***Choose n:***

     Start with two prime numbers, ***p*** and ***q***.  This time we try: p = 7 & q = 11.  Then n = p \* q = 7 \* 1 = 77.

***Calculate (n):***

     (n) = (p-1)(q-1) = 6 \* 10 = 60.

***Choose e & d:***

Let pick ***e***=13 and we need to compute ***d*** based on the equation:

***e\*d*** ≡ 1 mod (n)

e.g., 13 \* d ≡ 1 mod 

Note that we pick up ***e***=13 because gcd(*e*, (n))=1.

To compute ***d***, we use extended Euclidean algorithm:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | calculate ***d*** step by step |
| gcd(60,13) | 60=4\*13+8 | 8 = 60 - 4\*13 | *e* |
| = gcd(13,8) | 13=1\*8+5 | 5 = 13 - 1\*8 | *d* |
| = gcd( 8, 5) | 8 =1\*5+3 | 3 = 8 - 1\*5 | *c* |
| = gcd( 5, 3) | 5 =1\*3+2 | 2 = 5 - 1\*3 | *b* |
| = gcd( 3, 2) | 3 =1\*2+1 | 3 -1\*2 | *a* |
| = gcd( 2, 1) =1 |  |  |  |

Calculate ***d*** step by step

|  |  |
| --- | --- |
| 3 -1\*2 | *a* |
| 3 -1\*(5 - 1\*3) | *b* |
| 3 - 5 |  |
| (8 - 1\*5) - 5 | *c* |
| 8 - 3\*5 |  |
| 8 - 3\*( 13 - 1\*8) | *d* |
| 8 - 3\* 13 |  |
| (60 - 4\*13) - 3\* 13 | *e* |
| 60 - 23\*13 |  |
|  mod 60 = (60 - 23\*13) mod 60 | |
|  mod 60 = -23\*13 mod 60 | |
| -23\*13 ≡ 1 mod 60 ; note that ***e\*d*** ≡ 1 mod (n) | |
| ***d*** =-23 | |
| Have to pick ***d***=-23+60=37, we have to pick up positive number | |

***Verify*** ***e*** ***and*** ***d***

Since 13 \* 37 = 481 and 481 mod 60 = 1.

***Now test it out:***

     We know that

                   if   C = Pe mod n, then  P = Cd mod n.

     Let P = 2.

                   Then

                             C = 213 mod 77 = 8192 mod 77 = 30.

                   and we obtain P back again thus:

                   P = 3037 mod 77 = 4502839058909973630000000000000000000000000000000000000 mod 77

          = 2.