EE 720: An Introduction to Number Theory and Cryptography (Spring 2019)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Quiz 1 : 20 points — February 14, 2019

1. (5 points) Consider the following private-key encryption scheme $(\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ where message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ are both equal to $\{0,1\}^n$. Let the key space $\mathcal{K}$ be the set of all $n!$ permutations of the set $\{1, \ldots, n\}$.

   - `Gen`: Choose k uniformly from $\mathcal{K}$. Let $k = (k_1, k_2, \ldots, k_n)$. For example, if $n = 4$ then $k = (2, 1, 3, 4)$ is the permutation which swaps the positions of the first two elements.
   - `Enc`: For $m \in \{0,1\}^n$, let $m[i]$ denote the ith bit of m. Output the ciphertext $c \in \{0,1\}^n$ as
   $$c := (m[k_1], m[k_2], \ldots, m[k_n]).$$
   - `Dec`: Given $k \in \mathcal{K}$ and ciphertext $c \in \{0,1\}^n$, output the message m by inverting the permutation.

   Prove that this scheme is **not EAV-secure**.

2. (5 points) Let F be a length-preserving pseudorandom function having key length, input length, and output length all equal to n bits. Consider the following keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-1} \mapsto \{0,1\}^{2n}$ defined as
   $$F'_k(x) = F_k(0\|x)\|F_k(x\|1).$$
   Prove that the F' is **not** a pseudorandom function. Here $F'_k(x) = F'(k,x)$, $F_k(y) = F(k,y)$, and $\|$ is the string concatenation operator.

3. (5 points) Let F be a length-preserving pseudorandom permutation having key length, input length, and output length all equal to n bits. The CBC mode of encryption on messages of length ln is done as follows:

   - Let $m = (m_1, m_2, \ldots, m_l)$ where $m_i \in \{0,1\}^n$.
   - An initialization vector (IV) of length n bits is first randomly chosen.
   - $c_0 = IV$. For $i = 1, \ldots, l$, $c_i \coloneqq F_k(c_{i-1} \oplus m_i)$.
   - The ciphertext $c = (c_0, c_1, \ldots, c_l)$ is given as output.

   In CBC mode, a new IV is generated randomly every time the encryption function is called. Consider a modification of the CBC mode where the sender and the receiver agree on the following protocol:

   - For the first message $m = (m_1, \ldots, m_l)$ of ln bits, the sender generates a random IV and sets $c_0 = IV$. She uses CBC mode to generate ciphertext $c = (c_0, c_1, \ldots, c_l)$.
   - The receiver decrypts c using the usual CBC mode decryption.
   - For the second message $m' = (m'_1, \ldots, m'_l)$ of ln bits, the sender sets $c'_0 = IV + 1$ where IV was the initialization vector used to encrypt the previous message m. She generates $c'_i = F_k(c'_{i-1} \oplus m'_i)$ for $i = 1, \ldots, l$ and sends $c' = (c'_1, c'_2, \ldots, c'_l)$. Note that c'_0 is not sent. This helps reduce the ciphertext length by n bits.
   - The receiver calculates $c'_0 = IV + 1$ and decrypts $(c'_0, c'_1, c'_2, \ldots, c'_l)$ using the usual CBC mode decryption.
   - For the third message $m'' = (m''_1, \ldots, m''_l)$ of ln bits, the sender sets $c''_0 = IV + 2$, generates $c''_i = F_k(c''_{i-1} \oplus m''_i)$ for $i = 1, \ldots, l$ and sends $c'' = (c''_1, c''_2, \ldots, c''_l)$.
   - The receiver calculates $c''_0 = IV + 2$ and decrypts $(c''_0, c''_1, c''_2, \ldots, c''_l)$ using the usual CBC mode decryption.
   - And so on.

   Prove that that this modified CBC mode is not CPA-secure.

4. (5 points) Let F be a length-preserving pseudorandom function having key length, input length, and output length all equal to n bits. Consider the fixed-length MAC messages of length n bits defined as follows:

   - `Mac`: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, output the tag $t \coloneqq F_k(m)$.
   - `Vrfy`: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, and a tag $t \in \{0,1\}^n$, output a 1 if and only if $t = F_k(m)$. If $t \neq F_k(m)$, output 0.

   Prove that the above construction is a **secure** fixed-length MAC for messages of length n.