Please submit two copies of your paper to Canvas, one with name, and the other anonymous. Your anonymous paper will be used in the writing workshop #2.

1 (50 points) Let $E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a good PRF. Break the PRF security of $F_K(X) = E_K(X) \parallel E_K(E_K(X))$ using a few queries and analyze the advantage of your attack.

2 (50 points) Figure 2.1 below illustrates another way to do ciphertext stealing on CBC with a blockcipher $E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$. This variant CBC-S appears in textbooks but is actually insecure. Break the real-or-random security of CBC-S using a few queries and analyze the advantage of your attack.

3 (50 points) CBC-Chain is a stateful blockcipher-based mode of operation that was actually used in SSH. To encrypt, we use CBC with an IV that is the last ciphertext block produced from the prior encryption. Initially, the IV is a random string. Give an attack that breaks the left-or-right security of CBC-Chain[$E$] using a few queries, and analyze its advantage.