Lab 9 Shor's algorithm - using quantum period finding

Exercise T1 THEORY

Get familiar with using period finding for factoring (e.g. see section H http://www.lassp.cornell.edu/mermin/qcomp/chap3.pdf)

Exercise Q1 QUIDE

Use period finding function from last exercise to break RSA algorithm using simpler version (works with messages coprime with N)

Useful definitions:
b - encrypted message
G_N (i.e. group modulo N) - the set of all positive integers less than N (including 1) that have no factors in common with N.
*d is the inverse modulo of c in G_N if d*c=1 (mod N)*

The simpler version of RSA breaking algorithm:

1. Find r - period b^x mod N
2. Calculate d' - inverse modulo of c in G_r,
3. Calculate decrypted message a=b^d' (mod N)

Note: you'll need auxiliary functions:

1. Euclidean algorithm for greatest common divisor (you can use C# implementation)
2. Finding inverse modulo (you can use a loop with trying all possibilities or implement extended Euclidian algorithm)
3. Fast calculation of power using exponentiation by squaring (you can use C# implementation)

Exercise Q2 QUIDE

Use period finding function from last exercise to break RSA algorithm using the full version of the algorithm (by factoring i.e. finding p and q, where p*q=N)

1. Find p and q, (see section H of the document , to be explained during the lab)
2. Find d inverse modulo of c in G_(p-1)(q-1)
3. Calculate a=b^d (mod N)