Problem 0. Let $m_0$ be the message attack at dawn and $m_1$ be the message attack at dusk, and let $c_0, c_1$ be the corresponding ciphertexts. Since the message is encrypted using a one-time pad, say, $p$, we have:

$$c_0 = m_0 \oplus p$$

So we can obtain the one-time pad by XORing the ciphertext with the plaintext:

$$p = c_0 \oplus m_0$$

and, from there, it is easy to encrypt the new message:

$$c_1 = m_1 \oplus p = m_1 \oplus (c_0 \oplus m_0) = c_0 \oplus (m_0 \oplus m_1)$$

by XORing the first ciphertext with the XOR of the two plaintexts. Since the two plaintexts are identical until the last three characters, their XOR is zero until the last three characters, which are $awn \oplus usk = 61776e \oplus 75736b = 140405$. Then:

$$09e1c5f70a65ac51626bc3d25f17 \oplus 00 \cdots 00140405 = 09e1c5f70a65ac51626bc3c65b12.$$ 

Problem 1. (a) Alice can first pick a random key $K$ to encrypt the message $M$, and then she encrypts the key $K$ with both $K_{AB}$ and $K_{AC}$. In other words, Alice does the following:

$$E_{K_{AB}}[E_{K_{AC}}(K)] \ || \ E_K(M)$$

header

(b) Similar to Part (a), Alice does the following:

$$E_{K_{AB}}[E_{K_{AC}}(K)] \ || \ E_{K_{AB}}[E_{K_{AD}}(K)] \ || \ E_{K_{AC}}[E_{K_{AD}}(K)] \ || \ E_K(M)$$

header

(c) It is straightforward to generalize the above scheme to the case where any $k$ out of the $n$ recipients can decrypt, but any $k-1$ cannot. The length of the header would be $\binom{n}{k} = n! / k! (n-k)!$. Note that we have the inequalities:

$$\binom{n}{k} \leq \binom{n}{k} \leq \binom{ne}{k}$$

This shows that the proposed solution scales poorly.

Problem 2. (a) Let nodes $v_1, \ldots, v_{\log_2 n}$ be the nodes along the path from the root of the tree to leaf node number $r$. Since the tree is binary every node $v_i$ for $i = 2, \ldots, \log_2 n$ has exactly one sibling. Let
$u_2, u_3, \ldots, u_{\log_2 n}$ be the siblings of nodes $v_2, \ldots, v_{\log_2 n}$. Let $K_2, \ldots, K_{\log_2 n}$ be the AES keys associated with the nodes $u_2, \ldots, u_{\log_2 n}$. The header will contain the encryption of the content-key $K$ under all keys $K = \{K_2, \ldots, K_{\log_2 n}\}$. Clearly player number $r$ cannot decrypt the movie since it does not have any of the keys in $K$. However, any other player $t \neq r$ can decrypt the movie. To see this, consider the path from the root of the binary tree to leaf node $t$. Let $u$ be the highest node along this path that does not appear on the path from the root to leaf node $r$. Then the key $K_u$ associated with node $u$ is in the set $K$ (since the sibling of $u$ is a on the path to $r$). Furthermore, player $t$ contains the key $K_u$ and it can therefore obtain the content-key and then the movie. Hence, player $r$ cannot play the movie, but all other players can.

(b) For $i = 1, \ldots, k$ let $U_i$ be the set of consecutive leaves in the range $[r_i + 1, r_{i+1} - 1]$ (we are assuming $r_0 = 0$ and $r_k + 1 = n + 1$). For an internal node $v$ in the binary tree let $S_v$ be the set of leaves in the subtree rooted at $v$. We say that a set of leaves $U_i$ is exactly covered by internal nodes $v_1, \ldots, v_k$ if $U_i = \bigcup_{j=1}^{k} S_{v_j}$. We show below that each set $U_i$ can be exactly covered by a set of at most $2 \cdot \log_2 n$ internal nodes. This means that to exactly cover all sets $U_0, \ldots, U_r$ we need at most $c = 2(r+1) \log_2 n$ internal nodes. Let $v_1, \ldots, v_c$ be the internal nodes needed to cover all of $U_0, \ldots, U_r$. If we encrypt the content-key using the keys $K_i$ associated with each of these nodes then all players other than those in $R$ can recover the content-key while the players in $R$ cannot. This shows that using header containing at most $2(r+1) \log_2 n$ ciphertexts we can revoke all players in $R$ without affecting any of the other players.

It remains to show that given a set of consecutive leaves $U$ in some range $[a, b]$ it is possible to exactly cover $U$ using at most $2 \cdot \log_2 n$ internal nodes. Let $u_1$ be the highest node in the tree so that the subtree rooted at $u_1$ has leaf $a$ as its left most leaf, and all of the leaves in the subtree are contained in $[a, b]$. Let $v_1$ be the highest node in the subtree rooted at $v_1$ that has leaf $b$ as its rightmost leaf. Now, for $i = 2, \ldots, \log_2 n$ define $u_i$ to be the right sibling of the parent of $u_{i-1}$ (the right sibling of a node $w$ is the node at the same height as $w$ which is immediately on the right of $w$). Similarly, define $v_i$ to be the left sibling of the parent of $v_{i-1}$. Let $j$ be the smallest value so that $u_j = v_j$ or that $u_j, v_j$ are adjacent siblings in the tree. Then it is easy to see that $u_1, u_2, \ldots, u_j, v_j, v_{j+1}, \ldots, v_1$ is an exact cover of $[a, b]$. This covering set contains at most $2 \cdot \log_2 n$ nodes as required.

**Problem 3.** (a) First, we claim that any encryption scheme where the length of the ciphertext is the same as that of the plaintext must be deterministic. If the length of the plaintexts is $n$, then there are $2^n$ possible plaintexts and ciphertexts. Suppose that the encryption scheme is not deterministic, that is, that there exists a message $m$ with two ciphertexts $c \neq c'$. Let $M'$ be the subset of messages in the message space not equal to $m$ and let $C'$ be the subset of ciphertexts in the ciphertext space not equal to $c, c'$. Clearly, $|C'| < |M'|$. By correctness of the encryption scheme, the encryption function can only map elements in $M'$ to elements in $C'$. By pigeonhole principle, there must exist messages $m_1 \neq m_2 \in M'$ such that $\text{Enc}(m_1) = \text{Enc}(m_2)$, which contradicts the correctness property of the encryption scheme. Thus, each message in the message space can only be mapped onto one unique ciphertext in the ciphertext space, and we conclude that the encryption scheme is deterministic. As we have seen, deterministic encryption is trivially broken under a CPA-attack.

(b) Consider the following CPA adversary:

1. For $i = 1, \ldots, 2^{\ell/2}$, submit the CPA-query $(0^n, m_i)$ where the $m_i$ are arbitrary messages where $m_i \neq m_j$ for all $i \neq j$. Let $\{c_1, \ldots, c_{2^{\ell/2}}\}$ be the set of ciphertexts returned by the challenger.

2. Output $1$ if there exists $i \neq j$ such that $c_i = c_j$, and $0$ otherwise.

Consider the advantage of this adversary. In World 0, the adversary receives $2^{\ell/2}$ encryptions of $0^n$. Since each message is mapped onto exactly $2^\ell$ ciphertexts, with at least constant probability (around 0.4), the
adversary will obtain two ciphertexts $c_i, c_j$ where $c_i = c_j$ and $i \neq j$. This follows from the fact that the encryption scheme is stateless (so each ciphertext is an independent draw from some distribution over the $2^\ell$ possible ciphertexts for each message), and the birthday bound (even if the distribution of ciphertexts were non-uniform, the bound still holds, since the collision probability only increases with a non-uniform distribution). In World 1, the adversary receives encryptions of $2^{\ell/2}$ distinct messages, so it will never obtain two ciphertexts $c_i = c_j$ with $i \neq j$ (by correctness of the encryption scheme). Thus, the distinguishing advantage of this adversary is constant and non-negligible.

Problem 4. (a)

- We have $\Pr[W_0] = 1 = \Pr[W_1]$. Thus, $\text{Adv}(A_1) = |1 - 1| = 0$.
- We have $\Pr[W_0] = \frac{1}{2} = \Pr[W_1]$. Thus, $\text{Adv}(A_2) = |\frac{1}{2} - \frac{1}{2}| = 0$.
- We have $\Pr[W_0] = \frac{1}{2}$ and $\Pr[W_1] = 0$ so $\text{Adv}(A_3) = |\frac{1}{2} - 0| = \frac{1}{2}$.
- We have $\Pr[W_0] = \frac{1}{2}$ and $\Pr[W_1] = 1$ so $\text{Adv}(A_4) = |\frac{1}{2} - 1| = \frac{1}{2}$.
- We have $\Pr[W_0] = \frac{1}{2} + \frac{1}{2} = \frac{1}{2}$ and $\Pr[W_1] = \frac{1}{2}$, so $\text{Adv}(A_5) = |\frac{3}{4} - \frac{1}{2}| = \frac{1}{4}$.

Observe that any adversary that ignores the information from the coin toss has advantage 0.

(b) Let $X$ be the value that the adversary receives from the challenger. This is the only information that the adversary receives, so his/her actions can only be be a (probabilistic) response conditioned on $X$. That is, the adversary’s strategy is determined by selecting the following independent values:

- $P_H = \Pr[\text{output 1} \mid X = \text{HEADS}]$
- $P_T = \Pr[\text{output 1} \mid X = \text{TAILS}]$

We can now break the advantage into cases:

$$
\text{Adv} = \left| \Pr[W_0] - \Pr[W_1] \right|
= \left| \left( \frac{1}{2}P_H + \frac{1}{2}P_T \right) - \left( 0 \cdot P_H + 1 \cdot P_T \right) \right|
= \left| \frac{1}{2}(P_H + P_T) - P_T \right|
= \frac{1}{2} \left| P_H - P_T \right|
$$

Since $P_H, P_T \in [0, 1]$ are probabilities, the maximum difference between them is 1, and the advantage is at most $1/2$. Note also that the adversaries $A_3$ and $A_4$ from part (a) achieve this, so in fact $1/2$ is in fact the maximum possible advantage.

Problem 5. (a) Let $n$ be the block size for the encryption scheme, and let $F$ be the block cipher used for CBC-encryption. For instance, $n = 128$ for AES-128. Construct the following CPA-adversary:

1. Send a single-block query $(0^n, 0^n)$ to the challenger. The challenger replies with a ciphertext $c_0$.  
3
2. Send a single-block query \((c_0, c_0)\) to the challenger. The challenger replies with a ciphertext \(c_1\).

3. Send a single-block query \((c_1, c')\) where \(c' \neq c_1\) is an arbitrary element of the message space. The challenger replies with a ciphertext \(c_2\).

4. Output 1 if \(c_2 = c_1\).

Clearly, this is an efficient adversary. We now show that it achieves advantage 1 in the CPA security game. Consider the second CPA-query \((c_0, c_0)\). By construction, the challenger will use \(c_0\) as the IV used to encrypt the query message \(c_0\), and so, we have that \(c_1 = F(k, c_0 \oplus c_0) = F(k, 0^n)\). Note that \(c_1\) will be used as the IV in the final CPA-query. Consider the challenger’s response to the third CPA query:

- In World 0, the challenger will encrypt \(c_1\) using the IV \(c_1\) which yields \(c_2 = F(k, c_1 \oplus c_1) = F(k, 0^n) = c_1\). In this case, the adversary outputs 1 with probability 1.

- In World 1, the challenger will encrypt \(c' \neq c_1\) using the IV \(c_1\) which yields \(F(k, c_1 \oplus c')\). Since \(c_1 \neq c'\), \(c_1 \oplus c' \neq 0^n\), and since \(F\) is a PRP, \(c_2 \neq c_1\). Thus, the adversary outputs 1 with probability 0.

We conclude that the adversary has distinguishing advantage exactly 1.

(b) Apply the PRP to the last block of the previous ciphertext using a new key before using it as the IV. In order to predict the IV, the adversary would have to guess the output of a PRP. Security of the PRP implies that the adversary is able to do so with negligible probability.

(c) Consider the following CPA-adversary:

1. Send a single-block query \((0^n, 0^n)\) to the challenger. The challenger replies with \((IV', c_0)\).

2. Send a single-block query \((0^n, 1^n)\) to the challenger. The challenger replies with \((IV', c_1)\).

3. The adversary outputs 1 if \(IV = IV'\) and \(c_0 = c_1\), and 0 otherwise.

Again, the adversary is clearly efficient. We argue that the advantage of this adversary is \(\frac{1}{2^n}\). The IV is chosen independently and uniformly at random in both worlds so the probability that \(IV = IV'\) is \(\frac{1}{2^n}\). In World 0, if \(IV = IV'\), then \(c_0 = c_1\), so the adversary outputs 1 with probability \(\frac{1}{2^n}\). In World 1, if \(IV = IV'\), then \(c_0 \neq c_1\), so the adversary outputs 1 with probability 0. We conclude that the adversary’s advantage is exactly \(\frac{1}{2^n}\).

**Problem 6. (a)** A 1-query adversary can break the PRF with advantage \(1/2\) using the following strategy in the PRF security game:

- Query \(x = 0^n\) and receive \(y = F(k, x)\).

- Output \(b = 1\) if \(y\) ends in 0, and 0 otherwise.

The advantage is:

\[
\left| Pr[EXP(0) = 1] - Pr[EXP(1) = 1] \right| = \left| 1/2 - 1 \right| = \frac{1}{2},
\]

which is clearly non-negligible.

(b) Suppose we have an efficient adversary \(A\) that can break \(F_2\) with non-negligible advantage. We can construct an adversary \(B\) that breaks \(F\) as follows:
1. Start running adversary $A$.

2. Whenever $A$ issues a query for $x$, forward $x \oplus 1^n$ to the challenger. The challenger replies with a value $y$. Send $y$ to $A$.

3. Output the same guess $b$ as $A$ outputs.

We claim that $B$ perfectly simulates the view $A$ expects when interacting with a PRF challenger for $F_2$:

- In World 0 (PRF world), on a query $x$, $A$ receives from $B$ the value $F(k, x \oplus 1^n) = F_2(k, x)$.
- In World 1 (random), on a query $x$, $A$ receives from $B$ a truly random value $y$.

In both cases, $A$’s view of the PRF game is consistent with what it would expect had it been interacting with the real challenger for $F_2$. We conclude then that $B$’s distinguishing advantage is equal to that of $A$, which is non-negligible. But this contradicts the assumption that $F$ is a secure PRF, so we conclude that $A$ cannot exist, or equivalently, that $F_2$ is secure.

(c) Let $k_3 = k \parallel v$, where $k \in \{0, 1\}^n$ and $v$ is randomly selected from $\{0, 1\}$. Now, define:

$$F_3(k_3, x) = \begin{cases} F(k, x) & x \neq 0^n \\ v \parallel \text{the first } n - 1 \text{ bytes of } F(k, x) & x = 0^n \end{cases}$$

If the adversary knows $v$, we can construct an adversary that achieves advantage $\frac{1}{2}$, as follows:

- Query at $0^n$ to obtain a string $y$.
- Output $b = 1$ if the first bit of $y$ is $v$; otherwise, output 0.

In World 0 (PRF), an adversary that knows $v$ outputs 1 with probability 1. In World 1, an adversary that knows $v$ will output 1 with probability $\frac{1}{2}$, so the adversary’s overall advantage is $\frac{1}{2}$, which is certainly non-negligible.

To see that $F_3$ is secure if the adversary does not know the bit $v$, we show the contrapositive. Suppose we have an efficient adversary $A$ that can break $F_3$; we use $A$ to construct an adversary $B$ for $F$ as follows:

- Choose a random bit $v$ from $\{0, 1\}$.
- Start running $A$.
- Whenever $A$ makes a query $x$, forward $x$ to the challenger. The challenger replies with a string $y$. If $x = 0^n$, forward $v \parallel$ the first $n - 1$ bits of $y$ to $A$. Otherwise, forward $y$ to $A$.
- Output whatever $A$ outputs.

It’s clear that if $A$ is efficient, then $B$ is also efficient. Finally, we demonstrate that $B$ perfectly simulates the view $A$ expects when interacting with a PRF challenger for $F_3$:

- In World 0 (PRF world), on a query $x$, $A$ receives from $B$ the value $F(k, x) = F_3(k, x)$ when $x \neq 0^n$. When $x = 0^n$, $A$ receives $v \parallel$ the first $n - 1$ bits of $F(k, 0^n) = F_3(k, 0^n)$. Note also that $v$ is properly distributed (uniform).
• In World 1 (random), on a query $x$, $\mathcal{A}$ receives from $\mathcal{B}$ a truly random value $y$. Even if the adversary queried at $0^n$, $\mathcal{B}$ chose $v$ uniformly at random, so the result is still properly distributed.

Since $\mathcal{B}$ perfectly simulates the view of $\mathcal{A}$ when interacting with a PRF challenger for $F_1$, we conclude that $\mathcal{B}$’s distinguishing advantage is equal to that of $\mathcal{A}$, which concludes the proof.

(d) Let $F_4((k_1,k_2),x) = F(k_1 \oplus k_2, x)$. We show that $F_4$ is secure even if an adversary learned a single bit of $(k_1,k_2)$. Without loss of generality, suppose we have a PRF adversary $\mathcal{A}$ that can win the PRF game against $F_4$ if it learned a single bit of $k_1$. We can construct an adversary $\mathcal{B}$ for $F$ that operates as follows:

1. Start running adversary $\mathcal{A}$. Whenever $\mathcal{A}$ makes a query $x$, forward $x$ to the challenger. Send the challenger’s response $y$ to $\mathcal{A}$.

2. Output whatever $\mathcal{A}$ outputs.

Consider the adversary’s view in World 0 (PRF world). On a query $x$, adversary $\mathcal{A}$ is given $F(k, x)$ where $k$ is uniformly chosen from the key-space. It expects to see $F_4((k_1,k_2),x)$, where $k_1,k_2$ are both uniform over the key-space. Since $\mathcal{A}$ only knows a single bit of $k_1$, $k_1 \oplus k_2$ is uniformly distributed (since $k_2$ is uniform and independent of $k_1$). Thus, $F_4((k_1,k_2),x) = F(k_1 \oplus k_2, x)$ is identically distributed as $F(k, x)$ where $k$ is uniform. The adversary’s view in World 1 (random) is also correctly simulated, so we conclude that the distinguishing advantage of $\mathcal{B}$ is equal to that of $\mathcal{A}$.