Week 2 / Exercise 2

a) Prove $P \rightarrow Q$

P: DDH holds
Q: CDH holds

DDH

$x, y, z \leftarrow \$ \mathbb{Z}(\lambda)$ $b \leftarrow \$ \{0,1\}$

$X = g^x$, $Y = g^y$, $Z_0 = g^z$, $Z_1 = g^{x \cdot y}$

$\hat{b} \leftarrow A(\lambda, X, Y, Z_b)$
return $\hat{b} = b$

Attacker needs to guess whether they have been given the real $g^{x \cdot y}$ or a random g^z (by identifying $b = 0$ or 1).

CDH

$x, y \leftarrow \$ \mathbb{Z}(\lambda)$

$X = g^x$, $Y = g^x$, $Z = g^{x \cdot y}$

$\hat{Z} \leftarrow A(\lambda, X, Y)$
return $\hat{Z} = Z$

Attacker needs to be able to compute the $g^{x \cdot y}$ given both public keys.

By reduction, aim to prove $\neg Q \rightarrow \neg P$

ie: CDH doesn't hold → DDH doesn't

Assume that we have a CDH solver:
$f(X, Y) \rightarrow g^{xy}$

We are now given our DDH problem: X, Y, Z_b and we need to determine whether $Z_b = g^{xy}$ or a random value.

We use our CDH solver:
$f(X, Y) = g^{x \cdot y}$

Now compare Z to g^{xy}
- Equal: it's the product pair
- Not equal: it's a random group element

We have proven $\neg Q \rightarrow \neg P <= P \rightarrow Q$!

b) Prove $P \rightarrow Q$

P: CDH holds
Q: DL holds

We'll prove by reduction $\neg Q \rightarrow \neg P$.
Assume we have a DL solver:
$f(g^x) \rightarrow x$.

Take our CDH problem:
- Given X, Y
- Calculate $g^{x \cdot y}$

Invoke our solver twice:
$f(X) = x$
$f(Y) = y$

Efficiently calculate $g^{x \cdot y}$ using successive squares.

(Or even, just take $f(x) = x$, $Y^x = g^{xy}$)

We have proven $\neg Q \rightarrow \neg P <-> P \rightarrow Q$!

We don't actually need the facts listed in the exercise!