1. Consider a hash function SHU with the same architecture as SHA-0. However, SHU uses XOR (of five 32-bit words) in place of the ADD (add modulo $2^{32}$) operation and all 80 non-linear functions are MAJ, the majority function. SHU is similar to SHA-0 in all other respects.

   a. Tell how to find a collision in SHU if you can choose all 80 message blocks $W^{(i)}$ independently. Your solution should hash substantially fewer than $2^{80}$ messages.

   b. Tell how to find a collision in SHU if the message blocks $W^{(i)}$ are defined from the first sixteen blocks by the expansion formula of SHA-0. Your solution should hash substantially fewer than $2^{80}$ messages.

   Do not write any computer programs to solve parts a and b. If you feel the need to run a program, tell what the program would do, roughly how long it would run and what results you would expect from it.

2. The year is 2020. As the Chief Scientist of a large computer security company, you are implementing a new cryptosystem that uses 1000-digit primes as keys. The (dumb) algorithm chooses a random 1000-digit integer $R$ and then tests $R + 1, R + 2, \ldots$, for being prime until it finds the first prime number $R + k$ greater than $R$. What is the average (or expected) number of integers $R + i$ the algorithm tests for being prime?

3. Two problems about pseudoprimes.

   a. Show that if $n$ is a pseudoprime to base $a$ and a pseudoprime to base $b$, then $n$ is a pseudoprime to base $ab$.

   b. Find a composite number $n$ and two bases $a$ and $b$ so that $n$ is a strong pseudoprime to base $a$ and a strong pseudoprime to base $b$, but not to base $ab$.

4. Prove that if you are given a large odd composite integer $n$ and an integer $a$ so that $n$ is a pseudoprime to base $a$, but not a strong pseudoprime to base $a$, then you can factor $n$ in polynomial time.

5. A linear congruential generator $x_{i+1} = (ax_i + b) \mod m$ with $m = 65537$ (a prime) produces the three consecutive $x_i$ values 10413, 9953, 14267. Find $a$ and $b$. 