CS 435: Introduction to Cryptography **Fall 2016-17**

Homework 4 Solutions

Professor Somesh Jha

1. This question asks if a dropped ciphertext block affect the decryption of the other blocks. According to the decryption formulas (See the solution for the Question 4), **CBC** is the only mode that requires another ciphertext block, namely c_{i-1}, to decrypt the i-th ciphertext c_i. Therefore, only in **CBC** mode, missing block will affect the decryption of the next block (all the other blocks can be decrypted normally). In other modes, the missing block has no side effect on decryption.

   In conclusion, if a ciphertext block c_k is missing, **CBC** will fail to decrypt 2 blocks (c_k and c_{k+1}), whereas **OFB** and **CTR** mode will fail to decrypt one block (c_k).

2. We construct an adversary $\mathcal{A}$ that wins the indistinguishability game with non-negligible advantage. By Kerckhoffs' principle, we may assume that $\mathcal{A}$ already knows the block length n, and $\mathcal{A}$ will use messages m_0, m_1 of length $2 \cdot n$.

   Choose a string $m \in \{0,1\}^n$. Construct $2n$-bit strings m_0, m_1 as follows.

$$m_0 = (m+1)\|m$$
$$m_1 = m\|m$$

   where $+$ means an arithmetic addition modulo 2^n. Also, the choice of m_1 can be arbitrary, as long as it does not have a pattern of $(m'+1)\|m'$ for any $m' \in \{0,1\}^n$. For any ciphertext c that Π sends, $\mathcal{A}$ checks if the first half and the last half of c are identical, and output $b' = 0$ if so, $b' = 1$ otherwise.

   Now we show that this adversary wins the game with non-negligible advantage.

   If $m_0 = (m+1)\|m$ has been encrypted by Π, then

   - 1st ciphertext block $c_1 = F_k[\texttt{ctr} + 1 + (m+1)] = F_k[\texttt{ctr} + 2 + m]$ and
   - 2nd ciphertext block $c_2 = F_k[\texttt{ctr} + 2 + m]$

   should be identical for a fixed key k, so $\mathcal{A}$ outputs $b' = 0$ and always wins the game in this case.

   If $m_1 = m\|m$ has been encrypted by Π, then

   - 1st ciphertext block $c_1 = F_k[\texttt{ctr} + 1 + m]$ and
   - 2nd ciphertext block $c_2 = F_k[\texttt{ctr} + 2 + m]$

   are not same unless $F_k[\texttt{ctr} + 1 + m] = F_k[\texttt{ctr} + 2 + m]$, and for randomly chosen k and $\texttt{ctr}$, $Pr\big[F_k[\texttt{ctr} + 1 + m] = F_k[\texttt{ctr} + 2 + m]\big]$ is negligible

   Therefore, $\mathcal{A}$ loses only when $b = 1$, with negligible probability. In other words, $\mathcal{A}$ wins with probability $1 - \texttt{negl}(n)$ for some negligible function $\texttt{negl}(\cdot)$, therefore $\mathcal{A}$ wins the game with non-negligible advantage.

3. We construct an adversary $\mathcal{A}$ that wins the CPA-indistinguishability game with non-negligible advantage. By Kerckhoffs' principle, we may assume that $\mathcal{A}$ already knows the block length n, and $\mathcal{A}$ will use messages m_0, m_1 of length n.

   First, $\mathcal{A}$ choose any distinct m_0 and m_1. For any ciphertext $\langle c, IV\rangle$ that Π sends, $\mathcal{A}$ constructs a message m using m_0 and IV as,

   $$m = m_0 \oplus IV \oplus (IV + 1)$$

   then uses oracle access to compute $\mathsf{Enc}_k(m) = \langle c', IV + 1\rangle$. Finally, $\mathcal{A}$ just compares c and c', outputs $b' = 0$ if $c = c'$, and outputs $b' = 1$ otherwise.

   Now we show that this adversary wins the game with non-negligible advantage.

   Note that when we use the oracle access, $(IV + 1)$ is used as initialization vector, and we are only encrypting a single block. Therefore,

   $$\begin{aligned} c' &= F_k[m \oplus (IV + 1)] \\ &= F_k[m_0 \oplus IV \oplus (IV + 1) \oplus (IV + 1)] \\ &= F_k[m_0 \oplus IV] \end{aligned}$$

   is exactly same to the encrypted ciphertext when $b = 0$.

   If m_0 has been encrypted by Π, then $c = c'$ must hold by the equality above, so $\mathcal{A}$ can always win the game in this case.

   If m_1 has been encrypted by Π, then $c \neq c'$ unless $F_k[m_0 \oplus IV] = F_k[m_1 \oplus IV]$, and for distinct m_0, m_1, $Pr\big[F_k[m_0 \oplus IV] = F_k[m_1 \oplus IV]\big]$ is negligible.

   Therefore, $\mathcal{A}$ loses only when $b = 1$, with negligible probability. In other words, $\mathcal{A}$ wins with probability $1 - \mathtt{negl}(n)$ for some negligible function $\mathtt{negl}(\cdot)$, therefore $\mathcal{A}$ wins the game with non-negligible advantage.

4. The formulas for decryption are as follows. For detailed diagram of each decryption, you may look at the Wikipedia article about "Block cipher mode of operation" (`https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation`)

   - **ECB:** $m_i = F_k^{-1}(c_i)$
   - **CBC:** $m_i = F_k^{-1}(c_i) \oplus c_{i-1}$
   - **OFB:** $m_i = c_i \oplus o_i$ where $\begin{cases} o_0 = IV \\ o_i = F_k(o_{i-1}) \end{cases}$
   - **CTR:** $m_i = F_k(\mathtt{ctr} + i) \oplus c_i$

   The parallelizations of each decryption depend on if the decryption formula for each block contains some computation from some other blocks. **OFB** is the only mode that is not parallelizable, since $F_k(o_{i-1})$ should be computed from $(i-1)$-th block to decrypt i-th message m_i.