Foundations of Cryptography

Homework Set No. 8

Date Due: Januray 15th 2004

1. Let $c : \{0,1\}^* \mapsto \{0,1\}^*$ be a good error correcting code:

- Encoding is polynomial time
- The distance between any two codewords $c(x)$ and $c(x')$ is a constant fraction of $|c(x)|$ and furthermore It is possible to correct in polynomial time errors in a constant fraction of c of the locations.

Show that for $h(x,i) = c(x)_i$ (the ith bit of the c coding of x) and any one-way function f, no polynomial time algorithm A(y,i) can have probability of success better than a constant of computing $h(x,i)$ given $y = f(x)$ and i.

2. The Diffie Hellman (DH) Assumption for a (sequence) of group G_n: given g and $a = g^x$ and $b = g^y$ no polynomial time machine can find $c = g^{xy}$ with non-negligible probability. Show that under the DH Assumption Given $g, a = g^x, b = g^y$ and $r \in \{0,1\}^n i$ no polynomial time machine can guess the inner product of r and (bit representation of) g^{xy} with non-negligible advantage. This is for random x, y and r.