CS 355, Fall, 2019, Homework 7

1. Consider Shamir's Lagrange interpolating polynomial key threshold scheme. Let $t = 4$, $p = 11$, $K = 7$ and

$$h(x) = (x^3 + 10x^2 + 3x + 7) \bmod 11.$$

Compute shadows for $x = 1, 2, 3, 4, 5, 6$ and 7. Reconstruct $h(x)$ from the shadows for $x = 1, 3, 5$ and 7.

2. A small bank has an electronic safe which may be opened by certain combinations of the president, the two managers and the five tellers. Policy dictates that the safe may be opened if and only if

(a) the bank president decides to open it, or
(b) the two managers both decide to open it, or
(c) all five tellers decide to open it, or
(d) one manager and three tellers decide to open it.

Explain how you would choose the parameters and distribute the shadows of a Lagrange interpolation polynomial key threshold scheme to meet the requirements of this bank.

3. Consider the following simple signature algorithm which is like DSA except that it does not require a secret random number.

The public elements are a prime q and a primitive root g for q. Alice chooses a private key x in $1 < x < q$ and computes a public key $y = g^x \bmod q$.

To sign a message M, Alice computes $h = H(M)$ for some hash function H. It is required that $\gcd(h, q-1) = 1$. If this is not so, then append the hash to the message and compute a new hash. Continue this process until a hash h is computed which is relatively prime to $q - 1$. Then Alice computes z satisfying $zh \equiv x \pmod{(q-1)}$. The signature for M is $s = g^z \bmod q$. Bob verifies the signature by checking that $s^h \equiv y \pmod{q}$.

a. Show that the latter congruence will hold provided the signature is valid.

b. Show that the scheme is unacceptable by describing a simple technique for Eve to forge Alice's signature on an arbitrary message. (Assume that the Discrete logarithm problem cannot be solved modulo q.)