HW5 Writing problem

1、 $M=$"Hello!"

$H(M)=55=m$

(a) RSA

$n=493=17\times 29 \Rightarrow p=17.\ q=29.$

$\phi(n)=16\times 28=448$

$PR=(d,n)=(369,493)$

$369=e^{-1} \bmod 448 \Rightarrow e=17.$

$PU=(e.n)=(17,493)$

Sign:

$S=55^{369} \bmod 493=395$

Verify:

$m'=395^{17} \bmod 493=55$

$\because m'=H(M)=m$

$\therefore$ Pass#.

(b) ElGamal

$PR=(q.\alpha.X_A)=(113.17.37)$

$Y_A=17^{37} \bmod 113=79$

$PU=(q.\alpha.Y_A)=(113.17.79)$

$k=13.$

Sign:

$S_1=\alpha^k \bmod q=17^{13} \bmod 113=92$

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

$=13^{-1}(55-37\times 92) \bmod 112=69\times 11 \bmod 112=87$

Verify:

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

$Y_A^{S_1} S_1^{S_2} \bmod q=79^{92} 92^{87} \bmod 113$

$=60\times 75 \bmod 113=93$

$\because \alpha^m \equiv Y_A^{S_1} S_1^{S_2} \bmod q$

$\therefore$ Pass

(C) Schnorr

$PR=(p,q,a,s)=(293,73,53,29)$

$V=a^{-s} \bmod p=53^{-29} \bmod 293$

$=(53^{-1})^{29} \bmod 293=94^{29} \bmod 293=140$

$PU=(p,q,a,v)=(293,73,53,140)$

Sign:

choose $r=2 \Rightarrow X=a^{r} \bmod p=53^{2} \bmod 293=172$

$e=H(M||X)=17$

$y=(2+29\times 17) \bmod 73=57$

Verify:

$X'=a^{y}v^{e} \bmod p=53^{57}140^{17} \bmod 293$

$=186\times 149 \bmod 293=172$

$H(M||X')=17$

$\because H(M||x')=e=17$

$\therefore$ pass

(d) DSA

$PR=(p, q, g, x)=(293, 73, 53, 61)$

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

$PU=(p, q, g, y)=(293, 73, 53, 84)$

$k=13$

Sign:

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

$s = k^{-1}(H(M)+rx) \bmod q = 13^{-1}(55+39\times 61) \bmod 73$

$= 45 \times 25 \bmod 73 = 30$

Verify:

$(r', s')=(39, 30)$, $H(M')=55$

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

$u1=[H(M')w] \bmod q = 55\times 56 \bmod 73 = 14$

$u2= (r')w \bmod q = 39\times 56 \bmod 73 = 67$

$V=[(g^{u1}y^{u2}) \bmod p] \bmod q = [(53^{14}\, 84^{67}) \bmod 293] \bmod 73$

$=16\times 94 \bmod 293 \bmod 73 = 39$

$\because V=r'$

$\therefore$ pass.