# Applied Cryptography: Homework 5

(Deadline: 10:00am, 2020/10/21)

*Justify your answers with calculations, proofs, and programs.*

1. (10 points, question 4.8, page 132 of the textbook)

   Suppose that $X = (x_1, \ldots, x_n)$ and $X' = (x'_1, \ldots, x'_n)$ are two sequences of $n$ plaintext blocks. Define

   $$\mathbf{same}(X, X') = \max\{j : x_i = x'_i \text{ for all } i \leq j\}.$$

   Suppose $X$ and $X'$ are encrypted in CBC or CFB mode using the same key and the same IV. Show that it is easy for an adversary to compute $\mathbf{same}(X, X')$.

2. (20 points, question 4.10, page 133 of the textbook)

   Suppose a sequence of plaintext blocks, $x_1 \ldots x_n$, yields the ciphertext sequence $y_1 \ldots y_n$. Suppose that one ciphertext block, say $y_i$, is transmitted incorrectly (i.e., some $1's$ are changed to $0's$ and vice versa). Show that the number of plaintext blocks that will be decrypted incorrectly is equal to one if ECB or OFB modes are used for encryption; and equal to two if CBC or CFB modes are used.

3. (20 points, question 5.1, page 178 of the textbook)

   Define a toy hash function $h : (\mathbb{Z}_2)^7 \to (\mathbb{Z}_2)^4$ by the rule $h(x) = xA$ where all operations are modulo 2 and

   $$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

   Find all preimages of $(0, 1, 0, 1)$.

4. (10 points, question 5.8, page 181 of the textbook)

   Suppose that $f : \{0,1\}^m \to \{0,1\}^m$ is a preimage resistant bijection. Define $h : \{0,1\}^{2m} \to \{0,1\}^m$ as follows. Given $x \in \{0,1\}^{2m}$, write

   $$x = x' \| x''$$

   where $x', x'' \in \{0,1\}^m$. Then define

   $$h(x) = f(x' \oplus x'').$$

   Prove that $h$ is not second preimage resistant.