1. Show if an encryption scheme is perfectly secret, then
$Pr[Enc_K(m)=c] = Pr[Enc_K(m')=c]$ $\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$

If $Pr[C=c]=0$, then $Pr[Enc_K(m)=c] = Pr[Enc_K(m')=c] = 0$

Assume $Pr[C=c] > 0$.

$Pr[Enc_K(m)=c] = Pr[Enc_K(m)=c \mid M=m] = Pr[C=c \mid M=m]$

$Pr[C=c \mid M=m] = \frac{Pr[M=m \mid C=c] Pr[C=c]}{Pr[M=m]}$

$= \frac{Pr[M=m] Pr[C=c]}{Pr[M=m]}$ (by the definition of perfect secrecy)

$= Pr[C=c]$

Similiarly, $Pr[Enc_K(m')=c] = Pr[C=c \mid M=m'] = Pr[C=c]$

Thus $Pr[Enc_K(m)=c] = Pr[Enc_K(m')=c] = Pr[C=c]$

2(a) Fix a uniform distribution on message space $\mathcal{M}=\{m_0, m_1\}$.

This, $Pr[M=m_0] = Pr[M=m_1] = \frac{1}{2}$

Consider $Pr[M=m_0 \mid C=\hat{c}] = \frac{Pr[C=\hat{c} \mid M=m_0] Pr[M=m_0]}{Pr[C=\hat{c}]}$

$= \frac{Pr[Enc_K(m_0)=\hat{c}] \frac{1}{2}}{Pr[C=\hat{c} \mid M=m_0] Pr[M=m_0] + Pr[C=\hat{c} \mid M=m_1] Pr[M=m_1]} = \frac{Pr[Enc_K(m_0)=\hat{c}]}{Pr[Enc_K(m_0)=\hat{c}] + Pr[Enc_K(m_1)=\hat{c}]}$

Given that $Pr[Enc_K(m_0)=\hat{c}] > Pr[Enc_K(m_1)=\hat{c}]$, $Pr[M=m_0 \mid C=\hat{c}] > \frac{1}{2}$

$Pr[PrivK^{eav}_{A,\pi}=1] = Pr[M=m_0 \mid C=\hat{c}] Pr[C=\hat{c}] + Pr[M=m_0 \mid C \neq \hat{c}] Pr[C \neq \hat{c}]$

$= Pr[M=m_0 \mid C=\hat{c}] Pr[C=\hat{c}] + \frac{1}{2} Pr[C \neq \hat{c}]$

$> \frac{1}{2} Pr[C=\hat{c}] + \frac{1}{2} Pr[C \neq \hat{c}] = \frac{1}{2}$

Thus the probability of winning is greater than $\frac{1}{2}$

2(b) To show def. III $\Rightarrow$ def. II, we prove the contrapositive.

As shown in 2(a), $Pr[Enc_K(m_0)=\hat{c}] > Pr[Enc_K(m_1)=\hat{c}] \Rightarrow Pr[PrivK^{eav}_{A,\pi}=1] > \frac{1}{2}$

2(a) continue. Similiarly, $Pr[Enc_k(m_0)=\hat{c}] < Pr[Enc_k(m_1)=\hat{c}] \Rightarrow Pr[PrivK^{eav}_{A,\Pi}=1] \leq \frac{1}{2}$

Combine it altogether: $Pr[Enc_k(m_0)=\hat{c}] \neq Pr[Enc_k(m_1)=\hat{c}] \Rightarrow Pr[PrivK^{eav}_{A,\Pi}=1] \neq \frac{1}{2}$ which is just the contrapositive.

Thus, def. III $\Rightarrow$ def. IV.

3(a) $m = 1000101001$. To encrypt 10001 to 10001, the key has to be 00000, However the key 00000 connot encrypt 01001 to 11001

3(b) To get a $m \in M(c)$, we can do $m = c \oplus kk$, where kk is a concatenation of a valid key. Thus, to get a $m \notin M(c)$, we can do $m = c \oplus kk'$ where $k \neq k'$, because when we encrypt m with some k, we have $c \neq m \oplus kk$

4(a) Let $p(n)$ be a positive polynomial.

Then $q(n) = p(kn)$ is also a positive polynomial

Since $f(n)$ is negligible, $\exists N$, s.t. $f(n) < \frac{1}{q(n)} = \frac{1}{p(kn)}$, $\forall n > N$

Substitute n with $\frac{n}{k}$,

we get $\exists N'$, s.t. $f(\frac{n}{k}) < \frac{1}{p(n)}$, $\forall n > N'$, so $f(\frac{n}{k})$ is negligible

(b) Let $p(n)$ be a positive polynomial

Then $q(n) = p(n^k)$ is also a positive polynomial

Since $f(n)$ is negligible, $\exists N$, s.t. $f(n) < \frac{1}{q(n)} = \frac{1}{p(n^k)}$, $\forall n > N$

Substitute n with n^k

we get $\exists N'$, s.t. $f(n^k) < \frac{1}{p(n)}$, $\forall n > N'$, so $f(n^k)$ is negligible.

(c) Since $f(n)$ is negligible, $\exists N$, s.t. $f(n) < n^{-c}$, $\forall n > N$, $\forall c \in \mathbb{R}$

Since $a(n)$ is polynomially bounded, $\exists N, d$, s.t. $a(n) < n^{-d}$, $\forall n > N$

Thus, $\exists N'$, $a(n)f(n) < n^{-(c+d)} = n^{-c'}$, $\forall n > N'$, $c' \in \mathbb{R}$,

so $a(n)f(n)$ is negligible