**3.2** The adversary A just need to choose two strings m0 and m1 such shat |l(m0)|<|m1|. Now, if |c|<|m1| then A output 0, otherwise output 1. A always succeed because |l(m0)|<|m1|<|l(m1)|, thus m0 is chosen iff |c|<|m1|.

**3.6** Let G be a PRG with expansion factor l(n)>2n. Determine in each of the following cases, whether G’ is necessarily a PRG or not.

1. G’()=G(01…)
2. G’()=G(0|s|||)
3. G’()=G()||G(+1)
4. Yes, will post later. The idea is that: Given a string with length , =.

b) No. Let G’’()=G(01…) then G’’ is a PRG. Now let G’(s)=G’’(0|s|||)

=G(0|s|). We construct D as follow:

D(str)=1 if str=G(0|s|) and 0 otherwise.

We have ]=1 and =

It is trivial to see that their difference is not negilible, therefore G’ is not a PRG.

c) No. Let G’’()=G(01…) then G’’ is a PRG. Now let G’(s)=G’’(s)||G’’(s+1).

If sn=0 then G’(s)=G(01…)||G(01…). We construct D as follow:

Given a string str with length 2k, D(str)=1 if str[i]=str[k+i] for i=0,1,2,..,k-1 and 0 otherwise.

We have as half of the possible strings end with 0. **(1)**

If we randomly choose a string str with length 2l(n), the probability that it is equal to x||x for some string x with length l(n) is =. Therefore we have

]=  **(2)**

From **(1)** and **(2)** it is trivial to see that the difference is not negilible, therefore G’ is not a PRG.

**3.10** Let F be a length-preserving PRF. For the following keyed construction F’{0,1}nx{0,1}n-1->{0,1}2n, determine whether F’ is a PRF or not.

a) F’k(x)=Fk(0||x)||Fk(1||x)

b) F’k(x)=Fk(0||x)||Fk(x||1)

1. I believe the answer is yes, will give a proof later.
2. The answer is no. D will chooses two queries 0n-21 and 0n-1 and receives two strings c1 and c2. If the first half of c1 is equal to the second half of c2, output 1, otherwise output 0.

We have ]=1 and ]=, thus the difference is not negilible and F’ is not a PRF