

You have **1** free member-only story left this month. [Sign up for Medium and get an extra one](#)

# This Is the World's Only Unbreakable Encryption

But we can't use it to save us from the future



Ella Alderson

Follow

Jan 23 · 6 min read ★



Art from USA Network's "Mr. Robot".

How strange it is to think that some part of us exists online. Who we are no longer has a purely physical answer. Our work, thoughts, relationships, and obsessions exist online,

extensions of ourselves that make it possible for people to get to know us without ever having to occupy the same rooms as us. Or even the same country. This is the transition of the human to the cyborg — we are starting to shift more and more of our lives onto our machines.

Encrypting our messages, then, is about more than just protecting our money. It's about protecting some aspect of our humanity as well. And up until now we thought our information was very well protected. Cryptographers have come up with clever ways to keep our text messages and bank information safe from criminals and agencies. But all of that will someday change. As a seemingly inevitable computer revolution looms on the horizon, it casts an uncertain shadow on the privacy of our lives. By some estimates, it may already be too late to keep our sensitive information safe.

Current methods of encryption use something known as integer factorization. The security of this method is based on a straightforward mathematical problem: given a large number, what are the factors which multiply to give you that number? It's simple enough in theory, but in practice it can take even the world's most powerful supercomputers billions of years to answer. For information using the Advanced Encryption Standard (AES) of 128, 192, or 256 bit keys, it would take the combined computational power on all of Earth trillions of years to decrypt even the smaller 128 bit key. This kind of encryption is used for iPhone files and websites using HTTPS (like Medium).

Yet even this kind of encryption is at risk of becoming obsolete. As supercomputers advance and people have at their disposal ever greater amounts of computational power, experts understand that current internet encryption will not remain invulnerable forever. Perhaps the biggest threat to this security method bears the face of the quantum computer. Finding the factors of large numbers is a monumental task for a classical computer, but it's not much of a problem at all for quantum machines.

In fact, throughout the history of ciphers and cryptography, only one method of encryption has ever been mathematically proven to offer perfect security. It is the world's only unbreakable cipher. Yet its strength lies not in its digital complexity, but in its real-world simplicity.



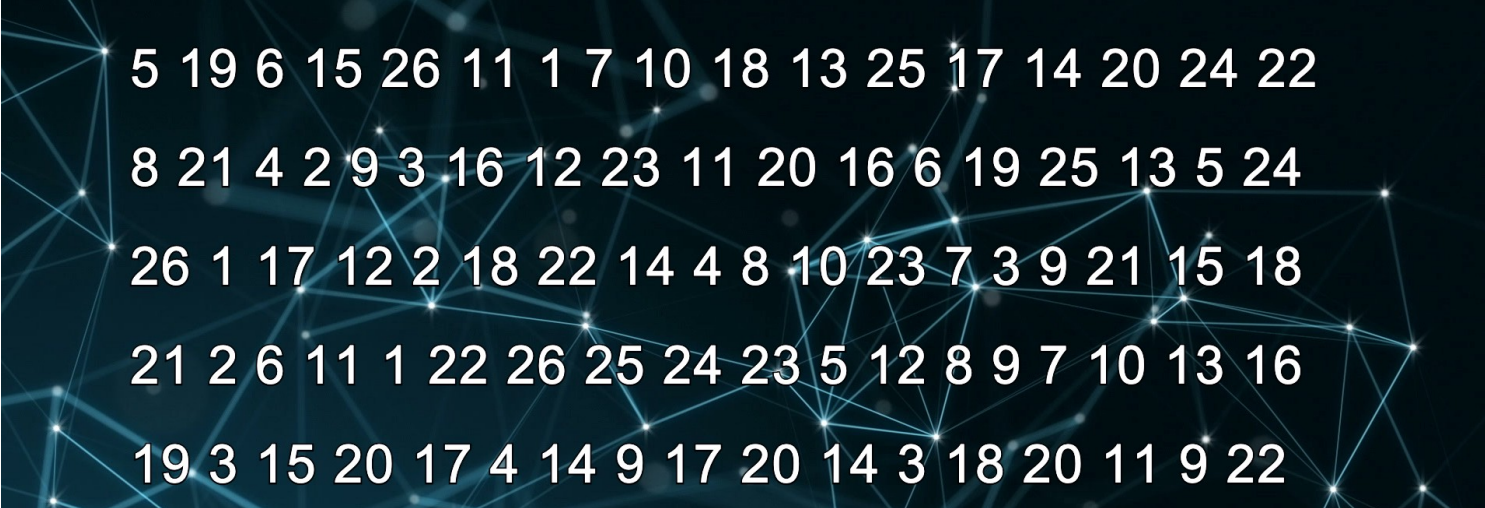
$$\Pr[M=m;C=c]=\Pr[M=m]$$

Mathematical proof by Claude Shannon that the OTP cipher is unbreakable.

The cipher is the one-time pad (OTP), so called because a pad of numbers can only be used once and must then be disposed of afterward. While there are many variations of the OTP cipher — some using binary, some grouping letters into sets, some using a Vigenere table, and so on — I'll give one of the easier encryption methods below.

We begin by first creating our OTP of numbers. It's important not to use an everyday number generator to do this. Computers rely on mathematics to come up with their “random” numbers, but patterns are prevalent throughout math. What seems like random numbers will be vulnerable to patterns if they're generated from a normal computer program. As this is the most important step in the OTP encryption process, you'll want to use Hardware Random Number Generators (RNG's). These kind of generators are based on physical events such as electrical noise from semiconductors or the passage of a photon through a filter. Alternatively, ten-sided dice can also be used to roll random numbers, making the entire encryption process non-digital.

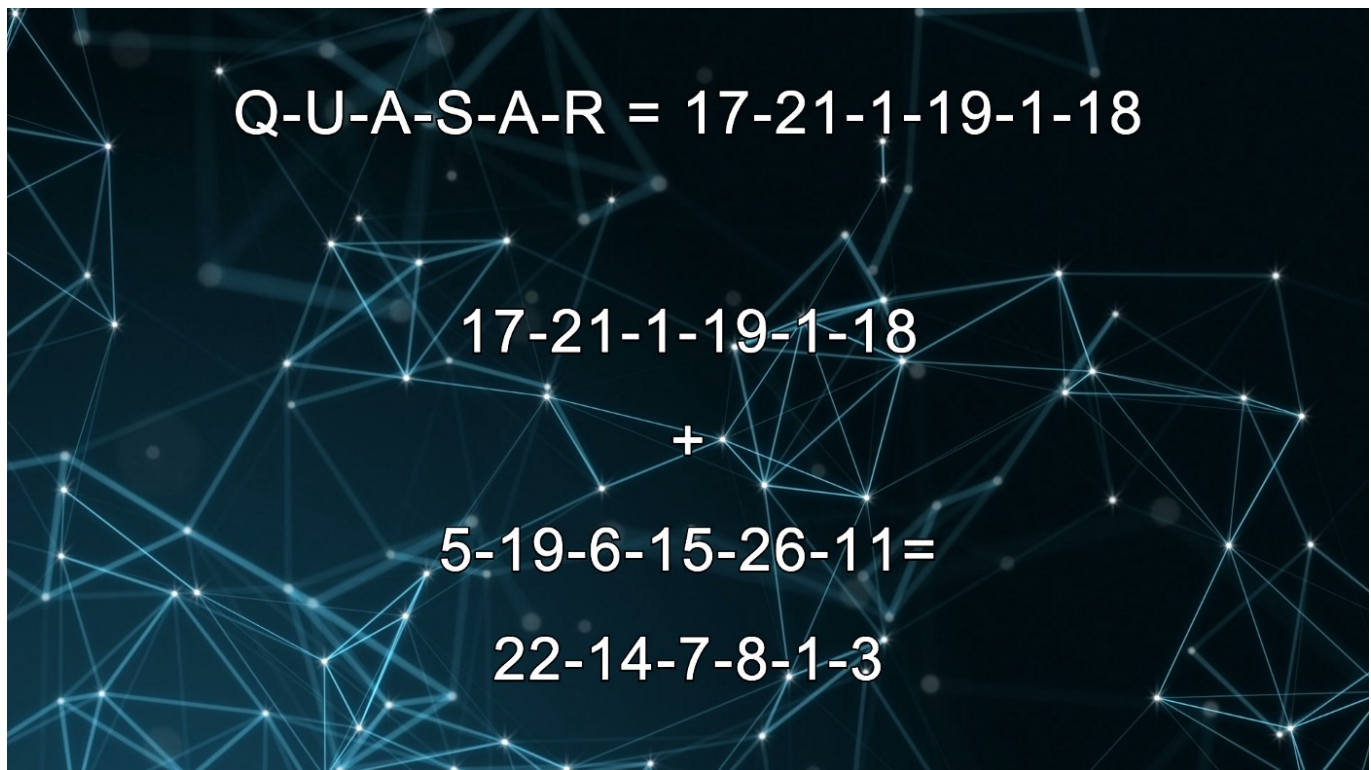
An OTP of random numbers will then look something like this:



5	19	6	15	26	11	1	7	10	18	13	25	17	14	20	24	22	
8	21	4	2	9	3	16	12	23	11	20	16	6	19	25	13	5	24
26	1	17	12	2	18	22	14	4	8	10	23	7	3	9	21	15	18
21	2	6	11	1	22	26	25	24	23	5	12	8	9	7	10	13	16
19	3	15	20	17	4	14	9	17	20	14	3	18	20	11	9	22	

One of the most inconvenient aspects of the OTP cipher is that both the sender and recipient of a message must have an exact copy of the numbers. Anyone who has access to this can decrypt your message.


Now let's imagine we want to send the word "quasar". We first find each letter's place in the alphabet. Q is 17 in the alphabet, u is 21, and so on. At the end we have this string of numbers to represent the word "quasar": 17-21-1-19-1-18. Using modular arithmetic, this string of 6 numbers will be added to the first 6 numbers in our OTP. 17 is added to 5, 21 to 19, 1 to 6, etc. The modular arithmetic is in place so that we don't end up with results larger than the number of letters in the alphabet, which is 26. So normally  $21 + 19 = 40$ , but with modular addition the 40 becomes 14.


$$\begin{array}{r} \text{Q-U-A-S-A-R} = 17-21-1-19-1-18 \\ 17-21-1-19-1-18 \\ + \\ 5-19-6-15-26-11 = \\ 22-14-7-8-1-3 \end{array}$$

Adding the 6 numbers of "quasar" with the first 6 numbers of our OTP gives us a new string of 6 numbers, seen at the bottom.

With our new set of numbers, we find the corresponding letters of the alphabet. The end result are the letters "VNGHAC" which are now the OTP encrypted version of "QUASAR".





This encrypted word shows how an OTP cipher is more efficient than something like a Caesar cipher. With Caesar encryption “QUASAR” could become something like “XBHZHY”, in which the letters are shifted by a certain amount. But their frequency is maintained. Because there are two letter a’s in the word quasar, there appear two letter h’s in the Caesar encryption. This is a major weakness. It means someone trying to decrypt the message will use their knowledge of letter frequency to figure out certain letters, compromising the security of the entire message. With OTP encryption, the word quasar may have multiple a’s yet the final encrypted word doesn’t repeat a single letter. Knowledge of letter frequency won’t be of any help.

The true strength of the OTP cipher, however, lies in the fact that there are two unknowns — the first being the encrypted text and the second being the random numbers of the pad. It is mathematically impossible to solve this encryption no matter how much time or computational power anyone might have. This perfect security is only ensured if one follows all of the OTP rules. Do not reuse numbers under any circumstances, destroy the OTP after use, and make sure the numbers are truly random.

OTP encryption was used during WW2 and the Cold War. Agencies like MI6 and the Russian Security Ministry still use it to this day. It’s not that a cipher like the One-time Pad is the future of security, but there is something poetic in realizing that the world’s most impenetrable form of encryption relies not on digital and computational power, but on simple actions between two people.

Perfect secrecy can't be found in the digital realm; but it does lie somewhere out here in the real world, taking the form of a piece of paper and a handful of dice. As the physicality of human beings begins to bleed into the machine, what does it say about the safety and security of our information going forward? Will our future descendants belong to themselves alone — or to someone else?

[Computer Science](#)   [Future](#)   [Technology](#)   [Education](#)   [Learning](#)

[About](#)   [Help](#)   [Legal](#)

Get the Medium app

