1 Problem 1

The protocol differs from that presented in class in that the user’s identity is divided into \( n+1 \) pieces rather than 2 pieces, and the spending and deposit protocols are modified accordingly:

\[
ID = ID_1 \oplus ID_2 \oplus \cdots \oplus ID_{n+1}
\]

As long as the user doesn’t overspend, her anonymity is obviously preserved. If she spends the coins \( n+1 \) times (or more), her identity should be exposed with probability \( 1 - \epsilon \). The main difficulty was to determine the number of times \( k \) that the user’s identity should be split into \( n+1 \) pieces to ensure that probability of \( 1 - \epsilon \). In the original scheme, \( k \) was fixed: \( k = 100 \). Now, we want to determine \( k \) as a function of \( n \) and \( \epsilon \).

If the user spends the coin \( n+1 \) times, the bank knows \( n+1 \) values chosen uniformly independently at random from the set \( \{ID_j\} \). The probability that these \( n+1 \) values are all distinct is:

\[
p = \frac{\text{choices of (n+1) distinct values}}{\text{all choices of (n+1) values}} = \frac{(n+1)!}{(n+1)^{n+1}}
\]

If we repeat this \( k \) times, the probability that the \( n+1 \) values are never distinct is \( \epsilon = (1 - p)^k \) and thus

\[
k = \frac{\log \epsilon}{\log(1 - p)}
\]

If we replace the value for \( p \) in this equation and simplify with Stirling’s formula for approximating factorials, we get:

\[
k \approx -e^{n+1} \log \epsilon
\]

This shows that \( k \) grows exponentially with \( n \). While our solution works well for small values of \( n \), it is not very scalable.

2 Problem 2

Part a:
The equation says that after revoking \( t \) pirated CD players, every player that was not revoked has at least one key not known to the revoked players. This key can be used to encrypt future content.
Part b:
Start with a set of $n$ keys and give each player a different subset of these keys of size $n/2$ (assume $n$ even). It is easy to verify that this family of subsets satisfies the condition of 2a for $t = 1$. Indeed, a subset of $n/2$ keys can never be fully contained within a different subset of the same size. The number of players we can support is:

$$m = \binom{n}{n/2} = \frac{n!}{(n/2)!/(n/2)!}$$

Stirling’s approximation for factorials gives:

$$n! \approx \sqrt{2\pi n}(n/e)^n$$

This allows us to simplify the formula for $m$:

$$m \approx 2^n \sqrt{\frac{2}{\pi n}}$$

And thus $\log m \approx n - 1/2 \log n$ which shows $n = O(\log m)$.

Part c:
Start with a set of $n^2$ keys indexed by $(i, j)$ for $1 \leq i, j \leq n$. Pick for each player a different subset $S$ of the integers in the range $[1:n]$ such that the subset $S$ is of size $n/2$. Give each player all the keys $(i, j)$ for which $i \in S$ and $j \in S$.

It is easy to convince yourself that the family of sets thus defined satisfies the condition of 2a for $t = 2$. Suppose users $A$ and $B$ have been revoked. Consider user $C$. Since $S_A \neq S_C$, there is at least an index $i$ which belongs to $S_C$ but not to $S_A$. Similarly, there exists an index $j$ which belongs to $S_C$ but not to $S_B$. The key $(i, j)$ is known to $C$, but not to $A$ or $B$.

The number of players supported by this scheme is as in 2b. Therefore $n = O(\log m)$ and the total number of keys is $n^2 = O(\log^2 m)$. 