

The Diceware™ Word List — Beale's Word List

Diceware lets you make highly secure passphrases that are relatively easy to remember. To use the Diceware list you will need one or more dice. Dice come with many board games and are sold separately at toy, hobby, and magic stores. Toys "R" Us in the US sells a package of five dice for about \$0.99. You can purchase five "casino-grade" dice online from Casinocom.com for about \$11.

First, decide how many words you want in your passphrase. We recommend a five word passphrase for use with PGP, S/MIME and similar encryption programs. For the paranoid, a six word pass phrase will make attacks on your passphrase infeasible for the foreseeable future. If you want to understand why, see the Diceware FAQ at www.diceware.com.

Now roll the dice and write down the results on a slip of scrap paper. Write the numbers in groups of five. Make as many of these five digit groups as you want words in your passphrase. You can roll one die five times or roll five dice once, or any combination in between. If you do roll several dice at a time, read the dice from left to right.

Look up each five digit number in the Diceware list and find the word next to it. For example, 21124 means your next passphrase word would be "clip". When you are done, the words that you have found are your new passphrase. Memorize them and then either destroy the scrap of paper or keep it in a really safe place. That's all there is to it!

Example

Suppose you choose a five word passphrase, as we recommend for most users. You will need 5 times 5 or 25 dice rolls. Let's say they come out as:

1, 6, 6, 6, 5, 1, 5, 6, 5, 3, 5, 6, 3, 2, 2, 3, 5, 6, 1, 6, 6, 5, 2, 2, and 4

Write down the results on a scrap of paper in groups of five rolls:

1 6 6 6 5 1 5 6 5 3 5 6 3 2 2 3 5 6 1 6 6 5 2 2 4

You then look up each group of five rolls in the Diceware word list by finding the number in the list and writing down the word next to the number. Your passphrase would then be: **cloak canal target lapel zt**

Copyright (c) 2004 by Matthieu Weber for the layout. Copyright (c) 1995, 2000 by Arnold Reinhold for the front page. The original document can be found at <http://world.std.com/~reinhold/diceware.html>. This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, v1.0 or later (the latest version is presently available at <http://www.opencontent.org/>)

In their February 1996 report, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security" a group of cryptography and computer security experts — Matt Blaze, Whitfield Diffie, Ronald Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, and Michael Weiner — stated:

"To provide adequate protection against the most serious threats... keys used to protect data today should be at least 75 bits long. To protect information adequately for the next 20 years ... keys in newly-deployed systems should be at least 90 bits long."

Each word in your Diceware passphrase yields 12.9 bits of entropy. A five-word Diceware passphrase has an entropy of at least 64.6 bits; six words have 77.5 bits, seven words 90.4 bits, eight words 103 bits, four words 51.6 bits. Inserting an extra letter at random adds about 9.5 bits of entropy to a 20 characters passphrase. Here is my best estimate of how much protection various lengths provide:

- Four words are breakable with a hundred or so PCs.
- Five words are only breakable by an organization with a large budget.
- Six words appear unbreakable for the near future, thought they may be within the range of large governments.
- Seven words and longer are unbreakable with any known technology.
- Eight words should be completely secure for some time to come.

Pick your passphrase size based on the level of security you want.

For extra security without adding another word, insert one special character or digit chosen at random into your passphrase. Here is how to do this securely: Roll one die to choose a word in your passphrase, roll again to choose a letter in that word. Roll a third and fourth time to pick the added character from the following table:

		Third roll					
		1	2	3	4	5	6
F	1	~	!	#	\$	%	^
o	2	&	*	()	-	=	
u	3	+	[]	\	{ }		
r	4	:	;"	,	<	>	
t	5	?	/	0 1	2 3		
h	6	4	5	6	7	8	9

