$P = 13 \quad Q = 41 \quad N = P \times q = 533$

Totient $= \phi(n) = (P-1)(q-1) = 12 \times 40 = 480$

if $1 < e < \phi(n)$ such that $\gcd(e, \phi(n)) = 1$

$\therefore$ 61 is fine as $\gcd(61, 480) = 1$

Now $61 \cdot x = 1 \bmod (480)$

where x is the inverse

Using Extended Euclidean Algorithm

$480 = 61(7) + 53$

$61 = 53(1) + 8$

$53 = 8(6) + 5$

$8 = 5(1) + 3$

$5 = 3(1) + 2$

$3 = 2(1) + 1$

$1 = 3 - 2(1)$

$= 3 - (5 - 3(1))$

$= 2(3) - 5$

$= 2(8 - 5(1)) - 5$

$= 2(8) - 3(5)$

$= 2(8) - 3(53 - 8(6))$

$= 20(8) - 3(53)$

$= 20(61 - 53) - 3(53)$

$= 20(61) - 23(53)$

$= 20(61) - 23[480 - 61(7)]$

$1 = 181(61) - 23(480)$

Taking mod on both sides

$181 \cdot 61 \equiv 1 \bmod 480$

$\therefore$ inverse of 61 is 181

if $e = 61$

then $d = 181$

$C = M^e \bmod n$

$M = C^d \bmod n$

Public key $(61, 533)$

Private key $(181, 533)$

Say I am encrypting J the asci

double("J") = 74

$\therefore C = 74^{61} \bmod 533$

$= 74^{32+16+8+4+1} \bmod 533$

$17^{61} \bmod 533$

2|61
2|30 -1
2|15 -0
2|7 -1
2|3 -1
1 -1

1 1 1 1 0 1
32 16 8 4 2 1

Encrypt
□
double(□) = 17

$17^1 \bmod 533 = 17$

$17^2 \bmod 533 = 17^2 \bmod 533 = 269$

$17^4 \bmod 533 = 269^2 \bmod 533 = 373$

$17^8 \bmod 533 = 373^2 \bmod 533 = 16$

$17^{16} \bmod 533 = 16^2 \bmod 533 = 256$

$17^{32} \bmod 533 = 256^2 \bmod 533 = 510$

$C = (510 \times 256 \times 16 \times 373 \times 17) \bmod 533$

$= 147$

$M = 147^{181} \bmod 533$

2|181
2|90 -1
2|45 -0
2|22 -1
2|11 -0
2|5 -1
2|2 -1
1 -0

1 0 1 1 0 1 0 1
128 64 32 16 8 4 2 1

$147^1 \bmod 533 = 147$

$147^2 \bmod 533 = 269$

$147^4 \bmod 533 = 269^2 \bmod 533 = 373$

$147^8 \bmod 533 = 373^2 \bmod 533 = 16$

$147^{16} \bmod 533 = 16^2 \bmod 533 = 256$

$147^{32} \bmod 533 = 256^2 \bmod 533 = 510$

$147^{64} \bmod 533 = 510^2 \bmod 533 = 529$

$147^{128} \bmod 533 = 529^2 \bmod 533 = 16$

$M = (16 \times 510 \times 256 \times 373 \times 269 \times 147) \bmod 533$

$= 17$

Now $M = 74$

$61 = 111101_2$

$C = 74^{61} \bmod 533$

$74^1 \bmod 533 = 74$

$74^2 \bmod 533 = 146$

$74^4 \bmod 533 = 146^2 \bmod 533 = 529$

$74^8 \bmod 533 = 529^2 \bmod 533 = 16$

$74^{16} \bmod 533 = 16^2 \bmod 533 = 256$

$74^{32} \bmod 533 = 256^2 \bmod 533 = 510$

$C \equiv 510 \times 256 \times 16 \times 529 \times 74$

$= 74$

$M = 74^{181} \bmod 533$

already'till $74^{32} \bmod 533$ solved above

$74^{64} \bmod 533 = 510^2 \bmod 533 = 529$

$= -4$

$74^{128} \bmod 533 = -4^2 \bmod 533 = 16$

$M = 74^{128+32+16+4+1}$

$= 16 \times 510 \times 256 \times 529 \times 74 \bmod 533$

$= 74$

$\therefore M = 74$ & we are back to J

∴ char (74) = J

2|181
2|90 – 1
2|45 – 0
2|22 – 1
2|11 – 0
2|5 – 1
2|2 – 1
1 – 0

10 11 0 10 1
128 64 32 16 8 4 2 1