***SHOR’s Algorithm***

**N = The number to be factored into p \* q.**

**g = A random number larger than 1 but less than N.**

**t = The Period (The exponent of g – 1 when gx mod N = g). (Algorithm Doesn’t work if it’s not EVEN!!!!)**

**a = gt/2-1 b = gt/2+1**

**p = GCD(a, N) q = GCD(b, N)**

**EXAMPLE:**

N = 221 g = 73 (Chosen random number)

Let’s find the value **t:**

**g1 = 73**, g2 = 25, g3 = 57, g4 = 183, g5 = 99, g6 = 155, g7 = 44, g8 = 118,

g9 = 216, g10 = 77, g11 = 96, g12 = 157, g13 = 190, g14 = 168, g15 = 109, g16=1, **g17 = 73**

**Now,** we know our **t** = 16 because it’s the exponent of g - 1 the first time gx mod N = g.

**Next,** we can calculate our **a** and **b** values:

a = gt/2 – 1 b = gt/2 + 1

**Since we know t = 16, and g = 73 lets just solve the equations.**

a = 7316/2 – 1 b = 7316/2 + 1

a = 738 – 1 b = 738 + 1

a = 118– 1 b = 118+ 1

**a =117** **b = 119**

**Finally,** we have everything to factor **N**!! So let’s Calculate the GCD of (**a, N**) and (**b, N**).

**Since we know that a =117, b = 119, and N = 221 we just need to do Euclid’s Algorithm to find p and q.**

GCD(a, N) GCD(b, N)

GCD(117, 221) GCD(119, 221)

221 = 117 \* 1 + 104 221 = 119 \* 1 + 102

🡨--------|🡨----------------| 🡨--------|🡨----------------|

117 = 104 \* 1 + **13** 119 = 102 \* 1 + **17**

104 = 13 \* 8 + 0 102 = 17 \* 6 + 0

Once your addition part of the equation is **0** you take the last **non-zero** addition value as your **p** and **q.**

In this case it’s **p = 13** and **q = 17,** Just to confirm our work multiplying **13 \* 17 = 221** which is our **N.**

**\*\*\*\*\*\*\*\*\*\*Meaning you were successful in factoring N.\*\*\*\*\*\*\*\*\*\***