1. **Structure of** $\mathbb{Z}_n^*$. Euler’s theorem states that for all $x \in \mathbb{Z}_n^*$ it holds that $x^{\varphi(n)} = 1 \mod n$. Nevertheless $\varphi(n)$ is not necessarily the smallest number with this property. The Carmichael function is defined as $\lambda(n) = \min\{t | t \geq 1 \text{ and } \forall a \in \mathbb{Z}_n^* : a^t \equiv 1 \mod n\}$. The Carmichael function has a complex relationship to the Euler function: using the definitions above prove the following:

$$
\lambda(n) =
\begin{cases}
\varphi(n) & n = 2^a, a \leq 2 \\
\frac{3}{2}\varphi(n) & n = 2^a, a \geq 3 \\
\varphi(n) & n = p^a, p \geq 3, p \in \text{PRIME} \\
\lcm_{i=1,...,k}\{\lambda(p_i^{a_i})\} & n = \prod_{i=1}^{k} p_i^{a_i}, p_i \in \text{PRIME}
\end{cases}
$$

The case $n = 2^a$ for $a \geq 3$ is extra credit.

2. **Commitment Schemes in the Random Oracle model.** A (non-interactive) commitment scheme $\langle \text{Commit}, \text{Verify} \rangle$ is a cryptographic primitive that satisfies the following properties: (i) correctness: for all $m \in \{0, 1\}^*$ $(c, \sigma) \leftarrow \text{Commit}(m)$ then $\text{Verify}(c, \sigma, m) = 1$, (ii) binding: it is hard to find $(c, \sigma_1, m_1, \sigma_2, m_2)$ such that $\text{Verify}(c, \sigma_1, m_1) = \text{Verify}(c, \sigma_2, m_2) = 1$ and $m_1 \neq m_2$, (iii) statistical hiding: for any $m_1, m_2$ the random variables $\text{Commit}(m_1)$ and $\text{Commit}(m_2)$ are statistically indistinguishable.

Design a commitment scheme in the random oracle model that satisfies the above three properties; give a separate proof for each property and state explicitly the assumptions that are involved in the proof (if any).

3. **Key Extraction in the DH Key-Exchange.** In class we showed that under the DDH assumption it holds that the Diffie Hellman Key Exchange satisfies “security against passive eavesdroppers”:

$$\forall A \forall V : \Pr[A(\tau) = V(\text{key}(\tau))] = \max\{\gamma, 1 - \gamma\} + \text{negl}(\lambda) \quad \tau \leftarrow \text{transcript}(1^\lambda)$$

where

$$\gamma = \Pr[V(\kappa) = 1] \quad \kappa \leftarrow \text{KEY}(1^\lambda)$$

Suppose now that after the termination of the protocol Alice and Bob want to extract a number of bits from the key they constructed (the value $g^{xy}$) and use them as e.g., a key for a
symmetric cipher. Extracting a bit from the key $g^{xy}$ is applying a function $V$ to $g^{xy}$ whose
$\gamma$-value is very close to $50\%$.

Suppose that $p = 2q + 1$ and $g$ is a generator of $QR(p)$ the subgroup of quadratic residues in
$\mathbb{Z}_p^*$. Now as an example, consider the transformation $H^{-1} : QR(p) \rightarrow \{1, \ldots, q - 1\}$ to $g^{xy}$
that is defined as follows:

$$H^{-1}(y) = \begin{cases} 
z - 1 & \text{if } z = y^{p+1} \text{ mod } p \in \{1, \ldots, q\} \\
2q - z & \text{otherwise}
\end{cases}$$

You can define all $V_1, \ldots, V_\nu$ in terms of $H^{-1}(\cdot)$. For example, $V_1(c) = \text{LBIT}_2(H^{-1}(c))$
is a possibility for you to investigate (note that $\text{LBIT}_2(\cdot)$ is a function that given an integer
returns its second least significant bit). You should define a sequence of bits $V_1, \ldots, V_\nu$ so
that the extracted bits are statistical indistinguishable from random strings in $\{0, 1\}^\nu$; Note
that you should maximize the value $\nu$. (extra credit: do not use $H^{-1}(\cdot)$ when defining $V_i$).