4.16. The minimum key length for the AES algorithm is 128 bit. Assume that a special-purpose hardware key-search machine can test one key in 10 ns on one processor. The processors can be parallelized. Assume further that one such processor costs $10, including overhead. (Note that both the processor speed and the prize are rather optimistic assumptions.) We assume also that Moore's Law holds, according to which processor performance doubles every 18 months.

How long do we have to wait until an AES key search machine can be built which breaks the algorithm on average in one week and which doesn't cost more than $1 million?

4.17. For the following, we assume AES with 192-bit key length. Furthermore, let us assume an ASIC which can check $3 \cdot 10^7$ keys per second.

1. If we use 100,000 such ICs in parallel, how long does an average key search take? Compare this period of time with the age of the universe (approx. 10^{10} years).
2. Assume Moore's Law will still be valid for the next few years, how many years do we have to wait until we can build a key search machine to perform an average key search of AES-192 in 24 hours? Again, assume that we use 100,000 ICs in parallel.