1. Exercise 3.9 from [KL].

2. Exercise 3.15 from [KL]. **Hint for (a)** Construct a pseudorandom generator $G$ such that $G(k) = G(k + 1)$ for every even $k$.

3. Consider a variant of CBC-mode encryption, where the sender uses $IV = 1$ the first time, $IV = 2$ the next time, $IV = 3$ the third time, etc. Show that this variant is *not* CPA-secure. Search the web for “BEAST SSL attack” to read about recent consequences of this problem.

4. Exercise 3.21 from [KL].