Assignment 4 Q3

watIAM: sh2yap
student ID: 21111395

(a) show:

if DDH is hard → the CDH problem must also be hard.

proof by contrapositive

suppose the CDH problem is not hard, and
∃ algorithm A that successfully solves CDH
problem.

means we are able to compute g^{ab} given g^a
and g^b

then since we know what g^{ab} is, we can
distinguish between g^{ab} and g^c for some
random c

∴ if we have

Algorithm B (g^a, g^b, g_{given})
g^{ab} = Algorithm A (g^a, g^b)

if $(g^{ab} == g_{given})$
then is g^{ab}
else
g_{given} is g^c

and Algorithm B solves DDH problem
⇒ DDH not hard
(# proven by contrapositive)

Q3 b) Show:

CDH problem is hard → DLOG must also be hard.

$\boxed{\text{Proof by contrapositive}}$

Suppose ∃ algorithm A that solves the DLOG problem, that is, given g^a, we can compute a.

Then we can form an algorithm B s.t.

Algorithm B(g^a, g^b) :

a = Algorithm A(g^a)
b = Algorithm A(g^b)
$ab = a * b$
return g^{ab} // Note that, we know what g is.

⇒ we can solve CDH problem ⇒ CDH is not hard

(# proven by contrapositive)

Assignment 4 Q3

c)

1) Compute a square modulo x

$$\gamma^2 \bmod p = x,$$

where $\gamma \in_R \mathbb{Z}$, p is the given prime

2) if g^a is a square modulo, then xg^a is a square modulo

similarly for g^b

so:

α	$O(\alpha) == \text{TRUE}$	$O(\alpha) == \text{FALSE}$
xg^a	g^a is square	g^a is not square
xg^b	g^b is square	g^b is not square

3) g^a is square, then $(g^a)^b$ is necessarily square] $\therefore$ g^{2i} for some i, $2i = a$ and taking $\sqrt{g^{2i}} = g^{\frac{2i}{2}} = g^i$

similarly if g^b is square then $(g^b)^a$ is necessarily square.

so: we can summarise as:

g^a	g^b	g^{ab}
✗	✗	?
✗	✓	✓
✓	✗	✓
✓	✓	✓

✓ = square
✗ = non-square
? = don't know.

4) $\therefore$ if g_{given} is not square, but at least one of g^a, g^b is, then we can conclude that $g_{\text{given}} \neq g^{ab}$