10955096. 杜峯.

H(M) = the last 6 bits of sha256 for message M
M = "Hello!" random key : k = 13
sha256(M) = ····· B7
⇒ 10||0111 ⇒ last 6 bits ⇒ 110111(binary) = 55(dec)

(a) $n = 493 = 17 \times 29$, $PR = (369, 493)$
$m = H(M) = 55$
$s = m^d \bmod n = 55^{369} \bmod 493 = 395$
sign M ⇒ (M, s=395)
Verify :
$e = d^{-1} \bmod \phi(n) = 369^{-1} \bmod 16 \times 28 = 369^{-1} \bmod 448$
$a_1 = 1$, $a_2 = 0$ (Extended Euclidean Algorithm)
$369 \bmod 448 = 369$ $q = 0$
$a_3 = a_1 - 0 \cdot a_2 = 1$
$448 \bmod 369 = 79$ $q = 1$
$a_4 = a_2 - 1 \cdot a_3 = -1$
$369 \bmod 79 = 53$ $q = 4$
$a_5 = a_3 - 4 \cdot a_4 = 1 - (-4) = 5$
$79 \bmod 53 = 26$ $q = 1$
$a_6 = a_4 - 1 \cdot a_5 = -1 - 5 = -6$
$53 \bmod 26 = 1$ $q = 2$
$a_7 = a_5 - 2 \cdot a_6 = 5 - (-12) = 17$ ⇒ $369 \cdot 17 \bmod 448 = 1$
$e = 369^{-1} \bmod 448 = 17$
PU = (e=17 , n=495)
PR : (d=369 , n=495)
$m' = s^e \bmod n = 395^{17} \bmod 448 = 55$
∵ m' = m = 55
∴ verified.

(b) $q = 113$, $\alpha = 17$, $X_A = 37$
⇒ $Y_A = \alpha^{X_A} \bmod q = 17^{37} \bmod 113 = 79$
for $m = H(M) = 55$, $k = 13$
$S_1 = \alpha^k \bmod q = 17^{13} \bmod 113 = 92$
$S_2 = k^{-1}(m - X_A S_1) \bmod (q-1) = 13^{-1}(55 - 37 \cdot 92) \bmod 112$

$= 13^{-1}(-3349) \bmod 112$

$= 13^{-1} \cdot 11 \bmod 112$

$a_1 = 1,\ a_2 = 0$ (Extended Euclidean Algorithm)

$13 \bmod 112 = 13 \quad q = 0$

$a_3 = a_1 - 0 \cdot a_2 = 1$

$112 \bmod 13 = 8 \quad q = 8$

$a_4 = a_2 - 8 \cdot a_3 = -8$

$13 \bmod 8 = 5 \quad q = 1$

$a_5 = a_3 - 1 \cdot a_4 = 1 - (-8) = 9$

$8 \bmod 5 = 3 \quad q = 1$

$a_6 = a_4 - 1 \cdot a_5 = -8 - 9 = -17$

$5 \bmod 3 = 2 \quad q = 1$

$a_7 = a_5 - 1 \cdot a_6 = 9 - (-17) = 26$

$3 \bmod 2 = 1 \quad q = 1$

$a_8 = a_6 - 1 \cdot a_5 = -17 - 26 = -43 \Rightarrow -43 \bmod 112 = 69 \Rightarrow 13 \cdot 69 \bmod 112 = 1$

$S_2 = 69 \cdot 11 \bmod 112 = 87$

sign $M \Rightarrow (M, S_1 = 92, S_2 = 87)$

Verify:

$\alpha^m \bmod q = 17^{55} \bmod 113 = 93$

$Y_A^{S_1} S_1^{S_2} \bmod q = 79^{92} 92^{87} \bmod 113 = 60 \cdot 75 \bmod 113 = 93$

$\therefore \alpha^m \bmod q = Y_A^{S_1} S_1^{S_2} \bmod q = 93$

$\therefore$ verified.

(c) $p = 293,\ q = 73,\ \alpha = 53,\ S = 29$

$PR = (293, 73, 53, 29)$

$PU = (293, 73, 53, v)$

$v = \alpha^{-S} \bmod 293 = 53^{-29} \bmod 293 = (53^{-1} \bmod 293)^{29} \bmod 293$

$a_1 = 1,\ a_2 = 0$ (Extended Euclidean Algorithm)

$53 \bmod 293 = 53 \quad q = 0$

$a_3 = a_1 - 0 \cdot a_2 = 1$

$293 \bmod 53 = 28 \quad q = 5$

$a_4 = a_2 - 5 \cdot a_3 = -5$

$53 \bmod 28 = 25 \quad q = 1$

$a_5 = a_3 - 1 \cdot a_4 = 1 - (-5) = 6$

$28 \bmod 25 = 3 \quad q = 1$

$a_6 = a_4 - 1 \cdot a_5 = -5 - 6 = -11$

$25 \bmod 3 = 1 \quad q = 8$

$a_7 = a_5 - 8 \cdot a_6 = 6 - 8 \cdot (-11) = 6 + 88 = 94 \Rightarrow 53 \cdot 94 \bmod 293 = 1$

$V = (94)^{29} \bmod 293 = 140$

choose $r = k = 13$

$X = a^r \bmod p = 53^{13} \bmod 293 = 39 \Rightarrow$ consider as "39"

$e = H(M \| X) = 110001$ (binary) $= 49$ (dec)

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

$= 1434 \bmod 73 = 47$

sign $M \Rightarrow (M, X = 49, y = 47)$

Verify:

$X' = a^y V^e \bmod p = 53^{47} 140^{49} \bmod 293 = 225 \cdot 133 \bmod 293 = 39$

$\because H(M \| X') = 110001$ (binary) $= 49$ (dec) $= e$

$\therefore$ verified.

(d) $p = 293, q = 73, g = 53, X = 61$

$y = g^x \bmod p = 53^{61} \bmod 293 = 84$

choose $k = 13$, $m = H(M) = 55$

$r = (g^k \bmod p) \bmod q$

$= (53^{13} \bmod 293) \bmod 53 = 39 \bmod 53 = 39$

$S = [k^{-1}(H(M) + Xr)] \bmod q$

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

$a_1 = 1, a_2 = 0$ (Extended Euclidean Algorithm)

$13 \bmod 73 = 13 \quad q = 0$

$a_3 = a_1 - 0 \, a_2 = 1$

$73 \bmod 13 = 8 \quad q = 5$

$a_4 = a_2 - 5 \cdot a_3 = -5$

$13 \bmod 8 = 5 \quad q = 1$

$a_5 = a_3 - 1 \cdot a_4 = 1 - (-5) = 6$

$8 \bmod 5 = 3 \quad q = 1$

$a_6 = a_4 - 1 \cdot a_5 = -5 - 6 = -11$

$5 \bmod 3 = 2 \quad q_7 = 1$

$a_7 = a_5 - 1 \cdot a_6 = 6 - (-11) = 17$

$3 \bmod 2 = 1 \quad q_8 = 1$

$a_8 = a_6 - 1 \cdot a_7 = -11 - (17) = -28 \Rightarrow -28 \bmod 73 = 45 \Rightarrow 13 \cdot 45 \bmod 73 =$

$S = [45(55 + 61 \cdot 39)] \bmod 73 = 45 \cdot 2434 \bmod 73 = 30$

sign $M = (M, r = 39, S = 30)$

Verify:

$W = (S')^{-1} \bmod q = (30)^{-1} \bmod 73$

$a_1 = 1 \quad a_2 = 0$ (Extended Euclidean Algorithm)

$30 \bmod 73 = 30 \quad q = 0$

$a_3 = a_1 - 0 \cdot a_2 = 1$

$73 \bmod 30 = 13 \quad q = 2$

$a_4 = a_2 - 2 \cdot a_3 = -2$

$30 \bmod 13 = 4 \quad q = 2$

$a_5 = a_3 - 2 \cdot a_4 = 1 - (-4) = 5$

$13 \bmod 4 = 1 \quad q = 3$

$a_6 = a_4 - 3 \cdot a_5 = -2 - 15 = -17 \bmod 73 = 56 \Rightarrow 30 \cdot 56 \bmod 73 = 1$

$W = 30^{-1} \bmod 73 = 56$

$u_1 = [H(M') \cdot w] \bmod q = 55 \cdot 56 \bmod 73 = 14$

$u_2 = r' w \bmod 73 = 39 \cdot 56 \bmod 73 = 67$

$v = [g^{u_1} y^{u_2} \bmod p] \bmod q = [53^{14} \cdot 84^{67} \bmod 293] \bmod 73$

$= [(6 \cdot 94 \bmod 293] \bmod 73$

$= 39 \bmod 73 = 39$

$\because v = r' = 39$

$\therefore$ verified.