Problem Set 6

Due on Friday, April 19, 2013.

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`.

As always, you must *properly* cite all resources that you use to solve the problems.

Problem 1: Indistinguishability

Happy's roommate, Naive Nelson, is building a pseudorandom sequence generator. He has found a PRSG G that takes a 128-bit seed s and outputs a bit string x of length 1000. Naive wants to generate bit strings of length $\ell = 100,000$, so he creates a new generator G' that works in stages. His idea is to use G repeatedly, obtaining 1000 bits each time. To avoid getting repetitions of the same 1000-bit string, he uses the last 128 bits of each block as a seed for the next block.

Here is his algorithm for computing $G'(s)$:

s is the initial seed;
$i \leftarrow 0$;
$y \leftarrow \lambda$;
while $i < 100$ **do**
  $x \leftarrow G(s)$;
  $s \leftarrow \text{last}(128, x)$;
  $i \leftarrow i + 1$
  $y \leftarrow y \,||\, x$
end while
return y;

In this notation, λ denotes the empty string, $||$ denotes concatenation, and $\text{last}(k, x)$ returns the last k bits of x.

(a) Explain in words why $G'(s)$ is not cryptographically strong.

(b) Describe a judge J (an algorithm) that can distinguish the distribution $G'(S)$ from U. Here, S is the uniform distribution over the seed space, and U is the uniform distribution over binary strings of length ℓ. Be sure to specify the parameters and the return value of J.

(c) Analyze J's behavior when presented with random inputs chosen from $G'(S)$ and from U, respectively.

Problem 2: Shamir Secret Splitting

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 20, 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 of friends 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? 🙂