HW 2.b ___ Jessup Barrueco

Q1 D-H, $q=71$, $\alpha=7$

a Given A has private key $X_A=5$, what is pub. key Y_A?

$Y_A = \alpha^{X_A} \bmod q = 7^5 \bmod 71 = \boxed{51}$

b B has $X_B=12$, find Y_B:

$Y_B = 7^{12} \bmod 71 = \boxed{4}$

c Shared secret key:

$4^5 \bmod 71 = 51^{12} \bmod 71 = \boxed{30}$

d If participants exchanged $x^\alpha \bmod q$ instead of $\alpha^x \bmod q$, an attacker would be able to easily recover the original value of x. Because α is a publicly known value, $x^\alpha \bmod q$ can be reduced α-times to recover $x \bmod q$.

$\boxed{Q2}$ X appends 64-bit hash code, encrypted w/ X's private key.

$\boxed{a}$ The Birthday Attack is carried out as follows. Attacker generates $2^{m/2}$ variations of a valid msg in msg-space m ($m=64$ in given question params), these msgs all have a similar (valid) meaning. Then, the attacker generates $2^{m/2}$ variations of a desired fraudulent msg. According to the Birthday Paradox, the probability of a fraudulent msg having the same hash value as a valid msg is >0.5. The user then signs the valid msg, so the attacker is able to use that valid signature with the fraudulent msg that has the same hash value.

$\boxed{b}$ For an M-bit message, the attacker would need $2^{m/2}$ memory. If $m=64$, the attacker would need 2^{32} memory. If $m=128$, memory needed $= 2^{64}$
(d)

$\boxed{c}$ 2^{20} hash/second, $2^{\frac{m}{2}+1}$ hashes in total.

$2^{33}/2^{20} = 2^{13}$ seconds for $m=64$

$2^{65}/2^{20} = 2^{45}$ seconds for $m=128$ (d)

Q3 Trapdoor One-Way Fcn

plaintext $P = 0101\,0111$

private key $S = \{5, 9, 21, 45, 103, 215, 450, 946\}$

note: set S is superincreasing

$a = 1019$ $\quad$ $p = 1999$

step 1: generate public key β: $\beta_i = a s_i \bmod p$

$$\beta = \{1097, 1175, 1409, 1877, 1009, 1194, 779, 456\}$$
$$\quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1$$

step 2: add elements of $\beta \bmod p$ according to plaintext

$$C = 1175 + 1877 + 1194 + 779 + 456 = 5481 \equiv 1483 \bmod 1999$$

step 3: to decrypt the ciphertext C back to obtain the plaintext, first find $a^{-1} \bmod p$. From Fermat's Little Thm, see

$$a^{-1} \bmod p = a^{p-2} \bmod p = 1019^{1997} \bmod p = 1589$$

$$C \cdot a^{-1} = 1483 \cdot 1589 \equiv 1665 \bmod 1999$$

step 4: verify 1665 is correct plaintext:

$$S = \{5, 9, 21, 45, 103, 215, 450, 946\}$$
$$\quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1$$

$$9 + 45 + 215 + 450 + 946 = 1665$$

$\Longrightarrow$ process successful