Cryptology: Problem Sheet 1

Topic: Classical Ciphers and Perfect Secrecy

1. If an encryption function Enc_K is identical to the decryption function Dec_K, then the key K is said to be involutary. Suppose $K = (a, b)$ be a key in an Affine cipher over $\mathbb{Z}_n$. Prove that K is an involutary key if and only if $a^{-1} \mod n = a$ and $b(a+1) \equiv 0 \mod n$.

2. Prove or Refute: An encryption scheme with message space $\mathcal{M}$ is perfectly secret if and only if for every probability distribution over $\mathcal{M}$ and every $c_0, c_1 \in \mathcal{C}$, we have

$$\mathsf{Pr}[C = c_0] = \mathsf{Pr}[C = c_1].$$

3. Consider an encryption scheme with the message space

$$\mathcal{M} = \{m \in \{0,1\}^n | \text{ the last bit of m is } 0\}.$$

   Gen chooses a uniform key from $\{0,1\}^{n-1}$. $\mathsf{Enc}_k(m)$ returns ciphertext $m \oplus (k\|0)$, and $\mathsf{Dec}_k(c)$ returns $c \oplus (k\|0)$. State and explain whether the above scheme is perfectly secret.

4. For the following encryption scheme, justify whether the scheme is perfectly secret or not. Assume that the message (and ciphertext) space is $\mathcal{M} = \mathcal{C} = \{0, \ldots, 4\}$.

   - Gen returns a key K chosen uniformly at random from the key space $\mathcal{K} = \{0, \ldots, 5\}$.
   - $\mathsf{Enc}_K(M)$ returns $[K + M \mod 5]$.
   - $\mathsf{Dec}_K(C)$ returns $[C - K \mod 5]$.

5. Let Π be an arbitrary scheme with $|\mathcal{K}| < |\mathcal{M}|$. Constuct an adversary $\mathcal{A}$ such that $\mathsf{Pr}[\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1] > \frac{1}{2}$.

6. Prove that, by redefining the key space, we may assume that Enc is deterministic without changing $\mathsf{Pr}[C = c|M = m]$ for any m, c.

7. Let Π denote the Vigenère cipher where the message space consists of all 3-character strings (over the English alphabet), and the key is generated by first choosing the period t uniformly from $\{1, 2, 3\}$ and then letting the key be a uniform string of length t. Define $\mathcal{A}$ as follows: $\mathcal{A}$ outputs $m_0 = aab$ and $m_1 = abb$. When given a ciphertext c, it outputs 0 if the first character of c is the same as the second character of c, and outputs 1 otherwise. Compute $\mathsf{Pr}[\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1]$ and conclude whether Vigenere cipher is perfectly secure or not.