EE 720: Introduction to Number Theory and Cryptography (Spring 2018)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 2: 10 points Date: January 23, 2018

Find the pdf file corresponding to your roll number in the directory `https://www.ee.iitb.ac.in/~sarva/courses/EE720/2018/assignments/assignment2/`. Upload the answers as a **pdf** file in Moodle. The **upload deadline** will be 11:00pm IST on Wednesday, January 31, 2018.

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 $\mathcal{M} = \{0, \ldots, 4\}$. Algorithm $\texttt{Gen}$ chooses a uniform key from the keyspace $\{0, \ldots, 5\}$. $\texttt{Enc}_k(m) = (k + m) \bmod 5$ and $\texttt{Dec}_k(c) = (c - k) \bmod 5$.

2. [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 $\mathcal{M} = \big\{m \in \{0,1\}^l \mid \text{the last bit of } m \text{ is } 0\big\}$. Algorith $\texttt{Gen}$ chooses a uniform key from the keyspace $\{0,1\}^{l-1}$. $\texttt{Enc}_k(m) = m \oplus (k \| 0)$ and $\texttt{Dec}_k(c) = c \oplus (k \| 0)$.

3. [5 points] When the one-time pad is used with the all-zeros key, i.e. $k = 0^l$, we have $\texttt{Enc}_k(m) = m \oplus k = m$. This means that the plaintext will be sent as it is. To prevent this, suppose we modify the one-time pad to use only non-zero keys, $k \neq 0^l$. The key generation algorithm $\texttt{Gen}$ picks key k uniformly from the set $\{0,1\}^l \setminus \{0^l\}$ which has cardinality $2^l - 1$. Is this modified scheme still perfectly secret? Justify your answer either with a proof or a counterexample.

4. [5 points] Consider a variant of the one-time pad with message space $=\{0,1\}^l$ and keyspace $\mathcal{K}$ restricted to all l-bit strings with an even number of 1's. Is this scheme perfectly secret? Justify your answer either with a proof or a counterexample.

5. [5 points] Prove that if only a single character is encrypted, then the shift cipher is perfectly indistinguishable. Prove this directly without proving the perfect secrecy of the scheme and then using the equivalence of perfect secrecy and perfect indistinguishability.

6. [5 points] Prove that the Vigenére cipher using period t is perfectly indistinguishable when used to encrypt messages of length t. Prove this directly without proving the perfect secrecy of the scheme and then using the equivalence of perfect secrecy and perfect indistinguishability.

7. [5 points] Let $\texttt{negl}_1$ and $\texttt{negl}_2$ be negligible functions. Prove that the function $\texttt{negl}_3$ defined by $\texttt{negl}_3(n) = \texttt{negl}_1(n) + \texttt{negl}_2(n)$ is negligible.

8. [5 points] Let $\texttt{negl}_1$ be a negligible function. Prove that for any positive polynomial p, the function $\texttt{negl}_2$ defined by $\texttt{negl}_2(n) = p(n) \cdot \texttt{negl}_1(n)$ is negligible.