

Homework 4

Answers to questions 1–4 are due at the *beginning* of class on Oct. 7
The programming assignment is due at the beginning of class on Oct. 14

All numbered exercises refer to the second edition of the book.

1. Let $G : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$ be a pseudorandom generator. Define the keyed function $F : \{0, 1\}^{2n} \times \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$ as $F_k(x) = G(x) \oplus k$. Prove that F is not a pseudorandom function by describing and analyzing a concrete distinguisher D .
2. Exercise 3.20. You should describe and analyze a concrete attacker.
3. Exercise 3.28.
4. Exercise 4.7.
5. Implement the padding-oracle attack discussed in class. The necessary files are available online. Please turn in any code you write, plus the plaintext that was encrypted to give the challenge ciphertext.