Homework 2

Cryptography

CS 435

Ritvik Upadhyaya

Solution 1

Part A

Since k is concatination of two identical strings, even though the two strings are random, they will repeat in the key. So we can say that while encrypting the message m, we essentially have a key of length $\frac{n}{2}$. We know from the theorem, *2.10* that if the $|\mathcal{K}| \geq |\mathcal{M}|$ then the scheme is secure. But we know here that the key space is $2^{\frac{n}{2}}$ and the message space is 2^{n}. Hence the scheme is not perfectly secure!

Part B

The probability of the $\mathcal{A}$ winning the indistinguishability game is 1.
Assume that $\mathcal{A}$ provides two strings m_0 and m_1 for the indistinguishability game.
However, one of the strings has identical halves, i.e. it is composed of two same substrings. Eg. "abab". Whereas the other one does not have identical halves. In such a situation, $\mathcal{A}$ will be able to distinguish the two fairly easily. Hence the probability of winning is 1 for the $\mathcal{A}$.

Solution 2

Part A

To prove: $p(n) \cdot f(n)$ is a negligible function.
We know that the $f(n)$ is a negligible function.
That means, for every polynomial $q(n)$, there is an N for which all n $\geq$ N, $f(n) < \frac{1}{q(n)}$ is true.
We also know that a *(polynomial · polynomial) = polynomial*. Hence, $q(n) \cdot p(n)$ is also a polynomial.
Since we know that $f(n)$ is negligible, $f(n) < \frac{1}{q(n) \cdot p(n)}$
$\Rightarrow p(n) \cdot f(n) = \frac{1}{q(n)}$
Hence for every polynomial $q(n)$, there is an N for which all n $\geq$ N, $p(n) \cdot f(n) < \frac{1}{q(n)}$ is true.
Hence $p(n) \cdot f(n)$ is negligible.

Part B

To prove: $\frac{1}{(\frac{1}{f(n)} + \frac{1}{g(n)})}$ is a negligible function. We know that $f(n)$ and $g(n)$ are negligible functions.
That means, for every polynomial $p(n)$, there is an N for which all n $\geq$ N, $f(n) < \frac{1}{p(n)}$ is true.
Similarly, for every polynomial $q(n)$, there is an N for which all n $\geq$ N, $g(n) < \frac{1}{q(n)}$ is true.

From that we see,

$$f(n) < \frac{1}{p(n)} \qquad g(n) < \frac{1}{q(n)}$$

$$\Rightarrow \frac{1}{f(n)} > p(n) \qquad \frac{1}{g(n)} > q(n)$$

adding both the sides,

$$\frac{1}{f(n)} + \frac{1}{g(n)} > p(n) + q(n)$$

$$\Rightarrow \frac{1}{(\frac{1}{f(n)} + \frac{1}{g(n)})} < \frac{1}{(p(n) + q(n))}$$

Since polynomial + polynomial = polynomial, we see that $p(n) + q(n)$ is a polynomial.
Hence for every polynomial $q(n) + p(n)$, there is an N for which all n $\geq$ N, where $\frac{1}{(\frac{1}{f(n)} + \frac{1}{g(n)})} < \frac{1}{(p(n)+q(n))}$ is true.
Hence $\frac{1}{(\frac{1}{f(n)} + \frac{1}{g(n)})}$ is negligible.

Solution 3

We know that both $G_0(s)$ and $G_1(s)$.
Then we know $|Pr[D(G_0(s)) = 1] - Pr[D(r) = 1]| \leq negl_1(n)$
and $|D(G_1(s)) = 1] - Pr[D(r) = 1]| \leq negl_2(n)$
But we can write the second expression as, $|Pr[D(r) = 1] - Pr[G_1(s)]| \leq negl_2(n)$ since the value on LHS is magnitude of the difference. The magnitude will still be less than the $negl_2(n)$.

Using the triangle inequality $|x + y| \leq |x| + |y|$ on both the inequalities mentioned above,

$$|Pr[D(G_0(s)) = 1] - Pr[D(r) = 1]| + |Pr[D(r) = 1] - Pr[D(G_1(s)) = 1]| \leq negl_1(n) + negl_2(n)$$
$$\Rightarrow |Pr[D(G_0(s)) = 1] - Pr[D(G_1(s)) = 1]| \leq negl_1(n) + negl_2(n)$$

We know that $negl_1(n) + negl_2(n)$ will also be a negligible function. Hence,

$$|Pr[D(G_0(s)) = 1] - Pr[D(G_1(s)) = 1]| \leq negl(n)$$

for some negligible function $negl(n)$

Solution 4

Part A

Since G is a PRG, let us take a distinguisher D,

$$|Pr[D(G(s)) = 1] - Pr[D(r) = 1]| \leq f(n) \qquad (1)$$

where $f(n)$ is a negligible function. Let us assume that G' is not a PRG. For an input of length n, we see:

$$|Pr[D(G'(s)) = 1] - Pr[D(r) = 1]| > negl(n)$$

So G' output a string of length $n/2$.
But, if we take an input string of length $2n$, for any negligible function $negl$, we see,

$$|Pr[D(G'(s)) = 1] - Pr[D(r) = 1]| > negl(2n)$$

But from 1 we also can compute,

$$|Pr[D(G'(ss')) = 1] - Pr[D(r) = 1]| \leq g(2n)$$

Where $g(n) = f(n/2)$, and s' is the other half of the seed. Since $f(n)$ is a negligible function, so is $f(n/2)$. This means that g is a negligible function. This contradicts equation (1) hence our assumption that G' is not a PRG was wrong, hence G' is a PRG.

Part B

Let H be a PRG with expansion factor $l(n) > 2n$. And we define G(s) = H(the last half of the seed s).
We still know that G is a PRG, but we see that $G'(s) = G(s||1^{|s|}) = H(1^{|s|})$.
This will generate the same output everytime the *Gen* will be called. This is because, the seed will remain the same, as H will dump the first half of the seed, which is s. It will only have $1^{|s|}$ as the seed every time. Hence G' is not a PRG.

Part C

G' should be a PRG. Since G is a PRG, giving it seed $\overline{s}$ will still be a PRG. We know that $\overline{s}$ belongs to the same seed space as s. Hence $G(\overline{s})$ will work the same way as $G(s)$. The expansion factor will be the same as G, hence nothing will really change except that the input will be complemented.