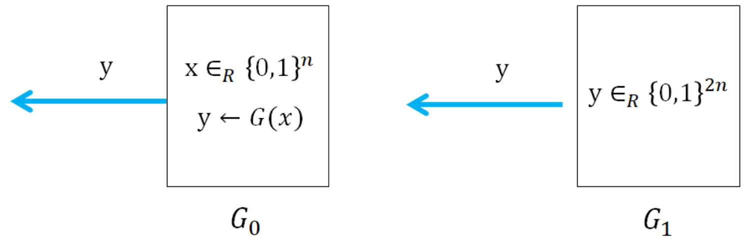
1. Read subsection 3.3.2, section 3.5, section 7.8 of the book. Give a short summary of each part.

2. Show that if $\mu(n)$ is negligible and $p(n)$ is polynomial then:

    1. $\mu(n) + 1/p(n)$ is non-negligible
    2. $\mu(n) \cdot p(n)$ is negligible.

3. Show that if $G : \{0,1\}^n \to \{0,1\}^{2n}$ is easy to invert (as defined below) then it is not a PRG. Do this by constructing a distinguisher D which distinguisher between G_0 and G_1. In more formal terms, construct a distinguisher D such that $|\Pr[D(G_1) = 1] - \Pr[D(G_0) = 1]| \geq 1/p(n)$ for some polynomial p.



Definition 1. *We say that $G : \{0,1\}^n \to \{0,1\}^{2n}$ is easy to invert if there exists a probabilistic polynomial time algorithm A, polynomial p such that*

$$\Pr[A(y) = x \mid y \leftarrow G(x),\ x \in_R \{0,1\}^n] \geq 1/p(n)$$

4. Suppose $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is a PRG, are the following also PRGs. Justify your answer by either providing an argument for why it is a PRG or produce a counterexample.

    1. $G'(r) := G(r \oplus 1^n)$
    2. $G'(r) := G(r) \oplus G(r \oplus 1^n)$
    3. $G'(r)$ is defined as the first $\ell - 1$ bits of $G(r)$
    4. Let G'' be a PRG, $G'(r) := G''(G(r))$

5. Let $M = \{1100, 0110, 1001\}$, let $F_k : \{0,1\}^n \to \{0,1\}^4$ be a pseudo-random function, and let $Enc(k, m) := (r, F_k(r) \oplus m)$ show that Enc is insecure against an adversary who is given acces to a validation oracle (an oracle which tells him whethever or not the ciphertext decrypts to a valid message).

6. If $M = \{0,1\}^4$, would the answer for the previous question still be the same.

7. Answer the following book questions: 3.9, 3.10, 3.13, 3.18, 3.22, 3.29

8. Jon, using the one-time mac, authenticated the message $m = 0$ resulting in tag $t = 51$ using $p = 183$. Can you forge a mac?