Introduction to Cryptography, 2021 Fall

Homework 5, due 4pm, 12/20/2021 (Monday)

Part 1: Written Problems

1. Let the hash function be H(M) = the last 6 bits of sha256(M) for a message M. Then, the last 6 bits are treated as a binary number for computing signature, such as, 100011 (binary) is 35 (decimal). To hash a decimal number x, we treat it as the ASCII string. For example, x=47 is treated as the ASCII string "47" or 3437 (Hex). For each of the following methods of specified parameters, sign "Hello!" with random k=13 (if needed), compute the verification key, and verify correctness of the signature.
   Note: You must provide reasonably detailed computation steps, not just the answers.

   a) RSA: n=493=17x29, private key = (493, 369)
   b) ElGamal: q=113, α=17, private key = (113, 17, 37)
   c) Schnorr: p=293, q=73, a=53, private key = (293, 73, 53, 29)
   d) DSA: p=293, q=73, g=53, private key = (293, 73, 53, 61)

H("Hello!") =SHA256("Hello!") = 55 = m

a) RSA: n=493=17x29, private key = (493, 369)

PU=(e,n)=(369^{-1}mod 448, 493) = (17, 493)

Sign：S=m^d mod n=55^{369} mod 493 =395

Verify:(H(M), S^e mod n)

395^{17}mod 493 = 55= H(M)，Pass。

b) ElGamal: q=113, α=17, private key = (113, 17, 37)

PU=(q, α, YA) = (113, 17, 17^{37} mod 113) = (113,17, 79)

Sign：

S1=α^k mod q =17^{13} mod 113 = 92

S2=k^{-1} (m- $X_A S_1$) mod (q-1) = 13^{-1} (55- 37* 92) mod (112)=87

Verify:

(α^m mod q , $Y_A{}^{S1}\ S_1{}^{S2}$ mod q)

α^m = 17^{55}=93=79^{92} x 92^{87} =60 x 75 mod 113。Pass。

c) Schnorr: p=293, q=73, a=53, private key = (293, 73, 53, 29)

v =a^{-s} mod p =53^{-29} mod 293 = 140

PU=(p,q,a,v)=(103,17,72,140)

Sign:

x = a^r mod p =53^{13} mod 293 = 39 (the r here means k = 13)

e = H(M||x) = 49

y=(r+se) mod q =(13+29x49) mod 73 = 47

Verify :

($a^y\ v^e$ mod p , x)

$a^y\ v^e$ mod p= $53^{47}140^{49}$ = 29925 mod 293 = 39 = x。Pass

d) DSA: p=293, q=73, g=53, private key = (293, 73, 53, 61)

y=g^x mod p = 53^{61} mod 293 = 84

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

Sign:

r =(g^k mod p)mod q =(53^{13} mod 293) mod 73 =39

s =k^{-1} (H(M)+xr) mod q = 13^{-1}(55 + 61*39) mod q = 30

Verify:

$(r , ((g^{H(M)} y^{r})^{(s\text{^-1} \bmod q)} \bmod p) \bmod q)$

$((g^{H(M)} y^{r})^{(s\text{^-1} \bmod q)} \bmod p) \bmod q = (53^{55} 84^{39})^{56} \bmod 293 \bmod 73 = 39 = r$，Pass。