CS 435: Introduction to Cryptography **Spring 2020**

Homework 4

Professor Somesh Jha **Due:** April 11

1. Show the decryption logic for the four modes of operations ECB, CBC, OFB, and CTR.

   Solution:
   The formulas for decryption are as follows:

   (a) ECB $\rightarrow m_i = F_k^{-1}(c_i)$

   (b) CBC $\rightarrow m_i = F_k^{-1}(c_i) \oplus c_{i-1}$

   (c) OFB $\rightarrow m_i = c_i \oplus o_i$ where $\begin{cases} o_0 = IV \\ o_i = F_k(o_{i-1}) \end{cases}$

   (d) CTR $\rightarrow m_i = F_k(ctr + i) \oplus c_i$

   For a detailed diagram of the encryption/decryption logic check out this link: `https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation`

2. Consider a stateful variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is not CPA-secure.

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

   (a) $\mathcal{A}$ chooses an arbitrary message m and queries the oracle to get $(IV; c)$

   (b) $\mathcal{A}$ chooses two messages: $m_0 = m \oplus IV \oplus (IV + 1); m_1 =$ any arbitrary message distinct from m_0.

   (c) $\mathcal{A}$ sends them over to Π.

   (d) Π returns $(IV + 1; c')$

   (e) If $c' = c$, A outputs $b = 0$, else outputs b = 1

   Note that when we send m_0 and m_1, (IV + 1) is used as the initialisation vector, and we are only encrypting a single block. Therefore if m_0 had been encrypted,

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

If m_1 had been encrypted by Π, then $c' \neq c$ unless $F_k(m_1 \oplus (IV+1) = F_k(m \oplus IV))$, and for arbitrarily chosen m_1 and $m, Pr[F_k(m_1 \oplus (IV+1)) = F_k(m \oplus IV)]$ is negligible.

3. What is the effect of a single-bit error in the ciphertext when using the CBC, OFB, and CTR modes of operation?

   Solution: A single bit error in the cipher text basically corrupts a single cipher block. According to the decryption formulas (see the solution for question 1), CBC is the only mode that requires another ciphertext block, namely c_{i-1}, to decrypt c_i. Therefore, in CBC mode, the corrupted block will affect the decryption of the next block (all the other blocks can be decrypted normally). In other modes, the corrupted block has no effect on the decryption of other blocks. In conclusion, if a ciphertext block ck is corrupted, CBC will fail to decrypt 2 blocks (c_k and c_{k+1}), whereas OFB and CTR mode will fail to decrypt only one block (c_k).

4. Let F be a pseudorandom permutation. Consider the mode of operation in which a uniform value $ctr \in \{0,1\}^n$ is chosen, and the ith ciphertext block c_i is computed as $c_i := F_k(ctr + i + m_i)$. Show that this scheme does not have indistinguishable encryptions in the presence of an eavesdropper.

   Solution:
   We construct an adversary $\mathcal{A}$ that wins the indistinguishability game with non-negligible advantage. By Kerckhoff's principle, we assume that $\mathcal{A}$ already knows the block length n, and $\mathcal{A}$ will chose messages of length $2n$.

   (a) $\mathcal{A}$ choses a $m \in \{0,1\}^n$. Constructs $2n$-bit strings m_0 and m_1 as follows:

   $$m_0 = (m+1)||m \tag{1}$$
   $$m_1 = m||m \tag{2}$$

   where + means an arithmetic addition modulo $2n$. Sends them over to Π.

   (b) Π returns c

   (c) $\mathcal{A}$ checks if the 1st half and the 2nd half of c are identical, and if so outputs $b = 0$ else outputs $b = 1$.

   If m_0 had been encrypted then

   - 1st half of $c = F_k(ctr + 1 + (m+1)) = F_k(ctr + 2 + m)$ and
   - 2nd half of $c = F_k(ctr + 2 + m)$

   would be identical.
   If m_1 had been encrypted then

   - 1st half of $c = F_k(ctr + 1 + m)$ and
   - 2nd half of $c = F_k(ctr + 2 + m)$

   would not same be the same unless $F_k(ctr + 1 + m) = F_k(ctr + 2 + m)$, and for randomly chosen k and ctr, $Pr[F_k(ctr + 1 + m) = F_k(ctr + 2 + m)]$ is negligible.