Crypto Assignment 2

1. Suppose $F:\{0,1\}^n \Rightarrow \{0,1\}^{2n}$ is a PRG that is also an injection. Define G to be a deterministic polynomial-time algorithm such that for any n and any input $s \in \{0,1\}^n$, the output G(s) is F(s)||s.

Find a distinguisher such that for any negligible function negl
$|Pr[D(G(s))=1]-Pr[D(r)=1]| \le negl(n)$ is false.

Let D be a distinguisher as follows:
For any input X to D, let Y be the last n digits of X and Z be the first 2n digits of X. D outputs 1 if and only if $F(Y) \oplus Z = 0^{2n}$, that is, if F(Y)=Z.

For any input string s, since F is an injective function, by definition F(s) = F(s). Since the output of G(s) is F(s)||s, we can say $F(s)\|s = Z\|Y$ and $F(Y)=Z$, and so D outputs 1 for all input strings s. Therefore $Pr[D(G(s))=1]=1$

Since F is a PRG, when the input to D is a randomly and uniformly selected string $r=Z\|Y$, F(Y) will be indistinguishable from a randomly selected string from $\{0,1\}^{2n}$, and so $Pr[D(r)=1]=Pr[F(Y)\oplus Z=0^{2n}]=\frac{1}{2^n}$ since for each ith of 2n digits there is a $\frac{1}{2}$ probability that the ith digit of F(Y) equals the ith digit of Y.

We can then say that $|Pr[D(G(s))=1]-Pr[D(r)=1]| \ge 1-\frac{1}{2^n}$ and so $|Pr[D(G(s))=1]-Pr[D(r)=1]| \le negl(n)$ is false. Therefore G is not a PRG.

2.

Prove that $|Pr[D^{F_k(\cdot)}(1^n)=1]-Pr[D^{f(\cdot)}(1^n)=1]| \le negl(n)$ does not hold.

For all messages x, let $y=F_k(0\|x)$. Pick any $x_1 \in \{0,1\}^{n-1}$. Obtain $y_1=F_k(0\|x_1)$. Let D be a distinguisher that takes a message Z of length 3n, and outputs 1 iff $A=NOT(B)$ where A is the first n bits of Z and B is the next n bits of Z.

By definition, for any input x, $G_k(x)[0:n] = NOT(G_k(x)[n+1:2n])$. Therefore $Pr[D^{F_k(\cdot)}(1^n)=1]=1$ is true.

On the other hand, since f is uniformly chosen from $Func_n$, $f(x_1)$ is a uniformly chosen random string of length 3n. Therefore $Pr[D^{f(\cdot)}(1^n)=1]=\frac{1}{2^{3n}}$. Then
$|Pr[D^{F_k(\cdot)}(1^n)=1]-Pr[D^{f(\cdot)}(1^n)=1]|=1-\frac{1}{2^{3n}} > negl(n)$ and $G_k(x)$ is not a PFF.

3.

Show that the scheme is not EAV-Secure.

Let $m_0=00$ and $m_1=01$. In the adversarial indistinguishability experiment, the experiment uniformly selects $b \in \{0,1\}$ and generates $c \leftarrow Enc_k(m_b)$. Let A be an adversary that outputs 1 iff the final bit of c is 1, that is $A(c)=c_{|c|-1}$. From the definition of Π', $Enc_k'(m)=Enc_k(m)\|xor(m)$. Since $\oplus 00=0$ and $\oplus 01=1$, $Enc_k'(m_0)$ will end with 0 and $Enc_k'(m_1)$ will end with 1. Therefore when $b=0$, $b'=0$ and when $b=1$, $b'=1$.
The adversary is always right, so we can say that $Pr[PrivK_{A,\Pi}^{eav}(2)=1]=1>\frac{1}{2}+negl(2)$ and so Π' is not EAV-secure.

4.
Prove $|Pr[D(G'(s))=1]-Pr[D(r)=1]| \le negl(n)$ (1) for any PPT algorithm D.

Since G is a PRG with expansion factor l(n) for all $n \in Z^+$, we can say that
$|Pr[D(G(s))=1]-Pr[D(r)=1]| \le negl(n)$ (2) for any PPT algorithm D.

For any PPT distinguisher D, let D' be an algorithm defined as $D'(s)=D(NOT(s))$ for all s where |s| > 0. That is, D' produces the output that D(s) would, if D had been run on an input of NOT(s). Since (2) holds for any distinguisher including any D', the following sequence holds:

- $|Pr[D'(G(s))=1]-Pr[D'(r)=1]| \le negl(n) \Rightarrow$
- $|Pr[D'(NOT\, G'(s))=1]-Pr[D'(r)=1]| \le negl(n) \Rightarrow$ Since $G(s)=NOT(G(s))$
- $|Pr[D(G'(s))=1]-Pr[D'(r)=1]| \le negl(n)$ (3) Since $D'(s)=D(NOT(s))$

Further, $Pr[D'(r)=1]=Pr[D(NOT(r))=1]$ By the definition of D'. Since r is uniformly and randomly selected from $\{0,1\}^{l(n)}$, $Pr[D(NOT(r))=1]=Pr[D(r)=1]$
Plugging these in to equation (3), we arrive at the original formula, which was assumed to be true at the start. I.E. $|Pr[D(G(s))=1]-Pr[D(r)=1]| \le negl(n)$ is equivalent to
$|Pr[D(G'(s))=1]-Pr[D(r)=1]| \le negl(n)$ and therefore G'(s) is a PRG for all s where |s| > 0.

5a.

Show that for each $n \ge 6$, $Dec_k(Enc_k(m))=m$ for each $m \in \{0,1\}^n$.

By definition $(c,l)=Enc_k(m)=(m\oplus k\oplus l, l)$ and $Dec_k(c,l)=c\oplus k\oplus l$
So $Dec_k(Enc_k(m))=Dec_k(m\oplus k\oplus l, l)=(m\oplus k\oplus l)\oplus k\oplus l$
Note that the XOR operation is commutative, associative, is an identity element, and is a self-inverse.
Therefore

1. $(m\oplus k\oplus l)\oplus k\oplus l \Rightarrow m\oplus k\oplus l\oplus k\oplus l$ By associativity
2. $m\oplus k\oplus l\oplus k\oplus l \Rightarrow m\oplus k\oplus k\oplus l\oplus l$ By commutativity
3. $m\oplus k\oplus l\oplus k\oplus l \Rightarrow m\oplus(k\oplus k)\oplus(l\oplus l)$ By associativity
4. $m\oplus(k\oplus k)\oplus(l\oplus l) \Rightarrow m\oplus 0\oplus 0$ By self-inverse
5. $m\oplus 0\oplus 0 \Rightarrow m$ By identity

Therefore $Dec_k(Enc_k(m))=m$ for each $m \in \{0,1\}^n$.

5b.

Prove that the following equation does not hold: $Pr[Priv_{k\,A,\Pi}^{mult}(n)=1] \le \frac{1}{2}+negl(n)$
Let A be an adversary that chooses $M_0=(0^n,0^n)$ and $M_1=(0^n,1^n)$. A's strategy for guessing b is: A outputs $b'=0$ iff $c_0\oplus c_1$ contains exactly two 1 bits and otherwise outputs $b'=1$.

The probability that this experiment outputs 1 is equal to the probability that b=0 and $c_0\oplus c_1$ contains exactly two 1 bits plus the probability that b=1 and $c_0\oplus c_1$ does not contains exactly two 1 bits.

This probably isn't typical mathematical notation, but I will denote a string s containing exactly two 1 bits as $\Sigma s=2$. And so,
$Pr[Priv_{k\,A,\Pi}^{mult}(n)=1]=Pr[b=0]\cdot Pr[\Sigma(c_0\oplus c_1)=2]+Pr[b=1]\cdot Pr[\Sigma(c_0\oplus c_1)\ne 2]$

Note that $Pr[b=0]=Pr[b=1]=\frac{1}{2}$

From the scheme definition, $c_0\oplus c_1=(m_0\oplus k\oplus l_0)\oplus(m_1\oplus k\oplus l_1)$ .Note that l is chosen uniformly and randomly at encryption time, so l_0 does not necessarily equal l_1. As a result of the method by which l is picked, there is a $\frac{1}{n}$ chance that $l_0=l_1$ and a $\frac{n-1}{n}$ chance that $l_0\ne l_1$.

Where $l_0=l_1$, $c_0\oplus c_1=(m_0\oplus k\oplus l_0)\oplus(m_1\oplus k\oplus l_1)=m_0\oplus m_1$ and where $l_0\ne l_1$, $c_0\oplus c_1=(m_0\oplus k\oplus l_0)\oplus(m_1\oplus k\oplus l_1)=m_0\oplus m_1\oplus l_0\oplus l_1$. In the latter case, because each l contains exactly one 1 bit, $l_0\oplus l_1$ must be a string that contains exactly two 1 bits, I.E. $\Sigma(l_0\oplus l_1)=2$

Determine the probabilities that the experiment outputs 1 in each case: b=0 and b=1

Case b=0:

Find the probability that $c_0\oplus c_1$ contains exactly two 1 bits, $Pr[\Sigma(c_0\oplus c_1)=2]$. As previously proven, when $l_0=l_1$, $c_0\oplus c_1=m_0\oplus m_1=0^n$ which has no 1 bits. However, when $l_0\ne l_1$, $c_0\oplus c_1=0^n\oplus l_0\oplus l_1$. Since $l_0\oplus l_1$ contains exactly two 1 bits when $l_0\ne l_1$, $c_0\oplus c_1=0^n\oplus l_0\oplus l_1$ must also be a string with exactly two 1 bits when $n\ge 2$. So the probability that A guessed correctly when b=0 and $n\ge 2$ is $Pr[l_0\ne l_1]=\frac{n-1}{n}$.

Case b=1:

Find the probability that $c_0\oplus c_1$ does not contains exactly two 1 bits, $Pr[\Sigma(c_0\oplus c_1)\ne 2]$. Once again, when $l_0=l_1$, $c_0\oplus c_1=m_0\oplus m_1$, however here $m_0\oplus m_1=0^n\oplus 1^n=1^n$, so $c_0\oplus c_1=1^n$, which does not contain exactly two 1 bits when $n\ne 2$. However, when $l_0\ne l_1$, $c_0\oplus c_1=m_0\oplus m_1\oplus l_0\oplus l_1=1^n\oplus l_0\oplus l_1$. Since $l_0\oplus l_1$ contains exactly two 1 bits when $l_0\ne l_1$, $c_0\oplus c_1=1^n\oplus l_0\oplus l_1$ will not have exactly two 1 bits when $n\ne 4$. Therefore when $n\ge 5$, the probability that A guessed correctly when b=1 is $Pr[l_0\ne l_1]+Pr[l_0=l_1]=\frac{n-1}{n}+\frac{1}{n}=1$

Therefore
$Pr[Priv_{k\,A,\Pi}^{mult}(n)=1]=\frac{1}{2}Pr[l_0\ne l_1]+\frac{1}{2}1=\frac{1}{2}\frac{n-1}{n}+\frac{1}{2}=\frac{1}{2}(\frac{2n-1}{n})=\frac{2n-1}{2n}\ge\frac{9}{10}>\frac{1}{2}+negl(n)$ for $n\ge 5$
This is trivially also true for $n\ge 6$. Therefore the scheme does not have indistinguishable multiple encryptions in the presence of an eavesdropper.

And I didn't even need to use the hint.