8. Refute. It follows from perfect secrecy that $|K| \geq |M|$.

9. True.

For any message m where $|m| = 1$, we have

$$Pr[M = \{\alpha\} \mid C = \{B\}] = Pr[K = k] \quad \text{s.t.}$$

$Enc_K(m) = C$, and $\alpha, B \in \{a, b, c, \ldots, z\}$. Then

$$Pr[K = k] = 1/26 = Pr[M = \{\alpha\}].$$

10. There are multiple ways to solve this problem. This is one way to construct a distinguisher D^{F_K}.

$\underline{D^{\overline{F_K}}(1^n)}$

return 1 if $\overline{F_K}(0^n) \oplus \overline{F_K}(1^n) = 1^n$

OW return 0

(10) Case 1: D is given F_K.

$Pr\left[D^{F_K}(1^n)=1\right] = 1$ since for all F_K, the distinguisher is able to identify this is not a random function.

Since $F_K(0^n) \oplus F_K(1^n) = G_0(K) \oplus 0^n \oplus G_0(K) \oplus 1^n$

$= G_0(K) \oplus G_0(K) \oplus 1^n$

$= 0^n \oplus 1^n$

$= 1^n$

Case 2 D is given a truly random function f.

$f(0^n) \oplus f(1^n) = 1^n \iff f(0^n) \oplus 1^n = f(1^n)$.

Since f is totally random $f(0^n) \oplus 1^n$ occurs uniformly since it is dependent on $f(0^n)$. Therefore the prob $f(1^n) = f(0^n) \oplus 1^n$ is $1/2^n$.

$$\left| Pr\left[D^{F_K}(1^n)=1\right] - Pr\left[D^{f}(1^n)=1\right] \right| = 1 - 1/2^n$$

#13. Part b note.

Attacker A has oracle access during $\text{PrivK}^{CPA}_{A,\Pi}$.

Therefore if A encrypts m_0, m_1 there are two cases.

Case 1. $Enc(m_0)$ or $Enc(m_1)$ returns m_b.

If $Enc(m_0)$ or $Enc(m_0)$ returns m_b then attacker can identify b with $pr = 1$. But attacker a can query Oracle $q(n)$ times. Therefore the prob of success is

$$\frac{q(n)}{2^n}.$$