HW 2 pt A

Nolan Pofi

1.

a).

$Y_A = \alpha^{x_A} \mod q = 7^5 \mod 71 = 20$

b).

$Y_B = \alpha^{x_B} \mod q = 7^{12} \mod 71 = 67$

c).

$Y_{AB} = \alpha^{x_A x_B} \mod q = (Y_A)^{X_B} \mod q$ or $(Y_B)^{X_A} \mod q = 20^{12} \mod 71 = 67^5 \mod 71 = 30$

d).

If $Y_A = x_A^\alpha \mod q$ then user B would not be able to compute the same key in the traditional way $(Y_A)^{x_B} \mod q$ user B However could do $(Y_A)x_B^\alpha \mod q$ and if user A does this aswell but with switched values they will get the same key. But since α is public this becomes easy for an attacker to get the secret values of x.

2.

a).

The Birthday Attack relies on the birthday problem and that the probability of common hash values can be quite high at a lower number of values than one would expect. An attacker generates $2^{n/2}$, where n is the number of bits in the hashcode, copies of the original message with small changes but so that the meaning is the same as the original and the attacker generates $2^{n/2}$ copies of a fraudulent message with each one differing but still meaning the same. The attacker then compares all the pairs hashcodes until a match is found. The attacker than attaches the valid hashcode to the fraudulent message and sends it.

b).

Attacker needs $2^{n/2}$ copies of original and $2^{n/2}$ copies of fraud so they will have $2^n = 2^{64}$ messages in total

Since each message is M bits they will need at least $M \times 2^{64}$ bits space

c).
Expected number of tries is $1.25\sqrt{H}$ where is is size of Hash space $= 2^{6}4$
$1.25\sqrt{2^{64}} = 5368709120$
Can do 2^{20} hashs a second so $5368709120/2^{20} = 5120$ seconds

d).
$M \times 2^{128}$ bit space
$(1.25\sqrt{2^{128}})/2^{20} = 2.2 \times 10^{13}$ seconds

3.
each elemnt i in the PublicKey $= S_i \times a \mod q$

$PK_0 = S_0 \times a \mod q = 5 \times 1019 \mod 1999 = 1,097$
$PK_1 = S_1 \times a \mod q = 9 \times 1019 \mod 1999 = 1,175$
$PK_2 = S_2 \times a \mod q = 21 \times 1019 \mod 1999 = 1,409$
$PK_3 = S_3 \times a \mod q = 45 \times 1019 \mod 1999 = 1,877$
$PK_4 = S_4 \times a \mod q = 103 \times 1019 \mod 1999 = 1,009$
$PK_5 = S_5 \times a \mod q = 215 \times 1019 \mod 1999 = 1,194$
$PK_6 = S_6 \times a \mod q = 450 \times 1019 \mod 1999 = 359$
$PK_7 = S_7 \times a \mod q = 946 \times 1019 \mod 1999 = 456$
PK = {1,097; 1,175; 1,409; 1,877; 1,009; 1,194; 779; 456}

Now inverse of a is needed
$1999 = (1019) \times 1 + 980$ $p_0 = 0$
$1019 = (980) \times 1 + 39$ $p_1 = 1$
$980 = (39) \times 25 + 5$ $p_2 = 0 - 1(1) \mod 1999 = 1998$
$39 = (5) \times 7 + 4$ $p_3 = 1 - 1998(1) \mod 1999 = 2$
$5 = (4) \times 1 + 1$ $p_4 = 1998 - 2(25) \mod 1999 = 1948$
$4 = (1) \times 4 + 0$ $p_5 = 2 - 1948(7) \mod 1999 = 359$
$p_6 = 1948 - 359(1) \mod 1999 = 1589$
Inverse = 1589

Cipher $= \sum_{i=0}^{n} P_i \times PK_i$
Cipher $= 1,097 * 0 + 1,175 * 1 + 1,409 * 0 + 1,877 * 1 + 1,009 * 0 + 1,195 * 1 + 779 * 1 + 456 * 1 = 5481$

Decrypt = Cipher$\times 1589 \mod 1999 = 5481 * 1589 \mod 1999 = 1665$
Since S is super Increasing start at back if $S_i >=$ Decrypt then P_i is 1 else 0
Then subtract S_i from Decrypt
$1665 > 946 \rightarrow P_7 = 1$
$1665 - 946 = 719$
$719 > 450 \rightarrow P_6 = 1$
$719 - 450 = 269$
$269 > 215 \rightarrow P_5 = 1$
$269 - 215 = 54$
$54 < 103 \rightarrow P_4 = 0$

$54 > 45 \rightarrow P_3 = 1$
$54 - 45 = 9$
$9 < 21 \rightarrow P_2 = 0$
$9 = 9 \rightarrow P_1 = 1$
$9 - 9 = 0$
$0 < 5 \rightarrow P_0 = 0$
so P = {0,1,0,1,0,1,1,1}
Which matches the original P.