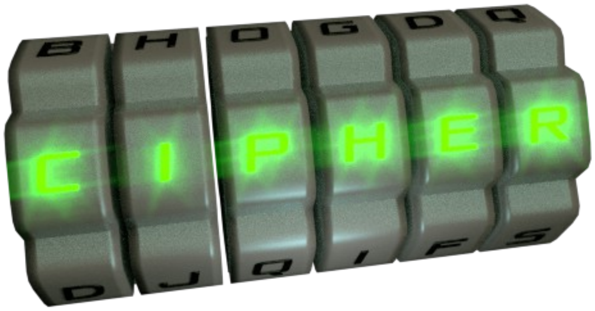


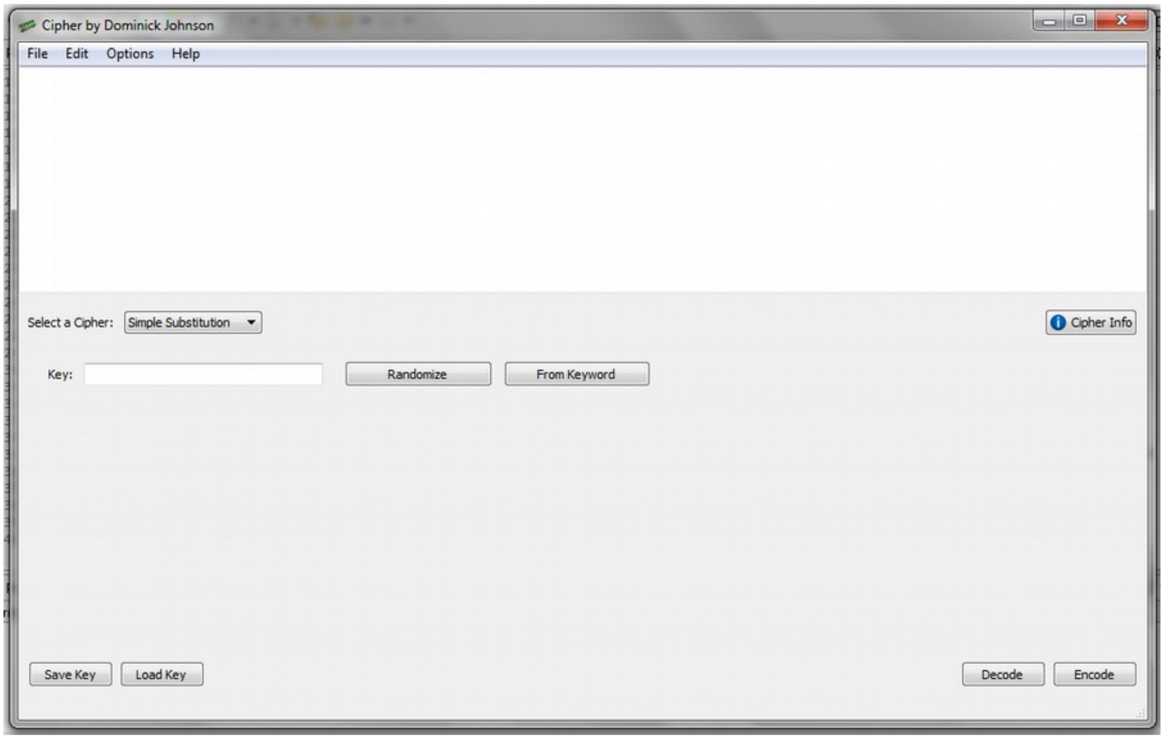
Cipher

Basic & Classical Encryption Software, by Dominick Johnson

Cipher is a form of basic encryption software designed to give you the ability to easily encrypt messages to send to your friends, family members, or co-workers. While by no means military grade encryption (Most of the ciphers included are hundreds of years old), they do a fine job of hiding information from most people. If you're afraid the government is spying on you, or want to keep something confidential, this may be the program for you!

Program Usage

Upon opening the program, you will be greeted by a screen like this:

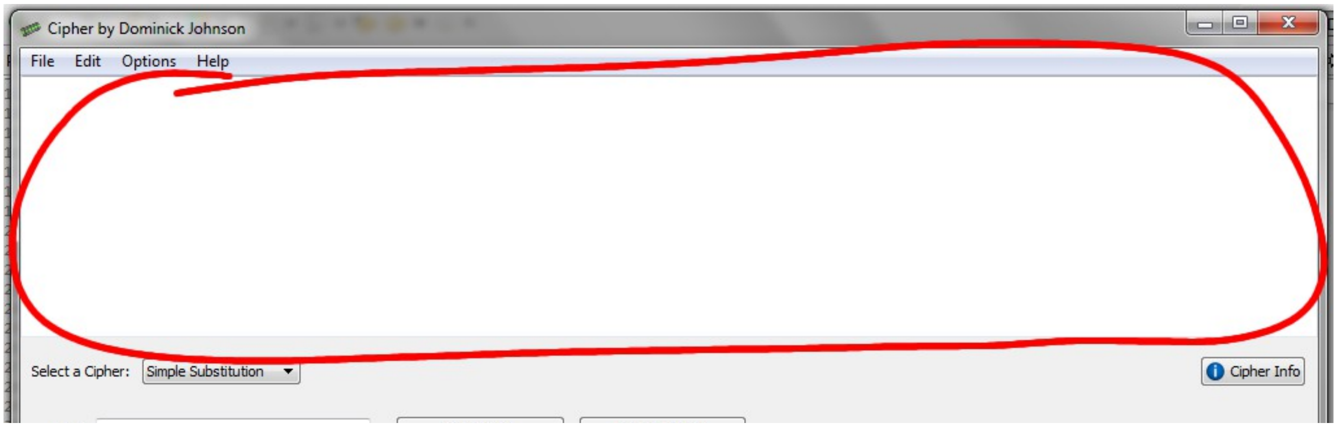

Cipher by Dominick Johnson

Select a Cipher: Simple Substitution

Key:

It will likely be slightly different for you, as the “default” cipher changes every time you start the program (A good way to let you sample all the different options).

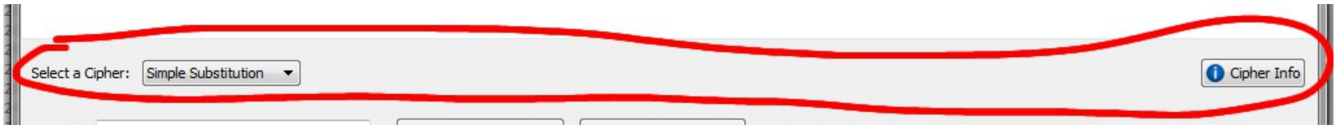
There are three important parts to the window layout. The first part is the text editor.



Select a Cipher: Simple Substitution

This is where you will enter your message to be encrypted. You can do this by typing it directly into the box, pasting it in from an external editor, or by opening a plain text file via File > Open. Depending on the options you have set, it may also be where the encrypted message appears after you press the "Encode" button. By default, this is shown in an external pop-up window, but you can change this by from Options > Text Display > Overwrite Existing Text.

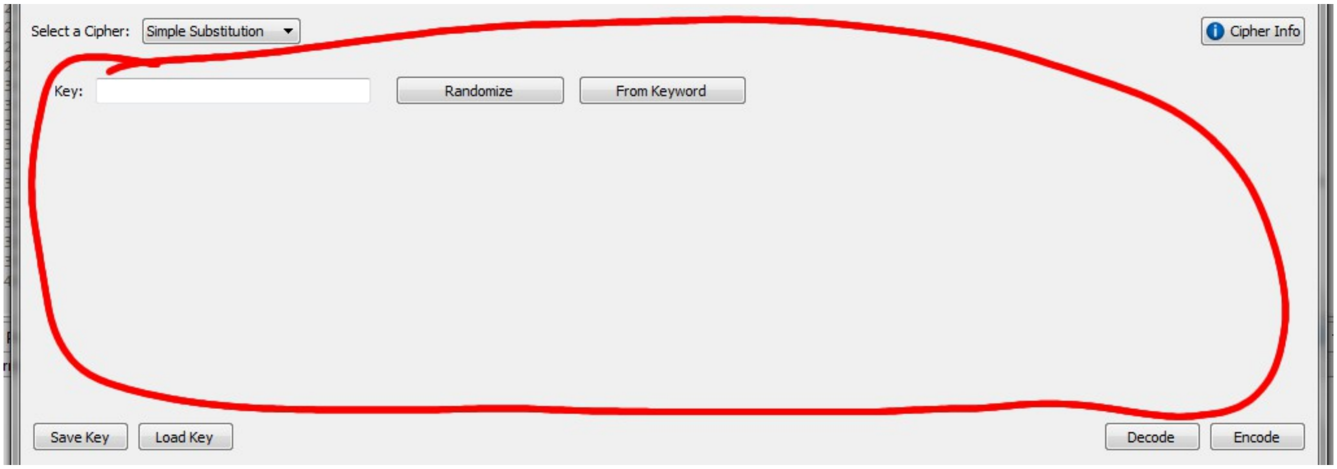
The next part of the window is the cipher bar.



Select a Cipher: Simple Substitution

This is where you can select the cipher you will be using. It also contains a Cipher Info button, which you can click to see information on whatever cipher you currently have selected. Is is basically just a condensed version of the information that appears in this manual.

Lastly, you have the cipher options area. This is where the settings and key entry for the current cipher are displayed. These options change depending on the cipher that is selected.



Select a Cipher: Simple Substitution

Below that, you'll see the Encode, Decode, Hack, and Save & Load Key Buttons (Though not all the buttons are displayed for every cipher.) These buttons each do exactly what they say.

Ciphers

The following is a quick overview of the ciphers implemented in this program.

Caesar Cipher

The Shift Cipher, also known as the Caesar Cipher due to the fact that it was often used by Julius Caesar, is a simple encryption technique in which every letter of the alphabet is 'Shifted' so many places over. For example, the letter 'A' shifted three places becomes 'D', while 'X' shifted three places becomes 'A'. The word “Hello” with shift 4 would become “Lipps”. This can be used to encrypt messages so that the meaning is not easily visible to an outside observer, however, it is not a very secure cipher. In fact, it is the weakest cipher available in this program. An average home computer using a brute force attack can break a Caesar Cipher message in a fraction of a second. Even done manually, a professional code breaker can crack a Caesar cipher in seconds.

Enigma Machine

The Enigma Machine was invented by the Germans in World War II for sending military messages. It consisted of a keyboard which send an electrical signal through a series of rotors which would each perform a simple substitution. When it reached the end, it would hit a reflector wheel which would send it back through the rotors, where it would light up a bulb on a board, indicating to the second operator which cipher letter to record. After each keypress, the first rotor would rotate one place. After the first rotor completed a full 360º rotation, the second rotor wound then rotate, which upon making a full rotation would cause the third rotor to rotate, and so forth.

Many Enigma Machines featured a plugboard which further complicated the process, adding another layer of security. This can be simulated here by adding a Substitution Cipher on top of the Enigma.

Hide

The Hide is not actually a real cipher, but it does do a fairly good job at scaring away any potential attackers. It works simply by hiding the message in the middle of a very large amount of “Garbage Data”, or, in other words, a huge mess of unintelligible and completely meaningless symbols. To solve it, the garbage data is stripped away by deleting the most frequently used characters in order to reveal the message. However, be warned that both enciphering and deciphering with this method takes a large amount of computer power owing simply to the massive amount of garbage encircling the message. The Hide can produce literally thousands of garbage symbols for each letter of the message. However, this disadvantage is also it's greatest advantage. It takes a LOT of work! More than enough work to scare off almost anyone who would want to read your message!

Null Cipher

The null cipher (Called such because it adds “null” or meaningless characters to the message) quite simply takes every letter in a message and replaces it with a word beginning with that letter. Plaintext words are separated by punctuation marks in the ciphertext. It is not so much an actual cipher as it is a fun puzzle for children but, if done manually, it can be done in such a way that others may not even realize that it actually contains any hidden messages. For example, "Meet at eight" could be disguised as “Mrs Emery eats tofu!? And tuna!? Ew, I'm gonna hurl tout-de-suite!” No one would even know it was a secret message! One problem with this cipher, however, is that you loose all "real" punctuation.

One Time Pad

The One-Time Pad cipher was named so because, for security reasons, a key may only be used one time. This is the cipher’s greatest downfall. However, if used correctly, the One-Time Pad cipher is impossible to decode without knowing the key. It was historically used by many military organizations throughout history, including the Soviet Union's infamous KGB.

Just to show how secure this cipher is, take a message as simple as a single word: "Hello". There are 11,881,376 different keys that could be used with this word, meaning that a brute force attack by a determined code-breaker would have to try each of those nearly twelve million variations, just for a word as simple as "Hello". The number of possible variation grows exponentially with each letter in the message, so an even longer message would have even more variations. A message with only 100 letters (Just a couple of sentences) would have over 3.143x10^{141} variations. Just to give you an idea of how huge of a number that is, it's more than the number of electrons scientists estimate are in the known universe!

But what makes the cipher 'impossible to break' is that multiple plaintexts could be derived from the same cipher text. For example, “P KLRY HSU” could be decoded to “I like pie”, “A mean dog”, “I feel ill”, “A gray van”, or any other sentence with a one-letter word, a four-letter word, then a three-letter word, depending on the key you use. And all those variations are just as likely.

The One-Time Pad cipher works by assigning each letter of the alphabet a numeric value from one to twenty-six. Then, using modular addition (With a modulus of 26), each letter of the message is added to the corresponding letter in the key.

Playfair

The Playfair cipher, named after Scottish scientist and politician Lord Lyon Playfair, who advocated it's use, was invented by English scientist Charles Wheatstone. It introduced a new type of cipher know as digraph substitution. Rather than encrypting letters one at a time, it took letters two at a time and encrypted them together. The playfair cipher consisted of a 5x5 grid of letters. As there would only be 25 squares in the grid, one letter, usually 'q' or 'x'. If two of the same letter are side-by-side, another letter, usually an uncommon letter so it will be easily recognized as an insertion, will be inserted between them.

To encode, two letters would be taken at a time from the message and located on the grid. Depending on the letters' position relative to one another, one of three rules would be used to encrypt them:

- If the letter are both in the same row, replace each with the letter directly to the right of it, wrapping if necessary.
- If the letters are in the same column, replace each letter with the letter directly underneath it, wrapping if necessary.
- Otherwise, replace each letter with the letter in its same row on the grid, but in the same column as the other letter.

Decoding is similar, except you go to the left instead of the right in the first rule, and up instead of down in the second.

Simple Substitution

Substitution ciphers are a type cipher in which every letter of the message is substituted by a different letter. Many of the ciphers in this program (Such as the Caesar Cipher, the Vigenère Cipher, and the One Time Pad) are substitution ciphers.

This particular substitution cipher, often simply known as "the" substitution cipher simply because it is the most well-known and straight-forward, maps every letter in the alphabet to exactly one letter in the key. For example, 'Q' might replace 'A' while 'G' replaces 'B', and so on.

Simple Transposition

The term "Transposition Cipher" refers to any cipher that changes the order of characters in the message rather than replacing them. Other examples of transposition ciphers include the Railfence Cipher and the Myszkowski transposition. (Neither of which are currently implemented here.)

This particular transposition cipher, one one of the simplest of its type, works by creating a grid. The number of columns in this grid will be your key. You write the letters of the message across the rows of the grid, then read them back from the columns. Decryption is the opposite.

Vigenère Cipher

The Vigenère Cipher was created as a way of increasing the security of the Caesar Cipher. Each letter of the key defines the Caesar Shift value to use for the corresponding letter in the message. As such, provided that the key is as long as or longer than the message, the Vigenère Cipher is identical to the One Time Pad. However, whereas the One Time Pad will not function with a key shorter than the message, the Vigenère Cipher uses one of two methods to expand the key to the proper length.

The method used when the cipher was first created was to simply repeat the key until it reached the required length. However, this proved not to be a very secure method. As such, the autokey method as an alternitive. In the autokey method, the actual plaintext message is appended to the end of the key so as to meet the length requirement.

Hill Cipher

The hill cipher is a form of block cipher that uses matrix multiplication to encode the message. Each letter is represented by a number (A=0, B=1... Z=25) and taken three at a time in a column vector, then multiplied (mod 26) by the key (a 3x3 matrix). Decryption is the same, except you multiply by the inverse mod 26 of the key matrix.

For example, to encode the word "and" you would do the following: (Note: the first matrix is the key matrix, the second represents the plaintext letters, and the result represents the ciphertext letters.)

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} x \begin{bmatrix} 0 \\ 13 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \\ 6 \end{bmatrix}$$

Encrypting it to "deg". To reverse the process, you would find the inverse matrix mod 26 of the key and substitute it for the key when multiplying.