Simple Encryption You Can Do On Paper

Originalartikel

Backup

<html> <p>It&#8217;s a concern for Europeans as it is for people elsewhere in the world: there have been suggestions among governments to either outlaw, curtail, or backdoor strong end-to-end encryption. There are many arguments against ruining encryption, but the strongest among them is that encryption can be simple enough to implement that a high-school student can understand its operation, and almost any coder can write something that does it in some form, so to ban it will have no effect on restricting its use among anyone who wants it badly enough to put in the effort to roll their own.</p><p>With that in mind, we&#8217;re going to have a look at the most basic ciphers, the kind you could put together yourself on paper if you need to.</p><figure id=„attachment_474660“ aria-describedby=„caption-attachment-474660“ class=„wp-caption alignright c1“><a href=„https://hackaday.com/wp-content/uploads/2021/04/Captain-midnight-decoder.jpg“ target=„_blank“><img data-attachment-id=„474660“ data-permalink=„https://hackaday.com/2021/05/12/simple-encryption-you-can-do-on-paper/captain-midnight-decoder/“ data-orig-file=„https://hackaday.com/wp-content/uploads/2021/04/Captain-midnight-decoder.jpg“ data-orig-size=„844,1000“ data-comments-opened=„1“ data-image-meta=„{&quot;aperture&quot;:&quot;0&quot;,&quot;credit&quot;:&quot;&quot;,&quot;camera&quot;:&quot;&quot;,&quot;caption&quot;:&quot;&quot;,&quot;created_timestamp&quot;:&quot;0&quot;,&quot;copyright&quot;:&quot;&quot;,&quot;focal_length&quot;:&quot;0&quot;,&quot;iso&quot;:&quot;0&quot;,&quot;shutter_speed&quot;:&quot;0&quot;,&quot;title&quot;:&quot;&quot;,&quot;orientation&quot;:&quot;0&quot;}“ data-image-title=„Captain-midnight-decoder“ data-image-description=„“ data-image-caption=„“ data-medium-file=„https://hackaday.com/wp-content/uploads/2021/04/Captain-midnight-decoder.jpg?w=338“ data-large-file=„https://hackaday.com/wp-content/uploads/2021/04/Captain-midnight-decoder.jpg?w=528“ class=„wp-image-474660 size-medium“ src=„https://hackaday.com/wp-content/uploads/2021/04/Captain-midnight-decoder.jpg?w=338“ alt=„A Captain Midnight secret decoder ring. Sobebunny, CC BY-SA 3.0.“ width=„338“ height=„400“ srcset=„https://hackaday.com/wp-content/uploads/2021/04/Captain-midnight-decoder.jpg 844w, https://hackaday.com/wp-content/uploads/2021/04/Captain-midnight-decoder.jpg?resize=211,250 211w, https://hackaday.com/wp-content/uploads/2021/04/Captain-midnight-decoder.jpg?resize=338,400 338w, https://hackaday.com/wp-content/uploads/2021/04/Captain-midnight-decoder.jpg?resize=528,625 528w“ referrerpolicy=„no-referrer“ /></a><figcaption id=„caption-attachment-474660“ class=„wp-caption-text“>A Captain Midnight secret decoder ring. Sobebunny, <a href=„https://commons.wikimedia.org/wiki/File:Captain-midnight-decoder.jpg“ target=„_blank“>CC BY-SA 3.0</a>.</figcaption></figure><p>There have no doubt been cryptologists and codebreakers at work as long as there have been humans capable of repeating messages, and the strong public-key cyphers we use today were created by mathematicians who stood on the shoulders of those before them in an unbroken line that goes back thousands of years. It&#8217;s the public-key ciphers that

are in the eyes of the lawmakers, but perhaps surprisingly they are not the only strong encryption scheme that remains functionally unbreakable. A much older and simpler cypher also holds that property, and it&#8217;s this that we&#8217;re presenting as the paper-based answer to strong encryption legislation. The so-called one-time pad was a staple in tales of Cold War espionage for exactly the properties we&#8217;re looking for.</p><p>To explain a one-time pad it&#8217;s necessary to first travel back to ancient Rome, for the simple alphabetic substitution cypher. In its most basic form an alphabet from A to Z is either shifted or randomised, and the resulting list of letters is used to encrypt the message into the cyphertext by direct substitution. The cyphertext is encrypted, but its flaw comes in that it preserves the frequency distribution of the letters in the message text. Frequency analysis was a technique developed and refined by the mathematicians of the Islamic caliphates, in which the frequency of individual letters in a cyphertext could be compared with that of letters in the language as a whole. By this technique a codebreaker could identify enough of the letters in the message to reconstruct it by guessing those which remained.</p><figure id=„attachment_474663“ aria-describedby=„caption-attachment-474663“ class=„wp-caption alignleft c2“><a href=„https://hackaday.com/wp-content/uploads/2021/04/Vigenere-Beispiel.png“ target=„_blank“><img data-attachment-id=„474663“ data-permalink=„https://hackaday.com/2021/05/12/simple-encryption-you-can-do-on-paper/vigenere-beispiel/“ data-orig-file=„https://hackaday.com/wp-content/uploads/2021/04/Vigenere-Beispiel.png“ data-orig-size=„727,662“ data-comments-opened=„1“ data-image-meta=„{&quot;aperture&quot;:&quot;0&quot;,&quot;credit&quot;:&quot;&quot;,&quot;camera&quot;:&quot;&quot;,&quot;caption&quot;:&quot;&quot;,&quot;created_timestamp&quot;:&quot;0&quot;,&quot;copyright&quot;:&quot;&quot;,&quot;focal_length&quot;:&quot;0&quot;,&quot;iso&quot;:&quot;0&quot;,&quot;shutter_speed&quot;:&quot;0&quot;,&quot;title&quot;:&quot;&quot;,&quot;orientation&quot;:&quot;0&quot;}“ data-image-title=„Vigenere-Beispiel“ data-image-description=„“ data-image-caption=„“ data-medium-file=„https://hackaday.com/wp-content/uploads/2021/04/Vigenere-Beispiel.png?w=400“ data-large-file=„https://hackaday.com/wp-content/uploads/2021/04/Vigenere-Beispiel.png?w=686“ class=„wp-image-474663 size-medium“ src=„https://hackaday.com/wp-content/uploads/2021/04/Vigenere-Beispiel.png?w=400“ alt=„A Vigin&#232;re square. Log(z)equalsY, CC BY-SA 3.0.“ width=„400“ height=„364“ srcset=„https://hackaday.com/wp-content/uploads/2021/04/Vigenere-Beispiel.png 727w, https://hackaday.com/wp-content/uploads/2021/04/Vigenere-Beispiel.png?resize=250,228 250w, https://hackaday.com/wp-content/uploads/2021/04/Vigenere-Beispiel.png?resize=400,364 400w, https://hackaday.com/wp-content/uploads/2021/04/Vigenere-Beispiel.png?resize=686,625 686w“ referrerpolicy=„no-referrer“ /></a><figcaption id=„caption-attachment-474663“ class=„wp-caption-text“>A Vigin&#232;re square. Log(z)equalsY, <a href=„https://commons.wikimedia.org/wiki/File:Vigenere-Beispiel.png“ target=„_blank“>CC BY-SA 3.0</a>.</figcaption></figure><p>Addressing this flaw in the substitution cypher leads us to 16th century Italy and the polyalphabetic cypher, which instead of using a single substitution alphabet uses a number of them, switching from one to the next in sequence. The Vigen&#232;re cipher uses a table of alphabets each shifted by one letter with respect to the previous one, and switches from one to the next with each successive letter. By the use of a keyword to&#160; determine the sequence of which shifted alphabets in the table would be used for the substitution it created a cypher which was considered unbreakable until the 19th century, when mathematicians including Charles Babbage succeeded in breaking it by spotting the repeating patterns of its keyword.</p><p>So the Vigen&#232;re cipher is compromised, but its weakness lies not with its method but in the use of a repeating keyword to implement it. If a short keyword is used, such as &#8220;hackaday&#8221;, then it becomes in effect a series of eight sequentially repeating substitution cyphers; alphabet shifts h, a, c, k, a, d, a, and y in order over and over again, and a more complex but still achievable set of calculations will reveal its secret. These calculations become more complex as the length of the keyword increases, to the point at which it is the same length as the cyphertext and the possibility for spotting its repeats no longer exists.</p><h2>A One-Time Pad</h2><figure id=„attachment_474669“ aria-describedby=„caption-attachment-474669“ class=„wp-caption alignright c2“><a href=„https://hackaday.com/wp-content/uploads/2021/04/hackaday-one-time-pad.jpg“ target=„_blank“><img data-attachment-id=„474669“ data-permalink=„https://hackaday.com/2021/05/12/simple-encryption-you-can-do-on-paper/hackaday-one-time-pad/“ data-orig-file=„https://hackaday.com/wp-content/uploads/2021/04/hackaday-one-time-pad.jpg“ data-orig-size=„1280,854“ data-comments-opened=„1“ data-image-meta=„{&quot;aperture&quot;:&quot;0&quot;,&quot;credit&quot;:&quot;&quot;,&quot;camera&quot;:&quot;&quot;,&quot;caption&quot;:&quot;&quot;,&quot;created_timestamp&quot;:&quot;0&quot;,&quot;copyright&quot;:&quot;&quot;,&quot;focal_length&quot;:&quot;0&quot;,&quot;iso&quot;:&quot;0&quot;,&quot;shutter_speed&quot;:&quot;0&quot;,&quot;title&quot;:&quot;&quot;,&quot;orientation&quot;:&quot;0&quot;}“ data-image-title=„hackaday-one-time-pad“ data-image-description=„“ data-image-caption=„“ data-medium-file=„https://hackaday.com/wp-content/uploads/2021/04/hackaday-one-time-pad.jpg?w=400“ data-large-file=„https://hackaday.com/wp-content/uploads/2021/04/hackaday-one-time-pad.jpg?w=800“ class=„wp-image-474669 size-medium“ src=„https://hackaday.com/wp-content/uploads/2021/04/hackaday-one-time-pad.jpg?w=400“ alt=„Who remembers the Hackaday one-time pad?“ width=„400“ height=„267“ srcset=„https://hackaday.com/wp-content/uploads/2021/04/hackaday-one-time-pad.jpg 1280w, https://hackaday.com/wp-content/uploads/2021/04/hackaday-one-time-pad.jpg?resize=250,167 250w, https://hackaday.com/wp-content/uploads/2021/04/hackaday-one-time-pad.jpg?resize=400,267 400w, https://hackaday.com/wp-content/uploads/2021/04/hackaday-one-time-pad.jpg?resize=800,534 800w“ referrerpolicy=„no-referrer“ /></a><figcaption id=„caption-attachment-474669“ class=„wp-caption-text“>Who remembers the Hackaday one-time pad? Anyone done a frequency analysis on it?</figcaption></figure><p>A Vigen&#232;re cypher whose key is the same length as its text is unbreakable by frequency analysis in an attempt to spot the repeating keyword. But if the keyword itself contains a recognisable pattern such as a passage from a book or even a pseudo-random sequence there is still a chance that it can be compromised <a href=„https://hackaday.com/2016/08/23/colossus-face-to-face-with-the-first-electronic-computer/“>particularly if it is re-used</a>, and hence we come to the idea of the one-time pad.</p><p>If every message uses a fresh encryption key composed of random characters that is the same length as its text then it contains no clues to help a code-breaker, because the entropy of the cyphertext is the same as that of the random key. Those cold-war spies achieved this in a low-tech manner using a pad whose pages contained random key text and from which each page could be torn and discarded once it had been used, hence the term &#8220;one-time pad&#8221;.</p><p>One-time pad encryption then. It&#8217;s unwieldy because both parties have to have a copy of the same pad, and even though it&#8217;s simple enough to do with a paper and pencil (or even a set of XOR gates) it&#8217;s probably not a sensible alternative to more modern forms of encryption. But it is genuinely strong end-to-end encryption, which would make it subject to any attempts to curtail encryption. So the point of this article hasn&#8217;t been to persuade you all to switch to using a Vigen&#232;re square and a notebook full of random digits, instead it&#8217;s been to write down just how simple secure end-to-end encryption can be. If a child can do it with a pen and paper then the most novice of coders can implement it in a script with nothing more than a text editor, so any proposal to censure it seems like closing the stable door after the horse has bolted.</p> </html>

From:
https://schnipsl.qgelm.de/ - **Qgelm**

Permanent link:
https://schnipsl.qgelm.de/doku.php?id=wallabag:wb2simple-encryption-you-can-do-on-paper

Last update: **2025/06/27 11:17**