1.1 Variant of the IND-CPA Bit-Guessing Problem

Goal: We explore that there is not just one way to formalize the idea behind IND-CPA security.

Let \( J^{\text{sym-ind-cpa}}_S; B \) be the bit-guessing problem from Definition 3.2 in the lecture notes (labeled \( J^{\text{sym-ind-cpa}}_S; B \) there). We define a new bit-guessing problem \( J^{\text{rrc}}_S; B \), where rrc stands for real-or-random challenge, by replacing step 3 of the description by the following.

3. \( S \) obtains one challenge message \( m \) and makes the following case distinction:
   - If \( B = 0 \), it computes the encryption of \( m \), i.e., \( c = E(m, k) \) for fresh and independent randomness, and returns \( c \).
   - If \( B = 1 \), it chooses a uniformly random message \( \tilde{m} \) of length \( |m| \) and computes the encryption of \( \tilde{m} \), i.e., \( \tilde{c} = E(\tilde{m}, k) \) for fresh and independent randomness, and returns \( \tilde{c} \).

Argue that the new problem captures the IND-CPA security notion equally good by proving the following two statements.

- a) Given a distinguisher \( D \) for \( J^{\text{rrc}}_S; B \), design a new distinguisher \( D' \) (which internally uses \( D \)) for \( J^{\text{ind}}_S; B \) so that \( \Lambda_D( J^{\text{rrc}}_S; B ) = \Lambda_{D'}( J^{\text{ind}}_S; B ) \).

- b) Given a distinguisher \( D \) for \( J^{\text{ind}}_S; B \), design a new distinguisher \( D' \) (which internally uses \( D \)) for \( J^{\text{rrc}}_S; B \) so that \( \Lambda_D( J^{\text{ind}}_S; B ) = 2 \cdot \Lambda_{D'}( J^{\text{rrc}}_S; B ) \).

1.2 On the Security of the One-Time Pad

Goal: We prove the security of the one time pad in general for finite groups.

Let \( \langle G; + \rangle \) be a finite group (written in additive notation) and \( U, X \) two independent random variables over \( G \), with \( U \) uniformly distributed. Show that \( U + X \) and \( X \) are independent.

Hint: As an intermediate step, you should show that since \( U \) is uniformly distributed, then so is \( U + X \).

1.3 Properties of the Distinguishing Advantage

Goal: We prove some basic results about the distinguishing advantage that are stated in the lecture notes without proof.

- a) Prove Lemma 2.1 in the lecture notes, i.e., show that for two random variables \( X \) and \( Y \), the advantage of the best distinguisher for \( X \) and \( Y \) is the statistical distance between \( X \) and \( Y \), that is,

\[
\Delta(X, Y) = \delta(X, Y).
\]

- b) Prove Lemma 2.4 from the lecture notes, i.e., for a bit-guessing problem \( [S; B] \), show that from a distinguisher \( D \) which is given either the pair \( [S, B] \) or the pair \( [S, U] \) for \( U \) uniformly distributed and independent of \( S \) (that is, \( D \) can interact with the system \( S \) and receives either the bit \( B \), correlated with \( S \), or the uncorrelated bit \( U \)), we can
construct a distinguisher $D'$ for the bit-guessing problem $[S;B]$ which has twice the same advantage, that is,

$$\Delta^D([S,B],[S,U]) = \frac{1}{2} \cdot \Lambda^{D'}([S;B]).$$

*Hint:* First show that $\Lambda^{D'}([S;B]) = \Delta^D([S,B],[S,\overline{B}])$, where $D'$ should make use of $D$ and a uniform bit $U$, and then show that $\Delta^D([S,B],[S,U]) = \frac{1}{2} \cdot \Delta^D([S,B],[S,\overline{B}])$ ($\overline{B}$ is the negation of the bit $B$).