Problem Set 6

Due on Monday, April 16, 2012.

Instructions Work the problems below, prepare your answers in electronic form, and submit your solutions using the submit script on the Zoo. Remember to specify "6" for the problem number argument to `submit`.

Some of the problems use terminology that we have not covered in class, even though we have talked about the concepts. You may use external resources to find out what these terms mean. As always, you must *properly* cite all resources that you use to solve the problems.

Problem 1: Shamir Secret Splitting **(40 points)**

Alice is leaving for a year of study abroad. She has surprising news that she wants to share with 12 friends, but she doesn't want to tell them before she leaves home since she would feel embarrassed to be present when they learn her secret. Although she trusts her friends, they are naturally curious. Moreover, she's concerned that the parents of two of her friends might discover their shares, and she really doesn't want the parents to find out what her surprise is.

She decides to split her secret into 12 shares and give one to each friend so that any three or more friends can cooperate to discover the secret, but two are not enough. She uses the (τ, k) threshold scheme that she learned in crypto, distributes the shares, and flies off. Unfortunately, unknown to everyone, one of the shares gets corrupted in transit.

By the time she leaves, three of her friends have gone home to Santa Monica, four have gone on a trip to Las Vegas, and the remaining five are still in New Haven.

Each of the three groups of friends then gets together in person and uses the algorithm presented in class to recover the secret.

(a) What values should Alice choose for τ and k?

(b) Following lecture 19, Alice needs to choose a polynomial $f(x)$ with coefficients in $\mathbf{Z}_p$. What are the requirements on p for the scheme to work and be secure?

(c) What degree should $f(x)$ be?

(d) Once Alice has chosen $f(x)$, how should she generate the shares?

(e) Do all three groups succeed in recovering a secret? Explain why or why not. [Remember that one share is bad, but nobody knows which one it is, not even the friend who happens to hold the bad share.]

(f) Of those groups that succeed in recovering a secret, do they all recover the *same* secret? Explain why or why not.

(g) The three groups text the results of each group's recovery attempt to each other, that is, whether or not it failed, and if it did succeed, the secret they recovered. Can everyone now figure out correctly what Alice's secret is?

(h) [0 points] What was Alice's surprising news that motivated her to do this? 🙂

Problem 2: Homomorphic Encryption **(30 points)**

Consider the Caesar cipher extended to strings. Using the definition of homomorphic encryption given in lecture 21, show whether or not the encryption function E_k is homomorphic with respect to operations $\odot_{\mathcal{M}}$ and $\odot_{\mathcal{C}}$, where $\odot_{\mathcal{M}} = \odot_{\mathcal{C}}$ is:

(a) Componentwise addition modulo 26;

(b) Componentwise multiplication modulo 26;

(c) String concatenation.

In each case, carefully define the mesage and ciphertext spaces that make sense for the operation, and give a careful definition of the operation. Then argue why E_k is or is not homomorphic with respect to $\odot_{\mathcal{M}}$ and $\odot_{\mathcal{C}}$.

Problem 3: Security Notions **(30 points)**

Read the Wikipedia page Ciphertext indistinguishability; then answer the following questions:

(a) What is semantic security, and what do the abbreviations IND, CCA, and CCA2 mean? (Don't just copy from the reference but explain in your own words so that it is clear you understand the concepts.)

(b) RSA is not IND-CPA. Give an algorithm for the adversary that allows him to always win the indistinguishability game, and explain why it works.

(c) Argue that Goldwasser-Micali encryption is IND-CPA, assuming the quadratic residuosity problem is hard.