I'm not a bot

Advisory: Historical results for the Third-Party Draw Service are currently unavailable. We are working on bringing them back. List Randomizer This form allows you to arrange the items of a list in random order. The randomness comes from atmospheric noise, which for many purposes is better than the pseudo-random number algorithms typically used in computer programs. Advisory: Historical results for the Third-Party Draw Service are currently unavailable. We are working on bringing them back. Dice Roller This form allows you to roll virtual dice. The randomness comes from atmospheric noise, which for many purposes is better than the pseudo-random number algorithms typically used in computer programs. Confused about terminology? The word ‘die’ is singular and ‘dice’ is plural. Advisory: Historical results for the Third-Party Draw Service are currently unavailable. We are working on bringing them back. Introduction to Randomness and Random Numbers by Dr Mads Haahr RANDOM.ORG is a true random number service that generates randomness via atmospheric noise. This page explains why it's hard (and interesting) to get a computer to generate proper random numbers. Random numbers are useful for a variety of purposes, such as generating data encryption keys, simulating and modeling complex phenomena and for selecting random samples from larger data sets. They have also been used aesthetically, for example in literature and music, and are of course ever popular for games and gambling. When discussing single numbers, a random number is one that is drawn from a set of possible values, each of which is equally probable, i.e., a uniform distribution. When discussing a sequence of random numbers, each number drawn must be statistically independent of the others. With the advent of computers, programmers recognized the need for a means of introducing randomness into a computer program. However, surprising as it may seem, it is difficult to get a computer to do something by chance. A computer follows its instructions blindly and is therefore completely predictable. (A computer that doesn't follow its instructions in this manner is broken.) There are two main approaches to generating random numbers using a computer: Pseudo-Random Number Generators (PRNGs) and True Random Number Generators (TRNGs). The approaches have quite different characteristics and each has its pros and cons. Pseudo-Random Number Generators (PRNGs) As the word ‘pseudo’ suggests, pseudo-random numbers are not random in the way you might expect, at least not if you're used to dice rolls or lottery tickets. Essentially, PRNGs are algorithms that use mathematical formulae or simply precalculated tables to produce sequences of numbers that appear random. A good example of a PRNG is the linear congruential method. A good deal of research has gone into pseudo-random number theory, and modern algorithms for generating pseudo-random numbers are so good that the numbers look exactly like they were really random. The basic difference between PRNGs and TRNGs is easy to understand if you compare computer-generated random numbers to rolls of a die. Because PRNGs generate random numbers by using mathematical formulae or precalculated lists, using one corresponds to someone rolling a die many times and writing down the results. Whenever you ask for a die roll, you get the next on the list. Effectively, the numbers appear random, but they are really predetermined. TRNGs work by getting a computer to actually roll the die — or, more commonly, use some other physical phenomenon that is easier to connect to a computer than a die is. PRNGs are efficient, meaning they can produce many numbers in a short time, and deterministic, meaning that a given sequence of numbers can be reproduced at a later date if the starting point in the sequence is known. Efficiency is a nice characteristic if your application needs many numbers, and determinism is handy if you need to replay the same sequence of numbers again at a later stage. PRNGs are typically also periodic, which means that the sequence will eventually repeat itself. While periodicity is hardly ever a desirable characteristic, modern PRNGs have a period that is so long that it can be ignored for most practical purposes. These characteristics make PRNGs suitable for applications where many numbers are required and where it is useful that the same sequence can be replayed easily. Popular examples of such applications are simulation and modeling applications. PRNGs are not suitable for applications where it is important that the numbers are really unpredictable, such as data encryption and gambling. It should be noted that even though good PRNG algorithms exist, they aren't always used, and it's easy to get nasty surprises. Take the example of the popular web programming language PHP. If you use PHP for GNU/Linux, chances are you will be perfectly happy with your random numbers. However, if you use PHP for Microsoft Windows, you will probably find that your random numbers aren't quite up to scratch as shown in this visual analysis from 2008. Another example dates back to 2002 when one researcher reported that the PRNG on MacOS was not good enough for scientific simulation of virus infections. The bottom line is that even if a PRNG will serve your application's needs, you still need to be careful about which one you use. True Random Number Generators (TRNGs) In comparison with PRNGs, TRNGs extract randomness from physical phenomena and introduce it into a computer. You can imagine this as a die connected to a computer, but typically people use a physical phenomenon that is easier to connect to a computer than a die is. The physical phenomenon can be very simple, like the little variations in somebody's mouse movements or in the amount of time between keystrokes. In practice, however, you have to be careful about which source you choose. For example, it can be tricky to use keystrokes in this fashion, because keystrokes are often buffered by the computer's operating system, meaning that several keystrokes are collected before they are sent to the program waiting for them. To a program waiting for the keystrokes, it will seem as though the keys were pressed almost simultaneously, and there may not be a lot of randomness there after all. However, there are many other ways to get true randomness into your computer. A really good physical phenomenon to use is a radioactive source. The points in time at which a radioactive source decays are completely unpredictable, and they can quite easily be detected and fed into a computer, avoiding any buffering mechanisms in the operating system. The HotBits service at Fourmilab in Switzerland, which operated from 1996-2022, was an excellent example of a random number generator that used this technique. Another suitable physical phenomenon is atmospheric noise, which is quite easy to pick up with a normal radio. This is the approach used by RANDOM.ORG. You could also use background noise from an office or laboratory, but you'll have to watch out for patterns. The fan from your computer might contribute to the background noise, and since the fan is a rotating device, chances are the noise it produces won't be as random as atmospheric noise. Thunderstorms generate atmospheric noise As long as you are careful, the possibilities are endless. Undoubtedly the visually coolest approach was the lavarand generator, which was built by Silicon Graphics and used snapshots of lava lamps to generate true random numbers. Unfortunately, lavarand is no longer operational, but one of its inventors is carrying on the work (without the lava lamps) at the LavaRnd web site, and Cloudflare is carrying on the mantle with their array of lavalamps to generate randomness for strong encryption. Yet another approach is the Java EntropyPool, which gathers random bits from a variety of sources including RANDOM.ORG, but also from web page hits received by the EntropyPool's own web server. Regardless of which physical phenomenon is used, the process of generating true random numbers involves identifying little, unpredictable changes in the data. For example, HotBits used little variations in the delay between occurrences of radioactive decay, and RANDOM.ORG uses little variations in the amplitude of atmospheric noise. The characteristics of TRNGs are quite different from PRNGs. First, TRNGs are generally rather inefficient compared to PRNGs, taking considerably longer time to produce numbers. They are also nondeterministic, meaning that a given sequence of numbers cannot be reproduced, although the same sequence may of course occur several times by chance. TRNGs have no period. Comparison of PRNGs and TRNGs The table below sums up the characteristics of the two types of random number generators. CharacteristicPseudo-Random Number GeneratorsTrue Random Number Generators EfficiencyExcellentPoor DeterminismDeterministicNondeterministic PeriodicityPeriodicAperiodic These characteristics make TRNGs suitable for roughly the set of applications that PRNGs are unsuitable for, such as data encryption, games and gambling. Conversely, the poor efficiency and nondeterministic nature of TRNGs make them less suitable for simulation and modeling applications, which often require more data than it's feasible to generate with a TRNG. The following table contains a summary of which applications are best served by which type of generator: ApplicationMost Suitable Generator Lotteries and DrawsTRNG Games and GamblingTRNG Random Sampling (e.g., drug screening)TRNG Simulation and ModellingPRNG Security (e.g., generation of data encryption keys)TRNG The ArtsVaries Quantum Events or Chaotic Systems? One characteristic that builders of TRNGs sometimes discuss is whether the physical phenomenon used is a quantum phenomenon or a phenomenon with chaotic behaviour. There is some disagreement about whether quantum phenomena are better or not, and oddly enough it all comes down to our beliefs about how the universe works. The key question is whether the universe is deterministic or not, i.e., whether everything that happens is essentially predetermined since the Big Bang. Determinism is a difficult subject that has been the subject of quite a lot of philosophical inquiry, and the problem is far from as clear cut as you might think. I will try and explain it here, but would also like to point out that Wikipedia has a concise account of the debate. Quantum mechanics is a branch of theoretical physics that mathematically describes the universe at the atomic and subatomic levels. Random number generators based on quantum physics use the fact that subatomic particles appear to behave randomly in certain circumstances. There appears to be nothing we know of that causes these events, and they are therefore believed by many to be nondeterministic. In comparison, chaotic systems are those in which tiny changes in the initial conditions can result in dramatic changes of the overall behaviour of the system. Weather systems are a good example of this, and you may have heard of the butterfly effect, a thought experiment in which a butterfly beating its wings in Brazil is able to affect the winds subtly but critically, just enough to cause a tornado in Texas. Proponents of random number generators of the quantum variety argue that quantum physics is inherently nondeterministic, whereas systems governed by physics are essentially deterministic. I am personally undecided as to where I stand on the determinism-nondeterminism scale, but for the sake of argument, I will put on my determinist hat and use RANDOM.ORG as an example. You could argue that the atmospheric noise used as a source for the RANDOM.ORG numbers can be viewed as a chaotic but deterministic system. Hence, if you knew enough about the processes that cause atmospheric noise (e.g., thunderstorms) you could potentially predict the numbers generated by RANDOM.ORG. However, to do this, you would probably need knowledge of the position and velocity of every single molecule in the planet's weather systems. This is of course infeasible, and the inaccuracy of weather forecasts is a good example of how difficult it is to give even a rough estimate of the behaviour of weather systems. For this reason, it is impractical to predict random numbers from RANDOM.ORG, even for a determinist. A similar case (on a different scale) could be made for random number generators based on lava lamps. Now, you may think that since there's dispute about the suitability of chaotic phenomena for generating randomness, then why not just stick with quantum physics? That would seem to be the safe bet. However, quantum generators aren't safe from critique either. Hard determinists will claim that subatomic particle behaviour isn't really random but rather exactly as predetermined as everything else in the universe has been since the Big Bang. The reason we think these specific particles behave randomly is simply that no human measurement has been able to account for their behaviour. In this view, subatomic events do indeed have a prior cause, but we just don't understand it (yet), and the events therefore seem random to us. To a hard determinist, quantum physics is exactly as suited for random number generation as is atmospheric noise or lava lamps. This is only one possible argument, and there are many others. When it comes down to it, I think the most meaningful definition of randomness is that which cannot be predicted by humans. Whether randomness originates from unpredictable weather systems, lava lamps or subatomic particle events is largely academic. While quantum random number generators can certainly generate true random numbers, it seems to me that they for all intents and purposes are equivalent to approaches based on complex dynamical systems. Suggested Reading Online and print sources that I think are interesting for the topic of randomness. If you have any suggestions, please email us. Can You Behave Randomly? A set of exercises by Dr Christopher Wetzel, which are intended to help you better understand randomness by getting you to try and behave randomly. Behaving randomly is surprisingly difficult for humans. Introduction to Probability and Statistics A great little introduction by John Walker, highly recommended. Exploring RANDOMNESS A book by Prof. Gregory J. Chaitin about algorithmic information theory. Advisory: Historical results for the Third-Party Draw Service are currently unavailable. We are working on bringing them back. Random String Generator This form allows you to generate random text strings. The randomness comes from atmospheric noise, which for many purposes is better than the pseudo-random number algorithms typically used in computer programs. Need more strings than this form supports? Check out our File Generation Service. Advisory: Historical results for the Third-Party Draw Service are currently unavailable. We are working on bringing them back. Frequently Asked Questions (FAQ) RANDOM.ORG is a true random number service that generates randomness via atmospheric noise. This page contains frequently asked questions (and answers!) related to the service. Section 1: Questions about the Service and Software Section 2: Questions about the Numbers Section 3: Questions about How to Use the Service Section 4: Questions about the Premium Generator and the Quota System Section 5: Questions about the Third-Party Draw Service Section 6: Questions about Scientific Publication and Media Coverage Section 7: Questions about Games and Gambling Q7.1: Will you help me break the bank on online gambling site X? Section 8: Questions about Parapsychology and Global Consciousness Section 1: Questions about the Service and Software Q1.1: I use RANDOM.ORG a lot. How can I show my appreciation? Excellent question! We suggest you either register for a RANDOM.ORG account or make a donation to Concern. In case you don't know them, Concern is a charity that helps poor people in the third world achieve self-sustainable improvements in their lifestyles. We recommend them because we agree with their mission statement (which they unfortunately removed as per January 2010, but it used to be here) and because they are pretty efficient compared to many of the other charities we have looked at. If you decide to make a donation to Concern because of RANDOM.ORG, it'd be great if you could tell us about it, since Concern don't automatically do that. (We suppose they have better things to do.) And it makes us so happy! Q1.2: Is the source code for the generator available? Not currently, no. Maybe we'll make it available as open source some day. Q1.3: Can I download the generator software and run it on my own computer? No. It's not just the software you'd need, but also three radios (or one, at any rate), which must be carefully adjusted to pick up atmospheric noise at the right volume. It's not completely trivial to set up. Q1.4: Could someone affect the numbers by broadcasting a radio signal? RANDOM.ORG uses radio receivers to pick up atmospheric noise, which is then used to generate random numbers. The radios are tuned between stations. A possible attack on the generator is therefore to broadcast on the frequencies that the RANDOM.ORG radios use in order to affect the generator. However, radio frequency attacks of this type would be difficult for a variety of reasons. First, the frequencies that the radios use are not published, so an attacker would have to broadcast across all frequencies of all bands used for FM and AM broadcasting. Second, this is not an attack that can be launched from anywhere in the world, only reasonably close to the generator. RANDOM.ORG currently has radio receivers in several different countries, which would make it difficult to coordinate this type of attack. Third, if an attacker actually did succeed at broadcasting highly regular signals (e.g., perfect sine waves) at exactly the right frequencies from the right locations, then the RANDOM.ORG real-time statistics would pick up the drop in quality very rapidly. In particular, the Source Purity and Information Entropy tests would start failing dramatically, which would raise an alert. Q1.5: Will RANDOM.ORG be around in X years? Probably, depending on your value for X. We have run the service since 1998 with no real interruptions, and it is more popular than ever. Q1.6: Does RANDOM.ORG perform custom jobs that require randomness? Yes. Perhaps you need more numbers than it's possible to get via the web forms, or perhaps you need them in a format that isn't supported. In those cases, we can set up a custom job for you to supply the numbers. We also act as independent observers for drawings and competitions via the Third-Party Draw Service. There is typically a charge associated with custom jobs. You can email us for further details. Q1.7: I seem not to be receiving emails from RANDOM.ORG. What is wrong? RANDOM.ORG will send email to you when you register for a Premium Account or if you have forgotten your password. It can also email you if you use the Premium Generator or the Third-Party Draw Service. If you have problems receiving any of these emails, please check your spam filter configuration. It should be set to accept emails from notifications@random.org. If you are still experiencing problems, please let us know. Q1.8: Can I advertise on RANDOM.ORG or buy a paid link? No. Section 2: Questions about the Numbers Q2.1: How can you be sure the numbers are really random? Oddly enough, it is theoretically impossible to prove that a random number generator is really random. Rather, you analyse an increasing amount of numbers produced by a given generator, and depending on the results, your confidence in the generator increases (or decreases, as the case may be). This is explained in more detail on my Statistical Analysis page, which also contains two studies of the numbers generated by RANDOM.ORG, both of which concluded that the numbers are sound. In addition, the continually updated Real-Time Statistics page gives you an indication of the quality of the numbers produced over time. Q2.2: Have the numbers been certified by an independent third party? The numbers produced by RANDOM.ORG have been evaluated by eCOGRA, which is a non-profit regulatory body that acts as the independent standards authority of the online gaming industry. For a typical gambling site, eCOGRA will oversee many aspects of its operation, including financial aspects, such as payout percentages. RANDOM.ORG is not a gambling site, so in our case, eCOGRA only evaluated the quality of the random numbers. They found that RANDOM.ORG consistently produced random numbers across scaling intervals and issued a certificate with their conclusion: ecogra-2009-06-25.pdf (1 page, 52 Kb) The numbers and software have also been evaluated by TST Global (part of Gaming Labs International) who in 2011 examined the generator for use in games hosted on Malta. TST's report stated that RANDOM.ORG ‘distributes numbers with sufficient non-predictability and fair distribution to particular outcomes’ and concluded that it ‘complies with the requirements of the applicable Technical Standard in the jurisdiction of Malta as regulated by The Malta Gaming Authority (MGA).’ Most recently, our service was evaluated by by Gaming Labs International who in 2012, 2017 and 2019 examined the generator for use in games in the UK and other jurisdictions. Their report concluded that it ‘distributes numbers with sufficient non-predictability, fair distribution and lack of bias to particular outcomes’ and that it ‘complies with the requirements of the applicable Technical Standard in the UK Remote Gambling jurisdiction, as regulated by the United Kingdom Gambling Commission (UKGC).’ Further details are available upon request. As of 2019, RANDOM.ORG is specifically accredited to generate randomness for use in games regulated by the following: RANDOM.ORG also holds a GLI-19 certification, which is accepted by many other jurisdictions, such as Curaçao. Certification documents for specific jurisdictions are available upon request. Q2.3: Should the tables of generated numbers be read across or down? For any form that allows the numbers to be formatted in multiple columns, the numbers are generated on a per-row basis, not per-column. Hence, if you want to read them in the order they were generated, you should read them across. Since they're random numbers, it doesn't really matter whether you do it one way or the other, but you should pick one of the two ways and read that way consistently. Q2.4: Are the numbers available in a secure fashion? Yes, since April 2007 you can access the server via We should probably note that while fetching the numbers via secure HTTP would protect them from being observed while in transit, anyone genuinely concerned with security should not trust anyone else (including RANDOM.ORG) to generate their cryptographic keys. Q2.5: What if I need more numbers than is allowed by the forms? Currently, there isn't a lot you can do, except email us and tell us this is a problem for you (see also question 1.6). For some of the forms, the limit is there because it requires time to generate random numbers and the server is pretty busy. For other forms, the restriction is related to the available memory in our servers. If you can do your own programming, you may be able to use the pregenerated files. They contain large amounts of pregenerated raw random data that you can download and use as you please. However, you will probably need to process the files for your specific purpose; hence the need for programming skills. Q2.6: What's the story with the different randomizations mentioned on some of the forms? Some of the forms allow you to choose between three different types of randomization. If you're not sure what to choose, you almost certainly want to ‘generate your own personal randomization right now,’ which is the first (and default) option. In this mode, your numbers (or strings or whatever) will be generated based on true randomness created especially for you and which will be discarded immediately after it has been used. There is no way to predict what these numbers will be, and there is no way to recreate the same numbers later. This is the standard way of using a true random number generator. The other two modes allow you to select a pregenerated randomization, which means that your numbers or strings will be based on randomness generated by RANDOM.ORG some time in the past. These modes allows you to replay a given sequence of numbers at a later stage, and allows multiple parties in different locations to get the same numbers in a predictable fashion. These modes effectively turn RANDOM.ORG into a pseudo-random number generator. Q2.7: Which probability distributions are supported? Currently, the generators support only the discrete uniform distribution. The only exception is the Gaussian Generator, which supports the Gaussian distribution (also known as the normal distribution). No other distributions are currently supported. If you would like to see other distributions, email us the details and we may choose to include them in the future. Q2.8: What if I don't think the die rolls or coin flips look very random? Sometimes people email us to say that they feel the Dice Roller produces too many repeated numbers (e.g., that it is hard to roll five dice without getting two or more identical rolls) or that the Coin Flipper produces too many heads or tails when used with several coins. Such concerns are great illustrations of how difficult it is for humans to deal with randomness. Human brains are so good at finding patterns that we tend to see them even where they aren't. (This is why statistical tests are useful and why the Real-Time Statistics for RANDOM.ORG's numbers are published online.) So let's do the math for an example where we're rolling five dice. Intuitively, you may expect that the five rolls should come up different a lot of the time. (At least this is what people often mention in emails.) So what's the chance of all the five rolls being different? The first die is trivial. Any of the six possible values is fine (none will result in duplicates), giving a probability of $6/6 = 1$. After you've rolled the first die, the chance of the second coming up different from the first is $5/6$, because there is now one less value you haven't seen before. The third is $4/6$, and so on. Hence the total probability of all your five rolls turning out different is: $6/6 \times 5/6 \times 4/6 \times 3/6 \times 2/6 \approx 9.26\%$ Hence, if you roll five dice repeatedly, you should expect over 90% of the rolls to contain duplicates. If you roll six dice, you can multiply the value above by a further $1/6$ and you'll get approximately 1.54%. Hence, if you roll six dice repeatedly, you can expect to get six different values only about once in every 65 rolls. The following table shows the probabilities: Number of Dice RolledChance of Duplicates 10% 2~16.7% 3~44.4% 4~72.2% 5~90.7% 6~98.5% For a great little introduction to calculating probabilities, check out John Walker's Introduction to Probability and Statistics. Q2.9: Do the numbers exhibit Benford's Law? No. Benford's Law describes an over-representation of lower values (in particular ‘1’) for the leading digit in many real-life data sets. Benford's Law can be observed for numbers that are distributed logarithmically, which is the case for many numbers that humans deal with, but not for the true random numbers generated by RANDOM.ORG. Like a die, RANDOM.ORG generates numbers that are uniformly distributed (see question 2.7). For that reason, there is no over-representation of leading digits in the lower ranges. If you are not convinced, try rolling a normal six-sided die many times and write down the results. You won't observe Benford's Law on the values you get. Q2.10: How are the raw random bits scaled to different ranges? The different web pages on RANDOM.ORG produce randomness in various different forms, such as coin flips, dice rolls and integers in configurable intervals. These web pages use a raw random bit stream as their source and scale it to suit their particular purpose. Different scaling algorithms are used, depending on the web page in question. For an introduction to scaling algorithms, please see this article by Doctor Jacques. Q2.11: Can numbers from the Sequence Generator and the Gaussian Generator be considered true random numbers? People who ask this question are interested in the characteristics of numbers picked from a non-uniform distribution or without replacement. Let's say you're generating a randomized sequence using the Sequence Generator. After the first number in your sequence is generated, the probability that the same number is picked again, is 0. When you reach the last random assignment in the sequence, the probability of getting the final unpicked number is 1. Can we really consider those numbers true random numbers? Generally speaking, the distinguishing feature of "true" (compared to "pseudo") random numbers is whether the randomness originates from a physical source of entropy, rather than whether the numbers follow a particular distribution. You'll find more details about this distinction (and the characteristics of each approach) in our Introduction to Randomness and Random Numbers. In addition, the issues of distribution and replacement are really separate - from each other and from the issue of true vs pseudo. The way to think about the Sequence Generator is that it produces a uniform distribution without replacement. This can be implemented using numbers from a uniform distribution with replacement, which is what our core generator produces and which is what most people think of when we talk about true random numbers. In practice, there are several ways to do this, such as those mentioned in Q2.10, but the origin of the data is still (in the case of RANDOM.ORG) true randomness. In a similar fashion to the Sequence Generator, our Gaussian Random Number Generator produces numbers from a normal distribution with replacement, based on the same stream of true random numbers that the Sequence Generator uses as its input. The algorithm used for that is called a Box-Muller transform. Section 3: Questions about How to Use the Service Q3.1: How do I pick winners for a lottery or drawing? Many people are using RANDOM.ORG for this purpose. Since March 2007, there is the Third-Party Draw Service, which is especially intended for holding drawings and which will keep records of the outcome. The records serve as evidence that the drawing was conducted fairly, in case someone should question it later on. See the Guide to Random Drawings and section 5 of this FAQ for further details. If you have no budget but a group of entrants who trust you, then you can use the Sequence Generator. In this case, RANDOM.ORG will not store a record of the result, so your entrants cannot verify the result. Let us assume you have sold or given out sequentially numbered lottery tickets, e.g., numbered 1-250 (if not, see the next question). Then do the following: Go to the Sequence Generator. Type in 1 as your smallest value and the number of tickets sold as your largest, then hit the submit button. On the resulting list, the first number is the number of the winning ticket. If you have a second prize in your lottery, the second number on the list is the number of the second winning ticket, and so on. Discard any unused numbers. Q3.2: How do I randomize a list of people's names? People who ask this question often want to use the service for picking people for drug screening or as winners for lotteries or drawings. In those cases, we really recommend that you use the Third-Party Draw Service instead. The Draw Service offers a high level of transparency to your entrants and also protects you against accusations of tampering by storing a record of the results on RANDOM.ORG. If you don't need transparency or protection against tampering, the List Randomizer will probably do what you want. If you don't want to use the List Randomizer, it's also pretty easy to do it using the Sequence Generator and a spreadsheet. Here's how: Format your names in one column in a spreadsheet. Let's call it column A. Go to the Sequence Generator. Type in 1 as your smallest value and the number of rows in your spreadsheet as your largest, then hit the submit button. Copy and paste the list produced into a separate column in your spreadsheet. Let's call it column B. The two columns contain the same number of rows and must match up. Sort the rows in your spreadsheet in ascending order using column B. Column A now contains your randomized names. You can use this technique with any type of data, not only names, but also employee numbers, etc. It will work with up to 10,000 entries, which is the maximum sequence length that the Sequence Generator allows. Q3.3: Can I use RANDOM.ORG to draw straws? Not directly, but there is David Goodrich's draw straws application, which uses numbers from RANDOM.ORG. Q3.4: Can RANDOM.ORG help me win the lottery? People who ask this question are usually using the Lottery Quick Pick or the Keno Quick Pick. The short answer is that RANDOM.ORG won't give you a better chance of getting a winning combination, but if you do happen to win, you are likely to get slightly better winnings than if you weren't using a quick picker. Now for the long answer. There are really two different parts to winning a great lottery prize. First, there is the chance of getting a winning combination on your ticket, and then there is the value that this ticket will have. If many others played the same combination as you, you will have to share the pot with them, which will result in a smaller payout for you. (Sharing is great in many aspects of life, but in lotteries, these are the facts.) So in answering this question, let's deal with (1) getting a winning combination and (2) estimating the size of the prize one at a time. With regard to getting a winning combination, a good few of the people who email me seem to believe that it is possible to predict the outcome of lotteries (or at least to improve your odds) by using a particular strategy. These strategies are typically based on analysis of past winning numbers and are often implemented as ‘lottery winning software.’ Unfortunately, we don't believe there is any strategy or software that will help you improve your odds. Such strategies are based on the idea that numbers or patterns that have come up in the past are less likely to appear in the future. However, for any properly operated lottery, the numbers are picked in a fashion that is statistically independent, which means that a number or a combination that has been picked in the past isn't less likely to occur next week. The belief that this is the case is an example of the Gambler's Fallacy. A simple way to think about it is that the machine that picks the winning numbers has no memory of what happened in previous drawings. The only way to improve your odds is to buy more tickets, but this gets very expensive very quickly and is more likely to make you poor than rich. So, like any other other properly constructed quick pick, RANDOM.ORG's Lottery Quick Pick will not give you any special advantages for obtaining a winning ticket. However, if you play the lottery on a regular basis, using a quick picker is likely to give you a small advantage over the players who don't use one. For all properly operated lotteries, all the possible combinations are equally likely to be drawn as the winning one. In reality, however, people often behave intuitively rather than rationally, so all the possible numbers are not equally popular with the players. Many people play their own birthdays or those of family members, which means that 1-31 and especially 1-12 (which of course can be a day as well as a month) are overplayed compared to other numbers. In addition, most people when filling in coupons by hand opt for combinations that visually ‘look’ random on the coupon, leading them to avoid straight lines, perfect squares and other combinations that, when the boxes are checked on the coupon, result in geometric shapes that seem ‘too regular’ to the human eye, but in reality have exactly the same chance of becoming the winning combination as any other combination. How often have you ever played all the corner numbers on a lottery coupon? By playing unpopular numbers or combinations, you can increase your expected payout, because you would (on average) share the pot with fewer other winners. You aren't any more likely to obtain a winning ticket, but in case you do, you're likely to win a bigger share. However, it should be noted that lottery odds are still not good, and that most lotteries give much poorer payouts (50% of revenues is not atypical) than many other types of gambling. Thanks to Dag Oystein Johansen for some of the thoughts on lotteries! Q3.5: Can RANDOM.ORG help me play the stock market? People who ask this question has often read A Random Walk Down Wall Street by Princeton economist Burton Malkiel who argues that share prices exhibit randomness in the form of random walk behaviour.Here at RANDOM.ORG, we have not experimented with playing the stock market using our numbers, and as disclaimer we'd like to stress that we don't have a very deep understanding of market behaviour. However, if Prof. Malkiel's thesis is correct, then we fail to see how RANDOM.ORG could be helpful in predicting stock movements. Certainly, true random numbers can be used to simulate a fictive stock market, but being based on randomness, the simulation will yield different results every time you run it, and each result is as likely to be as useful a predictor as the next one. One use of RANDOM.ORG that people have mentioned in relation to the stock market is if you need to make trades that are independent of market trends. As noted in our introduction to randomness, it is surprisingly difficult for humans to behave randomly, so if you need make trades that are certain not to be affected by your (conscious or unconscious) knowledge of the market, then RANDOM.ORG may be helpful. Some people who ask this question believe that the stock market is affected by (and/or affects) a type of human global consciousness. We have not seen any evidence to support this type of theory, but if it interests you see section 8 of this FAQ. Q3.6: How do I pick one or more items from a list at random? The easiest way to do this is to use the List Randomizer as follows: Enter all your list items on separate lines in the List Randomizer and submit the form. This will produce a randomized list. The item picked will be the first that appears on the randomized list. If you need to pick two items, use the first two from the randomized list, and so forth. Discard the remaining items. This will work with up to 10,000 items, which is the maximum number of items that the List Randomizer supports. If you have more items, you will need a subscription to the Premium Generator and should use the procedure described in question 3.7. Q3.7: How do I pick one or more items from a list of more than 10,000 at random? In this case, you will need a subscription to the Premium Generator. Then use the following procedure: Make sure all your items are numbered sequentially, for example by pasting them into rows in a spreadsheet. Go to the Premium Generator and enter the number of items you want to pick into the first field (the number of integers to generate). Enter the number of the first and the last item in your list (e.g., the row numbers in your spreadsheet) into the next two fields (the range for the integers). Select the ‘Unique’ option to make sure each item can only be picked once. Submit the form and use the resulting numbers as indices into your list. If you're using a spreadsheet, they will be the numbers of the rows that contain the items picked. This procedure will allow you to pick up to 10,000 items from a list of up to 1,000,000,000. (Actually, the list can be up to 2,000,000,001 items long but then you need to assign negative numbers to some of them, which can be a bit messy.) Q3.8: Can I use Excel to fetch numbers from RANDOM.ORG? Yes. Not being Excel macro wizards ourselves, we're not sure this is the easiest way, but it should work. Excel needs a URL to RANDOM.ORG that it can use to fetch the numbers. Check out the HTTP API to create the URL that'll give you the numbers you need. Most likely it will look something like this. Follow Microsoft's instructions on Different Ways of Using Web Queries in Excel to create a macro that will fetch the numbers from your URL. Some generous folks have donated macros that you're welcome to use. Thanks so much! Macro donated by Joey LoSurdo on 2016-07-28: Sub RandomOrgApi() Dim min As Integer: min = 1 'user defined Dim pop As Integer: pop = 10000 'user defined Dim num As Integer: num = 25 'user define Dim url As String: url = " & num & "&min=" & min & "&max=" & pop & "&seqnos=on&commas=on&sort=on&order=index&format=plain&rnd=new" Dim http As New WinHttpRequest http.Open "GET", url, False http.Send Dim resp As String: resp = http.ResponseText Dim lines As Variant: lines = Split(resp, ",") Dim sline As String Dim firstsline As Variant For i = 0 To UBound(lines) sline = lines(i) If i = o Then firstsline = Split(sline, ":") Range("a" & i + 1).Value = firstsline(0) Range("a" & i + 2).Value = firstsline(1) Else If InStr(sline, Chr(10)) > 0 Then Range("a" & i + 2).Value = Replace(sline, Chr(10), "") Else Range("a" & i + 2).Value = sline End If End If Next i End Sub Macro donated by Vance Joines on 2016-09-01: Function RandomNumber() Application.Volatile True Dim oXMLHTTP As Object Dim sRandomNumber As String Dim sURL As String 'Change the URL before executing the code 'You can customize your random.org URL at sURL = " 'Extract data from website to Excel using VBA Set oXMLHTTP = CreateObject("MSXML2.ServerXMLHTTP") oXMLHTTP.Open "GET", sURL, False oXMLHTTP.send sRandomNumber = oXMLHTTP.responseText 'Get webpage data into Excel RandomNumber = sRandomNumber End Function If you wish to donate another macro, please email us and we'll put it here. Section 4: Questions about the Premium Generator and the Quota System Q4.1: Why is there a limit to the amount of randomness I can use per day? Generating true random numbers takes time. The RANDOM.ORG setup uses an array of radios that pick up atmospheric noise. Each radio generates approximately 12,000 bits per second. The random bits produced by the radios are used as the raw material for all the different generators you see on RANDOM.ORG. Each time you use one of the generators, you spend some bits. By enforcing a limit on the number of bits you can use per day, the quota system prevents any one person from hogging all the numbers. (Believe us, this was a big problem before we implemented the quota system.) Q4.2: What exactly constitutes a bit and how many bits do I need? A bit is a value that can be either 0 or 1. On RANDOM.ORG, a bit is the basic unit of randomness. The generator essentially generates one long string of one 0s and 1s. Every time you request some numbers, flip some coins or use one of the other services, you use some of these bits. Exactly how many depends on which of the services you are using. For example, flipping a single coin with the Coin Flipper uses exactly one bit. If the bit is 0, your coin comes up reverse (typically tails) and if it's 1, the coin comes up obverse (typically heads). The other RANDOM.ORG services (such as the Integer Generator and the String Generator) require different amounts of bits, depending on how many numbers or strings you request. You can always check your quota to see how many bits you have left of your allowance. (See question 4.1 about why there is an allowance in the first place.) If you need to generate many numbers or strings, it is useful to know how many random bits it is going to require. The number of bits needed affects how fast you will be able to generate the numbers (or strings) if you are using the free daily allowance of bits. If you want to purchase an extra allowance, the number of bits required helps you estimate how large an extra allowance you need. It is a little tricky to calculate the exact number of bits required for generating numbers and strings, because the number of bits varies with the size of the interval for numbers and for the length of strings, etc. In addition, the bit cost can vary between requests due to the scaling algorithms used. For these reasons, the best way to estimate bit cost for your requests is simply to try it out by first checking your quota, then requesting a sizeable chunk of numbers or strings (e.g., 1,000) with the parameters you need, then check your quota again immediately afterwards. The difference in your quota level before and after will tell you how many bits were required for your request. You can then use that number to calculate the average bit cost per number or string, and then estimate the total number of bits you need in order to generate all the numbers or strings that you want. Section 5: Questions about the Third-Party Draw Service Q5.1: What is the Third-Party Draw Service for? The Third-Party Draw Service is for professional operators of raffles, sweepstakes, promotional giveaways and other lottery type services. In a similar fashion to a certified official, RANDOM.ORG acts as an unbiased third party who conducts the drawings in a manner that is guaranteed to be fair and truly random. It has been operating since 2007 and is being used by bloggers [example], charities [example] and by PR and Media companies [example] for promotional campaigns and competitions. It is the most reputable and convenient solution for holding random drawings online. Q5.2: How much does it cost? There is a per-drawing cost, which depends on the number of entrants. The Price Calculator will tell you exactly how much. A drawing can have multiple winners (1st, 2nd, etc.), which does not affect the cost. To use the service, you must create a RANDOM.ORG Premium Account with at least $4.95 worth of prepaid credit. The prepaid credit is used to pay for your drawings. There is no maintenance fee for use of the Third-Party Draw Service, only the cost of the drawings. Q5.3: How do the different types of drawings work? When you hold a drawing, you can choose to make the permanent record private, public or entrant-accessible. You can also hold test drawings. Private drawings are only visible to someone who holds the username and password associated with the owner account. This is useful if you expect your drawing to be audited but do not necessarily want everybody to be able to view the details. Public drawings have records where the full details are visible to anyone who visits the RANDOM.ORG web site. This is useful if you want anyone to be able to verify that the drawing was conducted as you promised, but you need to be aware that the entrant identifiers will be displayed publicly and that there may be privacy concerns. Please see question 5.4 for further details. Entrant-accessible drawings have records in which the full details of entrants and winners are only visible to the owner, but where entrants who know their identifiers can query the record to see if they were entered and whether they were picked as winners. Test drawings allow you to familiarize yourself with the service. They don't generate records and don't cost anything. Feel free to hold as many test drawings as you like. Q5.4: Why do I need to be careful with public drawings? When you hold a public drawing, the full lists of winners and entrants will appear on the drawing's record. This means they will be visible to anyone and that they will be indexed by search engines. For this reason, you should be careful about what you use for entrant identifiers in public drawings. It is generally fine to use anonymous identifiers (such as ticket numbers or internal database identifiers), but you should avoid using identifiers that your entrants don't want to see published on the web, such as full names or email addresses. If you wish to use people's email addresses, you should choose a private or entrant-accessible drawing instead. Please see question 5.3 for further details. Q5.5: How long do the records of drawings persist? The record of a given drawing persists for at least five years from the time at which the drawing was completed. Q5.6: How many entrants and winners can there be in a drawing? The Third-Party Draw Service currently supports up to 3,000,000 entrants and 50,000 winners in a single drawing, but more can be accommodated on request. Q5.7: Are my entrant identifiers safe with RANDOM.ORG? RANDOM.ORG will never use the entrant identifiers (e.g., email addresses, customer numbers, etc.) that you upload for anything else than allowing people to verify their participation in your drawings. We respect your entrants' privacy and disapprove of spam as much as you do. If you use entrants' email addresses to hold drawings, please make sure your drawings are entrant-accessible or private. This ensures the email addresses will not appear on the records of your drawings. Q5.8: Can I modify the record of a drawing once it has been completed? No. Q5.9: Can I make a public drawing private or vice versa? No. It is not possible to modify the record of a completed drawing. Q5.10: Can the same entrant appear multiple times in a single drawing? Yes. If you specify the same entrant identifier multiple times, then that entrant will have as many winning chances as their identifier was listed. And if your drawing is entrant-accessible, then the drawing's record will tell each of your entrants exactly how many chances he or she had. To make sure you really want to give your entrants multiple chances, the Third-Party Draw Service will give you a warning when you upload such an entrant list, but you can proceed past the warning if that is really your intention. Important note: If you have multiple winners in your drawing, then the Third-Party Draw Service does not prevent entrants with multiple chances from winning multiple times. For example, if someone has two chances in your drawing and is picked as 1st winner, then that entrant will still have one chance left to be picked as 2nd or 3rd winner, etc. If you wish to prevent an entrant with multiple chances from winning more than once, then you must hold a separate drawing for each winner. A future release of the Third-Party Draw Service will allow entrants with multiple chances to be eliminated from your drawing once they have been picked as winner once. Q5.11: Can I use something else than email addresses in my drawing? Yes, you can use any text strings or numbers as entrant identifiers. (See also Q5.12 about phone numbers.) In particular, customer numbers, user nicknames and ticket numbers (as in numbered tickets sold in a raffle) are all popular options. However, there are a couple of things you should be aware of: If your drawings will be public or entrant-accessible, you should make sure that each entrant knows what their entrant identifier is before the drawing takes place. This protects you from accusations of holding the drawing first and assigning the identifiers later. People know what their email addresses are, which is why they are often a good choice as entrant identifiers. If your drawings will be private, you should choose your entrant identifiers such that you cannot change how they map to your entrants. Again, this is to protect you from accusations of holding the drawing first and then deciding which entrants gets the winning identifiers. Customer numbers are a good choice (especially if your customers know what they are), but row indices into a spreadsheet are not. Q5.12: Can I use phone numbers instead of the email addresses in my drawing? The Third-Party Draw Service will work fine with phone numbers instead of email addresses, and your drawing will cost the same regardless. The only concern is that all phone numbers must be formatted exactly the same way (even down to the use of spaces, brackets, etc.) and that entrants who wish to verify their participation must enter them in that way. If you are in the USA, a good way of formatting a phone number in a way that doesn't cause confusion is not to use brackets or spaces, but simply use dashes to separate the groups of digits, e.g., 123-456-7890. (You can also use dots, such as in 123.456.7890, but dashes are a little more common.) Don't forget to tell your entrants how you write their phone numbers. Section 6: Questions about Scientific Publication and Media Coverage Q6.1: Are there any scientific publications that document RANDOM.ORG? Not currently. We don't really consider it research as such, more like a useful piece of engineering. See question 6.3 for how to cite RANDOM.ORG. Q6.2: Has the service been cited in peer-reviewed publications? Yes, see the Media and Citations page for details. If you publish a peer-reviewed publication that references RANDOM.ORG, it would be great if you could drop us an email. Q6.3: Can I link to RANDOM.ORG or cite it as a scientific publication? You are certainly welcome to do so, and you don't need my express permission to do either. Since we haven't yet documented RANDOM.ORG in a scientific publication, we suggest you cite the web site. Section 7: Questions about Games and Gambling Q7.1: Will you help me break the bank on online gambling site X? No. Occasionally, people send us datasets of observations they have made from playing online poker, roulette or other games and ask for help to show that the results are so unlikely that there must be something wrong with the gambling site. At other times, we're asked to help exploit the perceived anomalies to break the site's bank. If the gambling site you use is legitimate, it will be regulated by the government in the jurisdiction where it resides, such as the Gambling Commission in the UK or the Gambling Supervision Commission on the Isle of Man. One role of such regulators is to ensure that the random numbers used are of good quality. The exact requirements vary between jurisdictions, but unless there are serious flaws in the gambling site's software, we don't think you'll have much luck predicting the numbers. Section 8: Questions about Parapsychology and Global Consciousness Q8.1: Are the numbers suitable for parapsychological experiments? Probably not. The numbers generated by RANDOM.ORG are buffered, which means that they are actually generated before you request them. We understand that this precludes their use in those parapsychological experiments that attempt to measure whether it is possible for individuals to affect otherwise random events. We are not currently planning to offer an unbuffered randomizer. Q8.2: Were there anomalies in the numbers on 11 September 2001? People who ask this question have usually read about the Global Consciousness (GC) Project. The GC people collect data generated by true random number generators and analyse it for anomalities occurring at the same time as events affecting large groups of people, such as major earthquakes, Lady Diana's funeral or the 9/11 attacks. Seemingly, the GC results show strange anomalies in data generated around the time of the attacks. This has lead people to ask if we have noticed any change in the numbers generated by RANDOM.ORG on that day. The short answer to this question is really no. However, we should qualify to say we don't think it's meaningful to compare, and that a comparison doesn't say anything (either way) about the GC results, simply because the software we're using is not intended to be used for the type of experiment the GC people are doing. First, we don't keep the numbers around for later; they're discarded as soon as they've been served to clients. Second, the generator doesn't produce a constant stream of numbers (like we presume the GC project's generators do) but works in a kind of start-and-stop mode, depending on whether the numbers are needed or not. For this reason, there are sometimes periods of time where the generator is not producing numbers. Q8.3: Were there anomalies in the numbers during the Asian tsunamis on 26 December 2004? In short, no. Like for 9/11 (see question 8.2), we haven't analysed the logs thoroughly with this in mind, and the generator isn't at all geared towards this type of experiment. Q8.4: Is the universe deterministic? Yes. No. Maybe. Well, we hope not, because if the universe is deterministic, then all this randomness business is really a bit pointless. Hard determinism also seems to preclude the idea of free will, which is a somewhat unsettling idea. Wikipedia has a good article on the subject of determinism and there is also our own essay about randomness. Advisory: Historical results for the Third-Party Draw Service are currently unavailable. We are working on bringing them back. Lottery Quick Pick This form allows you to quick pick lottery tickets. The randomness comes from atmospheric noise, which for many purposes is better than the pseudo-random number algorithms typically used in computer programs. If your lottery is not listed, pick any country, then select ‘Other Lottery’ and fill in the other fields. You can also email us the lottery details. If you want to know more about your chances, you can use Gerry Quinn's Lotto Odds Calculator (requires Java). See the FAQ about whether RANDOM.ORG's lottery quick pick will help you win. Advisory: Historical results for the Third-Party Draw Service are currently unavailable. We are working on bringing them back. Random Sequence Generator This form allows you to generate randomized sequences of integers. The randomness comes from atmospheric noise, which for many purposes is better than the pseudo-random number algorithms typically used in computer programs. Note: A randomized sequence does not contain duplicates (the numbers are like raffle tickets drawn from a hat). There is also the Integer Generator which generates the numbers independently of each other (like rolls of a die) and where each number can occur more than once.