Midterm Assignment **Due: Nov 10** **CAS762 Fall 2010**

1. Suppose that for any given constant $c \in \mathbb{N}$ we have a random number generator r_c, given as $r_c : \mathbb{N} \longrightarrow \{0,1\}^*$, where $r(n)$ is a random string of length n^c. Suppose also that each string in $\{0,1\}^{n^c}$ has a probability $\frac{1}{2^{n^c}}$ of appearing.

   Show how to use r to construct a random permutation generator; that is, a random function $\pi : \mathbb{N} \longrightarrow S$ where $\pi(n) \in S_n$. Here S_n denotes the set of $n!$ permutations $\sigma : [n] \longrightarrow [n]$.

   In your construction try to make c as small as possible; i.e., use as few random bits as possible. Also, make sure that the permutations are uniformly distributed.

2. Show how to combine DH key-agreement with the authentication technique used in the "3-way protocol" to obtain a key-exchange protocol, with authentication, and with forward secrecy.

3. Suppose E sees your RSA signature on m_1 and on m_2, that is, E sees $m_1^l \pmod n$ and $m_2^l \pmod n$. How can E now compute the signature of any $m_1^i m_2^j \pmod n$, for any $i, j \in \mathbb{Z}$? How can we prevent this?

4. A divulges a public key $\langle n, v \rangle$ where n is the product of two large primes (just like in RSA), and v is a number for which only A knows the square root $\pmod n$: A simply chooses a random r and squares it $\pmod n$ to obtain v.

   To prove its identity to B, A does the following: choose random numbers $r_1, r_2, \ldots, r_k$ and sends $r_i^2 \pmod n$ to B. Then B chooses a subset S_1 of the "squared-and-modded" r_i's, and lets S_2 be the complement of S_1. Now A sends:

   $$\begin{cases} sr_i \pmod n & \text{for each } r_i^2 \pmod n \text{ in } S_1 \\ r_i \pmod n & \text{for each } r_i^2 \pmod n \text{ in } S_2 \end{cases}$$

   and B squares the replies of $A \pmod n$. For the replies corresponding to S_1 B checks that the square of the reply is $vr_i^2 \pmod n$ and for those in S_2 that it is $r_i^2 \pmod n$.

   You may assume that squaring $\pmod n$ is as difficult as factoring; show that this authentication scheme works. In particular, if some C overhears the exchange, why is it that C cannot impersonate A?

5. A and B use elliptic Diffie-Hellman key exchange with the following parameters:

   $$p = 2671 \qquad E : y^2 = x^3 + 171x + 853 \qquad p = (1980, 431) \in \mathbb{Z}_p$$

   A sends the point $p_A = (2110, 543)$ to B; B on the other hand, decides to use the secret key $b = 1943$.

   (a) What point p_B does B send to A?

   (b) What is the secret share value of A and B?

   (c) Write a simple script, in any language of your choice, to find a.

6. The instructor has a GPG public key with ID `9B070A58`. This key can be retrieved from the PKI (Public Key Infrastructure), on the `https://pgp.webtru.st/` server. Please type your assignment in LaTeX and encrypt the resulting PDF with this key, and email it to the instructor.