. Note that decryption will always fail if one or more characters in the ciphertext have been altered (except for characters involved in line breaks). Inserting or removing line breaks in the ciphertext does *not* pose a problem.

The clipboard encryption is not intended for encrypting very long texts. (Please use a file encryption utility for this purpose.) To avoid memory problems PWGen currently limits the text length to 64 megabytes.

Important note: The encryption scheme has been changed in version 2.1.0. For backwards compatibility, that is, to decrypt ciphertexts generated with older versions, you can select the option “PWGen <2.1.0” when decrypting texts. It is strongly recommended to re-encrypt any existing ciphertexts with the new version. The encryption scheme was changed in order to enable using other encryption algorithms (such as *Serpent* and *Twofish*) in future versions of PWGen.

- **Create Random Data File**  (F5):



Creates a file consisting of purely random (that is, *cryptographically random*) data. First, select an existing file (by clicking on the **Browse** “...” button) or enter the **name of the file** where the random data is to be stored. Then enter the desired **file size** in *bytes*, *kilobytes* (1,024 bytes) or *megabytes* (1,048,576 bytes) and select the appropriate list entry. Note that you can enter floating-point numbers (e.g., “0.5”, “3.14”, “2.25e3”, etc.), but the number of bytes to write will be converted to an integer, of course. In case of a file size of more than 1 megabyte, you have the possibility to stop the creation process by clicking on the “*Cancel*” button in the progress window. *Note:* PWGen cannot handle file sizes >2 gigabytes. Entering file sizes greater than 2,147,483,647 bytes will cause an error. If you need to generate very large files, please contact me. I will then consider adding this feature in a future release.

Options

- **Language:** Changes the program language. You will receive a warning message if the language version is not compatible with the program version. The program has to be restarted to load the language file. If you downloaded a language file from the PWGen homepage, extract it into the program directory. PWGen will find it on startup and add the language as an item to this menu.
- **System Tray Icon:**
 - **Show Constantly:** Shows PWGen’s program symbol in the system tray (next to the system clock). Clicking on the symbol will open a menu where several functions of the program are accessible.
 - **Minimize Program to System Tray:** If checked, PWGen’s taskbar button will be hidden when the program is minimized, and the program symbol will be displayed in the system tray instead. If “*Show Constantly*” is unchecked, the symbol will be removed when restoring the application.
- **Set Hot Key:**



The “hot key” option allows you to associate a special key combination with PWGen. Whenever you press the designated key(s), PWGen is called and performs an action of your choice: The main window can be shown or restored (if minimized), and/or password(s) can be generated.

- **Activation:** Activate “*Activate hot key*” to associate a hot key with PWGen. Place your cursor inside the input box on the right and press the desired key combination, for example Ctrl+Alt+P, Ctrl+F12, Alt+F8, etc.
- **Actions:** Select the action(s) which are to be performed when you press the hot key on the keyboard. Note that when “*Generate password and show it in a message box*” is selected from the list, the main window will always be restored, so that the message box can be placed in the foreground; if you close the box afterwards, the program is minimized again if necessary.

Note that some key combinations may already be registered by other applications and thus not be accessible.

- **Save Settings on Exit:** If checked, all program settings will be saved in an *.ini* file (default: *PWGen.ini*) when the user exits the program.
- **Save Settings Now:** Saves the settings instantaneously.

Help

- **Open Manual**  **(F1):** Opens this manual.
- **Visit Website:** Opens the homepage of PWGen in your default browser.
- **Donate:** Donations to the project via [PayPal](#) are highly appreciated!
- **Timer Info:** Shows information about the high-resolution timer (HRT) called by PWGen whenever you press a key, move your mouse, or click with your mouse (refer to *Technical Details* for more in-depth information). “N/A” means that a HRT is not available on your system; a low-resolution system date and time value is used

instead, providing a resolution in the millisecond range (roughly 1-15 ms). Note that it is recommended to run PWGen on systems where a high-resolution timer (*RDTSC* or *QueryPerformanceCounter*) is available. The current 64-bit value (ranging from 0 to 18,446,744,073,709,551,615) of the timer is also displayed in the message box.

- **About:** Shows copyright information about the program.

Additional Menus

System Tray Menu

The system tray menu, which opens when you click on the PWGen symbol in the system tray, allows you to access some useful functions of the program. In addition to the self-explanatory functions and those already explained above, there are two new menu items that are only available in this menu:

- **Generate Password:** This function quickly generates a password using the settings given in PWGen's main window and copies it to the clipboard. It's like clicking on the "*Generate*" button with the difference that the password is not displayed but copied to the clipboard instead. This quick generation may be useful when you need a password for a website or so.
- **Generate and Show Password:** Generates a password (see previous menu item) and displays it in a message box before copying it to the clipboard. In the message box, choose "*Yes*" to copy the password to the clipboard, "*No*" to generate and display a new password, or "*Cancel*" to cancel the process. Note that if the password is very long (longer than 1000 characters), it won't be shown and will just be copied to the clipboard.

Password List Menu

In the *password list* window, you can access some useful functions by right-clicking with your mouse:

- **Copy:** Copies the current text selection to the clipboard.
- **Select All:** Selects the entire text.
- **Save As File:** Writes the text to a file of your choice.
- **Change Font:** Changes the text font.

Command Line Options

Command line switches have to be prefixed by either one or two minus characters (“-” or “--”), or by a slash character (“/”). PWGen currently supports the following switches:

Switch	Meaning
<code>ini=<file name></code>	Uses the INI file specified by <i><file name></i> for reading and storing the settings of the program (instead of using the default INI file, <i>PWGen.ini</i>). Include the file path in quotation marks (“”) if it contains any spaces. If the file does not exist, PWGen loads the default settings on start up and will try to create the file when the settings are to be saved.
<code>readonly</code>	Prevents any automatic writing to the disk/volume where PWGen is located, that is, PWGen will not <i>automatically</i> save any data to the INI file and the random seed file (<i>randseed.dat</i>). The user can still save the program settings by actively calling the corresponding function in the main menu. If no INI file is specified by the user, PWGen will load the default <i>PWGen.ini</i> ; if this file does not exist, PWGen will load its default options. The random seed file will be read on startup but otherwise will not be modified in any way.

Example: `PWGen.exe /ini="c:\my passwords\my.ini" /readonly` loads the settings from the file `my.ini` in the folder `c:\my passwords`, and prevents any automatic writing to the disk/volume where it is executed (e.g. `c:\Program Files\PWGen`).

Questions & Answers

Which security level is appropriate for my password?

As always, this depends on your specific needs. Passwords corresponding to the lowest security level—for example, account passwords for not-so-important websites (there are certainly many of this kind)—should have *at least* 40-48 bits. A higher (say, “intermediate”) security level is provided by 64-bit passwords. For sensitive data, a password of at least 72 bits is reasonable. To protect *really* sensitive data, the security should be at least 90 bits. Data that have to be protected for several centuries (if not thousands of years) should be encrypted with a password of at least 112, better 128 bits. Currently, it’s technically infeasible to break 128-bit keys, and this statement will hold for many, many years. (In fact, it’s *quite* unlikely that there will be ever found a practical way to search a 128-bit key space by brute force. If you don’t trust in this assumption, go with 256-bit passwords—they are practically unbreakable.)

The following table shows the lengths of *N*-bit passwords created by different character sets and word lists.

N (bits)	A) letters A-Z (4.7 bpc)	B) upper-/ lower-case letters, numbers 0-9 (5.9 bpc)	C) B + including 37 “special characters” (6.6 bpc)	D) words from list with 8192 words (13 bpw)	E) combination of D and B (examples)
40	9 (=42 bits)	7 (=41 bits)	6	3 (=39 bits)	2 w., 3 ch.
48	10 (=47 bits)	8	7-8	4 (=52 bits)	3 w., 2 ch.
64	14 (=65 bits)	11 (=65 bits)	10 (=66 bits)	5 (=65 bits)	3 w., 5 ch. / 4 w., 3 ch.
72	16 (=75 bits)	12 (=71 bits)	11	6 (=78 bits)	3 w., 6 ch. / 4 w., 4 ch.
90	19 (=89 bits)	15 (=89 bits)	14 (=92 bits)	7 (=91 bits)	4 w., 7 ch. / 5 w., 5 ch.
112	24	19 (=113 bits)	17	9 (=117 bits)	5 w., 8 ch. / 6 w., 6 ch.
128	27 (=127 bits)	22 (=131 bits)	20 (=132 bits)	10 (=130 bits)	5 w., 11 ch. / 6 w., 9 ch. / 7 w., 7 ch.
256 (max.)	54 (=253 bits)	43	38 (=251 bits)	19 (=247 bits)	10 w., 21 ch.

In the table header, “bpc” means “bits per character” and “bpw” means “bits per word”. The table shall give you an idea of the lengths of passwords composed of different character sets. It shows how the size of the character set or the size of the word list, respectively, influences the overall password length. It’s obvious that the higher this size (that is, the

more items there are to randomly choose from), the shorter the resulting password for a given “security” in bits.

The next table shows the times to search the entire key spaces of N -bit passwords (given by 2^N); that is, for every N -bit password, it shows the time to “break” it. The speed (number of keys per second) with which this “brute force attack” can be carried out is limited by the attacker’s financial resources (the amount of money the attacker can dispense), as well as by current technology. Note that neither of these variables can grow infinitely: first, we’re all frequently short of money, this is a commonplace **sigh**; second, the computer power is limited by the propagation speed of electromagnetic waves. Considering this second assessment, it becomes evident that attacks on 128-bit keys are infeasible (at least in this universe ...).

N (bits)	10^6 s^{-1}	10^9 s^{-1}	10^{12} s^{-1}	10^{15} s^{-1}	10^{18} s^{-1}	10^{21} s^{-1}	10^{24} s^{-1}
40	12.7 days	18.3 min	1.1 s	< 1 s	< 1 s	< 1 s	< 1 s
48	8.9 years	3.2 d	4.7 min	< 1 s	< 1 s	< 1 s	< 1 s
64	5.8E5 y	584.9 y	213 d	5.1 h	18.4 s	< 1 s	< 1 s
72	1.5E8 y	1.5E5 y	150 y	54.6 d	1.3 h	4.7 s	< 1 s
90	3.9E13 y	3.9E10 y	3.9E7 y	3.9E4 y	39 y	14.3 d	20.6 min
112	1.6E20 y	1.6E17 y	1.6E14 y	1.6E11 y	1.6E8 y	1.6E5 y	165 y
128	1.1E25 y	1.1E22 y	1.1E19 y	1.1E16 y	1.1E13 y	1.1E10 y	1.1E7 y

To give you an idea of the computer power available nowadays: The network [distributed.net](#) broke a [64-bit key in 1757 days](#) (searching 83% of the key space) with a rate of 10^{11} keys per second. Over 70,000 computers took part in this challenge. A similar [project, aimed at breaking a 72-bit key](#), is still running with a current rate of $1.4 \cdot 10^{11}$ keys per second. Provided that the rate remains constant over the entire running time, it still takes over 1000 years to search the entire key space. So, given an attacker who has access to a computer power comparable to that of *distributed.net* with a rate of 10^{12} keys per second, a 72-bit key may be considered secure. To put it another way, a 72-bit key is sufficient for protection against attackers who lack large financial resources. Now imagine an attacker who can afford a search rate which is *one million times* higher than that of *distributed.net*, resulting in approximately 10^{18} key trials per second. A 72-bit key is not sufficient here, so we should resort to a key of at least 90 bits in size. If the attacker is able to afford even more money and thus more computer power, a key size of 112 bits and more should be strongly preferred.

Of course, these incredibly big numbers for key spaces and their complexity are pretty impressive—but don’t be misled by the conception that a sufficiently long, randomly chosen key automatically provides 100% security! Only megalomaniac fools try to break keys that are far beyond the scope of computer power. Clever attackers know that there are easier, faster and more effective methods to get hold of a password. Think of spyware,

keyloggers, computer viruses, security flaws in operating systems, spies, double agents, truth drugs, torture... only to name a few malicious non-academic methods to find a key (you may call them “real-life brute force attacks”).

Which security measures should I take when generating a strong password?

First, you should make sure that your system is not infected with malicious software (like spyware, etc.). Before generating a “really strong” password, make sure that the random pool is “full of entropy”, that is, the “total entropy bits” counter has a value of at least 256 bits. When you copy passwords to the clipboard, clear the clipboard if you don’t need them any more (click on the “*Clear Clipboard*” button or select the corresponding menu item in the system tray menu). To clear the password box in the main window, just click on “*Generate*”, so that the contents of the box will be overwritten. To clear the password list, just close the window. PWGen automatically overwrites the text in this list when the window is closed or when a new password list is generated. Don’t save sensitive passwords *as plaintext* anywhere on your hard disk. Instead, it is recommended to encrypt them (use the text encryption utility for this purpose, see above) and save them as ciphertext.

Last but not least, I recommend you to regularly wipe the free space on your hard disk, because it could contain remains of sensitive data which were swapped out by Windows some time. A first-rate tool for accomplishing this task is [*Eraser*](#).

Is it possible to memorize those random passwords?

Yes, it is, although it may appear rather impossible on first sight. Maybe *passphrases* composed of random words are easier to memorize for you than random characters. Try to memorize the passphrase by “visualizing” the words or by making up a funny “story” where these words play a role. Random characters can be memorized by really learning them by heart; if necessary, write them down somewhere for a *short time*, and as soon as you have succeeded in truly memorizing them, destroy the material *irreversibly*. You could also try to make up a story, the words of which begin with a character of the password. You see, lots of possibilities. So with some effort, you will eventually succeed in memorizing a strong password generated by PWGen.

In most cases, it’s sufficient to memorize one or two really secure passwords (that is, having a security of at least 72 or better 90 bits); the others can be easily stored in a password safe (see below).

What about pronounceable passwords?

Yes, pronounceable passwords are certainly a nice feature, but their quality in terms of

security is difficult to assess, because their generation has to obey very specific phonemic rules. Thus not all character patterns are equally probable, which results in an entropy reduction. While pronounceable passwords are certainly better than those based on personal data, I would prefer randomly chosen passwords or passphrases anyway. However, PWGen allows you to create artificial, pronounceable “words” by applying the “*Format Password*” option (see examples above). Passwords generated by the rule `%4[%3[%c%v%] %]` will look like this: `sapifu kixezu cehiwu lukuro`. You can play around with the placeholders for consonants and vocals to create passwords that suit your needs.

Can I use PWGen as a password safe?

Yes, this is possible via the text encryption function of PWGen (see above). You can use a simple text editor (like [Notepad++](#), but Windows’ rudimentary *Notepad* does it, too) to manage your “password safe”. Whenever you need a password, for example, for an Internet service, use PWGen to create a random password of any length and store it together with the user name (or the URL as an alternative) in the safe. To “close” the password safe, copy the whole text block to the clipboard, encrypt it with a secure master password and replace the plaintext of your password safe with the ciphertext in the clipboard.

This may not be as comfortable as using a real password safe (like [KeePass](#) or [PasswordSafe](#)), but it works and is secure (as long as your master password is secure, of course).

Which kind of word lists does PWGen accept?

In principle, PWGen accepts all text files containing some kind of “words”. These words must be separated by a line break, a space or a tabulator. The upper limit for the word length is 30 characters (you may decrease this length down to 1, see above). Word lists must contain at least 2 different words. Note that PWGen does not accept duplicate words; the procedure that checks for duplicates is case-sensitive, i.e., it does *not* ignore upper-case and lower-case letters! However, you can force PWGen to convert all letters to lower-case via “*Advanced Password Options*” (see above). PWGen will not add more than 65,536 words—upon reaching this limit, the program will stop the progress. If your word list contains more words, you can try to select shorter words by decreasing the maximum word length.

As explained before, the program accepts text files consisting of words. Here is an example which uses the words in *license.txt* to create the following passphrase:

`original, (and number. (whether judgment`

Note that PWGen does not remove punctuation marks or other non-letter symbols. However, non-text ASCII characters may be ignored when reading the file, because it is read in “text mode”.

How shall I interpret the information about the random pool?

Whenever you generate “indeterministic” events by pressing keys, clicking with your mouse or by moving your mouse within PWGen’s windows, the application collects “entropy” from messages sent by Windows, as well as from a high-performance counter (RDTSC processor instruction, if available; alternatively, the program calls functions provided by the Windows API). Additionally, the program derives entropy from several system-specific parameters, which is done in regular intervals in the background.

The actual “random pool” has a size of 32 bytes and can thus provide a maximum Shannon entropy of 256 bits. As explained in the *Step-by-Step Tutorial* above, the pool is completely filled with entropy if the progress bar is full—but the entropy counter can exceed this limit anyway. Note that this counter only serves informational purposes—it’s absolutely impossible for the random pool to yield more than 256 bits of Shannon entropy! The counter just informs you about the total amount of entropy bits added to the pool, which might be of your interest if you consider PWGen’s entropy estimations as too optimistic.

If you generate passwords, PWGen uses the pool contents as key for the AES (*Advanced Encryption Standard*) cipher which is then used for generating random numbers. This means that a certain amount of entropy is “consumed”, so to say, from the random pool. As a consequence, the entropy counters will be decreased by the entropy bits in the generated password(s). So generating five 48-bit passwords will consume 240 bits of entropy from the pool. (Of course the counters cannot fall below 0.)

Mind you: this loss of entropy only applies to the case that you actually *use* the generated password(s). If you discard it (for example, by simply generating a new one), the entropy has *not* been lost. However, PWGen presumes that you use every password you generate. So once you have filled the random pool with entropy, you may effectively ignore the loss of entropy when generating passwords, as long as you don’t use them. What’s the reason for this? Imagine you generate a 90-bit password using a full random pool of 256 bits. After this process where 90 bits are consumed from the pool, it cannot provide the original 256 bits any more, but only 166 bits, because otherwise it would be (in theory!) easier for an attacker to “guess” the 256 bits of the random pool than to guess $90+256=346$ bits! (Remark: This calculation is a bit simplified, because PWGen uses additional time stamps, independent of the random pool, when generating random numbers. This makes a brute-force attack much more difficult.)

Technical Details

Random Pool

Whenever you interact with your computer—for example by pressing a key, by clicking with your mouse or by moving your mouse—you create an event that is, unlike most internal computer events, to a certain degree indeterministic or unpredictable. The term “indeterministic” means here that these events can afford a certain amount of randomness—and let it be just a few bits. (Due to their random character, indeterministic events are sometimes—rather loosely—referred to as “*entropy*”; this is not to be confused with the entropy term in thermodynamics!) By calling a high-performance timer (like the RDTSC processor instruction available on all modern CPUs, see below) when the user generates such an event we can efficiently make use of its random character. Moreover, the operating system Windows provides additional (and again partly indeterministic) information such as the type of Windows control where the message was sent to, the cursor position and the (low precision) date and time when the message was sent.

We can gather all this entropy from user-generated events in a so-called *random pool*. At this point it is essential to note that this data does not have to be purely random—it is sufficient that it contains some bits of uncertainty (the more, the better, of course). The “trick” is now to apply a *cryptographic hash function* to this entropy in order to “distil” randomness from this data. This operation yields data that looks truly random, although it cannot contain more information than the original partly-random data. If we now collect entropy amounts large enough to provide (in total) sufficient uncertainty, we can generate sequences that do not only look random, but in effect *are* random. For example, to generate a highly secure 128-bit password, we fill the random pool with enough user inputs (that is, entropy) first—by entering some text on the keyboard, or by moving the mouse, etc. Then we use this data to distil the required 128 bits of truly random data from the pool and convert it to a secure password. This is the basic concept of random number generation in PWGen. The “real implementation” is a bit different.

In mathematical terms, the process looks as follows: $HMAC\text{-}SHA\text{-}256(K, M)$ is used as secure hash function. The HMAC algorithm uses an additional key K to compute the 256-bit message-digest of a message M . (Note that in this case, the “key” does not have a special purpose here; we simply use the HMAC algorithm instead of the plain hash function because the former is thought to have better “randomness extraction” properties compared to the latter.) To distil randomness and to generate a new pool, the old pool contents and the entropy data are processed in the following way:

$$(1) \quad P_{\text{new}} \leftarrow HMAC(P_{\text{old}}, S \parallel T),$$

where P is the random pool (32 bytes), $HMAC$ is the HMAC hash function, S is the entropy data of any length, and T is a time stamp from a high-resolution timer. “ \parallel ” denotes simple

concatenation of the sequences. PWGen uses a memory block of a defined length to buffer subsequent entropy inputs; when this buffer is full, it will be hashed according to eqn. (1) and cleared (overwritten with random data) afterwards.

To generate cryptographically secure random numbers, PWGen uses the AES (*Advanced Encryption Standard*) encryption algorithm in counter (CTR) mode. AES is set up with a 256-bit key and operates on 128-bit blocks. In order to derive a key K for AES, the pool is first updated (eqn. (1)), then the pool is hashed:

$$(2) \quad K \leftarrow \text{HMAC}(T, P).$$

This procedure ensures that P cannot be derived from K , and vice versa. Random numbers are then generated by encrypting a 128-bit block counter C (3a), which is incremented by 1 afterwards (3b):

$$(3a) \quad R \leftarrow E_K(C),$$

$$(3b) \quad C_{\text{new}} \leftarrow C_{\text{old}} + 1.$$

C is initially derived by encrypting two 64-bit time stamps. R is the next 128-bit random output, and E_K is the encryption function with key K . As the attacker neither knows K nor C , he cannot predict the next number R , even if he knows the entire previous sequence. Furthermore, K and C are changed regularly to ensure that, even in case of a *state compromise* (leakage of sensitive data in K and C to the attacker), the attacker cannot reconstruct those random blocks generated before the key change (“forward secrecy”). Using time stamps when updating the pool and when generating secret counter values C adds to the security of the construction, since they provide a certain degree of unpredictability.

All sensitive data (random pool, entropy buffer, AES key, counter, ...) are held in RAM to prevent it from being swapped out to the hard disk. The pool is made indistinguishable from random by clearing all buffers with random data after use. This will make it difficult to locate the pool in RAM by means of any easily identifiable sequences.

For performance reasons, PWGen delays the recognition of mouse movements. For every mouse input, PWGen counts a maximum of 10 bits of entropy (max. 8 bits for the timer plus 2 bits for cursor coordinates); for every keystroke, PWGen counts a maximum of 9 bits (1 bit for the key code). In addition to these user inputs, PWGen collects entropy from various system parameters every 15 seconds, which yields 24 bits of entropy in PWGen’s estimations. Note that these estimations are rather conservative—the “real” quality of these entropy sources is likely to be higher.

In order to preserve the entropy collected during runtime, PWGen writes a random seed file (*randseed.dat*) in the application folder. This 32-byte file is read on start up, its

contents are fed into the random pool, and the seed file is immediately overwritten with new data afterwards. PWGen updates this file in regular intervals while running and on exit. If you don't want PWGen to write this file, you can use the `/readonly` command line switch (see section *Command Line Switches* above).

Text Encryption

The text encryption can be divided into four steps: Text compression, HMAC generation, encryption and base64 conversion. First, the text is compressed using the LZ01X-1 compression algorithm. Second, the 256-bit HMAC of the compressed text is generated. Third, the compressed text is encrypted using AES with a 256-bit key. Fourth, the encrypted text (ciphertext) is converted into "readable" characters (base64 character set).

Let's start with an overview of the encryption procedure: To derive the 256-bit key from the password provided by the user, a version of the key derivation function *PBKDF2* is used, which applies the hash function HMAC-SHA-256 to the user password along with a randomly chosen 128-bit initialization vector (IV; also called "salt" in this context). This process is repeated many times (8192 iterations) in order to make password cracking much more difficult.

The text which is to be encrypted consists of a header structure (4-byte "magic" identification string and length of the uncompressed text) and the compressed text (variable length). This assembly is encrypted in CBC (*Cipher Block Chaining*) mode in order to hide patterns in the plaintext:

$$(1a) \quad C_i \leftarrow E_K(P_i \text{ xor } C_{i-1}).$$

C_i describes the i th block of ciphertext (that is, the encrypted text) and P_i the i th block of plaintext (that is, the unencrypted text). C_0 is the IV which is also used in key derivation. Again, E_K is the encryption function with K as key. "xor" denotes an "exclusive-or" bit operation. In decryption mode, eqn. (1a) can be reversed in a simple way:

$$(1b) \quad P_i = D_K(C_{i-1}) \text{ xor } C_{i-1},$$

where D_K is the decryption function.

Before encrypting the plaintext, a so-called HMAC (*keyed-Hash Message Authentication Code*) of the text is calculated. In general terms, the HMAC can be considered as a message digest of the ciphertext with K as parameter. It serves to check the decryption process in two ways: 1) *Is the key correct?*, and 2) *Has the ciphertext been altered in any way (data integrity)?* Note that PWGen cannot distinguish between these questions, that is, it can only check if the HMAC is correct or not, but it cannot tell you (on the basis of the HMAC) if the decryption failed because of a wrong key or because of a corrupt ciphertext. As the attacker doesn't know the key, he cannot compute valid HMACs himself; in

particular, he cannot modify the ciphertext in some way and then make any valid modifications to the HMAC due to the strong non-linearity of the HMAC algorithm. Any modifications of the ciphertext will be recognized during the decryption process. PWGen uses HMAC-SHA-256 to generate a 256-bit HMAC of the entire plaintext block. This 32-byte sequence is appended to the ciphertext after encryption.

In the last step, the binary encrypted data generated in the previous three steps are converted to the base64 format (a character set consisting of 64 “readable” characters: mixed-case letters, numbers, and the characters “+”, “/” and possibly “=”) in order to make it “readable” by text editors, e-mail programs, etc. In the encoding scheme used by PWGen, lines are wrapped after 76 characters to allow for a smooth display of the text in editors. (Some editors, such as Windows’ *Notepad*, may crash [or take a *very long* time] when the user attempts to paste very long texts consisting of only one single line. Therefore, it seems to be prudent to create multi-line texts with shorter but more numerous lines.)

The decryption procedure is essentially the reverse of the encryption procedure:

1. The ciphertext is converted from base64 (6-bit) characters to 8-bit bytes. If there are illegal characters in the text, or if the resulting text is shorter than 64 8-bit bytes, or if the text length is not a multiple of 16, the ciphertext structure is invalid, which means that the text is either corrupted or not encrypted by PWGen.
2. The first 16 bytes of the ciphertext are decrypted and the “magic string” in the header structure is checked. If the decrypted identification string and the default string do not match, then either the key is wrong, or the beginning of the ciphertext (first 32 8-bit bytes) has been modified.
3. The remaining ciphertext is decrypted to give the compressed plaintext.
4. The HMAC is generated and checked. If this verification fails, either the key is wrong, or there were modifications *somewhere* within the entire ciphertext. However, as the verification of the identification string in the header must have succeeded in step (2), it is actually more likely that the ciphertext has been modified.
5. Finally, the plaintext is decompressed to give the original plaintext. Note that the decompression can *theoretically* fail, although this should *never* happen under “normal” circumstances. If this error really occurs, the most probable cause is a heavily manipulated ciphertext, that is, a text that has *not* been generated by PWGen.

Note of caution: *Always check the correct decryption of the ciphertext before discarding the plaintext!*

High-Resolution Timer

If possible, PWGen uses a high-resolution timer (HRT) the value of which is added to the pool when you press a key, move your mouse, or click with your mouse. It is also used when generating cryptographically strong random numbers to increase the security of the generator. Due to the high resolution of this timer every value possesses a certain degree of unpredictability, particularly when measuring the timer intervals between user-generated events such as keystrokes and mouse clicks. Therefore, it can provide a relatively high amount of entropy. Moreover, consider the following worst-case scenario that an attacker got hold of the entire state of the random pool (“*state compromise*”) and thus could theoretically predict the entire sequence of random numbers that will be generated. Adding the HRT value before generating the next random sequence offers a certain protection against this scenario: The attacker can read the timer value himself, of course, but it is actually very unlikely that he reads the same value due to the high time resolution of the timer (typically nanoseconds on modern CPUs). Since the HRT is available very quickly, it is used in every critical situation of the random pool, that is, when updating the pool and when generating random numbers.

PWGen can use the following timers (listed with descending priority):

1. **Time stamp counter (RDTSC instruction):** The RDTSC processor instruction returns the number (64-bit) of cycles since reset. The time resolution therefore depends on the clock rate of the processor: On a 3 GHz processor, for example, each cycle takes ~0.3 nanoseconds. The RDTSC instruction is present on all x86 processors since the Pentium and provides an excellent high-resolution, low-overhead way of getting CPU timing information.
2. **QueryPerformanceCounter (Windows API function):** According to the *Windows SDK*, this function returns the current value (64-bit) of the high-performance counter. This is probably just a wrapper for the time stamp counter on most systems, but the return value may be different on multicore computers. Calling this function is slower than executing RDTSC.
3. **Low resolution timer (Windows API):** Alternatively, if neither RDTSC (1) nor QueryPerformanceCounter (2) are available, PWGen retrieves the current date and time of the system. The resolution of this timer is only in the millisecond range and thus *much* lower (by several orders of magnitude) than that of the high-resolution timers (1) and (2), but may still be sufficient for measuring keyboard and mouse events.

On start up, PWGen checks if the RDTSC instruction (1) is available, which should be the case on all modern computers (Pentium processor onwards). If this check fails, PWGen tests QueryPerformanceCounter (2). If both tests fail, PWGen uses the current system date and time (3). However, if (1) or (2) are allegedly available, PWGen briefly checks if

they can really hold the high resolution; this test might fail when PWGen runs on emulated systems, for example, and if it fails, PWGen uses (3) instead.

Note that PWGen constantly checks the resolution of the timer values and decreases the entropy rating if the resolution is low (that is, in the millisecond region). Although the security of the random generator does *not* entirely depend on the entropy of the timer values because a lot of other parameters are additionally incorporated into the pool, it is strongly recommended to run PWGen on systems where a high-resolution timer (1 or 2) is present due to the higher entropy and due to the increased security in critical situations of the random generator. You can check which timer is used by selecting the item *Timer Info* from the *Help* menu.

Contact

If you have further questions, critical remarks, suggestions for the future development, bug reports or something else to tell, feel free to contact me via e-mail:

c.thoeing@web.de

Translations

Translations of PWGen into languages other than English and German are always very welcome. For a list of translations that are available so far, see [here](#). If you want to update an existing translation file or create a new one, I recommend you to use the [PWGen Translation Utility](#) that I have created especially for this purpose. This program uses the file *German.lng* (which accompanies all releases of PWGen) as a template for your own translation.

Word Lists

Have a look at the [PWGen project page](#) to access additional word lists suitable for generating passphrases. If you have created a word list and want to share it with other users, please send me the text file, so that I can publish it on the web. Alternatively, you can find special word lists in several languages on the [“Diceware” homepage](#); however, you may want to extract the actual words (instead of the numbers/indices) first before using the “Diceware” lists in PWGen.

Please Donate!

As you can certainly imagine, developing and maintaining a software project like PWGen requires a lot of effort and commitment, especially if you have other responsibilities in your regular job as well as at home. If you like PWGen and use it frequently, please [donate to the project](#). Your donations will encourage me to further develop the application and keep it bug-free. *Thanks!*

Acknowledgement

Thanks to Brainspark B.V., M.F. Oberhumer, A.G. Reinhold, Aha-soft, D. Reichl, S. Tolvanen, M. Hahn, T. Ts’o, R.J. Jenkins, and W. Dai for code & inspiration! Thanks to all the users for their donations, helpful comments and suggestions!