2019-11-14: Cryptography continues.... (as it will for the rest of the semester)

```
> with(StringTools) :
```

First, let's build our alphabet. Today we like to distinguish between uppercase and lowercase.

```
> AllAscii:=convert([seq(n,n=1..127)],bytes):
> Alphabet:=cat(Select(IsUpper,AllAscii)," ",Select(IsLower,
  AllAscii));
Alphabet :=                                                              (1)
    "ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz"
```

Let's recreate the Caesar cipher from last time.

```
> StringToList:=proc(str::string)
    global Alphabet;
    return(map( s->SearchText(s,Alphabet), Explode(str)));
  end:
> ListToString:=proc(nums::list)
    global Alphabet;
    return(Implode(map(k->Alphabet[k],nums)) );
  end:
> StringToList("This is a test")
          [20, 35, 36, 46, 27, 36, 46, 27, 28, 27, 47, 32, 46, 47]        (2)
> ListToString(%)
                         "This is a test"                                (3)
> Caesar:= proc(msg::string, shift::integer)
    local numlist, alen, shifted;
    global Alphabet;
    alen:=length(Alphabet);
    numlist:=StringToList(msg);
    shifted:= map(x-> modp(x+ shift-1,alen)+1, numlist);
    return(ListToString(shifted));
  end:
> Caesar("Veni Vidi Vici",3)
                         "YhqlcYlglcYlfl"                                (4)
> Caesar(%,-3)
                         "Veni Vidi Vici"                                (5)
```

OK, all good.

Some discussion about ROT13, which is just a (form of a) Caesar cipher with a shift of 13. This can a common way to post some information such as a spoiler so someone doesn't read it by accident -- it is its own inverse. Maple has this built-in. There are other similar things... see the Encode help page.

```
> Encode(Alphabet,rot13)
    "NOPQRSTUVWXYZABCDEFGHIJKLM nopqrstuvwxyzabcdefghijklm"              (6)
> Encode("Bruce Willis is actually dead.", rot13)
                 "Oehpr Jvyyvf vf npghnyyl qrnq."                        (7)
```

```
> Encode(%,rot13)
                    "Bruce Willis is actually dead."                    (8)
```

Now back to what we were doing....
Discussion of the Vignere cipher, which can be viewed as several Caesar ciphers, and gives much better encryption.
First lets do it by hand.

```
> StringToList("MESSAGE")
                        [13, 5, 19, 19, 1, 7, 5]                        (9)
> StringToList("CAT")
                              [3, 1, 20]                                (10)
```

Here we get our shifts by repeating the key-shifts for the length of the message.

```
> ListToString([16,6,39,22,2,27,8])
                              "PFlVB H"                                 (11)
```

Now let's write it.

```
> Vignere:= proc(msg::string, key::string)
    local numlist, alen, klen, i, shifted, shifts;
    global Alphabet;
    alen:=length(Alphabet); # length of alphabet
    klen:=length(key); # length of key
    shifts:=StringToList(key); # turn my key into a list of shifts.
    numlist:=StringToList(msg); # convert message to numbers
    # now walk through the numlist, shifting by the appropriate
  amount.
    for i from 1 to length(msg) do
      numlist[i]:= modp(numlist[i]+shifts[modp(i-1,klen)+1] -1,
                       alen)+1;
    od;
    return(ListToString(numlist));
  end:
> CryptoCat:=Vignere("MESSAGE","CAT")
                       CryptoCat := "PFlVB H"                           (12)
```

We can calculate the set of shifts which undoes the orginal. It is off by one since there is no character corresponding to 0

```
> InvKey:=ListToString(map(x->-x-1,StringToList("CAT")))
                          InvKey := "wyf"                               (13)
> Vignere(CryptoCat,InvKey)
                             "MESSAGE"                                  (14)
```

This is conceptually messy, so let's write a procedure to do it for us.

```
> UnVignere:=proc(cryptext::string, key::string)
    local yek;
    yek:= ListToString(map(x->-x-1,StringToList(key)));
    return(Vignere(cryptext, yek));
  end:
> UnVignere(CryptoCat,"CAT")
                                                                        (15)
```

```
                              "MESSAGE"                                  (15)
> Poe:=Vignere("Once upon a midnight dreary while I pondered weak
  and weary", "Raven")
Poe :=                                                                   (16)
   "fPZKOMRkTOsBiOSFKcNhrFnKPJ WbWANaFwrRkTSwTaJOOGXQOsP
   FkwCnd"
> UnVignere(Poe,"Raven")
     "Once upon a midnight dreary while I pondered weak and weary"       (17)
> Longer:=Vignere("Once upon a midnight dreary while I pondered
  weak and weary", "Raven just tapping away")
Longer :=                                                                (18)
   "fPZKOV jgUBUOZUXXOIVXFqwCndOXSdeZACBfeXSMSGaBvwCgFPOOVpZBl
   "
> UnVignere(Longer,"Raven just tapping away")
     "Once upon a midnight dreary while I pondered weak and weary"       (19)
```

A discussion about one-time pads and a fake one-time pad using a pseudo-random generator.
Random gives us a random string of characters.

```
> Random(32,Alphabet)
                 "y KNhcGKmxYYTxRAPYLRkyzmiKLEfLmm"                      (20)
> Random(32,Alphabet)
                  "fFAydhnlfmMJoYQsFlWdUdEhl GQnsAH"                     (21)
> Randomize()
                            50662192345                                  (22)
> Random(32,Alphabet)
                  "FxzlqRHsccuhkkKZSxtHgNYkqGdXiPwW"                     (23)
> Random(32,Alphabet)
                 "y KNhcGKmxYYTxRAPYLRkyzmiKLEfLmm"                      (24)
```

Randomize(n) sets the seed for the randomizer so you can start at the same place in the "random" sequence. If (n) is the same, you get the same sequence of random characters.

```
> Randomize()
                            16914684608                                  (25)
> Randomize(5); Random(32,Alphabet); Random(32,Alphabet)
                                 5
                  "c HOvIeZpNKpquBlPp ACcFCVjNKAyjp"
                 "DgHSuneikDizVqpDdlmkCQwBTNvpocUQ"                      (26)
> Randomize(5); Random(32,Alphabet); Random(32,Alphabet)
                                 5
                  "c HOvIeZpNKpquBlPp ACcFCVjNKAyjp"
```

```
"DgHSuneikDizVqpDdlmkCQwBTNvpocUQ"                (27)
> Random(32,Alphabet); Random(32,Alphabet)
"XNPxchAfPWnQVqvsG OaLylQFRkkbGqM"
"PcmElgxLFUoYHZQTPrQuqtXMZLRbnsFR"                (28)
```

Can make a fake one-time pad from this, but there is no time left.