Problem 1

In this question you will investigate the hardness of the distributional Diffie-Hellman problem in cyclic groups. Assume $p$ and $(p - 1)/2$ are both prime numbers. Recall that $\mathbb{Z}_p^*$ is the group \{1, \ldots, p - 1\} under multiplication modulo $p$ and $Q_p = \{y^2 : y \in \mathbb{Z}_p^*\}$.

(a) Choose a generator $h$ of $\mathbb{Z}_7^*$. Calculate the distributions $h^{xy}$ where $x, y$ are chosen uniformly and independently from \{1, \ldots, 6\} and $h^z$ where $z$ is chosen uniformly from \{1, \ldots, 6\}.

(b) Repeat part (a) for $Q_7$ instead of $\mathbb{Z}_7^*$.

(c) Let $h$ be a generator of $\mathbb{Z}_p^*$. Show that there exists a circuit $A$ of size polynomial in the number of bits of $p$ (i.e. $\log p$) such that

\[
\Pr_{x,y \sim \{1, \ldots, p-1\}}[A(h^{xy}) = 1] - \Pr_{z \sim \{1, \ldots, p-1\}}[A(h^z) = 1] \geq \varepsilon
\]

for some constant $\varepsilon > 0$. You may assume that adding, multiplying, and powering numbers modulo $p$ can be done by circuits of size polynomial in the number of bits of $p$.

(d) Is part (c) true if we replace $\mathbb{Z}_p^*$ by $Q_p$?

Problem 2

Prove Theorem 4 from Lecture 10. You do not need to match the exact parameters as long as the loss of security is polynomial.