Applied Cryptography: Homework 7

(Deadline: 10:00am, 2020/11/11)

Justify your answers with calculations, proofs, and programs.

1. (15 points, question 5.14, page 182 of the textbook)

   Message authentication codes are often constructed using block ciphers in CBC mode. Here we consider the construction of a message authentication code using a block cipher in CFB mode. Given a sequence of plaintext blocks, $x_1, \ldots, x_n$, suppose we define the initialization vector IV to be x_1. Then encrypt the sequence $x_2, \ldots, x_n$ using key K in CFB mode, obtaining the ciphertext sequence $y_1, \ldots, y_{n-1}$(note that there are only $n-1$ ciphertext blocks). Finally, define the MAC to be $e_K(y_{n-1})$. Prove that this MAC actually turns out to be identical to CBC-MAC, as presented in Section 5.5.2.

2. (15 points, question 5.18, page 183 of the textbook)

   Compute Pd_0 and Pd_1 for the following authentication code, represented in matrix form:

key	1	2	3	4
1	1	1	2	3
2	1	2	3	1
3	2	1	3	1
4	2	3	1	2
5	3	2	1	3
6	3	3	2	1

3. (15 points, question 5.19, page 184 of the textbook)

   Let p be an odd prime. For $a, b \in \mathbb{Z}_p$, define $f_{(a,b)} : \mathbb{Z}_p \to \mathbb{Z}_p$ by the rule

   $$f_{(a,b)}(x) = (x+a)^2 + b \bmod p.$$

   Prove that $(\mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Z}_p \times \mathbb{Z}_p, \{f_{(a,b)} : a, b \in \mathbb{Z}_p\})$ is a strongly universal (p,p)-hash family.

4. (15 points, question 6.11, page 247 of the textbook)

   Suppose that $n = pq$, where p and q are distinct odd primes and $ab \equiv 1 (\bmod\ (p-1)(q-1))$. The RSA encryption operation is $e(x) = x^b \bmod n$ and the decryption operation is $d(y) = y^a \bmod n$. We proved that $d(e(x)) = x$ if $x \in \mathbb{Z}_n^*$. Prove that the same statement is true for any $x \in \mathbb{Z}_n$.

   HINT Use the fact that $x_1 \equiv x_2 (\bmod\ pq)$ if and only if $x_1 \equiv x_2 (\bmod\ p)$ and $x_1 \equiv x_2 (\bmod\ q)$. This follows from the Chinese remainder theorem.