CS 202 - Introduction to Applied Cryptography **Fall 2016**

HomeWork 3

October 19, 2016 *Liangjian Chen*

Problem 1 **Solution:**

(a) Expansion rate: $|H(x)|= |G(1|x)|= 2|x|+2$.
Yes, it is a secure PRG.
Proof: Suppose, there is a efficient attack A against H. Then we use attack A against G. Assume $p_A = |\Pr[A(H(s)) = 1] - \Pr[A(r) = 1]|$, $p_B = |\Pr[B(G(s)) = 1] - \Pr[B(r) = 1]|$. If the beginning of s is 1, B is same with A. If th beginning of s is 0, B is always incorrect. So $p_B = p_A/2 + 0/2 = p_A/2$ which is still non-negligible. So it violets the assumption that G is a secure PRG. Thus H is a secure PRG.

(b) Expansion rate: $|H(x)|= |G(x_L|x_R)|G(x_R|x_L)|= 4|x|$.
No, it is not a secure PRG.
Proof: Assume it is a secure PRG, then construct $F = H(x_L|x_R)|H(x_R|x_L)$. According to assumption, F is secure. However, $F = G(x_L|x_R)|G(x_R|x_L)|G(x_R|x_L)|G(x_L|x_R)$, the first and fourth quarter of bits are same, second and the third quarter of bits are same. So we can easy construct a D, which check the first, fourth quarter, and second and third quarter. Then $\Pr = |1 - 2^{2n}|$ is non-negligible which contradict with F is a secure PRG. So it is not a secure PRG.

(c) Expansion rate: $|H(x)|= |G(z_L)|G(z_R)|= 2|G(x)|/2 * 2 = 4|x|$.
Yes, it is a secure PRG.
Proof: Suppose, there is a efficient attack A against H. Construct attack B against G as follow:
Since knowing $G(x)$ now, we are able to calculate $G(G(x)_L)|G(G(x)_R)$. Then use A to attack it. Since $H(x) = G(z_L)|G(z_R) = G(G(x)_L)|G(G(x)_R)$, B is a efficient attack which contradict with the assumption. Thus H is a secure PRG.

Problem 2 **Solution:**

Suppose we have an efficient algorithm A to attack H. Then construct B as follow: B choose m_0 and m_1 and send them to D, and get the cipher-text c from D. Then calculate $w_0 = m_0 \oplus c$. if $B(w_0)$ returns 1, A returns 0, otherwise, A returns 1. If the H in problem 1 is secure PRG, then its stream cipher is secure. Otherwise it is not secure.

Problem 3 **Solution:**

Assume attacker A breaks MM-CPA of E. Construct sequence D as follow, for every i, $m_0^i = m_1^{i-1}$, $b_i = i\%2$. According to hint, there must exist a i, that a distinguishes D_i and D_{i-1} with a probability $\epsilon'_A = \epsilon_A/p(n)$. Since D_i and D_{i-1} differ on a single cipher-text(m_1^i), the probability of the difference between m_1^{i-1} and m_0^i is non-negligible. Thus, in attack A', choose $m'_0 = m_1^{i-1}$ and $m'_1 = m_0^i$. Then A' is a efficient attacker of CPA of E.