An Engineer’s Brief Introduction to Cryptography

Originalartikel

Backup

<html> <div class=„sp-content-block“> <div class=„lead“ itemprop=„headline“>This primer on cryptography will help you understand the encryptions that are necessary for modern IoT device security.</div> <p>Humans have shared information over great distances in written form for millennia. But when written messages are intercepted, and the text is plainly read by an enemy, an angry politician can start a war, or an otherwise competent general can lose a battle. So the need for encryption has existed as long as there were armies to lead and alliances to forge.</p> <p>All of that time, humans made incremental improvements. One big development in the field of cryptography happened just prior to World War 2 when engineers created an unbreakable code, and the British subsequently broke it. But cryptography really found its feet in the computer era with the invention of the Diffie-Hellman algorithm.</p>

<h3>Simple Ciphers</h3> <p>The simplest way for schoolchildren to share a secret is with a substitution cipher. This method simply swaps one character for another character or symbol. The sender of the message would obfuscate the meaning by changing the characters in the message for a predetermined character/symbol.&#160;The receiver of the message would use a matching codebook to determine the original symbol.</p>

<p class=„c2“><img alt=„“ src=„https://www.allaboutcircuits.com/uploads/articles/Introduction_to_cryptography_fig01.gif“ class=„c1“/></p> <h5 class=„c3“><em>Three substitution ciphers are shown above, each simply replaces one letter of the alphabet with another letter/symbol. &#160;</em></h5>

<p>This method has several flaws. For example, if the code is of sufficient length, an analyst can perform what is known as n-gram analysis or frequency analysis. The English language has spelling and grammar rules that cause letters and combinations of letters to appear with a predictable frequency. Once someone feeds the secret message into a computer, they can begin to guess which letters in the secret message correspond to letters in the original text.</p> <p>Below are frequency analysis and 2-gram analysis of the New Oxford Dictionary (no foreign or special characters) and Rudyard Kipling&#8217;s &#8220;The Jungle Book&#8221;. A cryptographer deciphering a secret message might infer that the most common character is e, and the least commonly used is q, x, or z, and so forth.</p>

<p class=„c2“><img alt=„“ src=„https://www.allaboutcircuits.com/uploads/articles/Introduction_to_cryptography_fig02.jpg“ class=„c4“/></p> <h5 class=„c3“><em>Frequency and n-gram analysis for &#8220;The Jungle Book&#8221; and the &#8220;Oxford Dictionary&#8221;</em></h5>

<p>But there is a bigger problem. &#160;Once an enemy deciphers a single message, they can decipher all messages that use this code.</p> <p>I use this childish example to illustrate three points:</p> <ul><li>Both the sender and receiver must agree on how to encode/decode the secret message</li> <li>A secret message of sufficient length that relies on the same substitutions can be cracked. &#160;In our example, the encryption scheme should be changed at a minimum every 26 letters.</li> <li>A cryptography system should provide forward-secrecy. &#160;So that if one message is deciphered, other messages cannot be.</li> </ul> <h3>Enigma Code</h3> <p>The Germans worked around this limitation with their use of the <a

href=„https://en.wikipedia.org/wiki/Enigma_machine“ target=„_blank“>Enigma Machine</a>. Inside was a typewriter keyboard, a series of rotors, and a lighted display. The rotors were electromechanical substitution ciphers with wires that would connect 27 inputs to 27 outputs. Every time a user pressed a key, an electrical current would run through the rotors connecting the key to the light. Then the rotor would rotate into a new position. A user could press the same key over, and over again, and each time would create a different connection to a new light. &#160;</p> <p>In short, the encryption rules didn&#8217;t change every 27 letters; the encryption rules changed with each and every key-press. The receiver would simply set up everything in reverse, plug the received message in, and pull the secret message out.</p>

<p class=„c2“><img alt=„“ src=„https://www.allaboutcircuits.com/uploads/articles/Introduction_to_cryptography_fig03.png“ class=„c5“/></p> <h5 class=„c3“><em>Enigma machine courtesy of the Museo della Scienza e della Tecnologia „Leonardo da Vinci“ [<a href=„https://creativecommons.org/licenses/by-sa/4.0“ target=„_blank“>CC BY-SA 4.0</a>]. Image by&#160;Alessandro Nassiri</em></h5>

<p>This was an absolutely brilliant scheme that took several governments and millions of man-hours over the course of several years to solve. And that involved capturing the machine and a codebook from the Germans.</p> <p>The issues the Enigma machine didn&#8217;t solve? &#160;There was some forward secrecy&#8212;once the Allies had figured out one code&#8212;they only had the codes for a single day&#8217;s worth of messages.&#160;But in an ideal situation, one code broken would lead to just a single message compromised. Also, the Germans still had to share physical code-books from one location to another location, which means the books could be intercepted or copied by spies.</p>

<h3>The Beauty of Asymmetry</h3> <p>Whitfield Diffie and Martin Hellman came up with an ingenious realization. The same properties of multiplication that allow the multiplication numbers in any order allow the multiplication of numbers in different locations. The article that follows this one will explain the Diffie Hellman algorithm and modular arithmetic in detail. But essentially the sender and receiver each calculates half of a math problem, exchanges their answer with the other, and then completes the calculation. &#160;</p> <p>What the sender and receiver are left with is a number that can be used to encode/decode a secret message. The information that is shared is known as a public key, and when it is multiplied by a private key, it creates a shared secret. The private key of one user is multiplied by the public key of the other.</p> <p>This arrangement allows for secrets to be created in full view of an enemy, with the enemy unable to do anything with the information.</p>

<h3>What&#8217;s next?</h3> <p>The next two articles will cover the <a href=„https://www.allaboutcircuits.com/technical-articles/the-diffie-hellman-exchange-in-embedded-cryptography/“ target=„_blank“>Diffie-Hellman exchange</a> as well as elliptic-curve cryptography (ECC) and elliptic-curve Diffie Hellman.</p>

</div> </html>

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

Permanent link:
https://schnipsl.qgelm.de/doku.php?id=wallabag:an-engineers-brief-introduction-to-cryptography

Last update: **2021/12/06 15:24**