Evaluation I.

The question has 3 parts:

i. Designing a zero knowledge proof (ZKP) for DLP

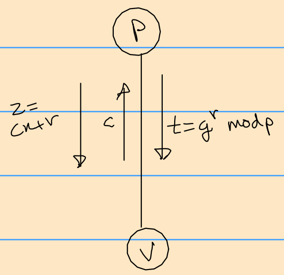
ii. Show how to build a digital signature scheme using DLP and hash functions

iii. Show how to design collision resistant hash functions based on the hardness of DLP.

i. ZKP for DLP

Assuming an interactive solution is allowed, we can design a ZKP as:

- Prover (P) and Verifier (V) agree on a group $\mathbb{Z}_p^*$ and generator g
- Prover proves knowledge of x ($y = g^x \bmod p$)



1. P picks $\boxed{r \in_R \mathbb{Z}_p^*}$, sends $\boxed{t = g^r \bmod p}$ to V
2. V sends to P a challenge $\boxed{c \in_R \mathbb{Z}_p^*}$
3. P sends to V $\boxed{z = cx + r}$
4. V checks that $\underline{g^z = y^c \cdot t}$. If it is true, accept/repeat. If false, reject.

Parameters:

Completeness: $g^z = g^{(cx+r)} = (g^x)^c \cdot g^r = y^c \cdot t$

$\Rightarrow$ if Prover knows x, Verifier will never reject.

Soundness: If prover does not know x, it has to guess.
But if P can guess r with $>$ negl(), it can guess x too (c and r are known), which means it can solve DLP with $>$negl() probability, which is contradiction.

zero-knowledge:
- Assuming hardness of DLP, V cannot get x from y, g, p.
- To get x from z, V needs r. but r is random, and V only knows $t = g^r \bmod p$. Due to DLP hardness, again V cannot get r.

2. Digital signature scheme based on ZKP above

This cannot be interactively done. We assume, by the Random Oracle Model, that outputs of hash functions are seemingly random.

Scheme:

Users agree on group $\mathbb{Z}_p^*$, generator g, hash function $H: \{0,1\}^* \to \mathbb{Z}_p^*$

GEN: private key $x \in \mathbb{Z}_p^*$

public key $y = g^x$

SIGN: $r \in_R \mathbb{Z}_p^*$

$t = g^r \bmod p$

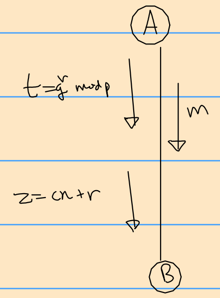
$c = H(t \| m)$ [m = message]

$z = cx + r$

Send: message (m) with signature (z, t)

VERIFY: get $c = H(t \| m)$

verify $\underline{y^c \cdot t = g^z}$



3. Collision Resistant Hash Functions using DLP

for group G of order p

generator g

Let $h \in_R G$

Then $s = \langle G, p, g, h \rangle$

Given def^n $H: \mathbb{Z}_p \times \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$,

$$\boxed{H^s(x_1, x_2) = g^{x_1} \cdot h^{x_2}}$$

Collision Resistance of H^s

Consider colliding inputs: x_1, x_2 and x_1', x_2'

Collision (Pr > negl) $\Rightarrow g^{x_1} \cdot h^{x_2} = g^{x_1'} \cdot h^{x_2'} \bmod p$

$\Rightarrow g^{(x_1 - x_1')} = h^{(x_2' - x_2)} \bmod p$

g is a generator $\Rightarrow h = g^t$

$\Rightarrow (x_1 - x_1') = t(x_2' - x_2) \bmod p-1$

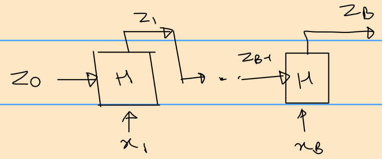
This can be solved to get t. But that would mean we have a solution to DLP $h = g^t \bmod p$, which is a contradiction

⇒ an adversary finding colliding inputs with non-negligible Pr is contradictory to hardness assumption of DLP.

For arbitrary H's : $\{0,1\}^* \to \mathbb{Z}_p$ we use Merkle-Damgard Transform.

Take $l = \log_2(p) + 1$

1. $B = \lceil \frac{L}{l-1} \rceil$. Pad x with 0 till $l-1 \mid$ length of x
2. set $z_0 = p-1$
3. For $i = 1 \ldots B$ compute $z_i = H(z_{i-1}, x_i)$, x_i is the ith block.
4. Return z_B



<u>Collision resistance of H's</u>

For x_1, x_2 to collide, output is z_B for both.

⇒ ∃ index i st $z_{i-1}, x_i \neq z'_{i-1}, x'_i$, but $z_i = z'_i$

- let i^* be the rightmost such index
- then we have distinct colliding inputs. But we know Pr. of this must be negligible.

⇒ Hardness of collision in H' = hardness of collision in H = DLP hardness.