

USING MAPLE IN CRYPTOLOGY

Useful commands:

```
isprime(p);    tests whether  $p$  is prime
ifactor(n);    factors the integer  $n$ 
ithprime(n);   finds the  $i$ -th prime
nextprime(n);  finds the smallest prime  $> n$ 
prevprime(n);  finds the largest prime  $< n$ 
gcd(a,b);     finds the gcd of  $a$  and  $b$ 
power(a,e) mod n;  raises  $a$  to the power  $e$  and reduces mod  $n$  (works with very
large numbers)
power(a, -1) mod n; finds the inverse of  $a$  mod  $n$ 
```

-To enter a text, eg “Fourscore and seven years ago” and call it “ptext”:

```
ptext := [F,O,U,R,S,C,O,R,E,A,N,D,S,E,V,E,N,Y,E,A,R,S,A,G,O];
```

(This defines the expression “ptext” as an ordered list.)

-To find the number of letters in the text:

```
nops(ptext);
```

-To get the i -th letter in ptext:

```
ptext[i];
```

-To change letters in “text” to numbers with output “ntext”:

```
ntext := subs(A=1, B=2, C=3, D=4, E=5, F=6, G=7, H=8, I=9, J=10, K=11,
L=12, M=13, N=14, O=15, P=16, Q=17, R=18, S=19, T=20, U=21, V=22,
W=23, X=24, Y=25, Z= 26, text);
```

-To change numbers in “ntext” to letters with output “text1”:

```
text1 := subs(1=A, 2=B, 3=C, 4=D, 5=E, 6=F, 7=G, 8=H, 9=I, 10=J, 11=K,
12=L, 13=M, 14=N, 15=O, 16=P, 17=Q, 18=R, 19=S, 20=T, 21=U, 22=V,
23=W, 24=X, 25=Y, 26=Z, ntext);
```