EE 418 - Problem Set 2

Total Points: 80/80
Autumn Quarter, 2017
Department of Electrical Engineering
University of Washington, Seattle, WA 98195

Assigned: Oct 17th (Tue); Due: in class, Oct 26th (Thur)

Readings: Chapter 1 of D. Stinson, 3rd Edition.

1. (Permutation Cipher, 5 pts x 2)
   (a) Prove that a permutation $\pi$ in the Permutation Cipher is an involuntary key if and only if $\pi(i) = j$ implies $\pi(j) = i$, for all $i, j \in \{1, 2, ..., m\}$.
   (b) Determine the number of involuntary keys in the Permutation Cipher for $m = 2, 3, 4, 5$ and 6.

2. (Steam Cipher, 10 pts) Consider the following linear recurrence over $\mathbb{Z}_3$ of degree three:
   \[ z_{i+3} = (z_i + z_{i+2}) \mod 3, \] (1)
   where $i \geq 0$. For each of the 8 possible initialization vectors $(z_0, z_1, z_2) \in (\mathbb{Z}_3)^3$, determine the period of the resulting key stream.

3. (Steam Cipher, 10 pts) Consider a linear feedback shift register that works mod 3 instead of mod 2, so that the $(i + m)$-th element of the key stream is given by
   \[ z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \mod 3. \] (2)
   Let a recurrence of length $m = 2$ be used to generate the sequence 1, 1, 0, 2, 2, 0, 1, 1. Compute the next four elements of the key stream. (Exam #1, Fall 2012)

4. (Cryptanalysis of Vigenere Cipher, 20 pts) Given the following ciphertext from a Vigenere Cipher, your task is to determine the plaintext.
   Give a clearly written description of the steps you followed to decrypt the ciphertext. This should include all statistical analysis and computations you performed.
5. (Cryptanalysis of Hill Cipher, 10 pts) Suppose we are told that the plaintext 

\textit{breathtaking}

yields the ciphertext

\textit{RUPOTENTOIFV}

where the Hill Cipher is used (but \(m\) is not specified). Determine the encryption matrix.

6. (Stream Cipher, 10 pts) Given the plaintext and corresponding ciphertext generated using stream cipher

\[\begin{align*}
\text{Plain} &= [1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1]
\text{Cipher} &= [1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0]
\end{align*}\]

Find the 5-stage linear recurrence used to generate the key stream.

7. (10 pts) In the Euclidean Algorithm (Fig. 1 in Handout 2, or Algo. 5.1 on Pg. 164 of Stinson), prove that

\[\gcd(r_0, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{m-1}, r_m) = r_m\]

and hence, \(r_m = \gcd(a, b)\).