EE 720: An Introduction to Number Theory and Cryptography (Spring 2020)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Quiz 1 : 20 points February 13, 2020

1. (5 points) State whether the following encryption scheme is perfectly secret or not. Justify your answer either with a proof or a counterexample.

   The message space is $\mathcal{M} = \{0, 1, 2, 3, 4\}$ and ciphertext space is $\mathcal{C} = \mathcal{M}$. Algorithm `Gen` chooses a uniform key k from the keyspace $\mathcal{K} = \{0, 1, 2, 3, 4, 5\}$. $\texttt{Enc}_k(m) = (k + m) \bmod 5$ and $\texttt{Dec}_k(c) = (c - k) \bmod 5$. Here $x \bmod 5$ is equal to $r \in \{0, 1, 2, 3, 4\}$ such that $x - r$ is divisible by 5.

2. (5 points) Prove that if $F : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}^n$ is a length-preserving pseudorandom function, then $G : \{0, 1\}^n \to \{0, 1\}^{5n}$ defined below **is a pseudorandom generator.**

   $$G(s) = F_s(1) \| F_s(2) \| F_s(3) \| F_s(4) \| F_s(5).$$

   Here $\|$ denotes the string concatenation operator. For i such that $1 \le i \le 5$, by $F_s(i)$ we mean the output of $F_s(\cdot)$ when the input is the n-bit string representing the integer i.

3. (10 points) Let $F : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}^n$ be a length-preserving pseudorandom function. Consider the encryption scheme $\Pi = (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ defined as follows:

   (i) `Gen`: Choose a key k uniformly from $\{0, 1\}^n$.

   (ii) `Enc`: Given $m \in \{0, 1\}^{2n}$ and $k \in \{0, 1\}^n$, $\texttt{Enc}_k : \{0, 1\}^{2n} \to \{0, 1\}^{3n}$ operates as follows:
   - Parse m as $\langle m_1, m_2 \rangle$ where $m_1 \in \{0, 1\}^n$ and $m_2 \in \{0, 1\}^n$.
   - Choose r uniformly from $\{0, 1\}^n$.
   - Set the ciphertext $c = \langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r + 1) \rangle$

   From $r \in \{0, 1\}^n$, $r + 1$ is obtained by interpreting r as a non-negative integer and incrementing it modulo 2^n. For example, if $n = 4$ then $r = 0010$ gives $r + 1 = 0011$. And $r = 1111$ gives $r + 1 = 0000$.

   (iii) `Dec`: Given $c = \langle r, s_1, s_2 \rangle \in \{0, 1\}^{3n}$ and $k \in \{0, 1\}^n$, $\texttt{Dec}_k : \{0, 1\}^{3n} \to \{0, 1\}^{2n}$ operates as follows:
   - Set the decrypted message $m = \langle s_1 \oplus F_k(r), s_2 \oplus F_k(r + 1) \rangle$

   Note that this scheme is a special case of the CTR block cipher mode with fixed message length. **Prove that the scheme Π is CPA-secure**. You cannot just say this scheme is CPA-secure because CTR mode is CPA-secure.