Monsoon 2023 CS2361 A1

Bhumika Mittal

Collaborators: NONE

Question 1

username = bhumika.mittal_ug24@ashoka.edu.in
$x = 996$
concatenated string = bhumika.mittal_ug24@ashoka.edu.in996

Question 2

The order of 4 is 26

Question 3

All generators of $G = \mathbb{Z}_{13}^*$ are 2, 6, 7, 11

Question 4

Input: $((G = \mathbb{Z}_{17}^*, q = 8, p = 17), g = 2, h = 2)$
Output: $\alpha = 1$

Question 5

Given the dlog instance with the following parameters:

$$G = \mathbb{Z}_{17}^*, \quad q = 8, \quad p = 17, \quad g = 2, \quad h = 2, \quad \alpha = 1$$

KeyGen

- $\alpha = 1 \in \mathbb{Z}_8$
- $h = g^a \mod p = 2^1 \mod 17 = 2$
- pk = (p = 17,q = 8,g=2,h=2)
- sk = $\alpha = 1$

Sign

- $z = 7 \in \mathbb{Z}_{17}^*$

- $r = 1 \in \mathbb{Z}_8^*$
- $c_1 = (g^r \mod p) \mod q = 2^1 \mod 17 \mod 8 = 2$
- $c_2 = r^{-1}(z + ac_1) \mod q = 1^{-1}(7 + 1.2) \mod 8 = 9 \mod 8 = 1$
- Output signature: $\sigma = (c_1, c_2) = (2, 1)$

Verify

- $z = 7$
- $e_1 = zc_2^{-1} \mod q = 7 \mod 8 = 7$
- $e_2 = c_1c_2^{-1} \mod q = 2 \mod 8 = 2$
- $(g^{e_1}h^{e_2} \mod p) \mod q = 2^7 2^2 \mod 17 \mod 8 = 2 = c_1$
- **VERIFIED**

Question 6

The inverse of $g = 53 \in G = \mathbb{Z}_p^*$ where p= 16868678779879798798798797465465479 is:
14640740073103221598957446856819095

Question 7

$G = \mathbb{Z}_n^*$ such that $n = 793872007422642643069$.

Since the gcd of $a = 3478293847392$ and 793872007422642643069 is 1, $a \in \mathbb{Z}_n^*$. The inverse of $a = 258451230485580583150$

Since the gcd of $b = 70934603673$ and 793872007422642643069 is 23644867891, $b \notin \mathbb{Z}_n^*$.

Question 8

$G = \mathbb{Z}_p^*$ for some prime p and $g \in G$.

$o(g) = q < p - 1$ and $1 \leq a, b \leq q$ such that $a \cdot b \equiv 1(\mod q)$

$ab = kq + 1$ for some $k \in G \implies g^{a \cdot b} = g^{kq+1} = g^{kq} \cdot g = (g^q)^k \cdot g = 1^k \cdot g = g$

Question 9

For some $h \in G$, if $h = g^\alpha$, then dlog is hard problem when it is difficult to obtain α.

Also, we know that both g and h are the random generators of G. This means, we can say that $h = g^c$

$H(a.b) = g^a \cdot h^b = g^a \cdot (g^c)^b = g^a \cdot g^{bc} = g^{a+bc}$

Let p: dlog is a hard problem $\implies$ $a + bc$ is not easy to find $\implies$ c is not easy to find because we already know (a, b).

Let q: collision resistant $\implies$ if $g^a h^b = g^{a'} h^{b'}$ then $(a, b) = (a', b')$.

We will prove this by using contra-positive proof. Assume $\neg q$. This means, if $g^a h^b = g^{a'} h^{b'}$ then there can be distinct (a, b) and (a', b').If we have distinct (a, b) and (a', b') for $g^a h^b = g^{a'} h^{b'}$, then $a + bc = a' + b'c$. From this, we can easily find c, hence showing dlog is not hard.

Therefore, $\neg q \implies \neg p$. From the contrapositive proof, $p \implies q$.

Hence, if discrete log problem is hard on G then H is a collision resistant compression function.