Homework 5

Due date: Friday, April 21th 11:30 AM

Question 1 (25 points)

Consider the following protocol for two parties A and B to flip a fair coin.

1. A trusted party T publishes her public key pk;
2. Then A chooses a uniform bit b_A, encrypts it using pk, an announces the ciphertext c_A to B and T;
3. Next, B acts symmetrically and announces a ciphertext $c_B \neq c_A$;
4. T decrypts both c_A and c_B, and the parties XOR the results to obtain the value of the coin.

- Argue that even if A is dishonest (but B is honest), the final value of the coin is uniformly distributed.
- Assume the parties use EI Gamal encryption (where the bit b is encoded as the group element g^b before being encrypted — note that efficient decryption is still possible). Show how a dishonest B can bias the coin to any values he likes.
- Suggest what type of encryption scheme would be appropriate to use here. Can you define an appropriate notion of security for a fair coin flipping and prove that the above coin flipping protocol achieves this definition when using an appropriate encryption scheme?

Question 2 (30 points)

Suppose three users have RSA public keys $(N_1, 3)$, $(N_2, 3)$, and $(N_3, 3)$ (i.e., they all use e =3), with $N_1 < N_2 < N_3$. Consider the following method for sending the same message $m \in \{0,1\}^\ell$ to each of these parties: choose a uniform $r \leftarrow Z^*_{N_1}$, and send to everyone the same ciphertext

$$< [r^3 \; mod \; N_1], [r^3 \; mod \; N_2], [r^3 \; mod \; N_3], H(r) \oplus m > \qquad (1)$$

where $H : Z^*_{N_1} \rightarrow \{0,1\}^\ell$. Assume $\ell \gg n$

- Show that this is not CPA-secure, and an adversary can recover m from the ciphertext even when H is modeled as a random oracle.
- Show a simple way to fix this and get a CPA-secure method that transmits a ciphertext of length $3\ell + O(n)$.

Question 3 (15 points)

Secret sharing is a problem in cryptography where n shares $X_1, ..., X_n$ (called shadows) are given to n parties where some of the shadows or all of them are needed in order to reconstruct the secret (M) which is a number (i.e. there is a specified threshold t, such that any t shadows make it possible to compute M which is a bit string). Consider the following secret sharing algorithm:

1. Choose at random $t-1$ positive integers $a_1, ..., a_{t-1}$ with $a_i < P$ (P is a prime number) and let $a_0 = M$.
2. Build the polynomial $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_{t-1}x^{t-1}$.
3. Create n shadows that are: $(1, f(1)(\mod p)), ..., (n, f(n)(\mod p))$ (i.e. every participant is given a point (an integer input to the polynomial, and the corresponding integer output).

Note: Suppose $t < P - 1$
Based on the above protocol, answer the following questions:

Part 1 (6 points) In above protocol, arithmetic is all modulo p to build the polynomial. Suppose that we mistakenly calculate the shadows as $(x, f(x))$ instead of $(x, f(x)(\mod p))$, can an eavesdropper gain information from M or not if the eavesdropper sees some of the points (e.g. Suppose the eavesdropper finds (1,f(1)) or (2, f(2)))? If your answer is no, please prove it otherwise provide an example that shows the eavesdropper can gain information about M.

Part 2 (9 points) Suppose we modify the scheme such that $M = a_0 + a_1 + \ldots + a_{t-1} \mod p$. Does having t or more shadows make it possible to compute M ? Does having fewer than t shadows reveal nothing about M? Please justify your answers.

Question 4 (30 points)

A strong one-time secure signature scheme satisfies the following: given a signature σ' on a message m', it is infeasible to output $(m, \sigma) \neq (m', \sigma')$ for which σ is a valid signature on m (note that $m = m'$ is allowed)

- Give a formal definition of strong one-time secure signatures.
- Assuming the existence of one-way functions, show a one-way function for which Lamport's scheme is not a strong one-time secure signature scheme.
- Construct a strong one-time secure signature scheme based on any assumption use in the book.

  Hint: Use a particular one-way function in Lamport's signature.