CSE 107 Hw 5

Corrected

#2.1a p is prime $\mathbb{Z}_p^* = \{1 \ldots p-1\}$

g is a generator of $\mathbb{Z}_p^*$, $|\langle g \rangle| = |\mathbb{Z}_p^*|$

Ex: $g = 2$

i:	0	1	2	3	4	5	6	7	8	9	10
$2^i \bmod 11$:	1	2	4	8	5	10	9	7	3	6	1

$\langle 2 \rangle$: {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

$h = g^2 = 4$

i:	0	1	2	3	4	5	6	7	8	9	10
$4^i \bmod 11$:	1	4	5	9	3	1	4	5	9	3	1

$h = \langle 4 \rangle$: {1, 3, 4, 5, 9} $= 10/2$

Order of $g = p-1$

Order of $h = \frac{p-1}{2}$

#2.1b $\gcd(e, q) = 1$

Claim: $c^d = h$

(2.1b)

Prove: $c^d = h$ for a "d" coprime to q

Since d & e are coprimes of q, $\gcd(e, q) = 1$ & $\gcd(d, q) = 1$

$|Z^*_p| = (p-1)$ and we can use this order to mod the exponent of $c^d = h$ & $h^e = c$

$c^{d \bmod (p-1)} \bmod p = h \quad c = h^{e \bmod (p-1)} \bmod p$

↳ These can be done based on the exponent simplification slides from lecture

$(h^{e \bmod (p-1)})^{d \bmod (p-1)} \bmod p = h \rightarrow h^{e \cdot d \bmod (p-1)} \bmod p = h$

- Since e & d ∈ q & q ∈ p, that means $e = e \bmod (p-1)$; & $d = d \bmod (p-1)$

$e \cdot d = 2p - 1 \Rightarrow h^{(2p-1) \bmod (p-1)} \bmod p = h \pmod p$

$\Rightarrow h' \bmod p = h \pmod p \Rightarrow h = h$

Ex: $p = 23 \quad q = 11 \quad e = 9 \quad d = 5$

$h^{(9 \cdot 5) \bmod 22} \bmod 23 = h \Rightarrow h^{45 \bmod 22} \bmod 23 = h$

$h' \bmod 23 = h \pmod{23}$

$h = h \pmod{23}$

$h = c^0 = (h^a)^{-n}$ h^{-n}

(c) 0 is not in $\mathbb{Z}_q^*$ because anything divided by 0 would be 0, so it does not have a common divisor.

(d)

$T(K,1) = h^{1/K[0] + 1/K[1]}$

$T(K,-1) = h^{1/K[0] - 1/K[1]}$

$T(K,2) = h^{1/K[0] + 1/(2K[1])}$

$T(K,-2) = h^{1/K[0] - 1/(2K[1])}$

(e) $p, q, h, h^{1/K[0]}, h^{1/K[1]}$ are known values

$(h^{1/K[0]})^{h^{1/K[1]}} = h^{1/K[0] + 1/K[1]}$ if

$M = 1$

$$\left(h^{1/K[0]}\right) \cdot \left(h^{1/K[1]}\right)^{\frac{1}{M}} = h^{1/K[0] + 1/(M \cdot K[1])}$$

This means that if we apply the inverse of our randomly created message on $h^{1/K[1]}$ by raising the value to the power of inverse of the message, we can get the tag for that message, by multiplying $h^{1/K[0]}$ & $h^{1/M \cdot K[1]}$

In this case we can call MOD-EXP on $h^{1/K[1]}$ with MOD_INV(M) as the exponent & "p" as N

= MOD-Exp($h^{1/K[1]}$, M^{-1}, p) will get us $h^{1/M \cdot K[1]}$.

#13

It took me 2 hours for Problem 1.
It took me 14 hours for problem 2.

16 hours total