Introduction to Cryptography: HW 3

1. (30 pt)Assume that you are given a secure pseudo-random function $F : K \times \{0,1\}^n \mapsto \{0,1\}^n$. Let $E : K \times \{0,1\}^n \mapsto \{0,1\}^n$ be symmetric key encryption scheme. Show that $E_K(M) = (r, F_K(r) \oplus M)$ for randomly chosen r is a secure encryption scheme. Specifically, Let A be an adversary (for attacking the IND-CPA security of SE) that runs in time at most t and asks at most q queries, these totaling at most q n-bit blocks. Then there exists an adversary B (attacking the PRF security of F) such that

$$Adv_{SE}^{ind-cpa}(A) \leq Adv_{F}^{prf}(B) + \frac{q^2}{2^n}$$

   (Hint: Condition on what happens if r is repeated)

2. (20 pt)Bellare-Rogaway Book: Problem 4.4

3. (20 pt)Bellare-Rogaway Book: Problem 5.1 (Correction $Y_i = E_K(Y_{i-1} \oplus M_i)$)

4. (30 pt) Bellare-Rogaway Book: Problem 6.3