CS206: Applied E-commerce **Spring 2002**

Assignment #6

Due: Tuesday, May 28th, 2002.

Problem 1. Anonymous digital cash has the property that if a user double spends a coin, the user's identity is exposed. In some applications a user should be allowed to spend a single coin n times (as opposed to just once). If the user spends the same coin $n+1$ times, the user's identity is exposed with probability $1-\epsilon$ for arbitrarily small $\epsilon > 0$ (assume ϵ is known ahead of time). If the user spends the coin n or fewer times she remains anonymous. Show how to extend the protocol described in class to accommodate this scenario. (note that the user should not be asked to maintain state between different spendings of the same coin).

More about digital cash:
David Chaum: Achieving Electronic Privacy; Scientific American, August 1992, 96-101.
B. Schneier, Applied Cryptography, Second edition, Section 6.4
S. Brands, `http://ntrg.cs.tcd.ie/mepeirce/Project/Mlists/brands.html`
Micropayments. Payword: `http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.pdf`

Problem 2. The recording industry decides to embed a set of keys in every CD player it ships. The embedded keys are some subset of a set $K = \{K_1, \ldots, K_n\}$ of keys. Say, the i'th recorder (for $i = 1, \ldots, m$) is given all keys in the set $S_i \subseteq K$. Initially, every CD shipped contains music encrypted under all keys in K. This means all CD players can play the CD. Now, if CD player i is broken into and the keys in S_i are exposed, the recording industry will encrypt all future CD's using $K \setminus S_i$. This disables the pirated keys and pirated CD players derived from these keys from playing this music. Clearly, we should avoid disabling any other CD players.

a. Fix some value $t > 0$. Show that if for any $i \in \{1, \ldots, m\}$ and any $j_1, \ldots, j_t$ not containing i we have:

$$S_i \setminus \{S_{j_1} \cup \ldots \cup S_{j_t}\} \neq \emptyset$$

then up to t pirated CD players can be safely disabled without any legitimate CD players breaking down.

b. Fix the number of users m. Show how to construct the sets $S_1, \ldots, S_m$ satisfying part (a) for $t = 1$ and $n = O(\log m)$.

c. Fix the number of users m. Show how to construct sets $S_1, \ldots, S_m$ for $t = 2$ and $n = O(\log^2 m)$. If you cannot achieve $n = O(\log^2 m)$ give a construction for the smallest n you can achieve.