

- [1] 1. What is the complexity class P?
- [2] 2. In Penney's game, which player has the advantage, and what is the best strategy?
- [1] 3. How many different reasonable encoding formulas are there for a Caesar cipher as defined in class?
- [3] 4. A message was encrypted using the one-time pad **TEAM**. The encoded message is **NJLR**. What was the original message?
- [1] 5. What is XOR? Compute  $1101 \oplus 1001$ .
- [4] 6. You have receive the encoded message **CXFCWD**. Though you don't know the one-time pad, you realize that if it was **NJZTEY**, then you get an original message that makes sense. What is that message, and can you assume that you guessed the correct one-time pad?
- [2] 7. Name one advantage and disadvantage of the one-time pad over the Affine cipher.
- [1] 8. What does it mean for a problem to be NP-complete?