Homework Assignment 1

1. *(multiplicative one-time pad).* We may also define a “multiplication mod $p$” variation of the one-time pad. This is a cipher $\mathcal{E} = (E, D)$, defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, where $\mathcal{K} := \mathcal{M} := \mathcal{C} := \{1, \ldots, p - 1\}$, where $p$ is a prime. Encryption and decryption are defined as follows:

$$E(k, m) := k \cdot m \mod p \quad D(k, c) := k^{-1} \cdot c \mod p.$$ 

Here, $k^{-1}$ denotes the multiplicative inverse of $k$ modulo $p$. Verify the correctness property for this cipher and prove that it is perfectly secure.

*(Hint: Check the proof in Theorem 2.9, page 33 in Katz and Lindell’s book.)*

2. *(Exercising the definition of a secure PRG).* Suppose $G(s)$ is a secure PRG that outputs bit-strings in $\{0, 1\}^n$. Which of are the following derived generators are secure?

(a) $G_1(s_1 \parallel s_2) := G(s_1) \land G(s_2)$ where $\land$ denotes bit-wise AND.

(b) $G_2(s_1 \parallel s_2) := G(s_1) \lor G(s_2)$.

(c) $G_3(s) := G(s) \oplus 1^n$.

(d) $G_4(s) := G(s)[0..n - 1]$.

(e) $G_5(s) := (G(s), G(s))$.

(f) $G_6(s_1 \parallel s_2) := (s_1, G(s_2))$. 
3. **(Simple secret sharing).** Let $E = (E, D)$ be a semantically secure cipher with key space $K = \{0, 1\}$ A bank wishes to split a decryption key $k \in \{0, 1\}$ into three shares $p_0, p_1, p_2$ so that two of the three shares are needed for decryption. Each share can be given to a different bank executive, and two of the three must contribute their shares for decryption to proceed. This way, decryption can proceed even if one of the executives is out sick, but at least two executives are needed for decryption.

(a) To do so the bank generates two random pairs $(k_0, k_0')$ and $(k_1, k_1')$ so that $k_0 \oplus k_0' = k_1 \oplus k_1' = k$. How should the bank assign shares so that any two shares enable decryption using $k$, but no single share can decrypt?

**Hint:** The first executive will be given the share $p_0 := (k_0, k_1)$.

(b) Generalize the scheme from part (a) so that 3-out-of-5 shares are needed for decryption. Reconstituting the key only uses XOR of key shares. Two shares should reveal nothing about the key $k$.

(c) More generally, we can design a $t$-out-of-$w$ system this way for any $t < w$. How does the size of each share scale with $t$?

4. Before HMAC was invented, it was quite common to define a MAC by $\text{Mac}_k(m) = H^*(k \| m)$ where $H$ is a collision-resistant hash function. Show that this is not a secure MAC when $H$ is constructed via the Merkle-Damgård transform.