Bullwinkle $p=11$, $q=31$ $\therefore n=pq=341$ ⇐ public

$(p-1)(q-1)=10\cdot 30=300$

Choose $e<341$, relatively prime to 300

(for example, $e=7$ works) ⇐ public

We'll need: sol'n to $ex\equiv 1 \mod (p-1)(q-1)$

$7x\equiv 1 \mod 300$

Use Euclid:

$300=7\cdot 42+6$

$7=6\cdot 1+1$

$6=1\cdot 6+0$

$\therefore 1=7-6\cdot 1=7-(300-7\cdot 42)\cdot 1$

$1=43\cdot 7-1\cdot 300$

(1·300: divisible by 300)

$\therefore 43\cdot 7\equiv 1 \mod 300$

Take $d=43$ private

Rocicy

To send $M = 123$:

$C = \text{code} = M^e \mod n$

$= 123^7 \mod 341$

$= 216$

) Hard work - see last page (or wolfram Alfa)

⇝ 216 to Bullwinicle

Bullwinicle

$C^d \mod n = 216^{43} \mod 341$

$=$ (really hard work!)

$= 123$ ✓

How to compute 123^7 mod 341 by hand:

$123^2 = 15129$

$\equiv 125 \bmod 341$

$$\begin{array}{r} 44 \text{ remainder } 125 \\ 341 \overline{)\,15129} \\ 1364 \\ \hline 1489 \\ 1364 \\ \hline 125 \end{array}$$

$125^2 = 15625$

$\equiv 280 \bmod 341$

(note $\equiv 123^4 \bmod 341$)

$$\begin{array}{r} 45 \text{ rem } 280 \\ 341 \overline{)\,15625} \\ 1364 \\ \hline 1985 \\ 1705 \\ \hline 280 \end{array}$$

$123^7 = (123^2)^3 (123)$

$\equiv (125)^3 \cdot 123 \bmod 341 = (125)^2 \cdot 125 \cdot 123 \bmod 341 \equiv 280 \cdot \underbrace{125 \cdot 123}_{=15375} \bmod 341$

$$\begin{array}{r} 45 \text{ rem } 30 \\ 341 \overline{)\,15375} \\ 1364 \\ \hline 1735 \\ 1705 \\ \hline 30 \end{array}$$

$\equiv 280 \cdot 30 \bmod 341 \equiv 8400 \bmod 341$

$$\begin{array}{r} 24 \text{ rem } 216 \\ 341 \overline{)\,8400} \\ 682 \\ \hline 1580 \\ 1364 \\ \hline 216 \end{array}$$

$\therefore 123^7 \bmod 341 = 216$