1. CINTA, Exercise 11.12.
2. CINTA, Exercise 11.13.
3. CINTA, Exercise 11.16.
4. CINTA, Exercise 11.17.
5. CINTA, Exercise 11.18.
6. This problem and the next consider generalizations of the notion of secure (symmetric key) encryption. Recall that in class, the basic notion of security was defined by a game in which the adversary submits two messages $m_0$ and $m_1$ to an “encryption oracle,” who responds with an encryption of either $m_0$ or $m_1$. The adversary’s job is to figure out which of the two messages is encrypted (as formally defined in terms of either distinguishing or guessing advantage).

Define a multi-message attack as follows.

- A key $k$ is chosen randomly from the key space, and a bit $b \in \{0, 1\}$ is chosen at random.
- The adversary submits a sequence of queries to an encryption oracle. The $i$th such query is of the form $(m_{ib}, m_{i1})$, and the encryption oracle gives the adversary the encryption of $m_{ib}$ under $k$.

Note that the encryption oracle uses the same values of $b$ and $k$ consistently throughout the attack. Also note that the adversary’s queries may depend in an arbitrary way on previous responses from the encryption oracle.

- The adversary outputs $\hat{b} \in \{0, 1\}$.

As usual, the adversary’s guessing advantage is defined as $|\Pr[b = \hat{b}] - 1/2|$, and security against multi-message attacks means that this advantage is negligible for all efficient adversaries.

Your task is to show that security against single message attacks does not imply security against multi-message attacks. For this purpose, assume the existence of an encryption scheme secure against single message attacks.

7. We now consider a different extension of the basic notion of security.

Define a multi-key attack as follows.

- A key bit $b \in \{0, 1\}$ is chosen at random.
- The adversary submits a sequence of queries to an encryption oracle. The $i$th such query is of the form $(m_{ib}, m_{i1})$. The encryption oracle responds to this query by choosing a key $k_i$ at random from the key space, and giving the adversary the encryption of $m_{ib}$ under $k_i$.

Note that while the encryption oracle uses the same value of $b$ for each query, it generates a fresh key for each query. As above, the adversary’s queries may depend in an arbitrary way on the previous responses from the encryption oracle.

- The adversary outputs $\hat{b} \in \{0, 1\}$.

Again, the adversary’s guessing advantage is defined as $|\Pr[b = \hat{b}] - 1/2|$, and security against multi-key attacks means that this advantage is negligible for all efficient adversaries.

Your task is to show that security against single message attacks does imply security against multi-key attacks.