|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Vigenère Cipher  **Description**  The Vigenère cipher is an example of a polyalphabetic substitution cipher. A polyalphabetic substitution cipher is similar to a monoalphabetic substitution except that the cipher alphabet is changed periodically while enciphering the message. This makes the cipher less vulnerable to cryptanalysis using letter frequencies.  Blaise de Vigenère developed what is now called the Vigenère cipher in 1585. He used a table known as the Vigenère square, to encipher messages. This page discusses two different versions of the Vigenère cipher, the autokey method and the keyword method.  Autokey Method  **Encipher**  In order to encipher a message using the Vigenère autokey method,  the sender and receiver must first agree on a *priming key*. The priming key is a single letter that will be added to the beginning of the message to form the key. The sender will encrypt the message by writing the plaintext on one line and writing the key on the line beneath it. The sender will use the plaintext and key letters to select a row and a column in the Vigenère square. The selected row is the row in which the plaintext letter is in the first column and the selected column is the column in which the key letter is in the first row. A ciphertext letter will be the letter that appears in the Vigenère square at the position corresponds to the selected row and  column. In the following example, to find the ciphertext letter, first locate the row in the Vigenère square that corresponds to plaintext letter T. Next locate the column that corresponds to the key letter L. The letter at which they intersect is the ciphertext letter, in this case E. Continue to do this for each pair of letters to form the compete ciphertext.   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Priming key: L     |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | plaintext: | T | O | B | E | O | R | N | O | T | T | O | B | E | | key: | L | T | O | B | E | O | R | N | O | T | T | O | B | | ciphertext: | E | H | P | F | S | F | E | B | H | M | H | P | F | |  |   **Decipher**  To decrypt a message, the row is selected using the priming key. Next, the receiver locates the first letter of the ciphertext in the selected row. The letter at the top of the column that contains the ciphertext letter is the first letter of the plaintext. Add the first letter of the plaintext to the key and use it with next ciphertext letter to continue decipherment.   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Example: Message: EHPFS FEBHM HPF Priming key: L   |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | key: | E | H | P | F | S | F | E | B | H | M | H | P | F | | ciphertext: | L | T | O | B | E | O | R | N | O | T | T | O | B | | plaintext: | T | O | B | E | O | R | N | O | T | T | O | B | E | |  |   **Security**  The Vigenère autokey method is not very secure. There are only 26 possible keys (the 26 letters of the alphabet). The code can be broken easily with an exhaustive search. Someone who wants to read a message encrypted using the autokey method need only try using each letter of the alphabet as the priming key until they produced a sensible message. This can be done, even without a computer, in a short amount of time. The basic idea behind the autokey Vigenère cipher can, however, be used to produce a more secure cipher.  Keyword Method  **Encipher**  The keyword Vigenère cipher is similar to the autokey method, but instead of using a single letter priming key, it uses a keyword. The keyword can be of any length greater than one, which provides an unlimited number of possible keys. To form the key, the sender writes the keyword repeatedly on the line underneath the plaintext. The plaintext-key pairs in each column will then be enciphered using the Vigenère square in the same way as the autokey method.  Example: Message: "What fools these mortals be"  Keyword: Puck   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | plaintext: | W | H | A | T | F |  | O | O | L | S | T |  | H | E | S | E | M |  | O | R | T | A | L |  | S | B | E | | key: | P | U | C | K | P |  | U | C | K | P | U |  | C | K | P | U | C |  | K | P | U | C | K |  | P | U | C | | ciphertext: | L | B | C | D | U |  | I | Q | V | H | N |  | J | O | H | Y | O |  | Y | G | N | C | V |  | H | V | G |   **Decryption**  To decrypt a message encoded with the Vigenère keyword method, first write the key repeatedly. Write the ciphertext beneath it. Decode each pair of key-ciphertext letters using the Vigenère Square the same way they were decoded with the autokey method.  Example: Message: LBCDU IQVHN JOHYO YGNCV HVG  Keyword: Puck   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | key: | P | U | C | K | P |  | U | C | K | P | U |  | C | K | P | U | C |  | K | P | U | C | K |  | P | U | C | | ciphertext: | L | B | C | D | U |  | I | Q | V | H | N |  | J | O | H | Y | O |  | Y | G | N | C | V |  | H | V | G | | plaintext: | W | H | A | T | F |  | O | O | L | S | T |  | H | E | S | E | M |  | O | R | T | A | L |  | S | B | E |   **Security**  The keyword Vigenère cipher is much more secure then the autokey method, but it is still vulnerable. The longer the keyword, the more secure the cipher. If the keyword is as long as the plaintext, for example, a previously agreed upon sample of text, the cipher is unbreakable if a new key is used for every message. In fact, suppose you received the following encrypted message:  JTLOM FJRCS XM  If the receiver uses the keyword hfikeniaoitz they would receive the message:  CODE IS BROKEN  If the receiver uses the keyword hfikenrnaygi they would receive te message:  CODE IS SECURE  Even if it were possible to calculate all the possible keywords of length 12 in a reasonable amount of time, the ciphertext would produce every sensible message of length 12. There is no way to determine which message the sender wished to communicate |