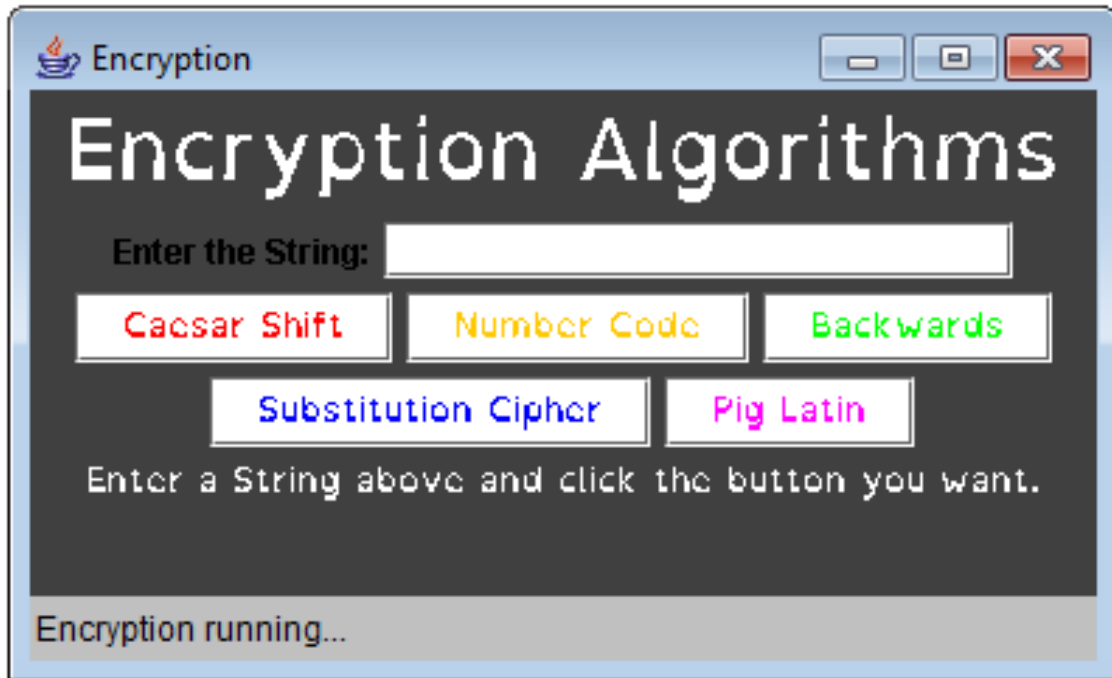


Encryption



Build the above applet. I will be in no way offended if you switch the colours. Look at http://www.gorskicompsci.ca/ICS3C/Unit5/B1_StringComparison.pdf to help with some starter code.

Write the code to make the buttons run. Your loops sheet should be helpful.

Code:

1. Caesar Shift
2. Number Code
3. Backwards
4. Substitution Cipher
5. Pig Latin

Hint:

This is the code to do a Caesar shift.

```
String shift1 = "bcdefghijklmnopqrstuvwxyz ";
String alpha = "abcdefghijklmnopqrstuvwxyz ";
String plainText = "plain text";
String cipherText = "";
for (int i = 0 ; i < plainText.length () ; i++)
    cipherText += shift1.charAt (alpha.indexOf (plainText.charAt (i)));
System.out.println (cipherText);
```

However, it is in a command line interface, so you will need to change the code in red to show the results in the applet instead. (use setText).

Bonus:

- Code another encryption algorithm.
- Obviously, this can produce many bonus codes. I will grant one for each algorithm.

If you can't find any online, read the following description from Martin Gardiner:

[1] The Rail Fence Cipher

Suppose you wish to encipher this message:

MEET ME TONIGHT

Count the number of letters. If the number is a multiple of 4, well and good. If not, add enough dummy letters at the end to make the number a multiple of 4. In this case there are 13 letters so we add three dummy letters, QXZ, to total 16. Such dummy letters are called "nulls." In a moment we will see why the nulls are added.

Write the message by printing every other letter a trifle lower on the page. The message will look something like a rail fence:

M E M T N G T X
E T E O I H Q Z

Copy the top row, then continue by copying the lower row.

M E M T N G T X E T E O I H Q Z

Encoding and decoding is simpler and more accurate if you divide the cipher text into groups of four or five letters each, because it is easy to keep that many letters in your head when you write. Besides, this makes the cipher harder to "crack" by the "enemy" because the divisions between the words are not indicated. In this book we will use a 4-group system. That was why three nulls were added in the preceding message. By increasing the number of letters to 16, we make sure that the last group of letters in the cipher text will have four letters like all the other groups.

This is how the final cipher text will appear:

MEMT NGTX ETEO IHQZ