Ex 2.
1. $L \in \text{BPP} \implies$ polynomial decider $D = \text{Verifier}$ on check $x \in \text{BPP}$ itself
2. decide $x \in L$ via $D$ defined as follows
   - let $(s, r) \leftarrow \mathcal{S}(x)$, sample random $a$, output $b = \text{Verifier}(TT, b)$
   - claim: $x \notin L$, then $\Pr[DC(x) = 1] \leq \frac{2}{3}$
   - as honest proofs verify due to completeness w.h.p., and $\Pi$ is ind. from honest proof
   - claim: if $x \in L$, then $\Pr[DC(x) = 1] \leq \frac{1}{4}$
   - as otherwise the prover $P$ that outputs simulated proofs can break soundness
3. ROM is not captured by the setting we consider
4. verify deterministic $\implies$ prover can collapse rounds into a $\mathcal{N}2^k \times y$, ex. 2

Ex 3.
1. Alice
   - let $a, r$

   \begin{align*}
   a \leftarrow g, a
   c \leftarrow C(x)
   \end{align*}

   open:
   - $a, b \leftarrow \text{check } C(s) \oplus b \cdot r = 1$

   hiding: $b$ hides $b \cdot r$

   binding: Alice needs to output $c, c', s$ s.t.
   \begin{align*}
   C(s) &= a \quad \text{and } C(c') = c \oplus r
   \end{align*}

   \begin{align*}
   c \oplus C(s') &= r \in 2k, a
   \end{align*}

   then on $2^m$ pairs $(s, s')$ but $2^m$ choices for $r$

   \begin{align*}
   \Pr[(3, s, c, s \oplus r)] &\leq 2^m
   \end{align*}

2. $\text{pp} \equiv \text{Shap}(a)$ is the function description
   - $Fpp(b, r) = \text{Comp}(b, r)$
   - assume $\exists A$ that breaks OWF property
   - sample $b \leftarrow \mathcal{U}(k)$, $r$
   - set $c = \text{Comp}(b, r)$
   - let $(b', r') \leftarrow A(c)$
     \begin{itemize}
     \item if $b = b'$ can use to break binding
     \item if $b \neq b'$ can use to break hiding
     \end{itemize}

Note: ex. 1 is from an old exam, so it is a good exercise for the preparation (without solutions).