CMPT 404 — Cryptography

Exercises on Pseudorandom Generators, Functions and Permutations.
Due: Thursday, March 1st (at the beginning of the class)

1. (a) Which of the following functions are superpolynomial:
   - $2^{\sqrt{n}}$;
   - $n^{\log n}$;
   - $n \log n$?

   (b) Prove that for every superpolynomial function T the function $\frac{(T(n^{\frac{1}{3}}))^{\frac{1}{3}}}{n^3}$ is also superpolynomial.

2. *(optional)* This exercise will unable to test your favorite pseudorandom generator. The test is based on a well known property of random integers: Given two randomly chosen integers m and n, the probability they are relatively prime (their greatest common divisor is 1) is $\frac{6}{\pi^2}$. Use this property in a program to determine statistically the value of π. The program should call the random number generator from the system library to generate the random integers. It should loop through a large number of random numbers to estimate the probability that two numbers are relatively prime. From this find an approximate value of π.

   Report the type/name of the random number generator(s), the number of pairs of numbers in your sample, and the approximate value of π.

3. Suppose you have a true random bit generator where each bit in the generated stream has the same probability of being a 0 or 1 as any other bit in the stream and that the bits are not correlated; that is the bits are generated from identical independent distribution. However, the bit stream is biased. The probability of a 1 is $1/2+\delta$, and the probability of a 0 is $1/2-\delta$, where $0 < \delta < 1/2$. A simple deskewing algorithm is as follows: Examine the bit stream as a sequence of non-overlapping pairs. Discard all 00 and 11 pairs. Replace each 01 pair with 0 and each 10 pair with 1.

   (a) What is the probability of occurrence of each pair in the original sequence?

   (b) What is the probability of occurrence of 0 and 1 in the modified sequence?

   (c) What is the expected number of input bits to produce k output bits?

   (d) Suppose that the algorithm uses overlapping successive bit pairs instead of non-overlapping successive bit pairs. That is, the first output bit is based on input bits 1 and 2, the second output bit is based on input bits 2 and 3, and so on. What can you say about the output bit stream? Is it independent?

4. Suppose we use a full length RC4 seed (256 bytes) in the Key Scheduled Algorithm. What such a RC4 key value leaves S unchanged during the KSA? That is, after the initial permutation of S, the entries of S will be equal to the values from 0 to 255 in ascending order.

5. The RSA SecurID card is a credit-card sized device that displays 6 digits that change every minute. The idea is that when you log into your account remotely (say when you want to log

into your UNIX account in SFU from an Internet Cafe) then you have to type the numbers that appear in the card in addition to your PIN or password.

(a) What is the security advantage of such a card over traditional password? That is, what sort of attack can this card resist which cannot be resisted using a standard password mechanism. (Assume that it's possible for users to remember a 6-digits PIN or a password with similar security.)

(b) Describe how you would implement such a scheme using pseudorandom functions. Assume that the PRF family takes a seed of size n, and that the number of possible devices is m (for $m < 2^n$). How many bits of storage does your implementation use at the server and each of the devices? (there is an implementation that uses at most $O(n)$ bits).

(c) *(optional)* Try to *define* what it means that such a scheme is *secure* and sketch a proof that your construction satisfies it (you don't have to formally define and prove if you don't want to — you can use English but try to be precise). Say how the security depends on n — the number of bits that the device stores in memory (where its running time is polynomial in n), and on k — the number of digits that we display to the user.

6. Let $\{f_s\}$, $f_s\colon \{0,1\}^n \to \{0,1\}^n$ be a secure RPR. Consider the family of permutations $\{f'_s\}$, $f'_s\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined as follows: for any $x, x' \in \{0,1\}^n$

$$f'_s(xx') = f_s(x)f_s(x \oplus x')$$

(xx' denotes the concatenation of x and x'). Show that $\{f'_s\}$ is not a secure PRP.

7. Let $\{f_s\}$ be a pseudorandom permutation collection, where for $s \in \{0,1\}^n$, f_s is a permutation over $\{0,1\}^m$. Consider the following scheme (E, D) that encrypts $m/2$-bit messages in the following way: on input $x \in \{0,1\}^{m/2}$, E_k chooses r at random from $\{0,1\}^{m/2}$ and outputs $f_k(x, r)$ (where comma denotes concatenation), on input $y \in \{0,1\}^{m/2}$, D_k computes $(x, r) = f_k^{-1}(y)$ and outputs x. Give an idea of a proof that (E, D) *is* a CPA-secure encryption scheme.

8. Prove that AES is a permutation.

9. Consider a Feistel network composed of 16 rounds with a block length of 128 bits and a key of length of 128 bits. Suppose that, for a given key k , the key scheduling algorithm determines values for the first 8 subkeys, $k_1, k_2, \ldots, k_8$, then sets

$$k_9 = k_8, \quad k_{10} = k_7, \quad k_{11} = k_6, \quad \ldots, \quad k_{16} = k_1.$$

Suppose you have a ciphertext C. Explain how, with access to the encryption algorithm as a black box, you decrypt C and determine the plaintext P using just a single query. This shows that such a cipher is vulnerable to a chosen plaintext attack.
Hint: You may need to read about general properties of block ciphers based on Feistel network (Stallings' book). As an optional exercise try to show that DES satisfies the required property.

10. (*optional*) Given a PRF $\{f_s\}$, $f_s\colon \{0,1\}^{|s|} \to \{0,1\}^{|s|}$, construct a PRF $\{g_s\}$ with $g_s\colon \{0,1\}^{|s|} \to \{0,1\}^{2|s|}$, which is a secure PRF as long as $\{f_s\}$ is secure.