1. Is the following notion of privacy achievable by a stateless, probabilistic encryption scheme? Scheme
\(\Pi = (K, E, D)\) is perfectly private against an adversary that asks two queries if for all distributions on
plaintexts \(\mathcal{M}\) and all \(m_1, m_2 \in \mathcal{M}\) and all \(c_1, c_2 \in \mathcal{C}\),
\[
\Pr[M_1 = m_1 \land M_2 = m_2 \mid C_1 = c_1 \land C_2 = c_2] = \Pr[M_1 = m_1 \land M_2 = m_2]
\]
where \(M_1\) and \(M_2\) are sampled independently from \(\mathcal{M}\) and \(C_1\) and \(C_2\) are obtained by encrypting
them. (Assume that \(c_1, c_2\) are restricted such that \(\Pr[C_1 = c_1 \land C_2 = c_2] > 0\).)

2. Secrecy from a random shuffle. Alice shuffles a deck of cards and deals it out to herself and Bob
so that each gets half of the 52 cards. Alice now wishes to send a secret message \(M\) to Bob by saying
something aloud. Eavesdropper Eve is listening in: she hears everything Alice says (but Eve can’t see
the cards).

**Part A.** Suppose Alice’s message \(M\) is a string of 48-bits. Describe how Alice can communicate \(M\) to
Bob in such a way that Eve will have no information about what is \(M\).

**Part B.** Now suppose Alice’s message \(M\) is 49 bits. Prove that there exists no protocol that allows
Alice to communicate \(M\) to Bob in such a way that Eve will have no information about \(M\).
(What does it mean that Eve learns nothing about \(M\)? That for all strings \(\kappa\), the probability that
Alice says \(\kappa\) is independent of \(M\): for all messages \(M_0, M_1\) we have that \(\Pr[\text{Alice says } \kappa \mid M = M_0] = \Pr[\text{Alice says } \kappa \mid M = M_1]\). The probability is over the the random shuffle of the cards.)

3. In class we informally defined the bit-commitment problem. Design a plausible bit-commitment scheme
using a blockcipher that has \(n\)-bit keys and \(n\)-bit blocks, say AES-128.