Q:1(a)

For an 8-bit processor that takes 1 clock cycle for an 8x8 bit multiply-and-add, we can assume that it will take (512/8) = 64 clock cycles to perform that operation on 512-bit numbers and (1024/8) = 128 clock cycles to perform that operation on 1024-bit numbers.

Now, for b = 512 bits, we will have 511 squarings and on an average (0.5*512) = 256 multiplications. Thus, a total of 767 squarings and multiplications. Assuming that a b-bit multiplication and a b-bit squaring requires the same number of clock cycles, we will then need (767*64) = 49088 clock cycles for this task. If we want to finish the processing in less than 0.75 s, our processor clock speed must be (49088/0.75) >= 65451 clock cycles per second.

Similarly, for b = 1024 bits, we will have 1023 squarings and on an average (0.5*1024) = 512 multiplications.
Thus, a total of 1535 squarings and multiplications. Assuming that a b-bit multiplication and a b-bit squaring requires the same number of clock cycles, we will then need (1535*128) = 196480 clock cycles for this task. If we want to finish the processing in less than 0.75 s, our processor clock speed must be (196480/0.75) >= 261973 clock cycles per second.

Q:1(b)
Yes this looks like a reasonable goal for a processor that is not allowed to clock faster than 8 MHz.

Q:2(a)
The code for both parts (a) and (b) can be found in the file *problem2.py* .

The original RSA primes are:

325843554290020688201140665925279443845543708457401927485109924627784654953338420651652755799293368558913688560151104594069623331272673870069396369848831

334301469993257483448640006272494244628292108904890367254969323741154383389865979911754311360062336498272475163394624599058002339277406938434646725893827813 9

Q:2(b)
The original RSA primes are:

480376430686880466877320770765933070656629585341766772849212382959994159673498647731509498600552023301592881989901931958911918608032201173680526001230091

284796482492763734499369296095528303278285596732115910788972545961232939572879374704491329977441164219390716314086379963609359046039013700472609406874343027 9