Pham Hoang Long Do
NetID: 2995060

Homework 3

CSE 3400
Ghada Almashaqbeh

Problem 1

1. Charlie's claim is **true** since we are not using the same key to encrypt each segment of the message again. Therefore, a CPA attacker can't recognize the pattern if a message has repeated words since repeated words use different key to encrypt so the ciphertext will be different. $E^i_{k_i}(m_i) \neq E^j_{k_j}(m_j)$ where $m_i = m_j$ since $k_i \neq k_j$
2. Ronald's claim is **true** since giving the attacker the advanced knowledge of $c_0(IV)$ doesn't let him gain advatage of knowing any information about the message since the security of the encryption scheme still rely on the key. The attacker will know about c_i where $i \in 0, 1, 2, 3, ..$ but without the knowledge of the key he can't decrypt the ciphertext to know m_b where $b \in 1, 2$. Therefore, this encryption scheme is still secure agaisnt CPA attacker.
3. part 3a
   (a) OFB: The whole message will be corrupted since IV is wrong. Therefore, $pad_1, pad_2, ..., pad_t$ will be wrong. In this situation, Bob can't recover or gain any information about the message that Alice sent.
   (b) CBC: The first 5 blocks of the message will be corrupted, the rest will be fine $(m_5, m_6, ..., m_t)$ since starting from c_5, it will depend on c_4 to get the correct message and c_4 is in the right order. Therefore, only first 5 blocks will be corrupted, and the rest is good.
   (c) CTF: The entire of the message will be corrupted since the initial value of the counter is c_1 not c_0.
4. part 3b
   (a) OFB: Yes. m_1 will correct. m_2 and m_3 will be corrupted since c_2 and c_3 are out of order. The rest of the message, $m_4, ..., m_t$ will correct.
   (b) CBC: Yes. m_1 will correct, but m_2, m_3, m_4 will be corrupted since these are affected by c_2, c_3 out of orderness. The rest, $m_5, ..., m_t$ will correct.
   (c) CTF: Yes. Only m_2 and m_3 are corrupted since we have the correct initial value of the counter but c_2 and c_3 are out of order. The rest of the message will be fine m_1 and $m_4, ...m_t$.
5. part 4
   (a) If Eve dropped c_0 then on the receiver side, the initial counter value won't be received hence it's impossible to decrypt the message.
   (b) If Eve dropped c_{13} then only m_{13} will be affected, the rest of the message from $m_0, ..., m_{12}$ and $m_{14}, ..., m_{20}$ will be intact and the receiver will be able to decrpyt those blocks.
   (c) If Eve dropped c_{20} then only the last block m_{20} will be affected. The rest of the message $m_1, ..., m_{19}$ will be intact and the receiver will be able to decrpyt those blocks.
   (d) If Eve flipped the order of the ciphertext then the entire message will be corrupted since the decryption depend on the initial counter value c_0 which is now become c_{20} and c_i where $i \in 1, 2, 3, ..., 20$ but now the order is swapped.

Pham Hoang Long Do
NetID: 2995060

Homework 3

CSE 3400
Ghada Almashaqbeh

Problem 2

Let $G : \{0,1\}^{n/2} \to \{0,1\}^n$ be a PRG, and $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF. For each of the following MAC constructions, state whether it is a secure MAC and justify your answers.

1. Given message $m \in \{0,1\}^{3n/2}$, parse $m = m_0 \parallel m_1$ such that $|m_0| = n$ and $|m_1| = n/2$, then compute the tag as $MAC_k(m) = F_k(m_0) \parallel G(m_1)$.
   - This is a **secure** MAC since the tag function $MAC_k(m) = F_k(m_0) \parallel G(m_1)$ produce an output of $\{0,1\}^{2n}$ which can cover the entire message of length $\frac{3n}{2}$. Basically, we can pad $\frac{n}{2}$ length of all zeros to the front of the message. In addition, since $F_k(m_0)$ a secure MAC since every PRF is a secure MAC. We can use the concatenation property which states that as long as either F or G is a secure MAC then the output will be a secure MAC.
2. Given message $m \in \{0,1\}^n$, compute $y = F_k(m)$, parse $y = y_0 \| y_1$ such that $|y_0| = |y_1| = n/2$, then compute the tag as $G(y_0)$.
   - This is a **secure** MAC since the output of y is the output of a PRF which is pseudo random. Taking y_0 which has length of $\frac{n}{2}$ as the input of a PRG will provide a indistiguishable pseudo random output. Therefore, the tag is secure and attacker has a probability of guessing the correct tag is $\frac{1}{2^n}$.
3. Given message $m \in \{0,1\}^{2n}$, parse m as $m = m_0 \parallel m_1$ such that $|m_0| = |m_1| = n$. Compute the tag as $MAC_k(m) = (F_k(0^n), F_k(m_0 \oplus m_1))$.
   - The first part of the MAC: $F_k(0^n)$ is fixed and deterministic, so an attacker will recognize the pattern of the first part after a few queries. In stead, he will focus on the second part, lets call it tag_2. The attacker can submit a querry m where $m = m_0 \parallel m_1$ and obtain tag_2. Since Xor is communicative; therefore, $m_0 \oplus m_1 = m_1 \oplus m_0$. The attacker can sumbit back to the oracle a new message $m^{'} = m_1 \parallel m_0$ along with the tag $m_1 \oplus m_0$. This message and its tag is valid since it hasn't been recored by the oracle. Therefore, it is **not a secure** MAC in which the attacker has a success chance of 1.
4. A variation of the CMAC construction: we compute a tage as $tag = CMAC_k(m) = CBC - MAC(L(m)) \parallel CBC - MAC_k(m)$, and m is a VIL (can be of any length such that it is an integer number of blocks) and $L(m)$ is a block representing the length of the message m.
   - Let $f = CBC - MAC(L(m))$ and $g = CBC - MAC_k(m)$. This is **not a secure** MAC since neither of f and g a secure MAC. For g, we know in class that a CBC-MAC without prepend is not secure. For f, the attacker can use to different messages but with the same length. For example, he can querry m_1 and receive the tag b. Now, he can submitting his answer to the oracle by submit a new message $m_2 = c \times m_1$ where $c = m_1 \oplus b$ and $|m_2| = |m_1|$. The tag for m_2 is still b (proved in class). This is valid since the attacker did not ask for m_2 and b is a valid tag for m_2. The successful chance of this attacker is 1.