Exercise 1.

**Definition 1** (Decisional Diffie-Hellman distribution). Let $G$ be a cyclic group of prime order $q$, and let $g$ be a publicly known generator of $G$. The decisional Diffie-Hellman distribution (DDH) is, $D_{DDH} = (g^a, g^b, g^{ab}) \in G^3$ with $a, b$ sampled independently and uniformly at random in $\mathbb{Z}_q$.

**Definition 2** (Decisional Diffie-Hellman assumption). The decisional Diffie-Hellman assumption states that there exists no probabilistic polynomial-time distinguisher between $D_{DDH}$ and $(g^a, g^b, g^c)$ with $a, b, c$ sampled independently and uniformly at random in $\mathbb{Z}_q$.

1. Does the DDH assumption hold in $G = (\mathbb{Z}_p, +)$ for $p = O(2^4)$ prime?
2. Same question for $G = (\mathbb{Z}_p^*, \times)$ of order $p - 1$.
3. Now we take $Z_p$ such that $p = 2q + 1$ with $q$ prime (also called a safe-prime). Let us work in a subgroup $G$ of order $q$ in $(\mathbb{Z}_p^*, \times)$.

(a) Given a generator $g$ of $G$, propose a construction for a function $\hat{G} : Z_q \to G \times G$ (which may depend on public parameters) such that $\hat{G}(U(Z_q))$ is computationally indistinguishable from $U(G \times G)$ based on the DDH assumption on $G$ (where, in $\hat{G}(U(Z_q))$, the probability is also taken over the public parameters of $G$).

(b) What is the size of the output of $\hat{G}$ given the size of its input?

(c) Why is it not a pseudo-random generator from $\{0, 1\}^\ell$ to $\{0, 1\}^{2\ell}$ for $\ell = \lceil \lg q \rceil$?

Exercise 2.

**Definition 3** (Learning with Errors). Let $\ell < k \in \mathbb{N}$, $n < m \in \mathbb{N}$, $q = 2^k$, $B = 2^\ell$, $A \leftarrow U(\mathbb{Z}_q^{m \times n})$. The Learning with Errors (LWE) distribution is defined as follows: $D_{\text{LWE}, A} = (A, A \cdot s + e \mod q)$ for $s \leftarrow U(\mathbb{Z}_q^m)$ and $e \leftarrow U \left( \left[ -\frac{B}{2}, \frac{B}{2} - 1 \right] [\mathbb{Z}_m^m] \right)$.

Note. In this setting, the vector $s$ is called the secret, and $e$ the noise.

The LWE assumption states that, given suitable parameters $k, \ell, m, n$, it is computationally hard to distinguish $D_{\text{LWE}, A}$ from the distribution $(A, U(\mathbb{Z}_q^m))$.

Let us propose the following generator: $G_A(s, e) = A \cdot s + e \mod q$.

1. Given the binary representation of $s, e$, compute the bitsize of the input and the output of the function $G$ with respect to $k, \ell, m, n$.
2. Evaluate the cost of a brute-force attack to retrieve the input $s, e$ in terms of arithmetic operations in $\mathbb{Z}_q$.
3. What happens if $B = 0$? $\Rightarrow$ This bound can prove useful: $\prod_{i=1}^n (1 - 2^{-i}) > 0.288$.
4. Given the previous question, refine the brute-force attack of question 2. What does it mean for the security of the generator $G$?
5. What happens if $\ell = k$?
6. Given suitable $\ell, k, n, m$ such that the LWE problem holds in this setting, show that $G_A$ is a pseudo-random generator.
Exercise 3. One-time pad is semantically secure.
Let us recall the one-time pad scheme to encrypt a message \( m \in \{0, 1\}^\ell \) for \( \ell \in \mathbb{N} \).

**Keygen**\((1^k)\): Outputs \( k \leftarrow U(\{0, 1\}^\ell) \)

**Enc\(_A\)(m)**: Outputs \( c = m \oplus k \)

**Dec\(_A\)(c)**: Outputs \( m' = c \oplus k \)

1. Recall the definition of semantic security for a symmetric encryption scheme (for one-time key and chosen plaintext attack).
2. Prove that one-time pad is semantically secure.

Exercise 4. \textit{Sub-bits of a Generator.}
Let \( G : \{0, 1\}^s \rightarrow \{0, 1\}^n \) be a pseudo-random generator, \( S \subseteq [1, n] \cap \mathbb{Z} \) of size \( \ell \). Let us define the function \( G' : \{0, 1\}^s \rightarrow \{0, 1\}^\ell \) as \( x \rightarrow G(x)_S = \|_{i \in S} G(x)_i \), where \( \| \) denotes the concatenation.

1. Given that \( G \) is secure, prove that the distribution defined by the output of \( G' \) on \( x \leftarrow U(\{0, 1\}^s) \) is indistinguishable from the uniform distribution over \( \{0, 1\}^\ell \).

Exercise 5. \textit{Increasing the expansion factor of a PRG.}
We recall that the advantage \( \text{Adv}^{PRG}_A[G] \) of an algorithm \( A \) against a PRG (pseudo-random generator) \( G : \{0, 1\}^n \rightarrow \{0, 1\}^m \) is the difference of the probabilities that \( A \) returns 1 when it is given \( G(x) \in \{0, 1\}^m \) for \( x \) uniformly sampled in \( \{0, 1\}^n \), and when it is given \( u \) uniformly sampled in \( \{0, 1\}^m \). We say that \( G \) is a secure PRG if, for any probabilistic polynomial-time \( A \), the advantage of \( A \) is negligible in \( n \), i.e., \( \text{Adv}^{PRG}_A[G] \leq n^{-\omega(1)} \).

We assume that we have a pseudo-random generator \( G : \{0, 1\}^n \rightarrow \{0, 1\}^{n+1} \).

1. Consider \( G' : \{0, 1\}^n \rightarrow \{0, 1\}^{n+2} \) defined as follows. On input \( x \in \{0, 1\}^n \), \( G' \) first evaluates \( G(x) \) and obtains \( (x', y') \in \{0, 1\}^n \times \{0, 1\} \) such that \( G(x) = x' \parallel y' \). It then evaluates \( G \) on \( x' \) and eventually returns \( G(x') \parallel y' \). Show that if \( G \) is a secure PRG, then so is \( G' \).

An arbitrary-length PRG is a function \( G \) taking as inputs \( x \in \{0, 1\}^n \) and \( \ell \geq 1 \) in unary, and returning an element of \( \{0, 1\}^\ell \). It is said to be secure if for all \( \ell \) polynomially bounded with respect to \( n \), the distributions \( G(U(\{0, 1\}^n), 1^\ell) \) and \( U(\{0, 1\}^\ell) \) are computationally indistinguishable.

2. Let \( n \geq 1 \). Propose a construction of an arbitrary-length PRG \( G^* \) based on \( G \). Show that if \( G \) is a secure PRG, then so is \( G^* \).

Exercise 6. \textit{Increasing the advantage of an attacker.}
Let \( G \) be a pseudo-random generator from \( \{0, 1\}^s \) to \( \{0, 1\}^n \) for some integers \( s \) and \( n \). Let \( i \in \{1, \cdots, n\} \) and let \( A \) be a PPT algorithm such that, for all \( k \in \{0, 1\}^s \), we have

\[
\Pr[A(G(k)_{1\cdots i-1}) = G(k)_i] \geq \frac{1}{2} + \varepsilon,
\]

where the probability runs over the randomness of \( A \). Note that unlike the definition of the advantage seen in class, here we consider only the probability over the randomness of \( A \) and not over the random choice of \( k \) (we will see why later).

Our objective is to construct a new attacker \( A' \) with an advantage arbitrarily close to 1 (for instance \( \Pr[A(G(k)_{1\cdots i-1}) = G(k)_i] \geq 0.999 \) for all \( k \in \{0, 1\}^s \)).
1. Propose a method to improve the success probability of $A$.
   Let $m$ be some integer to be determined. Let $A'$ be an algorithm that evaluates $A$ on $G(k)_{1\ldots i-1}$ $2m+1$ times, to obtain $2m+1$ bits $b_1, \ldots, b_{2m+1}$ and then outputs the bit that appeared the most (i.e. at least $m+1$ times).

2. Give a lower bound on $\Pr[A'(G(k)_{1\ldots i-1}) = G(k)_i]$, for all $k \in \{0,1\}^s$. We recall Hoeffding’s inequality for Bernoulli variables: let $X_1, \ldots, X_{2m+1}$ be independent Bernoulli random variables, with $\Pr(X_i = 1) = 1 - \Pr(X_i = 0) = p$ for all $i$, and let $S = X_1 + \cdots + X_{2m+1}$. Then, for all $x > 0$, we have
   \[
   \Pr[|S - E(S)| \geq x\sqrt{2m+1}] \leq 2e^{-2x^2}.
   \]

3. What should be the value of $m$ (depending on $\varepsilon$) if we want that $\Pr[A'(G(k)_{1\ldots i-1}) = G(k)_i] \geq 0.999$ for all $k$? It may be useful to know that $e^{-8} \leq 0.0005$.

4. Do we have $\text{Adv}_{\text{unpredictability}}(A') \geq 0.999$ if $\Pr[A'(G(k)_{1\ldots i-1}) = G(k)_i] \geq 0.999$ for all $k$?

5. What condition on $\varepsilon$ do we need to ensure that $A'$ runs in polynomial time?
   Let now $A$ be an attacker such that
   \[
   \text{Adv}(A) = \Pr_{k \leftarrow U(\{0,1\}^s)}[A(G(k)_{1\ldots i-1}) = G(k)_i] \geq \frac{1}{2} + \varepsilon.
   \]
   Note that we are now looking at the definition of advantage given in class, where the probability also depends on the uniform choice of $k$. We want to show that in this case, we cannot always amplify the success probability of the attacker by repeating the computation.
   In the following, we write $\Pr[A(G(k)_{1\ldots i-1}) = G(k)_i]$ when we only consider the probability over the internal randomness of $A$ (and $k$ is fixed) and $\Pr_{k \leftarrow U(\{0,1\}^s)}[A(G(k)_{1\ldots i-1}) = G(k)_i]$ when we consider the probability over the choice of $k$ and the internal randomness of $A$.
   Suppose that $s \geq 2$ and define
   \[
   G(k) = \begin{cases} 
00 \cdots 0 & \text{if } k_0 = k_1 = 0 \\
G_0(k) & \text{otherwise},
\end{cases}
   \]
   where $G_0$ is a secure PRG from $\{0,1\}^s$ to $\{0,1\}^n$.

6. Show that there exists a PPT attacker $A$ with non negligible advantage (for the unpredictability definition) against $G$.

7. Show on the contrary that there is no PPT attacker $A$ with $\text{Adv}(A) \geq 7/8$ (assuming that $G_0$ is a secure PRG).