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.

   $H(M) = 110111_2 = 55_{10} = m$

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

      $\Phi(493) = (17\text{-}1)\ (29\text{-}1) = 16*28 = 448$

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

      Sign: $S = m^d \bmod n = H(W)^{369} \bmod 493 = 395$

      Verify: $(H(W), S^e \bmod n)$

      $395^{17} \bmod 493 = 55 = H(W)$, Pass.

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

      $PR = (q, \alpha, X_A) = (113, 17, 37)$

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

      $PU = (q, \alpha, Y_A) = (113, 17, 79)$

      Sign:

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

      $S_2 = k^{-1}(m - X_A S_A) \bmod (q\text{-}1) = 13^{-1}(55 - 37*92) \bmod 112 = 87$

      Verify: $(\alpha^m \bmod q,\ Y_A^{S_1} S_1^{S_2} \bmod q)$

      $\alpha^m = 17^{55} = 93 = 79^{92} \times 92^{87} \bmod 113$, Pass.

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

      $v = a^{-s} \bmod p = 53^{-29} \bmod 293 = 140$

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

      Sign:

      $x = a^r \bmod p = 53^{13} \bmod 293 = 39$

      $e = H(M \| x) = 110001_2 = 49_{10}$

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

      Verify: $(a^y v^e \bmod p, x)$

      $a^y v^e \bmod p = 53^{47} 140^{49} \bmod 293 = 39 = x$, Pass.

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

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

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

Sign:

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

$s = k^{-1} (H(M) + xr) \bmod q = 13^{-1}(55 + 61*39) \bmod 73 = 30$

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

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