1. Prove or diprove: an encryption scheme is Perfectly Secret - PS $\leftrightarrow$ $\forall$distributions M over $\mathcal{M}$, $\forall c_0, c_1 \in \mathcal{C}$ (ciphers):
$$Pr[C = c_0] = Pr[C = c_1] \;\; C = Enc(K, M)$$

2. Alternatve definition to PS: prove that the following definition is equivalent to other definitions of PS.
$GAME^{IND}_{\Pi,A}(\lambda)$:
    1. C samples $k \leftarrow\$ \mathcal{K}$
    2. C samples $b \leftarrow\$ \{0,1\}$
    3. A sends to C messages m_0, m_1
    4. C calculates $c = Enc(k, m_b)$ and sends it to A
    5. A sends back b'

   A wins (i.e. output 1) if $b' = b$.

   $\forall A \; Pr[GAME^{IND}_{\Pi,A}(\lambda) = 1] = \frac{1}{2}$

3. One-way NP puzzle fo relation R
$Gen(1^\lambda)$: $(y, x) \leftarrow\$ Gen(1^\lambda)$ s.t. $R(y, x) = 1$.
y is a puzzle and x a solution for y.

   It is OW because $\forall A \; Pr[R(y, x') = 1 | (y, x) \leftarrow\$ Gen(1^\lambda), x' \leftarrow\$ A(y)] \leq negl(\lambda)$

   Prove that OWFs are equivalent to OW-NP Puzzle

4. Every PRF is a MAC. Show that there is a MAC which is not a PRF.

5. Let $H : \{0,1\}^{2\lambda} \to \{0,1\}^\lambda$ be a RO (i.e. a PRF in ROM). Prove $F(k, r) = H(k \| r)$.

   Need to show $\forall A$, $R \leftarrow\$ \mathcal{R}_{\lambda,\lambda}$, $H \leftarrow\$ \mathcal{R}_{2\lambda,\lambda}$.
$|Pr[A^{H(k,\cdot),H(\cdot)}(1^\lambda) = 1] - Pr[A^{R(\cdot),H(\cdot)}(1^\lambda) = 1]| \leq negl(\lambda)$

Not sure what F is, maybe the F found as a solution (see the notebook) for the previous exercise

6. Let f be a length preserving OWF with hardcore predicate h.
Show that $G(x) = f(x) \| h(x)$ is not a PRG.

7. Let $\mathbb{G}$ be a group of order q, with generator g.

   Square DH:
Let $params = (\mathbb{G}, g, q) \leftarrow\$ GroupGen(1^\lambda)$
$$Pr[y = g^{a^2} | a \leftarrow\$ \mathbb{Z}_q, y \leftarrow\$ A(params, g^a)] \leq negl(\lambda)$$

   Prove CDH $\leftarrow$ Square DH. May assume it's possible to compute square roots in $\mathbb{G}$.

8. Variant for unforgeability: Random UnForgeability under Random Message Attack - RUF-RMA
    1. C samples keys $(p_k, s_k) \leftarrow\$ KGen(1^\lambda)$
    2. C sends pk to A and sends back (m, σ), where $m \leftarrow\$ \mathcal{M}, \sigma)Sign(sk, m)$ (can repeat poly-times) $\boxed{\text{How can A send C's } sk\text{?}}$
    3. C sends to A message $m^* \leftarrow\$ \mathcal{M}$
    4. A sends back σ^*

    Output 1 is $Verify(pk, m^*, \sigma^*) = 1$

    (a) Prove/Disprove: UF-CMA $\rightarrow$ RUF-RMA

    (b) Prove/Disprove: RUF-RMA $\rightarrow$ UF-CMA

    (c) Show textbook RSA satisfies RUF-RMA

9. Let $G = \mathbb{Z}_p^*$. DL is a OWF in $\mathbb{G}$.
    Show that $lsb(x)$ is NOT hard-core for f_{DL}, where $f_{DL}(x) = g^x\ mod\ p$