1. H(M) = sha256("Hello")'s last 6 bits = $110111_{(2)} = 55$

a) verification key $PU = 369^{-1} \bmod (17-1)(29-1) = 17$ #

448		1	0
369		0	1
79	1	1	-1
53	4	-4	5
26	1	5	-6
1	2	-14	17

signature = $55^{369} \bmod 493$:

group 17	group 29
$55 \bmod 17 = 4$	$55 \bmod 29 = 26$
$369 \bmod 16 = 1$	$369 \bmod 28 = 5$
$4^1 \bmod 17 = 4$	$26^5 \bmod 29 = 18$

$s = [4 \cdot 29 \cdot (29^{-1} \bmod 17) + 18 \cdot 17 \cdot (17^{-1} \bmod 29)] \bmod 493$

$= 395$

$395^{17} \bmod 493$:

group 17	group 29
$395 \bmod 17 = 4$	$395 \bmod 29 = 18$
$17 \bmod 16 = 1$	$17 \bmod 28 = 17$
$4^1 \bmod 17 = 4$	$18^{17} \bmod 29 = 26$

$[4 \cdot 29 \cdot (29^{-1} \bmod 17) + 26 \cdot 17 \cdot (17^{-1} \bmod 29)] \bmod 493$

$= 55 = H(M) \Rightarrow$ verified #

(b) $S_1 = \alpha^k = 17^{13} \bmod 113 = 92$

$S_2 = k^{-1}(m - X_A S_1) \bmod (q-1)$

$= 13^{-1}(55 - 37 \cdot 92) \bmod 112$

$= (69 \cdot 11) \bmod 112$

$= 87$

112		1 0
13		0 1
8	8	1 -8
5	1	-1 9
3	1	2 -17
2	1	-3
1	1	5 -43
1	1	-8 69

signature: (92, 87)

verification key $PU = (q, \alpha, \alpha^{X_A} \bmod q)$

$= (113, 17, 17^{37} \bmod 113)$

$= (113, 17, 79)$ #

$\alpha^m \equiv 17^{55} \equiv 93 \pmod{113}$

$Y_A^{S_1} \cdot S_1^{S_2} \equiv 79^{92} \cdot 92^{87} \equiv 60 \cdot 75 \equiv 93 \pmod{113}$

$\Rightarrow \alpha^m \equiv Y_A^{S_1} \cdot S_1^{S_2} \pmod q \Rightarrow$ verified #

c) $x = a^r \bmod P = 53^{13} \bmod 293 = 39$

$e = H(\text{"Hello!39"}) = 49$

$y = (r + se) \bmod q = (13 + 29 \cdot 49) \bmod 73 = 47$

signature : $(49, 47)$

verification key $PU = a^{-s} \bmod P = 53^{-29} \bmod 293 = 94^{29} \bmod 293$

$= 140$ #

293	1	0	
53	0	1	
28	5	1	-5
25	1	-1	6
3	1	2	-11
1	8	-17	(94)

$x' = a^u v^e \bmod P$

$= (53^{47} \cdot 140^{49}) \bmod 293$

$= (225 \cdot 133) \bmod 293$

$= 39$

$H(\text{"Hello!39"}) = 49 = e \Rightarrow$ verified #

d) verification key $PV = g^x \bmod P = 53^{61} \bmod 293 = 84$ #

$r = (g^k \bmod P) \bmod q = (53^{13} \bmod 293) \bmod 73 = 39$

$S = [13^{-1} \cdot (55 + 61 \cdot 39)] \bmod 73$

$= (45 \cdot 2434) \bmod 73$

$= 30$

signature : (39, 30)

73		1	0
13		0	1
8	5	1	-5
5	1	-1	6
3	1	2	-11
2	1	-3	17
1	1	5	-28
1	1	-8	45

$w = (30^{-1}) \bmod 73 = 56$

$u_1 = [H(M) \cdot w] \bmod q$

$= (55 \cdot 56) \bmod 73$

$= 14$

$u_2 = (r \cdot w) \bmod q$

$= (39 \cdot 56) \bmod 73$

$= 67$

73		1	0
30		0	1
13	2	1	-2
4	2	-2	5
1	3	7	-17
1	3	-23	56

$V = [(g^{u1} \cdot y^{u2}) \bmod P] \bmod q$

$= [(53^{14} \cdot 84^{67}) \bmod 293] \bmod 73$

$= ((116 \cdot 94) \bmod 293) \bmod 73$

$= 39 = r \Rightarrow$ verified #