Crypto HW 2

(1) a) $Y_A = \alpha^{X_A} \bmod q$

$Y_A = 7^5 \bmod 71$

$Y_A = 51$

b) $Y_B = \alpha^{X_B} \bmod q$

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

$Y_B = 4$

c) $K_{AB} = \alpha^{X_A \cdot X_B} \bmod q$

$K_{AB} = \alpha^{60} \bmod q$

$K_{AB} = 30$

d) This would not work because it would no longer create a discrete logarithm problem for the adversary to solve, and thus it would not be a one way function

(2) a) The attacker would generate 2^{32} variations of a valid message, and another 2^{32} fraudulent messages. Now, the sets are compared to find a pair of a valid message and a fraudulent message such that they have the same hash value. Once this is found, we have the user sign the valid message, and we now have a valid signature for the fraudulent message

b) $(2^{33})(M)$ bits

c) $2^{33}/2^{20} = 2^{13}$ seconds

d) $(2^{65})M$ bits

$2^{65}/2^{20} = 2^{45}$ seconds

(3) $t_i = a \cdot s_i \bmod p$

$t_i = \{1097, 1179, 1409, 1877, 1009, 1194, 779, 456\}$

C_i : $y = 1179 + 1877 + 1194 + 779 + 456 = \boxed{5481}$

$Z = a^{-1} y \bmod p$

Find a^{-1}:

$1999 = 1 \times 1019 + 980$
$1019 = 1 \times 980 + 39$
$980 = 25 \times 39 + 5$
$39 = 7 \times 5 + 4$
$5 = 1 \times 4 + 1$

$1 = 5 - 4$
$1 = 5 - 39 + 7 \times 5$
$1 = 8 \times 5 - 39$
$1 = 8 \times (980 - 25 \times 39) - 39$
$1 = 8 \times 980 - 200 \times 39 - 39$
$1 = 8 \times 980 - 201 \times 39$
$1 = 8 \times 980 - 201 \times (1019 - 980)$
$1 = 8 \times 980 - 201 \times 1019 + 201 \times 980$
$1 = 209 \times 980 - 201 \times 1019$
$1 = 209 \times (1999 - 1019) - 201 \times 1019$
$1 = 209 \times 1999 - 209 \times 1019 - 201 \times 1019$
$1 = -410 \times 1019$

$1999 - 410 = \boxed{1589}$

$Z = 1589 (5481) \bmod 1999$
$Z = 1665$

$946 + 450 + 215 + 103 + 45 + 71 + 9 + 26 = 1665$
✓ ✓ ✓ ✗ ✓ ✗ ✓ ✗

$\boxed{\{0,1,0,1,0,1,1,1\}}$