Edoardo Persichetti Lecture 3: Discrete Logs 05/03/2014

Exercise 1 Suppose the ElGamal signature scheme was used to sign non-hashed messages $m \in \mathbb{Z}_N$. Show that is is easy to produce a forgery in this case (by just using the public key).

Exercise 2 On average, the BSGS algorithm finds a collision after performing half the giant steps, so that the average-case running time is $3/2\sqrt{N}$ group operations. The numbers of stored elements is $\sqrt{N}$ (List 1). Show how to obtain an algorithm that requires. in the average case, approximately $\sqrt{2N}$ group operations and $\sqrt{N/2}$ elements of storage.

Exercise 3 Check that $F(t) = t^2 e^{-t^2/2}$ has continuous derivative.

Exercise 4 Evaluate the integral $\int_0^\infty t^2 e^{-t^2/2} dt$.

Hint: use integration by parts first, and then polar coordinates.

Theorem 1 (Birthday Paradox) *In a room with at least 23 people, two of them will have the same birthday with probability at least 1/2.*

Exercise 5 Determine what is the minimum number of elements that need to be sampled from S in order to get a collision with probability 1/2. Then, prove the Birthday Paradox.

Exercise 6 Show how to apply the Pollard's ρ algorithm to the factoring problem.