Assignment #6 – Solutions

Problem 1

Show that y is *not* a square modulo $N = pq$ without revealing the factorization of N.

- Verifier generates 100 known squares $y_i = {x_i}^2 \bmod N$.
- Verifier randomly flips 100 coins $b_i \in \{0,1\}$.
- Verifier forms 100 challenge values $z_i = y_i \cdot y^{b_i} \bmod N$.
- Verifier gives all of the z_i to the prover.
- Prover responds with the correct b_i values.

Note that this interactive proof is *not* zero-knowledge since the prover can be used as an oracle to distinguish squares.

Problem 2

CA wants to certify only *strong* RSA keys.

- Subject generates 100 strong RSA keys $N_i = p_i q_i$.
- Subject gives all of the N_i to the CA.
- CA randomly selects an $j \in \{1, 2, \ldots, 100\}$.
- Subject reveals p_i and q_i for all $i \neq j$.
- CA certifies N_j.

Note that this is a *weak* form of interactive proof typically known as “cut and choose”.

The probability of failure is 1 in 100 (not 1 in 2^{100}).

Problem 3

Reconstruct secret from shares: $(1,37)$, $(4,12)$, and $(5,62)$.

$$P_1 = 37(x-4)(x-5)/((-3)\cdot(-4)) \bmod 101$$
$$P_4 = 12(x-1)(x-5)/((3)\cdot(-1)) \bmod 101$$
$$P_5 = 62(x-1)(x-4)/((4)\cdot(1)) \bmod 101$$

$$12^{-1} \bmod 101 = 59$$
$$(-3)^{-1} \bmod 101 = -34$$
$$4^{-1} \bmod 101 = 76$$

$$P_1 = 62(x-4)(x-5) \bmod 101 = (62x^2 + 48x + 28) \bmod 101$$
$$P_4 = 97(x-1)(x-5) \bmod 101 = (97x^2 + 24x + 81) \bmod 101$$
$$P_5 = 66(x-1)(x-4) \bmod 101 = (66x^2 + 74x + 62) \bmod 101$$

$$P = (23x^2 + 45x + 70) \bmod 101$$

Problem 3

Reconstruct secret from shares: $(1,37)$, $(4,12)$, and $(5,62)$.

$$P_1 = 37(x-4)(x-5)/((-3)\cdot(-4)) \bmod 101$$
$$P_4 = 12(x-1)(x-5)/((3)\cdot(-1)) \bmod 101$$
$$P_5 = 62(x-1)(x-4)/((4)\cdot(1)) \bmod 101$$

$$12^{-1} \bmod 101 = 59$$
$$(-3)^{-1} \bmod 101 = -34$$
$$4^{-1} \bmod 101 = 76$$

$$P_1 = 62(x-4)(x-5) \bmod 101 = (62x^2 + 48x + 28) \bmod 101$$
$$P_4 = 97(x-1)(x-5) \bmod 101 = (97x^2 + 24x + 81) \bmod 101$$
$$P_5 = 66(x-1)(x-4) \bmod 101 = (66x^2 + 74x + 62) \bmod 101$$

$$P = (23x^2 + 45x + 70) \bmod 101$$

$$S = 70$$

Problem 3 (alternate approach)

Reconstruct secret from shares: $(1,37)$, $(4,12)$, and $(5,62)$.

$$P(x) = (a_2 x^2 + a_1 x + a_0) \bmod 101$$

$$P(1) = (a_2 + a_1 + a_0) \bmod 101 = 37$$
$$P(4) = (16a_2 + 4a_1 + a_0) \bmod 101 = 12$$
$$P(5) = (25a_2 + 5a_1 + a_0) \bmod 101 = 62$$

$$a_2 = 23$$
$$a_1 = 45$$
$$a_0 = s = 70$$

Problem 4

$$P(x) = a_3x^3 + a_2x^2 + a_1x + S$$

$A_3 = g^{a_3}$, $A_2 = g^{a_2}$, $A_1 = g^{a_1}$, and $A_0 = g^S$

$$P(5) = 125a_3 + 25a_2 + 5a_1 + S$$

$$g^{13} = g^{P(5)}$$

$$= g^{125a_3+25a_2+5a_1+S}$$

$$= g^{125a_3} \cdot g^{25a_2} \cdot g^{5a_1} \cdot g^S$$

$$= {A_3}^{125} \cdot {A_2}^{25} \cdot {A_1}^{5} \cdot A_0$$