The Diceware Passphrase Home Page

This page offers a better way to create a strong, yet easy to remember passphrase for use with encryption and security programs. Weak passwords and passphrases are one of the most common flaws in computer security. Take a few minutes and learn how to do it right. The information presented here can be used by anyone. No background in cryptography or mathematics is required. Just follow the simple steps below. If you'd like to know even more about passphrases, see the Frequently Asked Questions (FAQ), and please checkout the Diceware Security Blog, for commentary on the latest developments in computer security and shared secret authentication.

This page is also available in Chinese, Esperanto, Finnish, French, Italian, Japanese, Polish and Spanish. There are also Bulgarian, Catalan, Danish, Dutch, Esperanto, Finnish, French, German, Italian, Japanese, Maori, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish and Turkish word lists, all kindly contributed by our users.

Try our free Big Number Calculator Java applet. It lets you perform many of the calculations used in public key cryptography. It should work on most modern browsers on computers that support Java (that does not include Apple's iOS, sorry).

What Is A Passphrase?

A passphrase is a bunch of words and characters that you type in to your computer to let it know for sure that the person typing is you. Most security programs allow you to enter a passphrase instead of just a short password for added protection against attackers. Some programs also use your passphrase to form a cryptographic key to encrypt your data.

- Passphrases are used with Wi-Fi wireless network security systems such as WPA and WPA2, when used in personal shared key (PSK) mode. The security of both systems depends on the strength of the passphrase you chose.

- Phil Zimmermann's popular encryption program PGP requires you to make up a passphrase that you enter whenever you sign or decrypt messages. So does the open-source version, GnuPG.

- Popular password manager programs require a master password or passphrase to protect the data they store.

- Passphrases are used with disk encryption programs such as PGPdisk and Apple's FileVault. Many organizations require disk encryption on laptops to meet regulatory requirements for protecting sensitive information.

- The latest versions of most popular operating systems, including Windows 10, MacOS (formerly OS-X) and iOS, let you use longer passphrases for log-on identification.
- Digital currencies such as BitCoin use passphrases to protect the “coins” from misappropriation.
- Using a short passphrase as an answer to a required "security question" (like "What city were you born in?") protects you against attempts to discover your answer by researching your online data.

You should follow the Diceware instructions here to create your passphrase *before* installing a WiFi router, creating your PGP or GPG key, opening a new security account or setting up an encrypted disk.

Passphrases differ from passwords only in length. Pass*words* are usually short, six to ten characters. Short passwords are OK for logging onto computer system that are programmed to detect multiple incorrect guesses and protect the stored passwords properly, but they are not safe for use with encryption systems. Passphrases are usually much longer -- typically 25 to 50 characters (including spaces), sometimes more. Their greater length makes passphrases more secure. Modern passphrases were invented by Sigmund N. Porter in 1982. If all you need right now is a login password, click here. Otherwise, read on.

Picking a good passphrase is one of the most important things you can do to preserve the privacy of your computer data and e-mail messages. A passphrase should be:

- Known only to you
- Long enough to be secure
- Hard to guess -- even by someone who knows you well
- Easy for you to remember
- Easy for you to type accurately

What Is Diceware?

Diceware™ is a method for picking passphrases that uses dice to select words at random from a special list called the Diceware Word List. Each word in the list is preceded by a five digit number. All the digits are between one and six, allowing you to use the outcomes of five dice rolls to select a word from the list.

Here is a short excerpt from the Diceware word list:

```
16655 clause
16656 claw
16661 clay
16662 clean
16663 clear
16664 cleat
16665 cleft
16666 clerk
```

21111	cliche
21112	click
21113	cliff
21114	climb
21115	clime
21116	cling
21121	clink
21122	clint
21123	clio
21124	clip
21125	clive
21126	cloak
21131	clock

The complete list contains 7776 short words, abbreviations and easy-to-remember character strings. The average length of each word is about 4.2 characters. The biggest words are six characters long. The English list is based on a longer word list posted to the Internet news group *sci.crypt* by Peter Kwangjun Suk. An alternative list, edited by Alan Beale, contains fewer Americanisms and obscure words. And there are lists for several other languages. You can also download the Diceware word list in PDF format or in PostScript format.

Using Diceware

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. Braille dice are also available. You can purchase a set of five casino-grade dice online from Amazon.com or Ebay.com for about $16, but they are overkill for this purpose. *Do not use a computer program or electronic dice generator.*

1. Download the complete Diceware list or the alternative Beale list and save it on your computer. Print it out if you like. Then return to this page.

2. Decide how many words you want in your passphrase. A five word passphrase provides a level of security much higher than the simple passwords most people use. We recommend a minimum of six words for use with GPG, wireless security and file encryption programs. A seven, eight or nine word pass phrase is recommended for high value uses such as whole disk encryption, BitCoin, and the like. For more information, see the Diceware FAQ.

3. Now roll the dice and write down the results on a slip of 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.

4. 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" (see the excerpt from the list, above).

5. 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 want a six word passphrase, as we recommend for most users. You will need 6 times 5 or 30 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, 4, 6, 4, 3, 2, and 6.
```

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
6 4 3 2 6
```

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:

```
1 6 6 6 5 cleft
1 5 6 5 3 cam
5 6 3 2 2 synod
3 5 6 1 6 lacy
6 5 2 2 4 yr
6 4 3 2 6 wok
```

Your passphrase would then be:

```
cleft cam synod lacy yr wok
```

Some Tips

- For maximum security make sure you are alone and close the curtains. Write on a hard surface -- not on a pad of paper. After you memorize your passphrase, burn your notes, pulverize the ashes and flush them down the toilet.

- If you are using a passphrase for file encryption, we recommend you keep a copy written down in a safe place. If you don't and you forget your passphrase, your files are lost forever.

- If you want to work from a printed copy of the word list, download the the Diceware word list in PDF format or PostScript format. These files are formatted with 4 columns and 54 lines per page. You will get a neat, 36 page printout in which the first two dice throws are the same for each page. This makes look-ups especially easy. If you prefer a more compact printout, here is an 11-page version from Patrick Feisthammel. *Be careful not to mark the printed copy in any way while you are selecting words.* You can also find the word list as an Appendix to Internet Secrets.

- If you need to make up passphrases often, get a shoe box or a food storage box about the same size. Put five dice in the box, shake them up vigorously -- at least ten hard shakes -- and then tip the box to let all the dice slide down to one edge. Now open the box, read the dice from left to right, or front to back if a few line up. Then just look up the corresponding word list entry. Repeat this process until you have enough words for your passphrase.

- We recommend that you use the passphrase exactly as generated. If you want a stronger passphrase, select an additional word using the diceware method.

- Because some words on the diceware list are two characters or less, you can get a very short passphrase. If your passphrase, including the spaces between the words, is less than 17 characters long, we recommend that you start over and create a new passphrase. You should also start over if your passphrase is a recognizable English sentence or phrase. (These situations are extremely rare.)

- See the Diceware FAQ for suggestions on how to memorize your passphrase.

Optional stuff you don't really need to know

- 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
```

- For the technically inclined, each word in your Diceware passphrase yields 12.9 bits of entropy, the way passphrase security is measured. A five word Diceware passphrase would have an entropy of at least 64.6 bits; six words would have 77.5 bits, seven words 90.4 bits, eight words 103.2 bits. Inserting a letter at random adds about 10 bits of entropy. All this assumes, of course, that you actually keep your passphrase a secret.

- You'll find a lot more information you don't really need to know in the Diceware FAQ.

Why Diceware?

There are many different recommendations available on the Internet about how to pick a passphrase. Many are good, a few are bad, but almost all require the user to judge what will be hard for someone else to guess. Some give no guidance on how to do that, others have you make complex mathematical calculations. By contrast, the Diceware method of generating passphrases is:

- Easy to learn and use

- Very secure

- Totally prescriptive - we tell you exactly what to do at each step of the process

- Transparent - there are no "trust me"s

- Free - there is no computer software or hardware required, just the Diceware list and some ordinary dice

The prescriptive nature of Diceware is very important for new users of encryption. Here is one person's experience, as posted to the Internet newsgroup *alt.security.pgp*:

> "I just wanted to relate a personal story about how hard it is to convince a novice how important it is to select a secure password, and get them to understand what constitutes a secure password. I am an old-timer at both the Internet and security issues. My sister, however, is brand new to it having just opened an Internet account. She lives in [the mid-west] while I live [on the west coast]. As a result, we exchange quite a bit of very personal email.
>
> Recently, she wanted to give her Internet password to her husband so that he could get on line. However, she still wanted to be able to exchange private messages with me that he would not be able to read. I, of course, introduced her to PGP.
>
> I gave her the usual lecture about how important it is to select a password that nobody else can easily guess, and that the ideal password would be some obscure and nonsense word that would have meaning only to her. I told her all about not selecting birthdays, anniversaries, names, and the like. I didn't suggest a random combination of letters and numbers because we were not after world class security, we just wanted to keep her husband out of our private letters. So, after she selected her PGP password, I decided to give it a try at cracking it. The VERY FIRST password I tried worked! She was totally surprised at how easily I had found it, but it was a word that anyone knowing her would have access to. So, after giving her some more tips on good password selection, I let her try again. This time, it took me only 3 attempts before I found the right word. Finally, she gave up and let me pick a password for her."

Had she used Diceware, the author's sister's very first passphrase would have been totally secure and known only to her. Remember: in public key cryptography, the security of your message depends on the *recipient's* passphrase. Spread the word about Diceware!

Links And References

For more information on passphrases and Diceware see the following:

Diceware FAQ Questions and answers for people who want to know more about Diceware and passphrase generation.

Diceware Word List, the list in PostScript format, Beale word list, Diceware8k list for computer generation

A Survey of PGP Passphrase Usage A small poll I ran to find out what PGP users actually do to make passphrases, and some suggestions for improvement.

Diceware for Passphrase Generation and Other Cryptographic Applications Includes info on other uses of Diceware and an analysis of Diceware security.

Protecting Passwords by Gary McGraw and John Viega, An article in the IBM Developerworks Security Library that discuss passwords, pasphrases and Diceware.

Passgen: A Password Generator Java Applet Uses keyboard latency to generate random passwords based on a selectable format. Not as secure as the diceware method, but adequate for login passwords and similar applications. Includes source code.

Random Noise Sources A collection of information on sources of randomness for use with computers.

CipherSaber Home Page Learn how to build your own strong encryption program. It's easier than you think!

Other Papers on Cryptography by Arnold Reinhold P=?NP -- who Cares?, Cryptanalysis of Histocompatibility, etc.

S. N. Porter, *A Password Extension for Improved Human Factors,*
Advances in Cryptology: A Report on CRYPTO 81, Allen Gersho, editor, volume 0, U.C. Santa Barbara Dept. of Elec. and Computer Eng., Santa Barbara, 1982. Pages 81--81. Also in Computers & Security, Vol. 1. No. 1, 1982, North Holland Press.

Diceware in Other Languages

BG -- Bulgarian word lists (PDF) provided by yradunchev under the terms of the CC-BY-4.0 license. Here is a sample Bulgarian passphrase:

```
дави федрос успеем корков кле мамон
```

CA -- Catalan word lists (ASCII and UTF-8) provided by Marcel Hernandez under the terms of the CC-BY-4.0 license. Here is a sample Catalan passphrase:

```
radiar balca imaginar insula sinitizin dar
```

CN -- Chinese translated by Lian.

DA -- A Danish word list provided by Povl Falk-Jensen Here is a sample Danish passphrase:

```
odf simse gnid khmer bejae info
```

DE -- A German word list (PDF version) provided by Benjamin Tenne under the terms of the GNU General Public License. Here is a sample German passphrase:

```
distel ist landen kammer puffen nutze
```

EO **--** Esperanto translated by Makis Diras, including a Esperanto word list. Here is a sample Esperanto passphrase:

```
hirt neŭtr livre etern krank esoter
```

ES -- Spanish translated by Manuel Palao, including a Spanish word list. Here is a sample Spanish passphrase:

```
multa h64 quien enero tubo
```

FI ---Finnish translated by Kai Puolamaki, including a Finnish word list. Here is a sample Noppaware ("noppa" means a dice in Finnish) passphrase:

```
 olli kukot hoveli hintaa airoja
```

FR -- French translated by Joachim Dubuquoy-Portois. There is a French word list by Matthieu Weber, in several formats. Sample:

```
ileus humide diktat sbire peotte
```

IT -- Italian translated by Tarin Gamberini with an Italian word list (pdf format). Here is a sample Italian passphrase:

```
casi botole stadi maglia venivo
```

JP -- Japanese translated by Hiroshi Yuki, with a Japanese wordlist in Romaji by J Greely. Here is a sample Japanese passphrase:

douse aho socchi bidou tosou ob

MI -- A Maori word list provided by Rangi Kemara under a CC-BY license. Here is a sample Maori passphrase:

```
iatoto okaoka arawai takawa unene takoru
```

NO -- A Norwegian word list provided by Willy T. Koch under a CC-BY license. Here is a sample Norwegian passphrase:

```
kare puben aks snuse dulle sauen
```

NL -- A Dutch word list provided by Bart Van den Eynde under the terms of the GNU Free Documentation License. Here is a sample Dutch passphrase:

```
ijler 100 leperd akolei kolkje
```

PL -- Polish translated by Piotr (DrFugazi) Tarnowski, Computer Science Techniques Centre, University of Silesia, Katowice, PL, including a Polish word list. Here is a sample Polish passphrase:

```
plewka szpieg raban pruski ibi
```

PT – Portuguese word list translated by Patxi Pierce. Here is a sample Portuguese passphrase:

```
curso franja obeso berne perigo liquen
```

RU -- Russian word list provided by "kitten," and a version in rtf. Here is a sample passphrase:

```
кома жилет лысун кроль ерник вскрик
```

**SV -- **Swedish word list provided by Magnus Bodin. Here is a sample Swedish passphrase:

```
ark altan rodel lamm kyot
```

TR -- Turkish word list provided by Mert Dirik. Here is a sample Turkish passphrase:

```
derz permi turba um beniz
```

The Diceware Kit contains instructions on how to create a Diceware word list for other languages.

Special thanks to all the translators!

Other English word lists

A number of other groups are developing word lists for generating passphrases. In July 2016, the Electronic Frontier Foundation (EFF) published a new list. Their long list contains 7776 words, so its security is exactly the same as the Diceware word list. “The words in our [the EFF's] list are longer (7.0 characters) on average, than Reinhold's Diceware list (4.3 characters). This is a result of banning words under 3 characters as well as prioritizing familiar words over short but unusual words.” Here is a sample random EFF passphrase:

```
foundling confess henna figure congrats revival
```

We still think having a short passphrase is worth the bother of learning an unfamiliar word or remembering simple strings such as nnnn or xg, but the choice is purely a matter of taste, not security. Pick a word list that works for you.

For more information on PGP see:

The GNU Privacy Guard (GPG), an open source implementation of PGP

PGP International Home Page

PGP Home Page, now part of Symantic

PGP-Basics Newsgroup on Yahoo

Here are some other sites with recommendations on how to make your passphrase. I do not suggest that the information at these sites is wrong, just that it may be too complex for most people. Take a look and judge for yourself.

Passphrase FAQ by Randall T. Williams

Passphrase FAQ by Grady Ward

```
 Ascii key+  || 08d0a5d961603380e2949d682c
 10 Byte IV  || bfe8da5c1dec3aba9725d4f689
 Ron's No.4  || 40761763d4d38935e8bd8a44bf
All u need  ==== 4656a7bd7f9ae5d082a30cdfa7
 CipherSaber || f21a918d29c5917956d0468eaf
```

http://ciphersaber.org/ Learn how to write a simple yet strong encryption program of your own. If you have any programming skills at all -- even in Basic -- you can do it.

Arnold G. Reinhold
e-mail: my initials (3 letters) a t mac dot com
PGP Fingerprint:
FA C3 82 FB 05 5E 03 1A 34 04 79 EA 9E 76 7B 67

First published on usenet's sci.crypt.research 1995-8-1

Last updated 2017-1-10